The Future of EU's Digital Decade: A Look at Open Strategic Autonomy in the Cloud and Beyond

Anushka Kaushik, Senior Research Fellow & Cyber Lead, GLOBSEC

www.globsec.org

GLOBSEC

Vajnorská 100/B
831 04 Bratislava
Slovakia

www.globsec.org

August 2024

GLOBSEC
IDEAS SHAPING THE WORLD

Executive summary

This paper explores cloud infrastructure and AI-augmented security in the context of the technological sovereignty debates and the new paradigm of open strategic autonomy in the European Union (EU).

The paper begins by analysing the conditions and debates that informed the EU's technological sovereignty doctrine with a special emphasis on the perspective of the Central and Eastern European countries on strategic autonomy at large and technological sovereignty, in particular. This is followed by an analysis of Open Strategic Autonomy and its digital dimensions. The next section looks at the benefits of cloud infrastructure and AI-augmented security for cybersecurity and broader Transatlantic ties – especially in the wake of global threats to cybersecurity, as exemplified by Russia's war in Ukraine. This is followed by an examination of the EU's efforts in these spheres and with reflections on the way forward for the EU.

Debates on technological sovereignty

Technological sovereignty is a contested term. The term suffers from definitional ambiguity, and variants such as digital sovereignty and data sovereignty have also emerged, sometimes being used interchangeably. Broadly, most contemporary definitions highlight the significance of autonomy over technology policies, standards, and structural processes. A key component emerging from the European Union (EU) perspective has been the importance of control over citizens' data – where it is stored, where it is processed, who monetarily benefits from hosting it, and how privacy can be safeguarded. Economic dependencies – primarily seen in the EU's strategic autonomy paradigm – in critical technologies are also motivators for inculcating technological sovereignty in public policy. While strategic autonomy and technological sovereignty, are mostly associated with the European discourse –elements of the concept have seen articulation in the United States' Buy America policy, India's Make in India, and China's economic self-sufficiency. There are several factors that drive and inform the EU's need to be technologically sovereign. The EU is falling behind the US and China in technological advancement. Further, its structural dependencies on these countries, particularly in digital supply chains, have significantly influenced its agenda.

While European Commission President Ursula von Der Leyen mentioned the importance of investing in technological sovereignty in her 2020 State of the Union speech, arguing that "digital is the make-or-break issue,"[1] discussions on technological sovereignty at the EU level had already begun prior to 2020. Thierry Breton, the European Commission for the Internal Market, in 2019, highlighted the need for establishing technological sovereignty as a precondition for digital and green transitions – also importantly recognising bridging the digital gap and involving all Europe's regions.[2]

Technological sovereignty is part of the broader EU campaign on strategic autonomy. While the initial focus of strategic autonomy was as an approach to autonomy in security and defence matters, it has increasingly emerged as a tool to defend European interests in a hostile geopolitical environment, especially during the years of Brexit, the Trump presidency, and the COVID-19 shock.[3] The 2021 Trade Policy Review of the European Commission defines strategic autonomy as the "EU's ability to make its own choices, shape the world around it via leadership and engagement, reflecting its strategic interests and values."[4] Thus, the scope of European strategic autonomy has increasingly widened to most policy areas. EU policies and legislations are developed with strategic autonomy considerations in mind – this is also visible in regulations on

1 "Strengthening the Soul of Our Union," European Commission, September 2021, **https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701**
2 QUESTIONNAIRE TO THE COMMISSIONER-DESIGNATE Thierry BRETON Commissioner-designate for the Internal Market, (European Commission, 2019), **https://www.europarl.europa.eu/resources/library/media/20191113RES66410/20191113RES66410.pdf**
3 Mario Damen, EU Strategic Autonomy 2013-2023: From Concept to Capacity (European Parliament, 2022), **https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI(2022)733589_EN.pdf**
4 European Commission, Trade Policy Review – An Open, Sustainable and Assertive Trade Policy (Brussels: European Commission, 2021), **https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52021DC0066**

technology and cybersecurity. Concerns have been expressed about the inclusion of technological sovereignty in policies and legislation, and the EU is choosing to create layers of rules and regulations over new technologies instead of improving socio-economic systems conducive to innovation and disruption.[5]

One of the more fundamental issues regarding technological sovereignty, however, is the variations in definition, approach, and method. The EU has reiterated certain principles like autonomy in strategic sectors, reducing dependencies on outside countries, and providing impetus to local industries, among others, but technological sovereignty does not have a common approach among all Member States. Member States seem to have differing approaches based on their history, size of economy, and geopolitical considerations, among others. Central and Eastern European (CEE) countries are a good example of this. Ivan Bartos, in a speech during the Czech Presidency conference on digital innovation in November 2022, emphasised that the EU's strategic autonomy must also remain open, stating that "Closing ourselves up is not the way forward."[6]

Technological sovereignty in the CEE region

While there are differing positions on specific EU policies and legislations within the region, the countries in the CEE do share some common apprehensions regarding the EU's strategic autonomy and technological sovereignty narratives. This was also clearly visible in CEE countries' reservations that defence ties with the US would get adversely affected – the fear was that if Europe set out on the road to full Strategic Autonomy, not only would that goal be left incomplete, but the quest would have deleterious consequences for Transatlantic relations, leaving the CEE region vulnerable.[7]

During the Trump Presidency, when EU strategic autonomy started to expand beyond defence to several policy areas, CEE countries were cautious about the potential dismantling of ties and relations that, for economic and security reasons, they could not afford to sacrifice. Security considerations for CEE countries tend to trump other factors, given their historical and geographical proximity to Russia. This vulnerability to Russian threats has shaped the bulk of their internal policies and influenced their positions on the global stage. This is also why countries of the region are among the most vocal supporters of transatlanticism.[8]

