Digital Sovereignty Is Impossible Without Big Tech
A Call to Action

Freddy Dezeure, Prof. Lokke Moerel, and Dr. George Webster*

> *"We must have mastery and ownership of key technologies in Europe. These include quantum computing, artificial intelligence, blockchain, and critical chip technologies. (. . .) We need infrastructure fit for the future, with common standards, gigabit networks, and secure clouds of both current and next generations."*
>
> **Ursula von der Leyen, *inaugural speech as president-elect of the European Commission* (2019)**

Call to Action

By now most companies and governments use the cloud infrastructure of three dominant U.S. providers—Amazon, Microsoft, and Google. Realization has set in that the widespread reliance on these "big tech" companies could pose a threat to the *digital sovereignty* of the European Union (EU) and its member states. At a time when cyberattacks are part and parcel of warfare and ever-increasing cybercrime, cyber resilience has become a cornerstone of our national security, for which we largely depend upon on a few dominant commercial players, even in times of war. The complexity of their cloud-based infrastructure is such that very few European enterprises and public services still "have" the expertise and means to protect themselves, the rest of them "have not". This is creating huge social, economic, and geographic disparities. Generative AI systems (like *ChatGPT*), which are bolted onto their existing products (like Microsoft 365 Copilot), are already significantly accelerating this dependence. EU policy initiatives to curb the market powers of big tech seem to be having little effect on diminishing this reliance.

In this article we offer a counterintuitive solution. Given the pervasiveness and impact of cyber threats, we consider any form of EU digital sovereignty impossible without ***leveraging the scale of big tech as an opportunity***. Rather than trying to curb their powers, we **call upon big tech to use their massive infrastructure and their insight on cyber threat actors and their modus operandi to improve cybersecurity worldwide by implementing baseline security controls *as a default*.** We encourage them to show strong leadership and corporate responsibility and (re)configure their infrastructure and tools in such a way that the organizations using them are protected and their resilience is safeguarded. In turn, we call on the EU and U.S. governments to convene with big tech to facilitate a self-regulatory discussion on this goal, without the risk of violating antitrust and other applicable laws.

1. EU's digital sovereignty

The EU is feeling the threat of what is coined as *digital colonialism* of the U.S. and China,[1] where the EU member states are increasingly dependent on digital infrastructures that are in the hands of only a few foreign commercial players. The digital identity of most European citizens depends on their foreign email addresses and a staggering 92% of European data resides in the clouds of U.S. technology companies.[2] Besides supply chain dependencies, these companies operate proprietary ecosystems, which offer limited interoperability and portability of data and applications, resulting in EU data being locked in and having limited value for EU innovation.[3] Foreign social media platforms are increasingly defining the rules of the game of European democracies, due to their lack of measures to combat misinformation, fake news, and political influence (often pushed by hostile states) on their platforms.[4] By now, the realization has set in that Europe's digital dependencies are so great that the digital sovereignty[5] of the EU and its member states is at risk. The fears are justified, EU sovereignty (and the sovereignty of any state around the world for that matter) is under pressure due to a combination of disruptive digital transformation (with winner-takes-all suppliers), exponential growth of cyberattacks (in which smaller countries and non-state actors now also enter the global battlefield),[6] and rising geopolitical tensions.[7] Where at first digital sovereignty was discussed in the context of cybersecurity, military, and defense, the discussion now extends to concerns about the economy and society at large. The ultimate challenge is how the EU and its member states can retain control over their economies (essential economic ecosystems), their democracies, and the rule of law (trust in their legal system and the quality of their democratic decision-making).[8]

The sovereignty concerns have led to a U-turn in EU policy. Until as recently as 2017, Europe was very much in favor of the open liberal market economy and EU research had to be *open to the world*,[9] but now restoring Europe's *digital sovereignty* is a core ambition of the European Commission (**EC**). This is proving difficult to achieve at a time when digital technologies have become the battleground for the race for global leadership between the U.S. and China (aka the *tech cold war*). The EU increasingly finds itself the *piggy in the middle* in a bipolar world. Both the U.S. and China have chosen the route of *tech protectionism,* regularly drawing the *national security* card to justify addressing critical supply chain issues (exposed by the pandemic) by bringing manufacturing back to their countries, imposing stricter export controls of critical technologies, prior screening of any supply of information and communications technology (**ICT**) for involvement of foreign adversaries, and stepping up screening foreign direct investments into their countries. These protectionist measures affect the EU as well. If all ICT supply to the U.S. is screened for Chinese involvement (and *vice versa*), the EU will need to reconsider its own supply chain as well to maintain access to overseas markets.

