DOI: 10.66069/ojspub.26820805

Governing Trust: Cybersecurity Certification and Regulatory Power in the European Union and China

Xiaoyu Gu

University College London

Abstract: ***Cybersecurity certification has become an increasingly important mechanism for governing digital technologies and infrastructures. Although commonly understood as a technical process for evaluating security performance, certification increasingly determines which technologies, suppliers, and infrastructures are recognised as trustworthy. This article argues that cybersecurity certification should be understood as a form of governance infrastructure through which technological trust is institutionally produced. Building on research on regulatory power, standards governance, and digital sovereignty, the article develops a framework of technological trust governance centred on three dimensions: trust definition, trust verification, and trust diffusion. Through a comparative analysis of the European Union and China, the article identifies two distinct pathways through which regulatory power operates in digital governance. The European Union represents a model of market-mediated trust governance, where cybersecurity certification frameworks transform regulatory objectives into technical requirements and create incentives for external compliance through market access. China represents a model of state-coordinated trust governance, where cybersecurity standards are mobilised through institutional coordination, industrial alignment, and technological ecosystem embedding. The article contributes to debates on digital governance by demonstrating that competition over cybersecurity is not only a contest over technologies or standards, but also over the institutional authority to define and govern technological trust.***

Keywords: Cybersecurity certification; Regulatory power; Standards governance; Technological trust; Digital sovereignty; European Union; China.

1. INTRODUCTION

Cybersecurity certification has become an increasingly important mechanism for governing digital technologies and infrastructures. Traditionally understood as a technical process for assessing whether digital products and services satisfy predefined security requirements, certification is often presented as a neutral instrument for reducing uncertainty and improving confidence in complex technological systems. Yet the rapid institutionalisation of cybersecurity certification frameworks reveals a more political dimension. Certification systems increasingly determine not only whether technologies meet technical requirements, but also which technologies, suppliers, and infrastructures are recognised as trustworthy participants in digital markets. In this sense, cybersecurity certification has become an arena in which authority over technological trust is defined, institutionalised, and contested.

The growing importance of cybersecurity certification is particularly evident in the European Union and China, where digital security has become closely connected with broader questions of regulatory authority and technological governance. In the European Union, the Cybersecurity Act established a European Cybersecurity Certification Framework designed to create common mechanisms for evaluating and recognising the security of information and communication technologies (European Union, 2019). Through initiatives such as the European Common Criteria-based Cybersecurity Certification Scheme (EUCC), the EU has sought to translate cybersecurity objectives into technical requirements, assurance levels, and conformity-assessment procedures. These developments are linked to broader debates over European digital sovereignty, strategic autonomy, and the governance of critical digital infrastructures.

China represents a different institutional pathway. Rather than relying primarily on certification frameworks designed to harmonise market participation, China has developed cybersecurity governance through state-coordinated standards mobilisation. Institutions such as the National Information Security Standardization Technical Committee (TC260) translate cybersecurity objectives into technical standards and implementation practices. These standards operate within relationships among government institutions, industry actors, and technological ecosystems, shaping how security expectations are defined and embedded within digital development (Ernst, 2011; Kim et al., 2014).

Existing scholarship provides important insights into these developments but leaves a significant analytical gap. Research on cybersecurity certification has primarily examined certification as a mechanism for technical assurance, risk management, and regulatory coordination. Studies of European cybersecurity certification demonstrate that certification regimes involve political negotiations among market-integration objectives, security concerns, and institutional interests (Sivan-Sevilla, 2021). However, this literature has largely focused on certification as a question of internal governance rather than as a mechanism through which political actors project regulatory authority and shape broader technological environments.

Research on regulatory power has demonstrated how rules can become sources of international influence. Bradford's (2020) concept of the Brussels Effect explains how the European Union can externalise regulatory requirements through the combination of market size, regulatory stringency, and firms' incentives to comply. This literature has significantly advanced understanding of how domestic regulation can generate international effects. However, it has paid less attention to how regulatory power operates when governance is embedded within technical infrastructures. In digital domains, influence increasingly depends not only on formal legal rules but also on standards, certification procedures, and technical criteria that determine interoperability, security, and market participation.

