Decoding EU Digital Strategic Autonomy

Gérard Pogorel, Antonios Nestoras, Francesco Cappelletti

▶ **To cite this version:**

Gérard Pogorel, Antonios Nestoras, Francesco Cappelletti (Dir.). Decoding EU Digital Strategic Autonomy. 2022. hal-03713230

HAL Id: hal-03713230
https://hal.science/hal-03713230

Submitted on 28 Sep 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Techno-Politics Series: 1

Decoding EU Digital Strategic Autonomy

Sectors, Issues, and Partners

Edited by
Gerard Pogorel
Antonios Nestoras
Francesco Cappelletti

Series Editor
Antonios Nestoras

Techno-Politics Series: 1

Decoding EU Digital Strategic Autonomy

Sectors, Issues, and Partners

Edited by
Gerard Pogorel
Antonios Nestoras
Francesco Cappelletti

Series editor
Antonios Nestoras

Published by the European Liberal Forum. Co-funded by the European Parliament.

The views expressed herein are those of the author(s) alone. These views do not necessarily reflect those of the European Parliament or the European LiberalForum.

The European Liberal Forum (ELF) is the official political foundation of the European Liberal Party, the ALDE Party. Together with 47 member organisations, we work all over Europe to bring new ideas into the political debate, to provide a platform for discussion, and to empower citizens to make their voices heard. Our work is guided by liberal ideals and a belief in the principle of freedom. We stand for a future-oriented Europe that offers opportunities for every citizen. ELF is engaged on all political levels, from the local to the European. We bring together a diverse network of national foundations, think tanks and other experts. In this role, our forum serves as a space for an open and informed exchange of views between a wide range of different EU stakeholders.

© European Liberal Forum, 2022

ISBN: 978-2-39067-033-9 / 9782390670339
ISSN (print): 2791-3880
ISSN (online): 2791-3899

ELF has no responsibility for the persistence or accuracy of URLs for externalor third-party internet websites referred to in this publication and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Contents

Foreword

Daniel Kaddik, ELF Executive Director

DIGITAL STRATEGIC AUTONOMY: HOW TO UNLEASH THE POTENTIAL OF THE EUROPEAN DIGITAL MARKET

It may seem challenging to talk about strategic autonomy at a time like this. Russia's military aggression against Ukraine – a sovereign democratic country on the European continent and the EU's associated partner – has brought into focus the most fundamental assumption of the European project: the value of peace. Furthermore, this large-scale multi-faceted crisis has, once again, challenged the EU's ability to act in line with its interests and values in an increasingly interconnected world.

One of the Union's main tasks is to ensure that the bloc of free democracies is strong enough to stand up against illiberal currents and regimes that try to undermine its free and peaceful coexistence and cooperation. With international tensions growing and reshaping the balance of power in the world, the challenge is to develop strategies that in a long run support and strengthen this *raison d'être* of the Union. Critical dependency on untrustworthy partners or even ethical opponents undermines Europe's political credibility, integrity, and its freedom to choose its alliances. In the changing international security and economic landscape, the notions of 'sovereignty' and 'autonomy' have thus been acquiring an unprecedentedly central role in EU political and policy agendas.

'Strategic autonomy' has already become the dominant conceptual framework setting the EU's long-term development. Since 2013, the Council and the Commission have been referring to it as a possible European response to global developments that require the bloc to rely more on its own capabilities and resources. Until recently, the concept primarily concerned the security and defence domain, particularly in the context of relations with NATO and potentially decreasing US involvement in Europe's security concerns. This primary application of the term has gained in relevance and acquired new, urgent meaning since the peace on the European continent was shattered by Russian aggression. The EU has shown an unprecedented unity in lifting some of its longstanding taboos and making difficult choices, unthinkable in peaceful, less critical times. This is a big step and certainly one to celebrate. Yet this is not enough.

The ability to protect ourselves and provide our citizens and economies with necessary resources without compromising our core principles – this is a task which we cannot postpone any longer. While the autonomy in security concerns is yet to be achieved, defence is not the only domain in which the EU needs strategic sovereignty. In the past years, the emphasis on sovereignty has started to spill over into other 'strategic' domains and topics: from economy to climate, from industry to manufacturing and critical infrastructures. Another critical field is the digital domain, which is a lever for the fourth industrial revolution, while at the same time an international battlefield of its own. The challenges in this regard stem from technological rivals, or threats from traditional villains, spreading disinformation and cyberattacks, while cybercrimes are increasingly affecting our daily lives.

The increasing digitalization of our societies, affecting both private and public interests, is a major factor in shaping Europe's future. While new and future technologies will serve the purpose of making our daily lives better, they are effective and reliable only in a peaceful and stable world. Both the Ukraine war and the economic crisis that followed the COVID-19 pandemic have demonstrated the existing limitations and risks of the EU's dependency, which affect the supply chain and the

manufacturing of essential goods. In many ways, a future-oriented Europe thus had to come to terms with reality. If no steps are taken to address the shortcomings, Europe will remain in strategic risk. In this new context, thinking in terms of strategic autonomy seems to be the only viable solution for a long-term perspective.

In respect of digital strategic autonomy, the EU needs to ensure that the many strategies of the individual Member States converge within a co-ordinated approach. Aimed at strengthening Europe's sovereignty and autonomy, this umbrella project will become an EU strategy for both its internal and external interactions and partnerships. This decision towards a united approach has already been taken, but the current situation demands a decisive step forward.

Strengthening sovereignty has nothing to do with protectionism, however. Quite the opposite: autonomy does not mean isolation but better cooperation. Digital autonomy is impossible without a robust consensus framework with partners and allies, and finding the right partners for cooperation is a central part of a successful strategy. At the same time, Europe's thoughtful cooperation with technological rivals in the digital domain should be rebalanced in favour of a more assertive stance.

To achieve these goals, institutions will have to address the need for solid industrial policies and substantial industry inputs. This means having a strategy that implies strong incentives and regulatory requirements where the free market can play a central role, while any steps should be innovation-oriented from both a short- and long-term perspective.

This framework will allow us to unleash the full potential of the digital internal market. It will do so by fostering a paradigm shift where the regulatory approach to digital policies will follow a bottom-up logic and listening to the industry will be the main success factor. At the same time, it will encourage good practices in the industrial field that will foster a new mindset for both stakeholders and investors. While we might not have a European Silicon Valley, we can have many SMEs contributing together to create a more resilient EU digital architecture, encompassing (cyber)security, new technologies such as 6G and AI, quantum computing and overall for our societies.

This study, published by the European Liberal Forum and edited by Emeritus Professor Gerard Pogorel, Antonios Nestoras and Francesco Cappelletti, addresses a range of key concerns and opportunities associated with developing the EU's digital strategic autonomy, from research and education to strategic deployment of resources. The collection of up-to-date analytical papers written by leading experts provides food for reflection and a better understanding of what the EU needs to do to strengthen its position in the international digital domain of tomorrow. A long-term strategy for the EU's digital autonomy is needed right now. We, liberals, believe that a free market and better regulations to ensure 'smart' policies are the only way to unleash the true potential of our digital future, To fit our digital tomorrow, we have to start today.

Editorial: Digital Strategic Autonomy, A Crucial Imperative for Europe

Gerard Pogorel, Emeritus Professor of Economics & Management
Antonios Nestoras, Head of Policy and research, ELF
Francesco Cappelletti, Policy and Research Officer, ELF

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

INTRODUCTION

European Strategic autonomy was first used in the context of EU security and defence, and remained a concept that was not explicitly defined until it gained broader strategic ambition in the 2016 EU Global Strategy. Since that date, successive events and developments have given it yet greater traction and urgency. The Covid-19 Pandemic, concerns about the US's grip on international politics, trans-atlantic and trans-Pacific tensions in interrnational trade, the recognition of China as a strategic rival, compounded by concerns around dominance in world digital markets – all these have resulted in initiatives aiming to strengthen Europe's position as an autonomous actor and its status and role in world politics and the global economy. The Russian war of aggression in Ukraine now decisively highlights the necessity of immediate and longr-term policy requirements and choices for Europe.

ELF's aim in publishing this book is to offer an in-depth appraisal of world industry and trade realities in this drastically changed context. The future of today's intricate networks of information, knowledge, technologies, value chains, and markets is being questioned. This calls for an evaluation of critical economic and political change and opportunities and the precise definition of the EU's objectives and imperatives in a world that is very different from the one we lived in up to 2021. It also calls for a re-evaluation and recalibration of the geography of cooperation, within Europe and, increasingly, with its partners across all continents. Our economies will require a rebalancing of our industries and the innovation dynamics of competition and innovation, along with voluntary initiatives at Member State and EU levels. Simplistic views will not suffice. The reliance on free trade and open markets, internally and externally, must be re-examined; but this does not mean that the benefits of this model no longer exist or that, in our enlightened wisdom, we can now define a single, best economic path. Achieving an informed balance still is, and will continue to be, the key. More than ever, we still need at EU and Member State levels the operation of the collective intelligence of our democracy, solid and effective exchanges between political and social institutions, with knowledge centres and industries, pooling our collective expertise and avoiding illusory, easy solutions.

This book focuses on digital strategic autonomy. The EU's own smart digitisation, alongside its industry, energy, defence and sustainability policies, is a precondition of its strategic independence. We evidence here the increased effort of EU institutions to strengthen the internal digital single market. In this context, a European Digital Strategic Autonomy (DSA) policy has come to be considered and is being defined. Achieving European DSA encompasses a set of initiatives to strengthen the sovereignty of the EU in determining strategic sectors. The goal of strategic autonomy in relation to digital transformation is to promote the European digital internal market, ensuring that the deployment of innovative technologies will fit the economic, regulatory, and political framework while fostering competitiveness and openness at a global level. Ultimately, it involves achieving and strengthening independence and safeguarding resilience and security of

digital means and infrastructures across the Union. To achieve digital autonomy, the EU promotes internal programmes and European ecosystems in strategic fields such as connectivity, the supply and manufacturing of components, hardware and software, while ensuring that the overall deployment of innovative infrastructure (such as next-generation networks) and innovative technologies are embedded into a fair and digital strategic transition.

2022: HOW DOES EUROPE DEFINE ITS DIGITAL STRATEGIC AUTONOMY?

The implementation of what Europe means by its 'strategic autonomy' is under way. Broadly speaking, it is 'the capacity to act autonomously when and where necessary and with partners wherever possible' and to 'rely on one's resources in key strategic areas' as well as 'to choose when, in which area, and if, to act with like-minded partners' (Council's Conclusion, 2016; EPRS, 2020).

Notably, the concept of strategic autonomy, born from security and defence considerations, has spilled over from the security realm into the connected domains of economics, digital, energy, climate, and migration. It was affirmed as a policy objective of the 27 EU Member States in 2020 among the 'key objectives of the Union' (European Council 2020). With the changeover in the international landscape, culminating with war at the heart of Europe, atrategic autonomy takes centre stage.

What should be highlighted here is that, whatever the critical circumstances, strategic autonomy is not synonymous with defensive protectionism – that is, shielding domestic industries or markets 'as is'. On the contrary, it is a set of decisive initiatives supporting 'sovereignty' at European level and in a forward-looking way. Sovereignty entails elements of autonomy (Tocci, n.d.). It remains a set of attributes that are being urgently pursued: *the condition of being able to act autonomously, without influence of foreign parties and without the reliance on foreign parties to achieve particular objectives in specific strategic sectors.*

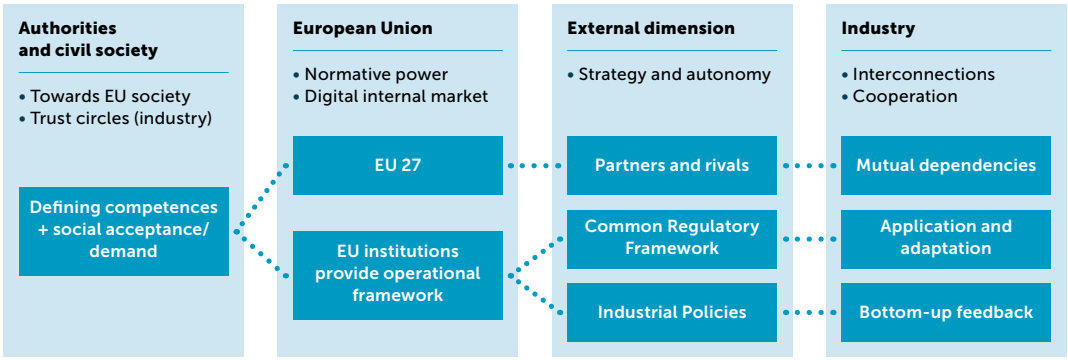
Difficulties are abundant. The current war in Europe acts as a litmus test for previous choices, the consequences of which were greatly underestimated or ignored.

The external dimension of strategic autonomy requires a clear awareness and identification of EU's partners, rivals, and potential enemies. In strategising a European approach to autonomy, we therefore need to make a distinction between:

- Areas where the local European dimension should prevail, whether concerning autonomous decision-making, local production, or overarching legislation;
- Areas where ecosystems of production and trade involving allied partners are put in place by industries, possibly with government assitance, to put together competencies and enjoy the benefits of scale, the division of labour and open trade;
- Areas where, on the basis of thorough investigations and assessments, and to the best of our knowledge, it is possible to do business with non-allies, or rivals, keeping in mind that it is necessary to dispose of *mutual market dissuasion* instruments, so that international trade relations are based on mutual trust and maintain an open playing field.

This implies a common vision and regulatory framework among the EU's 27 Member States. It creates a level playing field where similar actors can act competitively in a safe environment, where dynamics can reward industrial innovative leaders. In turn,

FIGURE 1: **Dimensions of 'Strategic Autonomy Europe' and sources of power**



this can help provide an indispensable competitive advantage for European companies as they operate in the global market, while at the same time acting as a deterrent to foreign companies, which will have to play by the rules of the internal market.

SUSTAINABLE SOVEREIGNTY IMPLIES PARTNERS, TRUST AND BALANCE (OF POWER?)

It is clear that strategic autonomy today has several dimensions. The first is high-level: the EU's International Relations doctrines. These aim to define *autonomy* and a *strategy* in the context of the EU's external relations, in political, defence, and economic terms. Moreover, as part of the European policy objectives, concepts of politics and power are now considered relevant when discussing strategic autonomy (Dahl, 1957).[1] While not associating autonomy with protectionism, it is nevertheless necessary to identify the attributes of power and its sources. Since strategic autonomy involves projecting power outward, the challenge, in this context where multiple sources of power interact, is to preserve as much virtuous competition and as many open international markets as possible.

The second dimension relates to the set of industrial and regulatory initiatives that aim to make the EU a digital continent. Thirdly, strategic autonomy as a prerequisite has a social dimension whereby EU Member States try to structure a common regulatory framework that strengthens European social standing in the world market and reinforces critical areas of EU competence.

STRATEGIC AUTONOMY SUPPOSES SUBSTANTIAL OPERATIONAL INDUSTRY INPUTS INTO PUBLIC INDUSTRIAL POLICIES

Digital Strategic Autonomy relates to different sectors within the internal digital market. It includes, for instance, the requirements for Mobile Network Operators (MNOs) to compete within the European market without the disadvantages of non-EU competitors. In the field of components manufacturers, the internal market is progressiveley reshaped according to different mindsets, involving stakeholders in a creative process supported by policymakers. When it comes to service providers, the EU has taken some steps in achieving control (thus a certain level of autonomy) within the Single Market by introducing the DSA/DMA.

The interconnected world we recognise today makes each nation's social and commercial interactions part of an intricate web of *mutual dependencies*. Digitising European economies, in sectors such as critical infrastructure and procurement (hardware or software) is taking place at EU level. The European macro-area competes and succeeds on the global scene. In the current context, favourable deals are often made with multinationals from allied countries to take advantage of their competencies. In such areas, *multiple sourcing* is the condition of resilience.

DSA CANNOT WORK WITHOUT A ROBUST CONSENSUS FRAMEWORK WITH PARTNERS AND ALLIES, BETWEEN THEM, AND REGARDING 'RIVALS'

The EU's Digital Strategic Autonomy cannot work without a robust consensus framework with partners and allies. Thus, supporting alliances and tackling strategic rivalries are relevant in the context of DSA. In developing such relationships, partners and allies promote *trust circles* among partner countries, combining industry strategies and geopolitical objectives. This implies avoiding hard-power confrontation (and protectionism), between Member States and between Member States and third parties.

Companies are factor-combining entities, not policy-making entities, whatever their goodwill and good intentions

A difficult question in the digital area is how far the world is going in 'de-coupling', creating blocks resulting in an*economic multipolarity.* First, it is absolutely necessary to avoid such a development between allies. A clear strategy is also needed in respect of rivals. We need to take firm positions on issues that underlie the success of the internal market. Regarding the US, Canada, the UK, Japan, South Korea, Taiwan, Australia, New Zealand, and other allies, partnerships must be strengthened and upgraded. In respect of China, on the other hand, it is necessary to have a straightforward understanding of what Europe can do, the overarching imperative being EU resilience, the capacity of absorbing exogenous shocks, aiming at strengthening strategic domestic capabilities in digital-related sectors.

A DEFINING MOMENT FOR EUROPE'S FUTURE

The challenge for EU strategic autonomy today is to preserve as far as possible the benefits of a rule-based free market, as international conflicts, defence imperatives, multiple calls on public finances, and social and political uncertainties exert ever-stronger pressures. The industry input into public industrial policies is key in achieving a reciprocal '*top-down+bottom-up*' approach, leading the EU towards a long-term innovation-oriented strategy. Positive factors are emerging. SMEs have greater opportunities to scale up. Although a lot still remains to be done, the virtuous circle of training, digital skills, change management know-how and digital investments has been triggered. The long-lasting debate on Europe as a relevant market and the right level of understanding of the competition vs digital champions dilemma is better understood.

Strong regulatory initiatives are under way at EU 27 level for enhancing the internal market and digital industry, along the current path towards digitalisation. The creation of *digital fora* combiing education institutions, digital industries, investors and consultants could speed up the process.

The following examples of EU Acts and regulations list *sources of strategic autonomy* for Europe.

TABLE 1: **Sources that contribute to strengthening European strategic autonomy**

EU's Political and Institutional Progress
European Monetary Union (1992)
European External Action Service (2010)
European Banking Union (2012)
Common Agricultural Policy / Common Fisheries Policy (2014)
Common Security and Defence Policy / PESCO (2017)
Transnational Electoral Lists in 2024 elections
EU's Soft Power Instruments – Normative Power Europe
NIS Directive (2016)
GDPR (2018)
Green Deal (2019)
A.I. Regulation (2021)
DSA + DMA package (2022)
EU's Technological and Industrial Strategic Autonomy
Roaming Regulation (2017)
European Electronic Communications Code (2018)
E.C. – A New Industrial Strategy for Europe (2020)
Fit 4/55 (2021)
European Industrial Alliances
5G Action Plan (2016) / Horizon Europe (2020)
Proposal for Batteries and Waster batteries regulation (2020)
Cybersecurity Act (2019)
Proposal for NIS2 directive (2021)
Proposal for European Chips Act (2022)
Proposal for EU Cyber resilience (2022)
Single Market Emergency Instruments (2022)

POLICYMAKERS STRATEGISING EUROPE: DSA IMPLIES VITAL REGULATORY REQUIREMENTS

Achieving European Digital Strategic Autonomy at a time of high risk and uncertainty calls for the definition of a *strategic intent*. This means:

- Let industry do what it does best, combine resources, select, and conquer markets.
- Put in place incentives to help and comply with high-level imperatives, when and where needed.

While supporting these processes, policymakers should not think in terms of 'planning': instead, an adjustable, free and open market will foster a pan-European approach among EU digital industries, allowing institutions and industry to align themselves with a common view, integrated within the internal market, in a competitive and adaptative manner.

On the basis of scientific knowledge, industry experience, public support, and risks assessment, 'trust circles' combine factors within a strategic intent. European institutions do well to send out strong signals, as is the case with regulations on the digital and microchip markets. Major projects for European digital industry embody a 'strategic' dimension. The industrial component remains central to the design and above all to the implementation of these plans. Industrial policy and regulation are only one pillar of EU economic policy, more significant than before but still just one pillar. The other pillar is innovation dynamics through competition. The two intersect in trust circles within which shared strategic intent and market competition combine. The trust circle is a versatile concept, as its boundaries are subject to constant redefinition and movement. But it helps testify movement by walking and improve through implementation. European digital investments are also made more dynamic by management flexibility. Companies are factor-combining entities, not policymaking entities, whatever their goodwill and good intentions. It is up to elected governments to regulate, incentivise, to achieve democratically determined macroeconomic societal goals. Conversely, it is up to governments to set broad principles and restrain from micro-managing.

CONCLUSIONS AND POLICY RECOMMENDATIONS

Fostering digital industry starts with a strategic concept at the managerial level. DSA cannot happen without firm EU policies and a robust civilisation, culture and democracy. Strategic investments go hand in hand with strong social and political cohesion.

We suggest the following conclusive framework:

a) DSA is not protectionism: DSA cannot work without a strong consensus framework with partners and allies. Whatever the critical challenges Europe is facing, strategic autonomy must be considered in its EU wide dimension. Moreover, given current geopolitical realignments, building strong cooperation among partners and allies is equally imperative. Competences and objectives are brought closer to one another. Trust circles and knowledge and industrial ecosystems are built. DSA must be long-term, innovation-oriented.
b) DSA implies strong regulatory requirements, concerning, data, networks, cybersecurity.
c) The telecomunications market regulation should be revisited to allow operators to contribute more to digital infrastructure deployment
d) DSA supposes strong industry and research centre inputs to public and economic industrial policies. More than ever, public policies must be

informed by the knowledge accumulated and developed by research centres and industries. An informal framework for building trust circles between industry and research should be put in place in parallel with public policy bodies, in particular regarding international cooperation and negociations

e) DSA means a delicate power balance with China. Given the reciprocal dependencies between Europe and China, a clear, evolving, policy framework should be put in place and its effects monitored in real time.

OVERVIEW OF THE STUDY

This study, organised in two parts, reflects on several aspects of the European Digital Strategic Autonomy. It considers different factors of the industry, infrastructure, and social transformative effects that digitisation has on the EU. It explores the interactions of digital technologies with economic and policy issues, assesses the main challenges and risks, describes best practices and viable policy options.

Part 1 – EU Digital Strategic Autonomy

In this first section, invited authors analyse DSA aspects of a series of digital issues. In the second part, authors present the point of view of the main political and economic partners of Europe. The aim here is to understand how Europe's partner governments envisage their own digital policy, their vision of EU initiatives and orientations, and which items loom highest on their discussion agenda with the EU.

David Bounie, Telecom Paris-Institut Polytechnique de Paris
Digital Strategic Autonomy: Industry Views and EU Policy Implications

Augusto Preta, ITMedia Consulting
Digital Content and European Culture: A New Paradigm?

Jan Büchel and Barbara Engels, German Economic Forum
The Importance of the Data Economy for Europe's Digital Strategic Autonomy

Julian Kamasa, ETH Zürich
Microchips as a Vital Element of EU Strategic Autonomy and Digital Sovereignty

Erik Bohlin, Chalmers University, and Simon Forge, SCF Associates Ltd
The EU Need for 5G Cybersecurity Capabilities

Paul Timmers, Oxford University affiliate
Resilience from a Strategic Autonomy Perspective

Arno Pons, The Digital New Deal Think Tank, Paris
EU Digital Strategic Autonomy: The French Experience

The chapter by Bounie analyses industry perspectives on DSA. It looks into the impacts of the changes in the international landscape and the enhanced EU strategic autonomy imperative. Businesses are by definition interdependent technology assemblers, which, to be competitive, must create and have access to the best technologies, whether manufactured in France, Europe or worldwide. Autarky is not an option. Ecosystems must extend within trust circles, among partners sharing the same values or at least be linked by reciprocal interests.

Preta's chapter focuses on Europe's cultural and audio-visual digital identity as a key dimension of its sovereignty policies. Its cultural heritage, landmarks

A single European data economy is a key part of Europe's digital strategic autonomy

and landscapes are without peer. They are assets worth building upon. Europe uniquely qualifies as an 'identity of cultural diversity'. The rationale for European support for its cultural activities illustrates, for Europeans themselves and for the entire world, a distinct civilisation, cultures worth showing and defending. This awareness, within Europe and internationally, is central to the affirmation of European sovereignty.

The chapter by Büchel and Engels analyses the importance of the data economy for Europe's Digital Strategic Autonomy. A single European data economy is a key part of Europe's digital strategic autonomy. Digital sovereignty and hence also data sovereignty are prerequisites for the ability to foster the innovative capacity and competitiveness of the European economy. To build a data economy acting as an engine for innovation and new jobs, the EU should combine fit-for-purpose legislation and governance to ensure the availability of data, with investments in standards, tools, and infrastructures such as Gaia-X as well as competences for handling data. The authors emphasise this must happen quickly, but not mindlessly. Europe has no time to lose.

Kamasa's chapter delves into the role of microchips as a vital industry, as the interplay of a pandemic, extreme weather events, and geopolitical crises and power dynamics have exposed the fragile networks underpinning the semiconductor industry. Because microchips are almost indispensable in daily life, the current shortage raises questions about supply chain security. He analyses how far Europe can seek to strengthen its own production capacities to avoid these types of vulnerabilities in the future.

The chapter by Bohlin and Forge investigates the EU's need for 5G cybersecurity capabilities. The mobile cellular technology that lies behind 5G networks promises both significant risks as well as promising potential rewards in terms of strategic autonomy. 5G may intensify the hazards for ordinary people, threatening their privacy and wellbeing, following the increasing seriousness of breaches. To respond adequately, novel trust models are needed for 5G that express enhanced security paradigms for 5G networks. These should cover both threats to physical infrastructure and personal lives – because the ultimate conclusion is that the most vulnerable of the core critical infrastructures in the increasingly digitalised EU may soon be the 5G networks themselves, posing a key strategic risk for different sectors.

Paul Timmers's chapter exposes the role of cybersecurity and resilience in a strategic autonomy perspective. Cybersecurity vulnerabilities and incidents are an ever-growing and profound threat to the functioning and resilience of our economy, society, and democracy. It is increasingly clear that cybersecurity threats affect the core of the EU's and Member States' autonomy. A three-pronged strategy on EU cybersecurity policy is needed from a strategic autonomy perspective: fill the gaps; build the bridges between policy interventions; assert our approach to cybersecurity, that is, the EU in the world. Concrete, integrated, and internationally oriented policy action is urgently needed. Cybersecurity resilience in a strategic autonomy perspective requires strategic, proactive, integrated, and continuous policy development. Achieving this at EU and national level should be a top priority.

The chapter by Pons provides insights into how the French experience of regulation can help design an open market for digital services.

Europe uniquely qualifies as an 'identity of cultural diversity'

Part 2 – International Partners' Views

This section of the book aims to reveal how Europe's partners' governments envisage their digital policy, their vision of EU initiatives and orientations, and which items loom highest on their discussion agenda with the EU.

Daniel S. Hamilton Johns Hopkins University, SAIS
Reconciling 'Digital Strategic Autonomy' with Transatlantic Partnership: A US–EU Agenda

Henry Ergas, University of Wollongong, and Joe Branigan
Digital Strategic Autonomy: An Australian Perspective

Simon Forge, SCF Associates Ltd
The United Kingdom and the EU: a Bet on the Future for Europe's Strategic Autonomy

Huai-Shing Yen, Chung-Hua Institution for Economic Research, Taiwan
Digital Autonomy and Taiwan–EU Partnership

Kiyotaka Yuguchi, Sagami Women's University
Japan: Digital Sovereignty as an Element of the Economic Security

Hamilton's chapter explores how renewed EU–US solidarity in the face of Russia's war on Ukraine and multi-dimensional challenges posed by China are shifting EU debates over 'strategic autonomy' to discussion of European 'strategic responsibility.' This is most noticeable in the areas of defence and energy, but it is also affecting EU notions of 'digital strategic autonomy.' US–EU commercial disputes continue, but now also in the context of transatlantic unity rather than division, amidst growing recognition that the transatlantic economy is the geo-economic base for both sides of the North Atlantic in an age of disruption. This mixture of competition within a frame of deeply integrated cooperation plays itself out across different sectors of the digital economy. Four sectors merit particular attention: ICT and cloud services; semiconductors; artificial intelligence; and clean technologies.

The chapter by Ergas and Branigan delineates how Australia has, in the recent period, taken a hard look at challenges to its independence and sovereignty. What are its methodologies and how does it come up with its distinctive policy decisions? Since the 1990s, and especially over the last two decades, Australian policymakers have substantially altered the way the issues arising in respect of strategic industrial capabilities are considered, notably in relation to national defence. The chapter focuses on identifying those capabilities which, if not present, would individually or collectively seriously increase Australia's vulnerability. This assessment is undertaken by examining the 'deprival value' of capabilities through careful scenario analysis.

Forge's chapter reveals how the UK's position in an EU digital autonomy context is dominated by Brexit and how this in turn is affected by the war in Ukraine. A possible UK interaction offering support for an EU digital strategic autonomy should come from harnessing very specific parts of the UK economy – firstly R&D resources, primarily those in the universities and then high technology industries, specifically defence, semiconductor technology design and manufacturing plus media production, especially graphics.

The chapter by Huai-Shing Yen identifies Taiwan's policy and concerns around digital trade issues and outlines Taiwan's perception of Europe's digital initiatives and orientations. The recent disinformation

warfare undertaken by Russia as part of its invasion of Ukraine further underscores the threat to and importance of digital autonomy. As Taiwan plays a central role in the world's digital economy, strong linkages are important for Europe. Based on both the EU and Taiwan's efforts in promoting digital autonomy, the author offers several recommendations, including creating a systematic dialogue and information-sharing mechanism, as well as forging partnerships in R&D collaborations, talent development, and data/privacy governance.

Kiyotaka Yuguchi's chapter details how the Japanese have long believed that water and safety are free except for natural disasters. The succession of international crises now has made the Japanese acutely aware of issues of economic security. Concerns about supply chain and digitalisation have been recognised. Young people have recently been aware of the serious risk of fake news and data circulation. The government takes measures for ensuring economic security such as geographical dispersion of connecting points between submarine cables and land circuits. International and regional geopolitics now urgently shape Japanese government policies.

NOTE

1. According to Dahl 'politics' has to do at the least with 'power' and 'authority'. Further conditions are that 'power' should be intended as 'legitimate' power (and thus 'authority'), supported by 'coercion': Dahl (1957).

REFERENCES

Council's Conclusion (2016), 'On Implementing the Eu Global Strategy in the Area of Security and Defence'

Dahl, R. (1957). 'The Concept of Power'.

European Parliament Research Study on ESA: 'On the path to 'strategic autonomy' - The EU in an evolving geopolitical environment', EPRS, (2020)

European Council, Conclusions (EUCO 13/20)

Nathalie Tocci, 'European Strategic Autonomy What it is, Why We Need It, How To Achieve It', p. 8.

Part 1

EU Digital Strategic Autonomy

Digital Strategic Autonomy: Industry Views and EU Policy Implications

David Bounie

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Digital technology has become a primary tool at the heart of all companies' production and distribution processes. This paper examines how economic (and political) sovereignty is intimately linked to digital sovereignty. It presents the results of a study conducted in 2021 among large French industrial companies with broad footprints in Europe and internationally.[1] What does this concept of digital sovereignty, or autonomy, entail for businesses? These questions have become more critical in 2022 as the Russian aggression in Ukraine brings European autonomy concerns to an even higher level. What are the technologies critical to digital sovereignty? And what levers are there for developing critical technologies and the instruments of EU digital autonomy?

THE AUTHOR

David Bounie is Professor of Economics, Head of the department of Economics and Social Sciences at Telecom Paris, Institut Polytechnique de Paris, and Academic Fellow at Institut Louis Bachelier. His research interest focuses on digital economics and specifically in how digital technologies are transforming the finance industry (digital payments, cryptocurrencies, artificial intelligence) in developed and developing countries (financial inclusion). He is the co-founder of the Chair 'Digital Finance' in partnership with Institut Louis Bachelier, Cartes Bancaires CB, La Banque Postale, and Caisse des Dépôts et Consignations.

THE AUTARKIC VISION OF DIGITAL SOVEREIGNTY IS A MYTH: COMPANIES TODAY ARE ASSEMBLERS OF COMPLEMENTARY AND INTERDEPENDENT TECHNOLOGIES

In the current context of international value chains, the autarkic vision of digital sovereignty is a myth: no company has all the technologies and all the skills to do everything by themselves. However, economic, political, and military sovereignty does not exist without technological sovereignty.

Technological progress has led to a complex integration of technologies of different kinds in the same product (e.g., the car). Companies today are assemblers of technology blocks; they speak of themselves as 'modular' companies.

To be sustainably competitive, companies engage in extensive international ecosystems. They assemble the best technologies, whether from France, Europe, or around the world. Getting rid of these technologies, or being denied access to them, would be counter-productive.

Given the openness of world capital markets, European companies have European and non-European shareholders and they often work alongside non-European players. These connections are now under review as the introduction of sovereignty considerations at political and industry levels are resulting in reasoned, structured framework rules. European companies forge international partnerships among major global industrial groups, as well as with research centres and start-ups. They establish factories abroad and market a decisive part of their products and services abroad, including in countries considered today as 'rivals' (e.g., China and even more so, Russia). Value chains are rooted in the availability of natural resources, skills, distinctive competences, and so on. International value chains were transformed after the 2008 financial

Sovereignty is to become as central to EU policy as the environment and sustainability

crisis and the subsequent international rebalancing. The resulting geographies are still under constant reassessment, subject to trade-offs regarding labour costs, robots financing charges, and transport rates. Increasing international political and trade tensions also cause changes, but industry relocation policies are limited.

The prevalent consensus is that the current international division of labour, with largely open borders, is mostly here to stay, and that high-level economic objectives such as income growth, the preservation of the European social model and ecosystem, and fending off international rivals are best served by and benefit from networks of *reciprocal interdependencies*. This means that autarky does not make sense, since some sort of interdependence is necessary to remain competitive in a globalised market.

INTERDEPENDENCE IMPLIES DEPENDENCE AND DEFINES RELATIONSHIPS OF POWER

It is the nature of this interdependence and the relationships of power it includes that are questioned today. The balance of power can be either positive – when a national company markets its technology abroad to a non-European company – or negative – unfavourable to European companies.

The balance of power is positive for the company when, for example, it imposes European technologies on or markets them to other non-European companies. The GAFAMs use technologies that are not only American or Chinese but also French or European, for example in cyber-security.

The balance of power can be negative and go against the company's interests. In this case, dependency is imposed, for example, in mainframes, cloud, and hyperscalers. Dependence has multiple dimensions for industries:

- Operational: being able to deliver the service (at a time t).
- Economic: in case of appropriation of value and loss of competitiveness, or critical control of the supply chain (choosing goods or elements in the critical production chain).
- Legal: US extraterritorial laws.
- Data-related: if critical data is jeopardised.
- Brand image management and reputational risk.
- Political (government-related): impossibility to operate in certain countries due to local decisions or embargoes.
- Corporate control: difficulty to control companies whose capital or ownership is not European.
- Military: defence and cyber-defence.

An unfavourable balance of power can be synonymous with inflicted dependence and a loss of value creation capabilities, resulting in a loss of competitiveness for companies or even in a very high risk of cannibalisation.

MASTERING CRITICAL TECHNOLOGIES TO REVERSE THE BALANCE OF POWER OF TOMORROW

To exit imposed dependence, it is necessary to master certain critical technologies and services. Europe has significantly lagged behind in certain digital technologies, and it will be difficult to catch up, even if a European awareness is emerging, as with recent initiatives in the European cloud (e.g., Gaiax-X, PIIEC plan on the cloud in 2022).[2] In the meantime, to ensure their competitiveness, European companies must be able to access the best technologies, and therefore work with non-European companies. They must use, for instance, information exchange technologies (messaging or videoconferencing), the cloud, centralised data

centres of digital platforms, and stochastic artificial intelligence (AI) technologies.

However, if for some technologies the balance of power is difficult to restore, for others the balance of power is not established, and here French and European companies can already perform well and continue to do so in the future. For example, this is the case with critical cyber-security technologies such as digital twins, biometric smart cards, identification (biometrics and behavioural analysis), detection of new attacks, and post-quantum cryptography. Similarly, the 5G telecommunications system is less dependent on physical infrastructure and will soon be virtualised, from SIM cards to the core network. This virtualisation disrupts the telecommunications sector and allows smaller companies, sometimes local ones, to offer their services. 5G also opens the way for edge computing, namely decentralised data processing at the edge of networks, giving rise to the creation of micro-data centres, for example, with 5G antennas close to business needs. Some services may replace the centralised data centres of big tech companies even if they are already positioning themselves on innovative offers.

Algorithm-based AI must be complemented by explainable rules to come up with a hybrid AI. Much focus is placed on stochastic AI, which is based on statistical learning and AI algorithms that are difficult to explain and whose outcomes are out of black boxes and cannot be trusted. Explaining the capabilities of AI, however, is fundamental to ensure trust in uses and certification by the competent sectoral regulatory authorities (e.g., finance or health). Without this, there will be no generalisation of AI in high-risk, or so-called critical, applications (e.g., health, defence, and so on). Hybrid AI makes it possible to combine expert systems (symbolic AI) and the power of statistical learning based on neural networks with formal knowledge rules. The hybridisation of the stochastic and the symbolic is the way forward.

Finally, quantum is undergoing a triple revolution: not only the computer, but also quantum sensors, in defence and civil applications (with the development of inertial sensors), and quantum communication networks (or the quantum internet).

THE LEVERS OF OUR DIGITAL SOVEREIGNTY

Sovereignty is to become as central to EU policy as the environment and sustainability. To ensure the EU's digital sovereignty and the development of these critical technologies, several priority levers must be activated.

- The first, and key levers, are science and research. Quantum mathematics, for example, requires the development of algebra and specific geometry at very high levels (for example, non-commutative geometry). There is considerable academic potential in Europe, and we are better positioned today than when stochastic AI was developed in the United States
- The second is related to the training, retention, and attraction of talent. New European programmes have been developed to fill the gap in digital skills, which has widened in the last decade. Talent training warrants a critical look at technological trends. Training on sovereign technologies is a guarantee of employability and attractiveness. This training of talents must also be accompanied by reliance on scientific knowledge. Culture, literature, the arts, cinema, and audiovisual works contribute to building a 'soft power' that goes hand in hand with ambitious ventures.
- The third is an economically integrated Europe.

Europe is a relevant market, and it becomes vital to integrate fragmented markets (e.g., economies of scale or market size). This integration must be accompanied by harmonised regulations and a renewed competition policy that will enable, where necessary, the emergence of European champions.

- The fourth is the development of competitive ecosystems. Vertical and horizontal integrations are very costly for companies. We must therefore innovate in the way companies partner to deliver innovative digital services. There are examples in France such as the Software République project. Led by Renault, Dassault Systems, Thales, Atos, and STMicroelectronics, the project aims to bring together their respective expertise in order to develop and market new systems and software intended for mobility propositions for territories, businesses, and citizens. The development of ecosystems also involves bringing together large groups and start-ups and creating structures that welcome entrepreneurs and strong partnerships with research centres. A strong partnership with expert consultants is also useful to support internal change and transformation efforts.

Balanced international ecosystems are the place where sovereignty, autonomy, and the benefits of open trade and multinational companies in an open economy intersect. This vision, however, will have to be re-visited in the light of the 2022 dramatic events in Europe.

Finally, the role of public authorities in the current phase is key. Although governments are not the locus of technological innovation, without the support of governing bodies the international balance of power cannot change. Public power is essential at several levels: regulation (extraterritorial laws); *ex ante* and *ex post* regulation of markets; investment; financing; training; public procurement; diplomatic or military initiatives; and so on. The higher the expectations of public decision-makers, the closer their exchanges with industries and centres of expertise.

NOTES

1. The study is a joint project of Observatoire Technologies et Souveraineté Numérique (Télécom Paris–Institut Polytechnique de Paris); Netexplo (Groupe Les Echos), with the support of the French Secretary of State for the Digital Transition and Electronic Communications. Industry participants include: Capgemini Invent; EDF; Renault; Orange Business Services; Thales and Les Villages by CA; Crédit Agricole Incubator; and Villa Numéris Think Tank. The author retains sole responsibility for the analyses presented in this paper.
2. The PIIEC (Important Project of Common European Interest) is a European instrument of industrial policy which authorises EU States to support their industries beyond R&D. It was first implemented in 2018 in nanoelectronics.

Digital Content and European Culture: A New Paradigm?

Augusto Preta

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Audiovisual content is not only an industry; it is also a fundamental element of a society that shares core common values defined as cultural identity. A key question today is whether or not we need market regulation. This chapter argues that we need regulation of a different sort. The Audiovisual Media Service Directive (AVMSD) is not the right tool: it is based on a sector-specific framework stemming from the era of analogue television, which cannot adequately adapt to a completely changed environment. Instead we need new, more effective tools to harmonise the different sectors into a (digital) single market. Legislative proposals such as the Digital Services Act (DSA, to the world of audiovisual media services may seem to be a foregone conclusion. In reality, however, audiovisual media services are little concerned with DSA, except in respect of AVMSD, which officially controls European audiovisual media policies, including cultural identity.

THE AUTHOR

Augusto Preta is an economist and market analyst. Professor in Media Economics, he is also founder and CEO of ITMedia Consulting. He has taken part in numerous projects at the European level and is a speaker at international conferences. He is a member of the Board of Directors and President of the Italian Chapter of the International Institute of Communications.

Audiovisual content is not only an industry; it is also a fundamental element of a society that shares core common values defined as cultural identity. What Europe lacked in the past – and perhaps still lacks today – is the sense of belonging to a single community and a belief in common ideas and values. To encourage such a sense of identity is an ambitious and vital task but also one which is very complex and difficult to achieve since Europe is based on cultural and linguistic diversity.

Audiovisual content (films, TV series), also defined as audiovisual media services, can therefore play a relevant role in reaching this scope. Conversely, in a time of profound changes in society, driven by the digital revolution, it can endanger the objective since globalisation and digital transformation may also bring cultural standardisation and lack of diversity.

Crucially, the audiovisual sector in Europe is now at a crossroad: developing a policy aimed at preserving the national industry from the entry of new global players, while also reducing the drive to innovate, to compete on the international stage, by fostering European and international investments and so enhancing the various European and national creative components of the sector.