Concerns of the superpowers go beyond ICT supply chain dependencies and extend to concerns about what their adversaries can do with the data of their companies and citizens. Both the U.S. and China consider access to each other's data a matter of national security (*data as a weapon*),[10] resulting in bans on the export of important data outside their territories. Where data exchange by the EU is increasingly becoming a *one-way street*, the EU is also reconsidering its options.

To address the dependencies, the EU has issued a suite of policy measures to increase cyber resilience of critical infrastructures and services in Europe,[11] setting up its own production of critical technologies, like semiconductor chips, in the proposed Chips Act,[12] regulating the market power of *gatekeepers* providing core platform services (such as search engines, social networks, video sharing, and cloud computing services) in the Digital Markets Act,[13] regulating large online platforms to decrease the spreading of illegal content, misinformation, and targeted advertising practices with the Digital Services Act,[14] and regulate artificial intelligence in the proposed AI Act.[15]

However, realization has set in that these policy measures are not sufficient. On October 3, 2023, the European Commission issued an urgent Recommendation calling for a further risk assessment on four critical technology areas for the EU's economic security. One of the critical areas is *AI and cloud computing infrastructures*, "as these have the highest likelihood of immediate risks related to technology security and technology leakage, having a wide range of dual-use applications."[16]

2. Realities of war

The European Commission is right in calling for such risk assessment. The war in Ukraine has shown that hybrid war and large-scale disinformation are a reality.[17] Never before has cyber been used in such a prominent manner, closely synchronized with physical war.[18] And there is evidence that state-sponsored groups have positioned malware in critical western infrastructures in preparation for potential future conflicts.[19]

The reality is also that big tech plays an important role in cyber defense, protecting entire countries, such as Ukraine,[20] by blocking destructive cyber-attacks, increasing resilience by moving systems into cloud environments, and enabling internet communication by satellite.[21] It requires little imagination to understand what the impact could have been on the battlefield if big tech would not have stepped in to mitigate the adversarial cyber operations.

The interventions by big tech in Ukraine and other areas are commendable. But they also demonstrate societies' strategic dependence on the goodwill of these providers, and the organizations' risk tolerance at any given moment in time, as demonstrated by the decision to switch off satellite-based communications during active combat in Ukraine.[22] The merits of this decision are not the point here, but rather the decision highlights the dependencies on private companies, even in times of war.

3. Increasing cyber crime

An important dimension of digital sovereignty is the *cyber resilience* of its critical sectors, processes, and data. The ever-increasing cybersecurity threats undermine digital sovereignty. Economic losses are growing by 15% per year, reaching an estimated 8 trillion USD in 2023.[23] The concerns extend to the entire spectrum of direct threats to the economy by blackmailing and disrupting businesses ("ransomware attacks") and systematic theft of intellectual property from knowledge-intensive industries ("economic espionage").

It is apparent that even crimeware gangs have become professionalized by providing *ransomware-as-a-service* and more difficult to stop by the average organization. Law enforcement and other public actions have not decreased the impacts of cybercrime.[24] There is no reason to assume this will change any time soon.

