Universidade do Minho
Escola de Economia, Gestão e Ciência Política

Ana Sofia Martins Almeida

Cyberspace Security in Light of the Netpolitik vs Digitalpolitik Dichotomy: The Chinese and South Korean Models

Abril 2026

Cyberspace Security in Light of the Netpolitik vs Digitalpolitik Dichotomy: The Chinese and South Korean Models
Sofia Martins
Uminho | 2026

Universidade do Minho
Escola de Economia, Gestão e Ciência Política

Ana Sofia Martins Almeida

Cyberspace Security in Light of the Netpolitik vs Digitalpolitik Dichotomy: The Chinese and South Korean Models

Master's Dissertation Project in International Relations

Under the scientific orientation of:

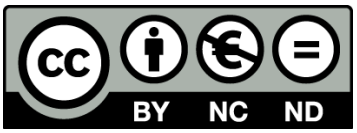
Professor José Palmeira, PhD

Professor Paulo Afonso B. Duarte, PhD

Abril 2026

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos. Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada. Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.



Atribuição CC BY

https://creativecommons.org/licenses/by/4.0/

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Professor Paulo Afonso B. Duarte, PhD, for his invaluable guidance, insightful feedback, and continuous support throughout the development of this dissertation. His expertise and dedication were fundamental to the completion of this work. In addition, I would also like to express my gratitude to Professor José Palmeira, PhD, for his invaluable contribution to the scientific orientation of this dissertation. I am appreciative of the intellectual stimulation and critical thinking fostered by the University of Minho during my master's in international relations, which contributed to my academic growth. The present project has had a significant impact on my perspective regarding both potential career paths and future research endeavours.

I extend my gratitude to my family, whose steadfast support, patience, and encouragement have been indispensable to the success of this endeavour. In addition, I wish to express my profound gratitude to my friends for their unwavering encouragement, insightful counsel, and for their constant presence, both during the challenging and the rewarding phases of this endeavour.

Statement of Integrity

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration. I further declare that I have fully acknowledged the Code of Ethical Conduct of the University of Minho.

Declaration on the Use of Artificial Intelligence (AI) Tools

I hereby declare having acted this academic work with integrity and confirm that I have not resorted to any form of undue use of AI tools, nor to the falsification or omission of information, sources, data, results or processes in any of the stages leading to its elaboration.

I further declare that any use of AI tools was done in a transparent and responsible manner, being duly noted in the work, and that I critically verified the accuracy of the content produced with their support, assuming full responsibility for what I submit.

I further declare that I have fully acknowledged the Code of Ethical Conduct of the University of Minho, as well as the applicable standards of academic integrity and data protection.

Cyberspace Security in Light of the Netpolitik vs Digitalpolitik Dichotomy: The Chinese and South Korean Models

Abstract

In a context of expanding digital interdependence and intensifying cyber threats, cyberspace has become a central domain of power and governance in international relations. Despite the growing scholarly attention to cyberspace governance, existing literature often treats China and South Korea in isolation or from predominantly Western perspectives, leaving a gap in comparative analyses that systematically contrast their digital governance models. This dissertation seeks to fill this gap by answering the following research question: How do China and South Korea navigate the tensions between openness and control in cyberspace governance within the frameworks of Netpolitik and Digitalpolitik? To this end, both Chinese and South Korean models of cyberspace governance will be analysed. The period studied spans from 2015 to 2025, a period marked by significant legal reforms and technological advancements in both countries. The methodology adopted employs a qualitative comparative case study based on primary sources, including national strategies, legislation and international communications, complemented by secondary sources of academic literature. In turn, the theoretical framework is grounded in the dichotomy between Netpolitik and Digitalpolitik, providing a nuanced understanding of the distinct yet interrelated governance models of China's state-centric Digitalpolitik and South Korea's hybrid approach combining elements of both frameworks. This research contributes to a deeper understanding of how different political systems navigate the tension between openness and control in cyberspace, and how these strategies influence the evolving global digital order.

Keywords: Cybersecurity, Cyberspace Governance, Digitalpolitik, Netpolitik, China, South Korea.

A Segurança no Ciberespaço à Luz da Dicotomia entre Netpolitik e Digitalpolitik: Os Modelos Chinês e Sul-Coreano

Resumo

Num contexto de crescente interdependência digital e de intensificação das ameaças cibernéticas, o ciberespaço tornou-se um domínio central de poder e governação nas relações internacionais. Apesar da crescente atenção académica dedicada à governação do ciberespaço, a literatura existente trata frequentemente a China e a Coreia do Sul de forma isolada ou a partir de perspetivas predominantemente ocidentais, deixando uma lacuna nas análises comparativas que contrastem sistematicamente os seus modelos de governação digital. Esta dissertação procura preencher esta lacuna, respondendo à seguinte questão de investigação: Como é que a China e a Coreia do Sul gerem as tensões entre abertura e controlo na governação do ciberespaço no âmbito das estruturas da Netpolitik e da Digitalpolitik? Para tal, serão analisados os modelos de governação do ciberespaço tanto da China como da Coreia do Sul. O período estudado abrange de 2015 a 2025, um período marcado por reformas legais significativas e avanços tecnológicos em ambos os países. A metodologia adotada recorre a um estudo de caso comparativo qualitativo baseado em fontes primárias, incluindo estratégias nacionais, legislação e comunicações internacionais, complementadas por fontes secundárias da literatura académica. Por sua vez, o quadro teórico assenta na dicotomia entre Netpolitik e Digitalpolitik, proporcionando uma compreensão matizada dos modelos de governação distintos, mas inter-relacionados, da Digitalpolitik centrada no Estado da China e da abordagem híbrida da Coreia do Sul, que combina elementos de ambos os quadros. Esta investigação contribui para uma compreensão mais profunda da forma como diferentes sistemas políticos geram a tensão entre a abertura e o controlo no ciberespaço, e de como estas estratégias influenciam a ordem digital global em evolução.

Palavras-Chave: Cibersegurança, Governação do Ciberespaço, Digitalpolitk, Netpolitik, China, Coreia do Sul.

Content table

List of abbreviations 10

List of tables 13

Introduction 14

i. Framework and justification of the topic 14
ii. Literature review 15
iii. Problematic 17
iv. Theoretical framework and methodology 18
v. Dissertation structure 19

1. Connecting the dots: Theoretical and Transversal Concepts 20

1.1 Netpolitik vs Digitalpolitik 21
1.2 Cyber Sovereignty, Cyberspace and Fragmentation 25
1.3 Digital Sovereignty, AI and Data Governance 31

2. China's approach to the cyberspace 37

2.1. National cybersecurity approach 37
2.1.1 Legal Framework 37
2.1.2 State surveillance and digital authoritarianism 42

2.2. International cybersecurity strategy 49
2.2.1 Cyber sovereignty and international cooperation 50
2.2.2 AI, Technical Standardisation and the Digital Silk Road 55

3. South Korea's approach to cyberspace 62

3.1. National Approach 62
3.1.1. Legal Framework and Institutions 63
3.1.2 Smart Cities, AI and Digital Governance 68

3.2. International Approach 77
3.2.1 South Korea's strategy through AI and emerging technologies 77
3.2.2 Cyberspace sovereignty and partnerships 81

4. Comparing the Chinese and South Korean models 86

4.1. Similarities 86
4.1.1 State-led cybersecurity governance and Integration of law, technology, and institutions 86
4.1.2 Public-Private collaboration and international engagement 91

4.2. Exploring the differences 97
4.2.1 Governance Models and Legal Frameworks in Data Governance 98
4.2.2 Surveillance, AI and International strategy 105

Conclusion 114

Bibliography 118

Primary Sources 118
Secondary Sources 121

List of abbreviations

AI - Artificial Intelligence

AISI - AI Safety Institute

ARF - ASEAN Regional Forum

ASEAN - Association of South East Asian Nations

BRI - Belt and Road Initiative

CAC - Cyberspace Administration of China

CAMP - Cybersecurity Alliance for Mutual Progress

CBDC - Central Bank Digital Currencies

CCAC - Central Cyberspace Affairs Commission

CCP - The Chinese Communist Party

CCTV - Closed-Circuit Television

CEO - Chief Executive Officer

CERTs - Computer Emergency Response Teams

CII - Critical Information Infrastructure

CISOs - Chief Information Security Officers

CPOs - Chief Privacy Officers

CSDSTC - Chinese Security and Defense Standardization Technology Committee

CSIRT - Computer Security Incident Response Team

CSL - Cybersecurity Law

DEPA - Digital Economy Partnership Agreement

DIFAP - Digital Integration Framework Action Plan

DNS - Domain Name System

DSL - Data Security Law

DSR - Digital Silk Road

DTA - Digital Trade Agreement

ESG - Environmental, Social and Governance

EU - European Union

FLOPs - Floating-Point Operations

FSI - Financial Supervisory Institute

GDPR - General Data Protection Regulation

GIDC - Government Information Disclosure Centre

GPU - Graphical Processing Unit

ICT - Information and Communications Technology

IEC - International Electrotechnical Commission

IT - Information Technology

IoT - Internet of Things

IP - Internet Protocol

IR - International Relations

ISO - International Organization for Standardization

ITU - International Telecommunication Union

KCC - Korea Communications Commission

KICJ - Korean Institute of Criminology and Justice

KISA - Korea Internet & Security Agency

KOICA - Korea International Cooperation Agency

KrCERT/CC - Korea Computer Emergency Response Team/Coordination Center

MLPS - Multi-Level Protection Scheme

MoIS - Ministry of Interior and Safety

MOLIT - Ministry of Land, Infrastructure and Transport

MPS - Ministry of Public Security

MSIT - Ministry of Science and ICT

NATO - North Atlantic Treaty Organisation

NCSC - National Cyber Security Centre

NGO - Non-Governmental Organizations

NGT - New Generation Technologies

NIRS - National Information Resources Service

NIS - National Intelligence Service

NSL - National Security Law

NSO - National Security Office

NSRI - National Security Research Institute

NSSP - National Strategic Smart City Program

ODA - Official Development Assistance

OECD - Organisation for Economic Co-operation and Development

PIPA - Personal Information Protection Act

PIPL - Personal Information Protection Law

SCO - Shanghai Cooperation Organisation

SCS - Social Credit System

SMEs - Small and medium-sized enterprises

SWIFT - Society for Worldwide Interbank Financial Telecommunication

UDPN - Universal Digital Payment Network

UN - United Nations

US - United States

VPN - Virtual Private Network

VR - Virtual Reality

WTO - World Trade Organisation

List of tables

Table 1. Comparative table: Netpolitik vs Digitalpolitik 24
Table 2. Key Concepts in Cyberspace Governance 30
Table 3. Core Concepts and Dynamics of Digital Sovereignty and AI Governance 36
Table 4. Core Digital Governance Laws and the Institutionalisation of Digitalpolitik in China 42
Table 5. Digital Governance and Surveillance Logic in China 44
Table 6. Digital Surveillance as State Power in China 46
Table 7. Infrastructure, Behaviour, and Digitalpolitik in China 49
Table 8. Principles of Cyber Sovereignty in China 52
Table 9. China's International Digital Cooperation and Digitalpolitik 54
Table 10. Overview of China's Approach to AI, Cyberspace, and Global Standards 57
Table 11. China's Cyberspace Governance and Digitalpolitik Dimensions 61
Table 12. South Korea's Cybersecurity Institutions & Digitalpolitik 67
Table 13. South Korea's Smart Cities and Netpolitik Alignment 70
Table 14. Overview of South Korea's Sejong and Busan Smart City Pilot Projects 71
Table 15. South Korea's AI and Smart City Governance: Netpolitik vs Digitalpolitik 76
Table 16. South Korea's AI and technology strategy - Netpolitik vs Digitalpolitik 80
Table 17. South Korea's Hybrid Cybersecurity Strategy 85
Table 18. China and South Korea's Cyber Governance through the Lens of Digitalpolitik 90
Table 19. State-Private Sector Collaboration in the Logic of Digitalpolitik 97
Table 20. Cyberspace and Data Governance in China and South Korea through the Logics of Digitalpolitik and Netpolitik 104
Table 21. Digital Governance Approaches of China and South Korea through the Logics of Digitalpolitik and Netpolitik 113

Introduction

i. Framework and justification of the topic

This dissertation is grounded in the theoretical frameworks of *Netpolitik* and *Digitalpolitik*, which offer complementary perspectives on how digital technologies are reshaping power, influence and state behaviour within the contemporary international system. As conceptualised by Bollier (2003), *Netpolitik* emphasises the empowerment of decentralised actors through digital networks that facilitate soft power, cooperative engagement and the diffusion of cultural and political influence beyond traditional, state-centric hierarchies. This reflects an open, participatory digital environment in which non-state actors, such as NGOs (Non-Governmental Organisations), academic experts and diasporic communities, play a significant role in shaping global platforms and discourse. In contrast, the concept of *Digitalpolitik*, as defined by McDonald and Mina (2018) and further developed by Duarte (2025), takes a realist and security-centred approach, emphasising state sovereignty, technological competition, and the strategic management of digital infrastructure and data. It conceptualises cyberspace as a contested arena in which states deploy coercive tools such as surveillance, cyber operations, censorship and data governance, to assert dominance, control information flows, and protect national interests within a fragmented global internet.

The dissertation justifies its focus on China and South Korea by highlighting their distinct yet interrelated digital governance models, which exemplify the interplay and tension between *Netpolitik* and *Digitalpolitik*. China embodies a Digitalpolitik approach, employing a centralised, state-led regime that integrates legal frameworks, sophisticated surveillance and data governance to reinforce regime stability, national security and cyber-sovereignty. The deployment of artificial intelligence (AI), alongside the export of information and communication technologies (ICT) infrastructure through initiatives such as the Digital Silk Road (DSR), illustrates the strategic use of digital technologies to exert geopolitical influence (Xiao & Xu, 2024). South Korea represents a hybrid model that combines elements of *Netpolitik* and *Digitalpolitik*. The country embraces regulatory flexibility, rights-based data governance, public-private collaboration and active participation in multilateral forums to promote cooperation, technological innovation and democratic oversight. At the same time, it emphasises digital sovereignty and security through domestic platform development and strategic AI governance (Yoo, 2025).

By framing these models within the evolving theoretical concepts of cyberspace, cyber-sovereignty, data governance and AI, the dissertation establishes a robust analytical foundation for examining how states negotiate control, cooperation and competition within the digital realm. This

framework elucidates the broader phenomenon of internet fragmentation and the evolving global digital landscape, thereby justifying the examination of China and South Korea's approaches as pivotal case studies that collectively demonstrate the complexity and diversity of modern digital governance and power dynamics. This dissertation seeks to address an important gap in the literature by comparing the Chinese and South Korean approaches. While these cases have often been analysed in isolation or from Western perspectives in existing studies, relatively few works have systematically contrasted their cyberspace governance models in light of the *Netpolitik* versus *Digitalpolitik* dichotomy. The present research is therefore justified both by its theoretical contribution to debates on digital power and governance and by its practical relevance, particularly in view of the growing impact of cyberspace on global security, technological interdependence and the stability of international relations.

The analysis period from 2015 to 2025 is justified on the grounds that it encompasses a pivotal decade during which significant transformations occurred in cyberspace governance, characterised by the establishment of key legal frameworks and technological advancements in both China and South Korea. From 2015 onwards, China enacted foundational digital legislation, including the Cybersecurity Law (2016), the Data Security Law (2021) and the Personal Information Protection Law (2021). Collectively, this legislation codified China's comprehensive digital policy approach, expanding state control over cyberspace (Creemers, 2023). Concurrently, South Korea intensified its hybrid strategy, with a focus on digital sovereignty, multilateral cooperation, and the standardisation of AI. This intensification is particularly evident in its leadership in AI safety standards and international regulatory alignment towards 2025 (Joo, 2025). This decade is distinguished by an evolving interplay between control, innovation, and international engagement, rendering it a pivotal period for understanding both the contrasting and converging governance models amid accelerating technological competition and emerging norms in the digital domain.

ii. Literature review

The academic discourse on cyberspace governance and security reflects the intricacies inherent in the digital era, marked by the emergence of novel forms of power. Within the field of international relations, scholars such as Nye (2010) have highlighted the role of cyber power in shaping state behaviour and the distribution of authority on the global stage. This concept of cyber power, understood as the capacity to achieve strategic outcomes through digitally interconnected resources, has the potential to redefine the landscape of contemporary international politics (Gosling, 2021). This transformation is further reinforced by digital diplomacy and soft power strategies, whereby states project influence not only through material means but also via networks, narratives, and cultural dissemination (Jin, 2024).

Within this broader discussion, the dichotomy between *Netpolitik* and *Digitalpolitik* provides an analytical framework through which contrasting models of cyberspace governance may be understood. Bollier (2003) is credited with pioneering the conceptualisation of *Netpolitik* as a liberal and multilateral approach, centred on transparency, cooperation and the defence of digital rights. In contrast, *Digitalpolitik* adopts a state-centric and competitive logic, wherein digital infrastructures, data, and technologies serve as instruments of strategic control and geopolitical rivalry, reflecting a more security-driven and national sovereignty-focused approach (McDonald & Mina, 2018).