The economic argument underscores the guarded approach taken by CEE countries to technological sovereignty. Firstly, there is a recognition of the reliance of these countries on American technology companies. Secondly, on the question of creating European front-runners in the technological field, two constraints from the CEE are particularly significant – these front-runners would perhaps emerge from larger European countries, possibly with subsidies or exemptions from mergers, which could inhibit a productive climate for innovative businesses and SMEs, which will not thrive in an environment fixated on celebrating global champions.[9]

SMEs form the bulk of business enterprises in most CEE countries– in Poland, they made up 99.8% of all non-financial enterprises in 2021[10]. In Slovakia, SMEs account for 99.9% of firms, 72% of jobs, and 58% of the value added.[11] In 2021, there were roughly 1.23 million active enterprises in the Czech Republic, 99.86% of these firms were SMEs with less than 250 employees each.[12]

5 Damir Marusic and Kinga Brudzinska, PhD, The EU Strategic Autonomy: Central and Eastern European Perspectives, (Atlantic Council, GLOBSEC, 2021), **https://www.globsec.org/sites/default/files/2021-06/The-EU-Strategic-Autonomy-CEE-Perspectives-Report.pdf**

6 Lucie Schniderova, "EU strategic autonomy must remain open, says Czech deputy PM," Euractiv, November 2022, **https://www.euractiv.com/section/digital/news/eu-strategic-autonomy-must-remain-open-says-czech-deputy-pm/**

7 Damir Marusic and Kinga Brudzinska, PhD, The EU Strategic Autonomy: Central and Eastern European Perspectives, 8-9. **https://www.globsec.org/sites/default/files/2021-06/The-EU-Strategic-Autonomy-CEE-Perspectives-Report.pdf**

8 Ibid

9 Ibid

10 Financing SMEs and Entrepreneurs 2024: An OECD Scoreboard (OECD, 2024), **https://www.oecd.org/en/publications/financing-smes-and-entrepreneurs-2024_fa521246-en/full-report/component-10.html#section-d1e59401-6134a3be79**

11 "SME and Entrepreneurship Policy in the Slovak Republic," OECD, June 2021, **https://www.oecd.org/en/publications/sme-and-entrepreneurship-policy-in-the-slovak-republic_9097a251-en/full-report/component-5.html#section-d1e2293**

12 Financing SMEs and Enterpreneurs 2024: An OECD Scoreboard (OECD, 2024), **https://www.oecd-ilibrary.org/docserver/fa521246-en.pdf?expires=1724066596&id=id&accname=guest&checksum=18F90E49887B276856A3025D7878AFBF**

Digital transformation indicators also indicate the extent to which CEE countries lag in key metrics - in that context, there is apprehension behind an overemphasis on autonomy and independence at the cost of economic and technological relations with the US. In 2021 SMEs made up 99.8% of all non-financial enterprises in Poland, numbering 2 352.2 thousand SMEs in total.

Experts also point to strong historical factors that drive CEE's guarded approach to strategic autonomy narrative - the interconnectedness with the rest of the world that led to CEE's successful transformation following the fall of the Iron Curtain and the internet, new technologies, trade flows are all representative of the introduction of freedoms that were denied in the region.[13]

Additionally, the role of the CEE region in the larger technological sovereignty discourse is yet to be adequately determined – what this means for CEE countries with respect to their position in the EU and whether it will serve them or increase existing divisions remains to be seen.

Emergence of Open Strategic Autonomy and its digital dimensions

The Open Strategic Autonomy (OSA) movement has emerged as a counterpoint to the prevailing model of digital sovereignty which emphasises tighter control over digital infrastructure and a focus on reducing dependency on non-European technology. It offers a different vision—one that seeks to balance sovereignty with openness. The European Commission has defined OSA as "cooperating multilaterally wherever we can, acting autonomously wherever we must."[14] A joint Spain-Netherlands non-paper on strategic autonomy while preserving an open economy was an important step toward the conception of the OSA. The non-paper posited that strategic autonomy did not mean isolation or retreat but, rather, a reformulation of how to understand sovereignty, advancing towards operational sovereignty, i.e., the capacity to promote an agenda of its own.[15] In the European Commission's Trade Policy in February 2021, the OSA was a central feature with Executive Vice President for Trade Vladis Dombrovskis stating that "We are pursuing a course that is open, strategic and assertive, emphasising the EU's ability to make its own choices and shape the world around it through leadership and engagement, reflecting our strategic interests and values."[16]

OSA was one of the main topics at the informal meeting of EU heads of state or government in Granada during the Spanish Presidency, with the aim of moving towards a more competitive and resilient EU in the face of global technological and geopolitical transformations. According to the Spanish government, OSA is emerging as a response to threats posed by excessive dependence on third countries without falling into protectionism or renouncing the European values of competitiveness, sustainability, and cohesion.

The quest of the EU OSA is emerging as a necessary response to the rapidly changing geopolitical situation as well as a response to the gradual erosion of the global multilateral political and economic order.[17] Open Strategic Autonomy might sound like a paradox, but openness and autonomy are not incompatible concepts. There is, however, less consensus on exactly what OSA entails. Avoiding protectionism and the impression of protectionism, as well as strengthening alliances with like-minded partners, have been offered as some principles to follow to increase the "open" component of strategic autonomy.[18]

In July 2023, a joint non-paper signed by Belgium, Finland, the Netherlands, Portugal, and Slovakia

13 Damir Marusic and Kinga Brudzinska, PhD, The EU Strategic Autonomy: Central and Eastern European Perspectives. **https://www.globsec.org/sites/default/files/2021-06/The-EU-Strategic-Autonomy-CEE-Perspectives-Report.pdf**

14 "Open Strategic Autonomy: Ensuring European Citizens' Welfare in the New Global Order," National Office of Foresight & Strategy, accessed in August 2024, **https://futuros.gob.es/en/our-work/OSA**

