Rolling out Secure, Resilient Digital Infrastructures for Europe

by Amelia Andersdotter

Summary

The EU has a number of opportunities in the field of cybersecurity. By investing in competitive research and leveraging capital from the west and talent from the east, the EU could establish itself as a global stronghold of innovation in cybersecurity and privacy technologies. Consistent and coherent governance, combined with competitively organised markets and standardisation, could ensure that European values are imbued not just in local technological projects, but in the global economy as well.

Keywords 5G – Standardisation – Cybersecurity – Securities – Privacy – Innovation

Introduction

The EU is an end-destination market for information and communication technology (ICT). From hardware design and manufacture to software service conceptualisation and implementation, Europe, its companies and its public institutions are dependent on other regions. To manage this complex cyber-environment with its fragile logistical chains, the EU needs to agree on a proactive cyber strategy. Cloud infrastructures, the Internet of Things and 5G/6G networks are all expected to enable industrial and administrative efficiency. Meanwhile, establishing and protecting EU sovereignty and leadership will require a combination of *ex ante* measures (certifications, standards and capacity), *ex post* measures (procurement, research and enforcement) and governance (consistency, law and regulation, and strategic development).

Building a complete European digital market must involve synergising access to capital and manufacturing in the west with the product- and service-development skills of the east. The reasons for this are not only related to equitable and fair growth in the Union, but are also practical. EU member states must increasingly coordinate their actions across policy fields such as climate change, security policy and strategic manufacturing, and will run up against the challenge that a certain level of institutional stability and experience, as well as domestic capital, is necessary to make these adjustments. When such stability and experience are absent in a country, its peoples and institutions may legitimately fear that committing to another country's technologies might reduce their autonomy. Cross-commitment makes sure everyone has a stake in the successful adjustment of the entire European economy.

At the same time, the EU is having to answer crucial questions about how to transform its legally established values into verifiably testable criteria for technology, while also safeguarding competition and innovation. At both the European and the national levels, institutions need to develop a less risk-averse culture, where bold investments can lead the way to both competitive markets and future technologies, but also provide important opportunities to learn from failures.

High-level governance tools such as harmonised standards and self-conformity assessments, the realisation from classical European competition law that robust and competitive markets require a minimum number of competitors to remain viable, and transparency as a core value for success are already in place.

Catching up or falling behind? Roadblocks for Europe

In the cybersphere, the EU is either trying to catch up or falling behind. In jest, observers remark that in our multipolar world, the US is responsible for innovation, China for manufacture and the EU for regulation.[1] The concern should be that neither service development nor material production occurs on European soil.

In fact, while the European single market has been under construction for more than 30 years, the market is anything but digital. European startups such as Workable (human resources management), Gorilla (electricity pricing), Revolut (fintech), ESET (security) and Spotify (streaming) have launched their services by first establishing themselves in their home member state, before advancing to either the Netherlands or the UK, and then conquering the US market, ahead of returning 'home' to Europe to capture other larger markets beyond their home market. This is a costly and time-consuming endeavour, in which EU-founded companies have to compete against US companies on the US market before even standing a chance in the EU market.

Western European markets remain closed not just to Eastern European service and product developers, but to all non-domestic companies. For example, in France, all spectrum licences for commercial mobile network operations are held by French entities.[2] Only Belgium has ever awarded a spectrum licence to an Eastern European player (a 5G licence to DIGI Communications).[3] A large part of this challenge is surely rooted in the linguistic diversity of the EU, but the spectres of mistrust and security policy still present effective barriers to both market integration and industrial prominence.

Ambitious projects to ensure cross-border service availability, such as Gaia-X for cloud services, end up doing little more than developing structured text files (JSON tags).[4] Even where frameworks for competitive procurement are being developed to help guide public-sector investments, they are rarely implemented and poorly enforced.[5]

These shortfalls of the European integration project can only be remedied by the member states; however, the EU needs to develop more robust mechanisms to call them out. Rather than retreating into autocracy and a 'not made here' mentality, the member states need to work out why European entities do not invest in each other.