Building on these theoretical perspectives, the literature examines key concepts such as cyberspace, cyber-sovereignty, digital sovereignty, data governance, and AI. These concepts are pivotal in understanding how states seek to extend their authority into the borderless digital domain. Cyber-sovereignty underlines states' efforts to impose jurisdiction and control over internet domains within national borders, while digital sovereignty emphasizes the capacity to manage digital ecosystems independently. Data governance and technical standards have emerged as fundamental mechanisms for ensuring the secure, ethical and interoperable use of data and AI systems, which are increasingly central to power dynamics and international cooperation (Haber & Topor, 2023). The reviewed literature also addresses the fragmentation of the global digital order, wherein competing national digital regimes challenge the open and global character of the internet. In this context, the tension between sovereignty, innovation and cooperation is particularly salient. In seeking to assert power both domestically and internationally, states leverage legal frameworks, technological infrastructure and AI capabilities (Mayer & Nock, 2025). Furthermore, the framework incorporates debates on the political and normative dimensions of digital governance, illustrating how divergent models reflect different political systems, with authoritarian informationalism characterising China's approach and a more regulatory and rights-based governance framing that of South Korea.

The available literature provides a comprehensive overview of the multidisciplinary insights relevant to this study, drawing upon international relations, cybersecurity studies and digital policy analysis. This comprehensive foundation enables a detailed analytical comparison of the cyberspace governance of China and South Korea. The research is situated within ongoing academic conversations about the evolving nature of power in the digital age, the strategic significance of AI and data, and the emergence of digital sovereignty as a cornerstone of contemporary statecraft. Notwithstanding the expansion of research in this area, there is an absence of systematic comparative studies between China and South Korea in the domain of cyberspace governance and cybersecurity. Existing literature

on the subject is predominantly case-specific or Western-centric in its perspective, often overlooking the intricate dynamics inherent within the Asia-Pacific region. The present dissertation aims to address this gap by analysing the Chinese and South Korean models side by side, through the lens of the *Netpolitik* versus *Digitalpolitik* dichotomy. This will contribute to a more nuanced understanding of how different political regimes and geostrategic contexts shape digital governance in the 21st century.

iii. Problematic

Global Internet fragmentation is intensifying as state-centric policies, such as China's cyber-sovereignty, and proprietary technologies challenge openness and interoperability. In contrast, countries such as South Korea adopt proactive cybersecurity measures and engage in international cooperation to maintain resilient, interconnected networks, thereby highlighting the growing geopolitical stakes in digital governance. The rise of "splinternets" poses a significant threat to the internet's foundational principles of openness and interoperability. Whereas the Internet historically connected diverse networks through open standards, political pressures and the proliferation of proprietary systems developed by private companies are increasingly generating fragmented, restricted, and non-interoperable online spaces (Perarnaud et al., 2022, p.5).

China has advanced internet fragmentation through its promotion of cyber-sovereignty, exercising control over domestic networks via mechanisms such as the Great Firewall and exporting this model internationally. In addition, Chinese technology companies, such as Huawei, have proposed technical changes that could give rise to non-interoperable networks, thereby challenging the internet's open and interconnected structure (Nocetti, 2024). China's promotion of cyber-sovereignty extends beyond its borders, raising concerns regarding global cybersecurity and the potential for espionage through Chinese technologies, particularly those associated with firms such as Huawei. The international diffusion of Chinese regulatory and technological practices is gradually reshaping global digital governance towards a more centralized, state-controlled model aligned with China's political and economic objectives (Assad, 2025). In response to internet fragmentation, South Korea combines proactive cyber defence with international cooperation. While its advanced digital infrastructure introduces certain cybersecurity vulnerabilities, the country mitigates these risks through a robust attack classification system and strategic alliances, thereby promoting a more resilient and interconnected cyberspace. The rapid evolution of the global digital environment further amplifies risks to state security and international relations, as increased connectivity and divergent political values heighten the potential for conflict (Roshan, 2025).

The core problematic lies in understanding how states navigate the dual imperatives of promoting cooperation and openness, as emphasised by *Netpolitik*, against the imperatives of security, control, and strategic advantage prioritised by *Digitalpolitik*. This dichotomy reflects a broader struggle between liberal-oriented frameworks, which value democracy, individual rights, and soft power, and realist, security-centred paradigms, which emphasise hard power, state dominance, and technological competition. The escalation of cyber-related conflicts, surveillance practices and regulatory measures highlights the challenge of balancing these conflicting logics within both domestic and international contexts. Furthermore, the dissertation examines how these tensions shape the governance models employed by prominent regional actors such as China and South Korea. The Chinese approach is characterised by a highly centralised, security-focused system that integrates legal regulation, AI-driven surveillance, and stringent information control to consolidate political stability and project influence globally (Chaskes, 2022). Conversely, South Korea has adopted a hybrid model that combines regulatory oversight, democratic norms, and multilateral cooperation with strategic objectives related to technological sovereignty and cyber resilience (Merril, 2025). This contrast illustrates the intricate interplay of political systems, legal frameworks, and cultural values in shaping digital governance strategies, thereby complicating the prospects for unified global digital governance.

Ultimately, the problematic extends to the implications of these divergent approaches for global stability, cooperation, and innovation. The fragmentation of cyberspace presents challenges for multilateral governance, complicates efforts to establish interoperable technical standards, and may exacerbate geopolitical rivalries. Understanding how digital sovereignty, data governance, and AI intersect with power dynamics is essential for addressing the risks of conflict, surveillance overreach, and normative contestation in the emerging digital order.

iv. Theoretical framework and methodology

This research adopts a qualitative and comparative approach, structured around a comparative case study of the cyberspace governance policies of China and South Korea. The methodology aims to explore in depth how these two powers promote distinct normative models of internet governance and cybersecurity at the regional, national, and international levels. It is grounded on document analysis, involving a critical and interpretative reading of primary sources such as national strategies, official speeches, diplomatic statements, regional agreements, international treaties, and communications and reports from relevant agencies and international forums involving both states. The analysis is complemented by secondary sources, encompassing relevant academic literature and documents from

international organisations, with the objective of mapping the practices and normative positions adopted by each country.

The conceptual framework adopted in this research is based on the dichotomy between *Netpolitik* and *Digitalpolitik*. This opposition enables an understanding not only of differing approaches to cybersecurity but also of the normative conflicts that arise from the digital rise of actors holding contrasting views on sovereignty, surveillance, and Internet 11 governance. The concept of *Netpolitik*, introduced by Bollier (2003), is grounded in a form of diplomacy oriented towards values such as "moral legitimacy, cultural identity, social values, and public perceptions" (2003, p. 14). It represents a liberal approach that regards the internet as a decentralised space of interconnection among individuals, promoting transparency, democracy, digital rights, and multilateral cooperation. By contrast, *Digitalpolitik* is an emerging concept associated with digital realism, centred on state competition, informational control, and the projection of power through digital technology (Duarte et al. 2024).

The normative dispute between *Netpolitik* and *Digitalpolitik* finds clear expression in the cybersecurity policies of China and South Korea. China, as a staunch advocate of digital sovereignty and state control over infrastructure and data, promotes a centralised, hierarchical, and strategic governance model consistent with the principles of *Digitalpolitik*. South Korea, by contrast, implements cybersecurity policies aligned with Western normative frameworks, upholding a liberal model akin to the ideals of *Netpolitik*. However, despite its similarities with Western liberal models, particularly the American model, South Korea exhibits certain nuanced characteristics of *Digitalpolitik*, rendering the analysis of its case both complex and distinctive.

v. Dissertation structure

The dissertation is structured to progressively develop a comprehensive analysis of cyberspace governance through theoretical frameworks, empirical case studies, and comparative insights. The opening chapter establishes the theoretical and conceptual foundations, introducing the key lenses of *Netpolitik* and *Digitalpolitik* and elucidating the manner in which digital technologies reconfigure power, influence, and state behaviour. The research proceeds to examine a range of key concepts, including cyber-sovereignty, digital sovereignty, data governance and AI. It highlights the role these concepts play in the fragmentation of the global internet and the contestation over digital spaces. The second chapter provides a detailed analysis of China's approach to cyberspace governance, including an examination of its national legal frameworks, surveillance infrastructure, and international strategies such as the DSR.

This chapter demonstrates how China operationalises a state-centric model that is aligned with *Digitalpolitik*. The third chapter examines South Korea's distinct governance model, characterised by its national legal and institutional frameworks and its focus on cybersecurity, smart cities, AI, and digital infrastructure. This chapter illustrates South Korea's hybrid cyberspace governance approach by identifying the integration of both *Netpolitik* and *Digitalpolitik* elements in its strategy. The final chapter compares the digital governance models of China and South Korea, highlighting both similarities and differences. The contrast between the two countries reflects their divergent political systems and strategic priorities, illustrating two distinct pathways in managing digital sovereignty and cyberspace governance within a fragmented global digital order.

1. Connecting the dots: Theoretical and Transversal Concepts

The first chapter establishes the theoretical and conceptual framework underpinning this dissertation. It introduces the key lenses of *Netpolitik* and *Digitalpolitik* to explain how digital technologies have transformed the nature of power, influence, and state behaviour. While *Netpolitik* highlights the role of digital networks in enabling decentralised actors, soft power, and cooperative forms of engagement (Bollier, 2003), *Digitalpolitik* reflects a more state-centric and competitive logic, in which digital infrastructures, data, and technologies are employed as instruments of strategic control and geopolitical rivalry (McDonald & Mina, 2018). Together, these perspectives provide the foundation for understanding the differences in China's and South Korea's approaches to cyberspace. Building on this theoretical lens, the chapter introduces the central concepts that structure the subsequent analysis. It first examines cyberspace and cyber-sovereignty, focusing on how states seek to extend authority into the digital domain despite its inherently borderless nature. The chapter then outlines the related concepts of digital sovereignty, data governance, and AI, which further illustrate the increasing centrality of control over data and digital infrastructures. Digital sovereignty emphasises the capacity of states to manage their digital ecosystems independently, while data governance and technical standards emerge as critical mechanisms for ensuring the secure, ethical, and interoperable use of data and AI systems (Mistra et al., 2025). Overall, this chapter provides the analytical foundations for the study by linking theoretical perspectives with key concepts. It demonstrates how the interaction between *Netpolitik* and *Digitalpolitik*, alongside evolving notions of sovereignty, fragmentation, and technological governance, shapes the contemporary digital landscape and informs the dynamics explored in the subsequent chapters.

1.1 Netpolitik vs Digitalpolitik

The rise of digital networks has transformed the communicative foundations of international relations by lowering the costs of information transmission and diminishing the centrality of traditional intermediaries, such as governments, corporations, and legacy media. This shift has empowered a diverse range of actors, including NGOs, academic experts, journalists, diasporic communities, and other non-state entities. These actors have been able to establish global platforms, mobilise allies, and exert cultural and political influence. To capture these dynamics, Bollier (2003) introduced the concept of *Netpolitik*, which emphasises the strategic use of digital networks to shape politics, values, and identities. The proliferation of open-source initiatives and the acceleration of information flows have compelled governments to adapt to more decentralised and participatory environments, where traditional hierarchies of authority are challenged and new modalities of influence emerge. Consequently, these developments have given rise to forms of influence that challenge conventional decision-making hierarchies (Bollier, 2003).

Within this framework, soft power assumes a significant role. Public diplomacy, understood as the use of persuasion, education, cultural engagement, and trade to build support and legitimacy for particular values and policies, is of critical importance in the contemporary global context. An excessive reliance on coercive instruments, however, risks undermining influence in the face of global media scrutiny. The internet amplifies these dynamics by providing digital platforms for non-state actors to project images, mobilise support, and contest state narratives. As communication becomes increasingly decontextualised from its original cultural and social setting, the strategic shaping of perceptions and narratives becomes paramount. *Netpolitik* therefore extends soft power into the digital realm, where influence often depends less on factual accuracy than on identity, values, and interpretive frameworks. Narrative is employed as a chain of causality linking otherwise disconnected events, thereby shaping meaning and guiding perception in the context of digital diplomacy. These processes subsequently reconfigure social values, cultural identities, and political participation, enabling novel actors to exert influence in international politics and giving rise to innovative forms of soft power rooted in credibility, legitimacy, and cultural resonance (Bollier, 2003).

The advent of cyber-related events, encompassing both major conflicts and isolated cyber-attacks, has prompted scholars to reconsider notions of power and strategy within international relations, generating renewed interest in *Netpolitik*. In this context, traditional paradigms such as *Realpolitik* are complemented or, in some cases, supplanted by cyber-oriented strategies, in which classical concepts of power and balance acquire new meanings. The complexity of the digital

environment extends beyond the realm of cyberwarfare to encompass digital practices such as e-diplomacy, e-government, and e-republic initiatives, which constitute the practical foundations of *Netpolitik* in cyberspace (Anuta, 2013). *Netpolitik* is grounded in the principle of avoiding amoral coercion, aligning with liberal-oriented approaches that prioritise trade, peace, and freedom. This theoretical framework emphasises the softer dimensions of international relations, including moral legitimacy, cultural identity, societal values, and public perception, contrasting with the hard power focus of *Realpolitik*. *Netpolitik* is closely tied to liberal ideals such as democracy, civil society, and the protection of individual rights. It employs social networks, decentralised mechanisms, and globalisation to exercise influence, foster cooperation, and strengthen cultural and geographical ties (Duarte et al., 2024). By emphasising cooperation, narrative shaping, and moral legitimacy, *Netpolitik* demonstrates how digital networks empower non-state actors and amplify soft power, offering a liberal-oriented alternative to traditional, hard power approaches.

The concept of *Digitalpolitik* was initially introduced by Sean McDonald and An Xiao Mina in their 2018 *Foreign Policy* article, “The War-Torn Web”. Their intervention sought to capture the emergent dynamics through which states, private corporations, and civil society actors increasingly seek to shape the global digital environment via policy instruments, market leverage, and security apparatuses. *Digitalpolitik* is not rooted in the long-standing traditions of disciplinary fields, rather, it emerges from observations of internet fragmentation and the deliberate projection of state strategy into the digital sphere. The term denotes an arena of strategic contestation in which digital infrastructures, governance regimes, and normative frameworks are actively constructed, contested, and utilised. As emphasised by McDonald and Mina, governments and other actors seek to "project influence in global digital markets," leveraging regulatory, economic, and technological capacities to consolidate influence (McDonald & Mina, 2018, p. 2).

This logic is directly tied to the phenomenon of internet fragmentation. McDonald and Mina's (2018) analysis explores the fracturing of the formerly unified online world into competing entities, a phenomenon they refer to as the "Internet's Warring States Period” (2018,p. 4). In this context, the presence of competing digital policies gives rise not only to discursive and regulatory rifts but also to material separations in infrastructure and standards, resulting in the emergence of what has been termed "parallel internets" (2018, p. 4). A range of divergent strategies has been employed in response to this challenge, including the implementation of censorship regimes, sovereign cloud initiatives, data protection frameworks, and the export of surveillance technologies. These strategies have led to the

establishment of distinct technical and normative ecosystems. Consequently, *Digitalpolitik* is both a cause and an effect of fragmentation. The pursuit of national advantage in the digital domain is manifested in a divergence of policies that produces technical separation, thereby reinforcing the emergence of digital borders. This suggests that, rather than a borderless and universally accessible internet, the contemporary landscape reflects a patchwork of nationalised networks and standards, underscoring the extent to which digital infrastructures themselves have become central sites of geopolitical contestation (McDonald & Mina, 2018).

In essence, *Digitalpolitik* endows states with the capacity to redefine global power dynamics, conceptualising digital technologies as inherently coercive instruments. States employ a range of tactics, including surveillance, espionage, and cyber operations, to assert influence, control information flows, and undermine adversaries by leveraging digital networks (Atkinson, 2021). This approach treats digital capabilities not merely as tools of convenience but as instruments of political action and diplomacy, integrated into broader national strategies aimed at achieving technological supremacy and safeguarding digital sovereignty (Duarte et al., 2024). *Digitalpolitik* is characterised by values and objectives that reflect a realist and security-centred worldview. These include the prioritisation of state dominance over individuals, the exercise of control over domestic data and infrastructure, engagement in espionage, disengagement from globalised networks when advantageous, and the emphasis on "sharp power" over soft power (Duarte, 2025, p. 137). The framework privileges technological competition, viewing the international system as a zero-sum arena in which states must develop superior technologies while constraining the progress of rivals (Atkinson, 2021). The implementation of cyber operations, cyberwars, and comprehensive data collection has become imperative to achieving these objectives, ensuring that states are able to prevent deviant actors from disrupting order or challenging authority (Duarte, 2025).