15 Spain-Netherlands Non-Paper on Strategic Autonomy While Preserving an Open Economy (Open Overheid), **https://open.overheid.nl/documenten/ronl-fd3bbc94-f598-45b3-abbd-75bfd5b18b97/pdf**

16 European Commission, "Commission Sets Course for an Open, Sustainable and Assertive EU Trade Policy," European Commission, February 2021, **https://ec.europa.eu/commission/presscorner/detail/en/ip_21_644**

17 Group of the Progressive Alliance of Socialists & Democrats in the European Parliament, S&D Group Strategy Paper on European Union Open Strategic Autonomy (Brussels: S&D, 2023), **https://www.socialistsanddemocrats.eu/sites/default/files/2023-02/S%26D_Group_Strategy_Paper_on_European_Union_Open_Strategic_Autonomy_230206_0.pdf**

18 Maaike Okano-Heijmans, Open Strategic Autonomy: The Digital Dimension (Clingendael, 2023), **https://www.clingendael.org/sites/default/files/2023-01/Open_strategic_autonomy_.pdf**

proposed a model for OSA on three pillars – reinforcing the EU's political-economic foundations, mitigating high-risk strategic dependencies, and expanding the EU's geopolitical capacity.[19] Importantly, the non-paper also called on the EU to enhance its capacity for geopolitical action by improving decision-making in foreign policy and a coordinated governance structure, with an executive vice-president overseeing OSA and inter-DG coordination to ensure the EU's global competitiveness and resilience.

In the digital domain, the Netherlands has been at the forefront of defining the contours of the OSA. According to a paper published by the Dutch government in October 2023, the digital OSA is reducing reliance on proprietary software and strengthening digital autonomy with an emphasis on open-source solutions to promote responsible and secure technology use within the country and Europe.[20] The Dutch government also recognized the importance of balancing innovation and citizens' rights. The paper highlights a plan for the potential creation of a Digital Sovereignty Fund and adjustments in procurement policies to facilitate open-source adoption. The agenda emphasizes cooperation with countries and partners sharing a vision for a secure and open digital environment, and collaboration involves initiatives like the European Digital Infrastructure Consortium and knowledge networks led by the European Commission's Open Source Program Office.

More recently, the government of the Netherlands published its vision on generative Artificial Intelligence, calling for a value-driven approach which offers opportunities for innovation based on safe use and equitable principles.[21] There is also a recognition that the Dutch government is largely dependent on language models from non-European countries and that this situation must change in the future. According to Robbert Dijkgraaf, Minister for Education, Culture, and Science, "The essence is to develop and to retain AI talent, to allow us to develop forms of generative AI that satisfy the standards and values of Europe. Therein lies the added value for Europe's digital open strategic autonomy."[22] The extent to which this approach is altered given the results of the November general elections and the Partij voor de Vrijheid (PVV) coming to power remains to be seen.

The basic tenet of OSA in the digital domain is the provision of an open and interoperable digital infrastructure that not only delivers economic and security benefits at a global scale but also adequately addresses the imperative of sovereignty needs. While there is no agreed-upon actionable framework of OSA yet, its broader goals are apparent - supporting EU innovation by providing access to secure, high-performance infrastructure, ensuring protection of sensitive data, and safe and secure data portability.

A look at Cloud infrastructure and AI-augmented security

The EU's Digital Decade - a strategic plan designed to achieve digital transformation across the continent by 2030 – sets certain targets for EU companies using cloud, AI, and Big Data, recognising the importance of cloud services in enabling the digital transformation of businesses, public services, and industries across Europe.

Cloud infrastructure has gained significant importance in the last few years. Cloud services offer tremendous benefits to businesses, especially to SMEs. Cloud infrastructure ensures scalability – this means businesses can address surges in demand and scale up or down their storage needs based on this variable demand, offering flexibility. Secondly - and relevant for SMEs - is the cost optimisation offered by cloud services, as businesses do not need to purchase expensive infrastructure and make use of the pay-as-you-go model. Data stored on the cloud is generally also more secure – owing

19 Belgium et al., Joint Non-paper on Open Strategic Autonomy of the EU (Open Overheid), **https://open.overheid.nl/documenten/5f3a6437-92b3-41bc-835a-e4d803ee6f6b/file**
20 Axel Thévenet, "Dutch Agenda for Digital Open Strategic Autonomy," European Commission, November 2023, **llection/open-source-observatory-osor/news/dutch-digital-open-strategic-autonomy**
21 "Dutch Government Presents Vision on Generative AI," Government of the Netherlands, January 2024, **https://www.government.nl/latest/news/2024/01/18/dutch-government-dutch-government-presents-vision-on-generative-ai**
22 Ibid

to rigorous vulnerability and patch management, multiple layers of encryption, continuous monitoring, and automated backups. More broadly, Cloud enables defence of the overall ecosystem by leveraging individual threat observations in a swift manner and ensuring a consistent and scalable level of protection.

Cloud infrastructure is also important for Transatlantic economic ties. With respect to ICT-enabled services, the US and EU are each other's most important commercial partners – Transatlantic data flows account for half of US flows and over one-half of EU's.[23] Both the US and the EU are deeply connected to the internet, and as a result, the largest intercontinental internet data flow is across the Atlantic. These data flows are now the backbone of the transatlantic economy, both for direct e-commerce purchases of goods and services and to facilitate virtually all business relations between the US and EU.[24]

The cyber threat landscape is evolving rapidly, leaving businesses and consumers particularly susceptible to attacks. There is an uptick in the targeting of third-party vendors and suppliers, compromising businesses' systems indirectly along with increased sophistication of ransomware attacks. Relentless cyber operations are becoming a norm alongside kinetic warfare. Russian threat actors – both known and with suspected links to the government – have been carrying out a combination of cyber-attacks, including deploying destructive malware and espionage activities since the invasion of Ukraine in 2022.[25] These include Distributed Denial of Service (DDoS) attacks, wiper malware, faux ransomware, and information stealers, among others. Criminal and state-sponsored threat actors are increasingly professionalising their operations and programs, becoming more sophisticated and organised in their approaches. Threat actor groups are developing tactics that regularly evade standard security controls, making traditional defence mechanisms less effective.