One example of the lack of cross-border cooperation is that of European participation and representation in industry-driven standards development. There are industry-wide platforms for the development of the common technical practices that underpin the entire global communications infrastructure, for example, the standardisation work of IEEE 802.11, the Internet Engineering Task Force, the UTF-8 Consortium or the USB Implementers Forum. In these fora, European companies are present and contribute, but do not lead the work. In fact, the only consortium of notable import founded and governed from European soil is the Open Radio Access Network (O-RAN) Alliance. This is not to denigrate the contributions of European companies to global technology standards, but rather to point out that they are neither interested in, nor capable of leading the way for others in the way we have come to expect from the Linux Foundation, the Kubernetes Foundation,[6] the Ceph and OpenStack foundations,[7] or the Connectivity Standards Alliance.[8]

---

1 C. Hobbs, 'Project Note: In Search of Europe's Digital Sovereignty', in European Council on Foreign Relations, *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US–China Rivalry* (30 July 2020).

2 ARCEP, 'Mon Réseaux Mobile'.

3 *Tweakers.net*, 'Nieuwe provider Digi Belgium start voor het einde van het jaar', 16 May 2024.

4 See Gaia-X Technical Committee, 'Gaia-X Architecture Document – 23.10 Release, Chapter 3: Conceptual Model', chapter 3.3.1 'Gaia-X Credentials'. These credentials implement a JSON-LD syntax from W3C, 'Verifiable Credentials Data Model v2.0', 19 October 2024, chapter 6.1.

5 Germany, Commissioner of the Federal Government for Information Technology, *Architekturrichtlinie für die IT des Bundes*, version 6.1 (Berlin, January 2024).

6 Founded by Google through a donation of source code developed in-house for assisting in the management of virtual server configurations.

7 Founded by IBM to enable industry-wide collaboration around cloud application programming interface developments.

8 Currently stewarding ZigBee and Matter, the latter being a connected-home-over-Internet-protocol framework originally developed by Amazon, Apple and Google.

Meanwhile, the European regulatory standards framework has its roots in the beginnings of the single market, but primarily functions well in the context of synergising and finding compromise on national standards. Harmonised standards are developed to counter technical barriers to trade in market areas ranging from radio to cement.

In the majority of cases, functional safety standards and requirements frameworks already existed in the member states before the initiation of the single market, and the European-level institutions simply serve to ensure that European integration does not degrade the quality and safety of food, construction materials or electrical safety. The European Committee for Standardisation, the European Committee for Electrotechnical Standardization and the European Technical Standards Institute provide the intergovernmental frameworks within which the harmonisation of standard requirements can occur. For markets where product cycles are much longer than the typical certification cycle, for instance, sewer-pipe linings, fire alarms or food preservatives, these harmonised standards function well. The long lead times for the development and application of the standard matter little when product lifetimes are longer than 10 years.

However, for ICT, the European standardisation system does not perform so well. It lacks the flexibility afforded by industry-led groups and is encumbered by political formalism. The same mechanisms that are a strength in terms of safeguarding the application of the precautionary principle in food and building safety become a hindrance on the ICT market, where product cycles are shorter than certification cycles. Added to this is the fact that most ICT standards are already in production (for instance, in the shape of finalised code) and ready for deployment by the time they are standardised. This contrasts, for instance, with steel-pipe manufacturing, where a standard is established before production begins. The EU would do well to invest in its capacity to benefit directly from sensible industry standards in these circumstances, namely, by absorbing the outcomes from industry-driven standards bodies directly into procurement guidelines, rather than forcing them through its already established intergovernmental frameworks.[9]

Finally, the EU needs consistent and coherent political leadership. Instead of sending the European Commission services scrambling to invent a way in which ‘European values’ make their particular unit especially important to the European economy, political leaders need to have a sufficiently shared understanding of what they are doing to help the services work in tandem with each other and the cabinets on what a good enforcement policy might look like. Terms such as ‘data protection’ or ‘trustworthy’ need to be imbued with practical meaning, both to assist with the understanding of current laws and to drive new legislation.

A path towards the future: reiterating what has already worked

As dire as the situation may appear, the EU has succeeded in establishing a portfolio of policy options with which to gather knowledge, fund projects and create regulation. In the last 10 years alone, the second Payment Services Directive[10] has paved the way for open application programming interfaces (APIs) in the banking sector, which has enabled lots of innovative products to be launched on the European markets that otherwise would not have been commercially feasible. The Digital Operational Resiliency Act[11] is expected to create a market space for multiple cloud-service providers, thereby ensuring that no single cloud-service vendor becomes

[9] A. Andersdotter and L. Olejnik, ‘Policy Strategies for Value-Based Technology Standards’, *Internet Policy Review* 10/3 (2021).