Scholarship on standards governance has likewise demonstrated that technical standards are not simply neutral coordination mechanisms. Standards are institutional arrangements shaped by participation, expertise, and procedural authority; actors capable of influencing standard-setting processes can shape technological trajectories and competitive conditions (Büthe & Mattli, 2011). Nevertheless, this literature has rarely examined cybersecurity certification as the mechanism through which security preferences are transformed into authoritative judgments about technological trust.

How do the European Union and China govern technological trust through cybersecurity certification and standards governance?

This article argues that cybersecurity certification has evolved from a technical assurance mechanism into a form of governance infrastructure through which political actors define, verify, and diffuse technological trust. Rather than treating trustworthiness as an inherent characteristic of digital technologies, the article conceptualises trust as an institutional outcome produced through governance processes. These processes involve three dimensions: the definition of security requirements, the verification of compliance, and the diffusion of trust judgments across markets and technological ecosystems.

Comparing the European Union and China, the article identifies two distinct models of technological trust governance. The European Union represents market-mediated trust governance, in which cybersecurity certification transforms regulatory objectives into technical requirements and creates incentives for firms to align with European security expectations. China represents state-coordinated trust governance, in which cybersecurity objectives are embedded through standards mobilisation, institutional coordination, and technological ecosystem development.

The article makes three contributions. First, it contributes to research on regulatory power by demonstrating that digital governance increasingly operates through technical infrastructures that structure how trust and access are organised. Second, it extends standards-governance literature by showing how certification systems transform technical criteria into forms of institutional authority. Third, it contributes to debates on EU-China digital competition by moving beyond a simple rivalry framework and identifying different pathways through which political economies construct technological trust.

The remainder of the article proceeds as follows. Section 2 reviews scholarship on regulatory power, standards governance, cybersecurity certification, and digital sovereignty. Section 3 develops a theoretical framework of technological trust governance based on definition, verification, and diffusion. Section 4 compares the EU's cybersecurity certification framework with China's cybersecurity standards governance. Section 5 draws out the comparative and theoretical implications, and Section 6 concludes.

2. LITERATURE REVIEW

2.1 Regulatory Power and the Transformation of Governance Authority

Research on global governance has increasingly challenged the assumption that political power is exercised primarily through territorial control or coercive capabilities. Scholars instead highlight how authority can emerge through the capacity to formulate, institutionalise, and diffuse rules beyond national borders. This perspective has been especially influential in the study of regulatory power, which examines how domestic regulatory choices generate international effects.

Bradford's (2020) Brussels Effect provides one of the most influential accounts of regulatory externalisation. Firms seeking access to the EU's large internal market may voluntarily adopt European requirements, sometimes extending those practices across their global operations. The resulting influence depends less on coercion than on the interaction between market size, regulatory capacity, and firms' incentives to comply. Drezner (2007) similarly locates global regulatory outcomes in the power and preferences of major markets, while emphasising the coexistence and competition of regulatory regimes.

These accounts clarify how rules travel internationally, but their main focus remains formal regulation and market mechanisms. Digital governance adds a technical layer. Interoperability specifications, security evaluations, and certification procedures increasingly determine whether technologies can enter markets or connect to infrastructures. Regulatory authority is therefore exercised not only by writing rules, but also by designing the institutional machinery through which those rules become technical judgments.

This shift matters because infrastructures distribute power through routine classifications and design choices. Technical arrangements that appear operational may stabilise institutional priorities and make some forms of participation easier than others (Larkin, 2013; Plantin et al., 2018). Cybersecurity certification is one such arrangement: it converts broad security aims into criteria, tests, assurance levels, and recognition decisions.

2.2 Standards Governance and the Politics of Technical Authority

The literature on standards governance provides a foundation for understanding how technical systems become politically significant. Standards are not merely neutral solutions to coordination problems; they are governance arrangements shaped by access, expertise, representation, and procedural authority (Büthe & Mattli, 2011). Actors with greater influence over standard-setting can affect development pathways and competitive outcomes.