In the current scenario, the cybersecurity advantages of cloud infrastructure are crucial for businesses and consumers, as well as for safeguarding a nation's strategic assets. For example, a few days before the invasion, on February 17, 2022, Ukraine authorised migrating national data to the public cloud from servers operating entirely within the country – which proved to be significant as it enabled critical data protection. This has since played a considerable role in the provision of services to Ukrainian citizens by allowing them secure access to national databases.[26]

With the advent of Artificial Intelligence (AI), there has been much debate on its benefits for defenders versus attackers. Malicious use of AI includes but is not limited to using Generative AI for deception/phishing, spreading misinformation and fake news by making the content look more authentic, and increasing hacking-based crimes. Attackers can use AI to create fake news, generate interactive fake phone calls, and produce deepfake images and videos. This added complexity can be challenging to manage, primarily as defenders suffer from resource and attention asymmetries. AI could also help attackers find new ways to exploit software or compromise devices.

While there has been a burgeoning emphasis on the malicious use of AI, significant strides have been made in AI-augmented security. It has allowed defenders to optimise processes – through learning (improving performance on its own in dynamic cybersecurity environments), speed (ability to rapidly evolve defences), and scale (analysing large data sets).[27] Additionally, Security research posits that as AI becomes more advanced, the tasks it can handle will grow in usefulness and complexity. This could have a significant impact on cybersecurity, where defenders are already overwhelmed by the sheer number of tasks and the difficulty of some of them – AI can help automate several repetitive cybersecurity tasks that burden

23 Daniel S. Hamilton, Forging a Transatlantic Technology Alliance: Opportunities and Challenges Related to ICT and Cloud (Transatlantic, 2021), **https://www.transatlantic.org/wp-content/uploads/2022/03/TTC-ICT-and-Cloud-January-2022.pdf**

24 Peter Chase et al., Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies (Belgium: European Parliament, 2016), **https://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU(2016)535006_EN.pdf**

25 Anushka Kaushik, The War on Ukraine: A Look at (Underemphasised) Russian Cyber Operations (Globsec, 2023), **https://www.globsec.org/what-we-do/publications/war-ukraine-look-underemphasised-russian-cyber-operations**

26 Michael Chertoff and Anushka Kaushik, "The unheralded success story of Ukraine's cyber-defences," Euobserver, March 2023, **https://euobserver.com/opinion/156766**

27 Haiman Wong, Amy Chang and Brandon Pugh, "The Transformative Role of AI in Cybersecurity: Understanding Current Applications and Benefits," R Street Institute, January 2024, **https://www.rstreet.org/commentary/the-transformative-role-of-ai-in-cybersecurity-understanding-current-applications-and-benefits/**

human analysts. AI could analyse complex datasets much faster. Industry research has emphasised two major paradigmatic shifts in cybersecurity brought on by AI: helping to manage the complexity that creates digital vulnerabilities and empowering all users to be better defenders of digital technology, with the potential to move from assistive to fully autonomous security systems. With a shortage of cybersecurity professionals, this could be particularly effective for EU Member States – allowing resource-constrained organisations to do more with less.

Where the EU stands

Cloud infrastructure

With respect to cloud services in the EU, the principles that govern technological sovereignty have also been extended to cloud infrastructure and services. Germany's Minister of Economy Peter Altmaier argued that Europe was losing part of its sovereignty when firms and agencies must store their data on US-based cloud platforms.[28] European Commission's 2020 'Communication on a European Strategy for Data' also stated the need to reduce technological dependencies in cloud infrastructure and services as a priority.[29] EU's Digital Decade initiative, as part of its 'Digital transformation for businesses' goal, set a target of 75% of EU companies using Cloud, AI, or Big Data[30].

EU Member States have also laudably experimented with developing their own cloud services – the most notable among these is Gaia-X, driven by the efforts of France and Germany. The project aimed to use open technical standards, shared data privacy and security standards, allowing businesses and customers to move data freely within the network. These features, along with the scale of the investment (10 million EUR), had positioned Gaia-X to be a success, but many argue that it is a catching-up operation that has to match the substantial existing investments of foreign cloud platforms, with many elements that still need to be clarified - such as migration, hybrid cloud, and participation of non-European suppliers.[31]

Furthermore, there were also concerns that while Gaia-X aims to promote European values, openness, and collaboration, major technology corporations influenced the project, potentially diverting funding away from fostering European technological competence. The primary risk identified was "corporate capture," where Gaia-X's founding members, despite emphasizing independence and European values, were reportedly relying heavily on non-EU technologies like OpenStack and Kubernetes, raising concerns about the project's true commitment to European sovereignty.[32] Similarly, in 2018, two state-owned Polish companies set up a project called State Cloud which was meant to provide cloud computing services for the Polish market, with ambitions to enlarge scale in CEE.[33]

Local players in the European market are lagging in market footprint – while European providers have more than doubled their cloud revenues since 2017, their market share in Europe has declined from 27% to under 16%, whereas Amazon Web Services (AWS), Microsoft Azure and Google Cloud now account for 69%[34]. In addition to protecting data privacy of EU citizens, regulating who controls it, and controlling which entities monetarily benefit from it, this is a strong motivator for the EU to facilitate the growth and competitiveness of European cloud service providers. The EU, therefore, has legitimate technical, economic, and value-based reasons to focus its efforts on developing its cloud market.