In practical terms, *Digitalpolitik* leverages digital networks to serve national interests. States use these networks to control critical infrastructure, disseminate narratives, spread disinformation, conduct espionage, and execute cyberattacks against adversaries (Atkinson, 2021). To secure global leadership in the digital domain, states must strategically manage technological advancement while restricting competitors. The framework thus positions technology and information control as central pillars of power, shaping international structures in ways that favour dominant actors rather than promoting cooperative global governance (Duarte et al., 2024). The repercussions of *Digitalpolitik* for global strategy are substantial. The digital sphere is redefined as an extension of traditional power politics, in

which cyber capabilities complement military strength and serve both offensive and defensive purposes. In contrast to approaches emphasising multilateral cooperation or shared digital governance, *Digitalpolitik* prioritises state survival, strategic advantage, and the projection of influence in competitive international arenas (Duarte, 2025). By integrating technological capability, information control, and cyber operations into national strategy, *Digitalpolitik* highlights the increasing centrality of digital power in shaping the contemporary world order. *Digitalpolitik* illustrates how states leverage digital technologies as instruments of power, prioritising security, control, and technological competition in international relations. By emphasising state dominance, cyber operations, and strategic influence, it reframes the digital sphere as an extension of hard power, offering a realist approach that contrasts sharply with cooperative, soft-power-oriented frameworks (Duarte et al., 2024). Table 1 below summarises the distinctions between the two concepts.

Table 1. Comparative table: Netpolitik vs Digitalpolitik

Aspects	Netpolitik	Digitalpolitik
Sovereignty	Globalisation	Digital sovereignty
Freedom vs Security	Freedom	Security
State vs Citizens	Protect individual rights	Prioritize state interests
Use of Digital Networks	Cooperation, connectivity	Power, influence
Actors	Non-state actors	Primarily states
Focus	Soft power, culture, legitimacy	Hard power, control, technology

Source: The candidate based on the sources above mentioned.

The comparison between Netpolitik and Digitalpolitik demonstrates how the digital domain has evolved from a space characterised by decentralised influence and soft power into one increasingly shaped by state control, strategic competition, and technological dominance. While *Netpolitik* emphasises openness, cooperation, and the role of non-state actors (Anuta, 2011), *Digitalpolitik* reflects a more security-driven logic, in which states seek to assert authority over digital infrastructures and information flows (Duarte et al., 2024). This subsection therefore builds on the theoretical foundation by

examining how sovereignty is applied in cyberspace and how competing approaches to cyber-sovereignty contribute to the fragmentation of the global Internet.

1.2 Cyber Sovereignty, Cyberspace and Fragmentation

The concept of sovereignty, traditionally a state's authority over its territory, faces new complexities in cyberspace. While the principle remains relevant, its application differs between states and legal scholars. Some emphasise it as a fundamental norm for internet governance and cyber activities, seeking respect for their digital space. Others adopt a more cautious approach, often in opposition to certain legal interpretations, without emphasising its significance. Many states recognise that international law applies to cyberspace, yet there is no consensus on how sovereignty should be interpreted or enforced. Experts debate its role as a regulatory norm or as a distinct legal rule. This ambiguity highlights the need for further development of international norms. Sovereignty in cyberspace remains an evolving concept, with its application varying and ongoing discussions concerning its legal nature, scope, and obligations. While most agree that sovereignty applies to cyber activities, how it constrains or guides them remains an active international debate (Krasikov & Lipkina, 2020).

Cybersecurity and sovereignty are central to the governance of cyberspace, shaping how states regulate, protect, and control their digital environments within the broader international legal framework. Sovereignty, traditionally understood as a state's supreme control over its territory and internal affairs, is challenged in cyberspace due to its borderless nature. As digital infrastructure spans multiple jurisdictions and involves non-state actors, states seek to control data, infrastructure, and cyber activities within their borders through measures such as data localisation, content regulation, and national firewalls, collectively referred to as efforts in digital sovereignty. These sovereignty claims influence cybersecurity policies by prompting states to prioritise national security interests over international openness and cooperation (Ivanova et al., 2022).

Examples include the use of internet shutdowns or stricter content controls, which can hinder the free flow of information and international collaboration, both essential for effective cybersecurity. International law shapes the negotiation and regulation of sovereignty at a global level, providing a framework for cyber governance based on principles such as sovereignty, non-intervention, and the prohibition of the use of force. It encourages responsible state behaviour and prohibits cyber operations that violate territorial integrity or involve coercive intervention. However, the absence of specific, tailored international agreements in cyberspace creates tensions. States interpret these principles differently, while some advocate strong control and protective measures reflecting sovereignty, others emphasise

keeping an open and interoperable internet. This divergence affects the development of international legal mechanisms for addressing cyber incidents. In sum, cybersecurity is closely linked to sovereignty, and both shape the evolution of international law in cyberspace. The dynamic and borderless nature of cyberspace requires ongoing normative development, balancing national sovereignty with collective security and cooperation (Gul et al., 2025).

The concept of cyber sovereignty refers to a nation's right to govern and regulate ICT infrastructure, data, and activities within its national borders. It asserts that sovereignty, traditionally understood as authority over territory, extends into cyberspace, enabling nations to determine their own cyber policies, manage internet content according to national conditions, and prevent foreign interference or activities that might undermine national security or interests. Cyber sovereignty emerged in response to the evolving internet and its governance architecture, a multi-stakeholder model criticised for its lack of a clear hierarchy and for the disproportionate influence of some participants. As the internet grew in importance, many states recognised the need to control their digital domains due to concerns about security, cultural values, and external influence. This has challenged the multi-stakeholder model and highlighted some states' desire for greater recognition of their authority over cyberspace. It has also fuelled discussions about balancing national security, human rights, freedom of expression, and the free flow of information. Cyber sovereignty remains a point of contention in international forums, where efforts to establish rules and norms for cyberspace are ongoing, producing differing visions of internet governance. Some advocate decentralised, inclusive governance to protect innovation and freedoms, while others emphasise national interests, security, and cultural values. Cooperation and competition coexist within the international community, and the future of internet governance remains evolving and fractious (Qiao-Franco, 2024).

Authoritarian and democratic countries adopt different approaches to cyber sovereignty, reflecting their political ideologies and governance priorities. Authoritarian states emphasise state control and national security, using cyber sovereignty to enforce strict surveillance, censorship, and control over their digital spaces. These measures suppress dissent, minimise foreign ideological influence, and maintain regime stability, but raise ethical concerns relating to freedom of expression, privacy violations, and the potential for digital authoritarianism. Additionally, such controls may stifle innovation and hinder international cooperation. In contrast, democratic countries seek to balance cybersecurity needs with preserving internet openness and protecting individual rights. Multi-stakeholder governance and cyber diplomacy encourage international cooperation. However, cyber threats require a

re-examination of policies such as data localisation, to protect national interests without compromising fundamental freedoms. Democratic states use cyber sovereignty to reconcile national security with the preservation of digital freedom and privacy, whereas authoritarian regimes use it to consolidate control and suppress opposition. Their strategies, and their impacts on internet governance and individual rights, differ (Ahktar & Iqbal, 2025). The Internet significantly influences global power dynamics. It enables authoritarian states to assert greater cyber sovereignty by creating restricted digital networks that filter and limit foreign influence, while controlling information flows, media, and online users within their borders, effectively erecting a "digital iron curtain" (Haber & Topor, 2023, p. 144).

By controlling all aspects of cyberspace, these countries are better able to protect domestic affairs from foreign interference and cyberattacks. This capacity also allows authoritarian states to more effectively employ cyber proxy warfare, as these "internet bubbles" make it more difficult for adversaries, particularly liberal democracies, to attribute cyberattacks or counter foreign influence (Haber & Topor, 2023, p. 145). Democracies generally face legal and constitutional constraints in imposing similar restrictions, placing them at a strategic disadvantage in defending against cyber proxy wars. The uneven capacity to govern cyberspace contributes to an asymmetry of power, favouring states with such internet bubbles. Furthermore, these bubbles fragment the global internet, affecting international relations by reducing shared norms, complicating cooperation, and amplifying risks and information warfare for states exercising sovereignty over their territories. Internet bubbles enhance authoritarian states' control and resilience in cyberspace, challenging the liberal democratic framework that previously enabled them to operate and defend their interests. This development fundamentally shifts global power dynamics (Haber & Topor, 2023).

This growing disparity in cyber governance and power directly contributes to broader processes of digital fragmentation across the global internet. Digital fragmentation is driven by technical, governmental, and commercial factors that challenge the global digital ecosystem. One key driver is national data regulation, which creates rules and constraints that impede internet services and technologies across borders. Another crucial factor is geopolitical competition, which extends to infrastructure, production, and financial systems. This raises the prospect of a "splinternet," in which the world fragments into separate blocs with distinct digital ecosystems (Mayer & Nock, 2025, p.2). Commercial practices by dominant platform firms also contribute to digital fragmentation, shaping how users and businesses interact in the global digital economy. These practices impose constraints and controls over access to services and data, while technical fragmentation hinders internet interoperability

and functionality. The pursuit of digital sovereignty by states and regions disrupts integrated global governance and supply chains, driven by broader policy shifts and new forms of state activism. Taken together, these factors shape a multifaceted landscape in which digital fragmentation is both a driver and a consequence of contemporary economic, political, and technological dynamics (Mayer & Nock, 2025).

Several factors exacerbate this fragmentation. First, infrastructural issues such as bottlenecks and congestion can cause delays in data transmission. Second, inefficiencies in protocol routing can create isolated regions. Third, the slow adoption of IPv6, the next generation of internet addressing, means some regions may be left behind. Finally, security measures such as firewalls, DNS filtering, and IP blocking, while designed to protect national interests, can also create divided networks by restricting cross-border data flows. These challenges are further compounded by geographical disparities in infrastructure, including damage to undersea cables or limited access to modern fibre-optic technology in developing regions. High latency and throughput constraints also degrade the user experience, particularly during peak periods, potentially reinforcing the emergence of more isolated networks. Internet fragmentation, driven by regional conflicts and national policies, constitutes a significant geopolitical concern. Such conflicts weaken the cyber resilience of affected countries, contributing to instability. Restrictions on data transfer and user filtering further divide the internet, undermining the free flow of information and eroding trust among global actors. The combined effect of technical and geopolitical factors fragments the internet, threatening its core principles of free, open, and universal connectivity (Svanadze et al., 2025).

Fragmented digital governance poses several challenges to international cooperation. It undermines the traditional model of an open and interconnected internet by creating informational borders that restrict the free flow of information across countries. Global digital trade and innovation are also hindered by such fragmentation. Increased operational costs and barriers for international companies arise from data localisation laws and stringent national regulations, which restrict cross-border data flows, thereby slowing technological advancement and complicating multinational business operations. The establishment of international cyber norms and agreements is further impeded by the absence of binding global standards. Without these, efforts to protect critical infrastructure and combat cyber-enabled influence operations remain limited. Increased state control and surveillance raise ethical concerns that erode trust between nations, thereby impeding collaboration and information sharing. These dynamics contribute to geopolitical tensions between those favouring open internet models and

those prioritising strict cyber sovereignty, complicating cyber diplomacy and potentially exacerbating conflicts in cyberspace governance. Fragmented digital governance thus challenges the global digital ecosystem, disrupting international cooperation on cybersecurity and complicating the balance between national security and individual rights and freedoms (Ahktar & Iqbal, 2025).

Legal ambiguities and enforcement challenges frequently arise from clashes between national laws and international agreements, as differing objectives and regulatory frameworks intersect. One key area of conflict lies between national data localisation mandates and the free movement of data under international trade agreements. Some countries require data to be stored and processed locally to enhance regulatory control, safeguard economic independence, and facilitate law enforcement access. However, such requirements may contravene international trade obligations, creating uncertainty for businesses and obstructing the development of a comprehensive and globally consistent cybersecurity governance framework. National regulations enforcing internet censorship, content filtering, and surveillance may also violate international treaties by restricting freedom of expression and privacy. The tension between national sovereignty and international legal principles in digital governance complicates coordinated action against cyber threats and undermines the open nature of the internet (Krishna, 2023).

Cyberspace, cybersecurity, and sovereignty are interconnected concepts central to modern international relations and state security. Sovereignty is traditionally grounded on physical territory and the authority exercised by states within their borders. However, cyberspace, which connects all regions globally and transcends state boundaries, challenges conventional understandings of sovereignty. Cyberspace underpins vital societal functions and is increasingly managed by the private sector, particularly in Western countries, while remaining essential for economic, political, and social interactions. Its original purpose was to foster connectivity and communication, however, it has evolved into a contested domain for data and digital technologies, facilitating cybercrime, espionage, and cyberwarfare. These activities threaten national security and state sovereignty by enabling malicious actors to operate anonymously across borders. Rapid technological advancements in areas such as AI and quantum computing further complicate cybersecurity, generating both opportunities and risks. States face challenges in protecting their digital infrastructure due to inadequate governance frameworks, asymmetrical threats, and limited resources. Cyber incidents can cause significant economic damage and provoke tensions between major powers with competing visions for cyberspace governance. Global governance of cyberspace remains fragmented, with no universal legal framework.

Multilateral, state-centric approaches emphasise government control and regulation, seeking to preserve sovereignty through national and international policies. By contrast, multi-stakeholder models advocate collaborative governance involving diverse actors and call for improved cooperation between nations to address security and sovereignty challenges posed by cyber activity. Inclusive governance approaches are therefore essential to balance sovereignty with global cooperation (Ijaz, 2024).

Cyberspace has transformed from a cooperative domain into one characterised by intense competition. Once governed largely by liberal Western norms, it is now fragmented into multiple domains aligned with the strategic interests of major powers. This fragmentation undermines the effectiveness of legal and diplomatic efforts to constrain strategic cyber competition. Such dynamics are likely to persist unless there is a significant realignment of relative power, typically associated with military conflict. In the absence of such a reset, cyberspace will remain a domain in which strategic competition continues below the threshold of armed conflict. Consequently, cyberspace has become a key arena in which states deploy cyber tools to gain economic advantage, undermine political cohesion, and erode trust in democratic institutions and governmental capabilities (Lynch, 2025). Table 2 below summarises the concepts illustrated throughout this subsection.

Table 2. Key Concepts in Cyberspace Governance

Concept	Definition	Key Idea
Cyberspace	A global digital environment for communication, economic activity and information exchange.	Challenges traditional sovereignty and provides space for asserting cyber sovereignty.
Cyber Sovereignty	A state's control over its digital space (data, infrastructure, content).	Imposes national controls over the internet and can drive policies that restrict openness and cause fragmentation.
Digital Fragmentation	The breaking of the global internet into separate, controlled or incompatible systems.	Cyberspace is divided due to cyber sovereignty policies and geopolitical/technical factors.
Dynamics Between Concepts	Interaction between global connectivity and national control.	Cyberspace enables connectivity → states assert cyber sovereignty → leads to fragmentation → fragmentation reshapes cyberspace and limits global cooperation.

Source: The candidate based on the sources above mentioned.

The analysis of cyber sovereignty, cyberspace, and fragmentation illustrates how state efforts to assert control over the digital domain have contributed to the emergence of a more divided and competitive global internet. These dynamics reveal not only the limitations of existing governance frameworks but also the growing importance of control over digital infrastructures and information flows as sources of power. As cyberspace becomes increasingly fragmented, the focus shifts from governance of the internet as a whole to the strategic management of data and digital technologies within and across borders (Ijaz, 2024). This subsection therefore builds on these insights by examining the concept of digital sovereignty in greater depth, with particular attention to its relationship with data governance, artificial intelligence, and technical standards in shaping contemporary global power structures.

1.3 Digital Sovereignty, AI and Data Governance

In today's digital age, digital sovereignty is crucial for security, stability, and independence. It refers to the ability to control and supervise digital assets, infrastructure, and data without reliance on external actors. Control over data is central to this concept, as data powers AI, IoT (Internet of Things), and other emerging technologies. Governments and industries must therefore ensure that personal, industrial, and national data are properly managed, processed, and protected, fostering trust through the ethical use of data. Digital infrastructure, including data centres, networks, and cloud platforms, is equally vital, underpinning the entire digital ecosystem. Investment in resilient digital architectures helps to prevent disruptions caused by cyberattacks, system failures, or geopolitical tensions, while also reducing dependency on foreign providers. Ensuring the authenticity, fairness, and explainability of AI systems further strengthens public confidence and upholds human-centric values. Maintaining control over data, infrastructure, and digital tools is thus essential for trust, resilience, and independence in an interconnected world. Collectively, these elements constitute the core of digital sovereignty, enabling nations and organisations to innovate responsibly while safeguarding their interests amid geopolitical complexities (Mistra et al., 2025).

Digital sovereignty is a concept that challenges global governance by emphasising national or regional control over digital infrastructure, data governance, and regulatory regimes. This fragmentation contributes to the fragmentation of the global digital ecosystem, contrasting with its previously more integrated nature. States increasingly implement their own regulations concerning data collection, critical infrastructure, and online censorship. This form of technological sovereignty disrupts global governance and affects international supply chains, challenging established digital governance and trade frameworks, as well as long-standing integration and cohesion. Geopolitical competition between

major powers further intensifies this fragmentation. Techno-nationalist policies that prioritise distinct techno-spheres may emerge, resulting in disconnected internets and decoupled global production networks. Such developments challenge traditional conceptions of a unified global digital space. Regional actors are attempting to navigate this evolving landscape by articulating varying concepts of digital sovereignty. However, these constitute a patchwork of approaches lacking a coherent, unified policy, thereby contributing to the complexity and fragmentation of global governance. There is also a tension between protecting digital sovereignty and maintaining collective global public goods, such as cybersecurity. State-driven regulation may enhance national control and privacy, but it risks diminishing the global collaboration that is essential for addressing cross-border digital challenges. Digital sovereignty shifts power away from global, multi-stakeholder, and international governance frameworks towards sovereign states and regional blocs seeking control over digital spaces. This reorientation generates new tensions, accelerates fragmentation, and poses significant challenges to existing digital governance frameworks (Mayer & Nock, 2025).

