EU CYBER DIRECT

RESEARCH PAPER

# SHAPING CONNECTIVITY

## The invisible governance of Internet standards diplomacy

Dr Konstantinos Komaitis

EU Cyber Direct, European Union Institute for Security Studies · November 2026

## Author

**Dr Konstantinos Komaitis**

*Resident Senior Fellow, Democracy + Tech Initiative*

**Atlantic Council**

### SHORT BIO

Dr Konstantinos Komaitis, a resident senior fellow at the Atlantic Council's Democracy + Tech Initiative, leads its digital governance work. He previously held senior roles at the University of Strathclyde, the Internet Society and the New York Times and he currently serves on the Global Network Initiative board and the Freedom Online Coalition's Advisory Network. He is also the author of the forthcoming book: *The Internet and How We Lost it: Legibility, Enclosure and the Fight for the Open Internet*.

## About EU Cyber Direct

EU Cyber Direct – the EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen the rules-based order in cyberspace and build cyber resilient societies. To that aim, the programme conducts research, supports capacity building in partner countries, and promotes multistakeholder cooperation. EU Cyber Direct is implemented by the EU Institute for Security Studies and is funded by the European Union.

**Disclaimer.** The author alone is responsible for the text and for any inaccuracies that may remain.

### SUGGESTED CITATION

Komaitis, Konstantinos (2026) Shaping Connectivity: The Invisible Governance of Internet Standards Diplomacy. Research paper, EU Cyber Direct, November 2026.

*This publication has been produced in the context of the EU Cyber Direct (EU Cyber Diplomacy Initiative) project with the financial assistance of the European Union. The contents of this document are the sole responsibility of the author and can under no circumstances be regarded as reflecting the position of the European Union or any other institution.*

ISBN 978-92-9462-533-5 · Catalogue number QN-01-26-010-EN-N · DOI 10.2815/2399795

Reproduction is authorised provided the source is acknowledged.

# Executive summary

Internet standards are among the most consequential yet least visible instruments of power in the digital age. Commonly perceived as technical specifications that enable devices, networks, and applications to communicate, standards do far more than ensure interoperability. They shape how data flows, how security is implemented, how users interact online, and increasingly, how political values, economic interests, and governance models are embedded into the architecture of the digital environment. In doing so, standards operate upstream of regulation, influencing policy outcomes long before governments or legislatures have an opportunity to intervene.

As digital technologies become central to economic competitiveness, national security, and geopolitical influence, standard-setting has evolved from a largely technical exercise into a strategic domain of international governance. Decisions taken in standards bodies increasingly affect market access, supply chain resilience, cybersecurity, privacy protections, and the future direction of emerging technologies such as artificial intelligence, digital identity systems, and next-generation telecommunications networks. Standards therefore determine not only how technologies function, but also who benefits from them and whose values are reflected in their design.

The institutions responsible for developing these standards are diverse. They range from open, engineering-driven organisations such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), to industry-led consortia, formal standards development organisations such as the International Organization for Standardization (ISO), and intergovernmental bodies such as the International Telecommunication Union (ITU). Although many of these organisations present themselves as open and inclusive, meaningful participation requires significant technical expertise, financial resources, and long-term engagement. As a result, influence is unevenly distributed.

Large technology companies are particularly well positioned to shape standards development. Their ability to deploy dedicated teams of engineers, lawyers, and policy specialists across multiple standards bodies gives them a structural advantage in agenda-setting, drafting, coalition-building, and implementation. At the same time, many governments, particularly those in developing countries, struggle to sustain participation due to capacity constraints and resource limitations. Civil society organisations and human rights advocates frequently face similar barriers. Consequently, standards processes often reflect broader inequalities within the global digital ecosystem.

These dynamics have become increasingly geopolitical. The competition between the United States and China over the future of digital governance has extended into standards-setting processes, particularly in areas such as telecommunications, artificial intelligence, cloud infrastructure, and digital identity. Standards have become mechanisms through which states seek to project influence, support domestic industries, export governance models, and reduce strategic dependencies. At the same time, growing concerns over digital sovereignty have led governments to recognise standards as instruments of strategic autonomy and statecraft.

The European Union occupies a distinctive position within this evolving landscape. Unlike the United States, which has historically relied on private-sector leadership, or China, which has pursued a more state-directed approach, the European Union increasingly seeks to shape standards through a combination of regulation, market power, and coordinated international engagement. European initiatives such as the Cyber Resilience Act, the NIS2 Directive, the AI Act, and the European Standardisation Strategy demonstrate the growing recognition that standards and regulation are mutually reinforcing tools of governance. Yet the EU's influence remains uneven, and questions persist regarding how effectively European institutions and Member States coordinate their engagement across international standards bodies.

The implications extend well beyond economics and geopolitics. Standards are foundational to cybersecurity. They determine how systems authenticate users, secure communications, manage routing, and protect critical infrastructure. A secure standard can improve resilience across billions of devices and users; a flawed standard can create systemic vulnerabilities at global scale. Debates surrounding encryption, routing security, 5G infrastructure, software supply chains, and AI security illustrate how technical design decisions can become matters of national and international security.

Standards also have profound implications for human rights. Decisions regarding encryption, identity

management, accessibility, interoperability, and data handling directly affect privacy, freedom of expression, inclusion, and non-discrimination. Although standards bodies rarely frame their work in rights-based terms, the technical choices they make often determine the practical conditions under which rights are exercised online. In this sense, standards function as a form of hidden governance, embedding societal values into technical systems that shape everyday digital life.

For diplomats and policymakers, the central challenge is timing. Standards are typically developed long before their political significance becomes apparent. By the time governments engage through regulation, procurement, or diplomacy, many key architectural decisions have already been made. This creates a structural asymmetry in which technical communities and industry actors exercise influence early and continuously, while public institutions often participate later and more sporadically.

The report argues that addressing this gap requires a shift in perspective. Internet standards should no longer be viewed as peripheral technical artefacts, but as strategic instruments of governance. Effective engagement requires sustained technical capacity within governments, stronger coordination between policy and engineering communities, greater participation by underrepresented actors, and a clearer recognition that standards are now integral to cybersecurity, economic policy, trade, human rights, and international diplomacy.

Ultimately, the report advances a simple proposition: Internet standards constitute a hidden layer of digital power. They shape the architecture of the Internet and AI technologies, define the parameters of technological development, and increasingly influence the distribution of power in the international system. For governments seeking to shape the future of the digital world, engagement in standards development is no longer optional but a necessary condition for exercising influence in the twenty-first century.

# Contents


**Executive summary** 3

**1. Introduction: the hidden layer of digital power** 7

**2. Why standards are increasingly geopolitical** 10
- From technical coordination to strategic competition 10
- Security, dependency, and technological resilience 12
- Beyond geopolitics: competing visions of governance 13
- A new strategic arena 13

**3. Security implications of Internet standards** 14
- Security by design or security by retrofit 14

**4. Human rights implications of Internet standards** 18
- Architecture as governance 18
- The participation problem 20
- Human rights by design 21
- From technical infrastructure to rights infrastructure 22

**5. The institutional ecosystem of Internet standards** 23
- Overlapping jurisdictions and regime complexity 26
- Institutions as arenas of governance 27

**6. How standards get made: process, power, and participation** 28
- The myth of purely technical decision-making 28
- Agenda setting: deciding what matters 28
- Drafting as a form of power 29
- Consensus and the politics of agreement 29
- Coalition building and informal diplomacy 30
- Corporate influence and structural advantages 30
- The role of governments 30
- From technical process to governance process 31

**7. The inequalities embedded in standards fora** 32
- Why participation matters 32
- Expertise as a gatekeeper 33
- Geographic and economic disparities 33
- Corporate concentration and influence 33
- The challenge for civil society 34
- Standards and the digital divide 34
- Capacity building as a governance strategy 35
- Beyond inclusion: power and governance 35
- The legitimacy challenge 35
- Inequality as a governance issue 36

**8. EU cyber diplomacy and standards governance** 37
- Europe's distinctive approach 37

Standards as an instrument of strategic autonomy 38
The European standards architecture 38
Europe as a standards power 39
Recommendation: forging a cohesive European standards strategy 40

**9. Why policymakers and diplomats must engage** 41
The cost of late engagement 41
Standards as strategic infrastructure 41
Strengthening standards diplomacy 42
Strengthening European coordination 42
Supporting inclusive participation 43
Bridging technical and policy communities 43
A strategic agenda for European engagement 44

**10. Conclusion: standards and the future of digital governance** 45

**Endnotes** 47

**Annexes** 48
Abbreviations 48
Lexicon (key terms and concepts) 48

**List of figures**

Figure 1. Standards operate upstream of policy 8
Figure 2. Three approaches to standards power 12
Figure 3. Five arenas where standards shape security 17
Figure 4. Where standards decisions meet fundamental rights 21
Figure 5. From open communities to intergovernmental bodies 27
Figure 6. Where influence is exercised in standards-making 31
Figure 7. What skews participation in standards bodies 36
Figure 8. From rule-amplifier to standards power 40

# 1. Introduction: the hidden layer of digital power

Internet standards rarely attract political attention. They are generally viewed as the domain of engineers, technical committees, and specialised organisations responsible for developing the protocols that allow devices, networks, and applications to communicate with one another. To most policymakers, standards appear as technical artefacts: necessary for interoperability, but largely disconnected from questions of power, governance, or diplomacy.

This perception is increasingly outdated.

As digital technologies become central to economic competitiveness, national security, democratic resilience, and geopolitical influence, Internet standards have emerged as one of the most consequential yet least visible arenas of governance in the digital age. The technical rules that determine how information moves across networks, how systems authenticate users, how data is protected, and how digital services interact are no longer merely engineering decisions. They are choices that shape markets, distribute power, enable or constrain rights, and increasingly influence the strategic position of states in the international system.[1]

At their most basic level, Internet standards are shared technical specifications that allow the global Internet to function. Protocols such as the Hypertext Transfer Protocol (HTTP), the Domain Name System (DNS), Transport Layer Security (TLS), and the Internet Protocol (IP) provide the common language through which billions of devices communicate every day. Without these standards, the Internet would fragment into incompatible networks, unable to sustain the seamless interoperability that has made it a uniquely global system.

Yet standards do far more than enable connectivity. They shape the architecture of the digital environment itself. Decisions about encryption protocols influence the balance between privacy and surveillance; choices regarding digital identity frameworks affect how users are authenticated, tracked, and governed online; standards governing interoperability determine whether markets remain open and competitive or become increasingly concentrated around dominant platforms; and security standards define the resilience of critical infrastructure and influence the vulnerability of societies to cyber threats.

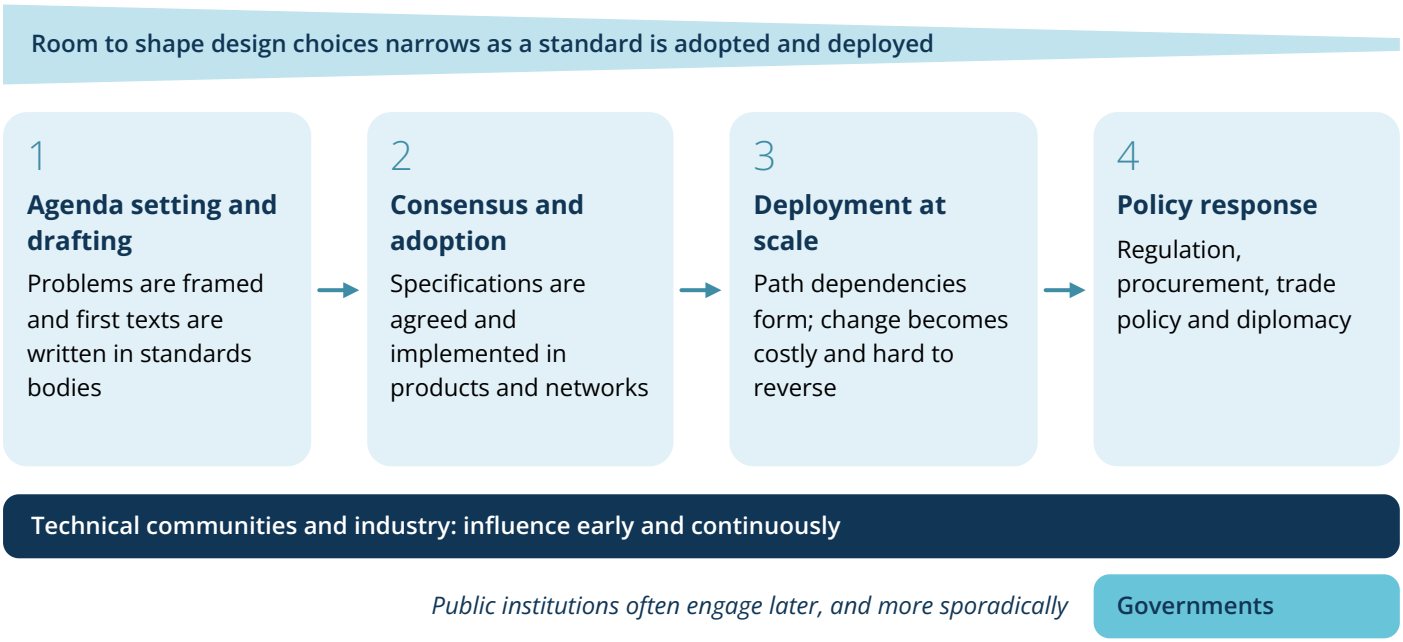
In this sense, standards operate upstream of policy. They establish the technical parameters within which future regulatory, economic, and political choices are made. By the time governments debate issues such as privacy, cybersecurity, platform governance, or artificial intelligence, many of the most consequential decisions may already have been embedded into technical architectures through standard-setting processes. Once widely adopted, standards create path dependencies that can be costly, difficult, and sometimes impossible to reverse.