MAIN TRENDS

There is no doubt that digital transformation is radically changing the media industry. After music, printed media, and radio, television is now experiencing the same rocky, disruptive path.

This trend has accelerated as the COVID-19 outbreak has led to increased streaming media consumption: the time spent on TV and video streaming has grown consistently since 2019, as efforts to stem the spread of the COVID-19 virus have led individuals to enjoy in-home entertainment. Given their increasing popularity, video-on-demand (VOD)

There is no doubt that digital transformation is radically changing the media industry

platforms have continued to register an uptick in the usage, involving also a part of the population less inclined to the use of digital technology. For example, in Italy, according to the media research company ITMedia Consulting, online TV (streaming) reached 10.1 million households in 2021, compared with 5.9 million in 2019, making broadband TV the leading platform for accessing audiovisual content in the country (ITMedia Consulting, 2021a).

VOD services therefore represent the latest revolution in the audiovisual sector. They have changed the way we watch content at home and on the move. They have also brought great changes to the production of audiovisual works, and given their increasingly significant position in the audiovisual media services market, they play an equally expanding role in fostering national and European audio-visual production and distribution. In consequence, they present a new point of reference in the eternal debate about European cultural identity.

Recently, in an article in *The Economist* with the indicative title 'How Netflix is creating a common European culture', one observer argues that 'An irony of European integration is that it is often American companies that facilitate it' and gives the example of Netflix pumping 'the same content into homes across a continent, making culture a cross-border endeavour' (The Economist, 2021). The author concludes that 'If Europeans are to share a currency, bail each other out in times of financial need and share vaccines in a pandemic, then they need to have something in common, even if it is just bingeing on the same series.'

Furthermore, relevant figures from a 2021 study by research company Digital i across the European Big Five (UK, France, Italy, Germany, and Spain) may support this suggestive and equally controversial argument (Advanced Television, 2021). Using its methodology to track full Netflix and Prime Video account viewing from a harmonised European panel, the data show that the two streaming platforms are beginning to 'democratise' non-English language content.

As a result, since 2019, the percentage of non-English language content available on Netflix has increased from 25 per cent to 31 per cent. Despite the catalogue makeup increasing by between 5 and 6 percentage points, the viewing behaviour has shifted more drastically. Netflix's UK viewers spent 22 per cent of their viewing time watching non-English language content in October 2021 in comparison with 10 per cent in the first quarter of 2019. The top non-English language titles during this time period were *Money Heist*, *Elite*, *Squid Game*, *Dark*, and *Lupin*.

For Prime Video, the percentage of the content catalogue made up by non-English language content increased from 19 per cent to 25 per cent from 2019 to October 2021. In terms of viewing, English language content viewing time dropped from making up 93 per cent of all Prime Video viewing to 84 per cent during the same period. Digital i forecasts that English language content will drop to 50 per cent of all mainstream subscription video-on-demand (SVoD) viewing in Europe by 2030.

THE ROLE OF REGULATION: THE EU APPROACH

In this fast-changing scenario, perhaps it is appropriate to start asking some questions: do we need regulation? And for what purpose?

Going back to the time when television was an activity developed on a national basis and subject to national legislation, EU regulation was specifically created to impose on national broadcasters, including public services, a set of rules to harmonise the system and to increase the number of European

productions. In the 1980s the overabundance of American films and TV series on the small screen with offers from the new private television channels was considered a major threat to domestic audiovisual industries.

In this regard, in 1989, through the Television Without Frontiers Directive, the EU considered it necessary to increase productions in Member States not only by establishing common rules opening up national markets but also by imposing quotas for European productions (European Council of the European Communities, 1989). In particular, more than 50 per cent of the broadcasting time had to be devoted to European works and 10 per cent broadcasting time or 10 per cent of the programming budget, dedicated to independent European producers.

The Television Without Frontiers Directive was radically overhauled in 2007, subsequently changed to the Audiovisual Media Service Directive (AVMSD) in 2010, revised and updated in 2018, and finally incorporated into national law by most EU Member States from 2019 (European Parliament and Council of the European Union, 2007); European Parliament & Council of the European Union, 2010); European Parliament and Council of the European Union, 2018). However, the quota obligations that apply to TV services have not changed since they were first introduced in 1989.

With regard to VOD services, while the 2010 version of the AVMSD introduced for the first time the distinction between linear services (broadcasting) and non-linear services (VOD), at the same time it required only a minimum level of regulation for the latter since VOD services, at the time, were still in their infancy.

In 2018, things dramatically changed, as we have seen, and accordingly the quota regime for linear services extended to VOD services, which were required not only to devote at least 30 per cent of their catalogues to European works but also to give them visibility. Obligations such as investments in European production remained optional, but, where introduced, they could also be imposed nationally on the basis of the revenues gained in each Member State.

From a historical perspective there has clearly been a need for regulation; but in practice regulation is far from being achieved. While the national audiovisual industry has maintained a certain level of production in terms of quality and quantity, it has been very bad at promoting European content and cultural diversity. The level of co-coproduction has slightly increased, while the circulation of national content in the Member States has been limited.

In a snapshot, European content has continued to be mainly a national business, with rare exceptions. Only with the arrival of the global (American) players has this scenario finally changed, providing a wider circulation of national works in the Member States.

EUROPEAN WORKS AND CULTURAL DIVERSITY

This brings us to a further question: does fostering European content still require regulation?

The answer, as for the previous questions, depends again on the scope. If we want to increase the volume of European works and their circulation around the world, undoubtedly the on-demand services are now the biggest producers in Europe and the ones that make possible the widest circulation and consumption of EU works. Netflix spent €4 billion on European films and series between 2018 and 2021, and Disney and Comcast, similarly, are increasing their expenditure on EU works (Barker and Abboud, 2022).

In this respect, the streamers have succeeded in making European works circulate across the EU as had never been done before, without the need for regulatory obligations or incentive as the AVMSD was not yet in force.

At the same time, as their role will be increasingly key to the development of European audiovisual productions in the coming years, it is essential to continue to attract the investments of these operators. A prescriptive, rigid regulation, left to the discretion of single Member States, imposing in a few cases fixed heavy investments in production for VOD services, is the worst scenario for a global player who has to decide in which country they want to invest more. This also carries a risk of shifting the focus away from producing high-quality content that consumers want, and could ultimately lead to less diversity, less innovation, and less availability of quality content (ITMedia Consulting, 2021b).

Moreover, it may also alter the market dynamics, although most streamers are already spending enough to meet investment obligations relatively easily anywhere. But, at some point in the future, when the market will no longer grow at the same spectacular speed as in the past (signs of this can be seen in the quarter ending 31 December 2021), they might be in a position in which they need to fall back on a more sustainable model (Hayes and Goldsmith, 2022). 'The regulation has thrown sand in the engine' (Godard, quoted in Barker and Abboud, 2022).

A different solution (and answer) might be given if we move from a mere market perspective to a cultural perspective linked to a subject such as European cultural identity.

The era in which we live is now clearly linked to profound cultural and social changes. The very concept of identity is no longer linked to the past, and the cultural revolution brought about by the new generations has meant greater attention to diversity and inclusiveness. We cannot expect this change to be right for everyone or to be accepted in the short term. However, it is a fact that the world has changed, society and its values have changed, and consequently so has art industry and its protagonists. This phenomenon has led to controversies and clashes, as well as to considerable closure and hostility on the part of those who grew up watching films or TV series in which the protagonists were essentially white, straight males (Harrison, 2020). Women, as well as those who belonged to any minority, were often either invisible or relegated to very limiting roles.

In this context, film and fiction TV therefore play a fundamental role, specific to popular culture: shaping social perceptions of Europe and European identity; and encouraging the development of engaging narrative formats made to enhance the values of diversity, mobility, and transcultural exchange in the constitution of a European identity.

In this case, it can be argued that successful international series such as *Money Heist*, *Lupin*, and *Call My Agent!* would not have had the same reach across borders without the global platform provided by Netflix.

At the same time, however, Netflix's border-crossing content policy does not necessarily originate in the EU. A recent spectacular example of this is the South Korean series *Squid Game*, which became the most successful series in Netflix history. It follows that if Netflix's strong investments in local production does not depend on specific territory, how we can expect Netflix to really care about European cultural diversity? (Cappello, 2021).

If we want regulation and not just market dynamics to deal with this goal, it is clear that the AVMSD

Netflix's UK viewers spent 22 per cent of their viewing time watching non-English language content in October 2021

is not the right tool. AVMSD is based on a sector-specific framework stemming from the era of analogue television, which tries to adapt to a completely changed environment. It does not take into due consideration the disruptive innovations that have reshaped the media and communications industry in the digital age and in practice is just an unlikely attempt to extend, re-adjust, and refit its past rules to the new ecosystem. Thus, in the context of digital transformation, an adaptive regulation cannot be the right way to foster European industry in the innovative global market of content or to promote Europe's values and cultural identity.

In this new framework, a more horizontal approach that tends to harmonise the different sectors into a (digital) single market seems a more consistent and desirable policy. The European Commission moved in this direction when it proposed two legislative initiatives to upgrade rules governing digital services in the EU: the Digital Services Act (DSA) and the Digital Markets Act (DMA) (European Commission, 2022). These initiatives form a single set of new rules applicable across the EU to create a safer and more open digital space where fundamental rights of users are protected and to establish a level playing field for businesses.

The extension of these legislative proposals, primarily DSA, to the world of audiovisual media services, through more advanced and effective horizontal policy tools, would therefore seem to be a foregone conclusion. In reality, however, audiovisual media services are concerned with DSA only in respect of coordination with AVMSD, which formally heads the development of European audiovisual media policies, including cultural identity.

REFERENCES

Advanced Television (2021). *Forecast: English language SVoD content down 50% by 2030*, 22 December 2021, https://advanced-television.com/2021/12/22/forecast-english-language-svod-content-down-50-by-2030/#:~:text=Using%20its%20methodology%20to%20track,democratise%20non%2DEnglish%20language%20content.

Barker, A. & Abboud, L. (2022). 'US streaming giants feel squeeze of regulation in Europe', *Financial Times*, 8 February, https://www.ft.com/content/bf70ada3-70fd-4fcb-b4e8-638bcc053025.

Cappello, M. (2021). 'SVoD services and the promotion of European culture', Powerpoint Presentation at *IIC Italy Chapter Webinar – Insights for a balanced regulation: considering platforms benefits and protection needs*, International Institute of Communications, 14 December. *Unpublished*

The Economist (2021), 'How Netflix is creating a common European culture: Streaming subtitled box sets is the new Eurovision', 31 March, https://www.economist.com/europe/2021/03/31/how-netflix-is-creating-a-common-european-culture.

European Commission (2022). *The Digital Service Act Package*, 4 March, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

European Council of the European Communities (1989). 'Council directive of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities', *Official Journal of the European Communities*, L 298, 23–30, 17 October, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31989L0552&from=EN.

European Parliament & Council of the European Union (2007). 'Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities', *Official Journal of the European Union*, L 332, 27–45, 18 December, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007L0065&from=EN.

European Parliament & Council of the European Union (2010). 'Directive 2010/13/EU of the European Parliament and the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)',

Official Journal of the European Union, L 95, 1–24, 15 April, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0013.

European Parliament & Council of the European Union (2018). Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities', *Official Journal of the European Union*, L 303, 69–92, 28 November, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808&from=EN.

Harrison, E. (2020). '11 of the most controversial films and TV shows on Netflix', *Independent*, 13 September, https://www.independent.co.uk/arts-entertainment/films/news/netflix-most-controversial-tv-shows-movies-cuties-365-days-b422001.html.

Hayes, D. & Goldsmith, J. (2022). 'Netflix narrowly misses subscriber target in Q4; stock tumbles', *Deadline*, 20 January, https://deadline.com/2022/01/netflix-earnings-fourth-quarter-streaming-squid-game-1234916609/

ITMedia Consulting (2021a). *Il Mercato TV in Italia 2021–2023* (Report XV), Decembre, http://www.itmedia-consulting.com/it/highlights/1601-xv-rapporto-itmedia-consulting-mercato-tv-in-italia-2021-2023-altri-operatori-crescono.html.

ITMedia Consulting (2021b). *Obblighi d'investimento in opere europee dei servizi a richiesta* (Report), 20 October 2021, http://www.itmedia-consulting.com/it/highlights/1583-obblighi-d-investimento-in-opere-europee-dei-servizi-a-richiesta-il-rapporto-itmedia-consulting.html.

The Importance of the Data Economy for Europe's Digital Strategic Autonomy

Jan Büchel and Barbara Engels

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

European companies need to have the ability to store, process, use, and share data securely and autonomously, for example by using cloud services based on agreed quality standards, values, and legislation. A survey conducted in autumn 2021 of 1,002 German companies from the industrial and industry-related services sectors shows that 71 per cent of companies in Germany are not data economy ready, while for 73 per cent data sharing does not play any role. The survey results show that the potential of the European data economy has not been well exploited, weakening Europe's digital strategic autonomy.

THE AUTHORS

Jan Büchel is an economist at the Institut der Deutschen Wirtschaft (IW). He earned his BA and MA in Economics at the Rheinische Friedrich-Wilhelms-Universität Bonn. His research interests are digitization, platform economy, AI, data sharing and games.

Barbara Engels is an economist at the IW, working in the field of structural change and competition. She studied economics at the Humboldt University in Berlin, at New York University and the Universitat Pompeu Fabra in Barcelona. She specialises in the effects of digital transformation on the economy and society.

A EUROPEAN DATA ECONOMY

A single European data economy is a key part of Europe's digital strategic autonomy. Digital sovereignty and hence data sovereignty are requirements for the ability to act as well as for the innovative capacity and competitiveness of the European economy. In this context, data economy readiness is defined as the ability of any company to store, manage, process, use, and share data efficiently and securely so that the company can increase its digital dividend, which is the value that is created based on digital technologies.

The largest companies in the world by market capitalisation, Alphabet (Google), Apple, Amazon, Meta (Facebook), and Microsoft (GAFAMs), have set an example with their unparalleled economic rise in the span of a decade. These companies use data in a new way and to a greater extent than any company before to optimise their value creation. While data has certainly become a very important resource for many companies, and rightfully so, the expectation and assessment of the potential for business value that can be created through data is strongly influenced by the success of the aforementioned GAFAMs. This expectation can be misleading (Engels and Schäfer, 2020). A direct comparison with the GAFAMs can create unrealistic expectations. Instead, it can be assumed that the potential for value creation from and with data depends on the company and the corporate culture, as well as on the company's product or service and the corresponding business model.

Exploiting the potential of company data hence need not necessarily mean creating business models based entirely on data, on sharing data with other companies, or on selling data-driven products but can also 'merely' mean making processes more efficient through the analysis of data.

In this context, companies in Europe need to have the ability to store, process, use, and share data securely and autonomously using cloud services based on European quality standards, values, and legislation. Failure to ensure such an environment could hinder companies from making full use of their data. This would be contrary to the European data strategy, which points to the need for Europe to quickly become stronger in the use of industrial data and to set a course that is independent from non-European actors by creating a single European data space (European Commission, 2020a).

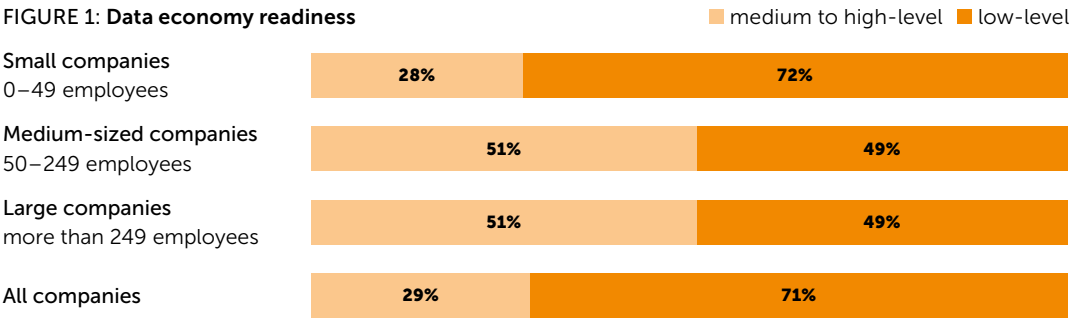
The proposed Data Act (European Commission, 2022) and Data Governance Act (European Commission 2020b) are flagship initiatives of European data strategy. In its Data Act impact assessment, the EU Commission correctly identifies the challenge of establishing a competitive market for cloud computing. To promote an open market, cloud users would need to be allowed to transfer data between different cloud service providers as easily as possible. The EU Commission hence wants to improve portability between cloud providers. To this end, it has proposed the introduction of a new portability law as part of the Data Act. This is intended to reduce technical, contractual, and economic barriers to data transfer in favour of an open cloud market and a strengthened user position. Indeed, providing mandatory standards for business-to-business contracts in the area of cloud computing services is warranted, especially when market failures can be identified.

How the Data Act can be implemented, is still largely unknown. It remains to be seen whether the EU Commission will be able to achieve its partly contradictory goals – simplifying data use by businesses while maintaining a very high level of data protection – and where compromises may be necessary. Data Act and the Data Governance Act imply legal challenges for companies that want to maximise the use of data, including compliance with data protection regulations, how to protect data from an intellectual property (IP) perspective, and ways to transfer it and license it. It is still unclear how explicit, systematic demarcations from other regulations are to be ensured, in particular from the General Data Protection Regulation (GDPR), the ePrivacy Regulation, and the Directive on the Protection of Business Secrets.

Gaia-X aims to create a federated open data infrastructure based on European values regarding data and cloud sovereignty. The mission of Gaia-X is to design and implement a data-sharing architecture that consists of common standards for data sharing, best practices, tools, and governance mechanisms. It also constitutes an EU-anchored federation of cloud infrastructure and data services, to which all 27 EU Member States have committed themselves (Gaia-X European Association for Data, and Cloud AISBL, 2021). Ideally, implementation of the Gaia-X infrastructure will encourage more companies to store, process, use, and share data in the EU, leading to a flourishing European data economy.

In order to examine to what extent companies already store, process, use, and share data, a representative survey was conducted of 1,002 German companies from the industrial and industry-related services sectors (survey period September–November 2021). This survey was part of the Incentives and Economics of Data Sharing (IEDS) project, funded by the German Federal Ministry of Education and Research.[1] Some of the results are presented in the following. They not only indicate the share of companies that are already 'data economy ready' but also point to potential obstacles to data sharing.

FIGURE 1: **Data economy readiness**



Note: Share of German companies (sectors: industry and industry-related service providers) obtaining the respective level of data economy readiness; n = 1,002. Source: German Economic Institute

DATA ECONOMY READINESS: THE STATUS QUO

Building on existing data readiness models, the study sought to determine to what extent companies have either a low or a medium to high level of data economy readiness (Röhl, Bolwin, and Hüttl, 2021). For this purpose, the response behaviour of the companies with regard to the three aspects of data economy readiness – data storage, data management (processing), and data usage – is of interest.

For the *data storage* component, companies were asked what types of data they store digitally. These data types include product, process, and personnel data related to the company's own production or workforce. Other data types comprise supplier data or customer usage data related to actors outside the company.

The *data management* component is concerned with how companies process their data. For example, companies were asked whether internal company data transfer is carried out via standardised and permanent interfaces, whether a classification and quality check of the data is carried out, and whether they regularly look for new data sources and possibilities for data use.

The *data use* component analyses the purposes for which companies use data. These include the (further) development of products, services, or business models. Data can also be used for automation and control of processes or offered for direct or indirect sale. (The results are shown in Figure 1, above).

Of all the companies surveyed, 29 per cent have a medium to high level of data economy readiness, and 71 per cent have a low level of data economy readiness. Most of the companies do not (yet) meet the technical and organisational requirements for efficient and effective data use. They are not ready to participate in the data economy.

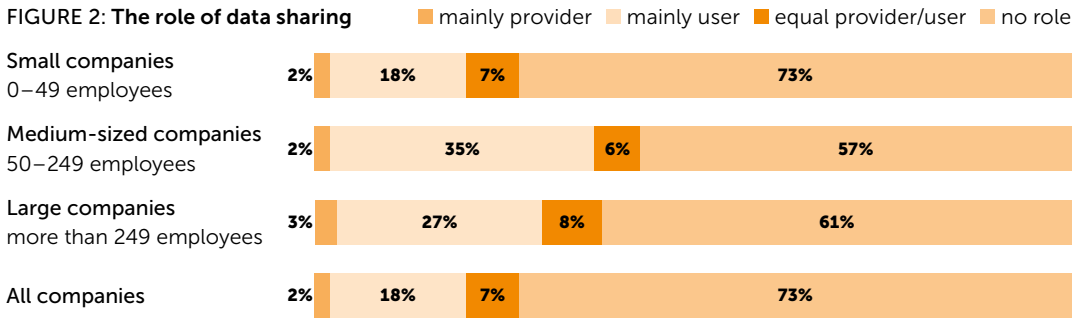
The medium-sized and larger companies perform better than the small ones. About half of the companies with at least 50 employees have a medium to high level of data economy readiness. Among small companies with up to 49 employees, this share amounts to 28 per cent. Therefore, the small companies in particular need to catch up, but the medium-sized and large companies also have extensive untapped potential.

Corresponding to the mostly low level of data economy readiness, most companies do not share data with other companies or other institutions (see Figure 2, opposite). If data sharing plays a role at all, it is mostly because companies receive data from others, not because they share data themselves. They are therefore most often data users, not data providers.

For 73 per cent of the surveyed companies, data sharing does not play any role. Of the remainder, 18 per cent categorise themselves as mainly data users, 2 per cent as mainly data providers, and 7 per cent are in roughly equal parts users and providers of data.

The performance of small companies with fewer than 50 employees matches the overall results once again. This is the case because about 97 per cent German companies are small companies (Destatis (2021). At 43 per cent, the share of companies for which data sharing plays a role is highest among medium-sized companies, ahead of large companies at 38 per cent. This result is surprising in that the share of companies with a high level of data economy readiness is the same for both company size classes. The higher relevance of data sharing among medium-sized companies compared with large companies is mainly due to the significantly higher share of data users (35 per cent for medium-sized companies and 27 per cent

FIGURE 2: **The role of data sharing**



Note: Share of German companies (sectors: industry and industry-related service providers) that are data providers or data users in relation to third parties; n = 987. Answers to the survey question: 'Do you offer data to other companies or institutions as part of your business model, do you see yourself more as a user of data provided by third parties, or does data sharing not play a role for your company?'. Source: German Economic Institute

for large companies). Medium-sized companies are thus more open to the use of external data than large companies. One explanation could be that medium-sized companies are more dependent on external partners and therefore more reliant on external data. Large companies represent a slightly higher share of the data providers and of those that are in 'roughly equal parts users and providers of data'.

The very low share of companies that provide their data to other parties points to potential obstacles to data sharing that are presumably more prevalent in the dissemination of a company's own data than in the use of external data. Specifically, the companies surveyed name several obstacles in the context of data sharing (see Figure 3).

Legal obstacles in particular stand in the way of data sharing. About 68 per cent of the companies surveyed observe legal barriers, while organisational (26 per cent), technical (22 per cent), and economic (22 per cent) barriers to data sharing, while far less critical, also play a role.

The main legal barrier involves privacy concerns. Of the companies surveyed, 88 per cent mentioned this barrier. However, many companies may not be aware of the scope of application of privacy regulations such as the GDPR. In particular, many companies may not be aware of the fact that much of the data that is relevant for sharing with other companies is non-personal data which does not fall under the GDPR. Therefore, privacy concerns arise as an obstacle to data sharing due to a lack of knowledge about which privacy rules apply, because the regulation itself is an obstacle – in fact it does not allow data sharing. Further analysis shows that small companies are more likely to perceive privacy concerns as a legal barrier, most likely because small companies have less knowledge about the topic as they do not have a legal department and hence perceive the legal hurdles to be higher.

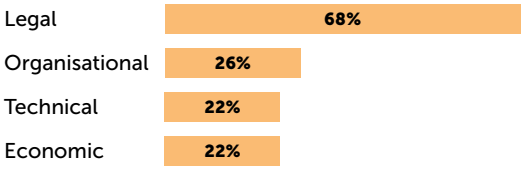
The main organisational barrier is a lack of organisational knowledge, the main technical barrier is a lack of data exchange standards, and the main economic barrier is a lack of understanding of the benefits of data sharing. Many of these obstacles could be mitigated in the future by using the information and infrastructure provided by Gaia-X.

Gaia-X has been criticised for including non-European companies such as large cloud providers from the United States in the development of Gaia-X standards. This criticism can at least in part be addressed by the recent announcement at the Gaia-X summit that Gaia-X certifications for service providers will be issued at three levels: a basic level for services that meet the minimum standards, a medium level for services offered on EU territory, and a high level if the provider is also a European company. However, it is still necessary to ensure that European values and hence Europe's digital strategic autonomy are not compromised.

The provision of trustworthy cloud services by Gaia-X could also potentially increase the share of companies that use cloud services. Currently, only 40 per cent of German companies uses cloud services such as mail, office, and customer relationship management software, virtual servers, or on-demand computing power (see Figure 4).

Cloud usage has already become part of everyday business life for many companies in Germany, but the majority still do not use cloud services. There is a substantial amount of untapped potential, in particular since companies often use rather low-threshold cloud services such as mail software, and more advanced cloud services such as on-demand computing power do not yet play a role.

FIGURE 3: **Obstacles to data sharing**



Note: Share of German companies (sectors: industry and industry-related service providers) obtaining the respective level of data economy readiness; n = 1,002. Source: German Economic Institute

OUTLOOK AND POLICY RECOMMENDATIONS

The aforementioned survey results show that the potential of the European data economy has not been well exploited, weakening Europe's digital strategic autonomy. While only German companies were surveyed, the results are also potentially valid for other EU countries. Many companies are not yet 'data economy ready'. Moreover, they do not share data with other companies or institutions. Instead, they encounter several obstacles that prevent them from sharing data. In order to strengthen the digital strategic autonomy of the EU, the potential of the data economy has to be realised, facilitated, and seized. There can be no digital strategic autonomy without the use of the most important resource of digital markets: data.

While it is neither sensible nor possible for all European companies to become entirely data-driven, it is crucial for the future viability of companies that they know which data they collect and that they can store and process it safely and sensibly. Companies must have the scope to experiment and to determine where data-based and digital approaches should be adopted, where it makes sense to remain analogue, and where the analogue can be combined with the digital. This is critical for companies to remain competitive in the international market and for Europe to achieve digital strategic autonomy.

The Gaia-X initiative will provide a suitable framework in which companies can experiment. It will mitigate obstacles to data sharing and pave the way for a flourishing European data economy. The goals of Gaia-X particularly address the legal, organisational, technical, and economic barriers that companies encounter when storing, processing, using, and sharing their data.

However, only 9 per cent of the German companies surveyed were aware of Gaia-X. Accordingly, it is important to communicate the benefits of the initiative in a company-oriented, easy to understand, and plausible manner. This is the only way to effectively convince companies to participate in Gaia-X, which will benefit the entire European data ecosystem. In addition, incentives can be created for companies to participate in the development of the Gaia-X standards. In this context, it would be helpful to quickly realise Gaia-X use cases such as Catena-X, a use case for a data space in the automotive sector.[2]

As already mentioned in the context of the European strategy for data (European Commission, 2020a), in order to build a data economy that acts as an engine for innovation and new jobs, the EU should combine fit-for-purpose legislation and governance to ensure availability of data, with investments in standards, tools, and infrastructures such as Gaia-X as well as competences for handling data. This must happen quickly, but not haphazardly. Europe has no time to lose.

NOTES

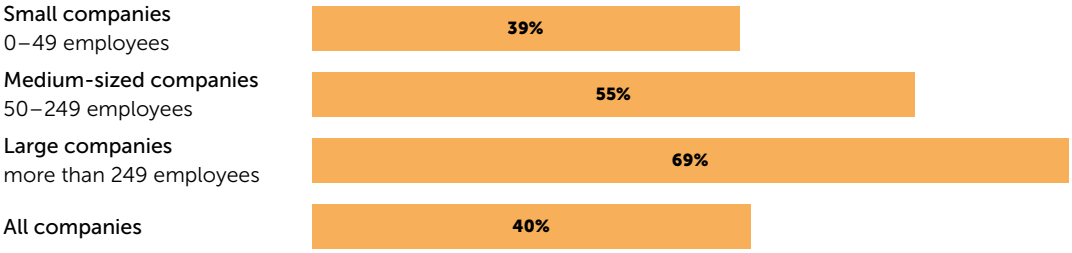
1. For more information, see https://ieds-projekt.de/
2. See https://catena-x.net/de/

REFERENCES

Demary, V, Fritsch, M., Goecke, H., Lichtblau, K., & Schmitz, E. (2019). *Bereitschaft der deutschen Unternehmen für die Teilhabe an der Datenwirtschaft, Gutachten im Rahmen des BMWi-Verbundprojektes'*. Cologne: Institut der deutschen Wirtschaft. https://www.iwkoeln.de/studien/vera-demary-manuel-fritsch-henry-goecke-alevtina-krotova-karl-lichtblau-edgar-schmitz-bereitschaft-der-deutschen-unternehmen-fuer-die-teilhabe-an-der-datenwirtschaft.html.

Destatis (2021). *Unternehmensregister. Rechtliche Einheiten und abhängig Beschäftigte nach Beschäftigtengrößenklassen und Wirtschaftsabschnitten*, 6 December. https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Unternehmensregister/

FIGURE 4: **Cloud usage**



Note: Share of German companies (sectors: industry and business-related service providers) using cloud services; n = 989.
Source: German Economic Institute

Tabellen/unternehmen-beschaeftigtengroessenklassen-wz08.html.

Engels, B. & Schäfer, C. (2020). *Data Governance in deutschen Unternehmen*. Cologne: Institut der deutschen Wirtschaft. https://www.demand-projekt.de/paper/Gutachten_DEMAND_Data_Governance_in_deutschen_Unternehmen.pdf.

European Commission (2020a). *A European Strategy for Data* [COM(2020) 66 final]. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN%20,%20p5.

European Commission (2020b). *Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)* [COM(2020) 767 final]. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN.

European Commission (2022). *Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)* [COM(2022) 68 final]. https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data.

Gaia-X European Association for Data, & Cloud AISBL (2021). *Gaia-X Architecture Document*. 21 September. https://www.gaia-x.eu/sites/default/files/2021-10/Gaia-X_Architecture_Document_2109.pdf.

Röhl, K.-H., Bolwin, L., & Hüttl, P. (2021). *Datenwirtschaft in Deutschland: Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?* Cologne: Gutachten im Auftrag des Bundesverbands der Deutschen Industrie.

Microchips as a Vital Element of EU Strategic Autonomy and Digital Sovereignty

Julian Kamasa

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Autonomy in the sense of the ability and capacity to act requires a strong and flexible industrial base. This strategic goal is not to be misinterpreted as a quest for ever more protectionism, however. In a globalised and interdependent world, openness and independence are not mutually exclusive. This is particularly true for the production of microchips, which are a key ingredient for a variety of the EU's internal and external interests.

THE AUTHOR

Julian Kamasa is a Senior Researcher at the Swiss and Euro-Atlantic Security Team at the Center for Security Studies (CSS) at ETH Zürich. He is also co-editor of the policy brief series CSS Analyses in Security Policy, which explores current developments in international security and strategic affairs. Julian holds a BA in History and Social Sciences from the University of Basel, and an MSc in EU Politics and International Relations of Europe from the London School of Economics and Political Science. Before joining the CSS in 2019, Julian worked in the Zurich-based Think Tank Avenir Suisse and in the Swiss Embassy in Warsaw. His areas of research include Swiss and European foreign and security policy as well as emerging technologies.

The concept of strategic autonomy is only vaguely defined and has the potential to be (mis)used for a whole range of political purposes. The same is true for the increasingly mentioned 'digital' or 'tech sovereignty'. Sovereignty and autonomy cannot be thought of in absolute terms in a century characterised by strong economic interdependence and globalised supply chains. Increased geopolitical competition may fuel protectionist tendencies, however (Evenett and Fritz, 2021). While protectionism may, to some extent, be applicable in traditional industries, it is impossible to sustain such an approach in the digital sphere, which is all about enabling open data spaces around the globe and not within nation states. Therefore, digital strategic autonomy must be conceptualised by combining elements of both openness and independence. Essentially, in this domain, there can be no independence without openness and vice versa.

RELEVANCE OF MICROCHIPS FOR EU STRATEGIC AUTONOMY

The interplay between openness and independence is of particular importance for the EU in the field of microchips since this industry branch is marked by a high degree of both fragmentation and specialisation. Hence, there is no state in which companies actually perform all tasks including raw material mining, product design, research and development, mechanical engineering, contract manufacturing, testing, assembly, and packaging. This means as well that no state is self-sufficient in chip manufacturing. However, it is worth noting that some regions, such as East Asia, are home to many dominant players. This is particularly true in segments such as contract manufacturing, with Taiwan accounting for more than 60 per cent of the world market (Fleming, Hollinger, and Hall, 2021). However, world-leading

companies in Taiwan and South Korea are heavily reliant on machines from ASML, a Dutch company unrivalled in this specific segment (TrendForce, 2021). This case exemplifies the extent of specialisation, which occurs in a few regions, with a handful of companies being highly focused on one task within the overall production process. This market structure creates complex interdependencies, making protectionist measures seem generally not applicable.

Against this background, the EU has some industrial clout in the semiconductor industry, but it lacks the capacity for larger-scale production. This has become particularly visible in the context of COVID-19 and its disruptive effects on global supply chains. Extreme weather events at crucial production sites in early 2021 as well as the already present geopolitical competition made matters worse, culminating in what was called a 'Chipageddon' in mid-2021 (Kleinhans and Hess, 2021). When supply chains are disrupted, geography matters. This is particularly relevant for the chip-reliant industry based in Europe, which is heavily dependent on the production of chips in East Asia. In order to be globally competitive and to transition to a greener economy as foreseen by the European Green Deal, the EU needs a strong industrial backbone supplied with microchips (European Commission, 2021). The same applies to the development of a technologically advanced European defence industry, which is crucial for closer defence cooperation among EU member states and, ultimately, for the concept of strategic autonomy. The Russian invasion of Ukraine has put increased urgency on the envisioned energy transition as well as modern European defence industry. The current deficiencies in chip manufacturing capacities in EU Member States are, thus, an obstacle on the path towards strategic autonomy and digital sovereignty. Therefore, increasing these capacities is crucial for the EU to be able to act more independently.

THE SITUATION OF THE EU

It would be incorrect to assume that there can be a globally competitive 'made in the EU' chip industry anytime soon. In fact, many false assumptions have found their way into the public discourse regarding the EU's role in the semiconductor industry. One such assumption is that the EU held a global semiconductor market share of 44 per cent in 1990 which then fell to about 10 per cent by 2021 (Kleinhans, 2021). This misleading statement by the CEO of Intel was quoted in the *Financial Times* in April 2021. The problem here is that the catchy number of 44 per cent market share is not only wrong; it also creates unrealistic expectations when assessing the EU's situation and setting goals for the mid- and long-term future. This misleading statistic was based not on the whole market but only on fabrication plants for the newly emerging format of 8-inch silicon wafers.[1] When looking at the whole market, the share in the 1990s accounted for about 10 per cent and has remained relatively steady. Why does that matter in this context? Because it is crucially important to get the assumptions right before proceeding to action on a political level. When it is assumed that the EU was once a global hub for microchip production, the narrative may be to 'get those capacities back', which may falsely appear rather easy to achieve with enough spending and political will. However, the truth is that there is nothing to 'get back'; rather, it must be built from scratch or, in some cases, extended. Capacity-building in this sector is a long-term process and goes beyond industrial policy and large spending. Even world-leading companies such as the Taiwan-based TSMC

To be globally competitive and to transition to a greener economy … the EU needs a strong industrial backbone supplied with microchips

need several years to extend manufacturing capacities (*The Japan Times*, 2021).

Unrealistic time horizons are a second false assumption. The Dutch company ASML is a case in point here. It specialises in producing extreme ultraviolet (EUV) machines, which are key for the manufacturing process of the technologically most advanced chips. EUV machines, each of which costs about 130 million euros, are a crucial component for chip manufacturers such as TSMC, Samsung, and Intel (Shead, 2021). Since no other company is able to supply these machines, the EU hosts a world-leading player with a massive competitive advantage. This position, however, was achieved through 30 years of research and development into perfecting the use of EUV machines in practice. Other significant European companies such as BASF, Linde, and Merck have a rich tradition in the chemicals sector and could build upon accumulated know-how in order produce chemicals required for semiconductor coating. Integrated device manufacturers such as Bosch, Infineon, NXP, and STMicroelectronics are in turn important suppliers of chips for the automotive industry (Kleinhans and Baisakova, 2020). The latter two are relatively young companies, having been founded around the turn of the millennium, while Bosch is a well-known brand in engineering and high-tech. Hence, in order to make the right choices on an EU level, it is important to keep in mind that capacity-building takes decades, and that Europe has never been a globally dominant actor in this sector.

CURRENT EU INITIATIVES AND POTENTIAL CHALLENGES

It is important to have accurate numbers and assessments in order to right-size potential subsidies as foreseen by what is called the EU Chips Act. This proposal issued by the European Commission is foreseeing public and private investments worth 43 billion euro. Its *first* aspect, a clear research strategy, is certainly noteworthy. However, some challenges remain to be solved for this proposal to advance. One is about defining the right scope and focus of research. Innovative ideas are often bottom-up in nature and result from academic cooperation rather than being the result of top-down strategies. Linked to that, the departure of the United Kingdom from the EU and the latter's strained political relations with Switzerland weigh particularly heavy. According to the QS World University Rankings 2022, nine of the ten highest-ranked European universities are in fact not in EU member states, but in the UK and Switzerland. In the fields of Engineering and Technology, five of the top ten European universities are in EU countries (QS Top Universities, n.d.). Given the ongoing competition among great powers such as the United States, China, and the EU for the smartest minds needed for cutting-edge research on new technologies, the bloc risks falling behind here by politicising research cooperation with like-minded European third countries. As already emphasised in the introduction, independence requires a certain degree of openness. Hence, a low-cost option for the EU Commission may be to distinguish between political and non-political relations with European third countries such as the UK and Switzerland.

The *second* aspect of the EU Chips Act, namely the development of production capacities, is aimed at addressing the lack of contract manufacturers in close regional proximity. Having capacities in EU countries would benefit not only machine suppliers such as ASML, but also customers such as the ever important automotive sector, which has not been able to recover from the crisis in 2020 due

Capacity-building in this sector is a long-term process and goes beyond industrial policy and large spending

to a shortage of chips. However, developing production capacities is not a simple matter. As examples of world-leading companies have shown, the accumulation of know-how and specialisation is a matter of decades. Essentially, the chip development and manufacturing process can take years, as not only the design of the chips, but also the facilities to produce them, must be carefully planned. Furthermore, planning processes must also always anticipate further technological development and market demands. For the EU, a cost-effective option may be to set incentives for leading chip manufacturing companies such as TSMC, Samsung, and Intel to build production facilities in EU countries. For chip manufacturers, this is beneficial due to the strong demand in chips across all industrial sectors in Europe. This step would bring production capacities geographically closer in the short to medium term. In the longer term, the case of Silicon Valley shows that the presence of big companies can result in a spillover effect, where many innovative start-ups form around big players, creating innovative ecosystems (Kushida, 2015). Such an approach would increase the EU's independence and its ability to supply its industrial base with chips, which is needed for the overarching ambition to be more strategically autonomous.

The *third* component, international partnerships and cooperation, is strongly interrelated with the first two aspects of the EU Chips Act. One might even argue that it is a precondition that must be met in order for the Act to succeed. This is particularly true for the semiconductor industry, which is highly fragmented around the globe. Neither increased production capacities nor research and development will be successful without international partners. It is therefore interesting that the EU Chips Act mentions this precondition last and not first. Instead of emphasising a research strategy and the development of production capacities, a better option would be to define a clear strategy of international cooperation and selected partners as a first step. In a second step, this would facilitate research and the development of production capaccities. The EU could capitalise on existing formats such as the recently operationalised EU–US Trade and Technology Council and address issues such as supply chain security (Guix, 2021). This is particularly critical for access to raw materials such as silicon, which is an essential natural resource for chip manufacturing. Currently, China controls a vast majority of those resources, providing Beijing with a powerful tool (for example, export restrictions) in ongoing geopolitical competition. Although it is in China's best interest to provide both the EU and the US with these materials, its restrictions on imports of coal from Australia have shown that Beijing does not shy away from imposing measures which ultimately result in negative impacts in China (Choudhury, 2021). A good option would be to minimise potential risks along the semiconductor supply chain through increased cooperation with like-minded partner states.

POLICY RECOMMENDATIONS

The extensive dependence of various branches of industry in the EU on the smooth functioning of global supply chains was clearly demonstrated in 2021. It is clear that, moving forward, the EU has to strengthen its own production capacities to avoid these types of vulnerabilities in the future. Three points stand out in this context. *Firstly,* it is crucial to act on the basis of accurate assessments. False assumptions such as the 44 per cent market share in 1990 may lead to inflated expectations and high spending, resulting in disappointment over the

absence of quick results. Hence, it is important to spend public money where it will have the biggest impact. The case of China shows that money alone does not necessarily guarantee success in this industry, at least not in the short term. A subsidy scheme worth billions of euros, as foreseen by the Chips Act, should be based on a realistic assessment of where the EU stands and what it can achieve most effectively, and in what specific area, in due time.

Secondly, the funding foreseen by the proposed Chips Act has to be spent wisely and be impact-oriented. The EU would be well advised to leverage pre-existing ecosystems such as the vibrant area around Dresden, which is also called 'Silicon Saxony' (Silicon Saxony, n.d.). Furthermore, it is worth noting that the EU could likewise leverage research partnerships with the UK and Switzerland, which are both excluded from essential cooperation programmes by the EU Commission due to strained relations on the political level. Excluding two countries with world-leading universities in the fields of science and technology cannot work in the EU's favour and will result in a zero-sum game at best. When looking at the bigger picture of geopolitical competition and a war at the EU's doorstep, openness and cooperation among European countries in the research domain appears to be essential. Therefore, strengthening cooperation in the fields of science and technology with like-minded partners may prove very effective and would probably be less costly than drafting and implementing a research strategy from scratch.