Digital sovereignty and expansionism are shaping prospects for global AI cooperation. Technical standard-setting for AI has become a critical battleground. These dynamics generate tensions, as each actor seeks to impose its policies on other countries. Divergent governance models risk fragmenting the field and impeding effective AI deployment. Nationalistic and competitive narratives that frame AI as a geopolitical rivalry may further intensify tensions and discourage states from collaborating on shared governance. Industry actors often resist regulations, further complicating the development of coherent governance frameworks. Such strategies generate extraterritorial conflicts and competition, undermining efforts to harmonise global AI governance (Roberts et al., 2023).

The rapid advancement of AI is reshaping global power structures, positioning digital capabilities as a central pillar of geopolitical influence. AI has become a strategic asset linked to economic strength, national security, and international status, with data emerging as a critical resource. Control over digital infrastructure, computational power, and data flows is essential for countries seeking AI supremacy and geopolitical dominance. Nations that cultivate advanced AI research ecosystems, secure digital infrastructures, and implement effective data governance are better positioned to influence global institutions and markets. However, tensions between national control and globalisation are intensifying, as states increasingly localise data storage, restrict exports, and promote domestic AI industries in pursuit of strategic autonomy. This trend contributes to a fragmented global AI landscape with divergent governance models. Without digital sovereignty, countries risk economic

instability and compromised national security in an era marked by cyber threats and the dominance of multinational technology firms. Consequently, states are investing heavily in AI to secure competitive advantage, shape international norms, and strengthen digital infrastructures across sectors such as supply chains, 5G, cybersecurity, and standards. Control over digital resources and innovation is thus becoming synonymous with geopolitical power, signalling a shift in which digital capabilities define the future balance of global influence (Tiwari, 2025).

Within this context, AI is transforming organisational operations, particularly in cybersecurity, regulatory compliance, and competitive intelligence. In cybersecurity, AI enhances threat detection by analysing network traffic and identifying malicious behaviour in real time. For example, hybrid neural networks improve sensitivity to sophisticated attacks, such as DNS tunnelling, enabling rapid detection and response. This capability is critical for protecting infrastructure against adversaries who continuously evolve their methods. In regulatory compliance, AI automates reporting and monitoring processes, reducing errors and biases that could undermine legal adherence. By parsing complex regulatory documents and flagging inconsistencies, AI helps organisations remain compliant in rapidly changing regulatory environments. AI also plays a pivotal role in competitive intelligence, particularly when combined with blockchain technologies. AI-driven analysis enables the processing of complex datasets, improving the identification of trends and patterns beyond traditional methods. Machine learning supports automated technology assessments and early-warning systems that detect anomalies in real time, while predictive analytics and scenario planning enhance strategic decision-making. Hybrid approaches that integrate human expertise with AI capabilities further optimise analytical outcomes. Concurrently, blockchain strengthens competitive intelligence by providing secure, tamper-resistant records. Its decentralised and transparent nature supports compliance, enforces regulatory frameworks, and reinforces autonomy and standard-setting authority. Blockchain also safeguards sensitive information and enables secure information sharing, ensuring the integrity of intelligence workflows. Together, AI and blockchain transform competitive intelligence into a proactive, real-time strategic capability, enabling nations and organisations to navigate technological competition while maintaining digital sovereignty and achieving technological leadership (Ezenwaka, 2025).

Despite these benefits, AI systems introduce significant challenges related to data governance, security, and trust. AI's reliance on data renders its performance and reliability highly dependent on data quality, provenance, and continuous monitoring. Poor data governance can result in biased algorithms, vulnerabilities such as data poisoning, and regulatory non-compliance. Robust data

governance frameworks are therefore essential to mitigate these risks. Such frameworks ensure data integrity, privacy, lawful use, access control, and ongoing oversight throughout the AI lifecycle, from data collection and storage to model development and deployment. They also align people, processes, and technology, establishing accountability and ethical stewardship while bridging gaps between cybersecurity, compliance, and business objectives. As AI adoption accelerates, embedding governance within AI strategies becomes critical for enabling secure, ethical, and trustworthy systems. Institutions that do so can meet regulatory requirements, unlock AI's potential safely, and sustain public confidence (Rajgopal & Yadav, 2025).

At the same time, the pursuit of digital sovereignty raises complex policy trade-offs between control and innovation. Different states adopt varying approaches based on their political values and strategic priorities. Some implement highly regulated digital environments characterised by strong government control, state-led industrial policies, and data localisation, which may support AI development aligned with national goals. Others favour less restrictive frameworks that encourage private-sector innovation, although growing public and security concerns are prompting increased regulation even in these contexts. While open policies may accelerate innovation, they can reduce control over data and systems. Conversely, restrictive policies may enhance security and protect social values but risk slowing technological progress. Strict digital borders can limit international cooperation, reduce interoperability, and fragment the global digital ecosystem, creating inefficiencies and hindering innovation. They may also contribute to geopolitical tensions and digital protectionism, undermining global norms and collaboration. Thus, while digital sovereignty aims to enhance security and autonomy, excessive control can ultimately constrain innovation and weaken economic and strategic outcomes (Woods, 2023).

States balance digital sovereignty with their reliance on global technology infrastructure by asserting control while collaborating with private actors. They seek to maintain digital sovereignty by controlling AI infrastructures and regulating powerful technology firms. Sovereignty is also understood as a social practice involving cooperation between governments and private companies. Public-private partnerships are common in domains such as smart city development, health initiatives, including COVID-19 contact tracing, and law enforcement surveillance efforts. These collaborations suggest that sovereignty is enacted through shared roles rather than implying exclusive state control. This balance recognises that frontier AI systems are primarily developed by private companies with global resources, as states cannot easily replicate them. Therefore, states use legislation and cooperation with these

companies to retain influence. Digital sovereignty does not imply total state control but illustrates the complex interplay between public and private power in global AI governance. States seek to manage AI infrastructure while working with global technology providers to address the challenges and opportunities of the digital environment (Srivastava & Bullock, 2024). These tensions are further reflected in the broader challenges of global AI governance. The absence of common technical standards complicates interoperability between AI systems worldwide, thereby hindering the development of cohesive regulatory frameworks. The uneven distribution of AI capabilities exacerbates global power imbalances, making consensus on governance norms more difficult. Concerns regarding privacy, national security, and commercial confidentiality further restrict data sharing, which is essential for many AI applications. This, in turn, limits cooperation and erodes trust in AI development and deployment. Additionally, overlapping and, at times, conflicting claims to authority among states, international organisations, and private actors result in fragmented norms, uneven accountability, and regulatory arbitrage. Large technology corporations often wield significant de facto regulatory power without corresponding state oversight. These challenges are intensified by the rapid and unpredictable evolution of AI technologies. Although there is widespread recognition of the need for international governance, establishing effective global AI governance frameworks remains a complex and ongoing endeavour (Yilmaz, 2026).

Data governance and technical standards can mitigate tensions between differing national approaches to digital sovereignty and AI governance by providing common frameworks and facilitating interoperability. Data governance, particularly regarding cross-border data flows, represents a key area for cooperation. By collectively establishing norms around data categories, states can reduce uncertainty, build trust, and help mitigate conflicts while fostering collaboration in AI development and deployment. Technical standards are essential for ensuring that AI systems are compatible, safe, and reliable. Standards can lower barriers to cooperation by enabling international collaboration. However, standard-setting is inherently political, reflecting underlying social and economic values. The technical and procedural nature of standard-setting provides a relatively neutral space for negotiation. Together, data governance frameworks and international standards offer practical entry points for multilateral engagement on AI governance. These mechanisms address operational and regulatory challenges, help build confidence, and lay the groundwork for global AI governance regimes. Focusing on these areas provides a strategic pathway to ease tensions and promote international cooperation in a contested digital landscape (Roberts et al., 2023). Table 3 below summarises the interconnection of the concepts presented in this subsection.

Table 3. Core Concepts and Dynamics of Digital Sovereignty and AI Governance

Concepts	Definition	Correlation
Digital Sovereignty	State control over digital systems, data, and technologies	Shapes data governance and AI development. Can restrict or enable cooperation.
Data Governance	Rules and frameworks for managing, protecting, and using data	Enables reliable, ethical AI and cooperation between countries.
Artificial Intelligence (AI)	Data-driven technologies used for automation, analysis, and decision-making	Depends on high-quality data governance and can become a tool of power under digital sovereignty
Technical Standards	Shared rules ensuring systems are compatible, safe, and interoperable	Enable cooperation between different sovereignty approaches to reduce fragmentation.
Dynamics Between Concepts	Interaction between control, innovation, and cooperation	Digital sovereignty influences data governance → data enables AI → AI drives competition → technical standards help maintain interoperability and cooperation

Source: The candidate based on the sources above mentioned.

In summary, the theoretical frameworks of *Netpolitik* and *Digitalpolitik*, together with the concepts of cyber-sovereignty, digital sovereignty, and fragmentation, demonstrate how control over cyberspace, data, and emerging technologies has become central to contemporary power dynamics. States increasingly leverage digital infrastructures, regulatory frameworks, and AI-enabled capabilities to assert authority, manage information flows, and shape both domestic and international digital environments (Haber & Topor, 2023). These dynamics produce a fragmented and competitive global internet, in which national strategies interact with technical standards, data governance, and international norms, highlighting the tensions between sovereignty, cooperation, and innovation (Mayer & Nock, 2025). Building on this foundation, the following chapter focuses on China's approach to cyberspace governance, analysing how its domestic legal, technological, and surveillance architecture supports cyber sovereignty, and how these principles are projected internationally through normative, diplomatic, and technological initiatives.

2. China's approach to the cyberspace

This chapter examines China's approach to the governance of cyberspace at both national and international levels. The Chinese president, Xi Jinping, has emphasised the importance of cybersecurity, as well as the development of technology and law-based governance of cyberspace (State Council, 2023b). The first part of the chapter analyses the national approach to cybersecurity and cyberspace governance, beginning with an examination of the legal and institutional foundations of China's cybersecurity regime. As Chaskes (2022) observes, three main laws constitute the bedrock legal infrastructure for achieving China's cyberspace and geopolitical ambitions. The chapter also explores how China's use of AI in its cyberspace strategy is linked to increasing surveillance and social control. The second part focuses on China's position on the international stage by analysing the concept of cyber sovereignty and the methods through which it is implemented. In this context, it examines China's articulation of internet sovereignty as a normative claim that seeks to legitimise state jurisdiction over segments of the internet within national borders (Wang, 2020). Finally, the chapter concludes with an analysis of how China employs technical standardisation and the global provision of ICT goods to influence the international order. China is a major provider of ICT products, encompassing both consumer devices and telecommunications infrastructure. The export of these products facilitates access to data-enabled services, with the DSR initiative playing a central role in China's strategy (Borgogno & Zangrandi, 2024).

2.1. National cybersecurity approach

China's national approach to cyberspace governance integrates technological development, law, and politics under state authority. Cybersecurity and digital governance form part of broader modernisation and regime stability objectives. This reflects the Chinese Communist Party's (CCP) commitment to governing cyberspace through institutional and technological means (Creemers, 2023). This approach has resulted in an extensive legal architecture and sophisticated monitoring systems, which together constitute the instruments through which national cyberspace policy is implemented (Zeng, 2022). The following subsections examine the legal and institutional foundations of China's cybersecurity regime and the expansion of state surveillance enabled by digital technologies, highlighting how these elements jointly sustain China's distinctive model of cyberspace governance.

2.1.1 Legal Framework

The Central Leading Group for Cybersecurity and Informatisation, now referred to as the Central Cyberspace Affairs Commission (CCAC), was established in 2014 under President Xi Jinping. This marked digital policy as the top national priority and contributed to the development of China's

"cyberpower strategy". As a result, the technology agenda has become a central component of China's attempts to adapt to the challenges of the “new era” proclaimed by Xi (Creemers, 2023, p.2). However, the potential benefits of informatisation depend on robust security measures. Xi emphasises that cybersecurity and informatisation are "two wings on the same body, and two wheels of the same vehicle" (Xi, 2014, p.2).

In line with this integrated approach to digital development and security, China's data governance framework is based on three laws. The Cybersecurity Law (CSL) (2016), the Data Security Law (DSL) (2021), and the Personal Information Protection Law (PIPL) (2021). These build on the principles set out in the National Security Law (NSL) (2015), alongside a large body of national and local regulations and standards to follow. The NSL codifies Xi Jinping's expansive national security vision, mandating a nationwide network and information security system to protect cyber sovereignty and development interests, and empowering the Cyberspace Administration of China (CAC). Despite the limited scope of the NSL, it established legal constraints on state organs and emphasised adherence to constitutional requirements, including the protection of citizens' rights. The subsequent "Three Laws" (2015,p.7) expand these constraints while operationalising cybersecurity, data governance and personal information protection, with a marked emphasis on promoting the security of cyberspace and the orderly flow of data to support economic and social development (Horsley, 2025). China's laws reflect its complex regulatory environment, coexisting with various national and local regulations and standards due to the absence of a unified data protection statute (Data Protection Laws of the World, 2025). The three statutes are interconnected, and collectively they establish a top-down regulatory framework in which national security is the principal concern (Niu, 2025).

The CSL incorporated the Multi-Level Protection Scheme [1](MLPS) while establishing a new Critical Information Infrastructure (CII) regime, creating potential overlaps where networks qualified under both systems. Drafts for an updated MLPS (MLPS 2.0) were never fully implemented, with only technical standards being issued. In 2021, the State Council of China promulgated definitive CII regulations, centralising authority under the MPS while sector-specific ministries retained operational responsibilities. The regulations introduced institutional measures, including the vetting of senior cybersecurity staff and the requirement for operators to develop incident response plans and technical support structures. The system as a whole indicates a shift towards more centralised oversight of

[1] The Multi-Level Protection Scheme (MLPS) of China is a legally mandated cybersecurity classification and protection framework that is stipulated within the nation's Cybersecurity Law. The scheme requires information systems to be categorised into five security levels based on their importance and potential impact on national security, public interests, and individuals' rights (Tencent Cloud, 2025).

critical networks, balancing sector-specific management with national-level coordination. However, the full integration and clarity of this system are still in a state of evolution (Creemers, 2023).

The evolution of China's cybersecurity governance through the integration of the MLPS and the establishment of a centralised CII regime provides an effective illustration of *Digitalpolitik* in practice. By consolidating oversight under the authority of the Ministry of Public Security of China while maintaining sector-specific operational responsibilities, the Chinese state projects strategic authority directly into the digital sphere, treating critical networks as instruments of national security rather than neutral infrastructures (Creemers, 2023). This approach aligns with the conceptualisation of *Digitalpolitik* as a form of strategic contestation proposed by McDonald and Mina (2018). In this context, states leverage regulatory and institutional power to shape digital environments and project influence (Duarte et al., 2024). It is evident that China's evolving CII framework exemplifies how *Digitalpolitik* functions both as a tool of digital sovereignty and as a manifestation of broader geopolitical competition. This integration of digital governance into national security strategy occurs while the framework remains in a state of adaptive and contested development.

Five years after the CSL was adopted, the DSL was introduced to regulate all data processing within China. This encompasses the collection, storage, use, processing, transmission, provision, and disclosure of data by companies, organisations, and regulators. It establishes a framework for categorising, grading, and regulating all data collected and stored in China by any type of entity, based on its potential impact on economic and social development, as well as national security. The DSL seeks to protect the public's rights and interests while also safeguarding data security, state sovereignty, and national security. It aims to ensure the free flow of data in an orderly and lawful manner, and to promote data utilisation to develop the digital economy and public services (Horsley, 2025).

The most significant contribution of the DSL is a tiered classification scheme for "important data" and "national core data", with national core data subject to the highest levels of restriction (Niu, 2025, p.3). This system is designed to protect data against misuse and risk. It defines data as either ordinary, important, or core. This proactive approach is supported by requirements for risk assessments, reporting, and early-warning mechanisms, with the aim of managing the new risks generated by informatics (Naughton, 2021). Following the governance logic of the cybersecurity MLPS under the CSL, the DSL regulates data handling and security through a hierarchical data classification mechanism. The DSL stipulates that the state must establish this mechanism and organise data under

it according to its importance to economic and social development, and the extent to which it could harm national security, public interests, and the legitimate rights of individuals and organisations. It sets out a top-down administrative process for implementing this mechanism at the state level (Chen & Sun, 2021).

China's PIPL has emerged as a central pillar in the country's evolving cybersecurity and data governance architecture. It represents a significant milestone in China's regulatory landscape by establishing comprehensive rules for the protection of personal information and imposing stringent obligations on enterprises. These obligations form an integrated framework for governing data and cybersecurity across digital environments, in conjunction with the earlier CSL and DSL (Calzada, 2022).Within this broader system, the PIPL further refines regulatory expectations by articulating individual data rights and expanding duties for data handlers, particularly concerning security safeguards, cross-border data transfer controls, and the management of "important data", thereby strengthening China's overarching data governance regime (Greenleaf, 2021, p.6).

