Digital Dominance: Understanding How we all depend on U.S. Tech

Digital Dominance: Understanding How we all depend on U.S. Tech

Bernard Sfez - 2026-02-09 19:17

In May 2025, the International Criminal Court lost access to its email system. Not because of a cyberattack or technical failure, but because Microsoft suspended the email account of ICC Chief Prosecutor Karim Khan after the U.S. President imposed sanctions on him. With a single executive order from Washington, an American corporation reached into a European institution based in The Hague and flipped the switch. This isn't a hypothetical scenario. This digital dependency touches everyone – even Europe's most sensitive institutions, designed to protect citizens and uphold justice, operate on American infrastructure that can be shut down instantly.

Review the events of your daily life and you'll feel dizzy. You turn on your computer, check your smartwatch, ask Siri or Alexa to play music, start your car, make a phone call, send an email, calculate a route... Each time, you go through a service, a server, a technology made in the USA. From hardware (Intel, AMD, NVIDIA) to systems (Windows, iOS, Android) to applications (Microsoft 365, Google Workspace, Zoom), the dependency is systemic. And your habits, your life, your information, your photos... everything that goes online is no longer yours or your company's...
How did we get here?

Introduction

This article is the first in a mini-series on the state of digital sovereignty and whether it's still possible to reclaim it. When we assembled all the content we gathered to provide depth and concrete examples on this crucial subject, we ended up with... an indigestible tome of several dozen pages. We therefore decided to divide this reflection into several complementary but autonomous articles.

In this first post, we establish a factual assessment: how did we arrive at this total digital dependency? We will map out the mechanisms that allowed this situation to develop. Future articles will explore the stages of regaining control and concrete solutions: what alternatives exist today? How can we migrate progressively without paralyzing our organization? What are the pitfalls to avoid and the strategies that actually work?
Let's start at the beginning: understanding where we stand.

A Methodically Constructed Dependency

American dominance in digital technology is not the result of chance or solely an aggressive strategy, but a formidable combination of historical and economic factors.

First Pillar of Dependency: Colossal Investments

Since the 1970s and sustained for decades, Silicon Valley and Hi-Tech have benefited from massive funding, both public (DARPA, NASA) and private (venture capital). The American entrepreneurial model "move fast and break things" favors immediate market deployment rather than theoretical perfection, allowing dominant positions to be conquered while others are still thinking.

Second Pillar of Dependency: Absorbing Innovation from Around the World

A formidable capacity to attract and capture work from researchers and entrepreneurs wherever they are. Contrary to popular belief, the United States didn't invent everything, but they have a formidable ability to seduce and capture innovations developed elsewhere. The World Wide Web? Created at CERN by British scientist Tim Berners-Lee. SMS and the GSM standard that revolutionized mobile telephony? Designed in Europe. DeepMind, the AI lab behind AlphaGo? Founded in London, then acquired by Google. Skype? Created by Estonians and a Dane, swallowed by Microsoft. WhatsApp? Co-founded by a Ukrainian, acquired for $19 billion by Facebook. Spotify? Born in Sweden, now listed on Wall Street and deeply integrated into the American ecosystem. The United States excels in the art of transforming these foreign innovations into dominant commercial products under their control, using the "American dream" to attract talent: extraordinary relocation conditions, astronomical salaries, preemptive buyouts of promising startups, global deployment thanks to their financial and marketing power.

Third Pillar: Cultural and Psychological Lock-in from Childhood

Partnerships between American giants and Education departments mean that, from primary school onwards, students worldwide are formatted to American tools – Google (Google Workspace for Education, Google Drive, Google Classroom) or Microsoft (Office 365 Education, Teams). These "free" or reduced-price licenses create deep cognitive dependency, and by age 18, a student has spent over ten years working exclusively on American tools. They know Word, but not LibreOffice. They master Google Docs/Drive, but not Nextcloud. When they enter the workforce, they naturally reproduce what they know, and companies rarely ask them to do otherwise. Any alternative is viewed with suspicion – a waste of time, a quirk of "idealists." The lock-in isn't technical, it's cultural, and raises serious ethical questions.

Layers of Systemic Dependency

This dependency isn't limited to a few visible applications. It extends across the entire technology stack, creating an entanglement that's difficult to escape.