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

29 European Commission, "A European Strategy for data," European Commission, 2024, **https://digital-strategy.ec.europa.eu/en/policies/strategy-data#:~:text=The%20open%20public%20consultation%20on,them%2C%20focusing%20on%20quantitative%20aspects**

30 "Europe's d: Digital Targets for 2030," European Commission, **https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en**

31 Paul Timmers ad Freddy Dezeure, Strategic Autonomy and Cybersecurity in the Netherlands (Cyber Security Council, 2021), **https://www.freddydezeure.eu/3-strategic-autonomy-and-cybersecurity-in-the-netherlands**

32 Oliver Noyan, "Cracks Appear as Gaia-X Celebrates its Progress," Euractiv, November 2021, **https://www.euractiv.com/section/digital/news/cracks-appear-as-gaia-x-celebrates-its-progress/**

33 Krzysztof Izdebski, "Partners or Competitors? Central and Eastern Europe's Technological Sovereignty," Visegrad / Insight, January 2021, **https://visegradinsight.eu/partners-or-competitors-sovereignty/**

34 Daniel S. Hamilton, Forging a Transatlantic Technology Alliance: Opportunities and Challenges Related to ICT and Cloud. **https://www.transatlantic.org/wp-content/uploads/2022/03/TTC-ICT-and-Cloud-January-2022.pdf**

However, the success of the EU in developing cloud infrastructure appears to be limited. In the current scenario, Europe's accelerating demand for cloud services, especially from certain innovators who are higher up the technology stack and require reliable services, may not be met purely through domestic means. It is in Europe's interest that it explores the next generation technology, available globally, to reap the benefits as well as develop a globally relevant technological ecosystem.

The debate surrounding the European Commission's proposed European Cybersecurity Certification Scheme for Cloud Services (EUCS) scheme highlights the broader tension between the OSA model and 'closed' digital sovereignty – with advocates of the former favouring swift access to IaaS capabilities, provided there are safeguards in place to protect EU data. Further in the wake of Russian threat, its incumbent that Europe collaborate with established international agencies to ensure potential benefits of cloud based AI security features.

The European Commission had tasked ENISA (the EU Cybersecurity Agency) to support the preparation of a candidate EU cybersecurity certification scheme on cloud services, in the context of the EU Cybersecurity Act. The candidate EUCS scheme investigates the certification of the cybersecurity of cloud services. In terms of local certification mechanisms for cloud services, France's SecNumCloud and Germany's The Cloud Computing Compliance Controls Catalogue (C5) stand out. However, the EUCS will be a scheme harmonized at the European level with quality guarantees using third-party assessment by accredited bodies and supervision by national authorities.[35] One of the main aims – which aligns with the EU's core values of transparency and openness – is to allow cloud service customers the opportunity to make informed decisions about cloud services and benefit from the evidence provided with certified cloud services.

The EU cloud market has also seen a burgeoning rise – in 2020, it was estimated at 53.9 billion euros – by 2025, it is expected to grow to 135.9 billion.[36] Further, European companies are increasingly adopting the cloud, with just 18 percent of all European companies using cloud services in 2014, compared to 41 percent in 2021.[37] The European Commission has set a target of 75 percent of EU companies using cloud by 2030,[38] with current adoption rates in SMEs at a mere 40%.

With the expanding cloud market in Europe and the European Commission's goal to increase adoption, the EUCS is timely. At its core, the EUCS is a crucial undertaking, enabling governments and consumers to make informed and reliable choices based on third-party certification across the 27 EU Member States. Creating a common technical framework to verify that every cloud service provider will be adhering to one framework serves to further competitiveness, the standard of cybersecurity, facilitating customer adoption, and inculcation of best practices. Further, frameworks can also serve as a baseline for evaluation - providing a useful benchmark that cloud customers can use to evaluate providers or compare security practices between providers.[39]

Concerns were expressed about specific aspects of the EUCS, eliciting pushback from industry associations in both the US and the EU. Most concerns were centred around what many were referring to as "digital sovereignty requirements," which were added in successive drafts. These stipulations included data localisation requirements, restrictions on foreign minority and majority ownership, and local staff requirements, with the most opposition to the provision necessitating companies to have their headquarters in the EU to apply for the highest assurance level within the framework.

According to the latest draft of the scheme, the bulk of these requirements have been waived

35 European Union Agency for Cybersecurity, EUCS – Cloud Services Scheme (European Union Agency for Cybersecurity, 2020), **https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme**

36 Justus Haucap and European Cloud Alliance, "Cloud computing matters to Europe: decision-makers should help it grow," Euractiv, July 2023, **https://www.euractiv.com/section/digital/opinion/cloud-computing-matters-to-europe-decision-makers-should-help-it-grow/**

37 Ibid

38 European Commission, "Questions & Answers on the First report on the State of the Digital Decade," European Commission, September 2023, **https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4620#:~:text=Under%20current%20trends,%20and%20without,and/or%20AI%20by%202030.**

39 Ed Moyle, "What is a cloud security framework? A complete guide," TechTarget, June 2024, **https://www.techtarget.com/searchsecurity/tip/What-are-cloud-security-frameworks-and-how-are-they-useful**

off, with cloud vendors only obliged to provide information about the location of the storage and processing of their customers' data and applicable laws.[40] However, the debate on sovereignty requirements is far from over – the final decision on the EUCS keeps getting delayed as advocates for the requirements continue to support their inclusion[41]. The impact of the shift to another EC mandate on these advanced negotiations remains to be seen.

In the wake of the Russian threat, it could be beneficial for the EU to explore partnerships with global cloud providers to leverage the potential benefits of cloud-based AI security features.

Artificial Intelligence

The EU, recognizing the critical role of AI in enhancing European innovation and security, is striving to take a leading position in global AI governance. The 2022 Strategic Compass highlighted the EU's ambition to become a global leader in AI by decreasing strategic dependencies on external actors – and thus, the EU sees AI as an area where it can bolster technological sovereignty.[42]

The EU AI Act, on which the European Parliament and European Commission reached an agreement in 2023, champions a risk-based approach and emphasises the responsible development of AI. AI systems are classified into several risk categories, and different degrees of regulation are applicable based on the risk level. There are four levels - unacceptable risk, high risk, transparency risk, and minimal risk. Prohibited AI practices have also been identified in the Act. These include the use of manipulative techniques where AI systems employ subliminal, deceptive, or manipulative methods that distort behaviour or impair informed decision-making, leading to significant harm. Among others, AI systems that exploit vulnerabilities due to age, disability, or socio-economic conditions, resulting in substantial harm, are also restricted.