It also establishes fundamental definitions for personal information and personal information handling, and identifies "personal information handlers" as entities that independently determine data-processing purposes and methods (Calzada, 2022, p.8). As defined by Torrisi (2023), the term personal information handling refers to "the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information" (Torrisi, 2023, p.30). These regulations designate sectors and data as vital to national security and the public interest. Through these linkages, the PIPL reinforces heightened security requirements for CII operators and other entities managing sensitive or strategically significant data. These measures serve to advance China's digital sovereignty and its influence over transnational data flows. More broadly, the PIPL's stringent security obligations, and its alignment with state cybersecurity and surveillance priorities, underscore China's efforts to construct a secure and tightly governed information environment, thereby furthering national strategic objectives and strengthening resilience in cyberspace (Greenleaf, 2021).

Furthermore, chapters four to six of the PIPL establish a multi-stakeholder governance framework, delineating the rights of individuals, the obligations of data handlers, and the supervisory responsibilities of state authorities. Individuals have greater control over their personal data, including rights to access, correct, delete, and obtain information about data processing, with some protections extending to deceased persons. Data handlers, particularly major online platforms, must adopt security measures, conduct impact assessments for sensitive data, and be subject to external oversight. State

authorities oversee compliance, address public complaints, and establish technical and regulatory standards. The PIPL clarifies these respective duties, aiming to safeguard individual privacy and guide enterprises towards lawful, transparent data practices, thereby fostering trust and promoting ethical data use (Calzada, 2022). With regard to the processing of personal information within China, it is important to note that such processing is carried out by Chinese companies or local affiliates of these companies. Multinational corporations are subject to the provisions of the PIPL, provided that the organisation is based in China (Torrisi, 2023). Prominent examples under the PIPL include companies such as Alibaba and JD, which collect a wide range of data on users. In accordance with the legal framework established by this law, digital platforms are obliged to provide users with comprehensive information regarding the nature of the data being collected, the manner in which it will be utilised, and the necessity of obtaining users' consent. Furthermore, it is essential that mechanisms are implemented to facilitate the withdrawal of consent by users, along with the subsequent deletion of their personal data (Huáng, 2025).

The introduction of the DSL and the PIPL represents a further consolidation of China's *Digitalpolitik* logic by extending state-centric control from network security into the domain of data itself. The Chinese state has institutionalised a hierarchical governance model that explicitly links data management to national security, social stability, and economic development (Niu, 2025). This top-down system mirrors the logic of the MLPS under the CSL, reinforcing a proactive, risk-based approach to governing digital resources as strategic assets (Chen & Sun, 2021). In the context of *Digitalpolitik*, this framework reflects the intentional extension of state power into digital infrastructures through regulatory instruments devised to protect sovereignty and oversee informatics-related risks, thereby contributing to the fragmentation of global data governance systems. Table 4 below summarizes the core functions and regulatory focus of these laws, as well as the connection between the logic of *Digitalpolitik*.

Table 4. Core Digital Governance Laws and the Institutionalisation of Digitalpolitik in China

Law	Adopted in	Function	Regulatory Focus	Digitalpolitk
Cybersecurity Law (CSL)	2016	Network and infrastructure security	MLPS, Critical Information Infrastructure (CII)	Anchors national security by institutionalising state control over networked infrastructures.
Data Security Law (DSL)	2021	Data security and state control	Data classification, national security	Shows data as a strategic resource, strengthening governance of data flows and sets.
Personal Information Protection Law (PIPL)	2021	Personal data protection	Individual data rights, obligations of data handlers	It combines personal data with a state-centred regulatory framework.

Source: The candidate based on the sources above mentioned.

China's legal and institutional frameworks for cybersecurity and data governance, exemplified by the CSL, DSL, and PIPL, establish the foundation for state control over networks and information flows (Greenleaf, 2021). The next subsection of the chapter will examine how these frameworks are operationalised in practice through China's digital surveillance systems, highlighting the integration of state authority into digital infrastructure and social behaviour.

2.1.2 State surveillance and digital authoritarianism

The digitalisation of Chinese society has produced significant and unexpected outcomes. It has made everyday life easier while enabling the government to exert control over society more efficiently (Cabestan, 2020). The CCP views technology as a primary driver of China's growth and influence. President Xi Jinping recognises the power of technology, particularly digital platforms, in driving economic growth, governance, and organisation. At the 2022 Party Congress, he reiterated the CCP's belief in an objective, intelligible set of social laws. Big data and AI are perceived not merely as tools to better understand these laws, but also as instruments to shape society in order to advance the Party's objectives (State Council, 2016).

The Chinese approach to cybersecurity is grounded in the concept of cyber sovereignty. From this perspective, substantial data collection and information gathering are indispensable foundations for

AI development, which in turn enables greater influence over global markets. As Chang (2023) argues, this ambition centres on promoting state-led surveillance as a legitimate governance practice, alongside restricting the free flow of information across borders. Internet security and information control represent a pivotal national priority for China, conceptualised ideologically through the doctrine of cyber sovereignty. Although the concept remains ambiguously defined, its manifestation is most clearly evidenced in extensive censorship practices and stringent restrictions on data access, whereby control over domestic data is effectively reserved for the CCP alone (Chaskes, 2022). A comprehensive understanding of cyber sovereignty and its implications therefore requires close attention to the Chinese model of centralised governance, as well as to the absence of clear theoretical or institutional boundaries between the public and private sectors within the Chinese political economy (Olson, 2020). In recent years, China has witnessed substantial advancements in its digital control capabilities, signalling a pronounced transition towards the adoption of progressively intrusive surveillance technologies. These technologies facilitate the collection of highly detailed data concerning citizens' daily activities (Chen & Zhan, 2025). The development of ICT, particularly in the domain of surveillance, has also addressed what is commonly referred to as the vertical information problem in authoritarian regimes. The facilitation of widespread digital communication among citizens by ICT generates vast quantities of digital data, which can be systematically accessed and analysed by the state to enhance governance and control (Xu, 2021).

The Chinese government employs numerous methods to control information, which is regarded as one of the most extensive and sophisticated censorship systems in the world. Consequently, China's surveillance regime is best understood as a complex system of public-private collaboration (Roberts, 2018). Driven by imperatives of regime stability and social control, China has constructed an advanced surveillance infrastructure by systematically leveraging the technological capacities of private enterprises. These firms do not merely execute state directives passively. They function as active participants within the surveillance ecosystem, often extending technological capabilities beyond the state's original expectations. Due to limited funds and technology, public security bureaux rely on private companies for advanced surveillance systems. This has created a competitive market in which major companies such as Hikvision and Dahua secure government contracts, while smaller firms focus on community and specialised systems (Woods, 2025). The Chinese government has established the Chinese Security and Defense Standardization Technology Committee (CSDSTC) to regulate the public-private interface and ensure interoperability among diverse surveillance systems. However, decentralised procurement practices and competitive pressures can result in excessive monitoring,

potentially provoking public resistance and undermining the effectiveness of surveillance (Huang & Tsai, 2022). The following Table 5 summarises the dimensions and logic behind China's digital governance and surveillance logic.

Table 5. Digital Governance and Surveillance Logic in China

Dimension	Core Logic	Outcome
Digitalisation	Convenience and control advance simultaneously	Expanded state governance capacity
Party-State Ideology	Technology serves political and developmental goals	Legitimation of data-driven social management
Big Data and AI	Data enables prediction and behavioural shaping	Governance through algorithmic control
Cyber Sovereignty	Cyberspace subject to state authority	Justification for censorship and data control
Surveillance System	ICT enables granular population monitoring	Resolution of information asymmetries
Public-Private Model	Surveillance co-produced with private firms	Intensified and decentralised social control

Source: The candidate based on the sources above mentioned.

In recent years, alongside state-led initiatives aimed at positioning China as a global leader in emerging technologies, the CCP has developed and deployed a range of advanced technological tools to monitor and regulate society (Qiang, 2019). Under the leadership of Xi Jinping, these efforts have intensified, marked by the expansion of digital surveillance infrastructures into rural areas and the integration of existing public security camera networks with privately operated camera systems. This increasingly comprehensive surveillance network now encompasses high-definition cameras, vehicle and licence plate recognition systems, and AI-driven facial recognition technologies, significantly enhancing the state's capacity for population monitoring and control (Rothschild, 2024). Surveillance is a key component of information gathering in China, used to suppress oppositional movements and maintain political control and social stability. Over the past decade, digital surveillance has become more widespread and intense. Instruments such as the Social Credit System (SCS) and monitoring technologies employed during the pandemic have been accepted by the public as necessary, beneficial, or convenient. As a result, public dissent typically emerges only when such measures are perceived as

unnecessary or devoid of purpose. China's system has demonstrated flexibility in incorporating new technologies, incentivising the adoption of digital tools that extend the state's capacity for surveillance and social control beyond traditional mechanisms of dispute resolution (Hu & Rossi, 2025).

The governance model is underpinned by the assumption that the ruling party inherently embodies and represents the interests of the public, and that the socialist core value system constitutes the guiding ideological foundation of Chinese legislation. Within this framework, social media platforms and public opinion channels function largely as conduits for official narratives, while voices operating outside the sanctioned system are framed as comparatively unreliable or untrustworthy (Huang, 2019). By 2017, China had deployed approximately 176 million CCTV cameras equipped with facial recognition. These technologies enabled authorities to conduct real-time monitoring, identify individuals, and access personal data held by private companies. Such systems can track movements, categorise demographic groups, and compile detailed citizen profiles, thereby facilitating centralised forms of social control. While these surveillance infrastructures provide powerful tools for security and policing, they also raise significant concerns regarding privacy (Vagianos & Stavrou, 2023).

China has implemented a large-scale digital surveillance and information control system, which can be understood as a consolidated expression of *Digitalpolitik*. In this context, digital technologies are systematically mobilised as instruments of state power, governance, and social control. The CCP's embrace of big data, AI, and digital platforms reflects a governing logic that treats technology both as an engine of economic growth and as a mechanism for shaping society in accordance with Party objectives and the principles of cyber sovereignty (Chang, 2023). The state has embedded national security and regime stability directly into digital infrastructure through extensive censorship, data extraction, and restrictions on information flows (Qiang, 2019). This exemplifies the security-centred and realist orientation identified in McDonald and Mina's (2018) concept of *Digitalpolitik*. The convergence of market forces and security apparatuses in advanced surveillance systems highlights the blurring of public-private boundaries and centralised control (Huang & Tsai, 2022). By normalising large-scale surveillance tools, such as AI-driven facial recognition, China has institutionalised a digitally specific governance model that contributes to internet fragmentation and positions information control as a core pillar of political authority and strategic power in the digital age (Hu & Rossi, 2025). Table 6 below showcases China's use of surveillance as a strategy to retain state power.

Table 6. Digital Surveillance as State Power in China

Focus Area	Governance	Political Effect
Technological Expansion	Surveillance tools are essential to modern governance	Enhanced capacity for social monitoring
Central Leadership	Digital control is prioritised under Xi Jinping	Accelerated and centralised oversight
Integrated Systems	AI and data fusion enable continuous identification	Real-time population tracking
Social Legitimacy	Surveillance framed as useful or protective	Broad public acceptance
Ideological Control	Official narratives define credible information	Marginalisation of dissent

Source: The candidate based on the sources above mentioned.

At the core of China's surveillance infrastructure is the Great Firewall, a sophisticated system comprising technological mechanisms and regulatory frameworks designed to restrict access to foreign websites, filter online content, and monitor digital activities (Griffiths, 2019). This system has effectively produced a distinct and insulated Chinese internet environment, within which the state can shape public discourse and limit citizens' exposure to politically sensitive or potentially destabilising information. State surveillance and information control extend beyond the digital sphere to traditional media platforms. The Chinese government exerts influence over these outlets by determining permissible content and regulating its production and dissemination. Journalists and media organisations face severe penalties for publishing material that challenges state authority or deviates from official narratives. Investigative journalism and independent media have been targeted in recent years, forcing many outlets to cease operations or function under significant constraints. Private companies operating online platforms in China are legally required to implement surveillance and content-control measures in accordance with government regulations, thereby integrating corporate actors into the state-led surveillance framework (Woods, 2025).

One of the most prominent and controversial manifestations of this surveillance architecture is the SCS, which seeks to evaluate citizens' trustworthiness on the basis of their behaviours and activities, including online interactions and consumption practices (Kostka, 2019). This initiative has attracted substantial academic and public attention for two main reasons. First, it represents a top-down

attempt to integrate traditional commercial credit rating mechanisms into the regulation of social behaviour (Meissner, 2017). Second, it entails the construction of centralised data infrastructures for large-scale data collection, mining, and analysis (Diab, 2017). Through automated and real-time monitoring practices, the government is progressively integrating previously fragmented surveillance platforms into what has been described as an "internet of surveillance," thereby constructing "an all-encompassing system penetrating, controlling and shaping society" (Liang et al., 2018, p.6).

Introduced in 2014, the State Council issued a policy circular outlining plans for the full establishment of the system by 2020. The SCS was officially intended to restore public trust in government institutions, the judiciary, economic actors, and fellow citizens. Concurrently, the system reflects the pervasive levels of mutual distrust that characterise contemporary Chinese society (Cabestan, 2020). The SCS extends beyond individual citizens to include both domestic and foreign enterprises, aiming to reduce transaction costs and mitigate economic risks by compelling the state to collect extensive legal, financial, and commercial data on firms (Meissner, 2017). It integrates mechanisms of accountability with broader methods of social control. Participation in the system is incentivised through access to a range of services and benefits, thereby encouraging societal engagement. Conversely, such participation also exposes individuals and organisations to potential sanctions, effectively holding them responsible for their behaviour within the framework of state-defined norms (Hoffman, 2017).

More broadly, the SCS has resulted in a substantial expansion of the party-state's authority to supervise business activities, intervene in market mechanisms, and exert control over the private sector, including foreign companies. This underscores the CCP's determination to maintain dominance over both the political system and the economy, while preventing the emergence of autonomous economic forces beyond its direct control. At the societal level, the SCS establishes an unparalleled degree of surveillance and micro-management of citizens, giving rise to significant concerns regarding individual freedoms, privacy protections, and the right to be forgotten. In this respect, the system promotes a form of "rule of trust" that is arbitrarily defined and enforced by the CCP, often at the expense of the rule of law (Chen et al., 2018, p.2).

The project can thus be understood as a comprehensive governance mechanism that monitors and directs the behaviour of citizens through the allocation of credit scores derived from the extensive collection of data by government agencies, private corporations, and digital platforms such as Alibaba and Tencent. The system is presented as a mechanism to promote reliable conduct and social stability,

focusing on incentivising compliance and disciplining misconduct through data-driven evaluations that may incorporate technologies such as facial recognition and social media surveillance. While proponents argue that the SCS fosters responsible behaviour, critics highlight the risks of pervasive privacy violations, societal homogenisation, and the erosion of democratic freedoms, as the system consolidates state and corporate power to monitor, influence, and discipline citizens, thereby raising significant ethical and human rights concerns (Vagianos & Stavrou, 2023).

Scholars have placed considerable emphasis on the far-reaching implications of the extensive data collection and data-sharing ambitions underlying the SCS. These concerns stem from the scale at which the Chinese government is reportedly gathering digital records of the social and financial behaviours of private citizens and organisations, with the technical and infrastructural support of major information technology firms such as Alibaba and Baidu (Chen & Cheung, 2017). At its conceptual core, the SCS promotes self-regulation among enterprises, encouraging businesses to comply voluntarily with laws and regulations, thereby reducing the burden on existing enforcement and compliance mechanisms. It is designed to complement other regulatory institutions by shaping the behaviour of individuals and firms, ensuring adherence to state policies, and incentivising corporate social and environmental responsibility. Rather than relying primarily on coercive force, the system governs behaviour through incentives and reputational mechanisms that encourage voluntary compliance and participation in state programmes. It has potential to penetrate deeply into the lives of citizens and organisations, generating extensive policy insights related to social and economic behaviour, as well as the well-being of citizens and employees (Aho & Duffield, 2020).

The implementation of the Great Firewall of China and the SCS serves as a prime example of *Digitalpolitik*, characterised by the integration of state authority into both digital infrastructure and societal behaviour. The Great Firewall has been identified as a mechanism for the creation of an insulated internet ecosystem, enabling the CCP to restrict access to foreign information, shape public discourse, and integrate private platforms into state-led surveillance (Griffiths, 2019). The SCS extends these capabilities by collecting, mining, and analysing vast quantities of personal, commercial, and social data to evaluate trustworthiness, enforce compliance with state-defined norms, and incentivise socially sanctioned behaviour through rewards and penalties (Kostka, 2019). This underscores the CCP's objective of consolidating influence across the political, economic, and technological domains. In accordance with the conceptual framework of *Digitalpolitik*, these mechanisms exemplify China's endeavours to assert its influence in the digital realm, encompassing the establishment of bespoke

infrastructures, governance frameworks, and incentive mechanisms that contribute to the fragmentation of the internet on a global scale. Table 7 below summarises China's model related to the concept of *Digitalpolitik*.