Research on global regulation also shows that expert communities and transnational institutions increasingly possess the capacity to establish legitimate rules and coordinate behaviour across jurisdictions (Mattli & Woods, 2009). Organisational scholarship reaches a similar conclusion: standards both order organisational fields and change through contestation among different logics of coordination, control, and diffusion (Brunsson et al., 2012).

This perspective is especially relevant for cybersecurity. Security standards establish expectations regarding acceptable risk, appropriate evaluation methods, and legitimate forms of assurance. Their content reflects choices about which vulnerabilities matter, whose evidence is credible, and how much confidence is sufficient. Yet standards become practically consequential only when they are connected to certification, procurement, market participation, or infrastructure deployment. Certification is the interface through which technical criteria become recognised judgments about trustworthiness.

2.3 Cybersecurity Certification and the Institutional Production of Trust

Cybersecurity certification scholarship has traditionally approached certification as a mechanism for reducing uncertainty in complex technological environments. Frameworks such as the Common Criteria, codified in ISO/IEC 15408, provide assurance by establishing evaluation methodologies, security requirements, and recognised levels of confidence regarding information-technology products. The Common Criteria Recognition Arrangement further supports cross-border recognition of certificates among participating authorities.

Recent research demonstrates that certification is also an institutional and political process. Sivan-Sevilla (2021) shows that development of the EU cybersecurity certification regime involved tensions between market-integration goals and core state powers. Harmonised certification consequently reflects bargaining over how cybersecurity governance should be organised and which institutions should possess authority over security evaluation.

Existing work nevertheless tends to focus on institutional design, regulatory effectiveness, and implementation.

Less attention has been paid to certification as a mechanism through which technological trust is politically constructed. Certification not only assesses whether a technology is secure; it establishes the criteria through which security is defined, authorises actors to evaluate compliance, and creates channels through which trust judgments circulate.

This article therefore conceptualises cybersecurity certification as trust governance: the institutional processes through which actors define security expectations, verify technological compliance, and diffuse particular understandings of trustworthy technology across markets and infrastructures.

2.4 Digital Sovereignty and Competing Models of Technological Governance

The strategic importance of digital technologies has generated growing debate over digital sovereignty. Sovereignty in the digital age concerns not only territorial control but also the capacity to shape the institutional conditions under which technologies are developed, regulated, and deployed. In the EU, this agenda combines regulatory autonomy with attempts to manage technological dependency while remaining connected to global markets.

Cybersecurity certification operationalises this ambition by translating sovereignty-related concerns into technical requirements and market procedures. The EU can seek greater governance capacity without producing all underlying technologies itself; it can instead shape the conditions under which products and services are recognised as secure.

China follows a different pathway. Research on China's standardisation strategy highlights the role of state coordination, industrial policy, and institutional participation in technological development (Ernst, 2011). Studies of information-security standardisation likewise identify relationships among government agencies, technical committees, and industry actors (Kim et al., 2014). Standards provide a mechanism through which security priorities are incorporated into technological practice and industrial ecosystems.

Discussions of EU-China digital competition often emphasise geopolitics or competing regulatory models. Such approaches can overlook the institutional mechanisms through which trust is produced. Connecting regulatory power, standards governance, and certification makes it possible to compare not merely standards outcomes but the processes through which different political economies define, verify, and diffuse technological trust.

3. THEORETICAL FRAMEWORK: GOVERNING TECHNOLOGICAL TRUST

Cybersecurity certification is commonly understood as a mechanism for assessing whether digital technologies satisfy predefined security requirements. This assumes that trust is primarily a technical outcome generated through improved information, evaluation, and assurance. While certification performs these functions, such a perspective overlooks the institutional processes through which security expectations are created and authorised.

This article treats trust as an institutional achievement rather than an intrinsic property of technology. Trust governance refers to the processes through which actors define what constitutes trustworthy technology, establish procedures for verifying technological reliability, and enable particular interpretations of trust to circulate across markets and infrastructures. Certification therefore does not simply measure security; it produces authoritative judgments about security.