[10] European Parliament and Council Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) no. 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L337 (25 November 2015), 35.

[11] European Parliament and Council Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) no. 1060/2009, (EU) no. 648/2012, (EU) no. 600/2014, (EU) no. 909/2014 and (EU) 2016/1011 (Text with EEA relevance), OJ L333 (14 December 2022), 1.

too big to fail. With this evaluation of the financial sector, it should be considered whether similar regulation could be useful in other areas. Home automation, vehicle sharing and digital-content platforms could be areas where functional requirements for interoperable APIs could help consumers to switch between providers.

Regulations such as the General Data Protection Regulation are only now beginning to take effect on the markets as enforcement authorities become more competent and confident. Despite this, privacy engineering and privacy-enhancing technologies mostly remain the public concern of large American tech companies,[12] while European companies have either failed completely or at least failed to advertise any enthusiasm for or engagement with the topic. Here, a cultural shift is needed in the leadership of the largest European companies, which can only be brought about by consistent and steadfast political leadership.

The US Defence Advanced Research Projects Agency has a strategy of funding multiple consortia to perform the same task, thereby ensuring that all pressing technical problems are addressed in a multiplicity of ways by different entities. Each challenge thereby gives rise to a competitive market for solutions already in the initial stage of development. The ongoing development of open-source electronic design automation libraries for chipsets is a prime example.[13] The EU would do well to replicate this strategy.

On the research front, the EU should further explore social science perspectives. Instead of looking only at technology development, the EU needs economic and social models into which technical innovations can be sensibly incorporated. This may include exploring European conceptualisations of leadership and industrial leadership, innovation management practices, and both business- and socially oriented interactions between European technology companies and the public sector. Consider, for instance, the application of cryptographic tokens to property sales in European jurisdictions where notaries mediate property transactions: instead of creating efficiency, cryptographic protocols introduced the necessity of having two notaries where previously only one was needed.[14]

To identify current gaps in enforcement and standardisation, the EU should not hesitate to use its full arsenal of institutional tools. The General Data Protection Regulation calls for data-protection-friendly technical standardisation:[15] a European Parliament special inquiry should be requested to investigate which industry-driven initiatives exist in this space and how they relate to the enforcement challenges currently faced by data protection authorities. The ePrivacy Directive calls for technical tools to enable stronger protection from tracking:[16] a European Parliament special inquiry should be requested to map the challenges and opportunities arising from this obligation. The Radio Equipment Directive formulates built-in data-protection and privacy features as an essential requirement of all radio equipment,[17] an obligation that has been present in European law since 1999, but which has still not been realised fully for all radios:[18] a European Parliament special inquiry should be requested to investigate industry-driven initiatives and regulator efforts to advance this essential requirement.

---

12 Google Cloud, 'Use Differential Privacy' (last updated on 15 October 2024); Amazon, 'AWS Clean Rooms Differential Privacy'; Github.com, 'Mozilla Prio Project' (archived on 13 February 2024).

13 See Defence Advanced Research Projects Agency initiatives Posh Open Source Hardware and Intelligent Design of Electronic Assets, and the initiatives sponsored under these programmes.

14 J.-F. Blanchette, *Burdens of Proof* (MIT University Press, 2012).

15 European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L119 (27 April 2016), 1, arts. 12(7)–12(8), 25 and 43(9).

16 European Parliament and Council Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L201 (12 July 2002), 37, art. 5(3).

17 European Parliament and Council Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance, OJ L153 (16 April 2014), 62, art. 3(e).

18 Although note, exceptionally, European Technical Standards Institute standard EN 303 645.

No other European body is as well placed as the European Parliament to maintain good relationships with all stakeholders, allowing it to survey the breadth and depth of industrial and social challenges in these already well-established priority fields of the Union.