This dynamic has profound implications for governance. Traditionally, states have exercised influence through legislation, regulation, procurement, trade policy, and diplomacy. Increasingly, however, influence is exercised earlier in the technological lifecycle. The actors that shape standards often help determine the future structure of markets, the distribution of technological capabilities, and the scope of policy options available to governments. Standards therefore function as a form of pre-regulatory power, allowing those who shape them to influence outcomes before formal political processes begin.

Today, standards are increasingly recognised as strategic assets. Governments understand that influence over standards can generate economic advantages, shape global markets, reduce technological dependence, and project political values beyond national borders. The growing competition between the United States and China over the future of digital governance has brought standards to the forefront of international politics,

FIGURE 1

## Standards operate upstream of policy




*By the time governments engage, many key architectural decisions have already been made (executive summary; Chapters 1 and 9).*

EU CYBER DIRECT

particularly in areas such as telecommunications, artificial intelligence, cloud computing, cybersecurity, and digital infrastructure. Standards bodies have become arenas where technical expertise intersects with industrial strategy, national security priorities, and competing visions of how the digital world should be governed.[2]

At the same time, the rise of digital sovereignty has encouraged governments to pay closer attention to the technical foundations of digital systems. Concerns regarding supply-chain security, technological dependency, strategic autonomy, and resilience have prompted policymakers to recognise that standards are not merely technical instruments but important components of statecraft. Increasingly, questions once confined to engineers are becoming matters of foreign policy, trade policy, and national security strategy.

The European Union occupies a particularly distinctive position within this landscape. While lacking the platform dominance of the United States and the state-directed industrial model pursued by China, the EU has emerged as an influential regulatory actor capable of shaping global technology governance through law, market size, and international coordination. European initiatives such as the AI Act, the Cyber Resilience Act, and the NIS2 Directive demonstrate an increasing awareness that regulation and standardisation are deeply interconnected. Yet the extent to which Europe can translate regulatory influence into sustained influence within international standards processes remains an open question.

The significance of standards extends beyond geopolitics and economics. Technical specifications increasingly shape the practical exercise of fundamental rights in the digital environment. Decisions concerning encryption, anonymity, accessibility, interoperability, and identity systems influence privacy, freedom of expression, inclusion, and non-discrimination. Similarly, standards are foundational to cybersecurity, determining how trust is established, vulnerabilities are mitigated, and resilience is built into critical digital infrastructure. The architecture of rights and security online is therefore often determined not in parliaments or courts, but in technical forums where design choices are negotiated and implemented.

Despite these far-reaching consequences, standards remain largely absent from mainstream policy discussions. Diplomatic efforts frequently focus on visible issues such as data governance, artificial intelligence, platform regulation, or cyber conflict, while overlooking the technical standards that underpin these debates. This disconnect creates a significant strategic blind spot. By the time policymakers engage, many of the parameters governing future choices may already have been established.

This report seeks to make visible this hidden layer of digital power. It examines how standards are developed, who participates in their creation, and how influence is exercised throughout the process. It analyses the growing geopolitical significance of standards, their implications for security and human rights, and the structural inequalities that shape participation in standards-setting institutions. Particular attention is given to the evolving role of the European Union and the challenges that standards governance poses for contemporary cyber diplomacy.

The central argument is straightforward. Internet standards are not merely technical specifications. They are instruments of governance, mechanisms of influence, and increasingly, strategic assets in international politics. Understanding who shapes them, how they are negotiated, and whose interests they reflect is therefore essential for anyone seeking to understand the future of digital power.

# 2. Why standards are increasingly geopolitical

For much of the Internet's early history, technical standard-setting was largely insulated from overt geopolitical competition. Standards were primarily developed by engineers, researchers, and technical communities focused on solving practical challenges related to interoperability, connectivity, and performance. Institutions such as the Internet Engineering Task Force (IETF) emerged from a culture that privileged technical merit, operational experience, and collaborative problem-solving. While political and commercial interests were never entirely absent, they remained secondary to the shared objective of building a global and interoperable network. That environment exists less and less.

Today, standards sit at the centre of international competition over technology, economic influence, and digital governance. As digital systems have become foundational to economic activity, critical infrastructure, military capabilities, and societal resilience, governments have increasingly recognised that standards are not merely technical instruments. They are mechanisms through which power is exercised, markets are structured, and governance models are projected across borders.

What was once viewed as a technical coordination function has evolved into a strategic arena where states, corporations, and international organisations compete to shape the future architecture of the digital world.

## From technical coordination to strategic competition

The growing geopolitical significance[3] of standards reflects a broader shift in the role of technology in international affairs. Digital technologies are no longer discrete economic sectors; they underpin virtually every domain of state activity, from communications and finance to energy, transportation, healthcare, and defence. As a result, influence over the technical foundations of these systems has acquired strategic value.

Standards determine how technologies interoperate, which firms gain market access, how security is implemented, and how future innovation occurs. They establish the rules that products and services must follow in order to participate in global markets. In doing so, they shape competitive advantage long before traditional policy instruments such as regulation or trade agreements enter the picture.

This is particularly important in emerging technological domains where standards remain unsettled. Decisions made today regarding artificial intelligence, cloud computing, digital identity, quantum communications, or next-generation telecommunications will influence technological trajectories for decades. Actors that successfully shape standards in these areas can gain significant economic, strategic, and political advantages.

Consequently, standards have become a form of pre-regulatory power. Rather than responding to rules established elsewhere, actors seek to influence the technical foundations upon which future rules will be built.

### *The United States: market power and multistakeholder governance*

The United States entered this competition with significant structural advantages. Many of the institutions that shaped the modern Internet emerged from American research networks, universities, and technology companies. The Internet's architecture was largely developed through organisations that emphasised open participation, technical expertise, and multistakeholder governance rather than formal state control. This model aligned closely with broader American preferences for market-driven innovation and private-sector leadership. As a result, US-based firms became deeply embedded within standards development processes. Companies such as Google, Microsoft, Apple, Amazon, Cisco, Meta, and numerous others maintain substantial

representation across standards bodies, often participating simultaneously in multiple organisations and working groups.

This ecosystem generates influence through several mechanisms. First, American firms possess significant technical expertise and implementation capacity. Second, they frequently control platforms and services that can accelerate the adoption of standards once they are developed. Third, they benefit from close connections between research institutions, standards communities, and commercial deployment.

Importantly, US influence has often been exercised indirectly. Rather than relying primarily on state intervention, influence has flowed through private-sector participation, market dominance, and the widespread adoption of technologies developed within American innovation ecosystems.

This does not mean the US government is absent from standards politics. Increasing concerns surrounding technological competition with China, supply-chain security, artificial intelligence, and critical infrastructure have prompted a more active governmental interest in standards strategy.[4] Nevertheless, the American approach remains fundamentally rooted in a multistakeholder model in which private actors play a leading role.

### *China: state coordination and strategic standardisation*

China has pursued a markedly different approach.[5] Recognising standards as a strategic instrument of industrial and geopolitical power, China has systematically expanded its engagement across international standards bodies over the past two decades. This effort has been closely linked to broader national strategies aimed at technological self-sufficiency, industrial upgrading, and global influence.

Unlike the more decentralised American model, China's approach combines state coordination with corporate participation. Government agencies, research institutions, and major Chinese technology firms frequently operate within broader strategic frameworks designed to align standards engagement with national priorities.

This approach has been particularly visible in telecommunications, where Chinese firms such as Huawei and ZTE have become influential participants in international standards processes. Similar efforts are increasingly apparent in areas such as artificial intelligence, smart infrastructure, industrial systems, cloud services, and digital identity.

The often-cited "China Standards 2035" initiative[6] has become a symbol of this broader strategy, although its significance is sometimes overstated. More important than any individual policy document is the underlying recognition that standards represent a mechanism for shaping future markets and governance structures. For China, influence over standards can generate multiple benefits simultaneously. It can support domestic firms competing internationally, reduce dependence on foreign technologies, promote Chinese technical approaches, and increase China's influence over the evolution of global digital infrastructure.

This has led many governments to view standards not merely as technical specifications but as instruments of strategic competition.

### *The European Union: between market leadership and strategic autonomy*

The European Union occupies a distinctive position within this geopolitical landscape. It has increasingly demonstrated an ability to shape global technology practices through legislation. Legislation such as the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA), the Digital Services Act (DSA), the

NIS2 Directive, the Cyber Resilience Act, and the AI Act have established Europe as a significant regulatory actor in the digital domain.

This regulatory influence extends into standards development. Many contemporary regulations depend upon technical standards for implementation. Compliance frameworks, security requirements, interoperability obligations, and conformity assessments frequently rely upon standards developed by European and international standards organisations. As a result, regulation and standardisation increasingly function as mutually reinforcing instruments of governance.

This creates a distinctive European model. Whereas the United States often influences standards through market power and China through strategic state coordination, the European Union increasingly shapes standards through a combination of regulatory authority, market access, and institutional engagement.

At the same time, Europe faces important constraints. Standards participation remains uneven across Member States; technical expertise is distributed unevenly; and coordination between national governments, regulators, industry actors, and standards organisations is often imperfect. Moreover, Europe continues to rely heavily on technologies, platforms, and infrastructures developed elsewhere. This creates an important strategic question for European policymakers: is the European Union primarily a rule-shaper, a rule-taker, or something in between?

The answer increasingly appears to be that Europe functions as a rule-amplifier. The EU may not always originate technical standards, but it frequently influences their adoption, implementation, and global diffusion through its regulatory and market power. Whether this will remain sufficient in an era of intensified technological competition remains an open question.

FIGURE 2

## Three approaches to standards power

| | **United States**<br>Market-driven | **China**<br>State-coordinated | **European Union**<br>Rule-amplifier |
|---|---|---|---|
| MAIN LEVER | Market power and the global adoption of its technologies | State coordination aligned with national strategy | Regulatory authority and access to its market |
| WHO LEADS | Private firms, within a multistakeholder model | State agencies, research institutes and major firms | EU institutions, regulators and standards bodies |
| HOW INFLUENCE TRAVELS | Indirectly, through participation and deployment at scale | Systematic engagement across international bodies | Regulation that relies on standards to be implemented |

*The EU may not always originate standards, but it shapes their adoption and diffusion (Chapter 2).*

EU CYBER DIRECT

## Security, dependency, and technological resilience

The geopolitical significance of standards is also driven by growing concerns about security and technological dependency.

Standards determine how systems communicate, authenticate users, secure information, and exchange data. They therefore influence the resilience of critical infrastructure and the vulnerability of societies to cyber threats.

The debate surrounding 5G provides a particularly revealing example.[7] What initially appeared to be a discussion about telecommunications equipment quickly evolved into a broader geopolitical dispute involving supply chains, national security, industrial policy, and standards governance. Questions concerning trust, resilience, and strategic dependence became inseparable from technical questions regarding network architecture and interoperability. Similar dynamics are now emerging in cloud infrastructure, artificial intelligence, semiconductors, software supply chains, and digital identity systems.

In each case, standards shape not only technical functionality but also strategic dependencies. States increasingly recognise that reliance on technologies developed elsewhere may create vulnerabilities that are difficult to address after deployment. Participation in standards development is therefore increasingly viewed as a means of reducing strategic risk and enhancing resilience.

## Beyond geopolitics: competing visions of governance

At its core, the geopolitical contest over standards is not simply a struggle for market share or technological leadership. It also reflects competing visions of governance.

Debates over standards often mirror broader disagreements about the relationship between states, markets, and individuals. Questions concerning privacy, security, interoperability, identity, content governance, and data access frequently reveal underlying differences in political values and institutional preferences.

The tension between multistakeholder and multilateral governance illustrates this dynamic particularly clearly. While some actors emphasise open participation and private-sector leadership, others favour stronger state involvement and intergovernmental oversight. These competing approaches increasingly shape debates within standards organisations and influence broader discussions about the future governance of the digital environment.

As a result, standards bodies have become more than technical forums. They are now spaces where competing models of digital order are negotiated, contested, and translated into operational systems.

## A new strategic arena

The growing geopolitical significance of standards does not mean that technical considerations have become secondary. Technical expertise remains essential to the development of effective and interoperable systems. However, technical expertise now operates within a broader environment in which economic interests, security priorities, industrial strategies, and political values are increasingly intertwined.

Standards bodies have consequently become arenas where multiple forms of power intersect. Engineers, corporations, governments, regulators, and international organisations all participate, bringing different priorities and different visions of the digital future.

The result is that standard-setting is no longer simply a process of technical coordination. It has become a strategic arena where economic competitiveness, technological leadership, security interests, and competing models of digital governance are actively contested. Understanding this transformation is essential for policymakers seeking to navigate an international environment in which technical decisions increasingly carry geopolitical consequences.

# 3. Security implications of Internet standards

Internet standards are foundational to the security of the digital ecosystem. They determine how systems communicate, how trust is established between devices and networks, how data is protected in transit, and how vulnerabilities are mitigated across interconnected infrastructures. Security is therefore not simply an additional feature layered onto technical systems after deployment; it is often embedded directly into the standards that govern their operation.

For policymakers, this has important implications. A widely adopted standard functions as a force multiplier. When security is built into a standard, protection can be extended across billions of devices, users, and services. When vulnerabilities are embedded within a standard, the resulting risks can likewise scale globally. Because standards operate at the architectural level, their security consequences are often more systemic and enduring than those associated with individual products or services.

The critical question is therefore not simply whether standards are secure, but how security considerations are incorporated into standards development and whose priorities shape those decisions.

## Security by design or security by retrofit

Many of the Internet's foundational protocols were developed during a period when security concerns differed significantly from those of today. Early Internet designers prioritised connectivity, reliability, and interoperability, often assuming a relatively trusted network environment composed primarily of academic institutions, research organisations, and government agencies.

As the Internet expanded into a global public infrastructure, these assumptions became increasingly problematic. Several core protocols were not originally designed with strong authentication, encryption, or integrity protections. As a result, security mechanisms often had to be added after deployment rather than incorporated from the outset. Retrofitting security into globally deployed systems has proven difficult, costly, and sometimes only partially successful.