EU's risk-driven approach is commendable, given the emphasis on responsible use and development. However, significant challenges remain: Europe spends less on AI research and development than the US, there is a concerted lack of large technology companies emerging out of Europe, and there is no unified approach to AI development among Member States. The extent to which the EU can contribute and shape the development of AI from a technological perspective remains to be seen. There have been criticisms that the EU is attempting to overcome the gap of lagging behind by implementing protectionist regulatory tools[43] and that the EU's AI sovereignty is underspecified and open to interpretations.[44] The extent to which the EU's goals of being a normative power align with its use of digital sovereignty and strategic autonomy is also questioned.[45]

The EU must leverage its proven collaborative ecosystem, i.e., establishing partnerships with academia and the private sector, as well as its scientific excellence and linguistic and cultural diversity, to take the lead in AI development.

Open strategic autonomy with AI in the EU context would balance independence in AI development and governance with active collaboration and engagement with global partners.

40 Foo Yun Chee, "EU drops sovereignty requirements in cybersecurity certification scheme, document shows," Reuters, April 2024, **https://www.reuters.com/technology/eu-drops-sovereignty-requirements-cybersecurity-certification-scheme-document-2024-04-03/**

41 "EUCS: Controversial Sovereignty Issues Continue to Drive Debate for Cloud Services," Hogan Lowells, June 2024, **https://www.engage.hoganlovells.com/knowledgeservices/news/eucs-controversial-data-sovereignty-issues-continue-to-drive-debate-around-the-eu-certification-scheme-for-cloud-services#:~:text=The%20latest%20EUCS%20draft%20in%20Q1%202024%20has%20not%20been,not%20necessarily%20a%20closed%20issue**

42 Raluca Csernatoni, Charting the Geopolitics and European Governance of Artificial Intelligence (Carnegie Europe, 2024), **https://carnegie-production-assets.s3.amazonaws.com/static/files/Csernatoni_-_Governance_AI-1.pdf**

43 Andrea Calderaro and Stella Blumfelde, "Artificial Intelligence and EU Security: The False Promise of Digital Sovereignty," European Security, vol. 31, no. 3 (July 2022): pp. 415-34, 10.1080/09662839.2022.2101885

44 Daniel Mügge, "EU AI sovereignty: for whom, to what end, and to whose benefit?" Journal of European Public Policy (February 2024): pp. 1-26, 10.1080/13501763.2024.2318475,

45 Dennis Broeders, Fabio Cristiano and Monica Kaminska, "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions," Journal of Common Market Studies, Vol. 61, no. 5, (February 2023): pp. 1261-1280, 10.1111/jcms.13462,

Way forward for the EU

The EU is at a critical point in its Digital Decade. While it is taking the lead in regulatory frameworks and championing its normative approach to emerging technologies, the EU needs to do more to leverage its core strengths and provide conditions for local players to thrive. Given the dynamic geopolitical environment, the EU has to balance its important strategic autonomy and technological sovereignty goals with providing its citizens with the highest levels of cybersecurity. Open Strategic Autonomy (OSA) can be a guiding principle for the European Union, aimed at ensuring that the EU has the capacity to make independent decisions and act independently in areas critical to its interests while maintaining open trade and cooperation.

In the context of cloud and AI technologies, the EU can take several strategic steps to align with this principle:

1. ***Establish a uniform vision of Open Strategic Autonomy principles*** *among Member States which can then be applied to different frameworks on emerging technologies. Implement these principles across different policy areas, such as AI, cloud computing, and cybersecurity, ensuring that OSA is consistently applied. This would complement the suggestion of some Member States for the EU to develop a comprehensive Technology Strategy.*
2. ***Emphasise a multidisciplinary approach to formulating an OSA framework****, given the various interconnected policy areas. OSA touches on a wide range of policy areas, including digital infrastructure, cybersecurity, industrial policy, trade, and education. The EU must include experts from diverse fields, such as technology, law, economics, international relations, and ethics, in the formulation of the OSA framework. This would help in understanding the complex interplay between different domains and in creating policies that are robust and well-rounded.*
3. ***Ensure that the OSA framework is adaptable*** *and can be applied to new and emerging technologies. This requires ongoing dialogue between technologists and policymakers to anticipate future challenges and opportunities in areas like AI, quantum computing, and digital sovereignty.*
4. ***Provide funding and incentives for European cloud service providers*** *– via grants and investments - to grow and innovate, ensuring that European businesses have access to competitive, high-quality cloud services within the EU. While supporting European providers, make use of sovereign controls offered by global cloud providers to ensure that EU data is protected from unauthorised access. This hybrid approach could provide businesses with flexibility while maintaining high standards of data security.*
5. ***Ensure that smaller European Member States, especially those in proximity to Russia and dealing with a unique set of challenges, are adequately supported in their cybersecurity goals*** *by creating conditions that facilitate access to robust security capabilities and cloud services. They should not suffer disproportionately in the EU's technological sovereignty ambitions.*
6. ***Provide access to secure and high-performance digital infrastructure such as AI-enabled cloud services*** *to support European innovation and facilitate their competition with global players.*
7. ***Target efforts on capacity building for cloud infrastructure*** *– this means enhancing the skills, knowledge, resources, and capabilities necessary to design, develop, implement, manage, and optimize cloud-based technologies effectively. Given the increase in regulatory compliance on critical ICT-third party providers – for example, the Digital Operational Resilience Act (DORA) which will be effective in 2025 – this capacity development should also include the regulatory side.*