Table 7. Infrastructure, Behaviour, and Digitalpolitik in China

Instrument	Function	Control	Digitalpolitik
Great Firewall	Regulates access to information	Censorship, filtering, monitoring	Embeds national authority into the internet.
Media and Platforms	Shapes public discourse	Content regulation, corporate compliance	Integrates private actors into state information control.
Social Credit System	Evaluates trustworthiness	Data aggregation, rewards and sanctions	Expands digital governance to behavioural regulation.
Data Ecosystem	Enables large-scale surveillance	State-corporate data sharing	Consolidates political and economic power through data-driven governance

Source: The candidate based on the sources above mentioned.

An analysis of China's domestic legal and surveillance architecture demonstrates how cyberspace governance is inherently connected to the overarching objectives of political authority and strategic control under the leadership of Xi Jinping. These internal governance practices have the capacity to influence not only domestic regulation but also China's external engagement with global internet governance and cyber sovereignty. The subsequent subsection therefore explores China's international approach, analysing how these principles are projected onto the global stage through normative, diplomatic, and technological initiatives.

2.2. International cybersecurity strategy

The promotion of cyber sovereignty and multilateral cooperation by China reflects a broader effort to shape international digital governance in accordance with state-centric principles under the leadership of Xi Jinping. These normative and diplomatic initiatives are increasingly complemented by material strategies centred on technological leadership and institutional influence (Sheehan, 2023). The following subsection thus examines China's advancement of its international objectives through the concept of cyber sovereignty and international partnerships, along with the utilisation of AI governance, technical standardisation, and the DSR.

2.2.1 Cyber sovereignty and international cooperation

As the world's second-largest economy, China is a central actor in the global digital economy. It is developing a distinctive data governance framework that may diverge significantly from models emerging in other jurisdictions. As a major global power, China can shape the international digital order by influencing other countries' data governance policies and exerting leverage within international forums, particularly amid growing tensions with the US (United States) China advances an alternative model of data governance grounded in national security considerations (Borgogno & Zangrandi, 2024). Within this framework, China supports the free flow of data related to merchandise trade transactions while restricting other forms of cross-border data flows. This position is consistent with China's international digital footprint, as the country hosts one of the world's largest e-commerce markets, which is increasingly expanding abroad (OECD, 2023).

While Western countries have advocated for a free and open internet, non-Western countries such as China have challenged the status quo. China was among the earliest countries to promote a closed cyber system tightly controlled by state authority. The prevailing perspective asserts that cyberspace is subject to national sovereignty, wherein the government assumes a pivotal role in rule execution and formulation (Hung, 2025). Given China's escalating global standing and expanding cyber capabilities, its pursuit of cyber sovereignty is the subject of close scrutiny. The country's substantial netizen population and its dynamic and evolving ICT sector have led to China being regarded as an ideal partner for non-Western states seeking to challenge the prevailing US hegemony in the digital space (Gao, 2022). Concerns regarding the dominance of US technology have prompted the Chinese leadership to prioritise the development of domestic core internet infrastructure. This initiative is presented as crucial for both national security and economic development. This emphasis was articulated by President Xi Jinping, who identified reliance on foreign-controlled core internet technologies as a major strategic vulnerability (Xi, 2016).

Furthermore, China has been a pioneering force in advancing the concept of cyber sovereignty, which asserts the application of national sovereignty to cyberspace. Under this framework, states are entitled to exercise independent jurisdiction over their domestic cyberspace, encompassing the formulation and enforcement of relevant laws and policies. States are also able to engage with other nations based on sovereign equality in cross-border coordination (Shen et al., 2025). At the 2015 World Internet Conference, President Xi Jinping asserted that the principle of sovereign equality in the UN Charter should also be applied to cyberspace. The governance system should be multilateral and

coordinated with all parties involved, including governments, international organisations, internet companies, technical communities, non-governmental organisations, and individual citizens (Xi, 2015).

In 2016, Chinese Ambassador Liu Xiaoqing also proposed that the concept of equal sovereignty should be applied to cyberspace. These statements reflect the Chinese government's understanding of cyber sovereignty, which emphasises the state's authority to control information within its territory, the autonomy to formulate policies regarding cyberspace, equitable participation in shaping global cyberspace rules, and the importance of respecting sovereignty in addressing international cyber-related matters (Xi, 2017b). In line with this vision, the Ministry of Foreign Affairs of China initiated the Strategy for International Cooperation in Cyberspace in March 2017. As articulated in the 2017 China White Paper on the subject, countries should refrain from using ICTs to interfere in other countries' internal affairs and should not exploit their own advantages to undermine the security of other countries' ICT supply chains (State Council, 2017).

The Chinese government has encouraged international cooperation to improve cybersecurity. Initially, this focus centred on access and technology, but as China's influence grew, it shifted towards trust-building. China has also utilised international forums to promote cybersecurity norms. At the UN, it called for increased technical and financial assistance from developed countries to enhance emergency response capabilities in developing nations. It emphasised the importance of multilateral, democratic, and transparent global cyber governance (Murniasari, 2024). China's proposal for multilateral cyber governance is grounded in the Westphalian system and is consistent with its commitment to national sovereignty. Furthermore, it seeks to import into cyberspace a conception of sovereignty whereby only sovereign states are entitled to determine the form and substance of the global cyber governance regime (State Council, 2023b).

The Chinese conception of cyber sovereignty is predicated on a state-centric model of control over cyberspace, grounded in principles of sovereign equality, non-interference, and national regulatory autonomy. The position advanced is that each state should exercise independent governance over its digital infrastructure, information flows, and online content in accordance with domestic legislation. The objective of this approach is to ensure regime stability and national security. It promotes the establishment of a multilateral global cyber order that contrasts with Western models of an open internet. Instead, it seeks to limit external influence and prevent cyber-enabled destabilisation. It can therefore be argued that China's cyber sovereignty framework reflects the nation's broader objective of

shaping a secure and orderly cyberspace aligned with its political values and leadership ambitions (Mirza et al., 2021).

China's definition of cyber sovereignty can be understood through four interrelated dimensions. First, China asserts supreme national authority in cyberspace against foreign governments and non-governmental actors. Second, cyber sovereignty is both a legal entitlement to exclusive national authority and a practical capability developed in the absence of formal international recognition. Third, the pursuit of cyber sovereignty is driven by objectives of establishing national boundaries in cyberspace and excluding unwanted external activities, seeking to replace foreign technologies and actors with domestic alternatives. Finally, these objectives are realised through legal and regulatory instruments and state-led policy support, including investment, infrastructure development, and capacity-building initiatives aimed at strengthening China's domestic digital ecosystem (Creemers, 2020). Table 8 illustrates China's cyber sovereignty principles.

Table 8. Principles of Cyber Sovereignty in China

Principle	Description
National Authority	Exclusive state control over domestic cyberspace
Legal and Practical Sovereignty	Authority exercised through laws and national capabilities
Boundary Protection	Restriction of foreign technologies and external interference
State Implementation	Enforcement via policies, infrastructure, and investment
Multilateral Equality	Sovereign equality in global cyber governance

Source: The candidate based on the sources above mentioned.

Building on its pursuit of cyber sovereignty and multilateral engagement, China has actively sought to establish partnerships to advance cybersecurity governance and protect its strategic interests. A case in point is its collaboration with ASEAN (Association of Southeast Asian Nations), which aims to address the region's fragmented cybersecurity landscape and rapidly expanding digital economy. This collaboration emphasises the development of unified cybersecurity rules, capacity-building through initiatives such as the ASEAN-China Cyber Dialogue, and technology transfer via mechanisms such as the China-ASEAN Technology Transfer Centre (Ramadhan, 2023). China and ASEAN share broad

common interests, particularly in light of their mutual vulnerability to cyber threats and the need to foster the secure growth of the digital economy. This is reinforced through strategic initiatives such as the China-ASEAN Partnership on Digital Economy and its Action Plan for 2021-2025, as well as through existing mechanisms such as the China-ASEAN Dialogue Mechanism on Cyber Affairs. Recent cooperation has expanded in areas including combating cybercrime, protecting data security, developing digital infrastructure, and governing cyberspace security (Hui & Xiaoxue, 2025). For China, such cooperation is critical not only to safeguard its substantial investments in Southeast Asia, but also to reinforce regional stability while adhering to its principle of respecting national sovereignty (Ramadhan, 2023).

The Chinese government has been proactive in its participation in trilateral cooperation with Japan and South Korea, combining efforts in the areas of cybersecurity, digital trade, and technological development. The three countries initiated the Trilateral Cyber Policy Consultation in 2014, with subsequent meetings held in Seoul (2015) and Tokyo (2017). These meetings provide a forum for exchanging views on national cyber strategies and policies. These discussions were complemented by the China-Japan-Korea Computer Security Incident Response Team (CSIRT) Annual Meetings, which facilitate practical cooperation on cybersecurity incident response (Murniasari, 2024). The basis for this trilateral cybersecurity cooperation is closely linked to their robust digital trade relations, which rely on shared technologies such as IoT and big data. The stability of digital trade among China, South Korea, and Japan is regarded as a mutually reinforcing factor in the development of regional cybersecurity. Digital Trade Agreements (DTAs) have been identified as mechanisms that foster synergy between trade and cybersecurity policies. Furthermore, the joint exploration of Central Bank Digital Currencies (CBDCs) based on blockchain highlights the need for collaboration in financial cybersecurity, distributed ledger technology, and personal data protection. Such accords facilitate the establishment of consensus-based standards and provide measurable frameworks for cybersecurity risk management, thereby reinforcing the integration of economic and security objectives in the region (Pei & Kim, 2023).

China's expansive approach to cyber sovereignty and international digital governance can be regarded as a practical embodiment of *Digitalpolitik*. By controlling cyberspace and embedding national security considerations into digital policies, China is shaping the global digital order. The strategies employed by the state, including the development of a distinctive domestic data governance system, the promotion of sovereign control over information flows, and the advocacy of state-centric multilateral frameworks in forums such as ASEAN and in trilateral cooperation with Japan and South Korea (Pei &

Kim, 2023), illustrate how digital infrastructure, regulatory instruments, and international cooperation are leveraged as instruments of power. The pursuit of cyber sovereignty, with restrictions on foreign technologies and an emphasis on domestic alternatives, exemplifies the realist, security-centred logic of *Digitalpolitik* by shaping norms, establishing technical and legal control over digital ecosystems, and reinforcing state dominance in strategic domains. China's involvement in international initiatives, including data and cyberspace discussions, demonstrates *Digitalpolitik*'s dual role in enabling national control and influencing global digital governance standards, thereby contributing to the fragmentation of international digital rules. Its cyber policies and partnerships reveal a strategy of using digital networks to strengthen national power, regulate information, and achieve geopolitical goals aligned with the principles of *Digitalpolitik*. Table 9 summarises the connection between China's international strategy and its connection to *Digitalpolitik*.

Table 9. China's International Digital Cooperation and Digitalpolitik

Partnership/Initiative	Key Activities	Digitalpolitik
China-ASEAN	Cybersecurity dialogue, unified rules, capacity-building, technology transfer	Uses multilateral frameworks to embed state control, promote norms, and protect strategic interests
China-Japan-South Korea	Trilateral consultations, CSIRT meetings, digital trade agreements	Shape regional digital governance under state leadership.
Global Cyber Policies	Domestic data governance, cyber-sovereignty advocacy, forum participation	Projects boost national power internationally by setting new standards.

Source: The candidate based on the sources above mentioned.

China's emphasis on cyber sovereignty and multilateral engagement highlights an attempt to legitimise state authority in cyberspace through diplomatic and institutional channels (Murniasari, 2024). These normative initiatives are increasingly accompanied by strategies aimed at embedding Chinese influence within technological systems and governance structures (Chang & Zeng, 2023). The following subsection therefore examines the significance of artificial intelligence, technical standardisation, and the Digital Silk Road as pivotal instruments in advancing this agenda.

2.2.2 AI, Technical Standardisation and the Digital Silk Road

The rapid rise of AI reflects the accelerating development of technologies for data processing, information manipulation, and online operations, thereby increasing the strategic significance of cyberspace. China has expressed a strong interest in assuming a leadership role in the governance of AI to regulate its development and deployment (Bartley, 2025).

China has introduced some of the world's earliest and most detailed national regulations governing AI and algorithmic systems, including those related to recommendation algorithms, deep synthesis, and generative AI. These regulatory frameworks influence the global digital landscape by shaping the default standards embedded in Chinese technology exports and by stimulating international AI research. While information control remains a central objective, the regulations also address broader social and economic concerns. This measured, application-specific approach is laying the foundation for a comprehensive national AI law, a development that is critical for global AI governance (Sheehan, 2023). Similarly, Cheng and Zeng (2023) argue that China can extrapolate its domestic regulatory system to shape international AI standards. China's domestic AI policy exerts a significant influence on its international approach, as it is used to justify the country's ambition to lead global AI governance. The development of comprehensive legal frameworks and ethical norms has created a regulatory environment that prioritises control, data security, privacy protection, and ethical standards. These policies reflect China's emphasis on state-centric sovereignty and the integration of AI into governance and social regulation, which in turn informs its efforts to shape international standards and norms in accordance with its values and governance model.

From a global perspective, China's promotion of open-source AI represents a deliberate strategy of asymmetric competition aimed at countering US dominance in the field. In the absence of proprietary models, extensive user bases, and unrestricted access to advanced semiconductors, China has increasingly relied on open-source AI to reduce development costs, accelerate technological iteration, and rapidly cultivate a domestic developer community. This approach enables China to circumvent direct competition in high-cost infrastructure while undermining US advantages through widespread, low-cost diffusion and relatively limited investment (Yang, 2025). State-led initiatives, such as the China-BRICS AI Development and Cooperation Centre, operationalise this strategy by fostering international coalitions and promoting Chinese technologies as credible non-Western standards for digital development (Ministry of Foreign Affairs, 2024). The adoption of Chinese open-source AI models has been shown to align closely with China's regulatory and governance standards (Chan et al., 2025). This alignment contributes to the creation of technological path dependencies and facilitates the

diffusion of China's digital governance framework internationally (Yu, 2025). Although these models do not explicitly export authoritarian practices, they provide a technological template that prioritises data localisation and content filtering, thereby extending China's digital governance norms beyond its borders (Meaghan, 2025). China's open-source AI strategy thus promotes global openness and technological accessibility while simultaneously reinforcing domestic political control. This dual function represents a significant development in digital authoritarianism, reflecting a transition from a predominantly internal, defensive model of control towards a proactive effort to shape international AI standards and governance practices (Yang, 2025).

China's approach to the technical standardisation of the internet further illustrates its broader strategy to transform global digital governance. The Shanghai Cooperation Organisation (SCO), led primarily by China and Russia, has played a significant role in promoting alternative governance models that prioritise state sovereignty, regime stability, and governmental control over cyberspace (Fung, 2022). Through technical standards, regulatory processes, and infrastructure diplomacy, China seeks to embed its governance preferences within the foundational architecture of the internet. Chinese firms, most notably Huawei, have actively promoted alternative technical protocols and advocated for shifting authority over standards-setting from multistakeholder institutions to more state-centric bodies. This strategy enables greater state influence over technical governance, reinforcing national sovereignty in cyberspace and constraining the role of non-state actors. Collectively, these initiatives demonstrate China's efforts to legitimise state-centric Internet governance and to challenge the universality of existing liberal and multistakeholder standards (Raymond & Sherman, 2024).

China's approach to AI and the technical standardisation of the internet constitutes a significant case study in *Digitalpolitik*, as it employs technological development, regulatory frameworks, and technical standards as instruments of state power to advance strategic, political, and security objectives. Through the promotion of open-source AI, China is able to disseminate its governance model internationally, embedding principles such as data localisation, content regulation, and state oversight within global digital ecosystems (Meaghan, 2025). Table 10 below summarises China's overarching approach to AI, cyberspace and global standards.

Table 10. Overview of China's Approach to AI, Cyberspace, and Global Standards

Category	Key points
AI and Cyberspace	AI growth → strategic importance of cyberspace
Domestic Policy	Control, data security, ethics, groundwork for national AI law
Global Influence	Shape international AI standards, justify leadership in governance
Open-Source AI	Reduce costs, grow developer base, counter US dominance
Digital Governance	Export Chinese norms, data localization and content control
Internet Standards	Promote state-centric governance, challenge multistakeholder models
Strategic Goal	Promote Chinese norms globally

Source: The candidate based on the sources above mentioned.

China's first national plan for a standardisation system was introduced in 2015, coinciding with the full-scale implementation of the Belt and Road Initiative (BRI) and the rapid expansion of the digital economy. Digital interconnection between China and BRI partner countries, alongside the promotion of Chinese technical standards across the BRI, was established as a national policy priority. China's influence over the digital economy and related standard-setting processes relies heavily on Huawei and other major technology firms and start-ups. This expanding Chinese presence in international technical standardisation has strengthened the authority of the party-state. By exerting influence over ICT standardisation, China seeks to control access to the technological enablers of data governance (Borgogno & Zangrandi, 2024). Building on this foundation, China has institutionalised its ambitions through the DSR. The DSR has emerged as a central component of China's BRI, often described as "a 'third' route of the BRI, alongside the 'Silk Road Economic Belt' and the 'Twenty-first Century Maritime Silk Road'" (Cheng & Zeng, 2023, p.4).