This experience has produced one of the most important lessons in Internet governance: security considerations must be part of standards development from the outset, rather than discussed only after widespread adoption. At the same time, however, in a decentralised system such as the Internet, it is impossible to anticipate and account for every potential security risk. A balance must therefore be struck. Preserving the agility and interoperability that underpin the Internet's functioning is just as important as enhancing its security and resilience.

### *Routing security: the hidden vulnerability of global connectivity*

One of the clearest examples of the relationship between standards and security can be found in Internet routing.

The Border Gateway Protocol (BGP), the Internet's routing system, determines how traffic moves between networks around the world. Every time users access a website, send an email, or connect to a cloud service, routing protocols help determine the path that information follows across multiple networks.

The original design of BGP prioritised functionality and scalability rather than strong authentication. As a result, networks generally trust routing information announced by other networks. This trust-based model has repeatedly created security challenges.

Over the years, numerous incidents[8] have demonstrated how incorrect or malicious routing announcements can redirect traffic away from its intended destination. Some incidents have resulted from accidental misconfigurations. Others have raised concerns about deliberate traffic interception or disruption. Because routing systems are highly interconnected, even a single erroneous announcement can have global consequences.

To address these vulnerabilities, the technical community developed mechanisms such as Resource Public Key Infrastructure (RPKI), which allows networks to verify the legitimacy of routing announcements. RPKI has achieved significant deployment in recent years[9], with routing security protections now covering a majority of Internet routes. Yet its implementation remains incomplete and uneven across networks and regions, illustrating a recurring challenge: designing a security standard is only the first step; achieving consistent deployment, operational maturity, and ecosystem-wide adoption is a far longer process.

For policymakers, routing security highlights an important reality. The resilience of the global Internet depends not only on technical innovation but also on sustained deployment and coordination across multiple stakeholders.

### *DNS security and the integrity of the Internet*

The Domain Name System (DNS) serves as the Internet's addressing mechanism, translating human-readable domain names into machine-readable IP addresses. Without DNS, users would need to remember numerical addresses for every service they access. DNS was designed for efficiency and scalability, but not initially for security.

This created opportunities for attacks that could redirect users to fraudulent websites, intercept communications, or manipulate traffic flows. In response, the technical community developed DNS Security Extensions (DNSSEC), which provide cryptographic mechanisms to verify the authenticity of DNS information. DNSSEC illustrates both the strengths and limitations of standards-based security.

On the one hand, it demonstrates how technical communities can identify vulnerabilities and develop effective solutions. On the other hand, deployment has been gradual[10], with only about 36% of global DNS queries currently DNSSEC-validated. The case underscores a broader lesson: security standards only improve resilience when they are implemented consistently across the ecosystem.

### *Encryption and the politics of trust*

Few standards issues better illustrate the intersection of security, rights, and politics than encryption. Encryption standards such as Transport Layer Security (TLS) underpin much of modern digital life. They protect communications, secure financial transactions, safeguard government services, and enable trust across digital systems. The widespread deployment of HTTPS, built upon TLS standards, has transformed the security baseline of the web by protecting communications against interception and manipulation.

Yet encryption has also become one of the most politically contested areas of standards development. Governments, law enforcement agencies, intelligence services, technology companies, and civil society organisations have frequently disagreed about the appropriate balance between privacy, security, and lawful

access. Proposals for exceptional access mechanisms, encryption backdoors, or alternative approaches to government access have generated intense debate.

What makes these disputes significant is that they are often resolved not solely through legislation, but through technical design choices embedded within standards. Once strong encryption becomes widely implemented, weakening it becomes considerably more difficult. Conversely, standards that permit exceptional access can introduce systemic vulnerabilities that affect all users.

The debate therefore illustrates a broader principle: technical standards frequently determine the practical boundaries within which policy choices can operate.

### *5G and the securitisation of standards*

The global debate surrounding 5G networks provides perhaps the clearest example of how standards have become intertwined with geopolitics and national security. Initially, 5G was seen as a technical evolution in telecommunications. In practice, however, debates surrounding 5G quickly expanded into broader concerns regarding supply chains, strategic dependence, industrial policy, and geopolitical competition.

Standards played a central role in this process. Participation in organisations such as the 3rd Generation Partnership Project (3GPP), which develops mobile telecommunications standards, became increasingly viewed as a strategic activity rather than a purely technical one. Governments paid unprecedented attention to standards processes, recognising that technical decisions could influence market leadership, equipment deployment, and long-term infrastructure dependencies.

The controversy surrounding Huawei demonstrated how standards, security, and geopolitics have become deeply intertwined. Concerns about network integrity, state influence, supply-chain risk, and strategic vulnerability transformed what might once have been considered technical procurement decisions into matters of national security and foreign policy.[11]

The lesson extends beyond telecommunications. Future debates concerning artificial intelligence, cloud infrastructure, quantum technologies, and digital identity are likely to exhibit similar dynamics.

### *Supply chain security and software integrity*

Modern digital systems depend upon highly complex and globally distributed supply chains. Software applications increasingly incorporate components developed by multiple organisations, often across different jurisdictions. Hardware systems similarly rely upon intricate international production networks.

Standards play a crucial role in managing this complexity. They define how components interact, how software dependencies are documented, how updates are delivered, and how trust is established across supply chains. Increasingly, standards are being developed to improve software transparency, vulnerability management, and supply-chain resilience.

Recent cybersecurity incidents have highlighted the importance of these efforts. Attacks targeting software update mechanisms, third-party suppliers, and development environments have demonstrated how vulnerabilities within supply chains can create cascading risks across multiple organisations and sectors.[12]

As governments seek to improve resilience, standards are becoming a key policy instrument for establishing minimum security expectations across increasingly interconnected ecosystems.

FIGURE 3

## Five arenas where standards shape security

A widely adopted standard is a force multiplier: security built into it protects billions of devices and users, and a flaw embedded in it can scale just as far.

| DOMAIN | STANDARDS | THE SECURITY ISSUE | WHERE THINGS STAND |
|---|---|---|---|
| **Routing** | BGP, RPKI | Networks largely trust the routing announcements of other networks, so a single error can have global effects | RPKI now protects a majority of routes, but deployment remains uneven across networks and regions |
| **Naming** | DNS, DNSSEC | Designed for efficiency rather than security, leaving room to redirect users or manipulate traffic | About 36% of global DNS queries are DNSSEC-validated |
| **Encryption** | TLS, HTTPS | Competing claims of privacy, security and lawful access, often settled through design choices | Strong encryption is widely deployed; exceptional access would add systemic vulnerabilities for all users |
| **Mobile networks** | 5G, via 3GPP | Trust, supply-chain risk and strategic dependence | Participation in standards bodies is now treated as a strategic, not purely technical, activity |
| **Software supply chains** | Transparency and update standards | Compromised updates and suppliers can cascade across organisations and sectors | Standards are becoming a policy instrument for minimum security expectations |

*Designing a security standard is only the first step; consistent deployment across the ecosystem takes far longer (Chapter 3; RPKI and DNSSEC figures as reported in endnotes 9 and 10).*

EU CYBER DIRECT

### *From technical specification to strategic security asset*

As societies become increasingly dependent on digital infrastructure, the security implications of standards will continue to grow. Decisions regarding encryption, routing, software supply chains, telecommunications, digital identity, and artificial intelligence increasingly shape national resilience and international stability.

Standards should therefore be understood not merely as technical specifications but as strategic security assets. They determine how trust is established, how vulnerabilities are managed, and how resilience is built into the systems upon which modern societies depend.

For governments, the implication is clear: cybersecurity policy can no longer be separated from standards governance. The technical decisions made in standards bodies today help define the security environment of tomorrow.

# 4. Human rights implications of Internet standards

Internet standards are typically evaluated according to technical criteria such as interoperability, efficiency, scalability, and security. Yet the choices embedded within standards often have profound consequences for the exercise of fundamental rights in digital environments. Decisions made in technical forums influence how individuals communicate, access information, protect their privacy, establish identity, and participate in social, economic, and political life online.

Unlike legislation or constitutional frameworks, standards rarely articulate rights-based objectives explicitly. They are not drafted as instruments of public policy. Nevertheless, because standards define the technical architecture through which digital systems operate, they frequently shape the practical conditions under which rights are exercised. In many cases, they determine what is technically possible, what is easy, and what is difficult long before courts, regulators, or legislators become involved. For this reason, standards increasingly occupy a critical position at the intersection of technology, governance, and rights protection.

## Architecture as governance

The relationship between standards and rights begins with a simple observation: technology is not neutral in its effects. The design choices embedded within technical systems influence the behaviour of institutions, companies, and users. Standards determine how information flows, how systems interoperate, how users authenticate themselves, and how data is collected, stored, and transmitted. These decisions establish the architecture within which social and political activity takes place.

This does not mean that standards predetermine outcomes. Human rights ultimately depend upon legal frameworks, political institutions, and social practices. However, technical architectures can enable or constrain those frameworks in important ways. They establish the conditions under which rights protections must operate and can make certain policy objectives easier or more difficult to achieve. As digital systems become increasingly central to economic and social life, the governance significance of technical design has become impossible to ignore.

### *Privacy and the technical foundations of data protection*

Perhaps the clearest connection between standards and rights concerns privacy. Technical standards determine how data is generated, transmitted, processed, and secured. Decisions regarding encryption, metadata exposure, authentication mechanisms, data minimisation, and identifier management all influence the degree of privacy available to users in practice.

Encryption standards provide a particularly important example. Modern encryption protocols enable secure communications across the Internet, protecting users against interception, surveillance, and unauthorised access. Without these standards, many of the privacy protections associated with contemporary digital communications would be impossible to achieve.

At the same time, standards often determine how much information is exposed by default. Design choices concerning metadata, tracking mechanisms, device identifiers, and data exchange protocols can significantly affect the ability of individuals to control their personal information.

Importantly, these choices are often made at the architectural level. Once privacy-enhancing or privacy-reducing features become embedded within widely adopted standards, changing them can be difficult and costly. As a result, standards frequently establish the baseline upon which legal protections must subsequently operate.

This dynamic has become increasingly relevant within the European Union, where regulatory initiatives such as the General Data Protection Regulation (GDPR) rely heavily on technical standards and implementation frameworks to translate legal principles into operational practice.

### *Freedom of expression and access to information*

Standards also influence the practical exercise of freedom of expression and access to information.[13] The Internet's architecture was historically designed to support open communication across interconnected networks. Many of the standards underpinning the network reflect assumptions about interoperability, decentralisation, and end-to-end connectivity that have contributed to the Internet's openness.

At the same time, technical design choices can affect how information is distributed, discovered, and controlled. Identity-related standards illustrate this tension particularly clearly. Systems that permit anonymity or pseudonymity may facilitate participation by vulnerable groups, journalists, activists, and political dissidents. Conversely, systems that require strong identity verification may support accountability and security objectives but can also increase the risks associated with surveillance, profiling, or self-censorship.

Similarly, standards governing interoperability influence the structure of digital ecosystems. Open and interoperable systems can lower barriers to participation and facilitate information exchange. Closed or proprietary architectures may increase concentration and reduce user choice. The objective is not to suggest that one design choice is universally preferable. Rather, it is to recognise that technical decisions frequently carry implications for how rights are exercised in practice.

### *Accessibility, inclusion, and digital participation*

Standards play a critical role in determining who can participate effectively in digital environments. Accessibility standards developed through organisations such as the World Wide Web Consortium (W3C)[14] have significantly improved the usability of digital services for individuals with disabilities. Requirements concerning screen-reader compatibility, alternative text, keyboard navigation, and interface design have helped make digital environments more inclusive and accessible.

The importance of these standards extends beyond disability rights. Technical assumptions regarding bandwidth availability, device capabilities, language support, and connectivity requirements can also affect participation. Standards designed primarily around the needs of highly connected and technologically advanced environments may inadvertently create barriers for users in lower-resource settings.

This highlights a broader point about inclusion. Participation in digital environments depends not only on legal rights but also on the technical architectures through which services are delivered. Standards can either reduce barriers or reinforce existing inequalities depending on how they are designed and implemented. As digital systems become increasingly central to education, employment, healthcare, and public services, these considerations take on greater significance.

### *Identity, authentication, and the governance of individuals*

Few areas demonstrate the human rights implications of standards more clearly than digital identity. Identity systems are becoming increasingly important components of digital governance. They facilitate access to public services, financial systems, healthcare, education, and private-sector platforms. At the same time, they create new questions concerning privacy, autonomy, surveillance, and control.

Standards play a central role in determining how identity systems function. They influence whether identity is centralised or decentralised, whether users maintain control over credentials, how much information must be disclosed during authentication, and how activities can be linked across different systems.[15]

Different technical approaches can produce very different governance outcomes. Highly centralised identity architectures may improve efficiency and administrative coordination while simultaneously increasing the potential for monitoring and data aggregation. Decentralised approaches may strengthen user autonomy but create other operational and governance challenges. The significance of these choices extends beyond technical design. They reflect broader societal decisions about the relationship between individuals, institutions, and the state.

Increasingly, these debates are occurring not only in legislatures and regulatory agencies but also within standards organisations that define the technical foundations of identity systems.

### *Artificial intelligence, data standards, and non-discrimination*

The growing deployment of artificial intelligence introduces new dimensions to the relationship between standards and rights. Although standards bodies do not directly regulate algorithmic outcomes, they increasingly shape the technical frameworks within which AI systems are developed, evaluated, and deployed. Standards influence issues such as data quality, interoperability, testing methodologies, transparency mechanisms, documentation requirements, and risk management processes.

These technical choices can affect the ability of organisations to identify, measure, and mitigate discriminatory outcomes. For example, standards governing data quality and documentation may influence whether biases can be detected effectively. Standards related to auditing and evaluation can affect accountability mechanisms. Interoperability standards may influence transparency and oversight capabilities.