8. ***Foster partnerships between the public sector and private companies to drive innovation in AI and cloud technologies**, ensuring that public sector needs are met while supporting the growth of European companies.*

9. ***Work towards the harmonisation of national regulations related to AI and cloud technologies** across EU member states, reducing regulatory fragmentation and creating a more cohesive internal market.*

Conclusion

The EU stands at a pivotal juncture in its Digital Decade, and its drive to reduce dependency on external actors and foster local innovation is evident. The EU's efforts to develop its cloud infrastructure and champion a risk-based approach to AI are crucial steps in this direction. However, challenges include but are not limited to differing resources among Member States, the dominance of non-European tech giants, and the need for greater investment in research and development. Achieving a balance between autonomy and openness could greatly determine its digital security in the future – especially given the rapidly evolving nature of cyber threats.

There are certain steps that the EU can take to advance OSA effectively, such as establishing a uniform vision of OSA principles among Member States, adopting a multidisciplinary approach in formulating the principles, and thus, creating a framework that is adaptable and responsive to new and emerging technologies. The EU should prioritise providing access to secure and high-performance digital infrastructure, such as AI-enabled cloud services, to support European innovation and enhance competitiveness with global players. While supporting European players, businesses can make use of sovereign controls offered by global cloud providers. This hybrid approach can provide businesses with the flexibility they need while maintaining stringent data security standards to protect EU data from unauthorized access.

Particular attention should be paid to smaller European Member States, especially those with proximity to Russia and facing unique cybersecurity challenges. It is crucial that these Member States do not suffer disproportionately in the EU's pursuit of technological sovereignty. The EU's commitment to open strategic autonomy will be tested by its ability to reconcile the need for independence with the benefits of global collaboration.

Reference list

Belgium, Finland, the Netherlands, Portugal, and Slovakia. "Joint Non-paper on Open Strategic Autonomy of the EU." Open Overheid. Accessed March 10, 2024. **https://open.overheid.nl/documenten/5f3a6437-92b3-41bc-835a-e4d803ee6f6b/file**

Broeders, Dennis, Fabio Cristiano, and Monica Kaminska. "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions." JCMS Journal of Common Market Studies 61, no. 5 (February 28, 2023): 1261–80. **https://doi.org/10.1111/jcms.13462**

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

Calderaro, Andrea, and Stella Blumfelde. "Artificial Intelligence and EU Security: The False Promise of Digital Sovereignty." European Security 31, no. 3 (July 3, 2022): 415–34. **https://doi.org/10.1080/09662839.2022.2101885**.

Chase, Peter, Sudha David-Wilp, Tim Ridout, and Policy Department, Directorate-General for External Policies. "Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies." Policy Department, Directorate-General for External Policies. 2016. Reprint, European Union, 2016. **https://doi.org/10.2861/173823**.

Chee, Foo Yun. "EU Drops Sovereignty Requirements in Cybersecurity Certification Scheme, Document Shows." Reuters, April 3, 2024. **https://www.reuters.com/technology/eu-drops-sovereignty-requirements-cybersecurity-certification-scheme-document-2024-04-03/**.

Chertoff, Michael, and Anushka Kaushik. "The Unheralded Success Story of Ukraine's Cyber-defences." EUobserver, March 1, 2023. **https://euobserver.com/opinion/156766**.

European Commission. "Commission Sets Course for an Open, Sustainable and Assertive EU Trade Policy," February 18, 2021. **https://ec.europa.eu/commission/presscorner/detail/en/ip_21_644**.

Csernatoni, Raluca. "Charting the Geopolitics and European Governance of Artificial Intelligence." Carnegie. Carnegie Europe, March 2024. **https://carnegie-production-assets.s3.amazonaws.com/static/files/Csernatoni_-_Governance_AI-1.pdf**.

Damen, Mario. "EU Strategic Autonomy 2013-2023: From Concept to Capacity." Report. EU Strategic Autonomy Monitor, July 2022. **https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI(2022)733589_EN.pdf**.

Government of the Netherlands. "Dutch Government Presents Vision on Generative AI," January 18, 2024. **https://www.government.nl/latest/news/2024/01/18/dutch-government-dutch-government-presents-vision-on-generative-ai**.

Hogan Lowells. "EUCS: Controversial Sovereignty Issues Continue to Drive Debate for Cloud Services," June 12, 2024. **https://www.engage.hoganlovells.com/knowledgeservices/news/eucs-controversial-data-sovereignty-issues-continue-to-drive-debate-around-the-eu-certification-scheme-for-cloud-services#:~:text=The%20latest%20EUCS%20draft%20in%20Q1%202024%20has%20not%20been,not%20necessarily%20a%20closed%20issue**.

European Commission. "A European Strategy for Data," 2024. **https://digital-strategy.ec.europa.eu/en/policies/strategy-data#:~:text=The%20open%20public%20consultation%20on,them%2C%20focusing%20on%20quantitative%20aspects**

European Union Agency for Cybersecurity. “EUCS – Cloud Services Scheme.” ENISA, EUROPA.EU, December 22, 2020. **https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme**.

European Commission. “Europe’s Digital Decade: Digital Targets for 2030,” n.d. **https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en**.

Financing SMEs and Entrepreneurs. “Financing SMEs and Entrepreneurs 2024.” Oecd.Org. OECD, March 13, 2024. **https://www.oecd.org/en/publications/financing-smes-and-entrepreneurs-2024_fa521246-en/full-report/component-10.html#section-d1e59401-6134a3be79**.

“Financing SMEs and Entrepreneurs 2024: an OECD Scoreboard.” Oecd-Ilibrary.Org. OECD, 2024. **https://www.oecd-ilibrary.org/docserver/fa521246-en.pdf?expires=1724053662&id=id&accname=guest&checksum=6601A2C3300398E3248B84AE2122B9C4**.