The concept of digital expansion within the BRI was first articulated in the 2015 policy document *Vision and Actions on Jointly Building the Silk Road Economic Belt and 21st-Century Maritime Silk Road*, issued by the National Development and Reform Commission, the Ministry of Foreign Affairs, and the Ministry of Commerce. The document states: "We should jointly advance the

construction of cross-border optical cables and other communications trunk line networks, improve international communications connectivity, and create an Information Silk Road" (Ministry of Foreign Affairs, 2015, p.5). Subsequently, the CAC intervened to redefine and expand the digital dimension of the initiative. In July 2015, the CAC publicly rebranded the "Information Silk Road" as the "Digital Silk Road" (Koepp, 2020). The DSR gained further strategic and political prominence in May 2017, when President Xi Jinping formally invoked the term during the first Belt and Road Forum for International Cooperation. In his keynote address, Xi (2017a) emphasised the centrality of innovation-driven development and frontier technologies to the DSR's mission, noting that the project had already begun to "bear rich fruit", particularly through enhanced policy connectivity, which he argued generated multiplier effects for international cooperation. The broader paradigm within which the DSR is situated draws heavily on what Xi Jinping (2017a) termed the "Silk Road spirit", emphasising openness and inclusiveness, mutual learning, and mutual benefit (Xi, 2017a, p.2). Connectivity is pivotal to this vision, encompassing multiple domains of transportation and communication, including land, maritime, air, and cyberspace. Infrastructure is thus presented as the foundation of cooperation, whether through economic corridors, logistics networks, or the harmonisation of policies and standards (Cheng & Zeng, 2023).

In the context of digital technology, China's ambitions extend across multiple domains, including technological development, economic expansion, and geopolitical influence. Although digital in nature, China's strategy is underpinned by extensive physical infrastructure, such as data centres, fibre-optic cables, satellites, semiconductors, and supercomputers, integrated with software systems including artificial intelligence, wireless computing, and advanced data analytics. Collectively, these components support China's aspiration for technological leadership and global digital interconnectedness. The initiative operates across three domains. It enhances global communication through fibre-optic networks, satellite systems, and 5G connectivity. It serves as a financial platform that promotes e-commerce, fintech, and digital payment ecosystems among partner states. Finally, it reinforces cybersecurity for Chinese digital infrastructure both domestically and internationally (Rahman, 2025).

As demonstrated by Gaida et al. (2023), China has made substantial technological advances and has become a global leader in several strategic sectors. Chinese companies such as Huawei and ZTE are leading competitors in 5G network technology. With strong state support, these firms function not only as commercial actors but also as strategic instruments through which China can influence the

technological trajectories of partner states participating in the DSR (Ghiasy & Rajeshwari, 2020). In the field of AI, Cheney (2019) observes that China prioritises AI and quantum computing as foundational technologies for facilitating its global ascendancy. Initiatives such as the Next Generation Artificial Intelligence Development Plan and the establishment of a national AI consortium, comprising Baidu, Tencent, Alibaba, and iFlytek, are aimed at securing leadership in AI by 2030.

From an economic perspective, China has benefited substantially from the liberal international order, which has contributed to its emergence as the world's second-largest economy (Cheney, 2019). The DSR has been identified as a key instrument for enhancing China's global standing by promoting the development of digital financial infrastructures, encouraging the adoption of digital currency exchanges, and fostering the use of non-dollar payment systems, including Central Bank Digital Currencies (CBDCs) and the Universal Digital Payment Network (UDPN) (Rahman, 2025). As Triolo (2022) observes, the UDPN seeks to streamline cross-border digital transactions while challenging the Western-dominated SWIFT (Society for Worldwide Interbank Financial Telecommunication) system, which has frequently been utilised by Western states as a tool of political and economic influence. Beyond the economic and security objectives initially pursued, the DSR has evolved into a key instrument of China's digital diplomacy and soft power. The development of cooperative digital governance frameworks, such as China's collaboration with ASEAN on cybersecurity standards, exemplifies efforts to foster digital trust and to position China as a leader in shaping the global digital order (Paudel, 2025). In this context, Southeast Asia has emerged as a pivotal region for the expansion of China's DSR, attracting substantial Chinese digital investments between 2017 and 2023. The region's rapid economic growth, young and technologically literate population, and strategic geopolitical significance make it an ideal partner for advancing China's digital ambitions (Wang, 2024).

Chinese corporations, including Huawei, Alibaba, and ZTE, have played a central role in developing 5G mobile networks, fibre-optic systems, data centres, and e-commerce platforms across Southeast Asia. These initiatives have consolidated China's presence in the region's digital markets and reinforced its broader soft-power agenda. Notable examples include ZTE's investment in a data centre in Indonesia and Huawei's contribution to Thailand's first 5G-enabled smart hospital, demonstrating China's commitment to creating a digital ecosystem shaped by its governance models and technical standards (Paudel, 2025). The DSR has institutionalised regional cooperation in Southeast Asia through frameworks such as the ASEAN-China Mechanism, the Digital Economy Partnership Agreement (DEPA), and the Cyber Dialogue, providing formal mechanisms to facilitate cross-border digital interactions

(Heydon, 2023). These cooperative initiatives are complemented by capacity-building programmes, such as Huawei's *Seeds for the Future*, which has trained thousands of government officials and university students, enhanced their technical expertise and fostering deeper engagement with Chinese technology and standards (Mutingwende, 2022). The ASEAN Digital Policy and the ASEAN Digital Masterplan 2025 establish the legal and governance frameworks that underpin the region's digital development, promoting digital transformation and enhancing readiness for digitalisation. ASEAN actively negotiates, adapts, and aligns Chinese digital initiatives with its own digital sovereignty objectives through projects such as DEFA (Digital Economy Partnership Agreement), DIFAP (Digital Integration Framework Action Plan), and other multilateral mechanisms, as exemplified by Malaysia's AI strategy and Thailand's digital integration efforts (Paudel, 2025).

Beyond infrastructure and investment, China's DSR represents a strategic effort to influence global digital governance, regulatory norms, and standards. By leveraging its digital footprint, China engages in cyber diplomacy, defined as "the use of diplomatic relations to shape international cybersecurity norms and policies" (Khan, 2025, p.529). This enables it to affect partner countries' approaches to privacy, data governance, and intellectual property. Through partnerships in technological projects, China encourages the adoption of its technical standards and aligns international perspectives with its policy positions in forums including the UN and the World Trade Organisation (WTO). By promoting a model of strong state control over data and digital services, China offers an alternative to Western, market-driven approaches, seeking to reshape digital governance to advance its political and economic interests. In regions such as Southeast Asia, Africa, and Central Asia, China enhances its soft power by providing affordable technologies and financial support, enabling these countries to bypass conventional development barriers and embed Chinese standards and governance practices within their digital ecosystems (Khan, 2025).

China's DSR exemplifies a pragmatic implementation of *Digitalpolitik*. The DSR integrates physical and digital infrastructure, including 5G networks, fibre-optic cables, satellites, data centres, and AI systems, with software platforms, fintech, and digital payment networks. This embedding of Chinese governance preferences within partner countries' technological and regulatory ecosystems is a central feature of the strategy (Rahman, 2025). China uses these measures to control technology, govern data, shape digital trade, cybersecurity and AI standards, and project soft power. This approach reflects *Digitalpolitik*'s core principles of influencing global governance, integrating security and economic objectives, and using infrastructure, technology, and standards to achieve long-term strategic goals. In

this way, China's DSR not only advances economic connectivity and technological development but also institutionalises a model of digital sovereignty. Partner states increasingly operate within a framework aligned with Chinese political and regulatory norms, illustrating the deliberate projection of state power into the international digital sphere (Cheng & Zeng, 2023). The following table showcases the connection between China's cyberspace governance and its connection to the logic of *Digitalpolitik*

Table 11. China's Cyberspace Governance and Digitalpolitik Dimensions

Policy Area	Key Instruments	Digitalpolitk
Technical Standardisation	Export of Chinese ICT standards via BRI-linked frameworks	Control global rules to gain power over digital infrastructure and data governance.
Digital Silk Road	Deployment of 5G, fibre networks, and data infrastructure abroad	Integrate Chinese tech and governance into partner states' digital systems
AI Strategy	State-led AI plan and global leadership target (2030)	Ensure technological dominance in shaping future governance
State-Corporate Coordination	Global expansion of Huawei and ZTE in 5G and ICT infrastructure	Use firms as geopolitical tools to set standards
Digital Financial Governance	Promotion of CBDCs and UDPN as alternatives to SWIFT	Avoid reliance on Western financial systems to boost autonomy
Cyber Diplomacy and Multilateral Engagement	Norm-shaping efforts in global forums	Shape global data, AI and cybersecurity standards to reflect state governance
Strategic Outcome	Integration of infrastructure, AI, standards, and diplomacy	Digital infrastructure and regulation are used to project geopolitical power

Source: The candidate based on the sources above mentioned.

In summary, China's approach to cyberspace governance reflects a tightly integrated strategy that combines legal regulation, state-led surveillance, and technological innovation to consolidate domestic control while projecting influence internationally. Domestically, the legal and institutional framework, together with AI-driven surveillance and data governance mechanisms, reinforces state authority and secures cyber sovereignty (Creemers, 2023). Internationally, China leverages cyber sovereignty, multilateral engagement, technical standardisation, and initiatives such as the DSR to shape global digital governance in ways that align with its strategic, economic, and political objectives

(Borgogno & Zangrandi, 2024). Taken together, these domestic and international strategies illustrate how China is constructing a distinctive model of cyberspace governance, combining state-centric regulation, technological leadership, and digital diplomacy to advance both national interests and global influence. The next chapter focuses on an analysis of South Korea's cybersecurity strategy, examining its domestic and international dimensions.

3. South Korea's approach to cyberspace

This chapter examines South Korea's approach to governance in cyberspace, AI, and digital infrastructure. The government has emphasised emerging technologies as central to national power, competitiveness, and security (Akhand, 2026). The first subsection analyses South Korea's national approach to cybersecurity, smart cities, and digital governance. It begins by examining the legal and institutional foundations of the cybersecurity regime, with particular attention to the roles of key state bodies and specialised institutions in managing cyber risks and protecting critical infrastructure. It then explores the development of smart cities, AI governance, and digital government initiatives, highlighting data-driven urban management, public–private partnerships, and ethical frameworks. Particular attention is given to flagship projects and surveillance technologies, illustrating the balance between participatory governance and security-oriented control. The second subsection focuses on South Korea's international digital strategy, analysing how the country projects influence through emerging technologies, global standard-setting, and international partnerships. It explores the role of firms and state-led initiatives in shaping standards in areas such as 5G, automated vehicles, and AI, as well as the "AI for All" agenda aimed at promoting technological sovereignty. The chapter further analyses South Korea's engagement with international organisations, including the UN, NATO, the ASEAN Regional Forum, and the G7, through which it promotes norms of sovereignty and cooperative cyber defence.

3.1. National Approach

South Korea's nationally coordinated approach to cybersecurity, smart cities, and the governance of AI reflects a broader effort to enhance institutional capacity and security-oriented oversight. This enhancement is pursued through regulatory frameworks, technological investment, and centralised coordination (Park & Kim, 2025). Domestically focused policies, grounded in data-driven governance, ethical AI frameworks, and integrated institutional leadership, demonstrate how digital technologies are mobilised to strengthen state resilience and administrative effectiveness (Lim et al., 2023). Under the leadership of President Lee Jae-myung, this consolidation of national digital governance highlights the

strategic importance attributed to emerging technologies in shaping internal security, public administration, and socio-economic development (Akhand, 2026). The following subsection therefore examines how these institutional, legal, and technological frameworks operate collectively within South Korea's domestic digital governance system.

3.1.1. Legal Framework and Institutions

In South Korea, cybersecurity governance is managed by several key institutions, each with defined roles and responsibilities, operating in a coordinated manner to ensure national cyber resilience. The national cybersecurity framework is centrally coordinated by the National Security Office (NSO), which functions as the highest-level control tower. The NSO is responsible for overseeing nationwide cybersecurity efforts and setting medium- to long-term policy directions (Park & Kim, 2025). Within this framework, the National Intelligence Service (NIS) serves as the lead agency for cyber crisis management, conducting cybersecurity-related intelligence, monitoring, and response activities to protect national security and public safety. In accordance with the provisions of the National Intelligence Service Act, the NIS is entrusted with collecting, analysing, reporting, and sharing cyber intelligence, including information relating to international and state-sponsored hacking groups. Furthermore, it detects and disrupts malicious cyber activities by North Korean and foreign actors (National Intelligence Service, 2026). To enhance national-level coordination, the government established the National Cyber Risk Management Unit, a public-private joint response mechanism overseen by the NSO and located within the National Cyber Security Centre (NCSC). This mechanism facilitates real-time information sharing between government agencies and industry, thereby supporting unified prevention and response to cyber crises (National Intelligence Service, 2026).

The Ministry of Science and ICT (MSIT) is the central government body responsible for national policies on science, technology, and ICT, including cybersecurity within its broader digital governance remit. The MSIT develops and implements national ICT and digital infrastructure strategies and promotes information security and resilience across the public and private sectors. It collaborates with subordinate organisations such as the Korea Internet & Security Agency (KISA) to conduct operational cybersecurity activities, including incident response and threat analysis. Its role encompasses formulating policies to safeguard information and communications networks, coordinating responses to major cyber incidents, and overseeing the implementation of information security frameworks and certification systems to foster secure digital environments (Ministry of Science and ICT, 2025a). The Ministry of Interior and Safety (MoIS) is responsible for the protection and management of national digital infrastructure, including that of local government agencies and critical infrastructure. The ministry

develops and operates cybersecurity systems such as the National Information Resources Service (NIRS) and cyber infringement response centres. Its responsibilities also include capacity building, personnel training, and the establishment of security standards for national and regional authorities. The MoIS has implemented real-time monitoring and proactive response systems to defend against cyber threats (Paz et al., 2025).

In addition to the main government bodies, South Korea's cybersecurity governance relies on specialised public institutions that collectively strengthen the country's digital resilience. KISA, a primary government-affiliated organisation under the MSIT, plays a central role in cybersecurity governance and digital safety. Its core mission is to protect the nation and its citizens from cyber threats by continuously operating cyber threat monitoring and response systems, analysing and mitigating hacking incidents, and managing national vulnerability reporting and preventive mechanisms. KISA also oversees the Korea Computer Emergency Response Team/Coordination Center (KrCERT/CC), which provides incident monitoring, analysis, and support to both the public and private sectors. KISA's contributions further include promoting personal information protection, developing secure ICT infrastructure strategies, supporting the information security industry, and facilitating cooperation with global cybersecurity entities (Korea Internet & Security Agency, 2026). Beyond KISA, the National Security Research Institute (NSRI) conducts research and development in cybersecurity technologies, cryptography, and threat mitigation, and operates training centres to enhance national cybersecurity capabilities. Other specialised institutions, including the Government Information Disclosure Centre (GIDC) and the Financial Supervisory Institute (FSI), oversee the development of cybersecurity infrastructure and financial cybersecurity, respectively. Together, these institutions form an integrated framework combining operational response, technological innovation, regulatory oversight, and sector-specific expertise (Paz et al., 2025).

South Korea's legal framework for cybersecurity and data protection comprises a combination of general and sector-specific legislation rather than a single comprehensive act. The Personal Information Protection Act (PIPA) governs the processing and protection of personal information. Other key laws include the Network Act, which imposes cybersecurity and information protection obligations on network service providers; the Electronic Financial Transactions Act, which regulates the security of electronic financial systems; and the Act on the Protection of ICT, which focuses on safeguarding critical information infrastructure. These laws specify technical, organisational, and incident notification requirements, including network stability measures and breach reporting obligations. The framework

intersects with constitutional data privacy rights and extends to non-personal data under the Public Data Act and the Data Industry Act. Major amendments to PIPA and related cybersecurity legislation were introduced between 2023 and 2024, with no further substantial changes anticipated in the near term (Baker McKenzie, 2026).

In October 2025, South Korea announced a new cybersecurity strategy in response to major data breaches and growing public concern. Key government bodies developed the strategy to strengthen national cyber resilience, emphasising cybersecurity as a strategic investment through enhanced corporate accountability measures. Listed companies are required to disclose their cybersecurity posture publicly, with Chief Executive Officer (CEO) responsibility formally established. The authority of Chief Information Security Officers (CISOs) and Chief Privacy Officers (CPOs) will be expanded, and public institutions must allocate dedicated budgets and personnel for information security. The strategy also seeks to develop the cybersecurity industry as a national priority by supporting next-generation security firms and strengthening workforce development, including elite cybersecurity training. It establishes a centralised incident response framework to improve interagency coordination and highlights international cooperation as a means of enhancing South Korea's global competitiveness (Kim, 2025).