Thirdly, the EU may want to distinguish between various time horizons in order to set realistic and achievable goals. Building up industrial capacity is a long-term project. Even highly experienced companies such as TSMC need significant time to expand production capacities. For example, TSMC does not expect to start production at a planned plant in Japan before 2024 (*Japan Times*, 2021). Unlike in other fast-moving tech industries, this relatively long time span shows that in the complex chip industry, manufacturing capacity cannot be developed flexibly and quickly. The EU does not have its own TSMC, which is why the bloc should promote openness for companies of this kind to invest in setting up production facilities in EU countries. The EU can leverage its economic power as a trading bloc as well as the single market. These three recommendations reflect the complex interplay between independence and openness in the context of promoting greater strategic autonomy in the digital space, which is essentially about maximising the ability to act and promote political, academic, industrial, and economic openness and flexibility.

In short, policymakers may want to take the following points into account:

- The EU's ambition to be strategically autonomous will require that it has a reliable chip supply chain.
- The chip industry is characterised by high specialisation and regional fragmentation.
- Moving forward, the EU needs to base its industrial policy on accurate assessments, the real demands of its industry, and the exploitation of potential niches in the world market.
- Potential subsidy schemes should not aim at a 'made by the EU' goal but rather emphasise a 'made in and for the EU' approach.
- Realistic time frames and goal-oriented partnerships with like-minded states are key to succeeding in this specific sector.
- Openness is a precondition of independence and vice versa.

NOTE

1. Wafers are circular and consist of semiconductor material such as silicon. The wafer is the foundation of a microchip, as multiple transistors and circuits are applied to it layer by layer. The wafer format depends on the complexity of the tasks to be fulfilled and on industrial needs.

REFERENCES

Choudhury, S.R. (2021). 'China needs more coal to avert a power crisis – but it's not likely to turn to Australia for supply', *CNBC*, 25 October, https://www.cnbc.com/2021/10/26/china-energy-crisis-beijing-not-likely-to-lift-coal-ban-on-australia.html.

European Commission (2021). *Digital technology, the positive force for climate action: Commissioner Thierry Breton keynote speech at the EU Pavilion side event of COP26 'EU initiatives in support of the green digital twin transition'*, 10 November, https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/digital-technology-positive-force-climate-action_en.

Evenett S.J., & Fritz, J. (2021). *Subsidies and Market Access: Towards an Inventory of Corporate Subsides by China, the European Union and the United States: The 28th Global Trade Alert Report* [Report]. Global Trade Alert, 25 June, https://www.globaltradealert.org/reports/gta-28-report.

Fleming, S., Hollinger, P., & Hall, B. (2021). 'Semiconductors: Europe's expensive plan to reach the top tier of chipmakers', *Financial Times*, 21 July. https://www.ft.com/content/d365bfe0-98c4-49b5-8e82-dc4386623ace.

Guix, P.R. (2021). 'Critical mass: Raw materials, economic coercion, and transatlantic cooperation', *ECFR Commentary*, 17 December, https://ecfr.eu/article/critical-mass-raw-materials-economic-coercion-and-transatlantic-cooperation/.

Japan Times (2021). 'TSMC looking to build Japan plant in 2022 and start operations in 2024', 14 October, https://www.japantimes.co.jp/news/2021/10/14/business/corporate-business/tsmc-looking-build-japan-plant-2022-start-operations-2024/.

Kleinhans, J.-P. (2021). 'Europe didn't have 44% of global chip production capacity in the 90s. Sorry', *LinkedIn*, 11 December, https://www.linkedin.com/pulse/europe-didnt-have-44-global-chip-production-capacity-90s-kleinhans/?trackingId=0vtTOeinTwmYIr%2B57Qagsg%3D%3D.

Kleinhans, J.-P. & Baisakova, N. (2020). *The global semiconductor value chain: A technology primer for policy makers*, Stiftung Neue Verantwortung, October, https://www.stiftung-nv.de/sites/default/files/the_global_semiconductor_value_chain.pdf.

Kleinhans, J.-P. & Hess, J. (2021). *Understanding the Global Chip Shortages: Why and How the Global Semiconductor Chain Was Disrupted* [Policy brief], Stiftung Neue Verantwortung, November, https://www.stiftung-nv.de/sites/default/files/understanding_the_global_chip_shortages.pdf;

Kushida, K. (2015). 'A Strategic Overview of the Silicon Valley Ecosystem: Towards Effectively "Harnessing" Silicon Valley', *SNVJ Working Paper* (2015-6). 11–17, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/strategic_overview_of_sv_ecosystems.pdf.

Morris, M. & Byrne, N. (2021). 'What does chipageddon have to do with climate change?', *ABC News*, 7 May, https://www.abc.net.au/news/2021-05-07/what-does-chipageddon-have-to-do-with-climate-change/13327926.

QS Top Universities (n.d.). *QS World University Rankings 2022*, https://www.topuniversities.com/university-rankings/world-university-rankings/2022.

Shead, S. (2021). 'Investors are going wild over a Dutch chip firm. And you've probably never heard of it', *CNBC*, 24 November, https://www.cnbc.com/2021/11/24/asml-the-biggest-company-in-europe-youve-probably-never-heard-of.html.

Silicon Saxony (n.d.). *Association*, https://www.silicon-saxony.de/en/about-us/association/

TrendForce (2021). 'Foundry revenue projected to reach historical high of US$94.6 *billion in 2021 thanks to high* 5G/HPC/end-device demand, says TrendForce', 15 April, https://www.trendforce.com/presscenter/news/20210415-10759.html.

The EU Need for 5G Cybersecurity Capabilities

Erik Bohlin and Simon Forge

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

The mobile cellular technology that lies behind 5G networks promises both significant risks and potential rewards. But behind the hype about massive Internet of Things applications may lie threats to our critical infrastructure based on a 5G networking environment. Moreover, the invasion of the Ukraine by Russia highlights how the subversion of high-speed ubiquitous Internet attached networks can disrupt energy generation and distribution, government services and also logistics systems for food and medical supplies. Such subversion may also offer the opportunity to build pervasive surreptitious surveillance systems for military intelligence. To respond adequately, novel trust models are needed for 5G that express enhanced security paradigms for 5G networks.

THE AUTHORS

Simon Forge is Director of SCF Associates Ltd, specialising in forecasting the impacts of telecommunications and computing developments. He holds a PhD (Digital Signal Processing), from the University of Sussex, UK, and is a Chartered Engineer (MIET).

Erik Bohlin is Professor at the Department of Technology Management & Economics at Chalmers University of Technology. He is Editor-in-Chief of the *Journal of Telecommunications Policy* and has published widely. He obtained his PhD at Chalmers University of Technology.

THE NEED FOR NEW LEVELS OF CYBERSECURITY WITH 5G

The majority of the EU population is highly dependent on mobile radio networking, especially for Web access, hence introducing a new generation of such technologies should present innovative advantages. However, unless it is carefully planned, it may also create new problems and even dangers in the online world. This future dependence on 5G networks and their centrality for the EU's well-being, competitiveness, and cybersecurity has been recognised in many EU documents (European Commission, 2016, 2020; European Commission, AIT Austrian Institute of Technology, Fraunhofer ISI, Imec, and RAND Europe, 2021; ETSI, 2020). As the mobile world increasingly connects devices that impact people's health, welfare, and even everyday finances, effective cybersecurity protection for 5G networking will become a critical goal.

That goal will require rethinking traditional cybersecurity to include the additional challenges of 5G and perhaps considering amendments to the eventual next generation, as 6G. Both research with simulation of operational vulnerabilities in 5G networks and actual attacks on today's networks (what are termed 3G, and by marketing, 4G, and in technical definitions as Universal Mobile Telecommunications System, UMTS, and Long Term Evolution (of UMTS) – Advanced, LTE-A) highlight the vulnerabilities that ubiquitous 5G broadband presents for our future infrastructure, both industrial and consumer. National administrations and regulatory authorities are increasingly beginning to recognise the real significance of the exposure and liability threats and the potential need for further measures.

Widespread recognition of the need for far higher levels of 5G security is therefore imperative. This would require wide-ranging analysis of the types of

incidents and attacks, to anticipate the major points of failure and also the intrusion strategies that malicious operators may use to compromise 5G networks and their attached systems and management controls.

Therefore, we need to determine where today's security practices may be deficient and incapable of anticipating future reality. With 5G's industrial applications increasing, exposure will only multiply, probably very quickly. Consequently, to defend lives, our natural environment, (for instance from the effects of failed sewage treatment systems that pollute rivers and the sea estuaries, as is occurring in the UK) and everyday life, 5G networks will demand new levels of protection, which will arise from research into possible countermeasures to secure these systems.

While 5G promises greatly expanded capabilities and new services – such as higher data speeds for broadband streaming (up to 500 Mbps and perhaps even as high as 100 Gbps) as well as industrial Internet of Things (IoT) applications and possible network slicing for different applications – it also poses several new security challenges. Considering the already precarious nature of cybersecurity, 5G networks and services will amplify the challenges in several dimensions and situations, particularly that of the quantity of data exposed and the capability to mine large information volumes thanks to accelerated data speeds.

This chapter will provide a brief overview of the particular and aggravated cybersecurity challenges that 5G will pose for security and privacy and provide some tentative ideas towards solutions for them (European Commission, Directorate-General for Communications Networks, Content and Technology, Blackman, Horvitz, & Forge, 2014).

OPPORTUNITIES FOR A WIDER SELECTION OF USE CASES WITH 5G

As is well known, the 5G business model sees a far richer assortment of possible applications than that of the traditional mobile industry (which offers voice telephony, data with Internet IP packet structures and Short Message Service, SMS, messaging). Using the IP data stream, 'Over the top' services via the mobile Internet are provided by the major social networking and search platforms today, in a 'walled garden' approach of services that do not interconnect – that is, they are 'walled off", ensuring customer lock-in to the platform. Here we note that 'over the top' (OTT) services refer to Internet services for voice, video chat, text messaging, email, and so forth from the major web platform operators that compete with those services from the mobile network operators (MNOs) – but which the MNOs cannot charge for. The MNOs can only charge for the plain data channel, not the web services running over it – and despite early attempts by MNOs to create walled gardens of Web services, these have never been as successful as the 'Big Tech' platforms for reasons of financing streams based on major differences in business models and cultures. These OTT services are clearly envisaged for a high-speed radio network connecting billions of devices. Moreover, the realistically achievable 5G broadband speeds (perhaps of the order of 10 Gbps, but varying by MNO and by location) and large volumes of data in circulation will present many diverse security concerns. Future 5G standards will ultimately have to reconcile these with its novel features and capabilities. Designing it with security embedded in the foundations, rather than adding it later, is a major concern here. Whether that is being considered sufficiently in the standards development organisations is a key question today. Certainly it is

With 5G's industrial applications increasing, exposure will only multiply, probably very quickly

now an important agenda item as telecommunications and public security regulators (for example, The European Networks and Information Systems Agency, ENISA in the EU) are becoming more aware of the potential security risks of 5G.

The three primary use cases for business models in the ITU IMT-2020 (International Telecommunications Union International Mobile Telecommunications-2020) are enhanced mobile broadband (eMBB); machine type communications (MTC), including vehicles to other vehicles and to the roadside infrastructure; and ultra-reliable communications with low-latency (URC/LL).

Each use case presents somewhat different challenges. The MNOs see eMBB as the most attractive application as it supports streaming video for their key business model. That presents a fairly moderate performance demand on the network compared with the other two – and possibly fewer cybersecurity compromises, with less at stake. The downside risks for the types of application envisaged for the other two use cases are far higher in socio-economic terms. These more demanding business models will have different impacts on both the core network and the radio access network (RAN) from a cybersecurity perspective, as explored further below.

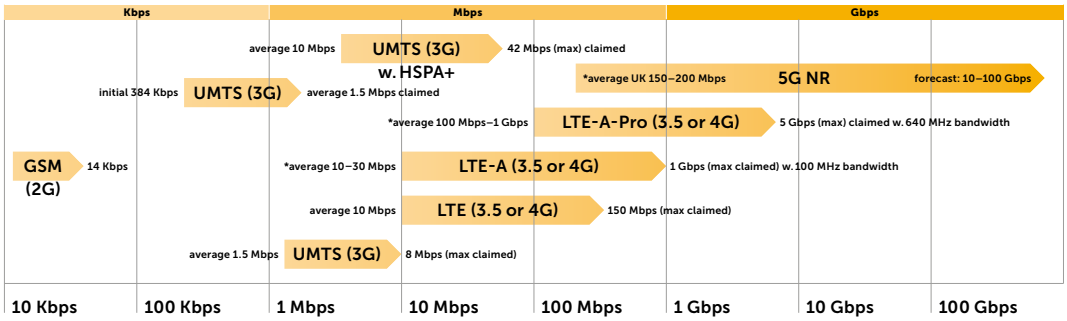
For instance, URC/LL will require high bandwidth in the RAN – a major challenge for 5G over-the-air transmission – combined with low latency in the core network, which demands a suitable level of parallel switching capacity. This is essential for applications such as e-health, so that edge caching may be necessary, as well as diversity of assets and routing for resilience. This also raises security issues for their protection as edge caching especially implies a further distribution of vulnerability points.

The MTC use cases may be far more variable in latency and volumes of data as some applications use slow-speed communications with relatively small data loads, possibly confined to specific (isolated) locations. How three such different demands are handled from a security perspective is part of a larger question – perhaps a re-engineering of the Internet fabric for different approaches to security to match diverse application demands – especially for the MTC business model. We return to rethinking these Internet basics for 5G security in a later section.

The two ITU business models (URC/LL and MTC) make greater demands on network performance and resilience. Until now, MNOs have been able to offer a best effort regarding reliability performance and down time and for matches to claimed technical benchmarks. 'Best Effort' here means that rather than strictly meeting regulated availability specifications, the MNOs are left free to attempt to meet targets (often set by marketing) with regulated ranges of compliance that may vary by EU Member State (European Commission, Directorate-General for Communications Networks, Content and Technology, 2015).[1] This laxity has been justified, to some extent, due to the nature of radio communications whose transmitted signal strength varies enormously due to the local ambient conditions This is especially true in the upper frequency ranges, for instance beyond 10GHz where the influences of weather, terrain and features such as wet foliage have major attenuation effects so the signal to noise ratio may change by orders of magnitude from one square metre to the next, especially in the shadow of tall obstacles and/or in the presence of multiple reflections.

Thus these two ITU business models of (URC/LL and MTC) require much greater effort to meet

FIGURE 1: Digital data transfer speeds for the various generations of mobile radio in terms of Kilobits/second up to Gigabits/second on a log scale



Sources: author; SCF Associates Ltd, 2021, 2022; digitaltrends, 2021; 5g.co.uk, 2018, 2021; *Vodafone UK, 2022, GSA, 2022 from first version 2020, updated 2021, 2022, web sources last accessed March 2022

technical specifications and to maintain industrial safety and security standards, for example for robotics. This may also hold further risks. For instance, envisaging connection of nuclear power plants with 5G networks, could offer today's rogue states having offensive cybersecurity assets the opportunity to create, at a minimum, disruptions of service and possibly massive loss of life.. Such protective effort for 5G control systems will be expensive in terms of both network engineering to create the secure 5G network and operational costs to maintain the specified levels with minimal down time. It will also require contractual guarantees that may involve health and safety guarantees as under the EU Machinery Directive, The Radio Equipment Directive, Medical Equipment Regulation and the Low Power Directive.

IMPLICATIONS OF A 5G WORLD AT TODAY'S LEVEL OF NETWORK SECURITY

Previous generations of mobile technology were essentially used just for voice telephony and messaging. But today, mobile via LTE-A offers broadband for social networking, e-commerce such as online shopping, e-banking, and any form of online transaction. However, LTE does have security vulnerabilities. 5G promises a new broadband highway with more connectivity. But inherently that capability amplifies the risks brought by its new fields of application with the IoT and real-time industrial deployments.

Unless the threats are countered, they are liable to act as serious downside risks to modern society. If 5G networks are insufficiently protected, the key risks that come with the rewards are twofold:

- Far more devices than ever before will be attached to a network with possible Internet access. The vast majority of devices may be of very simple types (for IoT sensors and actuators) and therefore will be difficult to protect as they have low security capability. But eventually they will number in the billions and perhaps even in the hundreds of billions, together with billions of human users who may share the same network (and air interface and spectrum) to communicate and to deliver services that control our digital infrastructures.
- There will be up to 1,000 times more data in transit over radio links: while 2G GSM mobile offered kbp speeds for data, 3G (UMTS) offers Mbps and LTE-A can provide up to 100 Mbps or more. But 5G data speeds may be between a hundred and a thousand times greater, with 10 Gbps to 100 Gbps. The scope for data loss and intrusion will only increase if effective countermeasures are not put into practice. The differences in speeds of the various technologies leading up to 5G (average and maximum peak data speed claimed) are shown in Figure 1 to compare how 5G, now termed as 'New Radio' for specifications (5G NR) will expand data rates if the technology fulfils its promise.

The substantial use of radio-based digital control systems as the control plane of the infrastructure fabric involves mixing very sophisticated high-security machines with massive volumes of very simple, low-cost devices for IoT applications, all exchanging data at speeds at which conventional security techniques will be overstretched and inadequate. Real-time security measures capable of responding with the low latency that 5G supports will be essential. The risk analysis involved will be of a level unseen before in previous mobile network generations. This means safeguards that have not yet been planned must be in place.

MASSIVE IOT AND CRITICAL INFRASTRUCTURES IN A 5G WORLD

The severity of these risks is illustrated by the possibility of using 5G networks for critical infrastructures – those that support services where the safety and lives of the population may be in jeopardy, as defined by the European Commission for energy, health, industrial processes, emergency services (Public Protection and Disaster Relief – PPDR), transport, and logistics (European Commission, Directorate-General for Communications Networks, Content and Technology, 2015). Massive IoT may bring these critical infrastructures into jeopardy as the foundations of the physical environment will become linked far more inextricably with the Internet and its major vulnerability problems.

The cybersecurity challenges resulting from such potentially broad use of 5G are diverse, including connected and autonomous cars, smart cities, real-time e-health, and new mobile financial payments and banking systems, all of which demand far higher reliability and some of which demand rigid low-latency limits. In view of the strategic threats of the current European war in the Ukraine, 5G could offer stealth channels for information gathering on a far wider scale than previously seen. A nationwide fleet of autonomous vehicles could be surreptitiously programmed act as a national data gathering instrument, especially vulnerable if they are beaming images to LEO (low earth orbit) satellites, a potentially more susceptible channel. The vehicle network could supply data on the location of assets, the local conditions when under attack and movements of key individuals.

In consequence, the overall risk is that the reliance on 5G will be far greater than it has been on past generations of mobile technologies, such as LTE. This is likely to be due to 5G's promise of greater performance. But perhaps it will introduce far more jeopardy. If it promises the capability for powering mission-critical applications that support society and propel the economy then major risk is introduced because:

- Attacks on 5G IoT networks will *mix the cyber and physical* realms, not just the networking domain as processing is immediately accessible.
- The devices used in IoT networks for sensors and actuators are simple and cheap, and they lack the capacity for cybersecurity capabilities in terms of processing power and memory to host complex code as well as any extra hardware; therefore, building secure networks with them is a major challenge.
- The real risks of 5G come from 5G's form of use of the Internet which is a literal extension of its native form, with no extra security measures. In a mobile global network, offering high speed data transfer, that opens the door to unauthorised entry for data and identity theft, phishing, especially theft of financial credentials. Connection to anyone anywhere with absolute trust and without suitable controls and verifications is open to abuse. Some measures for e-tailor payments for instance may be added by the web platform operators for their own payment apps. But these approaches do not prevent downloading of unannounced identifiers and loggers of financial details or substitution of false merchant platforms. Security in the current form of the Internet in terms of authentication of credentials, for instance for naming and addressing, depends entirely on additions by operators – either the MNO or the web platform operators for OTT services. Thus access by minors, criminals for ransom exploits or other extortions is open, via the most common user interface technology. Some

The cybersecurity challenges from 5G are diverse demanding far higher reliability and in some cases rigid low-latency limits

6 billion mobile users are exposed to online crime. Thus in 2021, threats against business increased over 45% and one in three global consumers have been targeted by global fraud [Transunion, 2022][2]

- Moreover, 5G may rely more heavily on *cloud-based processing and storage*, not just for applications but also for its own network management, which introduces a new set of problems in assuring a secure operational environment. This is because the 5G architecture has capability for virtualising its key network management operations in software inside a remote processor, sited in a distant data centre. That reduces the amount of hardware in outside plant, in the field, such as a whole hierarchy complex switches and multiplexers, It offers 'out of area switching' the principle of which is that it is cheaper to carry signals long distance at high speed over fibre optics to the data centres' switching software – and back again to where they are needed – than to purchase, install, provide power and maintain outside plant, in the form of local switches, multiplexers and compression processors for the mobile Core Network, and some of the edge processors between the RAN (radio success network) and the main switching network, the Core Network. The actual location of the data centre may be flexible by the use of virtual machines, in which the subject software is dynamically hosted on any available processor using a virtualisation software layer in which any piece of software of whatever binary format can run on any target machine. However the cloud paradigm and its market is notorious for the laxity of the reliability and care taken by the service providers in ensuring business continuity at the reliability needed by a telecommunications network (of the order of seconds per month). That needs to be enforced via a Service Level Agreement (SLA) with the cloud services provider (CSP) which has been difficult to agree and to enforce. In response, the European Commission is currently bringing out the Data Act, officially to be published in March 2022 to bring discipline and reliability to the cloud services market in the face of major opposition from the CSPs.
- 5G will remain a set of *immature technologies* for some time and may be *insufficiently intrusion tested* for the responsibilities of supporting critical infrastructure.

Consequently, 5G networks may tend to magnify whatever insecurity exists in processes, procedures, and policies for the IoT and for personal interactions. 5G cybersecurity protection must scale up in proportion to IoT vulnerabilities and privacy risks, evolving further in its security sophistication.

However, the basic 5G network architecture as currently explained in the standards includes new types of vulnerabilities, such as:

- Reconfigurable radio systems based on software-defined radios, which requires that the supply chain and subsequent software and firmware updates are carefully monitored;
- Network function virtualisation, which may offer single points of failure;
- Network slicing to enable multiple applications to run over the same network, which may enable the different applications to interfere with each other as the isolation of slices may be compromised by attacks at the operations management level despite countermeasures;
- A structure with a user plane that may need reinforced protection of its messaging and management in basic concept and encryption; and Cloud operations for management and data.

A NEW FORM OF INTERNET MAY BE NEEDED FOR 5G

In response to the concerns raised above, it may be time to move towards a future Internet with 5G that has security built into it, not added on top (much) later. The aim must be to create a new security environment within the proposed 5G architecture(s) to protect interconnection of the sensitive and vulnerable assets at its edges.

This new model will depend on a separation of the old Internet and a novel form of the current Internet in which the underlying security structure would be its foundation. To do this, it would also be necessary to reconsider the underlying software architecture of what forms the basis of the user interface, the World Wide Web, as well as the transport network. In view of the difficulties, this advance may be more viable for a future generation of mobile technology. The use of radio bearers will be the major challenge. One of the many new directions might be in the form of distributed authentication security services.

But if IoT networks are to be built from low-cost components with no cybersecurity mechanisms, a new set of security constructs will be necessary for 5G networking, perhaps in a redefined persistent control plane. That presents a major challenge in creating an overarching radio-centred environment for critical infrastructure applications and personal privacy.

The revision of the concept of the Internet for 5G means rethinking many basic interactions, from naming and addressing to routing algorithms to the loci of control. It also calls for a strategy for migrating from the legacy networking of the Internet of today.

SENSITIVITY TO PRIVACY: THE NEED TO QUANTIFY THE PRIVACY RISK

The expanding volume of personal data on the Internet gathered by both private- and public-sector bodies has raised public awareness and increasing concern about information privacy.

Cybercrime continues to expand rapidly and affect more and more people because fraud and malware are supported by inherent vulnerabilities in today's Internet. The driver for crime is ordinary people storing and sending ever increasing amounts of personal and financial data using mobile devices and networks. Concern about 5G insecurity will be a major barrier to take-up if it is not addressed as the main channel for mobile transactions. Individual security and privacy become essential as a growing portion of people's lives depend on the online environment.

Those links between the public world and the personal world are about to expand at least 100 times (if we assume a high-performance LTE upload/download link of 100 Mbps, which may become 10 Gbps or more).

Sensitivity to privacy intrusion will increase in proportion to data breaches occurring over 5G. There is a need to assess the privacy risk far more precisely and realistically using quantifiable terms.

Countermeasures are needed to address loss of personal information (in a transaction or on a database). With protection of personal data laws such as the General Data Protection Regulation (GDPR), metrics on damages are also needed at the level of *personal injury* for the loss of privacy and the *liabilities* imposed under the legislation.

One essential step is to quantify the various risks of loss of private data. The end goal is to find a way to defend large datasets of personal information. Today's Internet breach environment discloses the interactions among data relationships and data uses, which increases privacy risks. In such cases, privacy sensitivity does not stop at individual

personal data parameters. Private data is often more damaging when applied in concert with other data categories. New data types may be deduced from mining large-scale data breaches, by applying data analytics for sorting, filtering, and cross correlation. Associations of data types may become stronger or weaker, or new classes can even be made to appear which may yield further personal data types. Thus the concept of 'anonymised' data is undermined by modern data analytics.

For instance, income, status, and physical location may be deduced purely from online shopping data that reveals purchasing habits and deliveries. Data analytics enables assessment of the risk values of certain types of data.

Countermeasures imply privacy-by-design and service-oriented privacy-conservation approaches. The optimistic response for the latter is to call for various forms of mutual agreements on data usage and storage, with hopes of trust models that bring results among the various stakeholders (users, MNOs, the Internet over the top, over the top (OTT) platform providers, and apps and their developers and manufacturers).[3] In reality, the industry may not be able to reply adequately or rapidly enough. Instead, national regulatory authorities (NRAs), alongside the data protection and privacy authorities may play a role in exercising far more access control over data flows on 5G networks. They may mandate the structures for data storage and processing and their physical implementation for security, privacy, and reliable operation.

The pressures on 5G network operators to provide security will be far higher, influencing their business processes and financial structures, as external surveillance by regulators intensifies and breaches become difficult to recover from financially. This may follow increases in penalties far beyond the EU's GDPR limit of 4 per cent of annual revenue. Use of cloud-based approaches whereby mobile network operators can store and possibly process personal or commercially sensitive data remotely, and centrally, may become unacceptable. The pressures placed on 5G MNOs as a result of new privacy rules may change the use of the commercial processing architectures of today, with the current forms of cloud-based assets. More robust security may be necessary for database access with 5G networking, as today's remote server level protection may be considered inadequate for the expected volume of traffic. Therefore NRAs and data protection authorities may exercise far more control over data flows and database access over 5G networks.

In such circumstances, far more analysis of the risks and consequences of loss of privacy is essential. Estimating risk values requires an assessment of the probability of a loss and the monetary and other impacts of that loss – the downside in both personal and monetary terms. Note that privacy is included among the EU's core values and is protected in the relevant treaties on democratic values. Thus it is part of the EU Charter of Fundamental Human Rights and is embodied in legislation for cybersecurity, notably the GDPR (European Commission, n.d.). The data protection package adopted in May 2016 aims at making Europe fit for the digital age. More than 90 per cent of Europeans say they want the same data protection rights across the EU, regardless of where their data is processed.

With the amount of data that could be expected to be breached in a 5G network intrusion, the greatest threat is the probability that one type of data will reveal other types of data using quite standard analytics. Together, the originals and the inferences may have much higher value in terms of personal and financial losses to cybercrime.

Income, status, and physical location may be deduced purely from online shopping data

NEW TRUST AND SECURITY PARADIGMS FOR 5G NETWORKS

The integration of IoT applications may intensify the security threat to 5G, specifically in terms of privacy and especially in terms of critical infrastructure. As 5G will need reinforced security it may also be offered in standalone ('private') 5G network configurations if the spectrum regulation authorities permit. These private networks may be built by independent system and network providers (on a design/build/operate basis) as well as by the MNOs, or by the private entity that will be the owner/user. Many combinations using the private model are possible. Some countries are interested in hybrid configurations, with a national shared infrastructure (as in Malaysia and to some extent in Singapore) and a separate service provider who may offer independent 5G network services, These would be disconnected from the national networks. Consequently, this private model responds to a need to move away from today's single, central hierarchical mobile telecoms model that the standards still focus on. The centralised mobile network model offers a single point of failure to critical infrastructure attackers. However, pre-5G mobile networks do have some basic notions of the beginning of emebedded security. For example, LTE ensures the network and its users have a trust model for mutual authentication between all elements, with some privacy protection for data, voice, and messaging across the network, which usually works. But for 5G, far more effective protection is necessary, which is difficult to add after the design has been sold to the market.

For 5G, a single point of failure must be avoided. In its place, a set of distributed control centres for 5G with a specific limit on authorisation may be necessary. This might follow current thinking on distribution of trust in a large network. A distributed series of trust models would need to manage the edge functions as well as multiple central loci of control, which are deliberately redundant for resilience and to avoid single points of failure.

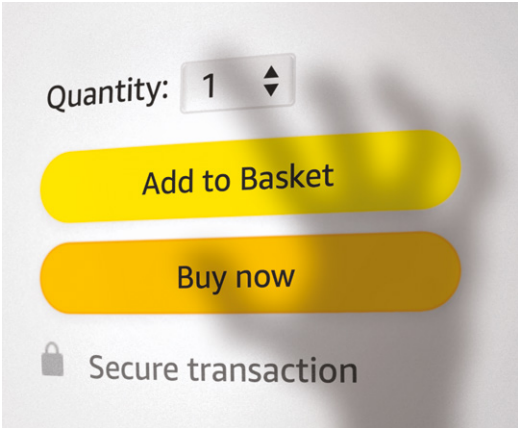
However, multiple centres of control require the establishment of trust between several centres, a difficult task given the rate of advance in malicious techniques for falsifying identity and credentials. If this problem can be solved, it could lead to new trust models for the 5G locus of control. Included in this would be the various operational user and management control layers, each of which would have to be oriented around end-to-end security layers.

WILL THE MOST CRITICAL INFRASTRUCTURE BECOME THE 5G NETWORK ITSELF?

In conclusion, major roll-outs of 5G are being deployed but major IoT applications are still pending. The networks so far are in a nascent stage of developing secure operations. The significant security threats are not yet visible and only partly understood (European Commission, 2019).

Further security measures are already being considered by various standards bodies, such as ETSI for the EU and the main international 5G standards groupings, 3GPP (Third Generation Partnership Project), as well as the IEEE in the United States and the ITU, globally. However, it is possible that the key operational networking layers will only be sufficiently reworked after major attacks have occurred. New standards for 5G managing structures and operational layers that are more resistant to compromise may only be deployed after security becomes the predominant concern, replacing performance.

At a conceptual level, end-to-end security for 5G will require revised principles of operation,



largely following enhanced security models. In this endeavour, instead of security being added as an afterthought, as in the most recent specifications of the 5G architecture, design of the architecture should start with security. However, for 5G it is in some ways too late, so conceptual rethinking is necessary for major points of failure:

- A trust model is needed, one that is appropriate for interactions across a 5G network. This would include its internal software and firmware components, the applications and the data repositories, as well as those entities that seem to be human correspondents, in order to counter all forms of attack. It should also cover the communicating mobile devices and peripheral systems. It may introduce key principles such as zero trust to dictate how the 5G operational networking will interact with active or seemingly passive entities. The fundamental concept is to create a trust model that redefines the bounds of trust of 5G networks.
- A new privacy model is needed that incorporates the monetary value of the loss of privacy to measure security – essentially, privacy is considered an inherent outcome of security – and thus its benchmark. Breaches may be measured in compensation terms for sociological expectations of trust by users. This would impact the network operators and drive suitable countermeasures.
- There is also a need for a multi-tiered model of security with rings of confidence to analyse levels of risk that formalises the vulnerability of the layers of the network – by social groups, individuals, business, technology, as well as regulatory and fiduciary obligations. This must be quite sophisticated in application. For instance, the use of 5G for connected vehicles would have to have high priority, for reasons of safety of life, if used for orienting the vehicle. Equally important, but also for military security, would be measures to keep interchanges to and from vehicles as secure as possible. Because a national population of vehicles reporting constant images of local scenes in high resolution to a constellation the LEO (Low Earth Orbit) satellites would be ideal for gathering information on the state of the country, the location of key citizens and the national conditions when under bombardment, including the effects of cyber attacks on energy networks, pipelines etc.

CONCLUSIONS AND POLICY RECOMMENDATIONS

In essence, we must ask whether the most crucial point of vulnerability of our core critical infrastructures will be the 5G network itself.

A selection of high-level pointers on how to conceptualise the 5G security and privacy threats should include:

- Considering the Internet as far more untrustworthy, with a new operational model having vertical and horizontal secure zones, perhaps using rings of confidence while understanding the inherent security weaknesses in the software architecture of the World Wide Web;
- Reviewing all 5G network operations from the viewpoint of massive attacks;
- For personal privacy, introducing new safeguards to block all additions to the user environment, particularly undeclared tracking apps using enhanced controls over software quality for 5G smartphones, with compliance tests (for example, as in application of Article 4 of the Radio Equipment Directive); Examining the innate risks in 5G's use of cloud technology, both as an insecure operational model and due to the poor

It may be time to move towards an Internet with 5G that has security built into it, not added later

experience of security and reliability of third party cloud service providers (who have priorities that may differ from the MNOs). Cloud technology is now being viewed as a potential hazard in the financial sector (Morris & Noonan, 2022). High cloud dependency could severely disrupt a 5G network through either internal cloud outages or malicious hacking, as the engineering of 5G networks will be increasingly based on hosting 'virtualised' real-time processes and management in remote cloud centres. This degree of remote data centre dependency is far greater than in previous mobile generations.

During the period in which 5G networks are being deployed, further EU initiatives to strengthen the security of 5G networks will be necessary. Current steps towards EU strategic autonomy may well serve such ends.

Here it should also be noted that 5G networks could well become a key part of the EU macroeconomy. This could introduce strategic risks as part of the security challenge that would be associated with 5G supply chains, which bring hazards of critical dependence. Most of the 5G component supply chain is located outside the EU. 5G technology is dependent on the latest advances in integrated circuits, the majority of which are only produced in Asia (generally in Taiwan and South Korea) as 5G requires the latest VLSI (very large scale integration of semiconductor circuits) with 7, 5, and 3 nm gate technology.

EU legislation for 5G cybersecurity is a further area of concern. This will depend on understanding the primary weaknesses of 5G operational networks, devices, and applications. The key risks and the mitigation of those risks must be made clear through suitable EU telecommunications regulations for 5G network operation. These could be prepared in terms of impact assessments that are realistic and also have appropriate normative standards for measuring levels of risk, severity of impacts, and levels of security achieved.

The notion of attribution of responsibility for 5G failures may need to be enhanced to cover the various parties involved. These parties are diverse and include 5G network infrastructure owners and operators, third party cloud providers, application and operating software publishers, including apps developers, for apps loaded by end users, as well as the 5G networking equipment suppliers. The latter will require normative specifications for the 5G network and for particular 5G attachments such as IoT equipment.

NOTES

1. The actual reliability of commercial mobile networks was examined, with research on MNO service levels for critical infrastructures. For instance in one MS, a mobile operator wasout of service for four days and companies dependent on its data services for their business were left with no second redress or compensation.
2. Global Fraud trends of 2021: report highlights increased threats since onset of pandemic. Examines fraud and identity management issues across the globe using a suite of fraud detection tools, summarised for first quarter of 2021 compared to 2020, including Covid-19 related fraud exploits. https://www.transunion.com/global-fraud-trends-Q1-2021
3. 'App' is used here in the traditional mobile industry connotation (originally termed 'Thingz' in 2003) which provides a mobile smartphone with a direct interface to a particular remote commercial application in the sense of a client server relationship, with the app provider having a server platform to provide its particular service – for instance for payments, or to call a taxi, or to order a pizza. Apps may be developed by the service provider, or a by a specialist app developer. There several thousand SMEs (small and medium-sized enterprise) app developers in the EU.

REFERENCES

ETSI (2020). *5G: Security Architecture and Procedures for 5G Systems (3GPP TS 33.501 version 16.4.0 Release 16)* (Sophia

Antopolis: ETSI). https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.04.00_60/ts_133501v160400p.pdf.
European Commission (n.d.). *The EU Charter of Fundamental Rights*, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en.
European Commission (2016). *5G Action Plan: 5G for Europe, Shaping Europe's Digital Future* [Policy], https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan.
European Commission (2019). *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks* [Pres release], 9 October, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.
European Commission (2020). *Strategic Plan 2020–2024: Directorate General Communications Networks, Content and Technology* [Strategic Planning and Programming No. Ares(2020)4565545], 2 September, https://ec.europa.eu/info/system/files/cnect_sp_2020_2024_en.pdf.
European Commission, AIT Austrian Institute of Technology, Fraunhofer ISI, Imec, and RAND Europe (2021). *5G Supply Market Trends* (Luxembourg: Publications Office of the European Union), https://op.europa.eu/en/publication-detail/-/publication/4fbb62aa-f981-11eb-b520-01aa75ed71a1/language-en.
European Commission, Directorate-General for Communications Networks, Content and Technology, Blackman, C., Horvitz, R. & Forge, S. (2014). *Is Commercial Cellular Suitable for Mission Critical Broadband? Study on Use of Commercial Mobile Networks and Equipment for 'Mission-Critical' High-Speed Broadband Communications in Specific Sectors: Final Report* (Luxembourg: Publications Office of the European Union), https://op.europa.eu/en/publication-detail/-/publication/246bc6ec-6251-40cb-aab6-748ae316e56d/language-en.
European Commission, Directorate-General for Communications Networks, Content and Technology (2015). *Is Commercial Cellular Suitable for Mission Critical Broadband?* SCF Associates Ltd, SMART 2013/0016.
Morris, S., & Noonan, L. (2022). 'Regulators fear for lenders' data security as they turn to Big Tech for cloud services', *Financial Times*, 11 January. Regulation (EU) 2016/679, 24 May 2016, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.
Transunion (2022). Global Fraud trends: report highlighting increased threats since onset of pandemic. Examines fraud and identity management issues across the globe using a suite of fraud detection tools, summarised or first quarter of 2021 compared to 2020, including Covid-19 related fraud exploits, https://www.transunion.com/global-fraud-trends-Q1-2021

Cybersecurity and Resilience from a Strategic Autonomy Perspective

Paul Timmers

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Cybersecurity vulnerabilities and incidents are an ever growing and profound threat to the functioning and resilience of our economy, society, and democracy. It is increasingly clear that cybersecurity threats affect the core of the EU's and Member States' sovereignty. Strategic autonomy and resilience in cybersecurity remain a top priority for EU leaders. The EU must act, with urgency, together.

A three-pronged strategy on EU cybersecurity policy is needed from a strategic autonomy perspective: fill the gaps; build bridges between policy interventions; and assert our approach to cybersecurity.

Cybersecurity resilience requires strategic, proactive, integrated, and continuous policy development. Realising this at EU and national level should be a top priority.

THE AUTHOR

Paul Timmers has been Chairman of eGovernmentAcademy's Supervisory Board since 2022. He is visiting research fellow at the University of Oxford, visiting professor at Rijeka University, Senior Advisor to the European Policy Centre and Chief Adviser to the European Institute of Technology and Health. Formerly he was director at the European Commission for e-government, digital health & ageing, smart cities/mobility/energy, cybersecurity and digital privacy. Paul holds a PhD in physics from Nijmegen University and an MBA from Warwick University.

Cybersecurity vulnerabilities and incidents are an ever growing and profound threat to the functioning and resilience of our economy, society, and democracy. It is increasingly clear that cybersecurity threats affect the core of the EU's and Member States' sovereignty. Strategic autonomy and resilience in cybersecurity remain a top priority for EU leaders. The EU must act, with urgency, together.

A three-pronged strategy on EU cybersecurity policy is needed from a strategic autonomy perspective: fill the *gaps*; build *bridges* between policy interventions; and assert our approach to cybersecurity – that is, *EU in the world*.

Concrete, integrated, and internationally oriented policy action is urgently needed – and can be provided – for the security of intellectual property produced in the EU, hardware security and confidential computing, connected products and services in the internal market, security in platform and open-source software development, trusted cloud, cyber-intelligence and cyber-hygiene skills, coping with large-scale cyber incidents and even hybrid war (cyber and kinetic) as we sadly witness with Putin's war against Ukraine.

Cybersecurity resilience from a strategic autonomy perspective requires strategic, proactive, integrated, and continuous policy development. Realising this at EU and national level should be a top priority.

ASSESSING THE PROBLEM

Cybersecurity vulnerabilities and incidents are an ever growing and profound threat to the short-term and long-term functioning and resilience of the economy, society, and democracy, creating a sovereignty gap (Kello, 2017). Resilience is the capacity to recover from disruption (KPMG Belgium, 2021).[1] Strategic autonomy consists of the capabilities,

FIGURE 1: **Five pillars of EU Cybersecurity Strategy**

Source: European Commission EC SWD(2017)295

capacities, and control – the 3Cs – to safeguard sovereignty in terms of in economy, society and democracy (Timmers, 2019).[2] Sovereignty concerns territory; the natural and digital resources 'that belong to us' – the people; authority and recognition in terms of internal legitimacy between the state and citizens; and external legitimacy between the state and third states.

Resilience is therefore a necessary but not a sufficient condition for strategic autonomy. Strategic autonomy and resilience should both be key goals of cybersecurity policy. However, despite top-level political attention and much work on interventions and actions, cybersecurity policy remains in catch-up mode. The sovereignty gap is growing rather than shrinking.

1. There has been impressive progress in EU and national cybersecurity policy. The recent geopolitical situation with Russia as an adversary engaged in a kinetic and cyber-war and China as a systemic rival the EU and likeminded partners show that they can act faster and in a coherent, joint way. However, we should not fool ourselves. Cyber incidents and resulting damage have until now developed even more quickly, and there is little sign that criminals and malicious state actors are being effectively reigned in. We are experiencing concrete cases of breakdown in resilience.[3] This undermines the credibility – the internal legitimacy – of governments. The gaps include:

- The necessary defences are not erected with sufficient speed and are not effective. This concerns technical and organisational means, but also skills, capabilities, and legislative mandates.
- The necessary deterrence is not sufficiently exerted, internationally or extraterritorially.

