What is Digital Sovereignty, and Who Possesses It?

(Translated)

Al-Rayah Newspaper - Issue 563 - 03/09/2025 CE

By Dr. Muhammad Jilani

When we speak of sovereignty, what comes to mind are borders, maps, and armies. However, in the age of electronic networks and digital transformation, another type of sovereignty has emerged: digital sovereignty. This is the ability of states to decide, without the guardianship of any external party, how their digital infrastructure is built, where their data is stored, which standards they adopt, and how they protect their economy and citizens from invisible attacks. Whoever possesses this ability does not merely protect their cyberspace; they also gain political and economic influence that transcends geography.

The story of digital (cyber) sovereignty begins with matters that at first glance may seem dry and technical: undersea cables stretching thousands of kilometers, data centers cooled by rivers, and Domain Name System (DNS) that link a website’s name to its digital address. Built upon this foundation are digital clouds, giant platforms, app stores, and artificial intelligence systems. Between each of these layers lie critical chokepoints, bottlenecks in chip design, tools without which no chips can be made, advanced manufacturing equipment sold by only a few, and technical standards, whose authors later dominate the market. Here lies the essence of digital sovereignty: being a maker of the foundation, not merely a user of it.

On this stage, there are three major blocs advancing, each with its own style and capabilities:

- **The United States**, acting as the architect of the global digital order. It holds heavyweight positions in cloud services, platforms, software, and AI, and maintains the most widely used chip design tools. Its power is not limited to technology; it extends to law, with the ability to access its companies’ data even abroad through treaties and legal frameworks, and alliances that drive many states to adopt its standards. In security, it possesses intelligence capabilities and deep partnerships that give it a wide-open eye on cyberspace.

- **China** builds its own narrative: a vast domestic market accompanied by wide-scale manufacturing, a “Digital Silk Road” extending outwards, with persistent efforts to substitute imports in chips, AI, and electronic payments. While still facing gaps and challenges in advanced chip-manufacturing equipment, China works to fill these holes through sovereign investment, massive financial injections, and a steadily integrating supply chain.

- **The European Union** uses a different weapon: regulation and standards in data protection, platform control, cybersecurity, and digital identity. Europeans write the rules of the game in these areas. However, their biggest challenge is not legal, it is industrial: how to transform regulatory power into global platforms and products that rival the giants.

There are also rising players such as India, which offers a national experience through a digital identity platform and government services reaching hundreds of millions, alongside growing ambitions in chips and open-source software. Meanwhile, Korea, Taiwan, and Japan hold critical positions in supply chains, from raw materials to equipment. Russia, despite economic restrictions, retains notable cyber-offensive capabilities that count in deterrence balances.

Cybersecurity itself is crucial because the modern economy depends on continuity, which in turn depends on the digitization of every stage from production to consumption. A cyberattack on a power grid, major bank, or telecom provider could freeze an entire city. The

U.S. itself once suffered a cyberattack by Russia that reached defensive networks, including nuclear weapons control systems, which was later contained following a meeting between President Putin and former U.S. President Biden. This is where sovereignty lies: a state maintaining multilayered defenses, monitoring its supply chain, quickly closing vulnerabilities, and building trust with its citizens and financial markets. Trust is a political and economic capital, no less valuable than oil and gas.

Who holds the upper hand in digital sovereignty today?

- Technically: The U.S. leads in cloud, platforms, software, AI, and chip design tools.
- China: has enormous domestic manufacturing momentum and rapid application growth, striving to cross the threshold of advanced equipment.
- Europe: strong in standards and certain segments of equipment and industrial innovation, but still searching for platforms to compete globally.
- Financially: The U.S. retains the center of venture capital and innovation financing, China builds through massive sovereign funding, while Europe balances with guided industrial policies.
- Politically: The U.S. relies on broad alliances that reinforce its standards, China extends influence via digital infrastructure projects and external funding, and the EU exerts normative power, that shapes company behavior within its market.

For middle-sized states, this map does not imply surrender. Digital sovereignty is not “all or nothing”; it is a constructive process, built layer by layer. A state can decide what to own domestically such as a national digital identity, a sovereign cloud for sensitive sectors, or data centers within its borders and what to procure externally, when local development is not immediately possible. They can diversify suppliers of chips, cloud services, and cables, enact balanced laws for data protection and cross-border transfer, and build human capital to safeguard cyberspace and advance AI. Most importantly, they must be active in standard-setting bodies, for whoever writes the standard today will sell the product tomorrow.

There are still states in Africa, Latin America, and the Muslim world that remain consumers of products from the U.S., Europe, China, Japan, and Korea, with only limited software production that itself depends on those industrial powers’ hardware, operating systems, and storage technologies.

Although this discussion seems technical, at its core it is a matter of sovereignty: Who owns data decisions? Who controls platforms? Who secures themselves without technological blackmail? In a world where trade, politics, and services run through networks, the answers to these questions determine the rank and influence of nations. Digital sovereignty is not a slogan or luxury; it is a state vision and plan: calculated investments, smart alliances, clear legislation, and capacity building that does not collapse at the first attack.

From here, serious thinking is necessary in this strategic field, especially regarding the upcoming establishment of the Khilafah (Caliphate), Allah willing, which must, both from a doctrinal (aqeedah) and political standpoint, possess absolute sovereignty in every domain. The Khilafah (Caliphate) will have the necessary elements to secure digital sovereignty, as an integral part of the absolute sovereignty Allah (swt) has commanded. Allah (swt) says, ﴿وَلَن يَجْعَلَ اللَّهُ لِلْكَافِرِينَ عَلَى الْمُؤْمِنِينَ سَبِيلاً﴾ **“And never will Allah grant to the disbelievers a way (to triumph) over the believers”** [TMQ Surah An-Nisa: 141].