This conceptualisation connects regulatory power, standards governance, and infrastructure politics. Regulatory-power scholarship explains how rules influence actors beyond their original jurisdiction; standards-governance scholarship reveals the politics of technical coordination; infrastructure perspectives show how technical systems embody institutional choices. Cybersecurity certification is a site where these processes converge.

3.1 Trust Definition: Constructing the Meaning of Security

The first dimension concerns the definition of trust. Before a technology can be certified as secure, institutions must decide what security means, which risks deserve priority, and what level of assurance is sufficient. These decisions entail political choices about acceptable vulnerabilities, strategic risks, and governance objectives.

In the EU, the Cybersecurity Act and scheme-specific documentation translate broad objectives into assurance levels and certification criteria. In China, bodies such as TC260 incorporate cybersecurity priorities into national standards-development processes. Both systems seek trustworthy digital environments, but they organise authority over security definitions differently.

3.2 Trust Verification: Institutionalising Authority over Evaluation

The second dimension is verification. Defining requirements alone does not create authority; institutions must establish recognised procedures through which compliance can be assessed. Certification bodies, evaluation laboratories, standards committees, and public authorities do not merely apply technical criteria. They participate in producing authoritative judgments about whether a technology meets accepted expectations.

The EU emphasises formal certification procedures that connect technical assessment with legal recognition and market acceptance. China's model places greater weight on standards-based alignment among governance institutions and industrial actors. The distinction concerns the institutional organisation of confidence, not the presence or absence of verification.

3.3 Trust Diffusion: Extending Governance Across Markets and Systems

The third dimension is diffusion. Regulatory influence depends on making trust judgments consequential beyond their immediate setting. The Brussels Effect identifies a market pathway: providers adapt to European requirements to preserve access to the EU market (Bradford, 2020). Cybersecurity certification can make this mechanism technically specific by linking recognised assurance to market participation.

Trust can also diffuse through institutional and infrastructural embedding. In China's case, standards become influential when incorporated into industrial practices, procurement expectations, infrastructure development, and technology ecosystems. Regulatory power thus need not follow a single pathway. Trust can travel through market-based compliance incentives or ecosystem-based coordination.

3.4 Analytical Framework

The framework asks three questions: Who defines secure and trustworthy technology? Who possesses the authority to evaluate and recognise compliance? Through what mechanisms do trust judgments influence firms, markets, and infrastructures? Applying these questions reveals two ideal-typical pathways: market-mediated certification governance in the EU and state-coordinated standards governance in China.

Table 1: Governing Technological Trust: Dimensions and Pathways of Regulatory Power

TRUST DEFINITION	TRUST VERIFICATION	TRUST DIFFUSION
Who defines technological security?	Who validates technological security?	How does trust travel across markets and systems?
Security criteria and assurance levels	Evaluation, certification, and recognition	Market incentives and ecosystem embedding
EU: certification frameworks and market access	EU: ENISA, national authorities, conformity assessment	EU: external compliance incentives
China: standards mobilisation	China: standards implementation and institutional alignment	China: industrial ecosystems and technological alignment

Note. Author's analytical framework. This editable schematic may be replaced with a publication-quality graphic after journal selection.

4. EMPIRICAL ANALYSIS

4.1 European Union: From Security Regulation to Market-Mediated Trust Governance

The EU case shows how certification can transform general regulatory objectives into a technical architecture of trust. The Cybersecurity Act established a European framework for cybersecurity certification of ICT products, services, and processes, while strengthening the role of the European Union Agency for Cybersecurity (ENISA) (European Union, 2019). The framework responds to fragmented national approaches by creating common scheme-building procedures and assurance concepts at the European level.

This institutional architecture matters because it assigns roles across multiple levels. The European Commission may request preparation of a candidate scheme; ENISA develops candidate schemes with expert input; member states remain involved through national cybersecurity certification authorities; and conformity-assessment bodies or other authorised actors conduct evaluations under scheme-specific rules. Certification therefore distributes authority while placing it within a common European framework.

4.1.1 Defining Trust Through Certification Schemes

The EU defines trust by translating broad cybersecurity concerns into scheme-specific requirements. The Cybersecurity Act provides a general vocabulary of assurance and establishes basic assurance levels, while individual schemes specify evaluation targets, processes, and evidence. This makes security administratively legible: a product or service is not simply described as secure, but assessed against an authorised combination of criteria and assurance expectations.