2. The EU is ever more dependent on foreign suppliers of cybersecurity in critical digital infrastructures throughout the economy, society, and democracy. This affects the internal and external legitimacy of governments. The gaps include:

- The necessary cybersecurity and digital industrial capabilities and capacities are not developing fast enough and control over them is insufficient and even eroding, while incidents escalate and geopolitical tensions mount.
- The EU is not sufficiently projecting internationally its market and diplomatic power in cybersecurity matters in order to strengthen its voice internationally, that is, its external legitimacy.

The risk is that in the EU we start accepting cyber damages as the new normal and underestimate the creeping and irreversible erosion of autonomy and sovereignty.

ASSESSMENT OF EU SITUATION

Policy

Over the past decade, cybersecurity has risen to the top of political agendas. It has become a *Chefsache*, not only in the EU where it has been addressed at several EU summits, but also internationally such as in the OECD, G7, G20, and UN.[4]

Since 2012, EU cybersecurity policy has been developed within a comprehensive framework, the EU Cybersecurity Strategy, which was updated in 2017 and again in 2020. The strategy consists of five pillars: cyber resilience, cybercrime, cyber defence, industry and technology, and international cyberspace (Figure 1).

Substantial *legislative* parts of the EU Cybersecurity Strategy are the cyber resilience Network and Information Security (NIS) Directive and

cyber-crime laws such as on e-evidence and non-cash fraud. The international dimension of these resilience and judicial cooperation laws is relatively weak and partially still under negotiation. The EU Cyber Diplomacy Toolbox includes a legal basis for sanctions in case of cyberattacks which has been activated on a few occasions.

Substantial *financing* for cybersecurity in the strategy is through the EU's research and development (R&D) programmes (Horizon 2020, Horizon Europe), the applied programme Digital Europe, the infrastructures deployment programme Connecting Europe Facility, and the COVID-19 Recovery and Resilience Facility.[5] Funding has also been allocated to international cooperation (for example, the EU–Africa Digital Partnership) (D4D Hub, n.d.). Substantial *governance* has followed from the strategy. This includes a reinforced EU cybersecurity agency (ENISA), Europol/EC3, NIS Directive Cooperation Group and Computer Security Incident Response Teams (CSIRTs) collaboration, and EU Cyber Crises Liaison Organisation Network (CyCLONe).

Initially, there was no strong linkage between the five pillars apart from an overall intention to pursue an 'open, safe and secure cyberspace'. Over time, however, linkages have increasingly been stressed, notably in the 2020 update.

There has been an impressive amount of policy development over the past ten years. However, the rate of cyber incidents has been growing faster than what policy can cope with, exposing policy gaps and limited effectiveness of interventions. Policy also remains fragmented across the EU and between policy areas. The NIS Directive had to be revised, amongst others, because national approaches varied widely. Fragmented policy is illustrated by the lack of explicit linkages between NIS legislation and the Digital Europe programme, the Resilience and Recovery Fund, the Horizon Europe programme or national funds for R&D; and by a lack of programmed internationalisation of EU standards in the revised NIS Directive, NIS2, or the proposed cybersecurity law for the financial sector, Digital Operational Resilience Act (DORA). There is also no institutional linkage between cybercrime and judicial legislation and the security part of the EU R&D programme Horizon Europe.

EU cybersecurity policy over the past ten years has largely focused on resilience and risk management. Only in the last few years, and only little by little, have strategic autonomy and alternative approaches to risk management (such as strategic partnerships of the like-minded) started to be addressed.

Market, industry, skills

Looking at the market, while definitions and estimates vary, the total European market for cybersecurity could, with strong growth estimated to be at least 10 per cent compound annual growth rate (CAGR), be in the order of 50 billion euros by 2025.[6] Cybersecurity expenditure per company varies by a factor of almost three across Europe (Statista, 2010). The list of the most important vendors, according to market research organisations, is overwhelmingly made up of US and Israeli companies, such as Broadcom, Cisco, Check Point, IBM, Palo Alto Networks, Symantec, CyberArk, and Proofpoint. European vendors that are mentioned in market research reports include Sophos, BAE Systems, F-Secure, and Avast (despite the fact that there are thousands of European cybersecurity companies). European vendors have strong positions in secure identity and access management, some position in hardware security modules, and a weak position in security and cloud.

There is much concern about the lack of cybersecurity skills, both professional skills – where there is a gap of some 291,000 cybersecurity professionals – and cybersecurity skills in small and medium sized enterprises (SMEs) and among the public at large (European Commission, Directorate-General for Communications Networks, Content and Technology, 2020).

Cyber incidents are ubiquitous and rampant: one in three companies experienced at least one incident in 2020, although informally it has been reported that most companies experienced at least one incident. Damages were estimated at 5 trillion euros in 2021 according to Cybersecurity Ventures – almost as much as the combined GDP of Germany and France (Econsult Solutions Inc, 2018). Particularly on the rise are ransomware and supply chain attacks (European Union Agency for Cybersecurity, 2021a).[7] The average ransom demand rose from 70,000 euros in 2019 to 155,000 euros in 2021.

CURRENT EU INITIATIVES

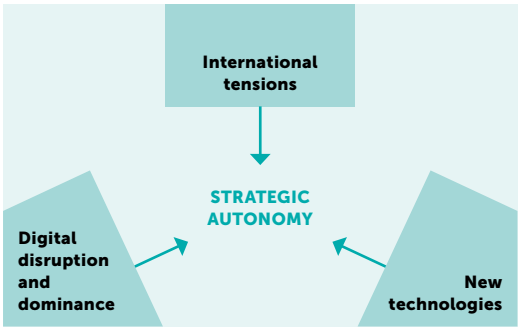
At the EU level, the most important legislation *en vigueur* for cybersecurity resilience is the NIS Directive (2016). It requires cybersecurity risk management from a range of critical service providers. It makes a distinction between selected physical service providers such as energy, transport, and hospitals, where national variation is allowed, and digital service providers (cloud, search engines, e-market places), for whom risk management is harmonised. Understandably this has led to fragmentation, which the proposed revision, the NIS2 Directive, is meant to overcome. NIS2 also extends the range of critical providers and supply chain cybersecurity.

Internal market-wide cybersecurity certification of selected products is addressed by the Cybersecurity Act (2019). Progress has been made on operational governance of such certification and work is ongoing for cloud and 5G certification (European Union Agency for Cybersecurity, 2021b). Also in force is a recommendation on cybersecurity in the energy sector (based on the NIS Directive) as well as specific legislation for the financial sector and recently a Delegated Act on cybersecurity of wireless consumer devices.

The legislative instruments normally include mandatory governance. This is complemented by the non-mandatory cooperation of Member States, European External Action Service (EEAS), and European Commission (EC) services (as well as CERT-EU the CSIRT of the EU institutions, ENISA and Europol), from the tactical/technical level to the political level, in addressing cyber incidents. Especially remarkable is the 5G Security Toolbox, which identified both technical and non-technical risks and demonstrated that Member States can work together and with the EC to establish a common approach even when the core concern is national security.[8] It is a promising example of a win–win situation at EU level. Nevertheless, the 5G Toolbox is no magic wand. It is vague on non-technical risks, and it remains rather soft and permits fragmentation (as it is based on a recommendation only).

Feeding into legislation and cooperation is research and innovation supported by Horizon Europe, as well as innovation, capabilities and skills support by Digital Europe. The focus in 2021–2022 of the latter includes the EU Cyber Shield as an EU-wide cyber-protection capability. Expertise is being reinforced through the Cybersecurity Competence Centre (ECCC) and networking of the Network of National Coordination Centres (NCCs). Further feeding into these is significant standardisation work, involving ENISA and the European

FIGURE 2: **Challenges to strategic autonomy in cybersecurity**



Source: author

Telecommunications Standards Institute ETSI, and national cybersecurity expertise.

Overall support is provided by ENISA whose resources have been increased with the Cybersecurity Act (2019). ENISA addresses cybersecurity best practices, technical and organisational specifications and standards, market understanding, and awareness/skills.

As already indicated, important new initiatives are under way. The French Presidency is committed to moving forward the revised NIS Directive, NIS2, and the proposed *lex specialis* for cybersecurity in the financial sector, the DORA Regulation. As already indicated, where previously the focus was on resilience, these new initiatives give greater weight to the wider challenge of strategic autonomy. Primarily this is the case as they address the security of the supply chain and thereby the trustworthiness of suppliers, not only technically but also in terms of other, more political dependencies. Nevertheless, supply chain requirements are still relatively soft (in the case of NIS2), or non-technical criteria such as systemic dependency are only imposed indirectly (in the case of DORA).

Stronger strategic cooperation should also result from the proposed Joint Cyber Unit, which will bring together cyber-protection capabilities. The European Commission President Ursula von der Leyen announced for 3Q2022 the Cyber Resilience Act, which is to include cybersecurity standards for a wider range of connected products and associated services that are placed on the internal market (Breton, 2021).

While this is all 'pure cybersecurity', there is a substantial amount of related current and pending policy that has high relevance for both cybersecurity *and* strategic autonomy. This includes the eIDAS Regulation (electronic *citizen* ID being a sovereign privilege par excellence), as well as the announced Chips Act, since hardware-based security based on advanced semiconductors is indispensable. It is of prime importance for strategic autonomy to be able to regulate foreign investment and takeovers. The Foreign Direct Investment (FDI) Scrutiny Regulation seeks to pre-empt strategic autonomy-sensitive FDI but is still rather weak (it addresses 'informing' and 'cooperating'). Still, political signals at the national level, in Germany, France, and the Netherlands for instance, indicate a willingness for further strengthening. The integration of 'cyber' in the defence context in the eagerly awaited Strategic Compass will be important for cybersecurity strategic autonomy.

It is against this background of measures that we need to understand (1) whether there are important gaps from a cybersecurity resilience and strategic autonomy perspective and (2) whether what is proposed is sufficiently effective. We can then propose appropriate policy. This is addressed in the next section.

FUTURE CHALLENGES AND OPTIONS

The strategic autonomy challenges in cybersecurity, at a high level, are (Figure 2):

- *The rise in geopolitical tensions*, and notably in US–China relations, pushing for the decoupling of value chains and in China itself the pursuit of 'dual circulation'.[9]
- *Disruptive change* in the economy and society with the wide dissemination of the Internet of Things (IoT), 5G, artificial intelligence (AI), cloud and data-driven business models, and the (sovereign) power shift to oligopolistic trillion-dollar platforms; and, with this, explosive growth in the attack surface for cybercrime and cyber threats, made worse by COVID-19.

- *Radically new technologies* such as AI, 5G/6G, edge and cloud+, advanced semiconductors, High-Performance Computing, smarter IoT, and quantum, most coming more or less at the same time and all essential for the EU's future.

In addition, public policy is hindered from keeping pace and ensuring effectiveness because of *legacy issues*, notably fragmentation in the EU and traditional, slow-paced policymaking.

These challenges involve technological, economic, social, behavioural, and political factors. We do not have a single comprehensive, integrated, and systematic approach to map these strategic autonomy challenges onto cybersecurity and resilience. Nevertheless, we can combine partial approaches.

As one step we can use Figure 3. This stack diagram focuses our attention for each layer on the question: do we have sufficient control or autonomy in the strategic autonomy sense over cybersecurity issues? From this we identify gaps as indicated in the diagram, such as lack of industrial presence in semiconductors that are essential for hardware security, lack of control over trusted cloud, lack of presence in international technology consortia, and so forth. Figure 3 indicates these gaps.

Such a technical diagram does not guarantee completeness of gap analysis. It also does not give much insight into the interplay of factors from (geo-)politics, economy, society, or democracy, and technology. Nevertheless, it can bridge the world of technology and law/international relations/politics.

We can also take a process innovation perspective, as illustrated in the funnel diagram in Figure 4. This diagram reveals process-related gaps for which – from a strategic autonomy perspective – we would need to address capabilities, capacity, and control in the EU. This includes a presence in international software specification and standardisation, and a degree of control on software development such as of software delivered by the GAFAMs (that is, Google, Apple, Facebook, Amazon, and Microsoft) and of open source, controls and capabilities related to data (quality, bias, availability, access), and missing governance in oversight and feedback (for example, no mandatory post-market surveillance on ICT products). Again, such a diagram has its limitations: much innovation does not follow a neat linear process and the diagram does not readily suggest integration of policy measures.

Finally, when we seek to integrate various perspectives, we can make use of a strategic assessment scheme, for instance the one developed by the Dutch national Cybersecurity Council (Timmers & Dezeure, 2021). This can be used to start from *triggers* that raise concern about cybersecurity and strategic autonomy such as major cyber incidents; critical takeovers; geopolitical interventions by the United States, China, or Russia; and so forth. It then combines this with a *systematic analysis* of current market, technology, and political developments as well as *ex post analysis* of the impact and effectiveness of current policy, as is done for policy impact assessment (Biden, Jr, 2021).[10] The approach here (see Figure 5) is to address both cybersecurity and strategic autonomy on the dimensions of specific vs general (sector-wide) and reactive vs proactive.

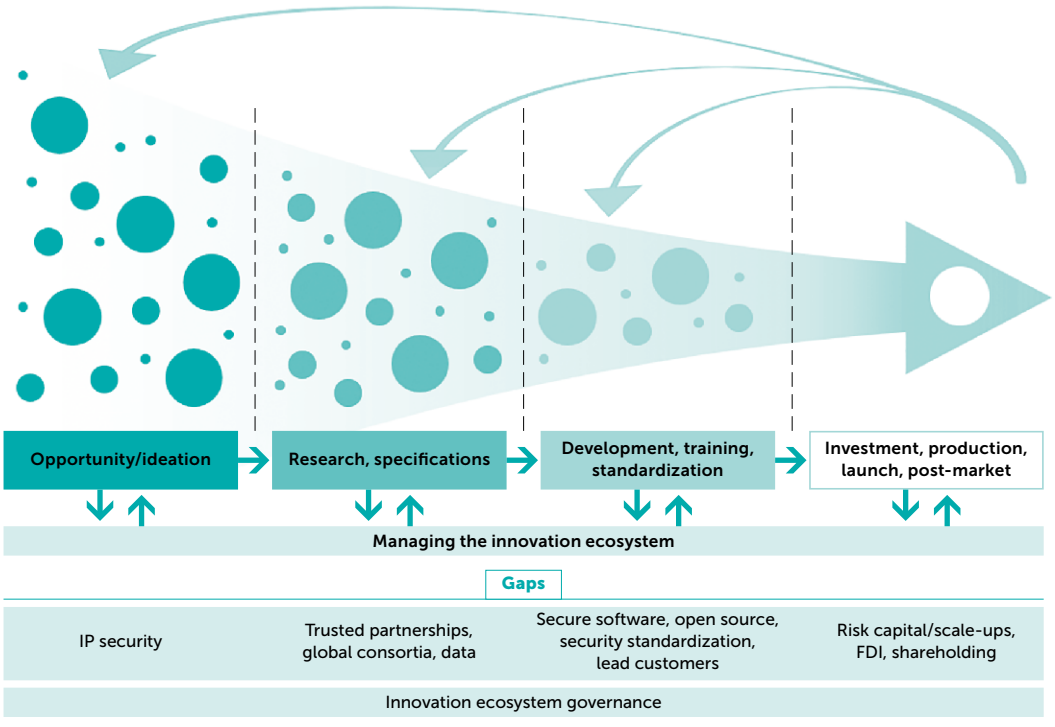
Let's illustrate how we can integrate perspectives. As an example, as a trigger we take the alarming theft of intellectual property (IP) as reported by intelligence agencies, so we address *IP security* as an example. We start in Figure 5 in Q1. What do we have under control in cyber-securing IP against theft and espionage? Clearly, IP from European-funded

FIGURE 3: **Gaps in a layered analysis**

Gaps	Layers	Instruments
Alliances, partnerships, joined-up diplomatic, economic, military presence and response	**People, states**	Cooperation, international law
Professional skills, exercises	**Apps and use cases**	Awareness, skills, self-regulation
Trusted cloud, sovereign eID and trust services	**Services, cloud**	
Platforms, data lakes, supply chain security, basic cloud	**Data and dataspaces**	Regulation
Supercomputing	**Networks and computing**	
Semiconductor industry, industrial quantum, government in IoT and 6G standardization, stake in confidential computing, secure hardware, AI investment, secure open source	**Semiconductors, devices/IoT**	Standards, certification, architectures
	Key enabling technologies	

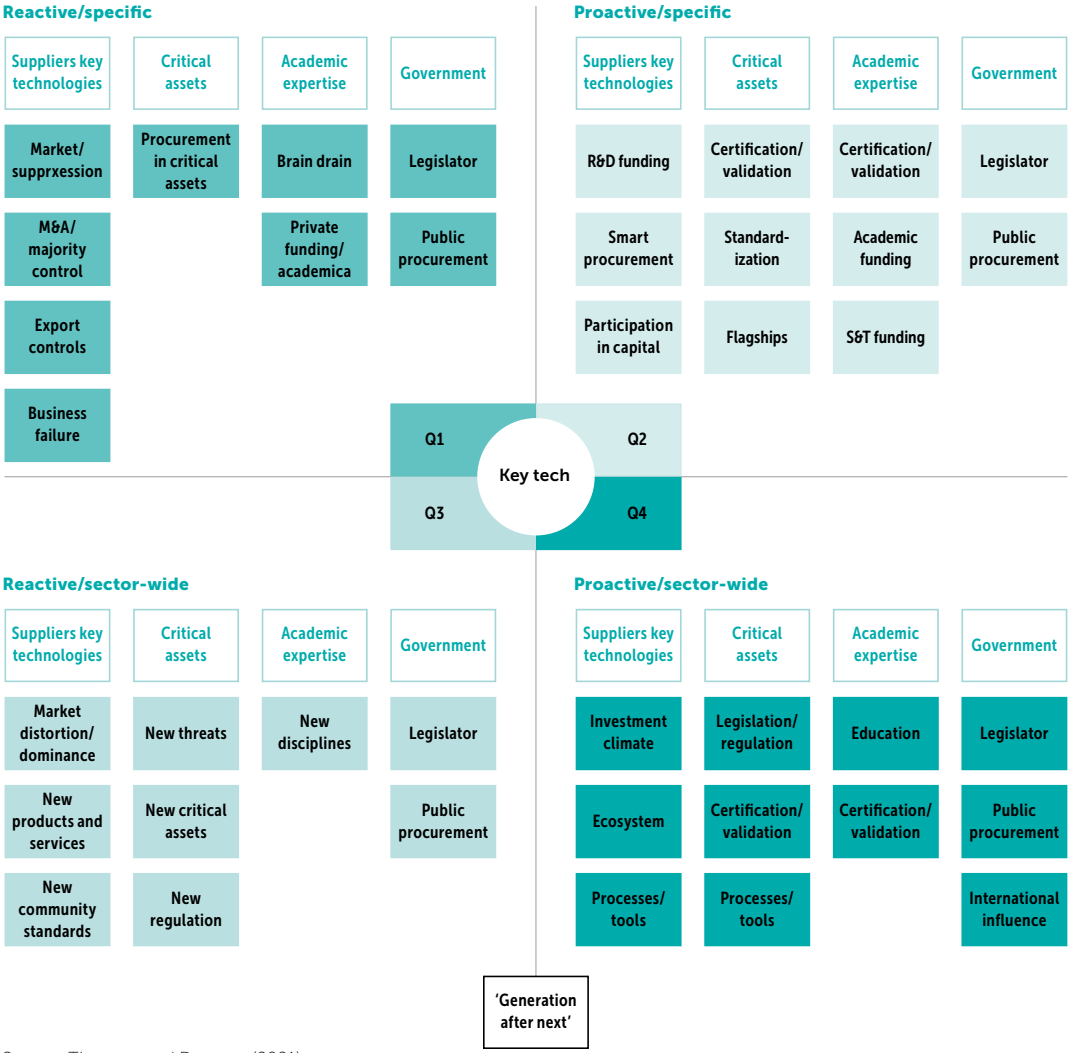
Source: author

FIGURE 4: **Innovation and deployment**



Source: author and http://www.hislide.io

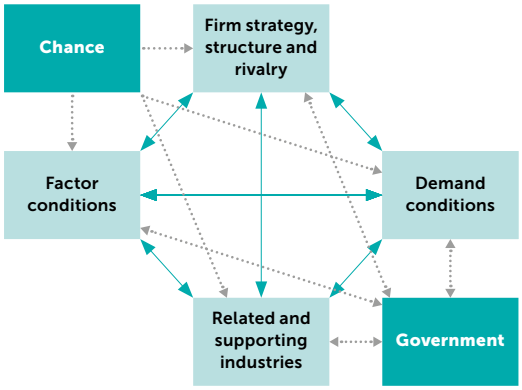
FIGURE 5: **Strategic analysis of cybersecurity and strategic autonomy**



Source: Timmers and Dezeure (2021)

FIGURE 6: **Porter's Diamond model of national competitiveness**

Source: https://hbr.org/1990/03/the-competitive-advantage-of-nations, https://www.business-to-you.com/porter-diamond-model/



research. We can impose IP security requirements in EU research. Can we ourselves cyber-protect IP? In the EU we have limited control over hardware and software (cloud, data management). But this is a wider problem. Therefore, let's look at Q2. Can we consider intervention through the broader instruments (for example, Horizon Europe, NIS Directive, eIDAS Regulation)? Can we involve the broader EU cybersecurity industry? For instance, Horizon Europe work programmes can prioritise research into secure protection of IP, and we can incentivise the EU cyber industry when Horizon Europe and national governments become early buyers. Moreover, legislation could make IP security an economy-wide legal requirement.

Being proactive, that is, moving to Q3, we would consider advanced research to protect IP in the longer-term future, that is, post-quantum, involving private and public parties. But we must consider whether our understanding of the market and industry and of government is complete and coherent. This can be done with an analysis of industry and national competitive ecosystems, such as with the Porter's Diamond model (Figure 6).

Applied to the case of IP security, it highlights that policy action should involve suppliers of knowledge on IP security (for example, research and innovation labs), a proactive demand side (for example, internal market legislation and harmonised protection of IP, and mandatory protection where EU funding is involved), related suppliers such as for cloud and semiconductors that can build in or support strong security, as well as government. In other words, here a private–public partnership would be in order.

Consequently, the analysis leads to the suggestion to link up a semiconductor initiative (such as the announced Chips Act), the Quantum Flagship, and cybersecurity requirements in the internal market (Cyber Resilience Act), and to connect this to the ongoing international development of post-quantum encryption. This may well be reinforced by EU–US cooperation in the Trans-Atlantic Trade and Technology Cooperation. We must, however, take into account and learn from what others are doing (notably China and the United States), and therefore we must also look at Q4 in Figure 5.

In summary, the security of IP produced in the EU is a core cybersecurity and strategic autonomy issue. It can be (and must be) addressed by a combination of legislative requirements, supply-side industry ecosystem investment, and demand-side promotion.

This is only one example. However, the approach can be used generally to identify challenges and gaps and to determine concrete policy actions. It is necessary – although it has yet to be done (!) – to *put in place systematic, continuous, top-level monitoring and analysis of strategic autonomy threats and opportunities*.

POLICY RECOMMENDATIONS

Using the analysis and approach outlined above, the recommendations that follow address 'what' is urgent for cybersecurity and strategic autonomy and also suggests the 'how' of policy action.

Filling gaps

There are two overarching recommendations:

1. *Put in place a systematic analysis of strategic autonomy and cybersecurity* at EU level. For speedier EU policy development, it will be important for Member States to do so too. The alternative is to continue operating in catch-up mode and to be a sitting duck for cybercriminals and third states in terms of EU and Member States' autonomy.

2. *Use the current political momentum now that sovereignty is so clearly under threat* with the acute geopolitical tensions, notably in the relations to Russia and China. The ambition should be with such a framework to join up policy domains as well as to communicate between civil and defence perspectives. The moment is right to do so given increased willingness for accelerated decision-making and for joint action at EU level and with like-minded partners.

In addition, the analysis identified the following as the most immediate concrete gaps and corresponding measures:

- Putting in place *IP security* by means of legislative intervention and private–public partnership.
- Maintaining and strengthening control on *secure hardware* including the hardware security module ecosystem through investments, public interest shareholding, and linking up various legislative and programmatic initiatives such as the EU Chips Act that was recently put forward by the EC and the forthcoming Cyber Resilience Act.
- Ensuring stronger EU presence in *confidential computing* (both homomorphic and multi-party computation as well as post-quantum cryptography) by an EU confidential computing initiative – which can be linked to the ongoing international confidential computing consortium.[11]
- Ensuring ICT security in *connected products* and associated services in the internal market by legislative requirements in the announced Cybersecurity Resilience Act, and consistently linking to this support by the Digital Europe or other, industrial, programmes.
- Addressing *software vulnerability* in closed-source (GAFAMs) and open-source development, to be addressed by legal requirements to providers and international open-source and supply chain security assessment.
- Increasing control over *trusted cloud* to be addressed by EU trusted cloud (building on Gaia-X) and stronger strategic partnerships between subsets of Gaia-X and like-minded parties.
- Preparing for *massive disruption* to be addressed by large-scale and joined-up incident simulation and exercises and international cooperation, which notably can be done in areas of common public interest such as critical infrastructures. Although the war in Ukraine has not (yet) changed the type of cyber-attacks, stark warnings have been issued about the risk of very damaging Russian-sponsored retaliation for imposed sanctions.[12]
- Finally, there are other, harder to address gaps and challenges. Of immediate concern is the *lack of skills*. Firstly, we need to raise political awareness that this is a hidden national security issue. Secondly, we need to explore ways to find a solution to the skills shortage inside instruments where the EU mandate is strong. Upcoming internal market legislation (notably, the Cyber Resilience Act) should contain a skills and capacity-building chapter with associated funding. This can be mirrored at the national level (Cabinet Office, 2021).[13]

Building policy bridges

As will be clear from the analysis, in many instances a well-considered *combination of policy interventions* will be necessary, such as internal market legislation, trade and export rules, financial participation, public procurement, civil–military cooperation, international diplomacy, and so forth. Yet one of the challenges is to build bridges between policy disciplines and their responsible persons, whether at EU or national level. This is due in part to the lack

The rate of cyber incidents has been growing faster than policy can cope with, exposing policy gaps and the limited effectiveness of interventions

of an established discipline of integrated policymaking, and in part to silo-thinking. The latter, however, is irresponsible given what is at stake.

At this stage it seems best to pursue two paths. The first is to address each of the instances of *'filling the gap' in integrated policymaking* and to insist on regulatory scrutiny such that no policy initiative passes the bar unless policy integration has been actively considered and likely been included. The areas that seem particularly suitable to embark upon right away are bridging diplomacy and international standardisation in 5G security and in IoT security; linking NIS2 legislation to funding for skills and capability-building, especially for SMEs; integrating, with funding and investment, the cybersecurity industrial ecosystems in the new initiative in semiconductors and in running ones such as on quantum technologies; and a combination of legislation, standardisation/certification, skills, and trade controls for supply chain security in sectors other than telecommunications.

The second path is one that is at the sharp edge when we address cybersecurity, resilience, and strategic autonomy but is increasingly relevant for other areas too. This is to consider flexible legislation and to *explore co-design law and technology*. The proposal for an EU Artificial Intelligence Act contains small beginnings of such regulatory flexibility in ir provisions on regulatory sandboxing.

The EU in the world

The final set of recommendations concerns the positioning of the EU in the world on the themes of cybersecurity, resilience, and strategic autonomy. In several instances – even if this may sound paradoxical – *EU strategic autonomy may be best served by promoting global technological and standards solutions*, namely in such a way that every state can be reassured about respect for sovereignty, yet solutions remain interoperable and efforts and costs are shared. This is the case in the domain name management of the Internet and a number of elements of Internet security as well as in many open-source solutions. The potential to pursue this approach also exists where global assets can be built such as global and secure collections of pandemic health data and climate data. Moreover, the EU has an interest to promote its solutions globally, to lower the costs of international supply and trade, and because the world is an export market. Finally, the EU is well placed and is probably the more credible partner between China, the United States, and the EU, with its experience in international collaboration and diplomacy.

As indicated earlier, when addressing the gaps, and when building bridges between policy areas, international, global cooperation often should be part of the package. This should be done systematically, from a strategic planning point of view and from an international diplomacy point of view. Areas that could immediately be addressed for the EU in the world in cybersecurity (from a resilience and strategic autonomy perspective) include *participating in international tech consortia* (for example, Confidential Computing) and *international standardisation* (5G/6G, eID and digital wallet, cyber-security incident data, cyber incident impact metrics, risk management and supply chain requirements as in NIS and NIS2 and with a focus on global sectors such as logistics, certification as in the Cyber Act), and addressing *cybersecurity in areas of global public interest*, notably pandemic and other public health threats.

The EU has an interest in promoting its solutions globally, to lower the costs of international supply and trade, and because the world is an export market

CONCLUSION

Cybersecurity resilience in the light of strategic autonomy in the EU requires a strategic, proactive, and sustained approach that integrates policy instrument and policy area, involves the private and public sectors, takes an industrial ecosystem approach, and is willing to consider all-of-society action, in order to defend freedom, fundamental rights, and sovereignty in the EU.

NOTES

1. Resilience can be defined as 'the capacity of an organization to survive, adapt and thrive regardless of what disruption they experience'.
2. Strategic autonomy can be defined as 'the capabilities and capacities to decide and act on essential aspects of the longer-term future of our economy, society and democracy'.
3. In 2021, for instance, the shutdown of Swedish supermarkets, Dutch VDL, a main industrial conglomerate, Portuguese TV station, a German hospital, disruption of Irish NHS; and IP theft at Volvo Sweden. There was also the high-profile shutdown of the US Colonial pipeline and, in late 2020, the European Medicine Agency and the US SolarWinds hacks and rampant disinformation campaigns including on COVID-19. Early 2022, a large disruption happened of the Viasat-owned satellite communications system, a.o. knocking out nearly 6,000 wind turbines.
4. For example, the European Council of 21 October 2021 addressed the 'marked increase in malicious cyber activities'.
5. 269 M Euro in the 2021–2022 work programme.
6. Mordor Intelligence: CAGR of 12.32 per cent (2021–2026); Market Data Forecast: 23.4 per cent, from USD 26.47 billion in 2020 to USD 51.40 billion by 2026; Graphical Research: 13 per cent in 2018 at USD 25 billion; ResearchAndMarkets: 14.9 per cent, from USD 8.56 billion in 2020 to USD 22.67 billion in 2027; OMR: 10.3 per cent (2019–2025).
7. The hardware and software that service providers are buying and likely regularly updating.
8. National security is under the Treaties reserved for the Member States (Art. 4(2), TEU, 'In particular, national security remains the sole responsibility of each Member State').
9. Dual circulation is China's strategy interpreted as stimulating as its basis a strong domestic economy, while benefitting from exports. It is seen as a signal, together with other Chinese policies, of striving to become ever more self-reliant.
10. The Biden administration has set up a Cybersecurity Safety Review Board for systematic follow-up and analysis of cyber-incident triggers of national security (that is, strategic autonomy) importance.
11. https://confidentialcomputing.io/
12. Interview with Kevin Mandia, 29 March 2022, https://www.ft.com/content/018dc68e-0975-4443-b003-f44ab567bd96
13. Inspiration can come from the recent UK National Cybersecurity Strategy 2022, where skills is a conditio sine qua non not only for resilience but also for technological leadership.

REFERENCES

Biden, J.R., Jr (2021). 'Executive Order on Improving the Nation's Cybersecurity', *The White House*, 12 May, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Breton, T. (2021, 16 September). 'How a European Cyber Resilience Act will help protect Europe', *European Commission*, https://ec.europa.eu/commission/commissioners/2019-2024/breton/blog/how-european-cyber-resilience-act-will-help-protect-europe_en.

Cabinet Office (2021). *National Cyber Strategy 2022* [Policy paper], GOV.UK, https://www.gov.uk/government/publications/national-cyber-strategy-2022.

D4D Hub (n.d.). *AU–EU D4D Hub Project: Supporting Africa's Digital Transformation*, https://d4dhub.eu/au-eu-project.

Econsult Solutions Inc (2018). *The Cybersecurity Imperative*, 16 October, http://econsultsolutions.com/the-cybersecurity-imperative/.

European Commission, Directorate-General for Communications Networks, Content and Technology (2020). *The EU's Cybersecurity Strategy for the Digital Decade* [COM JOIN/2020/18 final], https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN.

European Union Agency for Cybersecurity (2021a). *Cybersecurity Threat Landscape*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

European Union Agency for Cybersecurity (2021b). *ENISA Cybersecurity Certification Conference 2021*, 2–3 December, https://www.enisa.europa.eu/events/enisa-cybersecurity-certification-conference-2021/agenda.

Kello, L. (2017). *The Virtual Weapon and International Order.* New Haven: Yale University Press.

KPMG Belgium (2021). *Explore what makes an organization resilient* [Video]. LinkedIn, https://www.linkedin.com/posts/activity-6743230890727489536-Yf4V.

Statista (2010). *Cyber Security Expenditure of European Firms in 2020, by Country*, June, https://www.statista.com/statistics/1008302/european-firms-budget-cyber-security/.

Timmers, P. (2019). *Strategic Autonomy and Cybersecurity*, EU Cyber Direct, 10 May, https://eucyberdirect.eu/research/strategic-autonomy-and-cybersecurity.
Timmers, P., & Dezeure, F. (2021). *Strategic Autonomy and Cybersecurity in the Netherlands*, Cyber Security Council, https://www.cybersecuritycouncil.nl/documents/reports/2021/02/17/report-strategic-autonomy-and-cybersecurity-in-the-netherlands.

EU Digital Strategic Autonomy: The French Experience

Arno Pons

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Freedom of speech in digital services is a major area of concern for Europe. The EU intends to affirm its own rules and its own autonomous vision. The purpose of this paper is to explore the possibility of a new status, halfway between a total lack of responsibility on the part of the host and the full responsibility of the publisher. The taxation model now seems to be significantly challenged by the negative externalities of the digital revolution. This is an area where sovereignty and autonomy must be restored.

THE AUTHOR

Arno Pons is General Manager of the think tank Digital New Deal, which supports political and economic decision-makers to create a third digital way. For 15 years, he has been advising major groups and institutions on their digital transformation strategies. Arno Pons also teaches at Sciences Po Paris School of Management and Innovation, on issues of digital sovereignty linked to the centralisation of powers by Big Tech.

FIGHTING ILLEGAL SPEECH ON THE INTERNET AND PROTECTING FREEDOM OF EXPRESSION

The EU has made it its purpose to defend the rule of law in the era of platforms

Freedom of speech in digital services is a major area of concern for Europe (see Olivennes & le Chatelier, 2021). The European Union intends to affirm its own rules and its own autonomous vision. The purpose of this chapter is to explore the possibility of a new status, halfway between a total lack of responsibility on the part of the online host and the full responsibility of the print publisher. This would make it possible to regulate the freedom of expression of contributors not according to the internal rules of the platforms but by virtue of the law and under the authority of a judge. It is not a question of creating new offences, nor is it a question of leaving platforms free to define their own rules or to be in charge of deciding what is lawful and what is not; rather, it is to ensure compliance with the laws that frame freedom of expression (libel, defamation, incitement to hatred, and others).

The development of the Internet and social networks is constantly raising issues of freedom of expression. Every week, we see a new controversy. Platforms are criticized for allowing hate speech, conspiracy theories and fake news to develop, under the protection of anonymity, when they do not destabilize state operations. This was the case in the United States in times of peace, when they were accused of censoring the president of the United States (or another contributor by virtue of opaque and unjust internal policies); and this is true today in Ukraine when Facebook authorises biases that allow hate messages against the Russian military. The special nature of platforms, which are in some ways, by virtue of their weight and audience, the 'essential equipment' of democracy, justifies our thinking

Current texts do not provide sufficient guarantees for the fight against hate speech or freedom of expression

about how to regulate them in terms of freedom of expression.

The text of the Digital Services Act (DSA) directive, which predates the phenomenal development of digital platforms, is clearly inadequate to address the issues mentioned above. As the French Council of State wrote in its opinion of 16 May 2019 on the Avia PPL, 'the provisions of the e-commerce directive predate the creation of social networks by several years and the scale of the outpouring of hate content calls for urgent action to defend individuals' (Conseil d'Etat, 2019).

The European Council makes the same observation, stating that 'the extension and diversity of new digital business models and services have significantly changed over time and some services have raised new challenges which the existing regulatory framework does not always address' (European Council, 2020). Above all, the affirmation of the dual principle of limited liability of the hosting provider and the prohibition of a general monitoring obligation leads to situations where, in practice, illegal content can remain online for long periods of time at the risk of causing serious damage and/or harm.

To remedy these shortcomings, European institutions have developed codes of conduct to encourage hosting providers to implement the necessary means to fight the presence of illegal content, as provided for in Article 16 of the Directive of 8 June 2000. Therefore, at the initiative of the European Commission on 31 May 2016, a 'code of conduct on countering illegal hate speech online' was adopted, to which Facebook, Twitter, YouTube, and Microsoft subscribed, followed in 2018 by Google+, Instagram, Snapchat, and Dailymotion. Likewise, on 1 March 2018, the Commission issued recommendations on measures to effectively tackle illegal content online (European Commission, 2018). However, these initiatives, even though they are not to be underestimated, are part of a 'soft law' approach that is not very constraining for operators. The resulting degree of protection is thus necessarily limited, particularly for those who are directly affected by hate speech.

Conversely, in the European legislation currently in force, there is no provision for the hosting provider to block content or remove an account. Those actions, even if urgently required, may constitute a serious violation of respect for freedom of expression and are to be performed in compliance with legal procedures. Thus, the current texts do not provide sufficient guarantees either for the fight against hate speech or for freedom of expression.

Several proposals could be made to improve the Commission's proposal without risking censorship by the French Constitutional Court:

- The first could be to set a very short deadline (24 hours) for reacting to a referral by a trusted signatory. This obligation might only concern the very large online platforms (VLOP) (and not the other hosting providers). It should be noted that the code of conduct concluded in May 2016 already assigned such an objective to the VLOP signatories of the agreement.
- The time limit could be reduced to a shorter period for certain duly listed offences corresponding to particularly serious offences (child pornography, incitement to terrorism, and so forth).
- In the same way, the time limits for intervention should not be uniform but should depend on the audience of the beneficiary considered; the presence over a long period of time of content that may be seen by thousands (millions) of Internet users does not have the same consequences as

the same infringement that would concern only a few individuals.

- Penalties for non-compliance with these review periods could also vary according to the nature of the illegal content in question and the precise exemption clauses for the hosting provider defined by the future regulation.
- Hosting providers should draw up internal guidelines for combating illegal content, as defined exclusively by national or European law and not by internal rules of the platforms. This would be legally binding on the users of their services, whose disregard of the rules would make them liable. This charter would include elements relating to the functioning of moderation, the ordering of content, and the parameters of the algorithms and their evolution. The control of compliance with these commitments would obviously be ensured by the public authorities. Any infringement of these obligations is susceptible to call into question the liability of the hosting providers.
- Hosting providers would have a certain duty to monitor content, which does not call into question the principle of the absence of a general obligation to monitor, but which falls within the framework provided by Article 15 of Directive 2000/31/EC of 8 June 2000 (EUR-Lex, 2000).

However, the question of sanctioning hosting providers if they are not diligent enough in removing illegal content remains entirely open. At present, the sanctions imposed in this respect remain negligible. However, sanctions that are too severe must not appear 'disproportionate', as this could lead to self-censorship on the part of the platforms, which would ultimately be detrimental to the exercise of freedom of expression.

Another important question is the absence of a general monitoring obligation. The principle of the lack of a general monitoring obligation must be maintained. However, it is the possible consequences that the hosting provider faces from this, in particular regarding decisions to remove content or access, which must change. This point deserves specific attention (see below). Several additional proposals could be made under this heading:

- A monitoring obligation should be imposed on the hosting providers with regard to beneficiaries of services that have already been sanctioned because of the dissemination of illegal content; with regard to these entities, the powers of removal of content and access of hosting providers in the event of a 'repeat offence' could be reinforced.
- A monitoring obligation beyond a specific audience level; it seems legitimate to subject to exceptional monitoring those entities whose number of subscribers is singularly important and for whom the consequences of a possible infringement could be particularly heavy.
- Platforms carrying out monitoring operations on the content they host should also periodically report on this activity to the national coordinators; this obligation would make it possible to measure the intensity and nature of the activities carried out in this respect.

The question of appeals against the removal of content and access must also be considered. This issue was largely absent from the Directive of 8 June 2000. Nothing was said about the conditions under which the VLOP could remove content they considered illegal on their own initiative or suspend or even cancel the services they offered to certain

beneficiaries. This is crucial in terms of respect for fundamental freedoms and in particular freedom of expression. We can also see how a policy of withdrawing content or access in critical periods, such as electoral campaigns, could have a potential impact on the meaning of the vote and thus on the overall functioning of democracy.

The proposal does establish a complaints system, which is also open to persons who have had their service provision suspended or terminated. Article 17.3 states that these complaints must be dealt with 'in a timely, diligent and objective manner' (EUR-Lex, 2020). It will be agreed that the level of requirement is minimal in this respect.

In this context, the following proposals can be made.

- In the name of respect for freedom of expression, removal of content or access must only be justified by its unlawful nature, that is, ignoring a European or national norm. The European Parliament in its resolution of 20 October 2020 also calls for such a change. Moreover, one may wonder about the constitutionality of a removal for another reason in view of the case law of the Constitutional Council, which considers that free access to the Internet is today one of the modalities of the constitutional principle of freedom of expression. Regarding the protection of the operating rights of hosting providers, it would be surprising if the civil and commercial provisions applicable in this field did not effectively protect their rights on this precise point too. Therefore, 'incompatibility with the terms and conditions of the provider' should no longer be a reason to remove content or access in the future.
- It is also questionable whether certain 'content publishers' should not benefit from enhanced protection against the risk of content and/or access removal. Indeed, such measures can have a major impact on the conduct of public debate or the functioning of democracy. Thus, one could imagine a special procedure for certain beneficiaries of services such as political parties, associations receiving special recognition from the public authorities, and the media. For the media, one could imagine that the hosting provider would not have the right to proceed unilaterally with a decision to remove the information and that this decision would have to be preceded by a prior formal notice allowing the person concerned to put forward their arguments. Similarly, for this category of beneficiaries, appropriate means of redress, particularly judicial, should be provided to enable them to challenge removal decisions quickly and effectively.
- Finally, the issue of measures through which a hosting provider, without actually removing content, leads to its 'invisibilisation', that is, tends to make it disappear by means of sophisticated filtering devices, must also be addressed. These processes should not be overlooked as they result in a form of quasi-removal of content, with no guarantee for the person who issued it. This potentially serious situation, in addition to raising the question of the platform acting as a genuine content publisher, must be considered and given special treatment, either by requiring the hosting provider to notify the author of the content of the 'decision' thus taken, or by prohibiting it altogether.

