

# **DIGITAL SOVEREIGNTY IN A CHANGING WORLD**

**A EUROPEAN PERSPECTIVE ON CONTROL,  
RESPONSIBILITY AND TECHNOLOGY**

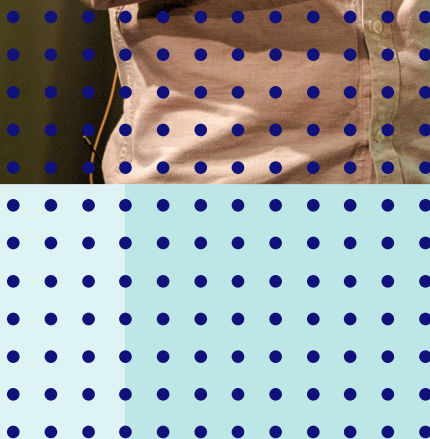
# Executive Summary

This paper reflects the perspective of Kristof Van Stappen, CEO of Jimber, a European cybersecurity company operating at the intersection of digital infrastructure, security architecture and regulatory compliance. The views expressed are based on practical experience working with organizations navigating changing requirements around control, resilience and long-term digital responsibility.



Digital infrastructure sits at the core of almost every modern organization. It shapes how data is accessed, how systems are protected and how operations remain available. For a long time, infrastructure choices were primarily evaluated on technical performance, scalability and cost. Where a solution was governed or controlled from was rarely a deciding factor.

That perspective is changing. Not because existing technologies have suddenly become unreliable, but because digital infrastructure itself has taken on a different role. It now directly influences legal exposure, operational resilience and strategic autonomy. As a result, infrastructure decisions can no longer be treated as purely technical or operational. They increasingly reflect broader questions around control, dependency and responsibility.



# A changing global context

This shift is not driven by a single country, a single provider or a single political event. It is the result of a broader transformation in how power, regulation and technology interact. Digital systems have become critical societal infrastructure, and with that comes increased scrutiny, influence and strategic interest from governments and regulators worldwide.

Extraterritorial legislation, supply chain risks and digital leverage are no longer theoretical concepts. They are part of the reality organizations operate in today. This does not invalidate global cooperation or long-standing partnerships, but it does change the assumptions on which those partnerships are built.

“The discussion is not about distrust. It is about understanding what happens when interests no longer fully align.”

In this context, dependency becomes visible. Not as a failure, but as an outcome of earlier choices made in a different environment. For years, efficiency and innovation rightly dominated decision-making. Today, resilience and control are joining that list of priorities.

## From efficiency to responsibility

### NIS2

Expands cybersecurity obligations across a much wider range of sectors.

### DORA

Focuses on operational resilience within financial services and their technology supply chains.

### Cyber Resilience Act (CRA)

The Cyber Resilience Act shifts attention toward the security responsibilities of product and software vendors themselves

As digital infrastructure became more deeply embedded in core business processes, its failure modes also changed. Outages, breaches or access restrictions no longer only affect IT departments. They can disrupt entire organizations, markets and public services. This evolution explains why digital risk is increasingly treated as a board-level concern rather than a purely technical one.

European policymakers have responded to this reality with a new generation of regulatory frameworks. These frameworks are often perceived as compliance pressure, but they serve a broader purpose. They signal that digital infrastructure is now considered a matter of systemic importance. Responsibility is no longer limited to implementation. It extends to governance, oversight and long-term risk management.

Importantly, these regulations do not prescribe specific technologies. They do not mandate local infrastructure or exclude global providers. Instead, they force organizations to ask harder questions about dependency, visibility and control. Regulation, in that sense, is not the solution. It is a catalyst.



# Rethinking digital sovereignty

Digital sovereignty is often misunderstood as an ideological concept or a push toward isolation. In practice, it is neither. It does not imply rejecting global technology ecosystems, nor does it suggest that everything must be built or hosted locally.

At its core, digital sovereignty is about choice. It is about knowing which parts of your digital environment you fully control, which parts you depend on externally and which risks follow from those dependencies. It is the ability to make informed decisions rather than implicit ones.

This perspective also brings nuance to the discussion. Not every system carries the same strategic weight. Not every dependency is problematic. The challenge lies in identifying which layers of infrastructure are critical enough to warrant stronger control and which can remain purely operational.



**“Sovereignty is not about doing everything yourself. It is about understanding where control actually sits when things go wrong.”**

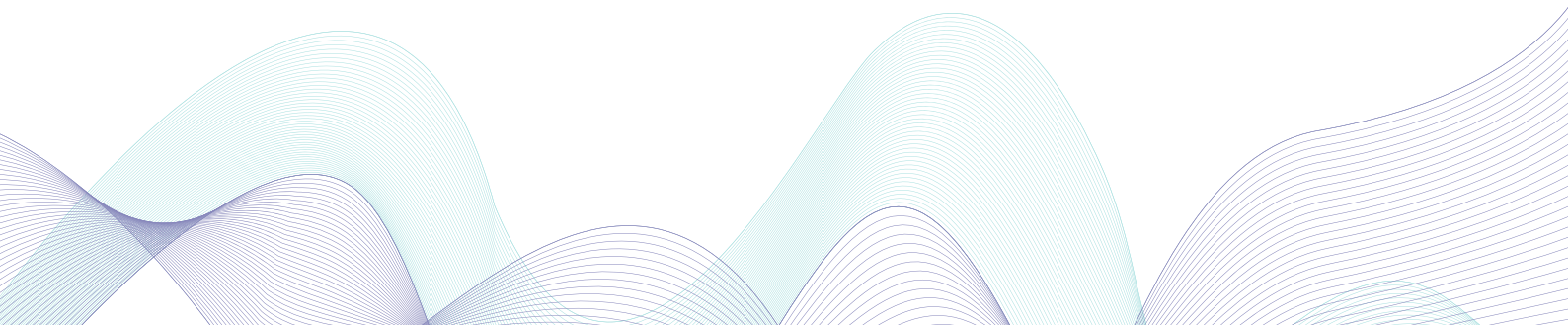


## Quality cannot be compromised

Any serious discussion about digital sovereignty must address quality head-on. Local or regional origin alone does not create resilience. Security, scalability, usability and operational maturity remain non-negotiable requirements. Organizations cannot afford to trade technical excellence for perceived control.

European technology ecosystems have matured significantly in recent years. Strong alternatives exist across multiple layers of the stack, including security, networking and identity. However, these alternatives are often less visible and less standardized than dominant global platforms. Finding and evaluating them requires more effort and more technical depth.

This is not a weakness, but a characteristic of an ecosystem that is still consolidating. Awareness, transparency and informed evaluation are essential to make meaningful progress.



# Awareness over urgency

The current moment does not call for panic or abrupt change. Organizations do not need to replace their infrastructure overnight. What is required instead is awareness. An understanding that digital infrastructure decisions have long-term consequences beyond cost and performance.

Digital sovereignty is not a switch that can be flipped. It is a direction that organizations move toward gradually, through architectural choices, governance models and risk assessments. Each step builds resilience without disrupting existing operations.

“The goal is not to change everything today, but to avoid being unable to change tomorrow.”



## About the author

Kristof Van Stappen is CEO of Jimber, a European cybersecurity company focused on secure network and access infrastructure. He works closely with enterprises, public organizations and technology partners on questions related to digital resilience, control and long-term infrastructure strategy.

**Connect with Kristof on LinkedIn**  
[linkedin.com/in/kristof-van-stappen/](https://www.linkedin.com/in/kristof-van-stappen/)