At the hardware level, Intel and AMD processors, both American, equip the majority of servers and workstations worldwide (outside China, which is attempting its own CPUs). ARM architectures, originally British, have come under international financial control with strong American influence: listed on Wall Street since 2023, majority American shareholders. NVIDIA graphics cards, now essential for artificial intelligence and intensive computing, are American. Even Asian chip

manufacturing giants (TSMC in Taiwan, Samsung in South Korea) depend on American licenses for design software (EDA: Cadence, Synopsys) and certain critical equipment, giving the United States veto power over who can produce what and for whom.

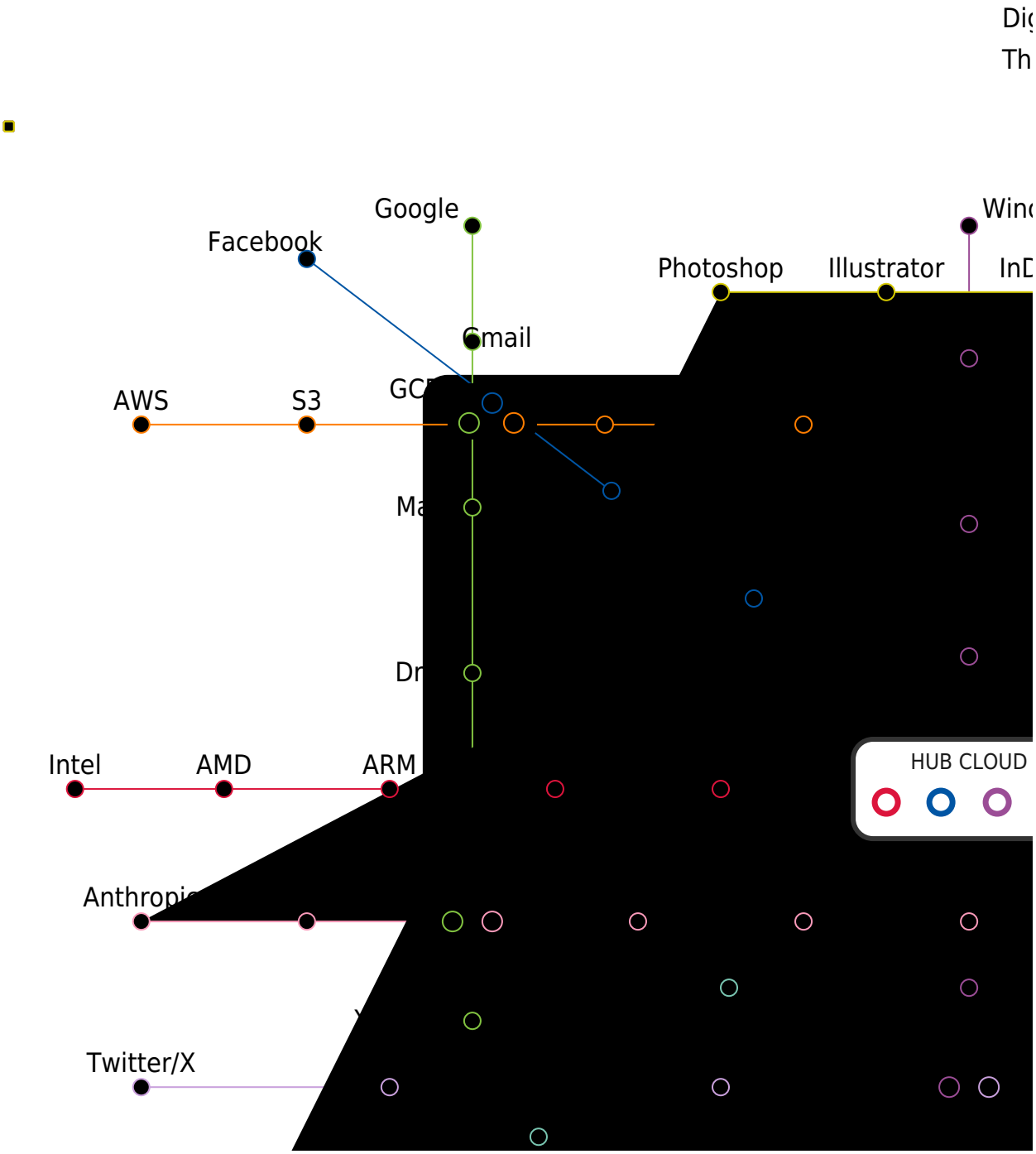
At the operating system level, Windows (Microsoft) dominates enterprise workstations with approximately 70% global market share. While servers run mostly on Linux, an open-source and international technology by nature, approximately 35 to 40% of Linux kernel contributions come from American companies (Intel, Red Hat/IBM, Google, Meta, AMD). In the mobile world, iOS (Apple) and Android (Google) share 99% of the global market, with no credible alternative outside China where HarmonyOS (Huawei) is attempting to establish itself.