Last but not least is the question of anonymity. This is the great absentee in this text, which says nothing about this issue, although it is essential. As the Commission nationale consultative des droits de l'homme reminds us in its 2015 report, 'the possibility

The entire tax field is in danger of evaporating from states, thereby cracking the cement of their sovereignty

of anonymity and the use of pseudonyms, which lead to a strong feeling of impunity', are one of the primary causes of the development of hate speech on the Internet (CNCDH, 2016). This is a major issue because it raises the question of the effectiveness of the sanction when the author of the incriminating remarks will in fact escape prosecution. In our view, it is not a question of calling anonymity into question, but of making the transmission of identification data inescapable in cases where it is necessary for the proper functioning of justice.

Several suggestions could be made to fill this gap.

The text should impose an obligation on the beneficiaries of services to prove their identity in order to access them. This would also be an effective way of preventing minors from being present on services to which they should not normally have access. In this respect, Article 8 of the draft regulation on injunctions that may be addressed to hosting providers by national authorities appears to be largely insufficient to combat the impossibility of transmitting identification data to judicial authorities.

This question must therefore respect a major distinction. The transmission of data should only concern hosting providers. Indeed, for removal measures to be effective, they must be able to be applied effectively to the persons who are the authors of the content concerned. Similarly, if it is necessary to go to court to effectively prosecute the persons responsible for the violation, their identity has to be communicated by the hosting provider.

On the other hand, there is no question of any lifting of anonymity regarding third parties. First of all, they may be other beneficiaries of the same service, in which case anonymity may protect the author of the content from certain forms of retaliation for the comments made online. Anonymity is then a form of protection of freedom of expression. This applies in particular to third parties whose knowledge of the author of the content could cause serious harm to those concerned. This is the case, for example, with whistle-blowers, who must be protected by the rule of anonymity; otherwise, they will be exposed to significant risks in the course of their work. It should be noted that the law of 22 December 2018 on the fight against information manipulation already imposes obligations on online platform operators to inform users of their services about the physical or legal persons who pay them remuneration in return for the promotion of information content relating to a debate of general interest.

This measure does not seem to us to threaten individual freedom in our democracies. The mechanisms for the protection of rights and freedoms are sufficiently effective and proven to protect citizens from the use of this power, which could jeopardise their situation or their rights.

DIGITAL TAXATION, THE SECOND ROUND

Providing public services, offering a social protection system, and regulating economic activity are all examples of missions fulfilled based on an efficient taxation system (see Renoux, 2021).[1] Its role is fundamental to our model of society. The state guarantees the general interest through the participation of all citizens, whoever they may be, via taxation. This model now seems to be significantly challenged by the negative externalities of the digital revolution. This is an area where sovereignty and autonomy must be restored.

On the one hand, the immateriality of the value created by the digital giants undermines the principle of territoriality on which the corporate tax system is partly based. On the other hand, the

nature of public services, financed by taxes, is being challenged by competition from private actors, who claim to replace public authorities in the administration of society. There is an urgent need to re-establish tax consent from all actors, the participation of all in our humanist ideal, the consent to our values. This need is urgent because it is the entire tax field that is in danger of evaporating from states, thereby cracking the cement of their sovereignty.

While the health crisis has consolidated Big Tech's power, it is essential to reinstate the societal model we are defending, which has been undermined by foreign digital corporations ostensibly trying to free themselves from it, whereas many French and European corporations, including digital corporations, continue to abide by it. It is a major competitiveness issue, and a consubstantial principle of fairness. This study presents insights aiming at feeding the debate and reinforcing France's actions on the front line of this European and worldwide struggle.

When discussing taxation with politicians or members of the government, giant international digital actors seem to be struck by a mysterious paralysis. If you listened to them, everything would depend on international bodies, Europe, the OECD. The only thing missing is the UN. Yet the ever growing French General Tax Code was not drafted with the prior approval of these bodies. It contains a multitude of international tax provisions and anti-abuse clauses. And yet, suddenly, we have lost all capacity to act, all fiscal sovereignty in the digital field? Indeed, we have been able to tax digital services, and France is willing to accept this provision. France has fallen out with the United States. But the quarrel with America was precisely the reason put forward for not taking any other measures independently, for example, to reject the concept of virtual permanent establishment. For this reason, but also in line with previous decisions, the risk of contravening the conventions was put forward.

Create a tax abuse provision

The United Kingdom did it. The British have introduced a 'diverted profit tax'. The Australians did the same thing. It brings in about 300 million pounds a year to the British Treasury. France has already lost three and a half years since the 2017 report. That is potentially 1 billion euros in tax revenue, but it is also an incentive to adopt more virtuous behaviour.

What we are calling for? A specific tax on profits diverted to France.

This tax would be at a dissuasive level, higher than the corporate tax. This tax would be collected by the procedure of *ex officio* taxation in order to determine the income and expenses attributable to the French operation. This would reverse the burden of proof on the foreign taxpayer, who would then have to prove that the profit determined by the tax authorities is overstated.

This tax is not a corporate tax. It is a tax of a purely internal and fiscal nature that punishes abuses. For purists who would once again risk invoking the existence of tax treaties to do nothing, we have a tax of 3 per cent on the market value of buildings held in France by foreign companies under Article 990 D of the General Tax Code. This tax is not in conflict with international conventions by nature. The fact that it has been drafted surely demonstrates that it is judged that it could be. The one we are proposing could be part of the General Tax Code too.

This tax would apply to all taxpayers, regardless of their place of residence. So it would apply to taxpayers resident in France or not. Let them be reassured, we have no knowledge of French digital

groups that have set up such artificial and convoluted arrangements. 'Name and shame' provisions could be added to damage the image of corporate groups that practice this type of tax evasion.

A significant digital presence in France, without having declared a taxable presence there, even though there is a virtual permanent establishment in economic terms and significant economic substance, would allow the foreign company to be included in the tax. Provision 43 could be made for a payment solidarity with companies of the group established in France, as long as they participate in artificial transactions with the foreign companies (for example by invoicing support services). In the case of companies without a tax presence in France, the tax would be recoverable from French customers as a deduction from the amounts due to the foreign companies concerned.

Coupled with the provisions on virtual permanent establishments, the aim of this tax is to encourage the declaration of a taxable presence in France. The fight against artificial arrangements is one of the future objectives of the European Commission, which encourages states to take national measures where they can.

Taxable income derived from standardised transfer pricing

Finally, the taxable income of foreign companies in France should be determined using the OECD transfer pricing technique.

There is nothing revolutionary about this proposal, since the techniques for determining taxable income by means of transfer pricing, using methods developed by the OECD, are very common practice for tax authorities when auditing international groups and are now frequently used by tax judges and public rapporteurs in their conclusions.

As highlighted in an excellent report by Bénédicte Peyrol, Member of Parliament, on international tax evasion by companies, France General Tax Code is not modern and transfer pricing is dealt with in a lapidary manner in Article 57 of the General Tax Code (Assemblée nationale, 2021).[2] It has always seemed to us that there should be clear rules of the game in tax matters, and that even if the practice of controls makes it possible to rely on these OECD methods, it would be healthy for these methods to be included in our tax law, in order to receive legal support that is more constitutional and more in line with the principle of the hierarchy of norms, rather than creating a piecemeal administrative instruction inspired by these methods.

Once again, it is a question of putting parliament back at the centre of legislative production, of setting the record straight, and of not leaving the executive alone in charge of such an important issue, with considerable financial stakes, or more precisely, its administration.

As we mentioned previously, use of the net operating margin method, which the tax authorities use extensively in their audits, is likely to be very disappointing in digital matters.

The philosophy of Pillar 1 of the OECD's work corresponds to a kind of ultra-simplified 'profit split', aimed in essence at recognising that it was necessary to remunerate local intangibles. In digital matters, for example, this would be the users who, when it is free, are the 'product'.

For the time being, in the absence of US participation in Pillar 1, we seem to be at a standstill in this area, although the proposals of the new Biden administration seem to be charting a new course in global taxation. In any case, things are moving and they seem to be moving in the right direction. However, while we wait for all this to come to

The virtual battlefield is vital: it is the antechamber of a real war

fruition, we can easily use the 'profit split' method which, allows us to recognise the full value of what is happening in France.

Once again, this is a classic method used by many international groups, particularly American ones. This method is well known to the control services and to the Ministry of Finance. If it is used, it will not create a competitive disadvantage for France, particularly since many foreign groups already use it on French soil. It is up to France's control services to use it in a more systematic way going forward.

It is therefore necessary to modernise our ultra-outdated Article 57 of the General Tax Code by including a reference to OECD methods (Legifrance, 2014).

Then, as Bénédicte Peyrol suggested in her report, the tax authorities should issue an instruction commenting on these provisions for use by digital companies (to date, the authorities have only issued an instruction for use by Small and Medium-Size Enterprises (SMEs) on transfer pricing). The administration could work with specialised valuation firms that know how to use this method and have experience of it with a dedicated budget. It could then issue a clear methodology that can be used by auditors in the field and that protects taxpayers in good faith on the basis of the provisions of Article L 80 A of the General Tax Code (taxpayers can invoke the comments of published administrative instructions) (Legifrance, 2014).

Thus, the principles proposed in this report are clear and concrete and must be the subject of a collective and relentless fight. It is true that companies operate according to the rules of the market, but at a time when humanity is facing its greatest challenge, the ecological transition, they must also put themselves at the service of a project that goes beyond them: the collective interest. There is therefore no objective reason why companies operating in a territory should not contribute to its development through appropriate taxation.

This measure does not seem to us to threaten individual freedom in our democracies. The mechanisms for the protection of rights and freedoms are sufficiently effective and proven to protect citizens from the use of this power, which could jeopardise their situation or their rights.

The situation in Ukraine and the Russian disinformation campaign that accompanies reminds us of how important it is to create the conditions to make the Internet a discussion space technologically sufficiently protected and legally sufficiently respected, so that information does not lose against the manipulation of opinion, communication against political propaganda. More than ever, we must defend the rule of law, the only guarantor of our democratic principles.

We must protect individual freedom, but we must also and above all protect our collective freedom. This virtual battlefield is vital; it is the antechamber of a real war.

NOTES

1. Contribution by Vincent Renoux, Digital New Deal, 2021: https://www.thedigitalnewdeal.org/en/digital-taxation-the-return-leg/
2. https://www.assemblee-nationale.fr/dyn/15/rapports/cion_fin/l15b4052_rapport-information

REFERENCES

Assemblée nationale (2021) 'Rapport d'information: no. 4052', https://www.assemblee-nationale.fr/dyn/15/rapports/cion_fin/l15b4052_rapport-information.pdf.
CNCDH (2016) 'Rapport d'activités 2015', https://www.cncdh.fr/fr/publications/rapport-dactivites-2015.
Conseil d'Etat (2019) 'Avis sur la proposition de loi visant à lutter contre la haine sur Internet', https://www.conseil-etat.fr/avis-consultatifs/derniers-avis-rendus/a-l-assemblee-nationale

-et-au-senat/avis-sur-la-proposition-de-loi-visant-a-lutter-contre-la-haine-sur-internet.
European Commission (2018) 'Commission recommendation on measures to effectively tackle illegal content online', C(2018)1177, https://ec.europa.eu/transparency/documents-register/detail?ref=C(2018)1177&lang=en.
European Council (2020) *Shaping Europe's Digital Future – Council Adopts Conclusions* [Press release], 9 June, https://www.consilium.europa.eu/en/press/press-releases/2020/06/09/shaping-europe-s-digital-future-council-adopts-conclusions/.
EUR-Lex (2000) 'Article 15 of Directive 2000/31/EC', 8 June 2000, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031.
EUR-Lex (2020) 'Proposal for a regulation of the European parliament and of the council on a single market for digital services (Digital Services Act) and amending directive 2000/31/EC', https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.
Légifrance (2014) 'Code général des impôts', article 57, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000029355359/.
Légifrance (2017) 'Code général des impôts', article 80, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033971416/.
Olivennes, D. & le Chatelier, G. (2021) 'Defending the age of law in the era of platforms: fighting illegal speech on the internet and protecting freedom of expression',
Digital New Deal, https://www.thedigitalnewdeal.org/en/defending-the-rule-of-law-in-the-age-of-platforms/.
Renoux, V. (2021) 'Digital taxation: the second round', *Digital New Deal*, https://www.thedigitalnewdeal.org/en/digital-taxation-the-return-leg/.

Part 2

International Partners' Views

Reconciling Digital Strategic Autonomy with Transatlantic Partnership: A US–EU Agenda

Daniel S. Hamilton

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Renewed EU–US solidarity in the face of Russia's war in Ukraine and multi-dimensional challenges posed by China is shifting EU debates over 'strategic autonomy' to discussion of European 'strategic responsibility.' This is most noticeable in the areas of defense and energy, but it is also affecting EU notions of 'digital strategic autonomy.' US–EU commercial disputes continue, but now in the context of transatlantic unity rather than division, amidst growing recognition that the transatlantic economy is the geo-economic base for both sides of the North Atlantic in an age of disruption. This mixture of competition within a frame of deeply integrated cooperation plays itself out across different sectors of the digital economy. Four sectors merit particular attention: ICT and cloud services; semiconductors; artificial intelligence; and clean technologies.

THE AUTHOR

Daniel S. Hamilton is Austrian Marshall Plan Foundation Professor and formerly Executive Director of the Center for Transatlantic Relations Johns Hopkins University, SAIS. He has also directed the Global Europe Program at the Woodrow Wilson International Center for Scholars and has served as a senior US diplomat.

THE AUTONOMY MUDDLE

The term 'digital strategic autonomy', now popular in some European circles, is derivative of an earlier discourse within the French strategic community, which came up with the phrase 'strategic autonomy' to describe France's ambition to boost its military capabilities and reduce its dependencies so that it could act alone if necessary to protect French interests, beginning with crisis management operations in Africa and along Europe's southern periphery.

About five years ago, France's national debate was elevated to the EU stage as concerns in Europe mounted about the United States' reliability as an ally under Donald Trump, China's rising technological and norm-setting challenges, and signs that the EU could be trampled as the American and Chinese elephants collided. Debate was further energised by signs of faltering European technological prowess, and especially by the COVID-19 pandemic, which exposed European dependencies across a number of health-related sectors.

The term has now assumed a far more expansive meaning. European concerns have spawned a raft of related phrases, such as 'economic sovereignty', 'health sovereignty', 'technological sovereignty', 'data sovereignty', 'cybersecurity sovereignty', 'digital sovereignty', and now 'digital strategic autonomy'. The result, as one European observer noted, is a 'muddle of words' (Libek, 2019). EU member states muddy things further by interpreting these assorted phrases very differently according to their diverse strategic cultures, threat perceptions, and calculations of self-interest.

Taken together, however, this jumble conveys a shared and deeply felt anxiety among many Europeans that their grand experiment of integration is being imperilled by internal weaknesses and external forces. In all its forms, the autonomy

narrative has been used to generate EU-wide consensus behind ambitious and often costly initiatives to bolster the bloc's technological, industrial, and norm-setting capabilities in ways that their proponents believe can preserve European competitiveness, lower strategic dependencies, and improve the EU's ability to resist geo-political or geo-economic coercion.

While 'strategic autonomy' has been popular in some European countries, it has rankled opinion in others. Policymakers in Finland, Sweden, Estonia, and the Netherlands, among others, have preferred to talk about Europe's strategic *responsibility*, which entails more substantial contributions to regional security, the readiness and ability to act together rather than alone, and downplays implicit trade-offs between a strong Europe and a strong transatlantic partnership (European Union, 2022).

Against the backdrop of Russia's brutal war in Ukraine and impressive US–European solidarity in response, there are signs that the EU debate is moving away from discussions of strategic 'autonomy' to that of strategic responsibility, and what that is likely to entail. The March 2022 EU Strategic Compass, for example, only refers to 'strategic autonomy' once, whereas it refers repeatedly to the EU's commitment to reinforce its 'strategic partnership' with NATO, and for Europe to take on greater responsibility for its own security in partnership with the United States, NATO, and other institutions and countries. Faced with a revanchist Russia and a revisionist China and finding renewed strength within the US–EU partnership, EU notions of 'autonomy' seem likely to turn on efforts to wean EU countries off of uncomfortable dependencies on Moscow and Beijing, while strengthening the deep connections that bind the two sides of the North Atlantic.

In this context, notions of 'digital sovereignty' or 'digital strategic autonomy' are also now evolving. According to EU Internal Market Commissioner Thierry Breton, digital sovereignty rests on three pillars: 'computing power, control over our data and secure connectivity' (Breton, 2020; see also Csernatoni, 2021). This requires the EU to free itself from its hardware and software dependencies on dominant external countries and companies. On paper, the agenda is rather breath-taking, extending from 5G/6G, artificial intelligence (AI), technological standard-setting, and infrastructure upgrades to supply chain resilience in key sectors such as semiconductors, pharmaceuticals, and critical materials. In reality, efforts are moving in fits and starts.

THE TRANSATLANTIC DIGITAL ECONOMY: COMPETITION WITHIN A FRAMEWORK OF DEEP INTEGRATION

There is a great deal of transatlantic competition across the transatlantic digital economy, as firms compete for advantage and as the US and the EU both seek to enhance the competitiveness of their companies in future technologies. US concerns centre on the motivations behind the collapse of the US–EU Privacy Shield governing transfers of personal data, the protectionist impulses behind the Digital Markets Act, industrial strategies intended to promote 'European champion' companies, and the EU proposal for a carbon border adjustment mechanism, which could disadvantage non-EU companies. The EU worries about the Biden administration's efforts to strengthen 'Buy America' rules, its proposals for electric vehicle tax credits, and its decision to postpone but not resolve transatlantic disputes on US steel and aluminium tariffs. Each party's efforts to subsidise its own digital economy could lead to subsidy wars that would only benefit China.

There are signs that the debate is moving away from discussions of strategic 'autonomy' to that of strategic responsibility

Despite these competitive pressures and ongoing disputes, Putin's war and China's tacit support of Russia's aggression have underscored how deeply reliant each side of the North Atlantic remains on a vibrant and resilient transatlantic economy, including its digital drivers. The transatlantic theatre is the fulcrum of global digital connectivity (Hamilton & Quinlan, 2022). Transatlantic flows of data continue to be the fastest and largest in the world, accounting for more than half of Europe's global data flows and about half of US flows. US exports of ICT-enabled services to Europe in 2020 were roughly double those to the entire Asia-Pacific region. The US, in turn, accounted for 22 per cent of the EU27's ICT-enabled services exports to non-EU countries, and 34per cent of EU digitally enabled services imports from non-EU countries in 2020. The EU's digital trade with one country – the United States – surpasses its digital trade with Asia and Africa combined.

Even more important than trade, however, is the delivery of digital services by US and European foreign affiliates. ICT-enabled services supplied by US affiliates in Europe were more than double US ICT-enabled exports to Europe, and ICT-enabled services supplied by European affiliates in the US were double European ICT-enabled exports to the US.

This mixture of competition within a frame of deeply integrated cooperation plays itself out across different sectors of the digital economy. Given space constraints, I will briefly discuss four: ICT and cloud services; semiconductors; artificial intelligence; and clean technologies.

ICT AND CLOUD

US and European goals in the ICT and cloud sectors align in various areas. However, instead of building on dense transatlantic digital interconnections and the shared principles that underpin them, in recent years the two parties have allowed a series of digital disconnects to roil US–EU relations.

Three developments in the deeply intertwined transatlantic cloud market bear watching. First is the shift in providers of cloud-like services from European and US telecoms companies to 'hyperscalers', mainly from the United States. While European providers have more than doubled their cloud revenues since 2017, their market share in Europe has declined from 27 per cent to under 16 per cent, whereas Amazon Web Services (AWS), Microsoft Azure, and Google Cloud now account for 69 per cent (Hardesty, 2021). This has generated concerns within Europe about US dominance, which could inhibit some possible avenues for deeper transatlantic cooperation. However, two other trends have the potential to mitigate such concerns, depending on how they unfold.

Firstly, by 2025, 80 per cent of all data is expected to be processed in smart devices closer to the user, known as edge computing. This could open opportunities for European providers able to offer multi-cloud options that ensure local control over data with the amplified possibilities that come from hyperscaled connections (European Commission, 2021a). Secondly, the evolution of 'cloud-as-a-service' to 'cloud-as-a-product' means that some European telecoms operators and companies in a range of other businesses now see their biggest opportunities in the cloud building on top of the basic infrastructure already rolled out by US companies, rather than trying to build their own. For instance, Siemens is building an ambitious 'industrial cloud platform' on top of the basic cloud infrastructure provided by Amazon, to enable it to become a key player in digital industrial manufacturing services. Thales, a French defence company, is forming

Each party's efforts to subsidise its own digital economy could lead to subsidy wars that would only benefit China

a joint company with Google to provide a sovereign hyperscale cloud service in France. Vodaphone has also formed a partnership with Google, and AWS will soon start selling private 5G networks directly to businesses (Pannier, 2021; Waters, 2021).

If one analyses the full technology stack, important opportunities emerge. Whereas the EU is relatively underdeveloped compared with the US in higher technology layers such as AI and platforms, the US is relatively underdeveloped compared with the EU in key parts of lower technology layers such as 5G. Moreover, after initial transatlantic turmoil generated by US efforts to oust Chinese 5G telecoms from critical networks, not only at home but in Europe and elsewhere, many – but not all – European allies have also acted to marginalise those companies' presence in their networks.

An overall bargain could conceivably be achieved by joint efforts to enhance open radio access network architectures (Open RAN), align on privacy standards, and guard against external and internal security threats and market abuses, coupled with US willingness to grant European firms greater access to its domestic 5G market and European willingness to cooperate more closely on platforms and AI. Since the potential gains and pains from such an overall arrangement would affect particular industry sectors and individual countries differently, opposition to such an overall arrangement could be significant. Yet the pieces are there.

A start could be made via US–EU efforts in the Transatlantic Trade and Technology Council (TTC), which the two parties created in 2021. It would be useful for both parties to reaffirm their joint commitment to core principles, such as transparency in legislation and regulation; the independence of regulatory authorities; open networks for consumers to access and distribute information, applications, and services of their choice; the importance of a strong and competitive shared environment for ICT development and use; strong yet flexible intellectual property (IP) laws; interoperable data protection regimes that enable innovation while also protecting privacy; agreement that governments should allow foreign participation in their ICT services; affirmative policies in support of digital trade; science and technology cooperation related to digital innovation and research; and robust international cooperation to manage policy differences. In addition, the two parties should foster industry codes of conduct for data protection in the cloud, building on efforts currently underway on each side of the Atlantic. If the two sides of the Atlantic prove able to harness their joint potential based on these principles, they could form the core of a wider technology alliance of like-minded democracies that can prove more vibrant than autocratic alternatives (IT Law Wiki, 2011; Wallace, McQuinn, Ezell & Castro, 2018).

SEMICONDUCTORS

The leading supply chains of common interest to the US and the EU revolve around semiconductors, which the two parties have called 'the material basis for integrated circuits that are essential to modern-day life and underpin our economies'. In this area, the two parties have acknowledged that they have 'some important respective strengths as well as ongoing, significant mutual dependencies, and common external dependencies'. Each has announced initiatives to mitigate those dependencies, improve security of supply, and boost their ability to design and manufacture the 'most powerful and resource efficient semiconductors' (White House 2021a, 2021b).

To understand how the US and the EU could accomplish these goals, it is important to look

at the key elements of highly fragmented, highly specialised, and global semiconductor production networks. The key stages are design; fabrication; assembly, testing, and packaging (ATP); and production of semiconductor manufacturing equipment (SME). While specific companies and countries may be leaders in one or more elements of the overall process, none has a lock on all (see Bown, 2021).

US enterprises are global leaders in SME production and in semiconductor design and associated design tools. European firms also show strength in design and SME production, and in some materials key to the semiconductor manufacturing process. The EU has a strong position in certain subsegments such as discrete semiconductors (global sales leader), analogue integrated circuits, microcontrollers, power electronics, sensors, chip architecture, and advanced chip-making equipment. The EU is also well positioned in the 'More than Moore' market (products made up of a mix of semiconductors), as well as in dedicated processors for applications in the automotive and industrial sectors (including machinery), which are all expected to grow significantly in the future (Szczepanski, 2021). Despite these respective strengths, each party relies heavily on third countries for highest-end chip manufacture, critical materials, and assembly packaging and testing.

Whereas EU leaders have used 'strategic autonomy' to animate their efforts to alleviate semiconductor supply chain dependencies, US leaders speak of 'decoupling'. The decoupling metaphor is easy to understand because it evokes a simple image of disconnecting a cable, in this case a worrying link to China. If drawn to their ultimate conclusions, however, both terms would wreak havoc on the US, European, and global economies. Despite each side's push for self-reliance, achieving fully independent chip supplies is unrealistic given the highly complicated, specialised, and global nature of semiconductor supply chains. Moreover, neither term is an accurate depiction of actual US or EU policies. Neither party is really trying to break free of its interdependencies; each is more intent on redefining the terms of those interdependencies in ways that can enhance its relative security and prosperity. Given each party's relative balance of strengths and weaknesses, the best course for the US and the EU to enhance security of semiconductor supply is not to 'decouple' or become fully 'autonomous' from all other semiconductor producers; it is to ensure that other semiconductor producers remain dependent on them, by doubling down on areas of strength (see Beattie, 2021; Busvine, 2021; Cerulus & Barigazzi, 2021; Duchâtel, 2021; Hancké, 2021; Jones, 2021; Miller, 2021; Poitiers & Weil, 2021).

For the US, this can mean efforts to mitigate strategic vulnerabilities such as reliance on foreign semiconductor fabrication, and assembly packaging and testing. It means working with the EU and other like-minded countries to ensure reliability of supplies of critical materials. Most of all, it means reinforcing US strengths in semiconductor design and SME production. For the EU, it means acknowledging that becoming completely autonomous in high-end semiconductor fabrication is just 'not doable', as EU competition chief Margrethe Vestager has acknowledged – not only because the EU has neither the incentives nor the resources to overtake the world's leading high-end fabricators, but also because the EU itself has relatively low demand (see Amaro, 2021; Hetzner, 2021; Kleinhans, 2021; Poitiers, 2021; Poitiers & Weil, 2021; van Manen, Gehrke, Thompson & Sweijs, 2021; Waters, 2021). As a whole, the EU accounts only for 9 per cent of global semiconductor imports, while Asia accounts

for 83 per cent of exports and 81 per cent of imports. Instead, the EU should focus its resources on areas of strength by fostering semiconductor subsectors upon which other countries, including the semiconductor superpowers, are reliant. Those strengths include research and development (R&D) projects in chip and software design, SME, and materials innovation for important chip manufacturing inputs, such as chemicals, sensors, power electronics, embedded security solutions, and security chips. Furthermore, potential exists for transatlantic complementarities and synergies.

While the TTC's potential regarding semiconductors is currently limited by France's insistence that the focus remain on 'short-term supply chain issues' rather than longer-term strategies, it offers a chance for the two parties to harness their respective strengths and mitigate their respective dependencies within semiconductor supply chains. The two parties have already agreed to jointly identify gaps and vulnerabilities, map capacity in the semiconductor value chain, and strengthen domestic semiconductor ecosystems. They could conduct a joint assessment of supply chain vulnerabilities, improve transparency throughout the semiconductor supply chains, build synergies between the US National Science Foundation and the Horizon Europe framework programmes, and work to design new microchips that could perform better – and require less energy – than silicon. US–EU cooperation could form the core of a broader semiconductor consortium of like-minded nations, including Japan, Taiwan, and South Korea, that could also consider forging a common innovation base with R&D of next-generation semiconductor designs and materials (Rasser, Arcesati, Oya, Riikonen, & Bochert, 2020; Barker, 2021; Gehrke, 2021; U.S. Chamber of Commerce, 2021).

ARTIFICIAL INTELLIGENCE

McKinsey estimates that widespread adoption of AI could grow European economic activity by almost 20 per cent by 2030. However, even though the EU has more specialised AI researchers than the US or China, it lags in AI investments, adoption, and R&D spending. The EU's fragmented market hampers the scale-up of small and-medium sized AI and blockchain enterprises and constrains the access of such firms to the creation of large, cross-country pools of data for building and testing their algorithms, limiting their ability to compete globally (Bughin, Seong, Manyika, Hämäläinen, Windhagen, & Hazan, 2019; Castro, McLaughlin, & Chivot, 2019).

When it comes to AI, the European Commission has prioritised risk management and trust. It has introduced draft legislation for a new regulatory framework through the Artificial Intelligence Act (AIA), which is the first effort to create a comprehensive AI law and another example of EU efforts to lead the world in making rules to govern the digital economy, which tracks with parallel efforts to regulate online content, competition in digital markets, and other areas. While a final law is only likely to emerge after several years, the current draft would apply to any company selling an AI product or service in the EU, so would be extraterritorial in nature, and thus could become a flashpoint between Washington and Brussels (Benaich & Hogarth, 2021; European Commission, 2021b; Veale & Zuiderveen Borgesius, 2021).

Despite potential transatlantic challenges, US policymakers share the EU's interest in mitigating risks associated with AI. US National Security Advisor Jake Sullivan welcomed the European Commission's AI draft, indicating the Biden administration's potential interest in fostering 'trustworthy AI' (Sullivan, 2021). The White House Office of Science and Technology

Even more important than trade is the delivery of digital services by US and European foreign affiliates

Policy is working with stakeholders to develop an 'AI bill of rights' that would guarantee protection from biased or inaccurate algorithms, ensure transparency, and safeguard citizens from pervasive or discriminatory surveillance (Lander & Nelson, 2021). In addition, even though the US is the world's AI leader, with the largest share of private investment, the most start-ups, and strengths in AI talent, R&D, data, hardware, and commercialisation of innovation, US public and private leaders are concerned about the country's ability to maintain this position, particularly in the light of rising Chinese competition. Here, too, there is potential for greater transatlantic cooperation (Aaronson, 2020).

US and EU policymakers are aligned around two core themes for AI policy: (1) enabling innovation and competition, and (2) ensuring trust and accountability. But there are important differences in these policy approaches. Washington tends to focus on the importance of innovation and growth, greater R&D funding, and light-touch regulation, whereas Brussels tends to focus on risk management and trust. The TTC could play a role by exploring to what extent these approaches can be aligned behind a US–EU effort to enable safe and responsible AI innovation and adoption globally. Whether the two parties can avoid costly divergence in the regulation of AI in the future will become apparent as discussions move to legal definitions and metrics for risk management requirements. The task is to seek common or complementary positions that balance AI risks against the risks inherent in slowing technological innovation. As Nigel Corey of the Information Technology and Innovation Foundation (ITIF) warns, the United States and the EU should seek common principles, norms, and regulations, 'but they should not expect to achieve complete convergence' (cited in Broadbent, 2021).

CLEAN TECHNOLOGIES

Digital technologies are transforming the way energy is produced, transported, and consumed. They will be indispensable to decarbonisation. Here again, competitive considerations come into play, as each side of the Atlantic is focused on promoting its own clean-tech commercial breakthroughs. Nonetheless, the immense scale of the climate challenge gives the two parties both need and opportunity to harness their respective strengths. European research and early-stage development of low-carbon technologies continues to be world-beating. Yet the EU is relatively weak when it comes to scaling and commercialising its innovations. The United States, in contrast, accounts for more than 65 per cent of global clean-tech growth equity funding and venture capital investments, yet it trails in areas of low-carbon research where Europe is strong. Given the deeply integrated nature of the transatlantic innovation economy, both parties stand to gain by harnessing their relative synergies to promote scaled-up demonstration projects that hold promise for commercialisation (CleanTech Group, 2021).

Such efforts are not just 'nice to do'; they take on added urgency when considering that autocratic governments such as China do not necessarily need to rely on purely market-based approaches to deploy the technologies of the future. Beijing directs massive resources to promote its own competitors in many clean-tech areas, based on differing norms than those likely to be found in democracies. A cautionary tale is offered by the solar industry, where pioneering US and European companies once led global markets. Today, thanks to substantial government subsidies, forced technology transfer, and predatory pricing, China produces three-quarters of global supplies.

Governments can set incentives and market signals to help make clean-tech innovations commercially viable

Leaders at the June 2021 US–EU summit pledged to 'work towards' a Transatlantic Green Technology Alliance. Both parties must use the TTC to make it real. A Green Technology Alliance could help both parties align on technical standards, address regulatory discrepancies, and mobilise public and private investment to rapidly scale up breakthrough technologies in hard-to-abate sectors so they can become more affordable, accessible, and attractive than their traditional, higher-carbon counterparts (Gates, 2021).[1] This will require greater public investment in demonstration projects, which is a major weakness in the clean energy innovation system. Public investments should not and cannot take the place of the far larger resources the private sector can bring to bear, but private investment is currently deterred by the high costs and risks still associated with scaled-up clean-tech demonstration projects. Governments can set incentives and market signals to help make clean-tech innovations commercially viable, spurring further investments and paving the way for widespread adoption and deployment by the private sector (Gates, 2021; Nguyen, Koester, & Hart, 2021; Simms Gallagher, 2022).

A related challenge is posed by the flow of critical raw materials. The International Energy Agency projects that global demand for critical materials generated by the widespread deployment of clean technologies will quadruple by 2040 and increase sixfold by 2050. EU demand is slated to increase tenfold (International Energy Agency, 2021; Sanderson & Sheppard, 2021). The largest reserves of such materials are in developing countries already struggling to lift their populations out of poverty even as they commit to low-carbon development. Many developed countries are likely to be as dependent on these critical-materials producers as they have been on fossil-fuel suppliers. The issue is particularly sensitive because the US and the EU are both inordinately dependent on China for many critical materials, potentially opening them up to economic coercion. China controls 50–90 per cent of the world's clean energy minerals supply chains and is dominant in their processing and refining. When it comes to rare earths, China accounts for 98 per cent of EU imports and 80 per cent of US imports (European Commission, 2020; Fannon, 2021a, 2021b; Gambosi, 2021; Tegler, 2021; Yu & Sevastopulo, 2021; Statista, 2022).

While both parties are slowly taking action to wean themselves off their respective dependencies, those efforts will take time and be incomplete. It is in the interest of both parties to work together, with other democratic market economies, and with key critical-materials suppliers, in strategic partnerships that can forge secure and sustainable supply chains and low-carbon development of these critical materials, which will literally provide the raw material for any EU effort at 'digital sovereignty'.

RULE-MAKERS – OR RULE-TAKERS?

For decades Europeans and American have been accustomed to setting global rules. Yet in a new era of diffuse power and disruptive challenges, they now face the prospect of becoming rule-takers – unless they manage their competition within a more effective frame of cooperation and coordination. Nowhere is this truer than with regard to the digital revolution.

NOTE

1. I am grateful to Ann Mettler for her insights on this issue.

REFERENCES

Aaronson, S.A. (2020). *America's Uneven Approach to AI and Its Consequences* (IIEP Working Paper 2020-7), George

Washington University, April, https://www2.gwu.edu/~iiep/assets/docs/papers/2020WP/AaronsonIIEP2020-7.pdf.
Amaro, S. (2021). *Achieving semiconductor independency is 'not doable', EU competition chief says*, CNBC, 29 November, https://www.cnbc.com/2021/11/29/eu-vestager-independent-semiconductor-production-isnt-doable.html.
Barker, T. (2021). 'TTC lift-off: The Euro-Atlantic tech alliance takes shape', *Internationale Politik Quarterly*, 30 September, https://ip-quarterly.com/en/ttc-lift-euro-atlantic-tech-alliance-takes-shape.
Beattie, A. (2021). 'The EU's unlikely ambition for sovereignty in semiconductors', *Financial Times*, 16 September.
Benaich, N., & Hogarth, I. (2021). 'State of AI Report', 12 October, https://docs.google.com/presentation/d/1bwJDRC777rAf00Drthi9yT2c9b0MabWO5ZlksfvFzx8/edit#slide=id.gf171287819_0_165.
Bown, C. (2021), 'Semiconductors and pandemic resilience', in *World Trade Outlook 2021,* WTO, Geneva, ISBN 978-92-870-5140-04 https://www.wto.org/english/res_e/booksp_e/wtr21_e/12_opinionpiece_by-chad-p-bown_e.pdf.
Breton, T. (2020). 'Europe: The keys to sovereignty', European Commission, September 10, https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en.
Broadbent, M. (2021). *Identifying Common Transatlantic Principles for AI Regulation*, Transatlantic Leadership Network, 29 November, https://www.transatlantic.org/wp-content/uploads/2021/12/11-30-2021-Broadbent_Identifying-Common-Transatlantic-Principles-for-AI-Regulation.pdf.
Bughin, J., Seong, J., Manyika, J., Hämäläinen, L., Windhagen, E., & Hazan, E. (2019). *Notes from the AI Frontier: Tackling Europe's Gap in Digital and AI*, McKinsey Global Institute, February, https://www.the-digital-insurer.com/wp-content/uploads/2019/06/1471-MGI-Tackling-Europes-gap-in-digital-and-AI-Feb-2019-vF.pdf.
Busvine, D. (2021). *Europe Should Invest in Chip Design, not a Mega-Fab: Think Tank*, Reuters, 8 April, https://www.reuters.com/article/us-semiconductors-europe-idUSKBN2BV1K2.
Castro, D., McLaughlin, M., & Chivot, E. (2019). *Who Is Winning the AI Race: China, the EU or the United States?*, Center for Data Innovation, 19 August, https://datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/.
Cerulus, L., & Barigazzi, J. (2021). 'France eyes control over chip agenda in EU-US tech alliance', *Politico*, 29 September, https://www.politico.eu/article/france-eu-chips-strategy-control/.
CleanTech Group (2021). 'New research concludes EU will miss climate goals unless Cleantech Innovation is scaled', March 2021, https://www.cleantech.com/release/new-research-concludes-eu-will-miss-climate-goals-unless-cleantech-innovation-is-scaled/.
Csernatoni, R. (2021). *The EU's Rise as a Defense Technological Power: From Strategic Autonomy to Technological Sovereignty,* Carnegie Europe, 12 August, https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134.
Duchâtel, M. (2021). *The Weak Links in China's Drive for Semiconductors*, Institut Montaigne, January, https://www.institutmontaigne.org/en/publications/weak-links-chinas-drive-semiconductors
European Commission (2020). *Critical Raw Materials Resilience: Charting a Path Towards Greater Security and Sustainability* [COM(2020) 474 final], 3 September, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0474&from=EN.
European Commission (2021a). '5G for Europe's digital and green recovery', 14 January, https://digital-strategy.ec.europa.eu/en/library/5g-europes-digital-and-green-recovery.
European Commission (2021b). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* [COM(2021) 206 final], 21 April, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206
European Commission (n.d.), 'Cloud computing', https://digital-strategy.ec.europa.eu/en/policies/cloud-computing.
European Union (2022). 'A Strategic Compass for Security and Defence,' March, https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
Fannon, F. (2021a). 'US needs to lead the way in building a new energy supply chain', *Financial Times*, 21 December.
Fannon, F. (2021b). 'New standards needed for the clean energy technology supply chain', *Financial Times*, 12 June.
Gambosi, J. (2021). *Rare Earth*, U.S. Geological Survey, January, https://pubs.usgs.gov/periodicals/mcs2021/mcs2021-rare-earths.pdf.
Gates, B. (2021). 'Funding clean technology is the way to avoid climate disaster', *Financial Times*, 31 October, https://techcrunch.com/2021/06/02/eu-and-bill-gates-make-joint-push-for-1bn-to-accelerate-clean-tech/.
Gehrke, T. (2021). *How 2400 Pages of Tech Industrial Policy Will Change Transatlantic Relations*, Egmont Institute, July, https://www.egmontinstitute.be/content/uploads/2021/07/spb-148-tobias.pdf?type=pdf.
Hamilton, D.S., & Quinlan, J.P. (2021). *The Transatlantic Economy 2021* (Washington, DC: Johns Hopkins SAIS/Wilson Center), https://transatlanticrelations.org/publications/transatlantic-economy-2021/.

Public investments should not and cannot take the place of the far larger resources the private sector can bring to bear

Hancké, B. (2021). 'Europe's call for semiconductor factories: A solution in search of a problem?' *London School of Economics*, 3 August, https://blogs.lse.ac.uk/europpblog/2021/08/03/europes-call-for-semiconductor-factories-a-solution-in-search-of-a-problem/.

Hardesty, L. (2021). *European cloud providers take hit from AWS, Google, Azure, says Synergy,* Fierce Telecom, 23 September, https://www.fiercetelecom.com/platforms/european-cloud-providers-take-hit-from-aws-google-azure-says-synergy.

Hetzner, C. (2021). 'Intel CEO says 'big, honkin' fab' planned for Europe will be world's most advanced', *Fortune*, 10 September, https://fortune.com/2021/09/10/intel-ceo-big-honking-fab-planned-eu-europe-most-advanced/.

International Energy Agency (2021). *Net Zero by 2050: A Roadmap for the Global Energy Sector*, May, https://www.iea.org/reports/net-zero-by-2050.

International Institute for Strategic Studies (2021). 'The EU's approach to artificial intelligence'. *Strategic Comments*, 27 (24), https://www.iiss.org/~/publication/74233822-70ef-42cb-96d8-3cbd3edf17f4/the-eus-approach-to-artificial-intelligence.pdf.

IT Law Wiki (2011). *European Union–United States Trade Principles for Information and Communication Technology Services*, 4 April, https://itlaw.fandom.com/wiki/European_Union-United_States_Trade_Principles_for_Information_and_Communication_Technology_Services

Jones, C. (2021). 'High demand is the oft-neglected aspect of supply-side shortages', *Financial Times*, 15 September.

Kleinhans, J.-P. (2021). 'The lack of semiconductor manufacturing in Europe', *Stiftung Neue Verantwortung*, 6 April, https://www.stiftung-nv.de/de/publikation/lack-semiconductor-manufacturing-europe.

Lander, E., & Nelson, A. (2021). 'Americans need a Bill of Rights for an AI-powered world', *Wired*, 10 October.