The European Commission, in its turn, is well-placed to enforce existing legislation and agreements between member states. The politically appointed functionaries need to focus on the challenges faced by apolitical civil servants and determine where there are gaps or difficulties in enforcement, not only where member state governments feel that this enforcement is opportune, but across the board. A well-functioning executive is at the heart of any enterprise, whether it be a small or medium-sized company or a grand international experiment in cooperation across borders.

The European institutions could have a key role to play in identifying current capital flows in the EU. Whose money is being invested where, and in which services? The French telecommunications regulator Autorité de régulation des communications électroniques (ARCEP) has already done a lot of heavy lifting in terms of showcasing energy flows in the network operator industry.[19] Similarly pedagogic presentations are required about investments in innovation and development to enable and inspire a more integrated and equitable European digital single market. With more and more EU countries in Central and Eastern Europe (CEE) fearing that they are being left behind, careful analysis and consideration of the actual conditions on the ground could help to bring a sense of cohesion and clarity to the development of the EU market.

This might include understanding how research and development or customer support activities are being outsourced to CEE countries by Western European companies, but it may also shed light on the extent to which Western European capital is flowing into home-grown CEE activities such as e-commerce (the Allegro group), airlines (WizzAir) or cybersecurity (ESET). More recently, Europe has been the destination for large investments in privacy technologies in fintech and encrypted ledgers, which has primarily benefited developer bases in CEE.[20] However, it remains unclear whether the EU will be able to capitalise on its contributions to these emerging markets.[21]

Conclusion

Europe needs consistent, coherent leadership and governance to fully benefit from its contributions to the digital economy. As a large consumer market, and an internally under-appreciated centre for technological development and innovation, with strong social and fundamental rights ideals, the EU should be able to shape global privacy and security standards in line with its foundational values. However, the Union must strive for greater maturity in its policy application.

Following up on already established policy directions, such as the commitment to data protection, privacy and procedure, will rationalise the European project for both citizens and businesses. The positive effects will reverberate throughout the technological stacks. But this needs to be coupled with paying greater attention to the capital flows to and within Europe, from east to west, and to the shared European funding of competitive and innovative research.

The EU should also develop procedures to benefit from existing mechanisms in standardisation. Translating European values into deterministic and predictable test criteria remains a challenge for policymakers and technology developers alike.

19 ARCEP and ADEME, *Assessment of the Environmental Impacts of the ICT Sector: Methodological Gap Analysis* (2023).
20 Electric Capital, *2023 Crypto Developer Report* (January 2024).
21 European Securities and Markets Agency, *Crypto Assets: Market Structures and EU Relevance* (Paris, 10 April 2024).

	Programme 1	Programme 2	Programme 3
	Creating digital resilience	**Ensuring digital sovereignty**	**Building future infrastructures**
Project 1	Establish (self-)certification schemes for products and services destined for the European market based on exact and replicable requirements. Continue to invest in European hardware infrastructure, including basic infrastructure such as long-distance cables and electricity grids.	Build capacity in project management for open-source code-as-infrastructure, especially in terms of industry-oriented fora (e.g. O-RAN Alliance). Trust, but verify: European open-source code libraries that address shared challenges should act as both public infrastructure and a trustworthy technology base.	Produce a standardisation strategy for 5G, O-RAN, cloud technologies and the Internet of Things that emphasises European values. Ensure fast deployment of the latest compliant technologies by allowing the flexibility of self-certification against approved standards with product recall penalties in the event of demonstrated infringements. Ensure that spectrum licences include requirements on the security of network equipment.
Project 2	Ensure technical resilience in investments across Europe. Use at least two vendors of network equipment from two different countries in any national network. Make the operation of a commercial system independent from features available from only one single upstream supplier (e.g. lock-in mechanisms, vendor-specific APIs or de facto standards).	Support technology development in Europe through strategic procurement, including where there is a risk of failure. Map capital flows into European technology industries and startups. Ensure that public money goes to public, open infrastructures, even code, that instil trust by being verifiable.	Hold a series of European Parliamentary inquiries into topic-specific enforcement activities in the area of cyber-excellence (e.g. activities regarding the essential requirement of radio equipment to respect data protection, as contained in Directive 2014/53/EU, art. 3(e)). Continue to focus on cyber-exercises and scenarios, especially in the cross-border context—consider the possibility of holding competitions that test sectoral, randomly selected teams, or similar, rather than national ones.
Project 3	Leverage the framework of harmonised standards. Develop shared open-source libraries for common goals and norms in public infrastructure, such as billing systems, personnel systems and so on. Support red-team research, responsible vulnerability disclosure and remedy/patching schemes.	Consistently recognise both the technical aspects of security (objective, deterministic criteria) and the organisational and legal aspects (venues of conflict resolution, jurisdiction and decision-making) when addressing cyber-governance. Bring together existing forces for capitalisation and market access to achieve pan-European service-launch opportunities.	Realise opportunities for innovators by opening up new regulatory spaces through replication of the changes in the fintech sector (with open APIs for specific bank payment systems in the 2010s) and the wireless local area network sector (when microwave bands were opened up to licence-exempt use in the 1990s).