EUCC illustrates this translation. Built on the Common Criteria tradition, it provides a European scheme for ICT products and establishes how security functionality and assurance claims are to be evaluated. Its significance lies not merely in adopting a technical methodology, but in embedding that methodology in a European legal and institutional setting. Technical criteria thereby become part of the EU's regulatory capacity.

The proposed EU Cloud Services scheme (EUCS) illustrates why definition is politically consequential. Debates around cloud certification have connected technical security, supply-chain dependence, provider eligibility, and sovereignty concerns. Even where scheme design remains contested, the debate reveals that defining security can affect competitive conditions and the organisation of digital markets.

4.1.2 Verifying Trust Through Recognised Procedures

Certification gains authority when verification is recognised. Under the European framework, evaluation is not simply a private claim by a vendor. It is performed through procedures, bodies, and oversight arrangements established or recognised by the relevant scheme. National authorities, accreditation systems, conformity-assessment bodies, and ENISA collectively constitute an institutional chain through which security claims acquire public credibility.

This arrangement does not eliminate politics or uncertainty. Different assurance levels require different evidence and oversight, and member states retain significant responsibilities in security-sensitive domains. Nevertheless, the framework establishes a common procedural language through which trust claims can be compared and recognised. Verification authority is thus institutionalised rather than assumed.

4.1.3 Diffusing Trust Through Market Incentives

The EU's pathway of diffusion is primarily market-mediated. Providers seeking to participate in European digital markets face incentives to anticipate certification requirements, align product-development practices, and generate evidence compatible with European schemes. Where certificates become linked to procurement, sectoral regulation, or customer expectations, the effects can extend beyond the legal scope of a single scheme.

This logic resembles the Brussels Effect, but cybersecurity introduces limits. Security is tied to national strategic interests, sensitive information, and geopolitical conflict; firms and governments may therefore resist requirements they view as discriminatory or sovereignty-enhancing. EU certification should not be treated as automatically global. Its power lies in structuring incentives and expectations around market participation, not in guaranteeing universal adoption.

The EU case consequently represents market-mediated trust governance. Regulatory authority emerges from the capacity to translate security objectives into certification requirements, organise recognised verification, and connect trusted status to participation in a large market.

4.2 China: From Standards Mobilisation to State-Coordinated Trust Governance

China's cybersecurity governance follows a different institutional pathway. Cybersecurity standards are developed within a broader system that connects state priorities, technical expertise, regulatory implementation, and

industrial development. TC260 occupies a central position in this system by organising standards work across areas such as cybersecurity technology, data security, and evaluation. Its committees and working groups connect government-related institutions, research organisations, and firms.

Standards in this setting should not be reduced to commands issued by a unitary state. Their production depends on expertise, organisational participation, and negotiation among institutions with different technical and industrial interests. At the same time, coordination is embedded within a state-led governance structure that links standards to statutory obligations, administrative guidance, procurement, and sectoral implementation.

4.2.1 Defining Trust Through National Standards

Trust definition occurs through the conversion of broad security priorities into national technical specifications and recommended practices. Standards clarify expectations that legal provisions often express at a high level. They can specify security controls, assessment methods, data-handling practices, and organisational processes, thereby making compliance operational.

This process links standardisation to technological development. China's standards strategy has long combined domestic capacity-building, industrial upgrading, and participation in international standardisation (Ernst, 2011). Information-security standardisation also reflects tensions between security objectives, trade principles, and integration with international technical regimes (Kim et al., 2014). Defining trust is therefore both a governance function and a component of technological strategy.

4.2.2 Verifying Trust Through Institutional Alignment

Verification in the Chinese model is less centred on a single harmonised certification framework than in the EU case. It operates through interaction among standards implementation, testing and certification activities, regulatory inspection, organisational assessment, and industry alignment. Standards provide common reference points across these processes.