Libek E. (2019). *European Strategic Autonomy: A Cacophony of Political Visions*, International Centre for Defence and Security, 19 December, https://icds.ee/en/european-strategic-autonomy-a-cacophony-of-political-visions/.

Miller, J. (2021). 'EU cash alone won't secure chip supply for region, says Infineon chief', *Financial Times*, 10 March.

Nguyen, L., Koester, S., & Hart, D.M. (2021). *Comments to the International Trade Administration on U.S. Clean Technologies Export Competitiveness Strategy,* Information Technology and Innovation Foundation, 1 October, https://itif.org/publications/2021/10/01/comments-international-trade-administration-us-clean-technologies-export?mc_cid=2ce02cc8a2&mc_eid=3d83286407.

Noyan, O. (2021). 'Europe's cloud dreams come crashing down to earth', Center for European Policy Analysis, 29 November, https://cepa.org/europes-cloud-dreams-come-crashing-down-to-earth/.

Pannier, A. (2021). *The Changing Landscape of European Cloud Computing: Gaia-X, the French National Strategy, and EU Plans,* Ifri, 22 July, https://www.ifri.org/sites/default/files/atoms/files/pannier_european_cloud_computing_2021.pdf.

Poitier, N. (2021). *Europe Doesn't Need a 'Mega Fab'*, Bruegel, 22 September, https://www.bruegel.org/2021/09/europe-doesnt-need-a-mega-fab/.

Poitiers, N., & Weil, P. (2021). *A New Direction for the European Union's Half-Hearted Semiconductor Strategy,* Bruegel, 15 July, https://www.bruegel.org/2021/07/a-new-direction-for-the-european-unions-half-hearted-semiconductor-strategy/

Rasser, M., Arcesati, R., Oya, S., Riikonen, A., & Bochert, M. (2020). *Common Code: An Alliance Framework for Democratic Technology Policy*, Center for a New American Security, October, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Common-Code-An-Alliance-Framework-for-Democratic-Technology-Policy-1.pdf?mtime=20201020174236&focal=none.

Sanderson, H., & Sheppard, D. (2021). 'High metal prices could delay transition to clean energy, warns IEA', *Financial Times*, 5 May.

Sims Gallagher, K. (2022). 'The coming carbon tsunami: Developing countries need a new growth model—Before it's too late', *Foreign Affairs*, January/February, https://www.foreignaffairs.com/articles/world/2021-12-14/coming-carbon-tsunami.

Statista (2022). *Distribution Rare Earths Production Worldwide as of 2021, by Country*, https://www.statista.com/statistics/270277/mining-of-rare-earths-by-country.

Sullivan, J. [@JakeSullivan46]. (2021). *The United States welcomes the EU's new initiatives on artificial intelligence* [Tweet]. Twitter, 21 April. https://twitter.com/jakesullivan46/status/1384970668341669891?lang=en.

Szczepanski, M. (2021). *EU–US Trade and Technology Council: New Forum for Transatlantic Cooperation*, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698037/EPRS_BRI(2021)698037_EN.pdf.

Tegler, E. (2021). 'The U.S. is trying to secure rare earth elements for national security. That goes beyond simple investment', *Forbes*, 26 February, https://www.forbes.com/sites/erictegler/2021/02/26/the-us-is-trying-to-secure-rare-earth-elements-for-national-security-that-goes-beyond-simple-investment/?sh=4fa9178b5c53.

U.S. Chamber of Commerce (2021). *U.S.–EU Trade & Technology Council Policy Priorities*, September, https://

www.uschamber.com/assets/archived/images/us_chamber_ttc_policy_priorities_-_september_2021.pdf.
van Manen, H., Gehrke, T., Thompson, J., & Sweijs, T. (2021). *Taming Techno-Nationalism: A Policy Agenda*, Hague Centre for Strategic Studies, 23 September, https://hcss.nl/report/taming-techno-nationalism/.
Veale, M., & Zuiderveen Borgesius, F. (2021). 'Demystifying the Draft EU Artificial Intelligence Act'. *Computer Law Review International*, 22(4), 97–112, https://doi.org/10.9785/cri-2021-220402.
Wallace, N., McQuinn, A., Ezell, S., & Castro, D. (2018), *How Canada, the EU, and the U.S. Can Work Together to Promote ICT Development and Use*, Information Technology and Innovation Foundation, June, https://www2.itif.org/2018-canada-eu-us-ict-development.pdf?_ga=2.136210481.122227442.1638825802-193437476.1635703355.
Waters, R. (2021). 'Every company may soon be a cloud company', *Financial Times*, 2 December.
White House (2021a). *U.S.–EU Trade and Technology Council Inaugural Joint Statement*, 29 September, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/.
White House (2021b). *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth*, June, https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.
Yu, S., & Sevastopulo, D. (2021). 'China targets rare earth export curbs to hobble US defence industry', *Financial Times*, 16 February.

Digital Strategic Autonomy: An Australian Perspective

Henry Ergas and Joe Branigan

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Australia has, in the recent period, taken a hard look at challenges to its independence and sovereignty. What are its methodologies and how does it come up with its distinctive policy decisions? Since the 1990s, and especially over the last two decades, Australian policymakers have substantially altered the way the issues arising in respect of strategic industrial capabilities are considered, notably in relation to national defence. It centres on the identification of the capabilities whose unavailability, individually or collectively, would seriously increase Australia's vulnerability. This assessment is undertaken by examining the 'deprival value' of capabilities through careful scenario analysis.

THE AUTHORS

Henry Ergas is Professor of Infrastructure Economics, University of Wollongong. He has worked at at the OECD, Australian Trade Practices Commission as well as at a number of economic consulting firms and universities internationally. He chaired the Australian Intellectual Property and Competition Review Committee set up by the Australian Federal Government in 1999 to review Australia's intellectual property laws as they relate to competition policy.

Joe Branigan is Director, Tulipwood Economics, and Industry Fellow, University of Queensland. A public policy economist, he deals in public infrastructure network economics (roads, rail, ports, electricity, telecommunications), regional economic development, policy, programme and public financial management analysis and advice.

INTRODUCTION AND DEFINITIONS

Digital strategic autonomy relates to a sovereign nation's (or group of nations') ability to maintain the integrity of its digital network infrastructure, including transmission and storage facilities such as undersea cables, data centres, and cloud computing infrastructure. European Council President Charles Michel stated, in a speech in early 2021, that 'there is no strategic autonomy without digital sovereignty', implying that digital strategic autonomy is a vital component of national sovereignty (Michel, 2021). Digital Strategic Autonomy means, in effect, that a sovereign nation (or group of nations) can deter and/or prevent clandestine or blatant state or non-state subversion of digital infrastructure for commercial, military, or strategic gain.

More broadly, 'autonomy' literally means, from the classical Greek, self-rule, or more properly, rule by rules one has given oneself. In practice and as a matter of policy, Australia's approach has always been to seek autonomy within the context of a rules-based international order, while ensuring the nation has the ability to cope with contingencies which may undermine, disrupt, or even destroy that order. As an island continent, remote from many of its closest allies, the need to assure Australia's resilience in the face of threats and risks has always been a matter of great concern.

We begin by outlining the manner in which priorities in that respect have been analysed more generally before turning to the issues associated with digital capabilities in particular.

THE INDUSTRY POLICY CONTEXT: SETTING STRATEGIC PRIORITIES

Since the 1990s, and especially over the last two decades, Australian policymakers have substantially

Systematic monitoring must be put in place to keep a watch on capabilities and their availability

altered the manner in which the issues arising in respect of strategic industrial capabilities are considered, notably in relation to national defence.

Historically, emphasis was placed on ensuring that when the Australian Defence Force (ADF) acquired materiel from overseas, those purchases were at least partially offset by some form of domestic content. That remains the case, with 'Australian Industry Participation' plans forming part of the material typically demanded in tenders from the suppliers of defence materiel.

However, it also became clear that the purchases those requirements generated were not targeted to the development of the industrial capabilities needed to preserve Australia's strategic autonomy. Rather, those capabilities had to be carefully identified and the means put in place to ensure they were available.

In essence, sovereign industry capabilities have been defined as those which build and sustain weapons and other related defence systems holding pivotal positions in the ADF's Order of Battle, cannot be reliably accessed from overseas in the event of a significant deterioration in Australia's military strategic outlook, and are not readily available from Australian-based suppliers in the normal course of business. All three conditions must be satisfied for sovereignty concerns to arise.

It follows from that definition that the starting point must be to identify the capabilities whose unavailability, individually or collectively, would seriously increase Australia's vulnerability. This assessment is undertaken by examining the 'deprival value' of capabilities through careful scenario analysis, where the scenarios must:

- Accommodate different degrees, forms, and durations of deprival.
- Consider the scope to replace capabilities with substitutes and examine the cost and consequences of doing so.
- Assess how each of those varies as the range of capabilities whose availability is threatened varies.
- On that basis, derive a willingness to pay for assured supply.

Given the results of that assessment, the second step is then to analyse the ways in which some assurance of continuity of supply may be obtained. Obvious alternatives include:

- Holding inventories of goods.
- Issuing contracts which ensure that capacity now used for other purposes can and will be converted to meet priority needs as and when they arise.
- Ensuring that firms which possess the required capabilities, or which can be funded to develop, retain, and extend those capabilities, are and remain viable.
- Assessing which of those options provide value for money, and designing portfolios of interventions which will put the most preferred options into effect.

Finally, but crucially, systematic monitoring must be put in place to keep a watch on the capabilities and their availability, given that both will evolve virtually continuously. Indeed, a crucial lesson to be drawn from Australian experience is that a far higher level of technical complexity – and associated administrative effort – is required to design and apply a method for checking the economic and managerial 'health' of sovereign capabilities than in capability definition, given the diverse and the often rapidly changing environment in which Defence and its supply chain industries function.

A further lesson is that adequate funding must be available on a continuing basis to preserve sovereign capabilities should issues arise. There is a tendency to think in terms of one-off contracts and budgets; however, many problems occur when unexpected contingencies arise that necessitate rapid intervention.

In short, the Australian experience, much of which was originally focused on defence, has generated analytical approaches to determining the value to be placed on strategic capabilities, and to select and implement interventions aimed at assuring them. It is more recently that those issues have arisen in the digital environment more generally, including in terms of civilian infrastructure. We therefore now turn to consider some areas where they have been addressed.

THE DIGITAL REVOLUTION AND ITS IMPLICATIONS

Rapid technological innovation and sustained investment in digital communications networks over the past 15 years have undoubtedly raised living standards. Digital infrastructure has also provided crucial flexibility in the face of economic shocks. A stark example is how the improvements to digital infrastructure networks allowed for up to one-third of the labour force in advanced economies to work productively from home during COVID-19 'lockdown' periods in 2020 and 2021. These digital network investments have significantly increased bandwidth and lowered latency and 'jitteriness', greatly expanding the products and services available to businesses that operate online and their customers.[1]

Reflecting these benefits and others, Australia's digital economy is growing rapidly as a proportion of GDP. The Australian Bureau of Statistics estimates that the digital economy accounted for 5.9 per cent of Australia's GDP in 2019–2020 and other estimates are higher for advanced economies such as the United States (Australian Bureau of Statistics, 2021; see Ergas, 2021). The increased economic importance of digital networks means there is an increased cost to their interruption or violation, whether for commercial, military, or strategic gain, by a foreign power.

Accordingly, countries are increasingly concerned about their digital security or cyber autonomy. For example, in Australia's case, digital security was specifically cited as an issue of strategic importance in its 2017 Foreign Policy White Paper:

'Globally networked information systems also make it easier for states and non-state actors to compromise national security and to target individuals and businesses. Cyber threats can range from unacceptable interference in democratic processes, such as the activities of Russian cyber actors during the 2016 US presidential election, to the theft and manipulation of information or disruption of government or commercial activity. At the extreme, cyber actors could attack critical national infrastructures such as power grids and financial systems.' (Australian Government, 2017)

Russia's full-scale invasion of Ukraine on 24 February 2022 provides a palpable modern example of the absolute necessity to maintain digital strategic autonomy in the face of an existential military threat. Ukraine has relied on its mobile phone network to intercept and disrupt Russian military communications, operate drones, coordinate defensive positions, maintain a first responder capability, and organise evacuation efforts (Detsch, 2022). And the Russian military has attempted to disrupt and degrade Ukraine's digital assets to weaken Ukraine's defensive capabilities, as well as use its own digital

communications network to launch precision missile strikes (Nakashima, 2022; Valance, 2022).

In 2021, the Russian military introduced Era, a cryptophone system designed to work 'in all conditions'. However, the system relies on 3G/4G networks to communicate, which the Russians destroyed in their largely indiscriminate attacks on Ukraine's eastern population centres such as Kharkiv. The Russian military was then forced to use unencrypted lines of communication, which allowed Ukraine's defence intelligence agency to, for example, assess Russian morale and claim that Russian general Vitaly Gerasimov, chief of staff of the 41st Army, was allegedly killed.

MAINTAINING DIGITAL STRATEGIC AUTONOMY

As the 2017 Australian Foreign Policy White Paper highlights, there are a number of channels via which a sovereign state is vulnerable to digital strategic attack. These threats can include:

- Cyberattacks to infiltrate government systems.
- Disabling digital communications infrastructure.
- Tapping into digital communications infrastructure
- Spreading misinformation.
  (Australian Government, 2017)

Achieving digital strategic autonomy requires managing these risks, which in turn requires capabilities, capacities, and controls to safeguard and strengthen digital sovereignty (European Union Agency for Cybersecurity, 2021). Strategic partnerships, such as the Five Eyes partnership between the United States, United Kingdom, Japan, Australia, and New Zealand, and Australia's ongoing close cooperation with its partners in Europe and in the Indo-Pacific, are vital if cyber threats are to be identified and controlled both before and as they occur. A recent paper from the European Union identifies the key components of threat management, as follows:

- Maintaining data security.
- Trustworthy software platforms
- Cyber threat management and response
- Trustworthy hardware platforms
- Cryptography
- User-centric security practices and tools
- Digital communication security
  (European Union Agency for Cybersecurity, 2021)

CHINA

China has greatly expanded its presence in the Indo-Pacific diplomatically, commercially, and militarily in recent years, including through its One Belt, One Road initiative (see Cai, 2017).[2]

While China's reach is extremely broad, the Pacific – and notably the Pacific Island states – have been a point of particular focus, with China's role growing strongly since 2006. Excluding Papua New Guinea (PNG), the region's two-way trade with China overtook that with Australia in 2013 and has continued to rise since then. For the Solomon Islands, two-way trade with China now accounts for almost half of its total trade. As a recent study by the Brookings Institution notes, as well as increasing trade flows:

'China has also dramatically scaled up its aid activities. According to Lowy Institute research, between 2006 and 2017 China provided close to US$ 1.5 billion in foreign aid to the Pacific Islands region through a mixture of grants and loans. As of 2017, China was the third-largest donor to the Pacific, contributing 8 per cent of all foreign aid to the region between 2011 and 2017. While China is by no means the dominant donor in the Pacific, the way in which it delivers its aid – large infrastructure projects funded by concessional loans – makes these

Strategic partnerships are vital if cyber threats are to be identified and controlled both before and as they occur

projects stand out. Chinese lending has also been used as a vehicle to get Chinese state-owned enterprises into the region. These companies are now competing in commercial activity across the board. According to China's own investment statistics, Chinese construction activity in the region was US$ 958 million in 2017, almost six times greater than its foreign aid activities.' (Pryke, 2020)

On 24 March, a draft 'Solomon Islands and China Initial Framework Agreement on Security Cooperation' that focussed on internal security provisions for the Solomon's (e.g. police training and equipment) was leaked on social media. The agreement, which has been already 'initialled' and needs to be 'cleaned up' for final signatures, provides for a capacity 'to respond to Solomon Islands soft and hard domestic threats' (O'Brien, 2022; Solomon Islands Government, 2022). There is a concern in Australia and the United States that this initial agreement could, ultimately, lead to the establishment of a Chines naval base in the Solomon's, less than 2,000 km from Australia's coastline (Greene, 2022; Macmillan, 2022).

One important component of China's Belt and Road strategy is the Digital Silk Road Initiative (DSRI). Launched in 2015, the DSRI aims to make the world more dependent on Chinese technology and standards. For example, the DSRI aims to strengthen the interoperability of critical digital infrastructure such as terrestrial and submarine data cables, 5G cellular networks, data storage centres, and global satellite navigation systems. According to one estimate, by 2018, DSRI-related investments in digital infrastructure projects outside of China had reached US$ 79 billion (Ghiasy & Krishnamurthy, 2021).

Obviously, increased trade and investment ought to be welcomed. There are, however, concerns which arise when it weakens the effective independence of states and poses threats to the rules-based international order. It is true that in many instances the dramatic expansion in China's presence has involved what are notionally private entities; but the reality is that China's system of government effectively subordinates both state-owned/run and private companies to the service of the state and more broadly to close supervision by the Chinese Communist Party. The risks this creates are especially acute in terms of digital infrastructure.

Thus, the Cyber Administration of China has repeatedly emphasised the need to develop controls so that 'the party's ideas always become the strongest voice in cyberspace'. This includes enhancing the 'global influence of internet companies like Alibaba, Tencent, Baidu [and] Huawei' and striving 'to push China's proposition of internet governance toward becoming an international consensus' (Cave, Hoffman, Joske, Ryan, & Thomas, 2019).

The issues this creates have received greater attention as a result of the COVID-19 pandemic, which both increased the importance of the digital infrastructure and highlighted the seriousness of the supply chain vulnerabilities affecting national economies. As the Australian Strategic Policy Institute argues in a 2021 paper:

'Supply-chain vulnerability has ignited work in Europe, North America and other regions to reduce dependence on China. Telecommunications companies such as Huawei and ZTE that are deemed 'high risk' by multiple countries are increasingly finding themselves locked out of developed markets. Amid the trade war between the US and China, which began in 2018, the Trump administration unleashed a relentless series of actions targeting Chinese companies in an effort to slow their advance. That onslaught has further convinced China's leadership to redouble its efforts to dominate the commanding

heights of technology as a source of strategic and economic power.' (Ryan, Fritz, & Impiombato, 2021)

RECENT AUSTRALIAN ACTIONS

Reflecting growing concerns about protecting digital sovereignty, the Australian government has undertaken a broad range of initiatives in recent years. These initiatives, which involve both domestic and regional interventions, aim at strengthening the security and integrity of Australia's digital infra-0structure and that of the countries in Australia's immediate region.

Australia's security agencies had been aware of the threat to Australia's national security from Chinese state-owned businesses for some time, with the Australian Security and Intelligence Organisation (ASIO) carefully monitoring activities it believes are of concern, and privately warning Australian companies about potential risks. As a result of warnings about Huawei, in 2010 the board of the National Broadband Network (NBN) quietly decided that it would not accept any of Huawei's bids to take part in the creation of the national broadband network. This followed a briefing from the then ASIO Director-General David Irvine and the government's National Security Adviser, Duncan Lewis. NBN's decision was publicly confirmed by the Gillard Labor government in 2012. In 2018, the Turnbull Coalition Government, after much internal deliberation, banned Huawei and ZTE from participating in constructing Australia's 5G network (Hartcher, 2021).[3]

The Australian government had considered limiting the deployment of Huawei's products to less sensitive parts of the 5G network, which was Australia's approach in accepting Huawei into its 4G system. However, as the Australian Signals Directorate's then Director-General Mike Burgess said in a 2018 speech: 'The distinction between core and edge collapses in 5G networks. That means that a potential threat anywhere in the network will be a threat to the whole network.' It has been reported that the former Prime Minister Malcolm Turnbull liked to summarise this in internal debates with the rhyme that 'the core is no more'. Burgess's final advice to Turnbull and his National Security Committee was that the risk of Huawei's involvement in Australia's 5G network could not be mitigated (Hartcher, 2021).

As Simon Lacey, the former vice-president of trade facilitation and market access at Huawei, writes: 'In China, it [Huawei] had to demonstrate unwavering loyalty to the goals of the Communist Party leadership. Outside China, it had to argue that it had little or nothing to do with the Chinese state' (quoted in van der Kley, 2020).

Investing in Digicel

As well as domestic action, Australia has adopted an approach of seeking to prevent Chinese entities from acquiring commercial positions in the South Pacific's digital infrastructure which might pose substantial risks to the security both of the South Pacific and of Australia.

In a very recent, and highly significant, example of this policy – which commentators have described as one of 'strategic denial' – in late 2021 the Australian government invested AU$ 1.78 billion (€1.13 billion) as part of Telstra's AU$ 2.14 billion (€1.36 billion) purchase of Digicel Pacific. Digicel Pacific, founded in 2001 by Irish entrepreneur Denis O'Brien, is the leading telecommunications operator in the South Pacific, providing mobile and network services in PNG, Nauru, Samoa, Vanuatu, Tonga, and Fiji, with around 2.5 million subscribers. It is overwhelmingly dominant in virtually all those markets and hence is the primary entity controlling and shaping

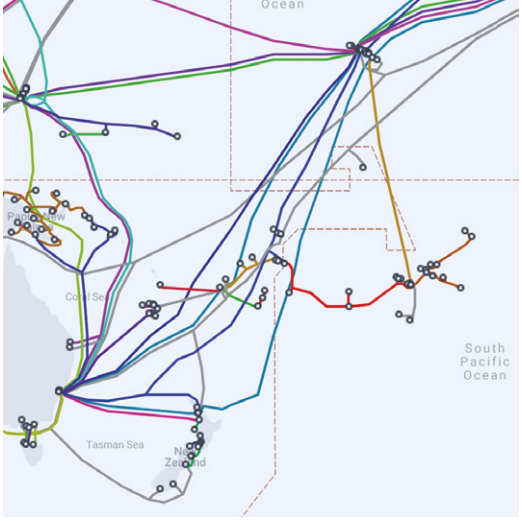


FIGURE 1: **Undersea telecommunications cables in the western Pacific Ocean**

Source: https://www.submarinecablemap.com/

their digital infrastructure. When it came on to the market, it was widely reported that Chinese entities with strong connections to the Chinese government were making offers to purchase it at valuations which were difficult to justify on a strictly commercial basis. So as to reduce the threats that posed, the Australian government decided to assist in Telstra's acquisition of the company, which – as well as yielding strategic benefits – provides an assurance that the South Pacific's digital infrastructure will continue to develop in the interests of the populations it serves ('Telstra decision', 2021).

Coral Sea Cable System

Because Australia is an island continent, achieving digital strategic autonomy requires ensuring the integrity of the undersea telecommunications cables that transport more than 95 per cent of digital traffic to and from the country. A large proportion of those cables lie in the Pacific Ocean, connecting Australia to New Zealand and the islands of the Pacific, and to the continental United States and Japan via Hawaii and Guam.

Undersea fibre-optic cables are the backbone of data transmission and intercontinental communications, carrying the vast bulk of Internet traffic at very high speeds and with high levels of signal clarity and stability. Additionally, undersea cables can be utilised to host undersea sensor networks to monitor submarine movements (Huang, 2017).

In 2019, the Australian government invested in the deployment of the Coral Sea Cable System, a very high-speed undersea cable system which will support the emerging digital economies of PNG and the Solomon Islands. The Australian government outbid Huawei Marine for the contract (Hillman, 2021). By 2018, PNG's existing undersea cable to Sydney was nearing the end of its useful life. The Solomon Islands had no undersea telecommunications cable link, leaving it dependent on expensive and unreliable satellite communications (Department of Foreign Affairs and Trade, 2018).

In the case of Palau, the Australian government worked closely with the United States and Japanese governments to ensure that an undersea cable could be funded and built without China's participation (Hillman, 2021).

CONCLUSIONS

The Australian government has consistently stressed the need for digital strategic autonomy and has invested heavily in recent years to achieve this goal. Efforts include:

- The 2016 Defence White Paper, which included a $400 million investment to enhance ADF cybersecurity capabilities.
- The 2017 Foreign Policy White Paper, which establishes the 'Step Up' in Australia's engagement with Pacific Island nations.
- Australia's intelligence agencies, including the Australian Signals Directorate (which is responsible for developing offensive cyber capabilities to disrupt, degrade, deny, and deter offshore cyberattacks), have been funded to vastly increase the scope and sophistication of their presence in the digital space.
- Investment in digital infrastructure in the South Pacific, including undersea cables and wireless networks.
- Bilateral and multilateral agreements to prevent state-sponsored cyber espionage, whether for commercial, military, or strategic purposes.

Australia's national security depends, in part, on regional security in the South Pacific. In Australia's

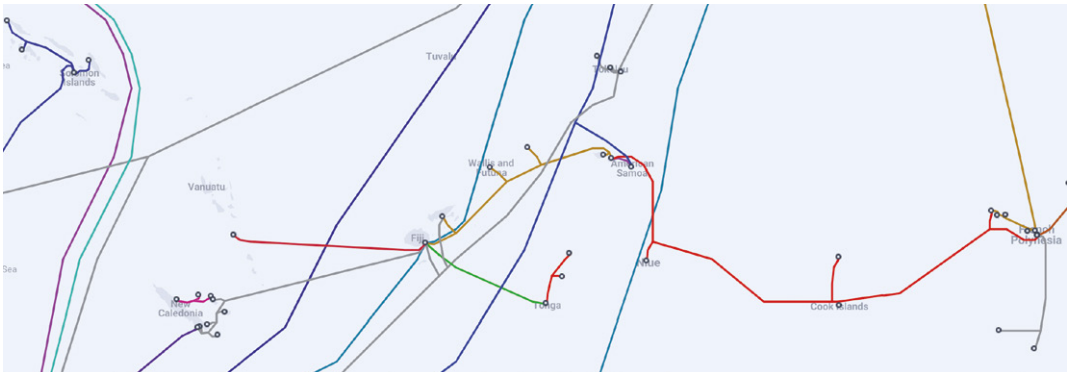


FIGURE 2: **Undersea cables between the Solomon Islands and French Polynesia**

Source: https://www.submarinecablemap.com/

2017 Foreign Policy White Paper, Foreign Minister Marise Payne pointed to the importance of a 'resilient Pacific' as one of five fundamental foreign policy objectives for Australia. Australia's 'Pacific Pivot' is an attempt at regional economic and security integration. In the digital age, digital strategic autonomy for Australia requires digital strategic autonomy for its Pacific neighbours, which is crucial both for their own development and sovereignty and for the peace and security of the region. In short, as this area increases in importance, so will Australia's efforts to preserve the rules-based international order which is the best guarantor of strategic autonomy over the longer term.

NOTES

1. 'Jitteriness' refers to the variation in latency over time.
2. Also known as the 'Belt and Road Strategy'.
3. ZTE is a Chinese telecommunications technology company listed on the Hong Kong and Shenzen stock exchanges. See ZTE's website: https://www.zte.com.cn/global/

REFERENCES

'Telstra decision to acquire Digicel Pacific'. Joint Media release by Ministers Payne (Foreign Affairs), Tehan (Trade, Tourism and Investment), and Seselja (International Development and the Pacific), 25 October 2021. *https://ministers.dfat.gov.au/minister/zed-seselja/media-release/telstra-decision-acquire-digicel-pacific#:~:text=Telstra%20decision%20to%20acquire%20Digicel%20Pacific%20Joint%20media,for%20Trade%2C%20Tourism%20and%20Investment%2025%20October%202021* .

Australian Bureau of Statistics (2021). *Digital Activity in the Australian Economy, 2019–20*, 29 October, https://www.abs.gov.au/articles/digital-activity-australian-economy-2019-20.

Australian Government (2017). *Foreign Policy White Paper*, https://www.dfat.gov.au/sites/default/files/2017-foreign-policy-white-paper.pdf.

Cai, P. (2017). *Understanding China's Belt and Road Initiative*, Lowy Institute, 22 March, https://www.lowyinstitute.org/publications/understanding-belt-and-road-initiative.

Cave, D., Hoffman, S., Joske, A., Ryan, F., & Thomas, E. (2019). *Mapping China's Technology Giants*, Australian Strategic Policy Institute, 18 April, https://www.aspi.org.au/report/mapping-chinas-tech-giants.

Department of Foreign Affairs and Trade (2018). *The Coral Sea Cable System: Supporting the Future Digital Economies of Papua New Guinea and Solomon Islands*, September, https://www.dfat.gov.au/about-us/publications/Pages/supporting-the-future-digital-economies-of-papua-new-guinea-and-solomon-islands.

Detsch, J. (2022). 'The Ukrainians are listening': Russia's military radios are getting owned', *Foreign Policy*, 22 March, https://foreignpolicy.com/2022/03/22/ukraine-russia-military-radio/.

Ergas, H. (2021). *Google's Contribution to Australia's Post-COVID Recovery*. Green Square Associates, October, https://services.google.com/fh/files/emails/google_dfi_report.pdf.

European Union Agency for Cybersecurity (2021). *Cybersecurity Research Directions for the EU's Digital Strategic Autonomy*, April, https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy/@@download/fullReport.

Ghiasy, R., & Krishnamurthy, R. (2021). 'China's digital Silk Road and the global digital order', *The Diplomat*, 13 April, https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.

Greene, A. (2022). 'Australian general says Chinese military presence in Solomon Islands would force ADF rethink', 31 March, *ABC News*, https://www.abc.net.au/news/2022-03-31/defence-general-warnings-chinese-military-solomon-islands/100954752.

Hartcher, P. (2021). 'Huawei? No way! Why Australia banned the world's biggest telecoms firm', *The Sydney Morning Herald*, 21 May, https://www.smh.com.au/national/huawei-no-way-why-australia-banned-the-world-s-biggest-telecoms-firm-20210503-p57oc9.html.

Hillman, J. (2021). 'What Australia is doing to counter China's digital ambitions?', *Financial Review*, 29 October, https://www.afr.com/policy/foreign-affairs/what-australia-is-doing-to-counter-china-s-digital-ambitions-20211027-p593ix.

Huang, E. (2017). *China's Cable Strategy: Exploring Global Undersea Dominance*, The Strategist, 4 December, https://www.aspistrategist.org.au/chinas-cable-strategy-exploring-global-undersea-dominance/.

Jiw, Y., & Wallace, J. (2021). *What is China's Belt and Road Initiative*, Chatham House, 13 September, https://www.chathamhouse.org/2021/09/what-chinas-belt-and-road-initiative-bri.

Macmillan, J. (2022). 'US admiral lashes 'concerning' Solomon Islands security pact with China', *ABC News*, 5 April, https://www.abc.net.au/news/2022-04-05/us-admiral-lashes-solomon-islands-security-pact-china/100967110.

Michel, C. (2021). *Digital Sovereignty Is Central to European Strategic Autonomy – Speech by President Charles Michel at 'Masters of Digital 2021' Online Event*. European Council, 3 February, https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/.

Moss, S. (2022). 'Ukraine: Russian military's own encrypted phones impacted after destroying 3G/4G towers, allowing comms to be intercepted', *DCD*, https://www.datacenterdynamics.com/en/news/ukraine-russian-militarys-own-encrypted-phones-impacted-after-destroying-3g4g-towers-allowing-comms-to-be-intercepted/.

Nakashima, E. (2022). 'Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say', *The Washington Post*, 24 March, https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/.

O'Brien, P. (2022). 'The China-Solomon Islands security deal changes everything', *The Diplomat*, 5 April, https://thediplomat.com/2022/04/the-china-solomon-islands-security-deal-changes-everything/.

Pryke, J. (2020). *The risks of China's Ambitions in the South Pacific*, Brookings, 20 July, https://www.brookings.edu/articles/the-risks-of-chinas-ambitions-in-the-south-pacific/.

Ryan, F., Fritz, A., & Impiombato, D. (2021). *Mapping China's Tech Giants: Reining in China's Technology Giants*, Australian Strategic Policy Institute, 8 June, https://www.aspi.org.au/report/mapping-chinas-technology-giants-reining-chinas-technology-giants.

Solomon Islands Government (2022). 'Solomon Islands and China initial framework agreement on security cooperation', 22 March, https://solomons.gov.sb/solomon-islands-and-china-initial-framework-agreement-on-security-cooperation/.

Vallance, C. (2022). 'Ukraine war: Major internet provider suffers cyber-attack', *BBC News*, https://www.bbc.com/news/60854881.

van der Kley, D. (2020). 'Huawei ban is just the start of the great decoupling', *Financial Review*, 28 July, https://www.afr.com/policy/economy/huawei-ban-is-just-the-start-of-the-great-decoupling-20200728-p55g2u.

The UK and the EU: A Bet on the Future for Europe's Strategic Autonomy

Simon Forge

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

The focus on the United Kingdom in this chapter is one of several case studies, commissioned by the European Liberal Forum, to assess the EU's critical dependence and levels of digital autonomy. This study aims at understanding how Europe's partner governments envisage their own digital policies, their vision of EU initiatives and orientations, and which items rank highest on their discussion agendas with the European Union (EU). The chapter introduces the current situation in the UK and its position on the EU; defines the problem as digital assets for EU strategic autonomy and the UK's relevance; assesses the current EU situation with relation to the UK; describes the state of affairs in current initiatives between the EU and the UK; discusses future challenges and options for UK support of EU digital strategic autonomy; and provides key policy recommendations. A final postscript section examines the impacts of the invasion of the Ukraine on the UK and its fallout for UK–EU strategic relations.

THE AUTHOR

Simon Forge is Director of SCF Associates Ltd, specialising in forecasting the impacts of telecommunications and computing developments, sometimes via micro/meso/macro models, for economic, social, business model, and technical projections, often for governments and international organisations. He holds degrees in digital signal processing and control engineering and is a Chartered Engineer (MIET).

THE UK POSITION WITH RESPECT TO THE EU AND ITS IMPACT ON CONTRIBUTING TO EUROPE'S DIGITAL STRATEGIC AUTONOMY

The role of the UK in an EU digital autonomy context is dominated by the Brexit situation, in four main areas. The first is its wide-ranging impact on central government policymaking. Secondly, it serves as the background to everyday national politics, often in unspoken ways as far as its economic impacts go. Thirdly, it has worsened relations with the EU due to the UK government's tactics on exit treaties, which may also negate specific areas of EU digital standards with its own digital regulation. Finally, the Brexit agenda has very differing impacts within the three smaller nations decreed by the UK's devolution statutes, most specifically on their long-term digital policies.

Note that the current UK central government is even more bluntly anti-EU than may be apparent in its direct interchanges with the European Commission during its recent negotiations. In November 2021 a UK government trade minister gave a speech in Atlanta, in the US state of Georgia, stating that Brexit had struck a blow for freedom and democracy – that is, she implied that the EU was neither free nor democratic. The administration likes to use themes that will support its move to the right. That indicates a considerable level of government antipathy, currently, towards any cooperation with the EU. However, as is often the case, the politics of the party in power may not be that of the majority of the populace, as is the case in states such as Belarus, Poland, and Hungary. To some extent, this may be indicative in the voting in the 2016 referendum. The UK vote was won by 37 per cent of the electorate voting to leave (17.4 million votes vs 16.1 million remain votes), some 4 per cent more than the remain votes (BBC News,

EU strategic autonomy is increasingly necessary as local hostility in the European theatre outside the EU advances

2016). That would imply that some 62.5 per cent of the electorate did not vote to leave. In addition, the under 30s (some 2.5 million potential voters, or around 5 per cent of the total) were largely unregistered. A fair majority might have voted to remain, which could have changed the result. This summary is included to emphasise potential possible chances for UK cooperation with the EU – but only when such actions are not directly prohibited by central government.

Moving forward to the situation today, it is unlikely that significant UK stimulation measures taken under the flag of Brexit can effectively reverse a decade of austerity within the time frame of the UK electoral cycle. Therefore, the degree of antipathy to the EU in the country is likely to decline. Against the background of a gradual recognition of the pandemic's long-term seriousness, the government is failing to deliver on its promise of an immediate international trading empire, while overall trade with the EU may shrink by 15 per cent in the long term and UK productivity may reduce, perhaps at 4 per cent per year, indicating a comparable shrinkage of the economy in the medium term. In comparison, the Bank of England expects COVID-19 to reduce GDP by only by 1 per cent (Office of Budget Responsibility, 2021).

The credibility of the UK government as a treaty partner is being eroded as it chooses which areas to deviate from in its agreed EU trading settlements of 2019/2020. But does this matter for the EU's strategic autonomy in digital areas (Wolf, 2021)?

The answer is probably not, for the reasons laid out here that will come into play as the current regime mutates under stronger economic and political pressures. Combined with the possible remedies suggested herein, these recommendations could become more viable in the longer term.

Digital strategy inside the UK and its implications for EU digital strategic autonomy (EU DSA)

Current UK government digital strategy for the public sector – and to some extent the private sector – exists at several levels. The basic aim of this digital strategy is to 'drive the UK digital economy'. Firstly, most activities of the UK government itself rely, to differing degrees, on digitalised processes. The majority of these are for mass interfacing with the populace, targeting many millions of citizens. Unfortunately that assumes a (very) high diffusion rate of median-level to high-level digital literacy among the UK population. COVID-19 testing and its government–citizen interfacing have not helped.

Secondly, the UK government is responsible for regulation of the national 'digital environment'. That ranges from spectrum use up to complex cybersecurity problems such as private data breaches while ruling on political manipulation by social network platforms (for example the 2016 Cambridge Analytica affair). It may now extend into acquisitions of 'national digital assets'. In theory, both levels can be synchronised under a single transparent policy – to establish trust in digital processes. In practice, the outcome is likely to be rather different as the necessary managerial and technical capabilities are not in place.

Revealingly, the UK government has delayed publishing its scheduled overarching digital strategy, in stark contrast with the devolved nations, all of whom have published detailed plans for pursuing digital economies. In 2017, a government policy paper detailed future digital strategy with revisions promised, specifically for 2021, presumably to update and fill gaps in its proposals (Department for Digital, Culture, Media and Sport, 2017). The 2021 date has been missed. However, borrowed from the

Biden White House is the idea of 'Build Back Better', which has seeded a series of UK central government documents (HM Treasury, 2021). In addition, the National Infrastructure Strategy report sets out the government's digital ambitions (HM Treasury, 2020).

Note, however, that central UK government strategy is not the only digital strategy in force. Policy across the UK is an amalgam of a central national agenda with additional policy setting locally and with implementation of the devolved policies at the level of the four nations. Of the UK population of around 67.1 million, some 56.5 million reside in England, with 5.5 million in Scotland, 3.2 million in Wales, and 1.9 million in Northern Ireland (Coronavirus (COVID-19) Infection Survey, 2021). Although the latter three devolved nations are far smaller than England (82 per cent of the UK population), they are disproportionately dynamic in creating detailed digital policies to progress their economies. They also look far more to the EU for their future, as several might be considering their options for remaining in union with England in the longer term. Generally they are far more likely to use EU digital standards for technical and social norms, be it for data privacy or electrical safety.

What is needed is an update to the overarching strategy to direct the UK public sector's digital aspirations, one of which is realistic, safe, and sensible – as far as its intended users' level of digital literacy goes. In practice, reliance on digital processes for governing EU and international trade may present significant problems. This is becoming evident with the new EU import/export controls (especially for smaller businesses) coming into force for the first time in January 2022 as the weight and complexity of regulation combines with low digital literacy – plus poor application user interfaces and gaps in infrastructure (for example, broadband is largely still over copper) (Forster, Dunai, & Shotter, 2021).

Digital literacy is a key problem with an ageing population. This is linked to UK education levels over the last three decades. State education standards and spending declined for the majority of those living in England by an average of 9 per cent in real terms between 2009 and 2019, but by 14 per cent for the most deprived 20 per cent of state schools (Institute for Fiscal Studies, 2021). Moreover, spending on adult education fell by 49 per cent over the same period (O'Connor, 2021). Thus, policy on state education for the majority is one of a declining investment over decades, reducing digital literacy for all ages, as government favours private schools for some 7 per cent of the UK school population.

In addition, concepts of an overarching industrial strategy for government-endorsed digitalisation of British industry seem to be absent. Perhaps this is because these are seen as more appropriate at a specialised level of the related ministries – business and industry, media and culture – that overlap with health, social security, taxation, pensions, justice, and policing. It may also be due to the current administration's political philosophy, which is sometimes opposed to central planning for industry – seeing itself as the party of 'free marketeers', from which standpoint industrial policy is not the responsibility of government. However, there are many exceptions in specific areas, for instance, increasingly in defence, with closer supervision over the last few years (see Cabinet Office, 2021). Furthermore, the ruling party recently made a political promise to restore prosperity to the North of England, effectively through an industrial investment policy (although it has recently broken its promises on northern rail transport infrastructure). This contrasting focus to its traditional principles

is driven by political pressures to maintain a parliamentary majority. It now abandons the traditional attitude of the ruling party, largely based on voters in south-east England working in the services sector.

Whether they are prompted by central government or by the devolved nations, these digital sector policies are generally aimed at nine specific subject areas:

- Digital infrastructure – largely physical networks, and some IT assets.
- Digital financial services – moves to electronic banking and so forth for the masses.
- Digital identification – for personal transactions and citizens' services.
- Supporting digital innovation and entrepreneurs.
- Digital literacy and widening digital education, a focus in the devolved nations.
- Digital platforms – software and hardware with services and skills.
- Telecoms assets and skills.
- Digital systems working for government.
- Health system applications.
- Taxation and social security applications.
- Digital management of the organs of government, for example the Governmental Digital Service, GDS.
- Industrial strategy for supporting the digital initiative and for exports.

ASSESSING THE PROBLEM

This section explores the relevance of digital autonomy to the formation of EU strategic autonomy. It examines the possibility of a UK contribution to the formation and progress of EU digital strategic autonomy.

EU strategic autonomy is increasingly necessary as local hostility in the European theatre outside the EU advances (but also, in three cases, within it, as populist movements using social media disinformation gather strength). Brexit might be cited as a case in point, with its promises of greater health services (NHS) funding used to win the 2016 Leave referendum.

The components that make up EU digital strategic autonomy are:

- Hosting production of key digital systems and components with the supply chains.
- Closer management of technology platforms that play a social-damage and political role.
- Integrating a common EU military force with all competences, that works within NATO, based on indigenous creation and production of digital technologies.
- Controlling the energy sources that ultimately power the EU's digital economies.
- Forming a common capital-markets base with appropriate regulation of its operations as a source of funding for its digital industries, especially the start-ups.