Bibliography

Amazon, 'AWS Clean Rooms Differential Privacy' (2024), accessed at https://aws.amazon.com/clean-rooms/differential-privacy/ on 26 October 2024.

Andersdotter, A. and Olejnik, L., 'Policy Strategies for Value-Based Technology Standards', *Internet Policy Review* 10/3 (2021), doi:10.14763/2021.3.1573.

ARCEP, 'Mon Réseaux Mobile', accessed at https://monreseaumobile.arcep.fr/ on 26 October 2024.

ARCEP and ADEME, *Assessment of the Environmental Impacts of the ICT Sector: Methodological Gap Analysis* (2023), accessed at https://en.arcep.fr/uploads/tx_gspublication/environment-impact-ICT-sector-methdological-gap-analysis_april2023.pdf on 26 October 2024.

Blanchette, J.-F., *Burdens of Proof* (MIT University Press, 2012).

Electric Capital, *2023 Crypto Developer Report* (January 2024), accessed at https://www.developerreport.com/developer-report-geography on 26 October 2024.

European Parliament and Council Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L201 (12 July 2002), 37.

European Parliament and Council Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Text with EEA relevance), OJ L153 (16 April 2014), 62.

European Parliament and Council Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) no. 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L337 (25 November 2015), 35.

European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L119 (27 April 2016), 1.

European Parliament and Council Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) no. 1060/2009, (EU) no. 648/2012, (EU) no. 600/2014, (EU) no. 909/2014 and (EU) 2016/1011 (Text with EEA relevance), OJ L333 (14 December 2022), 1.

European Securities and Markets Agency, *Crypto Assets: Market Structures and EU Relevance* (Paris, 10 April 2024), accessed at https://www.esma.europa.eu/sites/default/files/2024-04/ESMA50-524821-3153_risk_article_crypto_assets_market_structures_and_eu_relevance.pdf on 26 October 2024.

Gaia-X Technical Committee, 'Gaia-X Architecture Document – 23.10 Release, Chapter 3: Conceptual Model', accessed at https://docs.gaia-x.eu/technical-committee/architecture-document/23.10/gx_conceptual_model/ on 26 October 2024.

Germany, Commissioner of the Federal Government for Information Technology, *Architekturrichtlinie für die IT des Bundes*, version 6.1 (Berlin, January 2024), accessed at https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/architekturen-standard/ArchRL.html on 26 October 2024.

Github.com, 'Mozilla Prio Project' (archived on 13 February 2024), accessed at https://github.com/mozilla/prio-processor on 26 October 2024.

Google Cloud, 'Use Differential Privacy' (last updated on 15 October 2024), accessed at https://cloud.google.com/bigquery/docs/differential-privacy on 26 October 2024.

Hobbs, C., 'Project Note: In Search of Europe's Digital Sovereignty', in European Council on Foreign Relations, *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US–China Rivalry* (30 July 2020), 91–4, accessed at https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/#project-note-in-search-of-europes-digital-sovereignty on 26 October 2024.

Tweakers.net, 'Nieuwe provider Digi Belgium start voor het einde van het jaar', 16 May 2024, accessed at https://tweakers.net/nieuws/222022/nieuwe-provider-digi-belgium-start-voor-het-einde-van-het-jaar.html on 26 October 2024.

W3C, 'Verifiable Credentials Data Model v2.0, 19 October 2024, accessed at https://www.w3.org/TR/vc-data-model-2.0/ on 26 October 2024.