At the application level, domination is overwhelming. Microsoft 365 equips tens of millions of businesses worldwide for office productivity and collaboration. Google Workspace is the main alternative, still American. Salesforce structures sales departments, Adobe Creative Suite is essential for creative professions (though this front seems to be cracking in recent months), Slack/Zoom/Teams organize internal communications: all American. Databases (Oracle, MongoDB), analytics tools (Tableau, Power BI), business intelligence platforms: American.

Connected devices amplify dependency: smart cars with Android Automotive (Google), navigation apps like Waze (Israeli startup acquired by Google in 2013 for $1.3 billion, collecting all your routes), voice assistants dominated by Alexa (Amazon), Siri (Apple) and Google Assistant, smart speakers, watches, thermostats, security cameras... Each device continuously collects personal and professional data, expanding the scope of dependency.

Emerging technologies are already locked down: generative artificial intelligence is dominated by OpenAI (ChatGPT), Google (Gemini), Anthropic (Claude) and Microsoft (Copilot). Augmented reality and "spatial computing" are led by Apple (Vision Pro) and Meta (Quest). Specialized chips for AI (GPU, TPU, NPU) are American (NVIDIA, AMD, Google, Apple). Not only do we depend on the United States for the present, but the technological building blocks of the future are already in their hands.

<?xml version="1.0" encoding="UTF-8"?>



False Hopes of Sovereignty

Faced with this dependency, many believe they're protecting themselves with tools presented as "secure" or "sovereign." This is often an illusion.

Commercial VPNs (NordVPN, ExpressVPN, CyberGhost, Surfshark) promise protection and anonymity, but the vast majority are American or acquired by American funds. Even when sincere, they remain subject to the Cloud Act and Patriot Act: if US authorities request access to data, the company must comply, often under judicial secrecy. Your traffic passes through their servers, creating a perfect centralized control point for surveillance.

Cloud contracts offer reassuring guarantees: "Your data is hosted in Europe," "We comply with GDPR." But a datacenter in Frankfurt operated by AWS remains under US jurisdiction. Microsoft may promise that your Office 365 data doesn't leave Europe, but encryption keys and administrator access remain controlled from the United States. "SecNumCloud" certifications only

provide guarantees if the operator is truly European and independent, not a subsidiary of an American giant.

Even protection software is often American: antivirus (Norton, McAfee), popular password managers (1Password, or LastPass despite being hacked multiple times). US laws allow authorities to demand data access, despite marketing promises.

So, Can This Dependency Be Overcome?

The answer is yes, but only through coordinated action across multiple sectors.

Solutions already exist ! European hosting providers—such as OVHcloud and Scaleway in France, or Hetzner in Germany—offer high-performance infrastructure. Meanwhile, open-source software provides mature alternatives for every layer of the digital stack: Linux and Virtualmin for systems; LibreOffice and OnlyOffice for productivity; Syncthing or Nextcloud for collaborative storage; and Tiki Wiki for intranets and business applications. Specialized tools like Matomo for web analytics, Odoo for modular ERP, and Dolibarr for Financial and CRM further demonstrate European capability. Open source serves as a decisive lever for sovereignty, offering code that can be audited, modified, and maintained independently of any American publisher.

However, a full transition requires a coordinated commitment across the board.

Governments must invest massively in sovereign infrastructure, such as public datacenters and national clouds, while mandating the priority use of European solutions within public services, hospitals, and schools.

Companies must develop credible alternatives backed by strict legal guarantees, including 100% European infrastructure and encryption with customer-controlled keys to ensure a categorical refusal to cooperate with extraterritorial data demands.

Organizations and Citizens must integrate digital sovereignty into their daily decision-making, treating it as a core criterion alongside cybersecurity to maintain control over their own resources.

Breaking free from this dependency won't happen in a year or two, which can pose a problem for budgetary choices paced by electoral cycles – it's a multi-generational project. But every day without action strengthens the lock-in.

In our upcoming articles, we'll explore concrete solutions sector by sector and progressive migration strategies to, at your level, regain control of your digital infrastructure and information.