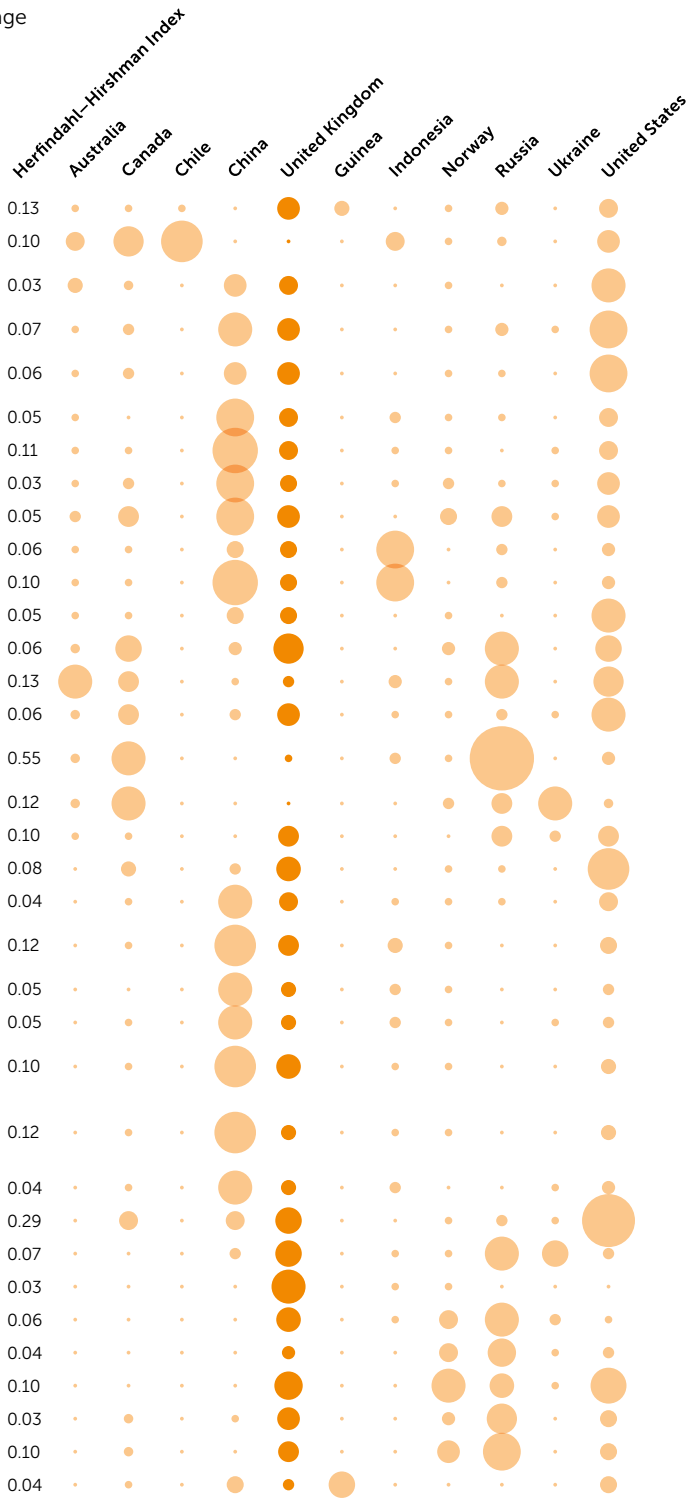
In terms of strategic imports to the EU from the UK, Eurostat data gives the following figure. As expected, China and the United States dominate, with Russia high in the EU's strategic energy supply as shown in Figure 1.

The UK contribution to strategic EU imports is far smaller, at under 5 per cent of total EU imports, but it is comprehensive, as might be expected for a former Member State, contributing in some key areas of digital products and services – computers and peripherals, telecommunications equipment, monitors, projectors, radio equipment, recording devices, aircraft, aircraft engines, satellites, launch vehicles, spacecraft, radioactive materials, medical/

FIGURE 1: **Imports from the UK compared with other countries in the EU supply chain**

The size of the circle indicates the percentage of contribution to the EU economy

20% 60%



Source: Data Eurostat, 2020, Institute for security studies, Daniel Fiott, Vassilis Theodosopoulos, Sovereignty over supply, the EU's ability to manage critical dependences while engaging with the world, December 2020.

pharmaceutical products, explosives, medical equipment, and so forth.

ASSESSMENT OF THE EU SITUATION FOR DIGITAL STRATEGIC AUTONOMY

This section analyses the potential for the digital autonomy strategy in the context of the EU economy and regulatory framework – and how the UK could contribute, with its views on interfacing in support of EU strategic autonomy.

EU digital strategic autonomy is not yet a viable reality, with seven possible main reasons for this:

1. Manufacturing: the EU has high dependence on external production assets and supply chains – up to 90 per cent of digital systems (software/systems/components).

2. That is accompanied by a lack of EU-centred supply chains and EU management of international supply chains.

3. Research and development (R&D) efforts and results in digital technologies are too small. While the EU orchestrates magnificent long-range R&D programmes, the follow-through into industrial products and enterprises is not organised or pursued.

4. Control of the 'tech platforms' and their abuses is still virtually absent. This could be countered via strong anti-trust measures whose powers may provide the sole remedies available globally – via the Digital Markets Act (DMA), the Digital Services Act (DSA), and Cybersecurity Act while also expanding the General Data Protection Regulation (GDPR) with comprehensive policing agencies, identification of infractions, and instant penalties. All will require faster-acting monitoring and abuse detection, court processes, and judgements (that is, in weeks not years) to keep up with the digital market leaders and their forays into new sectors. Effective measures would open new EU markets as well as create fresh players for those markets, for a more competitive EU digital environment.

5. Software production and its intellectual property rights (IPR) management represents a major gap, much of which might be filled by EU open-source software, especially in office systems and operating systems but also in mainstream software packages. Software law should similarly control consumer licencing and ownership issues for end-users to protect their rights, not those of monopoly publishers.

6. Large EU-sited and -owned storage and processing data centres for both retail and wholesale offerings (that is, 'cloud') as services are lacking within the EU. To change this would require that legislative and financial control be in the EU for both data and the software for storage and processing. Technology could be based on evolved EU grid technology and EU-defined service level agreements (SLAs) for cloud operations and failure reparation.

7. The EU produces a large amount of digital media content, but a common EU media streaming site for digital distribution is lacking (although some national media sites do exist, for example, BBC iPlayer in the UK, which has perhaps 25 per cent of the volume of content of the US leaders). Such media services could pool content from across the EU Member States with one or more competing hosting sites and content distribution networks (CDNs).

8. Perhaps an eighth reason, in pragmatic terms, is that implementation of the security and defence parts of the digital strategy will require formation of a comprehensive military capability across the 27 Member States. It will also require projection of capabilities into neighbouring areas and overseas.

The foundations of a UK contribution to EU digital strategic autonomy lie in what the UK political position will permit in view of Brexit

All of this will depend on an EU-hosted defence industry with full design and manufacturing capability.

The UK has capabilities to contribute to points 1, 2, 3, 5, 7, and especially 8 above.

Note that the EU has capabilities and experience in two essential components:

1. A strong regulatory framework for digital assets to support the EU's digital autonomy, with structures for standards and normative approvals (The European Telecommunications Standards Institute, ETSI, for telecommunications; the European Committee for Standardisation, for European Union standards, with the European Committee for Electrotechnical Standardisation, collectively termed CEN/CENELEC for all digital technologies). Existing normative organisations may be the basis to fill the gap. Those facilities could be augmented by EU resources to enact the DMA and DSA, with cybersecurity regulation and possibly a strengthened GDPR to reign in the web 'tech platforms' and to ensure the necessary legal processes are carefully prepared.

2. A first model for a framework to implement its digital autonomy strategy is in the way the Union has formed the legal EU structure and operating implementation for functioning across borders, for the 27 Member States, via the European Commission. But that cooperation would need to be vastly accelerated for defence operations within NATO.

What is the UK vision of the EU ambitions for strategic autonomy and in particular digital strategic autonomy?

Perhaps it is more useful to start by asking what the UK perspective is on EU initiatives and orientations. The dominant views regarding European policies are clearly not to contribute to EU prosperity wherever there is competition for trade. That is a prime consideration. Moreover, the general policy direction is to favour markets outside the EU, aiming to sign long-term trade agreements with the United States, Japan, Southeast Asia, Canada, Australia, plus Africa and Latin America, and so build a global trading empire to replace the EU as trading partner. The realism of that endeavour in terms of attainable levels of volume of trade and the time frames of negotiations is the key question for the UK economy. Today, it implies that the sale of products and services to the EU is preferred by UK government policy in the form of a transactional relationship, rather than transfer of pure digital technology and/or cooperation on technology with R&D projects, which might provide long-term competitive advantage to the EU. In consequence, the goals that loom high on the current UK central government's discussion agenda with the EU are to maintain its distance on any strategic support. Such a policy indicates that cooperation and support for EU strategic autonomy will be minimal, including for digital autonomy.

In contrast, there is a realisation in UK industry that the problems of Brexit for the economy could become more serious and the hope is for some form of middle ground to be found. That might support EU aspirations to build strategic autonomy. The same may be true in the UK military industrial complex and for relations in support of the EU, probably through NATO. At a later date, the exterior ministry (the Foreign Office) may also realise the wisdom of EU strategic autonomy in conserving UK security, in view of the international threats to the UK.

CURRENT EU INITIATIVES

Ongoing initiatives from the European institutions as well as those upcoming – that relate to the UK – are considered below.

Due to Brexit, the UK is increasingly excluded from EU digital programmes in science and technology, such as the Horizons series, be it in funding, exchange of knowledge in key areas, or joint initiatives for digital innovations or key information on cybercrime. Pockets of cooperation may continue, for example on spectrum regulation (through the Radio Spectrum Policy Group, RSPG, a grouping of the EU's telecommunications regulators that still includes the UK's OFCOM).

What may be most fruitful would be to make all EU digital-related research programmes and exchanges as inclusive as possible, because key communities in the UK could contribute to the EU digital autonomy strategy, principally those from:

- The UK university research community, in digital-related technologies.
- The design and media community, especially the major education centres for the arts (graphics, fine arts, fashion, architecture, industrial design, and so on).
- The medical and biological research community, pharmaceuticals, and chemicals.
- The UK military-industrial complex, including cybersecurity centres.

This would sow the seeds of cooperation for the future when the need for cooperation from both the UK communities and the EU becomes more critical, especially as the UK evolves politically.

On the EU side, future initiatives are unclear as the Brexit negotiations proceed but with little clarity on progress, real goals, or the possible final outcomes.

FUTURE CHALLENGES AND OPTIONS FOR UK–EU DIGITAL STRATEGIC AUTONOMY

Looking at a mid-term scenario (three to five years), this section examines the best options to strengthen EU strategic autonomy via support for EU digital autonomy, with UK contribution possibilities.

Considering the challenges, current EU supply chains are global, much coming from ASEAN (Association of Southeast Asian Nations) countries as well as from China. Some of these have critical vulnerabilities under current political stresses; for example, the world's largest wholesale fabrication of integrated circuits (ICs) with 5nm technology is located in Taiwan – currently a strategic target for invasion and seizure under the banner of nationalism. Moreover, only the largest 'fab' globally, TSMC (Taiwan Semiconductor Manufacturing Corporation), has 3 nm and 5nm processes, for very large scale integration (VLSI) fabrication, for the latest generations of mobile technology. Taiwan also hosts perhaps 50 per cent of circuit board and device assembly. Only ARM (based in the UK) licences microprocessor designs for low-power devices; these form the basis of 95 per cent of CPUs (Central Processing Units) and GPUs (Graphics Processing Units) in current and possibly future mobile devices as well as for servers generally, laptops, data centres, and industrial Internet of Things markets.

In terms of other challenges, the position and active role of the UK government is key, but it is not the whole story as the political situation changes (see sketches in Annex 2).

Should there emerge a more favourable political climate internally, the UK could provide increased support for EU digital strategic autonomy through:

UK economic projections of the economy's failings due to Brexit are still unclear

1. Contributing to the building of production for software, computing, and communications assets and their supply chains:

- Greater control over digital equipment and software supply via local value chains to reduce dependence on global production of components and systems.
- Expanding existing basic semiconductor technology R&D and its production, with advanced production techniques, for processors, and memory, also mass storage systems, networking platforms, mobile and consumer devices including those for (electric) vehicles, and so forth.
- European location of EU data for storage for security/access control.
- Creation and siting of media platforms for production and distribution – for example, via streaming of EU cultural assets from EU or global content providers with EU-based content distribution networks
- Commercial presence in space, especially as use of low earth orbits (LEOs) for micro-satellites becomes significant for mass public mobile communications, with sophisticated protection measures for in-orbit systems, especially for space debris.

2. Defence production to support strategic requirements for monitoring and detection, be it of 'cyberspace', aerial, naval, and ground forces and their movements, as well as the complete response systems.

3. Creation of dual-use technologies, perhaps funded by the defence budgets but released for application to consumer and professional products.

To achieve a UK–EU digital strategic autonomy drive, it will also be necessary to address key obstacles, which are, over the medium term:

- Opposition from the UK government, either by direct prohibition or by pressure on UK key assets and deciders to follow the general Brexit 'party line'. This could prevail for both general public opinion and specific key private sectors such as finance and defence (although the situation is more complicated in the case of the latter). Significant hostile press and TV campaigns would be expected.
- EU regulation covering cooperation with organisations in states outside the EU – potentially a major barrier.
- Lack of clarity on funding paths for EU support for the collaborative UK educational and research sector and also for the UK private technology sector.
- Obstacles to joint ventures between UK and EU enterprises similarly exist, if to be eligible for joint ventures requires enterprises to be EU sited.

It is essential to anticipate how these obstacles may develop over the next three to five years:

- UK economic projections of the economy's failings due to Brexit are still unclear, as COVID-19 effects cloud the picture (see Annex 2 for scenario sketches). Multiple factors may be in play currently, such as scarcity of skilled and less skilled workers, increases in supply chain restrictions on imports and exports and especially with the move new UK quality assurance certification standards. GDP contraction may be expected due to new UK regulation of goods exports/imports with customs processes and charges, as well as limits on ease of travel. The severity of the combined impacts

A high-security European cloud infrastructure would offer a safe repository for personal information

could also modify the populace's views on Brexit and thus future considerations of isolation vis-à-vis the EU.

- In practice, the effects of Brexit will only become clear in the longer term, but perhaps the direction of travel will become evident over the next two to three years, especially if the consequences of the shrinking UK economy are widely felt and not just in the deprived regions, perhaps with at least a 4 per cent long-term shrinkage in GDP. That would tend to diminish the appetite in the country for following the most fervent wing of the ruling party for Brexit isolation from the EU. As the realisation of the lack of new international markets to replace the EU also sinks in on the private sector, that will tend to reinforce business sectors turning to consolidate trading and technology exchanges with Europe.
- Moreover, in the devolved nations, in three to five years new plans at a political level will become more mature, perhaps with ambitions to become independent. For instance, in Wales new political alliances are forming (for example, Plaid Cymru with Labour in December 2021) to back national initiatives such as free childcare, a nationalised electricity supply company, and a construction group to build low-cost housing. By 2025, Scotland will be further down its declared road of independence and could hold its second referendum and even have won it, despite injunctions against it from Westminster. That might provoke a series of constitutional crises. All of these devolved nation initiatives may move their parts of the UK further towards general cooperation with the EU. The question is then one of what may occur for the remaining 82 per cent of the population, that is, England itself; it is perhaps the most internally divided of the UK devolved nations.

In this more benign context, there is a potential set of contributions that the UK could make to digital strategic autonomy – but the question is whether it can be counted on to participate in EU strategic autonomy support. The next section offers recommendations to increase the probability of cooperation with the EU for its future strategic autonomy.

POLICY RECOMMENDATIONS: CONCRETE SUGGESTIONS TO BE IMPLEMENTED IN THE POLITICAL AGENDA

The foundations of a UK contribution to EU digital strategic autonomy lie in what the EU and the UK will each need, as much as what the UK political position will permit in view of Brexit. Assuming the posture of hostility to the EU employed by the UK government has diminishing effects, there is a possibility of declining popular acceptance of this policy over the next three to five years. In this situation, various recommendations for how such support could be applied for EU DSA are considered below.

1. Harness UK contributions to digital technologies by organising facilities for cooperation in joint ventures, with both mature and early-stage companies:

- Create an organisation for easing cooperation – set up a support facility for new digital technology ventures with advice for legal and financial EU collaboration.
- Fund joint ventures (a) in the research and early product design phases, (b) in the first spin-off start-up enterprise phase with inward funding to the UK, shared perhaps with a mirror unit in an EU Member State; and c) explore hiring UK residents employed and paid by EU resident companies.

2. Set up facilities for UK universities to discuss ventures and funding from the EU with shared R&D outcomes for UK and EU expansion where appropriate. Moreover, such universities and centres of excellence should be encouraged to site an EU extension physically within an EU Member State for local teaching and research activities inside the EU, just as many such centres have been set up across the world.

3. Acquire key digital assets from the UK. Two major possible targets stand out that would give the EU digital autonomy strategy a realistic boost into the mainstream running of global digital industries (see Annex 1) with global CPU and GPU circuit design leadership. Targeting the design licence phase could be essential to building mainstream IC production at a global level. However, the two acquisitions of key digital design companies would be difficult to negotiate and expensive, fraught with sensitive issues for the UK. But the transaction long term might generate collateral advantages for relations with the UK. The only alternative is to seed comparable resources within the EU from new, which may be possible but more difficult and far riskier. However, this would require the EU to have an acquisition route, transfer of ownership, and ownership/management path, a capability which is quite alien to its structure and traditional goals. In this case, a solution perhaps combining the private sector and/or state venture capital organisations in the Member State might be considered.

4. Pursue military cooperation at five levels:

- Via NATO: EU cooperation and joint research projects within the remit of the organisation, for instance, joint initiatives under the Innovation and Enterprise Transformation programme between EU and UK small and medium-size enterprises (SMEs) and the NATO Defence Tech Accelerator for 2023. That would require creating a programme of projects in key areas applied to EU–UK SME cooperation, for example in production and manufacturing techniques, in specific digital technologies, or in wider challenges such as medical devices and treatment issues. This approach could also be applied to cooperation with research groups at UK universities. Projects should be for research groups and private sector enterprises that lie outside the traditional defence industrial base.

- If not already underway, create the EU equivalent of the agency that spawned the Internet, as ARPANET, the US Pentagon's Defense Advanced Projects Agency, DARPA, and open this new agency's calls for tenders for research projects to UK companies, research groups, and universities.

- Offer direct EU R&D contracts for appropriate joint research with the main UK defence and security companies for immediately applicable systems and devices. Again, direct cooperative university projects could be envisaged. Such contacts are monitored by the central government via the relevant ministry.

- Pursue longer-term ('far-out' high risk) research, with both UK defence and other digital technology companies, on much less defined target technology projects such as software quality, general processing techniques, levitation, tokamak fusion, displays, detection, cybersecurity, lower-power semiconductors, power source technology, materials sciences, adiabatic computing, mathematics of large-scale software verification, programme code semantics, and so on.
- Licencing to UK-based enterprises of military

research that can be applied to civilian uses for non-defence purposes for their products and services.

The long-term aim is to replicate US industrial innovation policy, through funding of dual-use R&D, whereby military technology innovations are funded by government but in reality subsidise mainstream technology companies. One example is the Apple iPod, often cited as a product whose technologies – mass storage, processing, display, and embarked power source – all came from military technology, much of it up to one or two decades previously. Another is the success of Qualcomm in digital signal processing ICs for mobile radio, based on research into signal processing for the US Army that was then freely patented and applied immediately to new products. The latter three initiatives could be under the 'EU DARPA' or separately managed.

5. Use the 'soft power' of the above initiatives to build a longer-term strategy for future UK interactions, as the progressive shrinking of the UK economy becomes more evident and the country becomes poorer. In consequence, the UK will tend to have a need of closer EU collaboration. The experience of engaging in the above programmes should help to generate mutual trust and build confidence. Applying this to support for the EU DSA requires expanding the interactive programmes as the UK's needs becomes clearer.

6. Create a high-security European cloud infrastructure (offered as a service) firstly to host services from EU service providers. It might also be extended to the UK. The infrastructure would also host all data within the EU. As such it would offer a safe repository for personal information both for the private sector and for public services. This would tend to integrate the digital environment in the UK with that of the EU and so extend mutual cooperation. Offerings for the UK should be at advantageous pricing levels. The UK–EU subsea cable infrastructure may need an enlarged capacity to handle the traffic.

7. Use the EU cloud infrastructure cited above to form a European content distribution network, for a media streaming platform to be used by all EU Member State media content owners and producers. Its design could mirror those now operating for national audiences and for global viewing from the US streaming services, but perhaps with greater capacity as it may serve up to 450 million users in the EU and a significant external community with its common languages content (Spanish, Portuguese, French, and others) in Latin America, Africa, and the United States, as well as English content.

This would require partnerships based on a suitable EC organisation to put the processes for continuous cooperation in place. Note that it is possible that the devolved nations, in spite of the UK central government's opposition policy towards the EU, might be interested in participating more constructively in the medium to longer-term (three to five years), but they are far smaller than England (with a total population of some 12 million). As noted previously, six main digital technology communities can be identified to help in building the EU DSA which have need of, or advantages in, greater integration with the EU. Each is anxious to differing extents to conserve ties for markets, R&D funding, and so on.

1. Firstly and perhaps most importantly for digital innovation are the university and research communities. They want access to EU research

The war has demonstrated that unprovoked aggression from Russia is now the major global threat

programmes for intellectual progress as well as funding, plus teacher and student exchanges with EU Member States and access to participation in EU start-ups. The absence of EU students means lower enrolments with associated impacts on funding.

2. Next are the design communities, firstly semiconductor design with two of the largest processor design houses in the world (see Annex 1), and also fashion design for clothing and accessories, textile design, industrial design of consumer and professional products, architecture and construction, graphic design, and so forth. Before Brexit this sector was larger than the UK manufacturing industries in net contribution to UK GDP, as sales were EU-focused as well as global. This community sees the EU as a high-value market making technical and design advances they wish to be part of. Some sectors, such as high-end fashion, have already migrated their business and key personnel to the EU.

3. The third community is the media sector, including video and film, music recording and events, advertising, and publishing, with training, exhibitions, promotions, and special events

4. The next community is that of military and security systems, software, and equipment – aerospace, cybersecurity, naval engineering. Partnerships across the EU into the UK have continued, including cooperation with BAE Systems for cybersecurity and with other UK companies for Airbus or in defence with Italian Leonardo and French Thales, and so on.

5. The fifth community includes pharmaceuticals and chemicals production and production equipment (much of which contribute to the digital equipment value chain), medical equipment, and medical devices.

6. The final community involves financial services of all kinds – share, bond, and currency exchanges, investments, commercial and retail banking, treasury, commodities trading and reserves, and so on, including financial technology companies.

CONCLUSION

UK interaction offering support for EU digital strategic autonomy should come from harnessing very specific parts of the UK economy – firstly R&D resources, primarily those in the universities and then high-technology industries, specifically defence, semiconductor technology design and manufacture, plus media production, especially graphics. The overall aim is to build up a level of research, design production, and production techniques with key production equipment (that is, expansion of the ASML/Philips core of expertise) to form a critical mass of consumer and dual-use military technology to reverse the 90 per cent dependency on non-EU supply chains.

POSTSCRIPT

Impacts of the war in Ukraine on EU–UK relations for digital strategic autonomy

The war in Ukraine reduces the timeframe in which the EU's digital strategic autonomy needs to be achieved, as well as the scope of what should be achieved. The war has demonstrated that unprovoked aggression from Russia is now the major global threat to the UK as well as to the EU.

That has already transformed the strategic directions of the UK defence establishment and its investments in military digital technology. It is reconsidering its previous global focus, in terms of the disposition and types of digital equipment to suit the expected forces. While the UK has been generous in donating surface weapons and training, the government took a much more reserved stance the migration matters, namely accepting Ukrainian

refugees to the UK. Presumably, this position follows Brexit policy, with much fewer entering than for the major EU Member States.

To address these issues, this section will examine the potential impact of the war in Ukraine on UK relations with the EU in the context of the EU's digital strategic autonomy. In the long term, the conflict will produce closer strategic relationships between the EU and the UK. But notable short-term difficulties can be expected due to the unusual political position of the UK's ruling party vis-a-vis the Russian administration.

Immediate influence of the war in Ukraine on EU-UK relations

The war highlights major difficulties in the way the UK government has developed relations with Russia over the past decade, with increasing financial flows into the London-based banks and bond and share trading markets and accepting major financial inflows from Russian businesses and private funds without differentiation on their origin. Many Russian companies are also registered in British overseas protectorates with banking laws that favour the anonymity of owners and transactions.

As a result, reacting to the situation in Ukraine makes the UK government face consequences and implications that are far more uncomfortable than those for any other non-EU country. Thus the parliamentary opposition has a greater responsibility for an adequate response to these events. For instance, one of the first acts of the current Prime Minister in 2020 was to appoint a member of the Russian business establishment – a UK resident and an owner of two UK newspapers – to the House of Lords, despite misgivings from the security services (Hughes, 2022).

Such influence matters. It limits the degree of active support that the current government may give to the EU's united effort to create the needed military infrastructure and respond adequately to the situation.

Noteworthy, while President Biden has publicly declared President Putin a war criminal, the UK cabinet via the foreign secretary (and not the PM) has refrained from any direct charge. It has noted that Russian forces have committed war crimes, without naming their president as responsible. Furthermore, the Ministry of Interior (the Home Office) following Brexit policy on immigration has been less eager to ease access to refugee entry visas for Ukrainians, compared to other European countries (France, Germany, Poland, Romania).[1]

Russian actions in Ukraine are condemned by the majority of the UK as well as by the armed forces and related groups. Most likely, the UK would let its military fulfil its duties as a full member of NATO and most likely would participate in building a common defence force with the EU and USA. However, it might be that the UK forces would prefer to act within a smaller sub-group. Thus, instead of joining the 30 or so NATO members, it would rather prefer cooperating with those within the EU that have a similar vision of the perceived threat as well as are adequately equipped. The group could take decisions faster to deliver an effective riposte to sudden threats.

Other relevant UK groups to be considered are those belonging to the cybersecurity community monitoring exploits by Russian groups and some parts of the intelligence well familiar with the EU's position.[2] Compared to the current party leadership, these communities may take a different view on the Russian administration, especially considering the assassinations on UK territory. Some representatives of these communities may feel that the Cold War has in fact never ended, particularly after

TABLE 1: **The nuclear balance of weapons, EU with the UK and other majors**

	Deployed warheads on missiles in bases	Warheads stored, or held in reserve	Delivery systems
UK	120	105	4 Vanguard class submarines (+4 Dreadnought submarines planned)
France	280	10	4 LeTriomphant class submarines; Cruise missiles, from 40 bombers
China	Not known	350	2 submarines; road-mobile ICBMs and in silos; 20 bombers with gravity bombs
Russia	1,625	4,630	11 nuclear submarines; 65 bombers, TU-160 Blackjack, TU-95MS Bear H; ICBMs; Sarmat missiles; Cruise missiles
USA	1,800	3,750	14 Ohio class submarines; silo ICBMs, in USA and NATO allies; 110 bombers, B-52 and B-21 with missiles and gravity bombs

Sources: Institution of Engineering and Technology, E&T, March 2022, *A Dangerous World*, multiple sources

the 2008 Georgian hostilities and the major cyber-attacks, such as the Notpetya debacle internationally.

Generally, they would tend to support increased EU digital strategic autonomy to build a concerted front across the 27 Member States, as part of a wider security effort with co-ordinated military defences, including cybersecurity measures. They certainly do not wish to stand alone against such a threat and, although the AUKUS community (Australia, UK, USA) is important, the recent reaction by France has shown that closer coordination within the EU would be necessary.

Direct impacts on UK–EU relations in the next three years

Taking into account the trends in UK public opinion on Ukraine, the level of support within the ruling party for the current Russian administration may decline or become far less prominent. It may be reset by eventual changes in the UK head of state and cabinet, possibly triggered by pressures from the opposition which led in the popular opinion polls in March 2022. Note that the UK has a small force in the Baltic states and has been providing training and supplying antitank weapons to Ukraine since 2015.

Consequences of the Russian invasion of Ukraine on direct UK military support and integration of UK forces with the EU and USA over the next 3–10 years

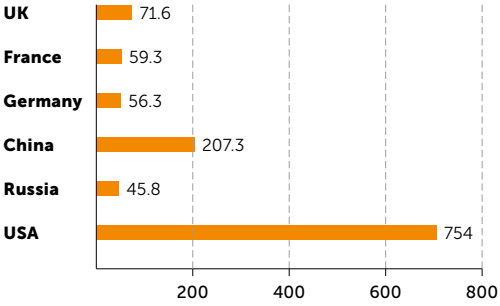
While digital systems are increasingly becoming a key part of the modern warfare, joint EU–UK development of these systems is probable. This could be realized through dedicated UK research establishments for airborne, subsea, space, and surface weapons, as well as its cybersecurity centres which constantly monitor hostile activities, devising new responses.

In the medium term (< 5 years), UK forces' technology collaboration programmes might take place only through NATO and more generally via dual use and military and commercial research projects with shared design and production for the resulting specific systems. The latter would tend to reinforce arguments for shared R&D programmes between the EU and the UK, especially for high-risk subject areas, for deliverables that have both military and civilian potential. Such an opportunity could also be considered for the EU–USA cooperation, perhaps via the DoD's DARPA. This would tend to positively impact the UK's level of cooperation, especially if an EU body equivalent to DARPA with close links was initiated.

Examining the UK military strategy in a medium/long term shows a major rupture with the previous defence review published March 2021 (UK Ministry of Defence, 2021). The preceding policy aimed at a global presence well beyond the EU and specifically at countering China with an Asian naval presence alongside the USA and Australia for the South China Sea, the Indian Ocean, and the Middle East. That implies a combined naval, space, and airborne capabilities. The apparently unexpected Russian land attack has moved global views towards the UK's own defence and specifically to the EU Member States bordering Russia, so an effective ground force becomes necessary. In comparison, China becomes a lesser geopolitical menace.

However, the stark reality is that the UK procurement function is in need of major overhaul as a number of expensive 'white elephants' have drunk the budget dry, such as the purchase of new light tanks, so far undelivered eight years from the original order. Moreover, the future budget is currently

FIGURE 2: **Defence Expenditures 2021 (US$ billions)**



Sources: HM Treasury, International Institute of Strategic studies, *Financial Times*, 30 March 2022

oriented to four Dreadnought submarines, plus aircraft carriers and their F-35 aircraft – for a global presence in Asia and the Middle East. A drastic policy revision could imply much closer EU-UK cooperation, specifically aimed at ground forces. Whether the current UK command and its policy advisors will see that remains an open question: ground forces are at low levels (some 73,000 regulars). Furthermore, another interesting question is whether a rapid move to local renewable energy, away from fossil fuels imported from the Middle East, would also change the defence policy focus on presence overseas.

Looking to defence spending, it is evident that Russia does not have the largest resources in terms of annual budgets and the UK's is actually larger.

But in terms of strategic response, namely nuclear weapons, the potential UK contribution to EU's overall strategic defence/response forces is not that significant, as shown below. If the MAD doctrine remains in place,[3] it might be a useful factor. In terms of a nuclear threat level, UK resources would approach a doubling of the EU's direct capabilities – but NATO weapons under the USA would be far more important. The UK contribution would expand the net capabilities of the EU in numbers of total deployed nuclear weapons but that would be under NATO, so the total capability would be the same.

CONCLUSION

The extremely brutal war in Ukraine demonstrates that the level of risk from Russia has changed the balance of geopolitical threat, forcing cooperation between NATO and EU Member States to a far higher level than might have been expected at the beginning of 2022.

That integrating force is also already acting on the UK's military stance to bring it closer to the EU and frontline Member States. EU–UK cooperation on military technologies could drive EU digital strategic autonomy. For that, it needs to be diligently managed in scope and objectives for real deliverables that may also have dual use applications.

NOTES

1. The Home Office requires applicants to create electronic documents in pdf with uploaded images in the midst of battle zones to apply for a visa; it does not just accept a Ukrainian passport: Letter section, *Financial Times*, 30 March 2022.
2. These internal tensions over financial influences have been explored in popular literature for some time – for instance J. Le Carré (2010), *Our Kind of Traitor.*
3. Mutually Assured Destruction – AJ Parrington, USAF, and Herman Kahn (second strike scenario and 44 step escalation ladder) RAND Corp.

REFERENCES

BBC News (2016). *EU Referendum Results*, https://www.bbc.co.uk/news/politics/eu_referendum/results.

Cabinet Office (2021). *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, 16 March, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf.

Coronavirus (COVID-19) Infection Survey (2021). Office of National Statistics, ONS, UK, 25 June, https://www.ons.gov.uk/peoplepopulationandcommunity/healthandsocialcare/conditionsanddiseases/bulletins/coronaviruscovid19infectionsurveypilot/25june2021/pdf.

Department for Digital, Culture, Media and Sport (2017). *UK Digital Strategy*, 1 March, https:/www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy.

Forster, P., Dunai, M., & Shotter, J. (2021). 'Businesses struggle to prepare for UK's post-Brexit import controls', *Financial Times*, 29 December, https://www.ft.com/content/eabd3113-c669-4792-95cf-b5ad0ea6da3b

HM Treasury (2020). *National Infrastructure Strategy*, November, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/938539/NIS_Report_Web_Accessible.pdf.

HM Treasury (2021). *Build Back Better: Our Plan for Growth*, 3 March, https://www.gov.uk/government/publications/build-back-better-our-plan-for-growth

ARM is delicately positioned globally ... designs could slowly be withdrawn ... regulatory oversight is impractical

Hughes, L. (2022). 'Vetting advice over peerage for Lebedev to be released', *Financial Times*, 30 March.
Institute for Fiscal Studies (2021). 01 December 2021, spend per pupil in England.
O'Connor, S. (2021). What a lost decade of education spending means for the economy', *Financial Times*, 6 December, https://www.ft.com/content/3dbbc60e-015d-45ff-8c9f-bf06515af929.
Office of Budget Responsibility (2021). *Economic and Fiscal Outlook – October 2021*, 29 October, https://obr.uk/efo/economic-and-fiscal-outlook-october-2021/.
UK Ministry of Defence (2021). *Defence in a Competitive Age*, CP 411.
Wolf, M. (2021). 'UK's game of chicken will end badly', *Financial Times*, 10 November.

ANNEX 1

Acquiring UK key digital assets that may already be in play for mergers and acquisitions

There are two assets that may be potential targets in a short time frame. The first is the circuit design house ARM, owned by Japan's SoftBank and now under offer from the United States' Nvidia but with strong opposition to this acquisition. ARM is expensive and irreplaceable. It serves the mobile device industry with design licences for low power microprocessor production. Over 95 per cent of smartphones are based on its designs, be they Apple or Android-based such as those from Samsung, Sony, Nokia, and the Chinese phone suppliers; they are also needed for low power processor applications in industrial systems (Internet of Things types). Consequently, ARM is delicately positioned globally. An industry-neutral 'safe pair of hands' is needed – which the semiconductor industry and key governments do not view Nvidia as being – as the current free and non-discriminatory equal access to ARM designs could slowly be withdrawn. Regulatory oversight is impractical. If a suitable EU ownership mechanism can be employed, the EU could, directly or indirectly, be that safe pair of hands, which demands long-term reliability and commitment to agreed contracts on design availability. If a suitable management or proprietorship mechanism is available, the EU could be the potential direct or shared owner of choice for a global design house with open industry access. Technical operations might also be spread across the EU, possibly with investment in centres of expertise such as Grenoble, Eindhoven, Barcelona, Milan, and Dresden.

However, an acquisition agreement would be hard to negotiate unless a 'win–win' strategy can be found. This would have to placate three opposing

forces. The first is the nationalist political side of the UK central government, possibly with the UK regulators, principally the Competition and Markets Authority. The second is the semiconductor industry as a whole, predominantly the wholesale microprocessor suppliers and consumer device makers – and their national regulators. Any agreements would have to ensure equal access to the IC design house for UK enterprises on the same conditions as those for any producer globally. The third consideration would be SoftBank, so the cost may be high as SoftBank was offered US$39 billion in cash and Nvidia shares some two years ago (Waters, 2021), shares that are now worth over US$82 billion, and ARM revenues have climbed more than 60 per cent this year as it enters new markets with new designs for industrial applications. It may be that a European venture capital group could be involved, with EU (EC?) participation.

The second possible target is Imagination Technologies, a producer of designs and products for advanced graphics processors (GPUs) and owned since 2017 by a Chinese enterprise, Canyon Bridge, headquartered in the Cayman Islands and financed by China Venture Capital, which is owned by China's State Council (Datenna, n.d.). Imagination Technologies is thus also a licencing design house with global customers. It was purchased for €619 million and is now in the limelight due to this somewhat controversial ownership, previously ushered in under the Cameron government's overtures to China after losing key customer Apple (now returned). Its ownership generated conflict and a boardroom battle in 2020 as Canyon Bridge tried to move the company to China, a plan blocked by the UK Secretary of State for Digital, Culture, Media and Sport. The Committee on Foreign Investment in the United States (CFUIS) committee had previously blocked Canyon Bridge from acquiring Lattice Semiconductor. Negotiating a change of ownership for Imagination would be difficult, but an EU 'ownership' or guiding initiative might be an attractive solution to all parties, even Canyon Bridge, which is effectively blocked. Note that a FRAND (Fair, Reasonable And Non-Discriminatory) agreement to supply product freely applied to the China link may be controversial. Imagination has offices in Romania, Poland, and Taiwan, plus a presence in China and India. It is moving from its GPU core offering back into CPUs (it sold off its product line from the CPU company MIPS it acquired in 2017) and is now entering electric vehicle (EV) automotive electronics with its GPUs, as well as the data centre, neural network (NN) processing, and desktop markets.

ANNEX 2

Four brief scenario sketches for building an EU digital strategic autonomy initiative with the UK (with a focus on its inherent instability)

Perhaps seeming melodramatic but possibly more realistic than is always apparent externally, these four scenarios are only suggestions of future possibilities – but no more.

1. The longer-term trend is more of the same (sort of)

The UK economy continues to be fairly successful despite reduced EU trading, with gradually declining GDP each year. However, with the current government being seen as fairly effective, nationalism is pushed further by its media supporters. But after five years of this, the public mood slowly changes to be less supportive and a coalition government

The EU produces a large amount of digital media content, but a common streaming site for digital distribution is lacking

of opponents enters power in a 2025 election. That begins to slowly thaw some relations with the EU on trade. The UK continues to be an external actor but is now a (weakly) supporting one – no longer painting the EU as an intransigent enemy, as is the current position. It passively watches the formation of complete European Strategic Autonomy (ESA), and specifically European Digital Strategic Autonomy (EDSA)

2. A new broom sweeps clean

A new government enters power in two or three years as the current ruling party is ousted by corruption scandals, instability, inflation, and mismanagement. An emergency election is called. The ageing UK demography is reduced substantially by new COVID variants and the collateral effects of rising death rates in care homes plus lack of NHS treatment for fatal conditions in the aged. The older voters' hold on power breaks down. They are replaced by a next generation of more educated, politically active, registered voters who have grown up poorer, deprived, and unable to own a home until middle age, if at all. They are heavily dependent on state benefits to supplement minimum wages. The contrast in government, now formed by a coalition of three opposition parties elected by tactical voting, precipitates a move to seek European Economic Area/European Free Trade Area (EEA/EFTA) status with the EU. That is pushed eagerly by UK industry to renew trading relations and seek limited EU funding support for UK industry. The four freedoms on movement of goods, capital, services, and citizens return. Backing for the key pillars that support EU DSA is endorsed by this government. It gives material aid through cooperation in R&D and university technical education, with military forces and assets under NATO organisation, allocating resources to expand defence production to support EU strategic autonomy.

3. Break-up

While dissension in the UK Parliament, especially in the ruling party, and in the country continues, the traditionally dominant party in Ulster is replaced by the opposition in a 2022 vote. A crisis is precipitated to stop the handover of power. That returns the state of Northern Ireland (NI) to direct rule from London but, sensing a wind of change, the other two small devolved nations hold and win referendums on seceding from the UK, despite central government's ban on such votes. As tensions slowly rise over 2023 and 2024, the blocked party in NI seizes the reins of power, despite threats of force against it, and it then combines with the two smaller nations to declare a non-England union, which is finally accepted by the English Parliament in London to end the increasingly violent turmoil due to the border to the south (with infantry regiments on alert) and the trade border in the Irish Sea. A new Gaelic–Celtic Union negotiates with the EU and rapidly wins membership. England continues alone, with its government pursuing a more belligerent anti-EU stance while the economy meanders on.

4. Slow meltdown

The UK descends into sharp economic difficulties with the demise of its trading position globally and then a more rapidly shrinking economy due to unexpected non-linear implosion effects possibly linked to energy prices and the bursting of investment bubbles based on margin trading in the US markets. Supported by the older vote, the current government remains in place despite its failures. It rejects overtures from the EU to provide aid from its support fund for underdeveloped economies.

Two major trends escalate. Firstly, the rate of emigration accelerates, some to the EU but many more to Canada and Australia, traditional migration destinations. Secondly, the economy implodes further: higher-value industries start to migrate in their entirety from 2026, especially in financial services and high-technology manufacturing, mostly to the EU. The aim of the EU at this point would be to attract migration by those in key digital industries, especially in R&D, in both the academic and private sectors, making citizenship as well as job placement offers, copying the Portuguese model.

It is emphasised that the above are only very brief sketches of the kinds of scenarios we would usually contribute in our major studies (gathering information from a wide range of sources, usually destined for the European Commission, or the European Parliament) so these are, just very brief abstracts of far more detailed analysis or 'stories about the future' – and no more – with possibly sharpened transformations to bring out the different trajectories.

REFERENCES

Datenna (n.d.). *The Acquisition of Imagination Technologies*, https://www.datenna.com/the-acquisition-imagination-technologies/

Waters, R. (2021). 'Arm's reach regulators pore over Nvidia takeover of chip designer'. *Financial Times*, 23 November.

Digital Autonomy and Taiwan–EU Partnership

Huai-Shing Yen

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Governments across different regions of the world have actively invested in initiatives that promote digital transformation to ensure nations' digital autonomy, with the EU as one of the leaders. The recent disinformation warfare undertaken by Russia as part of its invasion to Ukraine further underscores the threat to, and importance of digital autonomy. Based on both the EU and Taiwan's efforts in promoting digital autonomy, this chapter offers several recommendations, including creating a systematic dialogue and information-sharing mechanism, as well as forging partnerships in R&D collaborations, talent development and data/privacy governance.