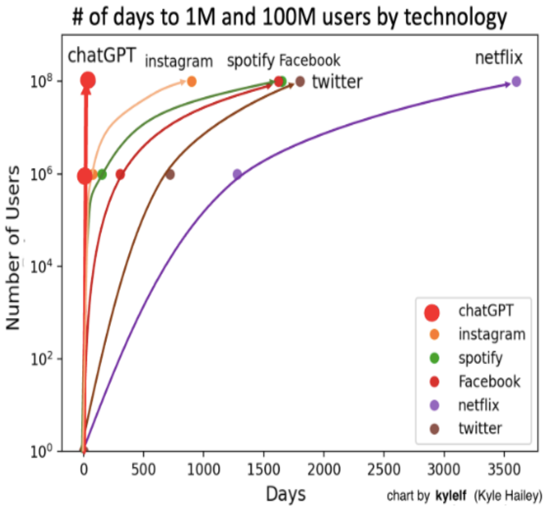
4. Complexity of IT infrastructure is beyond customers' comprehension

The COVID-19 pandemic has triggered a massive move of IT infrastructure and data into the cloud, with people increasingly working from home or in a hybrid fashion.[25] The distributed infrastructure offers many advantages in terms of availability and scalability, but the technical complexity of configuring and securing it are beyond the capacity of many of its customers, even mature ones. Most organizations struggle to grasp the central role of their data assets and IT infrastructure. As a result, most organizations are not well protected and will not be in the future, regardless of any cyber regulations that are being put in place to improve cyber resilience.

The complexity and scale of the current and future infrastructures will exacerbate the social and geographic disparity between the few elite organizations that have the capacity, skills, and resources to adopt these new capabilities in a safe manner and those that have not. And a "no-IT" or "no-data" situation is not an option any more.

5. 2023, the year AI broke through the roof

In 2022, the world entered into a new AI era exemplified by the public launch of ChatGPT. Rarely has any technology been adopted so quickly and so massively.



Adoption of ChatGPT, credit Kyle Hailey

But, more importantly, in 2023, AI has seen massive productization in all aspects of the economy and society, revolutionizing entire industrial sectors and forcing numerous workforce sectors to adapt or expire.[26] The broad adoption of AI and the incorporation of the new AI tools into the existing products and services of big tech are also making us ever more reliant on big tech. Like the office automation revolution in the eighties, internet in the nineties, and handheld devices in the beginning of the 21st century, AI has become embedded in our everyday needs, including our personal life (e.g., personal assistants, leisure recommendations, photography improvements, and identity controls), societal, or health- or business-related needs, and the next generation will not understand how we could have lived without AI.

6. 2023, the year that big tech confirmed its monopolistic traits

The IT market is dominated by a limited number of non-EU corporations. The top three cloud providers—Amazon, Microsoft, and Google—account for two-thirds of the worldwide market.[27] In office automation software, Microsoft and, to a lesser extent, Google are dominant.

Dominant players have a tendency to continue to solidify their positions, expanding their ecosystem by integrating new functionalities (such as cybersecurity and data analysis tooling) into their services, which will only increase *vendor lock in.*[28] They are also able to attract the best talent worldwide and have almost inexhaustible access to capital. They continuously monitor innovations and start-ups, which they take over at an early stage and integrate into their own offerings, and also aggressively compete and attempt to influence regulation.

We can see this happening in the AI space as well. Microsoft made its biggest investment ever in January 2023, with US$10 billion in OpenAI. Amazon and Google committed to invest US$4 billion and US$2 billion, respectively, in Anthropic, OpenAI's competitor. These same companies—Microsoft, Amazon, and Google—are massively scaling up their cloud infrastructures to execute their AI workloads,[29] and are also investing in custom AI chips to keep up with expected demand.[30] There is little doubt that these huge investments will increase the dominance of the main big tech players. As a case in point, these amounts alone dwarf all AI investments in the EU.

In the meantime, AI is being bolted onto existing products such as search (Bing Chat, Google SGE), office automation (Microsoft 365 Copilot, Duet AI for Google Workspace), security tools (Security Copilot), and tools generating AI applications and agents (Amazon Bedrock), potentially resulting in massive improvements in productivity, but also increased dependence.

7. Big tech has the means to improve cybersecurity and resilience at scale

The large footprint of the big tech providers and the massive move of IT infrastructure and data into the cloud creates important opportunities for cybersecurity and resilience at scale. Big tech has the capacity, the skills, and the resources to (re)configure infrastructure and tools in such a way that the organizations using it are protected and their resilience is safeguarded.

It should be feasible to define secure configurations and implement them as defaults, rather than as options which must be turned on by customers, or available at a premium. It should be the other way around; secure configurations and premium options should be the default (and included in the base pricing) and less secure variants should be optional.