As AI systems become more deeply embedded within employment, education, finance, healthcare, and public administration, the standards underpinning these systems will increasingly shape questions of fairness, accountability, and non-discrimination. This is likely to become one of the most important areas of interaction between standards governance and human rights in the coming decade.

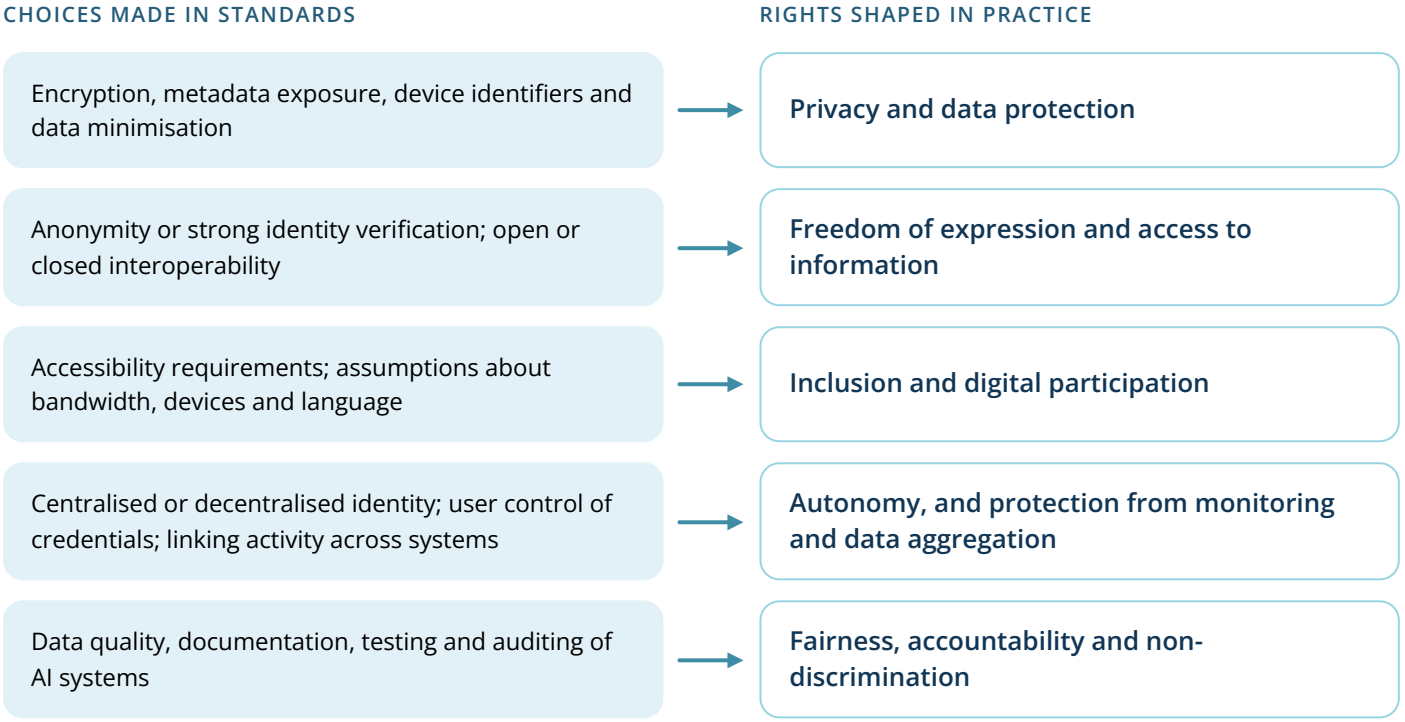
## The participation problem

A recurring challenge across standards development is the limited participation of human rights experts, civil society organisations, and public-interest advocates.

Most standards bodies were created to solve technical problems rather than address broader societal questions. Consequently, participation tends to be dominated by engineers, technical specialists, and corporate actors. While this expertise is essential, it can result in important social and rights-related considerations receiving less attention than technical performance, security, or commercial viability.

FIGURE 4

## Where standards decisions meet fundamental rights




*Standards do not replace law, but they frequently determine the terrain upon which law operates (Chapter 4).* EU CYBER DIRECT

This challenge is not unique to human rights issues. It reflects broader inequalities in standards participation, including disparities in resources, expertise, and institutional capacity. Nevertheless, the consequences can be significant. Decisions with important societal implications may be taken in forums where relevant expertise is underrepresented. Human rights concerns may only emerge after standards have already been widely adopted and deployed.

Addressing this challenge does not require transforming standards organisations into human rights institutions. It does, however, require greater awareness of the broader implications of technical design and stronger mechanisms for incorporating diverse perspectives into standards processes.

## Human rights by design

Growing awareness of these issues has led to increased discussion of "human rights by design" approaches to standards development. Such approaches seek to integrate consideration of rights implications into technical processes from the outset rather than treating them as afterthoughts. This can include human rights impact assessments, multidisciplinary review processes, greater participation from civil society organisations, and closer collaboration between engineers, policymakers, legal experts, and social scientists.

Importantly, this does not imply that every technical decision should become politicised. Rather, it reflects recognition that technical systems already produce political and social effects whether or not those effects are explicitly considered during development. The objective is therefore not to transform technical standards into policy instruments, but to ensure that those developing standards understand the broader consequences of the choices they make.

## From technical infrastructure to rights infrastructure

Internet standards are often described as the invisible infrastructure of the digital world. Increasingly, they can also be understood as part of its rights infrastructure. Among others, they influence how privacy is protected, how expression is exercised, how identities are managed, how accessibility is achieved, and how fairness is promoted within digital systems. They help determine the practical conditions under which individuals engage with technology and with one another.

For policymakers, this has important implications. Protecting rights in the digital age cannot be achieved solely through legislation, regulation, or judicial oversight. It also requires attention to the technical architectures that shape digital environments from the ground up.

Standards do not replace law, but they frequently determine the terrain upon which law operates. Understanding their role is therefore essential for anyone seeking to ensure that digital transformation remains compatible with democratic values, fundamental rights, and open societies.

# 5. The institutional ecosystem of Internet standards

Internet standards do not emerge from a single institution or governance process. Instead, they are developed through a complex and overlapping ecosystem of organisations that differ in structure, membership, authority, and decision-making processes. Some are open technical communities built around voluntary participation. Others are industry consortia, formal standards development organisations, or intergovernmental bodies. Together, they form a distributed governance architecture that shapes the technical foundations of the digital world.

This institutional diversity is one of the Internet's defining characteristics. It has contributed to innovation, interoperability, and resilience by preventing any single actor from exercising complete control over technical development. At the same time, it has created a fragmented governance environment in which influence is often difficult to trace and accountability can be uneven.

For policymakers, understanding where standards are made is as important as understanding the standards themselves. Different institutions embody different governance philosophies, distribute influence differently, and provide varying opportunities for participation by governments, companies, technical experts, and civil society organisations.

Unlike many traditional international governance domains, the Internet does not have a single treaty-based institution responsible for establishing global rules. Instead, governance is distributed across a network of organisations that address different layers of the technical stack. Some institutions focus on Internet protocols and network operations. Others develop standards for telecommunications, cybersecurity, software engineering, artificial intelligence, or digital identity. Their responsibilities frequently overlap, creating a governance environment characterised by cooperation, competition, and continual negotiation.

This institutional complexity reflects the Internet's historical evolution. Different technical challenges gave rise to different communities, each developing its own norms, procedures, and organisational cultures. As digital technologies expanded into new sectors, additional institutions emerged to address specialised domains. The result is not a hierarchical system but an ecosystem.

### *The Internet Engineering Task Force (IETF)*[16]

The Internet Engineering Task Force (IETF) remains one of the most influential standards organisations in the Internet ecosystem.

Established in the 1980s, the IETF develops many of the protocols that underpin the operation of the Internet, including standards related to routing, transport, security, email, and numerous other core functions. Its work has been fundamental to maintaining the interoperability of global networks.

The IETF is often cited as a leading example of multistakeholder governance. Participation is open to anyone willing to contribute, and individuals participate in their personal capacity rather than as formal representatives of governments or organisations. Decisions are generally reached through a culture famously described as "rough consensus and running code", reflecting a preference for practical implementation and broad agreement over formal voting.

This approach has contributed significantly to the Internet's technical success. It has enabled rapid innovation, encouraged experimentation, and fostered a strong engineering culture focused on interoperability and operational effectiveness.

At the same time, participation is not as open in practice as it appears in theory. Effective engagement requires significant technical expertise, sustained involvement, and substantial time commitments. As a result, participation is often dominated by individuals affiliated with major technology companies, research institutions, and well-resourced organisations. The IETF illustrates that formal openness does not necessarily guarantee equitable participation.

### *The World Wide Web Consortium (W3C)*[17]

The World Wide Web Consortium (W3C) develops standards for the World Wide Web, including technologies related to web browsers, accessibility, user interfaces, and web applications.

Founded by Sir Tim Berners-Lee, the inventor of the World Wide Web, the W3C has played a central role in ensuring the interoperability and openness of the web. Standards such as HTML, CSS, and numerous accessibility guidelines have emerged through its processes.

Compared with the IETF, the W3C operates through a more structured membership model involving companies, academic institutions, governments, and civil society organisations. It has often been particularly influential in areas where technical design intersects with public policy concerns, including privacy, accessibility, and digital inclusion. Although dominated by US technology companies, the W3C continues to be an important body for setting the standards for the web, the user-facing layer of the Internet.

### *The Internet Corporation for Assigned Names and Numbers (ICANN)*[18]

Although not primarily a standards organisation, the Internet Corporation for Assigned Names and Numbers (ICANN) occupies a central position within the Internet governance ecosystem.

ICANN coordinates critical resources such as domain names and IP address allocation systems that are essential for the operation of the global Internet. Its governance model has frequently been presented as a prominent example of multistakeholder governance, bringing together governments, private-sector actors, technical experts, and civil society organisations within a common institutional framework.

Because control over naming and addressing systems has important political, economic, and security implications, ICANN often serves as a focal point for broader debates regarding Internet governance, legitimacy, and international oversight.

### *ISO and IEC: formal international standardisation*

The International Organization for Standardization (ISO)[19] and the International Electrotechnical Commission (IEC)[20] occupy a different position within the standards ecosystem. Unlike organisations such as the IETF, which are rooted in open technical communities, ISO and IEC operate through national standards bodies. Participation is generally mediated through national delegations, creating a governance model that more closely resembles traditional international institutions.

These organisations develop standards across an enormous range of sectors, including information technology, cybersecurity, artificial intelligence, industrial systems, and digital infrastructure. Their influence is substantial because many governments, regulators, procurement authorities, and certification frameworks rely

upon ISO and IEC standards. In many cases, compliance with these standards becomes effectively mandatory for organisations seeking access to particular markets or regulatory environments.

The increasing importance of cybersecurity and artificial intelligence has further elevated the role of ISO and IEC in digital governance.

### *The International Telecommunication Union (ITU)*[21]

No institution better illustrates the geopolitical dimensions of standards governance than the International Telecommunication Union (ITU).

Founded in 1865 and now a specialised agency of the United Nations, the ITU predates the Internet itself. Historically, it played a central role in coordinating international telecommunications networks, spectrum management, and technical interoperability across national systems. Today, the ITU remains one of the most influential institutions in global digital governance.

Unlike the IETF or W3C, the ITU is fundamentally an intergovernmental organisation. States occupy the central position within its governance structure, although private-sector entities, technical experts, and other stakeholders also participate in various capacities.

This state-centric model distinguishes the ITU from many of the institutions that shaped the development of the modern Internet. For some governments, particularly those favouring stronger public oversight of digital systems, the ITU offers an attractive governance model because it places states at the centre of decision-making. For others, the organisation raises concerns about potential politicisation, bureaucratisation, or constraints on the openness and flexibility that have historically characterised Internet development. These differing perspectives have made the ITU a focal point for broader debates regarding the future governance of the digital environment.

### The ITU and geopolitical competition

The International Telecommunication Union (ITU) has increasingly become a venue through which states seek to shape the future architecture and governance of digital technologies. Far from being a neutral technical forum, the organisation has emerged as an arena where competing political visions of the Internet, artificial intelligence, and digital infrastructure are advanced through standards development and intergovernmental negotiations.

China's engagement within the ITU provides perhaps the clearest illustration of this trend. One of the most visible examples was the "New IP" initiative, a proposal introduced by Huawei and supported by Chinese actors within ITU-T discussions between 2019 and 2020. Framed as a next-generation networking architecture capable of supporting future applications such as industrial automation, holographic communications, and massive machine-to-machine connectivity, the proposal was also criticised by Internet governance experts for embedding greater centralisation and state control into the network architecture. Critics argued that the proposal reflected a top-down governance philosophy that differed fundamentally from the Internet's existing model of distributed control and voluntary technical coordination.[22]

Artificial intelligence has become another area in which China is seeking to expand its influence through international standards processes. Chinese policymakers have explicitly identified standards development as a strategic priority, both domestically and internationally. In recent years, Chinese government agencies and research institutions have accelerated efforts to develop AI standards covering foundation models, AI governance, risk assessment, testing methodologies, and sector-specific applications.[23] Chinese institutions

have also successfully advanced several AI-related standards within the ITU itself, including standards relating to foundation model platforms and large language model technologies. These developments reflect a broader strategy of ensuring that Chinese technical approaches and governance frameworks are represented in emerging global standards.