THE AUTHOR

Huai-Shing Yen is deputy executive director of the Taiwan WTO & RTA Center at the Chung-Hua Institution for Economic Research (CIER), a Taiwan-based international policy think tank for economic and industry-based research. The CIER offers expertise to government to help develop and implement economic and industrial policies and industrial development strategies. It also collaborates with academia, government, and industry for promoting sustainable development of the economy.

THE EU DIGITAL POLICY FRAMEWORK AND THE EMERGENCE OF A DIGITAL AUTONOMY POLICY

It is becoming a common trend globally for governments across different regions of the world to actively invest in initiatives that promote digital transformation with a view to ensuring national digital autonomy. The importance and urgency of digital transformation and autonomy has been amplified by recent Russia's invasion of Ukraine. In addition to military invasion, Russia also launched a large-scale disinformation exercise against Ukraine. According to EUvsDisinfo, Russia has 'waged a sustained and coordinated state-controlled disinformation campaign targeting the Russian population, Russia's neighbour countries, and the rest of the world, particularly aiming at influencing public opinion' (Delegation of the European Union to China, 2022). One of the possible consequences of Russia's disinformation warfare is that, instead of aligning with Russia's assertions, it has made the European Union and Taiwan alerted and better understood of the importance of digital autonomy, and therefore seek to accelerate the transformation process. This paper starts with reviewing the overall digital strategies implemented by the EU and offers policy recommendations to a closer Taiwan–EU partnership in digital autonomy that takes into account the recent development of Russia's disinformation campaign.

Driven by policies at Member State level, the EU is becoming a leader in digital transformation policy and is dynamically moving towards the goal of a 'Digital Single Market' that is one of the key pillars of a 'European digital future'. The European Commission has put forward key working programmes under the 'Europe Fit for the Digital Age' agenda in the 2019 policy framework, and for the issue of digital transformation, the EU aims to

The '2030 Digital Compass' spells out specific development goals blueprints, and milestones to be achieved at each stage

develop digital technologies that will enable all citizens and businesses to benefit and work with international partners to cope with major challenges.

Further, the '2030 Digital Compass' published by the European Commission during the COVID-19 pandemic spells out specific digital development goals (European Commission, n.d.), blueprints, and milestones to be achieved at each stage for the EU. The '2030 Digital Compass' also identifies a series of digital transformation-related legislations that have already been enacted, such as the Data Governance Act, the Digital Services Act, the Digital Markets Act, and Cybersecurity Strategy. In addition, the EU also supports the investments required for digital transformation through various funding mechanisms, including the Cohesion programmes, the Technical Support Instrument, and the Digital Europe Programme. The EU legislature is supporting Europe's digital transformation by dedicating at least 20 per cent of the funding from the Recovery and Resilience Facility. Four policy targets envisioned by the EU's '2030 Digital Compass' include a digitally skilled population; safe, efficient, and substantial digital infrastructures; digital transformation of businesses; and digitisation of public services. These targets reflect the EU's ambition to comprehensively enhance the digital capabilities of the society with an inclusive concept, promoting digital transformation, as well as safeguarding the development and basic values of the EU with the concept of digital sovereignty.

The concept of 'digital autonomy' began to draw the attention of EU Member States when French President Emmanuel Macron raised the issue of strategic autonomy in his 2017 speech at the Sorbonne (Macron, 2017). Since then, strategic autonomy, including digital autonomy, digital sovereignty, and technological sovereignty, have become popular political as well as geopolitical discussion topics (Codagnone, Liva, Gunderson, Misuraca, & Rebesco, 2021).

As defined by the European Political Strategy Centre (EPSC, 2019) of the European Commission, strategic autonomy refers to the capacity of a political entity to pursue its own course in international relations. It is also the capacity of states to decide and act upon essential aspects of their longer-term future in the economy, society, and their institutions. The EPSC further argues that as the EU's ability to defend and promote its interests, as well as its credibility as a strong foreign policy actor, is a function of its cyber resilience and technological command, the concept of strategic autonomy must be broadened to include at least the following three digital related dimensions: the protection and mastering of critical digital technologies, the protection of critical digital infrastructures, and the enhancement of cyber resilience.

TAIWANESE EXPERIENCES IN PROMOTING DIGITAL AUTONOMY

While there is no formal policy framework in Taiwan directly addressing the issue of digital autonomy as defined above, key aspects of digital autonomy as a policy consideration are already part of Taiwan's industrial and digital policies.

New legal framework proposals for enhancing digital autonomy

With a view to promoting the development of digital technologies and services, as well as of providing a new framework for data governance, Taiwan's government is preparing to introduce three major legislative proposals to provide a new legal framework that are also implicitly contributing to the enhancement of digital autonomy in Taiwan.

The first legislative proposal that is being considered is that of the Industrial Digital Development Promotion Act. The purpose of this Act is to create a sound environment for digital development with a light-handed regulatory approach, and to encourage digital innovation and experimental undertakings. The second proposal is the legislation for the promotion of government and public sector digital service. This bill will promote digital transformation of the public sector by way of elevating the effort on government and public sector digital services development and creating an environment for digital innovation in public services. The third proposal is for a new Data Governance Act. The aim of the Act is to build a common framework for cross-sector and cross-domain data governance in Taiwan.

In addition to the new digital legal framework envisioned in these proposals, amendments to two existing laws are also being discussed. The first proposed amendment relates to the Cyber Security Management Act, and the second is on revising the Electronic Signatures Act. The primary objectives of the amendments under consideration are to create an updated national information security policy and environment that are in line with emerging national security needs and commercial development trends.

The creation of a new Ministry of Digital Development

A major milestone in Taiwan's digital policy is the creation of the new Ministry of Digital Development (MoDD) in 2022. Currently the roles and jurisdictions of policy development, regulatory oversight, and most importantly forward-looking assessment on Taiwan's digital future and autonomy are divided across multiple government agencies. For instance, while the National Development Council is the overall digital policy planning body, the National Communications Commission also plays a key role in the development of the digital infrastructure, and there is an absence of main government authority in charge of overall cybersecurity resilience. Diversified approaches were adopted on data governance across different sectors, with the healthcare and financial sectors facing a significantly higher level of regulation while other sectors face little guidance.

Against this background, and with the recognition that sound digital policy is a key aspect not only of industrial development but also in the safeguarding of Taiwan's civil society and democracy, the concept of the MoDD was discussed, debated, and developed during President Tsai Ing-wen's first term in office and the legislation was tabled to parliament in 2021. On 28 December 2021, Taiwan's legislature approved the law to establish the new MoDD to be in charge of planning Taiwan's nationwide digital development policies.

The MoDD, which is expected to be in operation in 2022, is commissioned with three major assignments, namely: (1) the planning, coordination, promotion, review, and formulation and implementation of national digital development policies, resources, and digital infrastructure; (2) the establishment of a robust digital technology application and innovative development environment to support digital talent cultivation; and (3) oversight of national information security policies and supervisions. The MoDD is also the focal point for the development of public sector digital services, data governance, and openness. As such, from a digital autonomy policy perspective, the MoDD will serve as the competent authority as well as the main coordinator with respect to the design, planning, and delivery of digital autonomy policy in Taiwan.

Industrial policy supporting digital autonomy

Firstly, the pursuance of leadership and extensive participation in the development of critical digital technologies has always been a major element of Taiwan's industrial policy. In the latest industrial development programme published in 2020, Taiwan identifies six 'Core Strategic Industries' as priority sectors, including three digital technology-intense sectors, namely information and digital industries, the cybersecurity industry, and the precision health industry (National Development Council (Taiwan), 2021). The objectives of the programme are, inter alia, to maintain Taiwan's leading position in digital technology, export the artificial intelligence of things (AIoT) and smart medical solutions to the world, and secure a key role in the 5G global supply chain. For the cybersecurity industry, research and development (R&D) will be undertaken on protective technologies for 5G, semiconductors, AIoT, and healthcare, and an organisation will be established for cybersecurity defence and cross-country collaboration. Although not stated explicitly, there is a high degree of similarity (and complementarity) between these Taiwanese policy objectives and key dimensions of the EU's pursuance of digital autonomy.

RECOMMENDATIONS FOR TAIWAN–EU PARTNERSHIP IN DIGITAL AUTONOMY

International partnership has already been included as a major agenda in the EU's '2030 Digital Compass' policy. Specifically, in addition to focusing on its own digital transformation, the EU is also aiming at playing a key role in the global digitalisation process. For instance, the EU is committed to promoting the establishment of digital partnerships with the international community to foster the universal values that the EU upholds, such as fair competition in the digital market, safe and secure cyberspace, and the safeguarding of fundamental human rights.

Further, Russia's massive disinformation campaign on Ukraine provides a real-life demonstration of the threats that EU and all democratic countries faces regarding digital safety. Disinformation campaigns and cybersecurity attacks have been taken by Russia not only targeting Ukraine, but also on the EU. Faced with these exceptional situations, the EU has urgent need to explore with its partners more collaborations to safeguard cybersecurity and counter disinformation, and to enhance the resilience of the digital infrastructure.

Against this background, and considering the convergence of policy priorities and institutional architectures, this chapter presents five recommendations for future Taiwan–EU cooperation.

1. Create a systematic dialogue mechanism between the competent authorities

The first area of future cooperation between Taiwan and the EU is the pursuance of a systematic and formal dialogue mechanism between policymakers and authorities on the digital autonomy agenda. As discussed above, Taiwan is a latecomer in terms of digital policy harmonisation and coherence, yet Taiwan has one of the most extensive levels of experience in digital technology development and in mitigating cybersecurity threats from hostile forces as well. More importantly, it would be mutually beneficial for EU to share its experiences on the effectiveness of anti-disinformation tools learned during the Russia disinformation campaign, including possible new approaches to mitigate the threats. Exchange of information and experiences, as well as enhancement of policy priorities and best practices, is an important confidence-building process

A major milestone in Taiwan's digital policy is the creation of the new Ministry of Digital Development

that underpins broader collaboration in the future between Taiwan and the EU.

2. Establish an information-sharing mechanism in combating disinformation and foreign digital interference

Since Russia deploys cyber warfare and disinformation strategies in its war on Ukraine, online platforms, internet service operators etc. are playing important role in dispatching correct information. The EU has taken a number of measures to counter disinformation, yet considering the borderless nature of the Internet, it will be more effective to tackle the issues through enhanced international collaborations. To start with, Taiwan and EU should consider establishing an information-sharing system focusing on disinformation and information manipulation in the context of the Ukraine war, and a coordination framework for Taiwan's public and private stakeholders to cooperate with EU. This mechanism also helps to create a precedent to extent the collaboration to cover other incidents in the future.

3. Forge stronger partnerships in digital technologies and industries

Another area of cooperation is the strengthening of alliances and partnerships in digital technologies and industries. Taiwan and the EU have a long history of industrial partnership for both manufacturing and the services sectors, with experiences of partnership in third country (mainly China) market development. This foundation underpins cooperation and partnership in the area of digital technologies. In addition to new alliances in semiconductor manufacturing, sectors such as artificial intelligence (AI), smart medical products, and data/cyber securities can be regarded as priority sectors for Taiwan and the EU to elevate industrial cooperation.

Taking AI as an example, the EU's AI strategy, as reflected in its AI policy white paper (European Commission, 2020), is to create an AI 'ecosystem of excellence' by following each link of the AI value chain and formulating appropriate incentives to accelerate the adoption of AI-based industries in relevant industries, including small and medium-sized enterprises (SMEs). In Taiwan, the cost of introducing human–machine collaborative robots as a solution is relatively low, and there is an increasing number of SMEs in Taiwan, especially those that have returned to Taiwan because of the US–China trade war in recent years, that are eager to introduce smart manufacturing as the solution to mitigate cost and labour-shortage issues. Therefore, a policy and industrial alliance of AI and smart manufacturing between Taiwan and the EU would be a good starting point.

4. Deepen R&D collaborations and talent development

Furthermore, the EU intends to establish digital partnerships between industry, scientific research, and academia, especially in the fields of key technologies such as 6G mobile networks, quantum computing to digitally combat climate change and environmental challenges, and others, to maintain and continue to strengthen Europe's global competitiveness.

These are also areas that Taiwan considers key emerging technologies and areas of focus, and it is committed to investing in next-generation technology development and talent development. For instance, Taiwan enacted new legislation, the Act on National Key Fields Industry–University Cooperation and Skilled Personnel Training, in 2021 with a view to providing flexibility for universities to locate funding and create training programmes

through public–private partnership arrangements. Five new Graduate Schools for Advanced Technology or Schools of Semiconductor Research were subsequently establishment in five top tier universities cross Taiwan in 2021 through joint collaboration with the private high-tech sector (Reuters, 2022). The strong commitment and substantive actions taken by both Taiwan and the EU indicate that there is an extensive list of potential R&D topics and partnerships between Taiwan and EU in the area of next-generation digital technologies.

5. Enhance partnership in data governance and privacy protection regimes

Finally, in the area of data governance and privacy protection, the EU is the recognised global leader in the establishment of disciplines and institutions to deliver relevant policies. Taiwan has been learning from the EU model and its approaches to data governance. Partnership in this area would facilitate Taiwan's readiness and contribute to the EU's aim of creating a sound and robust global network on data governance and privacy protection between like-minded partners.

REFERENCES

Codagnone, C., Liva, G., Gunderson, L., Misuraca, G., & Rebesco, E. (2021). *Europe's Digital Decade and Autonomy* (Study PE 695.465), European Parliament, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695465/IPOL_STU(2021)695465_EN.pdf.

Delegation of the European Union to China (2022). 'Disinformation About Russia's invasion of Ukraine – Debunking Seven Myths spread by Russia', https://eeas.europa.eu/delegations/china/112997/disinformation-about-russias-invasion-ukraine-debunking-seven-myths-spread russia_en.

EPSC (European Political Strategy Centre) (2019). 'Rethinking Strategic Autonomy in the Digital Age', *EPSC Strategic Notes*, 30, https://doi.org/10.2872/231231.

European Commission (n.d.). *Europe's Digital Decade: Digital Targets for 2030*, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en#documents.

European Commission (2020). *On Artificial Intelligence – A European Approach to Excellence and Trust* [COM(2020) 65 final], https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

Macron, E. (2017). 'Sorbonne Speech of Emmanuel Macron', *Ouest France*, http://international.blogs.ouest-france.fr/archive/2017/09/29/macron-sorbonne-verbatim-europe-18583.html.

National Development Council (Taiwan) (2021). *Program for Promoting Six Core Strategic Industries*, https://www.ndc.gov.tw/en/Content_List.aspx?n=2D827BFE7E3598BE&upn=4D3DA452D04C42CC.

Reuters (2022). 'Taiwan invests in next generation of talent with slew of chip schools', 11 March, https://www.reuters.com/markets/funds/taiwan-invests-next-generation-talent-with-slew-chip-schools-2022-03-10/

Japan: Digital Sovereignty as an Element of the Economic Security

Kiyotaka Yuguchi

https://doi.org/10.53121/ELFTPS1 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

The terms 'digital sovereignty' and 'strategic autonomy' are neither officially nor generally used in Japan. Instead, the term 'economic security' ('keizai anzen hosyo' in Japanese) is commonly used in a general sense, without being clearly defined, and includes the EU's concept of 'digital strategic autonomy'. Thus, these two different policies have many similarities. The Japanese government is currently preparing legislation on 'economic security', and the range of regulations is currently under discussion in several expert meetings within the government. The draft law was approved in the Cabinet meeting and submitted to the Diet on 25 February 2022 and the law will be decided by June 2022. Keidanren (Japan Business Federation) supported this legislation in 9 February and called for early enactment of the bill in 14 March.

THE AUTHOR

Kiyotaka Yuguch is Professor at Sagami Women's University, Japan, Faculty of Human Society Department of Societal Management. Professor Yuguchi has published extensively on the telecommunications industry, mobile telephony, and radio spectrum policy issues in Japan and internationally.

The terms 'digital sovereignty' and 'strategic autonomy' are not commonly used by industry or the general public in Japan. For example, neither term appears in Wikipedia Japan. In other words, there is no official definition in Japanese. Instead of these terms, 'economic security' is more popularly used in Japanese, and both the government and industry have recently recognised its importance.

On 10 March 2021, *Nihon Keizai Shimbun* (Nikkei newspaper) introduced the term 'digital sovereignty in Europe' as its word of the day (Nikkei, 2021). Digital sovereignty in Europe means that the EU is taking the initiative in making international rules for the semiconductor industry, which affects competitiveness in digital industries, and for data, referred to as 'oil in the 21st century', by constructing an independent industrial base so that Europe is not dependent on any region or country outside the EU.

Many Japanese observers, thus, recognise digital sovereignty as economic security. However, there is no clear definition of 'economic security', and the concept has changed over time. In addition, national interests also vary among countries. Naoki Nakamura, a member of the Research Bureau for the Economy, Trade and Industry Committee of the House of Councillors, insists that the concept of 'economic security' must be redefined and a consistent policy system must be constructed (Nakamura, 2020). He has suggested that the term covers three political categories: (1) David A. Baldwin's concept of 'economic statecraft', (2) economic resilience and the strengthening of industrial power, and (3) the strengthening and restructuring of the international economic system.

RECENT POLITICAL MOVEMENTS

On 17 December 2013, Shinzo Abe, Prime Minister of Japan, officially determined the National Security

The aim is to achieve digitalisation and greening at the same time through creation of the 'smart island' of the whole of Japan

Strategy (NSS) in the Cabinet meeting and the National Security Council (Cabinet Secretariat, 2013a). The NSS replaced the Basic Policy on National Defense, which was decided in 1957, and would guide Japan's national security policy over the next decade.

The Ministry of the Economy, Trade and Industry held the Semiconductor and Digital Industrial Strategy Review Meeting in March 2021, and it published the Semiconductor and Digital Industrial Strategy in June 2021 during the Abe administration (Ministry of Economy, Trade and Industry, 2021). This strategy contained a dramatic change in the traditional Japanese industrial policy formed in the wake of friction between the United States and Japan over semiconductors in the 1980s and early 1990s. In order to secure the digital industrial infrastructure which supports the economy, society, and democracy, the strategy proposes that Japanese government becomes more deeply involved in private businesses beyond traditional support for the private sector, although the government still respects the principles of capitalism and free trade. The strategy envisions (1) the building of semiconductor plants in Japan with foreign manufacturers to realise domestic production of the next foundry technologies, (2) the promotion of a Japanese location for the core data centre in Asia, and (3) the cultivation of cloud service providers rooted in Japan. The aim of this strategy is to achieve digitalisation and greening at the same time through creation of the 'smart island' of the whole of Japan, so that Japan can export these innovations and systems and contribute to digitalisation and greening on a global scale.

The background of this political change was the significant decline in the Japanese semiconductor industry and the South Korea–Japan dispute after 2019. The semiconductor industry in South Korea holds more than 20 per cent of the market share in the world, whereas Korea imports many key materials such as high-purity hydrogen fluoride from Japan. However, the country has long been suspected of illegally selling these materials to China on the black market, and thus the Japanese government began strictly controlling exports. The Korean government strongly resisted Japan. In addition, in order to requisition Japanese firms' assets in South Korea as restitution for the unpaid salaries of mobilised Korean workers during the late stage of the Second World War, Moon Jae-in, President of South Korea, wanted to discard the Japan–Korea Basic Treaty signed in 1965, which included agreement on this unpaid debt, and under which Japanese and Korean companies have expanded their business ties (Ministry of Foreign Affairs of Japan, 2019). The Korean semiconductor industry has been severely affected by the Japanese government's strict application of export regulations. In this context, the Japanese government and industry have recognised the importance of economic resilience.

Fumio Kishida, who became Prime Minister of Japan on 4 October 2021, introduced 'creating the New NSS' and 'rule-making to bolster free and open global economic systems' as two major policies. He organised the first meeting of the Council for the Promotion of Economic Security on 19 November 2021 and opened the Office for Preparation of Legislation for the Promotion of Economic Security. Takayuki Kobayashi, Minister in charge of Economic Security, Minister of State for Science and Technology Policy, and Minister of State for Space Policy, organised the Expert Meeting on the Legislation for the Promotion of Economic Security. The Expert Meeting advances discussion at a rapid pace in order to submit the

draft law on the promotion of economic security to the 208th ordinary diet session, convened on 17 January 2022.

Prior to Kishida's initiatives, Ryota Takeda, Minister of Internal Affairs and Communications in Yoshihide Suga's Cabinet, referred 'consideration of modalities of ICT policy to 2030' to the Information and Communication Council on 30 September 2021. The General Policy Committee under the Info-communications Sub-council of the Information and Communication Council undertook this consideration and held its first meeting on 4 November 2021. The Expert Meeting and the Committee discuss the same issues of economic security in the ICT industry separately, while discussions on these two bodies may be mutually influenced each other. The partial report from the Committee will be submitted in June 2022.

ASSESSING THE PROBLEM

The sudden increase in discussion about economic security is a response to the urgent need to review economic policy from a national security viewpoint. New risks to public safety and security have appeared in the context of:

- The digitalisation and upgrading of the industrial infrastructure.
- Economic development in emerging countries and the deepening of the global value chain.
- The expansion of a range in national security from military domains to economic and technological domains.

Japan has, however, maintained its commitment to a free and open economy.

More concretely, a number of circumstances have arisen simultaneously:

- The government is strengthening its national resilience plan following a series of natural disasters including floods, earthquakes, and volcanic eruptions in addition to the Great Hanshin-Awaji Earthquake in 1995 and the Great East Japan Earthquake in 2011.
- Many Japanese manufacturers have withdrawn from the communications equipment business due to both the popularity of their competitors such as Apple and Huawei and the separation of the terminal price from the communications charge in Suga's initiatives to cut the consumers' communications costs.[1]
- Security issues have become apparent in networks and terminals as a result of the recent economic confrontation between the United States and China.
- The importance of securing strategic supplies became clear in the light of the unavailability of masks, vaccines, oral drugs, and semiconductors during the COVID-19 pandemic, as well as the Japan–South Korea dispute mentioned above.
- Many people aware delay of digitalisation in firms and business processes through some experiences during the COVID-19 pandemic, such as difficulty of remote work and reception of support money.

Apart from internal issues such as circumstance and the Japan–South Korea dispute, many of the issues and solutions addressed in the NSS by the Japanese government apply equally to European digital strategic autonomy, as mentioned in the next section.

Finally, the Japanese government is preparing the PS-LTE system, which connects many governmental bodies concerned with public safety via a single wireless network. Part of the system will start to function in 2022. There is no plan to substitute this new system for the communication network of each

body, although the PS-LTE was originally intended to make efficient use of public sector bands rather than responding to national security concerns. However, it is expected that sharing a common database will facilitate activities by multiple governmental bodies.

ASSESSMENT OF EU SITUATION

By assessing discussions in the Council for the Promotion of Economic Security, the Expert Meeting on the Legislation for the Promotion of Economic Security, and the General Policy Committee under the Information and Communication Council, we will see how the Japanese government and the experts assess the situations of the EU and the United Kingdom, as well as how they perceive the background, the current situation, and the scope and challenges of the economic security problems.

COUNCIL FOR THE PROMOTION OF ECONOMIC SECURITY

Japanese Prime Minister Kishida has introduced two major policies, 'creating the New NSS' and 'rule-making to bolster free and open global economic systems', and he has committed Japan to playing an active role in international rule-making in order to realise the Data Free Flow with Trust (G20 Osaka Leaders' Declaration, 2019; Prime Minister's Office of Japan, 2021).

At the first meeting of the Council for the Promotion of Economic Security on 19 November 2021, Kishida announced three priorities in the Japanese government's pursuit of economic security:

- Improve the autonomy of the Japanese economy by bolstering the supply chain and ensuring the reliability of the core infrastructure.
- Foster core technologies such as artificial intelligence (AI) and quantum, and ensure the superiority and indispensability of Japanese technologies.
- Aim to maintain and strengthen universal values, such as freedom, democracy, human rights and the rule of law, and the international order, which have until now underpinned the peace and prosperity of the international community.
  (Prime Minister's Office of Japan, 2021)

In the meeting, Takayuki Kobayashi, Minister of Economic Security, spoke about the need for engagement in four areas:

- Bolstering the supply chain of key commodities and important raw materials.
- Ensuring the reliability of the core infrastructure.
- Fostering and supporting core technologies by both public and private sectors.
- Preventing the outflow of subtle inventions, which may affect national security, through non-disclosing patents.
  (Cabinet Secretariat, 2021a)

Kishida then ordered him to prepare the legislation in these four areas and to organise an expert meeting for examination of the draft law.

EXPERT MEETING ON THE LEGISLATION FOR THE PROMOTION OF ECONOMIC SECURITY

After the council's first meeting, Kobayashi convened the Expert Meeting on the Legislation for the Promotion of Economic Security on 26 November 2021. Following an orientation session, breakout sessions were organised in each of the four areas (supply chain, core infrastructure, public and private partnership, and non-disclosure of patents) between the first and second meetings. These four

Prime Minister Kishida has introduced two major policies, 'creating the New NSS' and 'rule-making to bolster free and open global economic systems'

areas were selected after consideration of the political trends in the United States, China, and the EU (Cabinet Secretariat, 2021b). The following agendas and measures were listed as among European policy trends:

- A new transatlantic agenda for global change (in 2020).
- A framework for the screening of foreign direct investments into the Union in operation (in 2020);
- Implementing responsible research and innovation in Horizon 2020 (in 2014).
- The EU digital decade: A new set of digital targets for 2030 (in 2021).
- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, 'IT Security Act 2.0' in Germany (in May 2021).

In the second meeting on 28 December 2021, an open discussion was followed by presentations in breakout sessions in each area (Cabinet Secretariat, 2022). In this plenary meeting, the following European cases were introduced for consideration.

Referred cases and documents for discussion in the expert meeting:

- **Supply chain**: Updating the EU Industrial Strategy 2020 (in May 2021) (Cabinet Secretariat, 2021c)
- **Core infrastructure**: Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, 'IT Security Act 2.0' in Germany (in May 2021) (Cabinet Secretariat, 2021d)
- **Public and private partnership**: Funding the Advanced Research and Invention Agency (ARIA) in the UK in 2021. Funding the Federal Agency for Disruptive Innovation (SPRIN-D) in Germany in 2019 (Cabinet Secretariat, 2021e)
- **Non-disclosure of patents**: Comparing the UK and German non-disclosure systems of patents (Cabinet Secretariat, 2021f)

GENERAL POLICY COMMITTEE UNDER THE INFORMATION AND COMMUNICATION COUNCIL

Ryota Takeda, Minister of Internal Affairs and Communications in Suga's Cabinet, referred 'consideration of modalities of ICT policy with an eye on around 2030' to the Information and Communication Council on 30 September 2021. He gave the following reason for this inquiry:

'With the progress of digitalization due to the Covid-19 disasters, it is becoming more important to ensure the role of information and communication in people's lives and economic activities and the security associated with their use. In these circumstances, issues such as the growing presence of overseas platform operators and vendors in the content, service, terminal, and equipment layers, in particular, as well as supply chain risks in the information and communications field against the background of changes in the international situation such as tensions between the United States and China in recent years, have become apparent. Thus, in light of future trends in the information and communications market, technology, use, etc., I will consult on the future state of ICT policy from the perspective of realizing Society 5.0 and ensuring economic security, with an eye on around 2030.' (Minister of Internal Affairs and Communications, 2021)

He asked the Council to submit a partial report by June 2022, to include:

- Orientation towards taking measures to realise the Society 5.0 and to ensure economic security.

Europe has taken a different approach concerning AI, including its General Data Protection Regulation

- Response to matters immediately tackled among the measures referred in the previous clause.
- Other necessary issues.

These should be addressed in the light of future trends in the information and communications market, technology, use, and so forth with an eye on around 2030.

The Council decided that the General Policy Committee under the Info-communications Subcouncil was newly established for this purpose and should undertake this mission, with its first meeting taking place on 4 November 2021.[2] Dr Hiroyuki Morikawa, Professor at the University of Tokyo, became the chairman of the committee. The committee was asked to compile a draft report by March 2022 and to submit a concrete partial report in June 2022, after public consultation. Based on interviews with concerned mobile operators and manufacturers, the committee summarised the issues and challenges of measures to strengthen the Japanese ICT industry's international competitiveness with an eye on around 2030. They will examine two of them here:

- Measures for ensuring autonomy in strategic fields such as 5G and security.
- Comprehensive measures for strengthening research and development (R&D), standardisation, commercialisation, global deployment, and so forth in the field of Beyond 5G, quantum communications, and others. (Ministry of Internal Affairs and Communications, 2021)

The chairman invited four major mobile network operators – NTT, KDDI, Softbank, and Rakuten – and four major manufacturers – NEC, Fujitsu, Hitachi, and Toshiba – to attend the hearings.[3] There was a big difference in recognition of resiliency and its importance among these invitees, so that they seemed to have very different expectations of the governmental initiatives. There seems to be no direction to its industrial strategy.

At the committee's second meeting, Dr Satoru Tezuka pointed to the electronic Identification, Authentication and Signature Regulation (eIDAS), Data Free Flow with Trust (in 2019), and the 25th EU–Japan Summit on 17 July 2018 in Tokyo as good examples of the 'trust service' and its application in social security [4] and international mutual coordination.[5] Europeans benefit one-step forward from cross recognition of national eID schemes in the EU.

At the fourth meeting, Ryoji Mori, a lawyer, pointed to the EU's 'ePrivacy rules as a well-balanced case of privacy regulation compared to the traditional business custom, while they remain looser than the giant platformers' recent self-regulations.[6] The Center for Research and Development Strategy (CRDS), which was established in 2003 as an affiliated institution of the Japan Science and Technology Agency to independently carry out investigation and analysis and to make proposals on science, technology, and innovation policy, also presented a comparison of measures taken by the US, China, Europe, and Japan to advance R&D in AI and proposed a winning strategy for Japan.[7] According to this presentation, Europe promotes international study in AI, that is, 'AI for Europe', under the Horizon 2020/ Europe programme, as well as the AI strategies of each country. Moreover, Europe has taken a different approach from that of the United States, China, and the'GAFA (Google, Apple, Meta (Facebook), Amazon) in terms of international rule-making concerning AI, including its General Data Protection Regulation (GDPR), the ethical guideline for trustworthy AI, and the draft EU AI regulation. The

CRDS appreciated this European movement, which stresses the importance of ideological and ethical guidelines and tries to implement them from the point of view of 'trustworthy AI.', This European approach has weaknesses in initiatives for industrialisation of the AI of fourth generation compared to the United States and China, while it has strengths in rule-making processes.

SIMILARITIES BETWEEN JAPANESE ECONOMIC SECURITY AND EU DIGITAL STRATEGIC AUTONOMY

In Japan, the term 'digital autonomy' has not been used in the official debates. By contrast, the EU's concept of digital strategic autonomy already embraces economic security.

As mentioned in the second section, in June 2021 the Ministry of the Economy, Trade and Industry published the 'Semiconductor and Digital Industrial Strategy', which sets a goal of achieving digitalisation and greening at the same time. This strategy is similar to that of the EU's environmental policy in that digitalisation will help solve environmental problems.

In terms of policy, key materials such as semiconductors and key infrastructures should be under national or European control. As of June 2021, the key materials and infrastructures are limited to cutting-edge semiconductors and factories that produce them, data centres, and data cloud as well as related technologies. The range of these strategic materials and infrastructures will be greatly expanded and will include certain privacy data, communication networks and equipment, software, as well as public utilities such as transport networks and energy.

CHALLENGES AND DIRECTION OF JAPANESE POLICY

The Expert Meeting on the Legislation for the Promotion of Economic Security held plenary sessions on 19 January and 1 February 2022, in addition to eight sectional meetings, two in each field, and published its final proposal on 1 February 2022 (Expert Meeting on the Legislation for the Promotion of Economic Security, 2022).[8] The Cabinet Secretariat prepared the draft law based on this proposal and submitted to the Diet on 25 February 2022 after the Cabinet approval.[9] This date was fixed according to the Diet schedule and there is no relation between this submission and the Russian invasion of Ukraine.

The draft law shows only the orientation of regulations for economic security. The details will be legislated through modification of business acts, enforcement acts and orders in each sector. Thus, we can just guess what the government is aiming for by this legislation through the Expert Meeting's final proposal. Compared with discussions in the meetings, this proposal expressed moderate policies. Discussions in the initial stage as of December 2021, are referred to below.

As for the supply chain, although it is arguable what materials the government should seek to ensure stable supply through supply chain regulation, the following measures have been proposed:[10]

- Investigatory powers granted to the government to gain a clear understanding of supply chains.
- Mechanism for visualisation of bottlenecks.
- Incentives granted to the private sector to secure the upstream of supply chains.
- System design that allows quick decisions to be made.

As for the core infrastructure, the number of suppliers subjected to regulations should be minimized, in order to assure balance among national security, public safety, and freedom of economic activities, while not only efforts by the private sector but also a regulatory framework that allows the government to make comprehensive checks should be established through ex ante regulations.[11]

As for public–private partnerships in technologies, the government should play an active role in concentrated investment and in think tanks, including fostering human resources, through a conference body composed of industry, academia, and government which connects public needs to researchers and develops advanced technology.[12]

As for the non-disclosure of patents, complementary systems should be considered, such as duty of confidentiality, restriction of foreign application of the same patents, and compensation for loss. This non-disclosure system needs to be introduced as soon as possible.[13]

Keidanren (Japan Business Federation) appreciated the Expert Meeting on the Legislation for the Promotion of Economic Security's final proposal as a well-balanced one between freedom of economic activities, international rules and regulations as a whole, and supported this legislation on 9 February.

On the other hand, the General Policy Committee under the Information and Communication Council also organised hearings twice in January 2022 and meeting three times in February and March 2022.[14] As long as checking open documents and minutes, discussion in the Committee was directed to the orientation towards taking measures for to realising the Society 5.0 and was not referred to measures ensuring economic security. Although the reason for this change of direction is unknown, it is probable that the secretariat of the Council stopped to examine this issue until the detail of the draft law of the promotion of economic security is clear.

CONCLUDING REMARKS

Japanese economic security and the EU's digital strategic autonomy have many similarities. The term 'economic security' has been used ambiguously in Japanese national security policy and thus has no clear definition. The Japanese government has not defined the range of industries to be included under the (draft) law for economic security. The industrial sector is anxious about a possible expanded interpretation and excessive regulations to restrain economic activities in the private sector.

Recently, Yahoo! Japan, the second-most popular search engine service in Japan after Google, announced that it would withdraw from the European Economic Area and UK markets in April 2022 due to severe application of the GDPR. Japanese industry has begun to recognise the concept of digital strategic autonomy including the GDPR as troublesome. In Japanese 'economic security', the regulation of privacy may be defined more loosely than in the EU, whereas it may be more strict than current business customs in Japan. Discussions between the government and industry are continuing, and details regarding the plans for 'economic security' was made public through the Expert Meeting's final proposal in February 2022 and will be gradually decided after the draft law will be passed.

The Japanese have long believed that water and safety are free. Due to the COVID-19 pandemic, the Japanese gradually became more aware of issues of economic security. However, these issues are too complex for citizens to recognise as a familiar problem, and thus public opinion has not kept up with these debates. Young people enthusiastically

The Japanese industrial sector is anxious about a possible expanded interpretation and excessive regulations

embrace Korean culture. As a result, they are not concerned about the Japan–Korea geopolitical issues stemming from the economic confrontation between the United States and China. Concerns about the supply chain and digitalisation have become more widespread in the light of the lack of masks, alcohol-based sanitisers, domestic hot water systems, and more recently McDonalds' chips during the pandemic and delay of flat-rate benefits from the government. Young people have recently become aware of the serious risks of fake news and data circulation on the Internet in view of the suicide of a young woman due to anonymous accusation and information leakage of recruit.[15]

Thus, it has become a big issue in Japan how to make citizens recognise the importance of digital sovereignty and economic security.

NOTES

1. The iPhone series obtained around 50 per cent of the mobile terminal market in Japan according to Senoo (2021). In the traditional tie-in-sales model, the mobile operators made a commitment to the mobile terminal manufacturers to purchase a certain number of terminals instead of operators' initiative in their designs and prices. The mobile operators recovered these costs through communications fees.
2. Documents and minutes of the first meeting, https://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/joho_tsusin/sougou_seisaku/02tsushin01_04000631.html
3. Documents of each invitee are accessible from the following two URLs: https://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/joho_tsusin/sougou_seisaku/02tsushin01_04000640.html (mobile network operators), https://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/joho_tsusin/sougou_seisaku/02tsushin01_04000642.html (major manufacturers).
4. 'Trust service' means an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services.
5. Documents offered by Mori is accessible from the following URL; https://www.soumu.go.jp/main_content/000779166.pdf.
6. Documents offered by Dr. Tezuka is accessible from the following URL: https://www.soumu.go.jp/main_content/000783649.pdf.
7. Documents offered by CRDS is accessible from the following URL: https://www.soumu.go.jp/main_content/000783599.pdf.
8. The documents and minutes are accessible from the following URL: https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/index.html.
9. The text of the draft law and its deliberation progress are accessible from the following URLs: https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g20805010.htm and https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/keika/1DD5772.htm.
10. The document is accessible from the following URL: https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou3.pdf.
11. The document is accessible from the following URL: https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou6.pdf.
12. The document is accessible from the following URL: https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou9.pdf.
13. The document is accessible from the following URL: https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou12.pdf
14. Information of these meetings is accessible from the following URL: https://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/joho_tsusin/sougou_seisaku/index.html.
15. Several recruit information sites transmitted information on new graduates who continued to seek more desirable jobs through these sites, to the firms giving them a job offer.

REFERENCES

Cabinet Secretariat (2021a). *Meeting of Experts on Economic Security Legislation*, 26 November, https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai1/gijiyousi.pdf.

Cabinet Secretariat (2021b). Meeting of Experts on Economic Security Legislation, 26 November, https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai1/siryou3.pdf.

Cabinet Secretariat (2021c). *Meeting of Experts on Economic Security Legislation: Review Meeting on Supply Chain Resilience*, 9 December, https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou1.pdf.

Cabinet Secretariat (2021d). *Meeting of Experts on Economic Security Legislation: Review Meeting on Core Infrastructure*, 10 December, https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou4.pdf.

Cabinet Secretariat (2021e). Meeting of Experts on Economic Security Legislation: Review Meeting on Public–Private Technical Cooperation, 9 December, https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou7.pdf.
Cabinet Secretariat (2021f). Meeting of Experts on Economic Security Legislation: Review Meeting on Non-Publication of Patents, 6 December, https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou10.pdf.
Cabinet Secretariat (2022). *Second Meeting of Experts on Economic Security Legislation*, 28 February, https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/gijisidai.pdf.
Cabinet Secretariat (2013a). *National Security Strategy* https://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf.
Cabinet Secretariat (2013b). *National Security Strategy of Japan,* https://www.cas.go.jp/jp/siryou/131217anzenhoshou/pamphlet_jp_en.pdf.
Expert Meeting on the Legislation for the Promotion of Economic Security (2022). *Proposal for the Legislation for the Promotion of Economic Security, 1 February, https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai4/teigen.pdf.*
G20 Osaka Leaders' Declaration (2019). https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html.
Minister of Internal Affairs and Communications (2021). Consultation No.26 on ICT Policy towards 2030, 30 September, https://www.soumu.go.jp/main_content/000776637.pdf.
Ministry of Economy, Trade and Industry (2021). *Strategy for Semiconductors and the Digital Industry, 4 June,* https://www.meti.go.jp/press/2021/06/20210604008/20210603008-1.pdf; its English summary: https://www.meti.go.jp/english/press/2021/0604_005.html.
Ministry of Foreign Affairs of Japan (2019). *Background and Position of the Government of Japan Concerning the issue of former civilian workers from the Korean Peninsula (FACT SHEET), https://www.mofa.go.jp/press/release/press4e_002553.html, https://www.mofa.go.jp/mofaj/files/000499948.pdf.*
Ministry of Internal Affairs and Communications (2021). ICT Policy towards 2030, presentation document for the first meeting, 4 November, https://www.soumu.go.jp/main_content/000776641.pdf
Nakamura, N. (2020). 'Economic Security – for redefinition of the concept of the 'economic security' and construction of a consistent policy system', Rippou to Chosa [Legislation and Research], 428, pp.118–131,
https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/2020pdf/20201001118.pdf.
Nikkei (2021). 'What is European digital sovereignty? Semiconductors, data, aiming for independence', 10 March, https://www.nikkei.com/article/DGXZQOGR096QM0Z00C21A3000000/.
Prime Minister's Office of Japan (2021). *Diplomacy and security to protect the people*, https://www.kantei.go.jp/jp/headline/seisaku_kishida/diplomaticsecurity.html.
Prime Minister's Office of Japan (2021). *Economic Security Promotion Council*, 19 November, https://www.kantei.go.jp/jp/101_kishida/actions/202111/19keizaianpo.html.
Senoo, A. (2021). *Main smartphones, iPhone 45.7%, Android 47.0%: Teens and 20s Both Men and Women have iPhone Usage Rates Higher than Android Usage Rates*, Mobile Marketing Data Research Institute, 14 December, https://mmdlabo.jp/investigation/detail_2012.html.

This study, published by the European Liberal Forum and edited by Emeritus Professor Gerard Pogorel, Antonios Nestoras and Francesco Cappelletti, addresses a range of key concerns and opportunities associated with developing the EU's strategic digital autonomy, from research and education to strategic deployment of resources. The collection of up-to-date analytical papers written by leading experts provides food for reflection and a better understanding of what the EU needs to do to strengthen its position in the international digital domain of tomorrow. It argues that this is neither a protectionist nor an isolationist stance but a call for deeper cooperation and a robust consensual framework with partners and allies. A free market and better regulations for 'smart' policies are the only way to unleash the true potential of our digital future, To fit our digital tomorrow, we have to start today.

Daniel Kaddik, ELF Executive Director

ISBN 978-2-39067-033-9

9 782390 670339

Copyright 2022 / European Liberal Forum EUPF.

This publication was co-financed by the European Parliament. The European Parliament is not responsible for the content of this publication, or for any use that may be made of it.

liberalforum.eu