In technical terms, one can think of examples like automated patching, implementation of multi-factor authentication or passwordless-systems, limited privilege enforcement, application whitelisting, data encryption, secure backups, endpoint protection, event detection, sandboxing email attachments, enforcement of DMARC (Domain-based Message Authentication, Reporting and Conformance) and strong TLS (Transport Layer Security) protocols, data provenance, and governance enforcement, etc.

Furthermore, the main cloud providers have a very extensive visibility ("**telemetry**") on the adversary infrastructure and modus operandi, allowing them to block communications to dangerous places or to trigger detection alerts. Some of this telemetry is already deployed in browsers,[31] leaked credential detections,[32] or blocking IP addresses.[33]

Microsoft (Azure Security Center,[34] Microsoft Secure Future Initiative),[35] Google (Security foundations blueprint),[36] and Amazon (AWS Startup Security Baseline,[37] AWS Cloud Security)[38] have already worked on laudable efforts to create tools which could help to secure organizations by covering many of these elements. However, these efforts are not comprehensive, not widely known, and hard to understand for less mature organizations.

8. Our proposal

In the current situation most organizations struggle with adopting technology and ensuring proper protection, while big tech has the means to protect at scale but has not fully implemented all security features. We issue a call to action to big tech to voluntary agree to use their strategic advantage from their infrastructure, insights, and tooling to protect the whole of their user base, using best efforts. We believe it makes sense from the perspective of Microsoft, Amazon, Google, to look at the world as an enterprise to be protected and apply the same principles one would use in enterprise cybersecurity and resilience but doing it at scale, including by using key controls and metrics[39].

This protection would require the vendors to go above and beyond product and service security. Taking inspiration from cybersecurity frameworks, implementing the key controls that would make the most impact, and updating those controls across the board whenever the threat landscape requires,[40] at scale, and for every user worldwide. We believe that baseline IT security and resilience should be part of products and services like clean water from the tap or stable electricity from the wall socket.

A holistic and integrated cybersecurity approach is required and should be offered as the default option. Advancements in AI will continue to make these opportunities easier to convert into reality. But leadership and vision are required to make it happen, including convening the powers of our governments to facilitate self-regulatory discussions, without the risks of violating antitrust and other laws.

9. Drawbacks of our proposal

Improving the protection of the worldwide IT infrastructure generally may equally benefit cyber criminals and state actors alike. We believe that the benefits of protecting the community outweigh this drawback. In addition, one can assume that sophisticated adversaries are already deploying a more mature protection of their infrastructure and the proposal we make would not provide a significant benefit to them.

Big tech may react by indicating that our proposal would negatively influence their bottom and top lines by increasing cost (defining and deploying controls) and reducing revenues (less sales of optional security products). This will inevitably be balanced by customers contributing to the additional cost of deploying baseline security across the board. We believe that the benefits of our proposal far outweigh the additional costs of deploying it.

Big tech may be afraid of legal consequences in case the proposed protection at scale would still not be perfect. This "imperfect" protection is a situation to be expected, but it will be, in any case, a better situation than the current one. We call on the EU and U.S. governments to convene the big tech companies to facilitate a self-regulatory discussion. We further recommend accompanying the resulting voluntary commitments by big tech, with accompanying measures from the public side to provide legal and regulatory protection based on demonstrated efforts and achieved results.

Implementing our proposal may lead to the perception that our dependency on big tech will only increase, since our cybersecurity will depend on them. This consideration needs to be put in the balance with respect to the expected increase in cyber resilience across the whole of the economy and society. We believe that the threats and their potential impact are becoming too large to continue with our traditional approaches to mitigate them.

Finally, the big tech companies may see their responsible behavior as a justification for continuing monopolistic behavior leading to a sense of immunity against competition law. We expect this narrative to regularly appear in conversations but would recommend that both big tech and the regulators not fall in this trap and pursue responsible behavior.

10. Concluding words

The dominance of big tech and our strategic dependence are creating an uncomfortable situation, even more so because our infrastructure is complex and beyond the understanding of most organizations. With our proposal, we intend to contribute constructive and realistic solutions to make the best of this situation and turn it into an opportunity to make the world cyber resilient for all, including the digital "have nots."