At the same time, longstanding debates over critical Internet resources continue to surface within ITU processes. A recurring issue concerns the management of Internet Protocol (IP) addresses. For more than two decades, some governments, particularly from parts of the Arab region, Africa, and other developing-country groupings, have periodically questioned whether the current system of IP address allocation adequately reflects principles of national sovereignty and equitable participation. Proposals seeking a greater governmental or intergovernmental role in the allocation and management of IP address resources have appeared repeatedly in ITU discussions and have often resurfaced in the lead-up to major ITU conferences, particularly the Plenipotentiary Conference, where member states submit proposals seeking to expand or clarify the organisation's mandate in Internet-related public policy matters. While none of these proposals has fundamentally altered the existing system, their continued reappearance demonstrates that questions surrounding control of critical Internet resources remain politically salient for a number of governments.[24]

These debates are not merely about standards or technical administration. They reflect a broader contest over who should exercise authority over the digital environment and through which institutions such authority should be exercised. At the centre of this contest are two competing governance traditions. The first is the multistakeholder model that has shaped much of the Internet's evolution. Under this approach, governments participate alongside technical experts, private-sector actors, civil society organisations, and academic institutions in open and collaborative decision-making processes. Authority is distributed among stakeholders rather than concentrated within states. The second is the traditional multilateral model associated with intergovernmental organisations, where states retain primary decision-making authority and governance is exercised through formal diplomatic processes. The ITU, as a treaty-based United Nations specialised agency, naturally embodies many features of this latter approach.

In practice, the distinction is not absolute and most institutions contain elements of both models. Nevertheless, many of the most consequential debates within the ITU can be understood as manifestations of this deeper tension between multistakeholder and state-centric approaches to digital governance. Standards bodies have consequently become important arenas where competing visions of the Internet's future are not only debated but increasingly institutionalised.

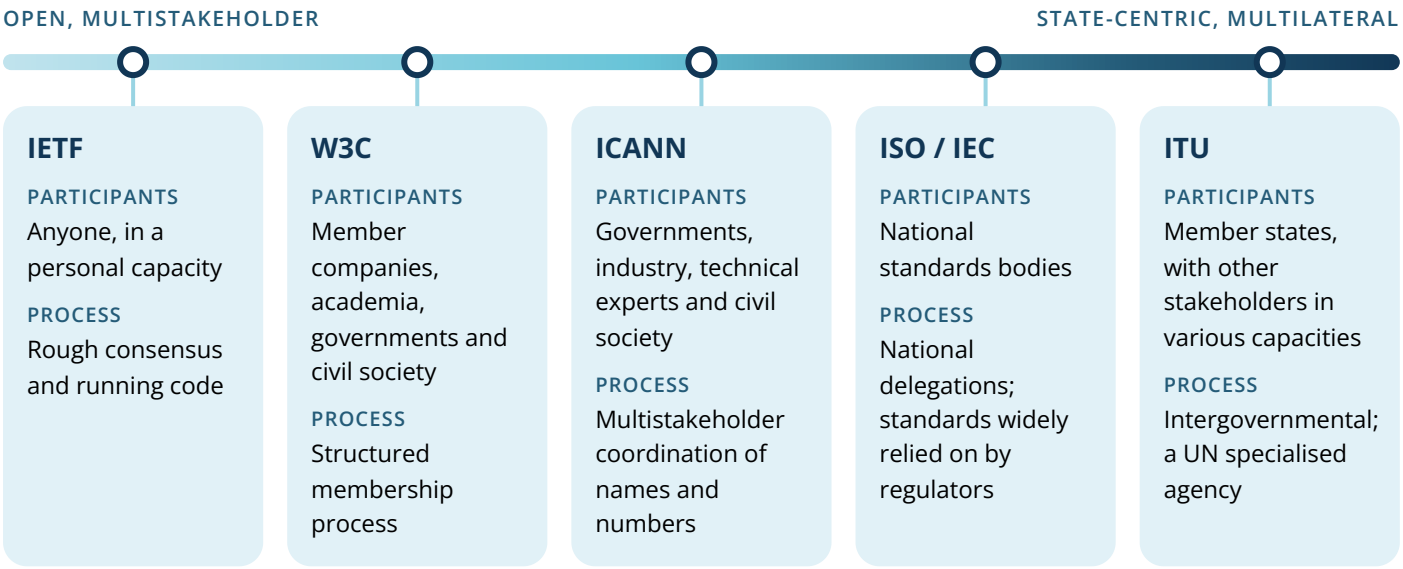
## Overlapping jurisdictions and regime complexity

The institutional landscape of standards governance is characterised by significant overlap. Multiple organisations may address similar issues from different perspectives. Cybersecurity standards, for example, can be found within the IETF, ISO, IEC, ETSI, ITU, and numerous industry-led initiatives. Artificial intelligence governance is similarly distributed across multiple institutions.

This overlap creates what is often described as regime complexity: a governance environment in which multiple institutions simultaneously address related issues without clear hierarchical relationships. Regime complexity can generate benefits. It allows experimentation, encourages innovation, and creates opportunities for diverse forms of participation. However, it can also create challenges. Organisations may duplicate efforts, adopt inconsistent approaches, or become venues for strategic competition among actors seeking favourable outcomes.

FIGURE 5

## From open communities to intergovernmental bodies




*Placement is indicative: most institutions combine elements of both models, and many debates within them reflect the tension between the two (Chapter 5).*

EU CYBER DIRECT

For policymakers, navigating this complexity requires a clear understanding of where influence is exercised and how decisions made in one forum may affect outcomes elsewhere.

## Institutions as arenas of governance

The institutions that develop Internet standards are often portrayed as neutral technical forums. In reality, they are governance arenas in which technical expertise, economic interests, political values, and strategic objectives intersect.

Different institutions distribute authority differently. Some privilege engineers and technical communities. Others provide stronger roles for governments, corporations, or national delegations. Each embodies assumptions about legitimacy, participation, and decision-making. These institutional differences matter because they influence who participates, whose voices are heard, and ultimately which standards are adopted.

Understanding the institutional ecosystem is therefore not simply an exercise in organisational mapping. It is essential to understanding how digital governance operates in practice. The standards that shape the Internet emerge not from a single centre of authority but from a diverse and contested landscape of institutions whose decisions increasingly carry global consequences.

# 6. How standards get made: process, power, and participation

Standards are often presented as the outcome of technical problem-solving. Engineers identify a challenge, develop a solution, test its effectiveness, and eventually agree upon a common specification that can be implemented across systems and networks. While this description captures part of the process, it obscures a more complex reality.

Standards development is not merely a technical exercise. It is also a social, institutional, and political process through which different actors seek to influence the design of technologies that may shape markets, security architectures, and governance outcomes for years to come. Technical merit remains essential, but it is only one factor among many that influence whether a proposal succeeds or fails.

Understanding how standards are made therefore requires examining not only formal procedures but also the dynamics of participation, coalition-building, negotiation, and influence that operate within standards organisations.

## The myth of purely technical decision-making

One of the enduring narratives surrounding standards development is that technical superiority ultimately determines outcomes. According to this view, standards emerge through objective evaluation of competing proposals, with the best technical solution prevailing through consensus. In practice, the process is considerably more complicated.

Technical quality matters enormously, and standards that fail to solve operational problems or cannot be implemented effectively are unlikely to gain widespread support. However, technical excellence alone rarely guarantees adoption. Standards must also attract sufficient support from participants, align with implementation realities, secure organisational backing, and often accommodate competing commercial, political, and institutional interests.

The challenge is particularly acute because standards development takes place before many technologies are fully mature. Participants are frequently making decisions under conditions of uncertainty, attempting to anticipate future technical requirements, market developments, and policy environments. As a result, standards development is best understood as a process of negotiated technical governance rather than purely objective engineering.

## Agenda setting: deciding what matters

Power in standards development often begins long before drafting starts. One of the most important forms of influence is determining which issues receive attention in the first place. Standards organisations have limited resources and finite capacity. Decisions about which problems are prioritised can significantly influence technological trajectories.

Agenda setting is frequently overlooked because it occurs at an early stage of the process. Yet it can have profound consequences. Actors that successfully define emerging challenges often gain a significant advantage in shaping subsequent discussions. They may frame problems in ways that favour particular technical

approaches, commercial interests, or policy objectives. Conversely, issues that fail to attract attention may remain unaddressed despite their broader significance.

This dynamic is particularly evident in emerging fields such as artificial intelligence, digital identity, cybersecurity, and quantum technologies, where standards processes are still evolving and future governance frameworks remain uncertain. The ability to identify emerging issues and mobilise support around them has therefore become an increasingly important source of influence.

## Drafting as a form of power

In most standards organisations, influence is exercised through drafting. Technical proposals do not emerge automatically from collective discussion. They are written by individuals and organisations willing to invest time, expertise, and resources in developing detailed specifications. Those who draft documents often play a disproportionately important role in shaping the direction of debate.

This influence stems from a simple reality: discussions usually begin with a text. The initial draft establishes terminology, assumptions, technical approaches, and boundaries for subsequent negotiations. Even when drafts are extensively revised, their authors often retain significant influence throughout the process because they possess detailed knowledge of the proposal and can respond effectively to objections or alternative approaches.

Consequently, organisations capable of dedicating personnel to sustained drafting efforts often enjoy structural advantages. Large technology companies are particularly well positioned in this regard. Many maintain dedicated standards teams whose primary responsibility is to participate in standards development, draft proposals, coordinate engagement across multiple forums, and support implementation efforts. Governments, academic institutions, and civil society organisations frequently struggle to match this level of sustained participation.

## Consensus and the politics of agreement

Most standards bodies avoid majority voting whenever possible. Instead, they emphasise consensus-based decision-making. This reflects a practical reality: standards only succeed if they are adopted. A technically excellent standard that lacks support from key implementers may never achieve meaningful deployment.

Consensus, however, should not be confused with unanimity. In practice, consensus often involves compromise, accommodation, and negotiation among participants with different priorities. Actors may support a proposal despite reservations because they view it as preferable to available alternatives. Others may accept modifications in exchange for concessions elsewhere.

This process can be highly productive. Consensus encourages dialogue, reduces fragmentation, and often improves technical outcomes by incorporating diverse perspectives. At the same time, consensus processes can create opportunities for strategic behaviour. Well-resourced participants may be better positioned to sustain long negotiations, attend multiple meetings, respond to technical objections, and build support across different stakeholder groups. Influence therefore depends not only on formal voting rights but also on the capacity to participate consistently over time.

## Coalition building and informal diplomacy

Much of the politics of standards development occurs outside formal meetings. Participants frequently build coalitions around shared technical approaches, commercial interests, policy objectives, or strategic priorities. These coalitions can be temporary or long-lasting, formal or informal, but they often play a decisive role in shaping outcomes.

Technology companies may coordinate around common implementation strategies. Governments may align around regulatory objectives. Regional groups may seek common positions on emerging technologies. Technical experts may collaborate around particular architectural principles.

The resulting interactions often resemble diplomatic negotiations more than traditional engineering discussions. Participants engage in persuasion, compromise, alliance-building, and strategic coordination. Informal conversations, working relationships, and long-standing professional networks frequently influence outcomes alongside formal deliberations.

For diplomats entering standards processes for the first time, this reality can be surprising. Technical expertise remains indispensable, but successful participation also requires many of the skills associated with international negotiation.

## Corporate influence and structural advantages

The growing role of large technology companies is one of the defining characteristics of contemporary standards development. This influence does not necessarily result from formal authority. Instead, it stems largely from structural advantages in resources, expertise, and implementation capacity.

Major technology firms often employ large numbers of engineers who actively participate across multiple standards organisations. They can support long-term engagement, monitor parallel discussions, draft technical proposals, and test implementations at scale. Perhaps most importantly, they frequently control products, platforms, and services through which standards are deployed.

This creates a powerful feedback loop. Companies that participate in standards development can often influence implementation, while implementation experience can strengthen their position in future standards discussions. It would be misleading to suggest that corporate influence automatically determines outcomes. Standards organisations retain important procedural safeguards, and many proposals fail despite substantial backing. Nevertheless, resource asymmetries can significantly shape participation and influence.

Understanding these dynamics is essential for policymakers seeking to assess how standards governance operates in practice.

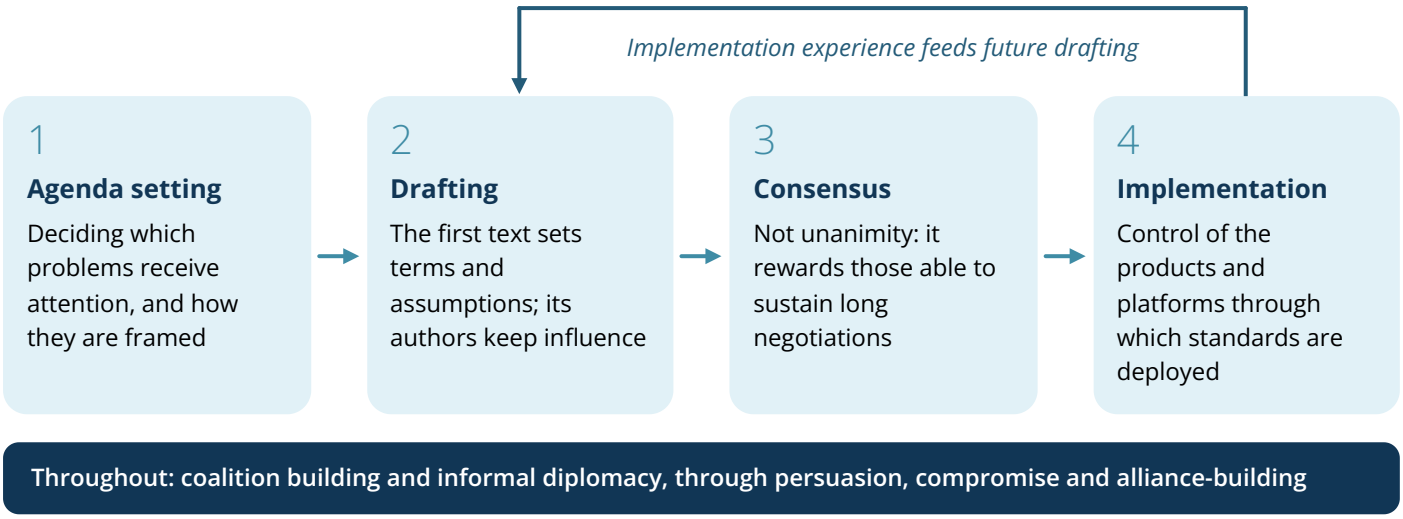
## The role of governments

Historically, many governments paid relatively limited attention to standards development, viewing it primarily as a technical domain best left to engineers and industry specialists. This approach is changing rapidly.