This does not mean that verification is informal or absent. Rather, authority is produced through a network in which technical expectations are reinforced by administrative and industrial relationships. Firms demonstrate alignment not only through a certificate, but also through conformity with standards used in regulatory guidance, procurement, testing, and operational practice.

4.2.3 Diffusing Trust Through Ecosystem Embedding

China's pathway of diffusion is rooted in ecosystem embedding. Standards become influential when incorporated into domestic industrial practice, infrastructure deployment, supplier relationships, and technology platforms. Large-scale adoption can create expectations that travel with products, vendors, and infrastructure projects, even without a direct equivalent to the EU's market-access mechanism.

International participation can amplify this process, but participation alone does not equal dominance. Influence depends on whether proposals gain institutional support, whether firms possess implementation capacity, and whether technologies built around particular specifications are adopted. China's regulatory power therefore derives from coordination capacity and infrastructural embedding rather than from the simple export of domestic rules.

The Chinese case represents state-coordinated trust governance: security objectives are translated into technical standards, verification is organised through institutional alignment, and trust judgments diffuse through industrial and technological ecosystems.

5. DISCUSSION: TWO MODELS OF REGULATORY POWER IN DIGITAL GOVERNANCE

The comparison demonstrates that cybersecurity governance is not simply a technical effort to improve digital security. It is a broader struggle over the institutional production of technological trust. Both the EU and China seek to determine which technologies, suppliers, and infrastructures should be recognised as secure and reliable, yet they organise this process through different mechanisms.

The distinction is not between regulation and standards, because both cases combine legal, technical, and organisational elements. It concerns how authority over trust is organised. The EU privileges certification frameworks that link security requirements to recognised assessment and market participation. China relies more heavily on standards mobilisation that connects security objectives to institutional coordination and ecosystem development.

Table 2: Two Models of Governing Technological Trust in Digital Governance

Dimension	European Union	China
Governance logic	Market-mediated regulatory governance	State-coordinated standards governance
Primary mechanism	Cybersecurity certification	Cybersecurity standards mobilisation
Core institutional actors	EU institutions, ENISA, national authorities, certification and conformity-assessment bodies	State agencies, TC260, standards committees, research institutes, and industry actors
Trust definition	Security requirements translated into assurance levels and certification criteria	Security objectives translated into national technical standards
Trust verification	Conformity assessment, evaluation procedures, and recognised certification schemes	Standards implementation, testing, regulatory alignment, and institutional coordination
Trust diffusion	Market-access incentives, procurement, and external firm adaptation	Ecosystem embedding, industrial deployment, and technological alignment
Main source of regulatory power	Regulatory capacity and market influence	Coordination capacity and infrastructural embedding
Representative instruments	Cybersecurity Act, EUCC, and EUCS	TC260 standards and the national cybersecurity standards system
Main governance outcome	Externalisation of European security expectations	Institutionalisation of Chinese technical expectations within ecosystems

5.1 Regulatory Power as Trust-Infrastructure Governance

The concept of technological trust governance extends regulatory-power scholarship in two ways. First, it identifies the institutionalisation of security judgments as a source of influence. Actors gain power not only by creating rules but by shaping the criteria through which technologies are classified as secure or insecure. Second, it identifies multiple pathways of diffusion. Market size matters, but standards can also acquire power through coordinated deployment and infrastructural embedding.

The EU case refines the Brussels Effect by showing that externalisation in digital governance depends on technical institutionalisation. Legal objectives must be converted into schemes, assurance levels, evidence requirements, and recognition procedures before they can structure market behaviour. This conversion creates influence, but also sites of contestation.

The Chinese case shows that standards power does not require control over global standard-setting bodies. Governance effects can emerge from the adoption and embedding of standards within a large technological ecosystem. Yet such effects depend on implementation, institutional capacity, and uptake; neither state sponsorship nor international participation guarantees diffusion.

5.2 Digital Sovereignty as Authority Over Trust

The comparison also clarifies digital sovereignty. Sovereignty concerns not only control over data, platforms, or technological resources, but authority over the processes through which technologies become recognised as secure and reliable. Certification and standards are therefore practical sites where sovereignty claims are operationalised.