* Freddy Dezeure is an independent strategic advisor and the former head of the EU's Computer Emergency Response Team (CERT-EU); Lokke Moerel is a professor of Global ICT Law at Tilburg University, a member of the Dutch Cyber Security Council, and the chair of the Netherlands Atlantic Association; George Webster is the CEO of a stealth startup and the former Chief Security Architect at HSBC. The introduction draws

on earlier publications on digital sovereignty of Lokke Moerel, see most recently “Europe’s push for digital sovereignty: Threats, E.U. policy solutions, and impact on the financial sector”, *The Capo Institute Journal of Financial Transformation,* nr. 55, May 2022.

[1] Kwet, Michael, Digital Colonialism: US Empire and the New Imperialism in the Global South (Aug. 15, 2018). For the final version, *see* Race & Class, Vol. 60, No. 4 (Apr. 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232297.

[2] Oliver Wyman, European Digital Sovereignty, Syncing values and value, 2020, https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2020/october/European%20Digital%20Sovereignty.pdf.

[3] Digital Services Act package, Impact Assessment, https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act

[4] European Commission, “Tackling online disinformation,” https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation.

[5] For definition, *see* https://eucyberdirect.eu/research/strategic-autonomy-and-cybersecurity.

[6] Sanger, D.A. (2018), *The perfect weapon. War sabotage and fear in the cyber age*, New York; Crown; Lucas Kello, The Virtual Weapon and International Order, Yale University Press, 2017; Corien Prins also points out that the new digital weaponry is changing the (geopolitical) order: “The balance of power is shifting, now that smaller countries can also enter the global battlefield. Without having to engage in a large-scale military confrontation or actually enter the territory of another state. In short, it is relatively easy to develop great clout,” https://www.njb.nl/blogs/consequenties-van-een-nieuw-type-oorlogsvoering/.

[7] Paul Timmers, Challenged by ‘Digital Sovereignty’, Journal of Internet Law, volume 23, nr 6, December 2019.

[8] https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/khGGovSY/rif_timmersmoerel-final-for-publication.pdf.

[9] “Horizon 2020 is open to the world,” https://ec.europa.eu/programmes/horizon2020/en/area/international-cooperation.

[10] https://www.theguardian.com/world/2021/jul/10/china-us-cold-war-data-markets-national-security; https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1701161043031.

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0046.

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925.

[14] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

[15] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf.

[16] https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en.

[17] https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/.

[18] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[19] https://www.theregister.com/2023/11/14/ncsc_cyber_readiness/

[20] https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

[21] https://www.theguardian.com/technology/2023/sep/07/elon-musk-ordered-starlink-turned-off-ukraine-offensive-biography.

[22] https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/; https://spacenews.com/space-force-we-expect-to-see-interfering-blinding-of-satellites-during-conflict/.

[23] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/.

[24] https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland

[25] https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever.

[26] The jobs most likely to be lost and created because of AI | World Economic Forum (weforum.org).

[27] Chart: Amazon Maintains Lead in the Cloud Market | Statista.

[28] *See* European Data Strategy, p. 7, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066.

[29] Financial Times, 5 November 2023; Tech giants pour billions into cloud capacity in AI push

[30] https://www.reuters.com/technology/amazon-announces-new-data-center-chip-microsoft-rivalry-intensifies-2023-11-28/.

[31] https://safebrowsing.google.com/.

[32] https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#common-questions.

[33] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[34] https://azuremarketplace.microsoft.com/en/marketplace/apps/microsoft.azuresecuritycenter?tab=overview.

[35] https://www.microsoft.com/en-us/security/blog/2023/11/02/announcing-microsoft-secure-future-initiative-to-advance-security-engineering/.

[36] https://cloud.google.com/architecture/security-foundations.

[37] https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-startup-security-baseline/welcome.html.

[38] https://aws.amazon.com/security/.

[39] https://www.researchgate.net/publication/374061802_Ten_Key_Insights_for_Informed_Cyber_Oversight

[40] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.