Hamilton, Daniel S. “Forging a Transatlantic Technology Alliance: Opportunities and Challenges Related to ICT and Cloud.” Transaltlantic, September 2021. **https://www.transatlantic.org/wp-content/uploads/2022/03/TTC-ICT-and-Cloud-January-2022.pdf**.

Haucap, Justus and European Cloud Alliance. “Cloud Computing Matters to Europe: Decision-makers Should Help It Grow.” www.euractiv.com, October 17, 2022. **https://www.euractiv.com/section/digital/opinion/cloud-computing-matters-to-europe-decision-makers-should-help-it-grow/**.

Iturbe, Eider, Erkuden Rios, Angel Rego, and Nerea Toledo. “Artificial Intelligence for next generation cybersecurity: The AI4CYBER framework.” ARES ’23: Proceedings of the 18th International Conference on Availability, Reliability and Security, no. 133 (August 29, 2023): 1–8. **https://doi.org/10.1145/3600160.3605051**.

Izdebski, Krzysztof. “Partners or Competitors?” Visegrad Insight, January 20, 2021. **https://visegradinsight.eu/partners-or-competitors-sovereignty/**.

Kaushik, Anushka. “The War on Ukraine: A Look at (Underemphasised) Russian Cyber Operations,” n.d. **https://www.globsec.org/sites/default/files/2023-07/Cyber%20Brief%20Russian%20Cyber%20Operations_0.pdf**.

Marusic, Damin, and Kinga Brudzinska. “The EU Strategic Autonomy: Central and Eastern European Perspectives.” Globsec.Org, June 2021. **https://www.globsec.org/sites/default/files/2021-06/The-EU-Strategic-Autonomy-CEE-Perspectives-Report.pdf**.

Moyle, Ed. “What Is a Cloud Security Framework? A Complete Guide.” TechTarget, June 5, 2024. **https://www.techtarget.com/searchsecurity/tip/What-are-cloud-security-frameworks-and-how-are-they-useful**.

Mügge, Daniel. “Eu AI Sovereignty: For Whom, to What End, and to Whose Benefit?” Journal of European Public Policy, February 28, 2024, 1–26. **https://doi.org/10.1080/13501763.2024.2318475**.

Noyan, Oliver. “Cracks Appear as Gaia-X Celebrates Its Progress.” www.euractiv.com, November 19, 2021. **https://www.euractiv.com/section/digital/news/cracks-appear-as-gaia-x-celebrates-its-progress/**.

OECD Studies on SMEs and Entrepreneurship. “SME And Entrepreneurship Policy in the Slovak Republic.” OECD, June 15, 2021. **https://www.oecd.org/en/publications/sme-and-entrepreneurship-policy-in-the-slovak-republic_9097a251-en/full-report/component-5.html#section-d1e2293**.

Okano-Heijmans, Maaike. “Open Strategic Autonomy: The Digital Dimension.” Clingendael, January 2023. **https://www.clingendael.org/sites/default/files/2023-01/Open_strategic_autonomy_.pdf**.

National Office of Foresight & Strategy. “Open Strategic Autonomy: Ensuring European Citizens’ Welfare in the New Global Order,” n.d. **https://futuros.gob.es/en/our-work/OSA**.

"Questionnaire to the Commissioner-Designate Thierry Breton: Commissioner-designate for the Internal Market." European Commission, n.d. **https://commissioners.ec.europa.eu/document/download/e6ed1032-beb1-457b-acf1-01b0364a06f7_en?filename=answers-ep-questionnaire-breton.pdf**.

European Commission. "Questions & Answers on the First report on the State of the Digital Decade," September 23, 2023. **https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4620#:~:text=Under%20current%20trends,%20and%20without,and/or%20AI%20by%202030**.

Schniderova, Lucie. "EU Strategic Autonomy Must Remain Open, Says Czech Deputy PM." www.euractiv.com, November 4, 2022. **https://www.euractiv.com/section/digital/news/eu-strategic-autonomy-must-remain-open-says-czech-deputy-pm/**.

S&D Group. "S&D Group Strategy Paper on European Union Open Strategic Autonomy," February 6, 2023. **https://www.socialistsanddemocrats.eu/sites/default/files/2023-02/S%26D_Group_Strategy_Paper_on_European_Union_Open_Strategic_Autonomy_230206_0.pdf**.

"Spain-Netherlands Non-Paper on Strategic Autonomy While Preserving an Open Economy." Open Overheid. Accessed July 1, 2024. **https://open.overheid.nl/documenten/ronl-fd3bbc94-f598-45b3-abbd-75bfd5b18b97/pdf**.

European Commission. "Strengthening the Soul of Our Union," September 15, 2021. **https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701**.

Thévenet, Axel. "Dutch Digital Open Strategic Autonomy." Joinup, November 13, 2023. **https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/dutch-digital-open-strategic-autonomy**.

Timmers, Paul, and Freddy Dezeure. "Strategic Autonomy and Cybersecurity in the Netherlands." Cyber Security Council, February 17, 2021. **https://www.freddydezeure.eu/3-strategic-autonomy-and-cybersecurity-in-the-netherlands**.

EUR-Lex. "Trade Policy Review - an Open, Sustainable and Assertive Trade Policy," February 18, 2021. **https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52021DC0066**.

Wong, Haiman, Amy Chang, and Brandon Pugh. "The Transformative Role of AI in Cybersecurity: Understanding Current Applications and Benefits - R Street Institute." R Street Institute, January 26, 2024. **https://www.rstreet.org/commentary/the-transformative-role-of-ai-in-cybersecurity-understanding-current-applications-and-benefits/**.

GLOBSEC
IDEAS SHAPING THE WORLD

Vajnorská 100/B
831 04 Bratislava
Slovak Republic

+421 2 321 378 00
info@globsec.org

www.globsec.org

Sponsored by Google