These models are ideal types rather than mutually exclusive systems. The EU also uses standards and public coordination; China also uses certification and market incentives. The analytical value of the distinction lies in identifying the dominant pathway through which trust judgments acquire authority and diffuse. Future research can test the framework against hybrid arrangements, sectoral variation, and cases in which recognition regimes overlap or conflict.

6. CONCLUSION

Cybersecurity certification has become an important arena in which the governance of digital technologies is organised. Although commonly understood as a technical mechanism for evaluating security performance, certification represents a broader form of governance infrastructure through which technological trust is institutionally produced. Certification systems do not merely assess whether technologies are secure; they establish the criteria through which security is defined, identify the actors authorised to verify compliance, and shape the channels through which trust judgments become influential.

The comparison of the European Union and China demonstrates that regulatory power operates through different pathways of trust governance. The EU represents market-mediated trust governance, where certification transforms regulatory objectives into technical requirements and creates incentives for firms to align through market participation. China represents state-coordinated trust governance, where cybersecurity standards are mobilised through institutional coordination, industrial alignment, and technological ecosystem embedding.

These findings contribute to debates on regulatory power, standards governance, and digital sovereignty. Digital regulatory power increasingly operates through technical infrastructures rather than formal rules alone. Standards and certification become politically significant when they establish authoritative judgments about technological trust. Digital sovereignty, in turn, includes authority over the processes through which technologies become recognised as secure and reliable.

The implications extend beyond cybersecurity certification. As 5G networks, cloud computing, artificial intelligence, and Internet of Things infrastructures become central to global digital development, competition over technological governance will increasingly involve competition over the production of trust. Future research should examine how different political economies construct and diffuse trust across these infrastructures, how recognition arrangements interact, and when certification systems generate convergence, fragmentation, or mutual dependence.

REFERENCES

[1] Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.
[2] Brunsson, N., Rasche, A., & Seidl, D. (2012). The dynamics of standardization: Three perspectives on standards in organization studies. Organization Studies, 33(5-6), 613-632. https://doi.org/10.1177/0170840612443620
[3] Büthe, T., & Mattli, W. (2011). The new global rulers: The privatization of regulation in the world economy. Princeton University Press.
[4] Common Criteria Recognition Arrangement. (n.d.). Common Criteria Recognition Arrangement.
[5] Drezner, D. W. (2007). All politics is global: Explaining international regulatory regimes. Princeton University Press.
[6] Ernst, D. (2011). Indigenous innovation and globalization: The challenge for China's standardization strategy. East-West Center.
[7] European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, 15-69.
[8] European Union Agency for Cybersecurity. (2024). EUCC: European Common Criteria-based cybersecurity certification scheme.
[9] European Union Agency for Cybersecurity. (n.d.). European cybersecurity certification framework.
[10] European Union Agency for Cybersecurity. (n.d.). European cybersecurity certification scheme for cloud services (EUCS) [Candidate scheme documentation].
[11] Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42-79. https://doi.org/10.1162/isec_a_00351
[12] International Organization for Standardization. (2019). ISO/IEC 15408: Information technology-Security techniques-Evaluation criteria for IT security.
[13] Kim, S., Lee, H., Kwak, J., & Seo, J. (2014). China's information security standardization: Analysis from the perspective of technical barriers to trade principles. Telecommunications Policy, 38(10), 909-921.
[14] Larkin, B. (2013). The politics and poetics of infrastructure. Annual Review of Anthropology, 42, 327-343. https://doi.org/10.1146/annurev-anthro-092412-155522

[15] Mattli, W., & Woods, N. (Eds.). (2009). The politics of global regulation. Princeton University Press.
[16] National Information Security Standardization Technical Committee. (n.d.). National cybersecurity standards documents [Institutional materials].
[17] Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. New Media & Society, 20(1), 293-310. https://doi.org/10.1177/1461444816661553
[18] Radu, R. (2019). Negotiating Internet governance. Oxford University Press.
[19] Sivan-Sevilla, I. (2021). Europeanisation on demand: The EU cybersecurity certification regime between market integration and core state powers. Journal of Public Policy, 41(3), 570-593. https://doi.org/10.1017/S0143814X20000099