As standards become increasingly important for cybersecurity, artificial intelligence, telecommunications, critical infrastructure, and digital sovereignty, governments are becoming more active participants. Ministries, regulators, national standards bodies, and diplomatic missions are devoting greater attention to standards processes and their strategic implications.

FIGURE 6

## Where influence is exercised in standards-making




*Technical merit remains essential, but it is only one factor among many that decide whether a proposal succeeds (Chapter 6).*

EU CYBER DIRECT

Government engagement takes many forms. Some states participate directly through standards organisations. Others coordinate through national standards bodies, regulatory agencies, or international coalitions. Increasingly, governments also seek to align standards engagement with broader objectives related to industrial policy, economic competitiveness, and national security. This growing state involvement reflects recognition that standards development has become an important arena of international governance.

## From technical process to governance process

The development of standards is frequently portrayed as a technical process that occasionally intersects with politics. Increasingly, the opposite description may be more accurate.

Standards remain fundamentally technical. Effective specifications require engineering expertise, operational experience, and rigorous testing. Yet they are also governance processes through which competing interests, values, and strategic objectives are negotiated and embedded into technological systems.

The actors that participate in these processes influence far more than technical functionality. They help shape market structures, security architectures, implementation pathways, and the future scope of policy options.

Understanding how standards are made therefore requires moving beyond a narrow focus on technical specifications. It requires recognising standards development as a site of governance where expertise, resources, institutions, and influence interact to shape the future of the digital environment.

For diplomats and policymakers, this insight is increasingly important. Influence in the digital age is often exercised not only through laws and treaties, but through the technical processes that define how technologies are built in the first place.

# 7. The inequalities embedded in standards fora

Standards organisations are often described as open and inclusive institutions. Many allow participation from anyone willing to contribute, regardless of nationality, organisational affiliation, or formal status. This openness has been one of the defining strengths of Internet governance, helping to foster innovation, technical excellence, and broad collaboration across sectors and borders.

Yet openness in principle does not necessarily translate into equality in practice. Participation in standards development requires resources, expertise, institutional support, and long-term engagement. These requirements create significant barriers that shape who participates, whose voices are heard, and ultimately whose interests are reflected in technical outcomes. As a result, standards processes frequently reproduce broader inequalities that exist within the global digital ecosystem.

Understanding these inequalities is not simply a question of procedural fairness. It is essential to understanding how influence operates within standards governance and why certain actors consistently exercise greater authority than others.

## Why participation matters

The importance of participation extends beyond questions of representation. Standards determine security properties, interoperability requirements, implementation pathways, market access conditions, and increasingly the practical realisation of public policy objectives. They influence how technologies are designed, deployed, and governed. Actors that participate effectively in standards development therefore help shape the technical foundations upon which future economic, security, and governance outcomes depend.

Exclusion from standards processes can have tangible consequences. Countries that do not participate may find themselves implementing standards developed elsewhere. Companies that lack representation may struggle to influence requirements that affect their products and services. Civil society organisations that are absent from discussions may have limited opportunities to raise concerns related to privacy, accessibility, inclusion, or human rights. Participation matters because standards themselves matter. The question is therefore not simply who has a seat at the table, but who possesses the capacity to influence outcomes once they arrive.

One of the most significant barriers to participation is resources. Effective engagement in standards development requires sustained investment. Participants must attend meetings, monitor multiple working groups, review technical documents, contribute to drafting efforts, and maintain expertise across rapidly evolving technological domains. This work often occurs over years rather than months.

Large technology companies are generally well positioned to meet these requirements. Many maintain dedicated standards teams composed of engineers, lawyers, policy specialists, and technical strategists whose primary responsibility is engagement in standards processes. These teams can participate simultaneously across multiple organisations, coordinate positions internally, and sustain involvement throughout lengthy negotiations. Smaller firms, start-ups, academic institutions, and public-interest organisations frequently lack comparable capacity.

Governments face similar challenges. While some countries maintain sophisticated standards strategies supported by technical experts and dedicated institutions, many struggle to allocate sufficient personnel and

resources to sustained participation. This is particularly true in developing countries where competing policy priorities and limited budgets constrain engagement. The result is a structural imbalance that favours actors capable of maintaining a long-term presence across multiple standards fora.

## Expertise as a gatekeeper

Technical expertise is another important source of inequality. Standards discussions often involve highly specialised topics that require substantial knowledge and experience. Understanding the technical substance of proposals can be challenging even for experienced participants, particularly in areas such as cybersecurity, telecommunications, artificial intelligence, cryptography, and network architecture.

This expertise requirement serves an important function. Standards must be technically robust, and effective participation depends upon meaningful engagement with complex issues.

At the same time, expertise can operate as a gatekeeping mechanism. Individuals and organisations lacking specialised technical knowledge may struggle to contribute effectively, even when standards have significant implications for broader societal interests. Human rights advocates, policymakers, consumer groups, and representatives of smaller organisations often face difficulties engaging in highly technical discussions despite possessing relevant expertise in other domains.

This creates a recurring challenge for standards governance. Technical competence is essential, yet an excessive reliance on narrowly defined expertise can limit the diversity of perspectives represented within decision-making processes.

## Geographic and economic disparities

Participation inequalities also reflect broader global disparities. Standards development has historically been concentrated in North America, Europe, and parts of East Asia. Many of the institutions, companies, research centres, and technical communities that have shaped the Internet emerged within these regions, creating enduring advantages in expertise, networks, and institutional influence.

Participants from developing countries often face additional barriers. Travel costs, time zone differences, language requirements, limited institutional support, and restricted access to technical training can all affect participation. While virtual participation has reduced some obstacles, significant disparities remain.

These challenges are particularly important because standards increasingly affect countries regardless of whether they participate in their development. Digital infrastructure, telecommunications networks, cloud services, cybersecurity frameworks, and artificial intelligence systems are often deployed globally. Consequently, decisions taken within standards bodies can shape technological environments far beyond the communities directly involved in their creation. This creates a paradox: those most affected by standards are not always those best positioned to influence them.

## Corporate concentration and influence

The concentration of influence among large technology companies has become one of the most significant features of contemporary standards governance. This concentration is not necessarily the result of formal authority or procedural privilege. Rather, it emerges from the interaction of resources, expertise, implementation capacity, and sustained participation.

Major technology firms frequently employ large numbers of specialists dedicated to standards work. They possess extensive technical expertise, maintain relationships across multiple standards organisations, and often control platforms or products through which standards are implemented at scale. These advantages can translate into considerable influence over agendas, drafting processes, coalition-building efforts, and implementation pathways.

Importantly, corporate participation is not inherently problematic. Technology companies possess expertise that is often essential to effective standards development. Their operational experience, implementation capabilities, and understanding of technical challenges frequently contribute significantly to the quality of standards. The concern is not participation itself but concentration. When a relatively small number of actors possess disproportionate influence across multiple standards fora, questions arise regarding accountability and the distribution of decision-making authority.

## The challenge for civil society

Civil society organisations face a distinct set of challenges within standards governance. Many standards discussions have implications for privacy, accessibility, freedom of expression, inclusion, consumer protection, and human rights. Yet organisations working on these issues often lack the resources necessary for sustained participation in technical processes.

Unlike governments or corporations, civil society organisations frequently operate with limited budgets and small staffs. Maintaining engagement across multiple standards bodies can be difficult, particularly when discussions involve highly technical subjects requiring specialised expertise.

As a result, public-interest perspectives may be underrepresented relative to their broader societal importance. This challenge has become increasingly visible as standards development expands into areas such as artificial intelligence, digital identity, content authentication, and cybersecurity, where technical decisions frequently carry significant social and political implications.

## Standards and the digital divide

The inequalities embedded within standards development can reinforce broader patterns of digital inequality. Technical standards influence the design of products, services, and infrastructures used around the world. If participation is concentrated among actors from particular regions, industries, or economic contexts, resulting standards may reflect assumptions that do not fully account for different realities and needs.

For example, standards developed primarily within highly connected environments may assume levels of bandwidth, infrastructure reliability, technical capacity, or institutional maturity that are not universally available. Such assumptions can inadvertently create barriers for communities operating under different conditions.

This does not imply intentional exclusion. Rather, it reflects the reality that participants naturally bring their own experiences, priorities, and operational contexts into standards development. Broader participation can therefore improve not only legitimacy but also the quality and adaptability of standards themselves.

## Capacity building as a governance strategy

Addressing participation inequalities requires more than procedural openness. Many standards organisations have taken steps to reduce barriers through remote participation options, outreach initiatives, mentorship programmes, and fellowship opportunities. These efforts have helped broaden participation and diversify engagement.

However, sustainable inclusion ultimately depends on capacity. Countries, institutions, and organisations require the expertise, resources, and institutional support necessary to engage effectively over time. This often involves investments in technical education, standards training, research communities, and international cooperation.

Increasingly, capacity-building efforts are becoming a component of digital diplomacy and development policy. Governments and international organisations have recognised that meaningful participation in standards governance is linked to broader objectives related to digital development, economic competitiveness, and technological sovereignty. The ability to shape standards is increasingly understood as a strategic capability rather than merely a technical activity.

## Beyond inclusion: power and governance

Discussions about participation often focus on inclusion, diversity, and representation. These concerns are important, but they do not fully capture the significance of the issue.

At its core, participation in standards development is about power. Standards establish technical rules that shape markets, influence security architectures, define interoperability requirements, and affect future governance options. Actors that participate effectively gain opportunities to influence these outcomes while actors that remain absent are often left adapting to decisions made elsewhere. The distribution of participation therefore affects the distribution of authority within the digital ecosystem. Understanding standards governance requires recognising that technical processes are also mechanisms through which power is exercised, contested, and institutionalised.

## The legitimacy challenge

The long-term legitimacy of standards governance depends in part upon its ability to address these inequalities. Standards derive much of their authority from expertise, voluntary adoption, and broad acceptance. If participation becomes increasingly concentrated among a narrow set of actors, institutions may face growing questions regarding legitimacy, accountability, and representativeness.

This does not mean that all participants should have equal influence regardless of expertise or contribution. Technical competence remains essential to effective standards development. However, legitimacy increasingly requires that diverse stakeholders have meaningful opportunities to participate and that structural barriers do not systematically exclude particular communities, regions, or interests.

As standards become more consequential for economic policy, cybersecurity, artificial intelligence, and human rights, these questions are likely to become even more important.

## Inequality as a governance issue

The inequalities embedded within standards fora are often treated as secondary concerns compared to technical performance or institutional efficiency. In reality, they are central to understanding how standards governance operates.

Participation shapes influence. Influence shapes outcomes. Outcomes shape the technologies that increasingly structure economic activity, political authority, security, and social life.

FIGURE 7

### What skews participation in standards bodies

**Resources**
Meetings, drafting and monitoring over years; dedicated standards teams

**Expertise**
Specialised technical knowledge acts as a gatekeeper

**Geography**
Travel costs, time zones, language and access to training

**Concentration**
A small number of large firms present across many fora

**Most often left adapting to decisions made elsewhere:** developing countries, smaller firms, academic institutions and civil society organisations

*Barriers to participation in standards development, as discussed in Chapter 7.*

EU CYBER DIRECT

The challenge is therefore not simply making standards bodies more inclusive. It is ensuring that the governance processes shaping the future of digital technologies are sufficiently representative, legitimate, and resilient to reflect the diversity of interests affected by their decisions.

For policymakers, this requires recognising that standards development is not only a technical process but also a distributional one. The question of who participates is inseparable from the question of who governs.

# 8. EU cyber diplomacy and standards governance

The European Union has increasingly recognised that standards are not merely technical instruments but strategic tools of governance. As digital technologies become central to economic competitiveness, cybersecurity, industrial policy, and geopolitical influence, the ability to shape standards has emerged as an important component of European digital strategy.

This recognition reflects a broader shift in how the EU understands power in the digital age. Traditionally, European influence has been associated with regulation, market size, and normative leadership rather than technological dominance. While Europe has produced globally influential regulations, it has generally lacked the platform companies and technology ecosystems that have enabled the United States and China to exercise influence through market power and technological deployment.

Standards governance occupies an important space between these models. It offers the European Union an opportunity to shape the technical foundations of emerging technologies while reinforcing broader policy objectives related to security, competition, human rights, resilience, and strategic autonomy. As a result, standards are increasingly becoming an integral component of European cyber diplomacy.

## Europe's distinctive approach

The European Union occupies a unique position within the global standards landscape. Rather than relying primarily on technological dominance or state-led coordination, Europe has increasingly leveraged its regulatory authority and market power to shape digital governance. This approach reflects the reality that access to the European market is often essential for companies operating globally. Consequently, European regulatory requirements frequently influence technological practices well beyond the Union's borders.

This dynamic has become known as the "Brussels Effect"[25], the capacity of European rules to shape global behaviour because firms find it more efficient to adopt common standards across jurisdictions than to maintain multiple compliance frameworks.

Increasingly, this influence extends beyond regulation and into standardisation. Many contemporary European regulatory initiatives depend upon technical standards for implementation. As a result, the boundary between regulation and standardisation is becoming increasingly blurred.

The European Union has long relied on standards as a mechanism for implementing policy objectives. Under the so-called "New Legislative Framework",[26] European legislation often establishes broad requirements while technical standards provide detailed implementation pathways. This model allows policymakers to define desired outcomes while enabling technical communities to develop specific solutions.

Historically, this approach has been used across a wide range of sectors. In the digital domain, however, its significance has grown substantially. Recent European initiatives demonstrate the increasingly close relationship between regulation and standards governance:

- The NIS2 Directive strengthens cybersecurity obligations across critical sectors and relies heavily on technical standards and risk-management frameworks.
- The Cyber Resilience Act (CRA) establishes cybersecurity requirements for digital products and services while creating significant demand for harmonised standards capable of translating legal obligations into operational practices.

- The AI Act depends on standards to support conformity assessments, risk evaluation, transparency requirements, and implementation mechanisms.
- The Data Act, Digital Markets Act, and Digital Services Act similarly create incentives for interoperability and technical coordination that are likely to influence future standards development.

## Standards as an instrument of strategic autonomy

The growing importance of standards is closely linked to European discussions regarding strategic autonomy and digital sovereignty. Over the past decade, concerns regarding technological dependence, supply-chain resilience, cybersecurity vulnerabilities, and geopolitical competition have encouraged policymakers to reassess Europe's position within global technology ecosystems.

The central concern is not isolation or technological self-sufficiency. Rather, it is the ability to maintain meaningful agency in an increasingly interconnected digital environment. Standards play an important role in this context. Participation in standards development provides opportunities to shape the conditions under which technologies evolve and are deployed.

For Europe, this has become particularly important in areas such as:

- Artificial intelligence
- Telecommunications infrastructure
- Cloud computing
- Cybersecurity
- Semiconductors
- Digital identity
- Industrial Internet of Things systems

In each of these domains, standards influence not only technical performance but also strategic dependencies.

The ability to contribute to standards development is increasingly viewed as part of Europe's broader effort to strengthen resilience and reduce vulnerabilities without undermining openness and international cooperation.

## The European standards architecture

Europe possesses one of the most developed regional standardisation systems in the world. Three organisations occupy central positions within this framework:

### *ETSI*

The European Telecommunications Standards Institute (ETSI) plays a particularly important role in telecommunications, cybersecurity, digital infrastructure, and emerging technologies.

ETSI's influence extends well beyond Europe. Through its participation in global standards processes and its relationships with international organisations, ETSI often serves as a bridge between European policy objectives and international technical development.

The organisation has been particularly influential in areas such as mobile communications, network security, identity systems, and next-generation connectivity.

### *CEN and CENELEC*

The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) support standards development across a broad range of sectors relevant to digital transformation.

As cybersecurity, artificial intelligence, and digital technologies increasingly intersect with traditional industrial systems, the role of these organisations continues to expand. Together, ETSI, CEN, and CENELEC form a critical institutional infrastructure connecting European regulation, industry, and international standards processes.

### *ENISA*

Although not a standards development organisation, the European Union Agency for Cybersecurity (ENISA) plays an increasingly important role within the European standards ecosystem.

ENISA contributes expertise, supports cybersecurity certification initiatives, and helps bridge policy and technical communities. Its growing involvement reflects the broader recognition that cybersecurity governance and standards governance are deeply interconnected.

## Europe as a standards power

The European Union has historically exercised a distinct form of power in digital governance. Rather than directly dominating technological markets or dictating technical standards from the top down, the EU has relied on its regulatory authority, market size, and institutional legitimacy to act as a global "rule-amplifier". Under this model, Europe transforms technical standards into globally significant governance mechanisms through downstream mechanisms such as procurement, certification, and regulatory alignment.

However, in an era of intensifying, state-driven technological competition, relying primarily on amplification is no longer a sufficient strategy for maintaining digital sovereignty. The growing geopolitical importance of standards presents familiar, pressing risks: Europe remains heavily dependent on technologies developed elsewhere and must navigate a highly fragmented international environment characterised by competing governance models.

While European technical experts remain active participants across various international standard-setting organisations, the EU currently lacks a cohesive leadership role. This deficit stems from a critical vulnerability: Europe has not yet fully internalised or operationalised the geostrategic value that technical standards play in modern geopolitics. For much of the Internet's history, standards development existed at the margins of diplomacy; today, however, it serves as a primary arena in which international influence is exercised and strategic interests are advanced. Standards now directly dictate outcomes in cybersecurity, economic competitiveness, technological resilience, and artificial intelligence governance.

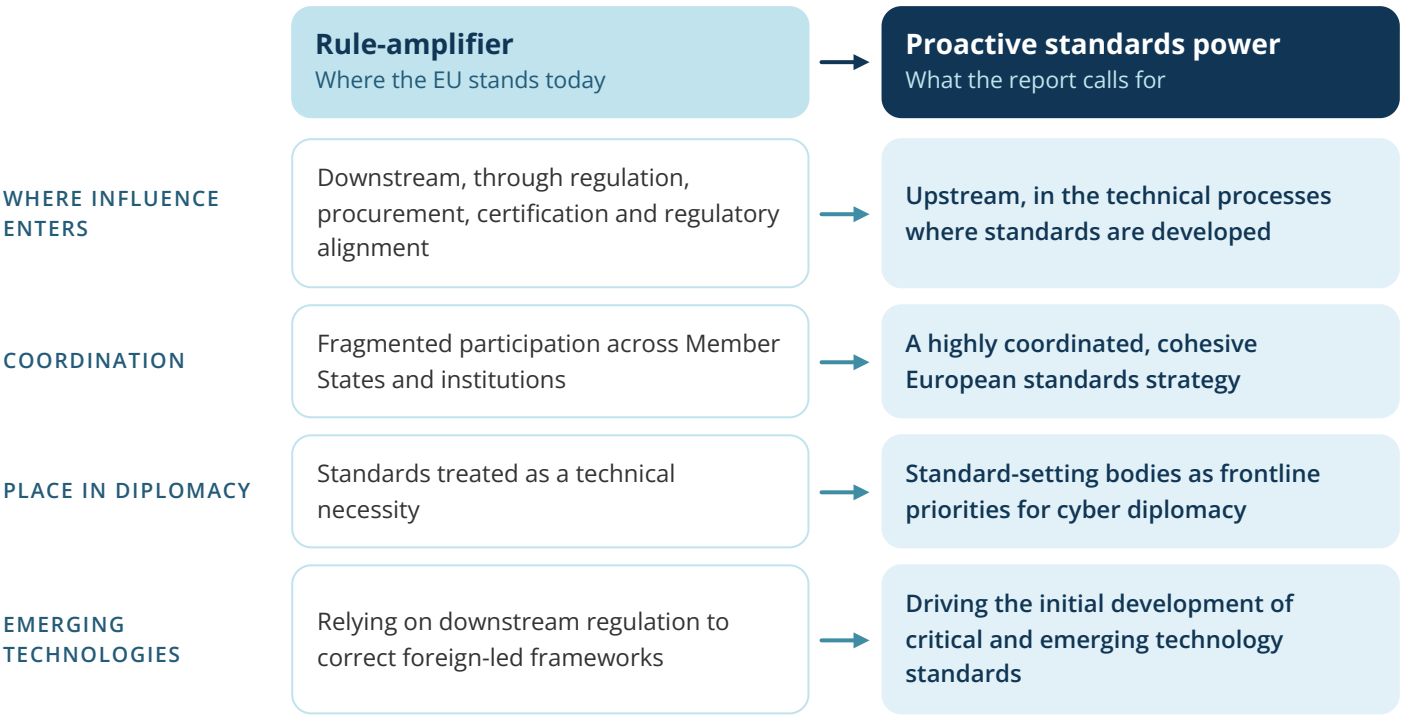
In contrast, systemic competitors, most notably China, have fully grasped this reality. China has successfully aligned its domestic industrial policies with a centralised, long-term global standards strategy, effectively using technical specifications as instruments of geopolitical influence and technological governance.

Despite these challenges, the current landscape provides a significant strategic opportunity. The European Union possesses formidable underlying assets: respected institutions, sophisticated regulatory frameworks, strong international partnerships, and extensive experience in balancing economic, security, and rights-based considerations. These assets uniquely position Europe to play a meaningful role in shaping the future

governance of digital technologies, provided it treats standards governance not merely as a technical necessity, but as a core diplomatic imperative.

FIGURE 8

## From rule-amplifier to standards power




*Europe's assets: respected institutions, sophisticated regulatory frameworks, strong international partnerships and experience balancing economic, security and rights-based considerations (Chapter 8).*

EU CYBER DIRECT

## Recommendation: forging a cohesive European standards strategy

For European cyber diplomats and policymakers, success will depend on moving beyond downstream regulatory leadership and securing sustained, effective participation in the technical processes where standards are actively developed. To safeguard its interests, Europe must step up and transition from a reactive rule-amplifier into a proactive standards power. This requires:

- **Strategic Unity:** Moving past fragmented participation towards a highly coordinated, cohesive European standards strategy that parallels the strategic intent of global peers like China.
- **Diplomatic Integration:** Elevating standard-setting bodies into frontline priorities for cyber diplomacy, recognising them as critical venues where the rules of the digital age are written.
- **Proactive Technical Leadership:** Actively driving the initial development of critical and emerging technology standards. This ensures Europe protects its digital sovereignty and strategic autonomy at the foundational layer, rather than relying on downstream regulation to correct foreign-led frameworks.

# 9. Why policymakers and diplomats must engage

Historically, a clear boundary separated the worlds of digital technology and statecraft. While lawmakers negotiated treaties, drafted legislation, and managed international relations, the foundational rules of the Internet were quietly written by engineers in niche technical forums. This traditional separation of duties has collapsed under the weight of the modern digital landscape.

Today, the technical blueprints established by standards organisations dictate the boundaries of core societal and geopolitical pillars. These specifications directly impact global economic strength, AI safety, robust supply chains, national defence, individual privacy rights, and cybersecurity. Because these engineering choices ultimately dictate the rules of daily life for global citizens, corporations, and governments, setting technical standards has evolved from a backroom task into a critical theater of geopolitical strategy. Consequently, for the European Union and its Member States, the focus has shifted entirely: the question is no longer whether they should intervene in this technical arena, but how they can maximise their strategic influence within it.

## The cost of late engagement

One of the central lessons emerging from this report is that standards often shape technological trajectories before policy debates fully emerge. Governments frequently become involved only after technologies have achieved widespread deployment. By that stage, policymakers are often responding to consequences rather than influencing underlying design choices. Regulatory interventions may still be possible, but they are often more difficult, more costly, and less effective than engagement during earlier stages of technological development.

This dynamic is particularly visible in areas such as social media, cybersecurity, digital platforms, and artificial intelligence, where standards and technical architectures frequently developed well before comprehensive regulatory frameworks were established. The result is a recurring asymmetry: standards bodies often make decisions early, while governments intervene later. Reducing this gap requires a more proactive approach to standards governance.

## Standards as strategic infrastructure

A second lesson concerns how standards are understood. Standards are often treated as technical specifications that support the operation of digital systems. While accurate, this description is incomplete. Increasingly, standards function as strategic infrastructure. They determine how trust is established across networks, how security is implemented, how interoperability is achieved, how identities are managed, and how emerging technologies are integrated into society. They also influence market structures, supply-chain resilience, and the practical implementation of regulatory objectives.

Just as governments invest in physical infrastructure because it supports economic and social development, they must increasingly view standards infrastructure as a strategic asset worthy of sustained attention and investment. Participation in standards development should therefore be understood as a long-term governance capability rather than a narrowly technical activity.

Effective participation in standards governance requires expertise. Governments cannot engage meaningfully in technical processes without individuals who understand both the technologies under discussion and the

institutions through which standards are developed. Yet many public administrations continue to face shortages of technical expertise, particularly in areas of emerging technologies.

Addressing this challenge requires investment in capacity building. Governments should support the development of technical expertise within ministries, regulatory agencies, diplomatic services, and national standards bodies. They should encourage closer collaboration between technical specialists and policymakers and create pathways that allow expertise to move more easily between government, academia, industry, and standards organisations.

Standards governance increasingly demands hybrid expertise that combines technical knowledge, policy understanding, and diplomatic skills. Developing such expertise will be essential for effective participation in future standards processes.

## Strengthening standards diplomacy

The growing strategic importance of standards has transformed them into a subject of diplomacy. Standards diplomacy is no longer limited to occasional participation in technical meetings. It increasingly involves coalition-building, international coordination, capacity building, and engagement across multiple governance institutions.

For European policymakers, this requires integrating standards considerations into broader diplomatic strategies. Diplomatic missions should develop greater awareness of standards-related developments. Cyber diplomats should engage more systematically with standards organisations. Ministries responsible for technology, trade, foreign affairs, cybersecurity, and industrial policy should strengthen mechanisms for information sharing and coordination.

The objective is not to politicise technical processes unnecessarily. Rather, it is to ensure that governments understand where important decisions are being made and possess the capacity to engage when strategic interests are implicated.

## Strengthening European coordination

The European Union possesses considerable strengths within standards governance, including strong institutions, respected standards bodies, significant regulatory influence, and a large internal market. However, these advantages do not automatically translate into influence.

Effective participation requires coordination among Member States, European institutions, standards bodies, regulators, industry, and civil society organisations. Without such coordination, European influence risks becoming fragmented across multiple institutions and policy domains.

Several priorities deserve particular attention.

First, information-sharing mechanisms between technical communities and policymakers should be strengthened. Important developments within standards organisations frequently remain invisible to broader policy communities until decisions have already advanced significantly.

Second, coordination between European standards bodies and international engagement strategies should be improved. Standards activities often intersect with trade policy, development cooperation, cybersecurity initiatives, and diplomatic engagement.

Third, Member States should continue investing in national standards capacities while strengthening mechanisms for collective action at the European level.

The challenge is not creating a single European position on every issue but ensuring that European participation is coherent enough to be effective.

## Supporting inclusive participation

As discussed in previous chapters, inequalities in standards participation affect governance outcomes. Many countries, smaller firms, academic institutions, and civil society organisations face significant barriers to effective engagement. These barriers can limit the diversity of perspectives represented within standards processes and contribute to the concentration of influence among a relatively small number of actors.

Addressing these challenges should be viewed not only as a question of fairness but also as a matter of governance quality. Broader participation can improve standards by incorporating different operational experiences, technical requirements, and societal perspectives. It can also strengthen the legitimacy of standards institutions and reduce the risk that important interests are systematically overlooked.

The European Union has long supported capacity-building initiatives within Internet governance and digital policy. Similar efforts should continue within standards governance, both within Europe and through international partnerships.

## Bridging technical and policy communities

One of the most persistent challenges in standards governance is the separation between technical and policy communities.

Engineers and standards experts often possess deep understanding of technological systems but limited engagement with broader policy debates. Policymakers may understand strategic objectives and regulatory concerns but lack visibility into technical processes occurring within standards organisations. This disconnect can produce misunderstandings, missed opportunities, and ineffective governance outcomes. Bridging these communities should therefore become a strategic priority.

Governments can encourage multidisciplinary engagement through joint training programmes, fellowships, secondments, research initiatives, and collaborative forums that bring together technical experts, diplomats, regulators, academics, and civil society organisations. The objective is not to eliminate differences in perspective but to improve mutual understanding and cooperation. The increasingly interconnected nature of digital governance makes such collaboration essential.

## A strategic agenda for European engagement

Taken together, the analysis presented in this report suggests four priorities for future European engagement.

1 **Build diplomatic and technical capacity**

Strengthen expertise within governments, diplomatic services, regulators, and national standards bodies. Develop pathways that combine technical knowledge with policy and diplomatic skills.

2 **Improve European coordination**

Enhance cooperation among Member States, European institutions, standards organisations, industry, and civil society. Ensure that standards governance is integrated into broader digital and foreign policy strategies.

3 **Support inclusive participation**

Reduce barriers to engagement through capacity building, training, funding mechanisms, and international partnerships. Promote broader participation across regions, sectors, and stakeholder communities.

4 **Treat standards as strategic infrastructure**

Recognise standards as foundational components of digital governance. Incorporate standards development into discussions concerning cybersecurity, industrial policy, artificial intelligence, digital sovereignty, and international cooperation.

# 10. Conclusion: standards and the future of digital governance

Standards are among the most powerful yet least visible mechanisms shaping the digital world. They determine how networks communicate, how devices interoperate, how security is implemented, how identities are managed, and increasingly how emerging technologies such as artificial intelligence are designed and deployed. Though often perceived as technical specifications, standards are in reality instruments of governance that influence economic outcomes, security architectures, human rights protections, and the distribution of power in the digital ecosystem.

This report has argued that the growing importance of standards reflects a broader transformation in the nature of governance itself. As societies become more dependent on digital infrastructure, the technical decisions embedded in standards increasingly shape the practical environment within which governments, businesses, and citizens operate. The question is no longer whether standards have political consequences; it is who participates in shaping them, through which institutions, and according to which values and priorities.

The geopolitical significance of standards has grown alongside intensifying competition over technology, security, and economic influence. Governments increasingly recognise that standards can shape markets, create dependencies, establish technological leadership, and influence the future direction of innovation. As a result, standards bodies that were once viewed primarily as technical fora have become important arenas of strategic competition. The debates taking place within these institutions are no longer solely about interoperability or engineering efficiency; they are increasingly about governance, influence, and the future structure of the digital order.

At the same time, standards remain fundamentally tied to some of the most pressing public policy challenges of our era. Security, privacy, accessibility, freedom of expression, digital identity, and artificial intelligence are all profoundly affected by technical choices made during standards development. These choices often establish the conditions under which laws, regulations, and public policies must subsequently operate. By the time policymakers become aware of a problem, many of the underlying technical decisions may already have been made.

This reality creates a challenge for governments and policymakers. Traditional approaches to governance frequently assume that public institutions intervene after technologies have emerged through regulation, oversight, or legislation. Standards governance reverses that logic. It is a site of anticipatory governance where decisions are often taken before technologies are widely deployed and before formal policy debates begin. Participation therefore offers a rare opportunity to shape technological trajectories at an early stage, when influence is still possible and before path dependencies become entrenched.

The report has also highlighted that standards governance is neither as neutral nor as inclusive as it is sometimes portrayed. While many standards organisations operate according to principles of openness and consensus, meaningful participation requires expertise, resources, institutional support, and sustained engagement. These requirements create structural inequalities that advantage some actors over others. Large technology companies, well-resourced governments, and established technical communities often enjoy significant influence, while many developing countries, smaller firms, academic institutions, and civil society organisations struggle to participate effectively. As standards become more consequential, addressing these

participation gaps becomes not only a matter of fairness but also a question of legitimacy and governance quality.

For the European Union, these developments carry particular significance. Europe has emerged as one of the world's most influential digital regulators, yet regulation alone is no longer sufficient to shape technological outcomes. Increasingly, the effectiveness of European policy depends on standards that translate legal principles into operational reality. The implementation of cybersecurity requirements, artificial intelligence governance frameworks, digital identity systems, and data governance regimes will all depend, to varying degrees, on standards developed through complex international processes.

This places standards governance squarely within the domain of European cyber diplomacy.

The European Union possesses important strengths. Its market size, regulatory influence, established standards institutions, and commitment to balancing innovation, security, and fundamental rights provide a strong foundation for engagement. Yet influence cannot be assumed. It requires sustained participation, strategic coordination, technical expertise, and the ability to engage effectively across the diverse institutions where standards are developed. In an environment characterised by growing geopolitical competition and increasingly consequential technical decisions, passive engagement risks leaving Europe in the position of responding to standards rather than helping to shape them.

The broader lesson of this report is that standards should be understood as part of the critical governance infrastructure of the digital age. They are not simply technical artefacts that emerge independently of politics and policy. They are mechanisms through which values are embedded, priorities are negotiated, and authority is exercised. The institutions that develop standards are therefore not peripheral to digital governance; they are among its most important sites.

For diplomats, policymakers, regulators, and political leaders, the implications are clear. Effective digital governance requires engagement not only with laws, regulations, and international agreements, but also with the technical processes that increasingly determine how technologies function. The future of cybersecurity, artificial intelligence, digital sovereignty, economic competitiveness, and fundamental rights will be shaped in part by decisions made within standards organisations today.

The Internet's history demonstrates that technical choices can have profound and enduring societal consequences. As the digital transformation accelerates and new technologies become embedded across every sector of society, the importance of those choices will only grow. Standards may remain largely invisible to the public, but they are increasingly central to the governance of the digital world.

# Endnotes


1 DeNardis, Laura. *The Global War for Internet Governance*. Yale University Press, 2014.

2 DeNardis, Laura and Mark Raymond. "Thinking Clearly About Multistakeholder Internet Governance". *Georgetown Journal of International Affairs*, 2013.

3 Rühlig, Tim et al. *Technical Standardisation, China and the Future International Order*. Swedish National China Centre, 2020.

4 United States International Cyberspace & Digital Policy Strategy: *Towards an Innovative, Secure and Rights-Respecting Digital Future*, 2024, U.S. Department of State, available at https://2021-2025.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/

5 Center for Intelligence Research and Analysis, *A New "Great Game"?: China's Role in International Standards for Emerging Technologies,* 2022, available at https://cira.exovera.com/wp-content/uploads/2022/08/NIST-Final-Report.pdf

6 Sheehan, Matt, Blumenthal, Marjory, Nelson, Michael. *Three Takeaways from China's New Standards Strategy,* Carnegie Endowment for International Peace, 2021, available at https://carnegieendowment.org/research/2021/10/three-takeaways-from-chinas-new-standards-strategy

7 Nocetti, Julien. *Europe and the Geopolitics of 5G: Walking a Technological Tightrope*, French Institute of International Relations, 2022, available at https://www.ifri.org/en/studies/europe-and-geopolitics-5g-walking-technological-tightrope

8 Madory, Doug. *A Brief History of the Internet's Biggest BGP Incidents*, NANOG, 2023, available at https://nanog.org/stories/articles/a-brief-history-of-the-internets-biggest-bgp-incidents/

9 Snijders, Job. *RPKI'S 2024 Year in Review,* RIPE Labs, 2025, available at https://labs.ripe.net/author/job_snijders/rpkis-2024-year-in-review/

10 *DNSSEC Validation by Country,* APNIC, 2026, available at https://stats.labs.apnic.net/dnssec

11 Bu, Q. *Behind the Huawei sanction: national security, ideological prejudices or something else?.* Int. Cybersecur. Law Rev. 2024, available at https://doi.org/10.1365/s43439-024-00112-6

12 Zhang, Xue & Ba, Xiaoya & Li, Bo. *Cyberattacks in supply chains: A multi-case study*. PLOS One. 21. 10.1371/journal.pone.0350010, 2026, available at https://www.researchgate.net/publication/405162216_Cyberattacks_in_supply_chains_A_multi-case_study

13 Kaye, David. *Speech Police: The Global Struggle to Govern the Internet*. Columbia University Press, 2019.

14 W3C Web Accessibility Initiative, available at https://www.w3.org/WAI/

15 UN Guiding Principles on Business and Human Rights, available at https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights

16 For more information, visit https://www.ietf.org/ (in particular RFC 8890: The Internet is for end users; RFC 3935: A mission statement for the IETF; RFC 7282: On consensus and humming at the IETF)

17 For more information, visit https://www.w3.org/

18 For more information, visit https://www.icann.org/

19 For more information, visit https://www.iso.org/home.html

20 For more information, visit https://www.iec.ch/homepage

21 For more information, visit https://www.itu.int/en/Pages/default.aspx

22 Internet Society, *Discussion Paper on the New IP Proposal* (2020), available at https://www.internetsociety.org/blog/2020/04/discussion-paper-now-available-about-the-new-ip-proposal/

23 China to develop more than 50 new standards for AI sector by 2026, Reuters, available at https://www.reuters.com/technology/artificial-intelligence/china-develop-more-than-50-new-standards-ai-sector-by-2026-2024-07-02/

24 Number Resource Organization (NRO), response to ITU proposals concerning IPv6 distribution and national sovereignty, available at https://www.nro.net/summary-of-nro-response-to-itu-comments-on-the-management-of-internet-protocol-ip-addresses/

25 Anu Bradford, *The Brussels Effect*, 107 Nw. U. L. Rev. 1 (2012), available at https://scholarship.law.columbia.edu/faculty_scholarship/271

26 For more information, visit https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

# Annexes

## Abbreviations

| | |
|---|---|
| **3GPP** | 3rd Generation Partnership Project |
| **AI** | Artificial Intelligence |
| **BGP** | Border Gateway Protocol |
| **CEN** | European Committee for Standardization (*Comité Européen de Normalisation*) |
| **CENELEC** | European Committee for Electrotechnical Standardization |
| **CRA** | Cyber Resilience Act |
| **CSS** | Cascading Style Sheets |
| **DMA** | Digital Markets Act |
| **DNS** | Domain Name System |
| **DNSSEC** | Domain Name System Security Extensions |
| **DSA** | Digital Services Act |
| **ENISA** | European Union Agency for Cybersecurity |
| **ETSI** | European Telecommunications Standards Institute |
| **EU** | European Union |
| **GDPR** | General Data Protection Regulation |
| **HTML** | Hypertext Markup Language |
| **HTTP** | Hypertext Transfer Protocol |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **ICANN** | Internet Corporation for Assigned Names and Numbers |
| **IEC** | International Electrotechnical Commission |
| **IETF** | Internet Engineering Task Force |
| **IP** | Internet Protocol |
| **ISO** | International Organization for Standardization |
| **ITU** | International Telecommunication Union |
| **ITU-T** | International Telecommunication Union Telecommunication Standardization Sector |
| **NIS2** | Network and Information Security Directive (specifically referring to the NIS2 Directive) |
| **RPKI** | Resource Public Key Infrastructure |
| **TLS** | Transport Layer Security |
| **W3C** | World Wide Web Consortium |

## Lexicon (key terms and concepts)

*Technical protocols and infrastructures*

**Border Gateway Protocol (BGP):** The Internet's routing system that determines the global path data traffic follows across interconnected networks.

**Domain Name System (DNS):** The Internet's addressing mechanism that translates human-readable domain names into machine-readable IP addresses.

**DNSSEC:** Cryptographic mechanisms developed to verify the authenticity and integrity of DNS information to prevent redirection attacks.

**Internet Standards / Technical Specifications:** Shared technical rules and protocols that enable devices, applications, and global networks to communicate seamlessly (ensure interoperability).

**New IP:** A next-generation networking blueprint proposed within the ITU-T by Chinese actors (2019-2020) intended to support advanced data demands but criticised for embedding top-down state control into network architectures.

**RPKI:** A routing security mechanism allowing networks to cryptographically verify the legitimacy of BGP routing announcements to prevent traffic interception or disruption.

*Governance and strategy frameworks*

**Anticipatory Governance:** A site or mechanism of decision-making (like standard-setting) where critical technological design choices are locked in long before the technologies are deployed or debated in formal political/regulatory venues.

**Brussels Effect:** The phenomenon where the European Union's regulatory requirements and market size effectively force global firms to adopt European standards across all jurisdictions for corporate efficiency.

**Multilateral Governance:** A traditional, state-centric international governance model associated with intergovernmental organisations (like the UN/ITU), where sovereign states hold primary decision-making authority.

**Multistakeholder Governance:** A distributed decision-making model where governments participate alongside technical experts, corporate entities, academic bodies, and civil society on an equal, open footing.

**Pre-Regulatory Power:** The operational advantage gained by actors who shape technical standards early in a technology's lifecycle, establishing parameters that dictate or constrain subsequent laws and regulations.

**Regime Complexity:** A fragmented governance environment where multiple distinct international institutions simultaneously manage overlapping policy domains without a clear hierarchical chain of command.

**Rule-Amplifier:** An actor (specifically the EU) that may not natively originate a technical standard but turns it into a globally impactful rule by mandating it downstream via regulatory frameworks, procurement rules, and certifications.

**Strategic Autonomy / Digital Sovereignty:** The capacity of a state or union (such as the EU) to maintain meaningful self-agency, reduce critical technological dependencies, and minimise supply chain vulnerabilities in a globally interconnected digital landscape.

AUTHOR

**Dr Konstantinos Komaitis**
Atlantic Council

EU CYBER DIRECT
The EU Cyber Diplomacy Initiative

Implemented by
euiss
European Union
Institute for
Security Studies

Funded by
the European Union