A Presidential Decree establishing the National AI Strategy Committee was approved by the MSIT in September, alongside broader technology and security reforms. This fulfilled President Lee Jae-myung's campaign commitment to establish a centralised national AI governance body. The Committee is responsible for overseeing national AI policies. At the same time, the MSIT, in collaboration with other ministries and the NSO, announced measures to address widespread hacking incidents and public concern, framing cybersecurity as a strategic investment. These measures include large-scale inspections of critical IT (Information Technology) infrastructure, enhanced consumer protection mechanisms, and consideration of a dedicated fund to support data breach victims. Institutional leadership is strengthened through the introduction of minimum security budgets and staffing ratios in the public sector, while mandatory disclosure of information security practices is extended to all listed companies and assessed through a public grading system. The government also seeks to promote next-generation security firms, expand the pool of cyber talent, and develop specialised training programmes and courses (Ministry of Science and ICT, 2025a).

South Korea's national cybersecurity governance exemplifies *Digitalpolitik*, illustrating how state institutions regulate digital infrastructure and control information flows. The NSO, the NIS, the MSIT,

and the MoIS coordinate surveillance, intelligence, and technological capabilities to safeguard national security and maintain digital sovereignty (Park & Kim, 2025). Specialised agencies such as KISA and the NSRI monitor, respond to, and mitigate cyber threats while contributing to the formulation of national ICT policies (Korea Internet & Security Agency, 2026). By structuring governance around intelligence, operational preparedness, and technological development, South Korea has adopted a realist, security-centred approach to the digital domain. This strategy integrates regulation, technological capability, and institutional authority to project state power and secure digital sovereignty. Sector-specific legislation reinforces data protection, infrastructure security, and corporate accountability (Baker McKenzie, 2026). The 2025 national cybersecurity strategy operationalises the logic of *Digitalpolitik* by integrating policy coordination, institutional alignment, and technological oversight to enhance resilience, mandate corporate responsibility, and develop cybersecurity as a strategic national asset. Centralised governance bodies and expanded interagency coordination further reflect *Digitalpolitik*'s emphasis on state-led control, strategic technological investment, and the pursuit of national advantage in global digital markets. Table 12 illustrates South Korea's cybersecurity governance and its connection to the concept of *Digitalpolitik*.

Table 12. South Korea's Cybersecurity Institutions & Digitalpolitik

Institution/Framework	Functions and Role	Digitalpolitik
National Security Office (NSO)	Central coordinator, sets national strategy, oversees agencies	Centralised control of cyberspace
National Intelligence Service (NIS)	Cyber intelligence, monitors threats, manages crises	Intelligence-driven digital sovereignty
National Cyber Security Centre (NCSC) / National Cyber Risk Management Unit	Coordinates public–private info-sharing, joint crisis response	State–industry integration for resilience
Ministry of Science and ICT (MSIT)	ICT and cybersecurity policy, sets standards, coordinates incidents	Regulation + tech capacity as power tools
Ministry of the Interior and Safety (MoIS)	Protection of public digital infrastructure, monitors critical system, trains personnel	Infrastructure security = digital sovereignty
Korea Internet & Security Agency (KISA)	Threat monitoring, incident response, vulnerability management	Operational enforcement of cyber resilience
National Security Research Institute (NSRI)	Cyber R&D, cryptography, threat mitigation, training	Innovation for strategic advantage
Legal Framework	PIPA, Network Act, Financial Transactions Act, sector-specific laws	Legal enforcement of control and accountability
2025 Cybersecurity Strategy	Corporate disclosure, centralised response, workforce and industry development	Align institutions, tech, and policy for national security
National AI Strategy Committee (2025)	Oversees AI policy, integrates tech and security reforms	State-led coordination of emerging technologies

Source: The candidate based on the sources above mentioned.

South Korea's national cybersecurity framework, coordinated by the NSO, NIS, MSIT, MoIS, KISA, and NSRI, establishes a foundation for state control over digital infrastructure and information flows (Park & Kim, 2025). The subsequent subsection of the chapter examines the practical application of this institutional and legal foundation through South Korea's smart cities, AI initiatives, and digital

governance programmes, highlighting the integration of technology, data, and public–private coordination in advancing citizen-centred and sustainable urban development.

3.1.2 Smart Cities, AI and Digital Governance

Smart cities have emerged as influential actors in international relations, functioning as both consumers and producers of global technology through the integration of IoT, AI, and data infrastructure. They are recognised not only for technological innovation but also for shaping global political and economic dynamics (Yoo, 2025).

South Korea has become a leader in smart city development due to early investments in ICT and a highly urbanised context. Its coordinated, state-led approach integrates central government, local authorities, the private sector, and academic institutions. This has enabled pilot smart city projects that function as experimental urban systems. South Korea's national smart city policy now prioritises data-driven urban governance, reflecting its strategy of using digital innovation for socio-economic development and environmental sustainability (Korea Information Society Development Institute, 2021).

Early efforts focused on ICT-based U-City projects, including networked buildings, traffic systems, and e-governance. Following criticisms regarding human-centred design, the 2024 Smart City Act[2] introduced a more inclusive, quality-of-life approach, formalising the government's commitment to innovation, sustainability, and participatory governance (Ministry of Legislation, 2026). South Korea's smart city strategy integrates technological, institutional, and citizen-oriented innovation domains that guide national and local initiatives. It is coordinated centrally by the Ministry of Land, Infrastructure and Transport (MOLIT), in collaboration with the Presidential Committee. This facilitates resource pooling, legal standardisation, and knowledge sharing between regions, while public–private partnerships engage major technology firms in project design and implementation (Ministry of Land, Infrastructure and Transport, 2021).

Contemporary smart city projects adopt a comprehensive approach to urban management, enabling data-driven decision-making and integrated public services. Smart cities aim to enhance urban sustainability and deliver citizen-centric services by leveraging advanced technological infrastructure (Lim et al., 2023). South Korea's smart city development builds on a history of using digital technology

[2] The 2024 Smart City Act aims to improve quality of life, competitiveness, sustainability, and national competitiveness by stipulating matters related to the efficient creation, management and operation of smart cities and industrial promotion (Ministry of Legislation, 2026).

for public benefit. The earlier Smart City Act[3][4] (2017) defines smart cities as urban systems that enhance quality of life and promote sustainable development through information and communication technologies, reflecting a policy orientation towards inclusive growth (Ministry of Legislation, 2026). Data is treated as public infrastructure within this framework, marking a shift from the previously hardware-focused U-City model. Through the promotion of open data standards, citizen participation mechanisms, and public–private partnerships, the government seeks to improve urban resilience and responsiveness (You, 2025). Smart cities in South Korea harness Fourth Industrial Revolution technologies to enhance quality of life, sustainability, and foster new industries. Government support through investment and deregulation has enabled 78 local governments to participate in smart city projects. The national smart city policy aims to resolve urban challenges through advanced technology, develop inclusive cities, and encourage global collaboration (Smart City Korea, 2024).

Smart governance introduces new methods of collaborative decision-making through ICT. It aims to create open, transparent, and participatory governance processes involving public agencies, private companies, academic institutions, and citizens. Digital technologies enhance communication, collaboration, and consensus-building among stakeholders, improving the effectiveness of urban planning and policymaking. Core smart governance principles foster inclusive, democratic participation, balancing public and private interests through technology-supported networks (Lim et al., 2023). The National Strategic Smart City Program (NSSP), South Korea's largest recent initiative (2018-2022), advanced sustainable and intelligent urban development. Coordinated by MOLIT and MSIT, it established a cloud-based data hub and piloted cutting-edge urban technologies, supported by investments from government bodies, local authorities, and the private sector. Objectives included developing smart cities, addressing urban challenges, improving quality of life, and promoting economic growth (Ministry of Land, Infrastructure and Transport, 2021). Evaluation of the NSSP indicated that it successfully drove sustainable urban development, with the cloud-based open data hub supporting services such as smart mobility, integrated energy management, and healthcare. Challenges included limited evaluation tools, the absence of quantitative targets, and insufficient attention to service quality and system maturity (Lee et al., 2025).

The smart cities component of South Korea's strategy aligns primarily with *Netpolitik*, as these urban systems are conceptualised as networked, participatory, and cooperative governance platforms

[3] The Smart City Act was established in 2017 with the objective of systematically promoting the creation and support of smart cities, as well as leading the development of related industries (Ministry of Land, Infrastructure and Transport, 2021).

rather than instruments of coercive state power. Emphasis on citizen-centric services, open data, public–private partnerships, multi-stakeholder collaboration, and soft power through innovation and sustainability reflects Bollier's (2003) conception of *Netpolitik*, which prioritises legitimacy, inclusiveness, and narrative-based influence. Although elements of *Digitalpolitik* remain in state-led coordination, strategic infrastructure investment, and policy integration, the focus on socio-economic development, sustainability, and global collaboration positions *Netpolitik* at the forefront. Table 13 below showcases the governance of South Korean smart cities and the correlation to the logic of *Netpolitik*.

Table 13. South Korea's Smart Cities and Netpolitik Alignment

Dimension	Key Features	Netpolitik
National Coordination	Central government coordinates with local authorities, private sector, and academia, resource pooling and legal standardisation	Networked, cooperative governance
Technological Integration	IoT, AI, cloud-based data hubs, U-City infrastructure, smart mobility, energy, healthcare	Enables participatory, citizen-focused systems
Policy and Legal Framework	Smart City Acts (2017, 2024), inclusive growth, sustainability, participatory governance	Transparency, legitimacy, multi-stakeholder collaboration
Citizen-Centric Services	Open data, public participation, quality-of-life improvements	Legitimacy and narrative influence
Public-Private Partnerships	Engagement of major technology firms in project design and implementation	Soft power through collaboration
Strategic Projects	NSSP 2018–2022, pilot smart cities	Experimental, networked urban systems
Outcomes	Urban resilience, sustainability, growth	Cooperative influence, participatory focus

Source: The candidate based on the sources above mentioned.

Regarding the implementation of AI technologies, South Korea's two national pilot projects, Sejong Smart City and Busan Eco-Delta Smart City, serve as prime examples. These function as urban modernisation initiatives and strategic digital infrastructures, strengthening digital sovereignty and economic competitiveness in an increasingly fragmented global digital order (Yoo, 2025). Sejong is a zero-energy city integrating autonomous mobility, AI-driven public services, and a citizen data hub. It is a

government-led platform employing advanced mobility systems and AI in public administration. Its strengths include integrated autonomous transport solutions supported by 5G infrastructure, semiconductors and control systems, and a digital twin platform. However, Sejong faces limitations regarding implementation, scalability, engagement, and innovation. Busan emphasises resilience and fintech innovation. Its integration of fintech applications represents a leading example of climate-adaptive urban development, with a focus on sustainability, water management, and maritime logistics. Its features include AI-enabled monitoring, a digital port management system, and the Busan data sandbox. The project faces challenges including institutional fragmentation, data harmonisation, insufficient commercialisation, and limited private-sector participation. The absence of a clear strategy for replication or export reduces its potential (Ministry of Land, Infrastructure and Transport, 2023). The following table 14 illustrates South Korea's two pilot projects in the development of smart city governance.

Table 14. Overview of South Korea's Sejong and Busan Smart City Pilot Projects

Aspect	Sejong Smart City	Busan Eco-Delta Smart City
Focus / Objective	Zero-energy city, government-led urban modernisation	Climate-resilient urban development, fintech innovation
Core Features	Autonomous mobility, AI-driven public services, citizen data hub	AI-enabled monitoring, digital port management, Busan data sandbox
Technology / Infrastructure	Integrated autonomous transport solutions, 5G networks, semiconductors and control systems, digital twin platform	Fintech applications, water management systems, maritime logistics, AI for climate adaptation
Implementation Approach	Government-led platform, centralised management	Public-private collaboration with emphasis on sustainability
Strategic Goals	Strengthen digital sovereignty, enhance economic competitiveness, modernise urban services	Promote resilience, drive fintech innovation, enable sustainable maritime and water management

Source: The candidate based on the sources above mentioned.

Smart technology also underpins South Korea's urban safety policies, visualising and managing risks in crime prevention, disaster response, health, and environmental governance. The MoIS and

MSIT have integrated digital technologies into law enforcement to enhance public perceptions of safety. Examples include drones, robots, location-tracking tags, and autonomous patrol vehicles (Yang, 2025). Seoul's 'Smart Public Safety' project aims to minimise safety blind spots and reduce public anxiety by expanding key infrastructure. This includes an AI-powered citywide surveillance and security network, replacing outdated cameras and upgrading 70,000 existing units with AI and infrared functionality. The integrated safety platform supports the network and enables emergency centres to receive real-time footage and respond rapidly. Smart security lights equipped with IoT signal devices are being installed in vulnerable areas and linked to the Ansimi app, which uses AI to detect falls and assaults, automatically sharing emergency footage and activating brighter lighting when safety features are triggered (Seoul Metropolitan Government, 2025). Similarly, the Goalie Patrol robot, a government-run location-based tracking service, illustrates AI-driven urban safety. The Goalie Patrol robot operates in areas with a high concentration of single-woman households and relies on multiple cameras and 5G connectivity to transmit real-time footage to a control centre, improving urban visibility and addressing blind spots. The initiative, framed by the slogan "Our vision is your freedom," aims to enhance safety and public liberty, although concerns have been raised regarding reliance on surveillance and the extent of its benefits (Yang, 2025, p.10).

Many Koreans view surveillance technologies, particularly CCTV, as symbols of safety. A survey by the Korean Institute of Criminology and Justice (KICJ) found that 88.9 per cent of Korean adults believed CCTV to be effective in preventing crime, and 65 per cent wanted more in public spaces, residential areas, schools, and childcare facilities (Korean Institute of Criminology and Justice, 2019). Although there is no direct causal link between CCTV and crime reduction, public opinion is generally favourable. The proliferation of smartphones, cameras, and micro-sensors has led to an exponential increase in street CCTV. These examples demonstrate the pivotal role of AI in smart cities, integrating and analysing data across domains such as transportation, energy, healthcare, and governance. IoT provides the real-time data foundation for these capabilities, distinguishing AI-driven smart cities from earlier ICT models by enabling continuous feedback loops between sensing, analysis, and action. AI enhances sustainability by optimising resource use, reducing pollution, and promoting renewable energy (Yang, 2025).

South Korea has invested heavily in IoT and smart governance, amplifying the impact of AI in urban environments. Sensor networks, connected devices, and data infrastructure form the backbone of the IoT. These sensors collect real-time data on urban factors such as environment, transport, public

safety, and health, which are then analysed by AI systems to inform decision-making. South Korea's smart governance employs a structured framework for using AI insights, with data-sharing platforms and transparent decision-making. This approach enables AI to analyse IoT data and translate it into actionable interventions. The government uses AI-powered systems for urban safety, traffic, and public health, leveraging IoT data to make informed decisions. Smart governance mechanisms, including data security and public participation, ensure trustworthy AI-driven decisions that respect privacy and secure social acceptance (Bokhari & Myeong, 2023).

AI applications in smart cities improve urban living, governance, and sustainability. Key applications include urban safety and security, where AI-powered cameras, facial recognition, and analytics monitor public spaces, detect anomalies, and respond to threats. These technologies enhance security and crime prevention, making cities safer. AI is also applied to transportation and traffic management, where algorithms analyse IoT sensor data to optimise traffic flow, reduce congestion, and coordinate public transport, improving mobility and reducing pollution. Furthermore, AI facilitates environmental monitoring and management by analysing data on air quality, weather, and energy consumption, enabling officials to enhance environmental health and promote sustainability. AI-driven models predict pollution and advise on mitigation, fostering healthier urban ecosystems (Bokhari & Myeong, 2022).

South Korea's digital government innovation agenda seeks to employ digital technologies ethically and securely to enhance public services. The MoIS is leading efforts to build a resilient and responsive digital government. The strategy focuses on identifying citizen needs and delivering seamless, non-contact services through the reengineering of administrative processes and innovative service delivery models. It emphasises the use of data to enable a data-driven administration while strengthening citizens' data sovereignty, alongside fostering a digital ecosystem through public–private cooperation and investment in digital infrastructure. These priorities are reflected in initiatives such as AI-based chatbots for citizen interaction, mobile digital identification, digital document wallets, and the My Data initiative, which empowers citizens to manage and selectively share their personal information held by government agencies (Ministry of the Interior and Safety, 2025).

The public sector in South Korea is utilising AI to improve policy development, public service delivery, and internal administration. In late 2025, the Organisation for Economic Co-operation and Development (OECD) conducted a survey of 13 public institutions, finding that most are using AI to support internal operations, policymaking, and service provision. AI is being applied to improve

productivity, efficiency, and accountability. It also enables more proactive and inclusive public services and policies. South Korea has introduced generative AI applications to enhance access to legal and administrative information, particularly in complex regulatory domains. While the use of AI for auditing, fraud detection, and impact evaluation remains limited, emerging applications in public procurement demonstrate notable efficiency gains and strengthened compliance monitoring. Overall, these developments highlight AI's growing role in reinforcing administrative capacity and accountability in South Korea's public sector (Organisation for Economic Co-operation and Development, 2025).

South Korea has developed tools to regulate and support the trusted use of AI in public services, covering governance, infrastructure, data, skills, and procurement. The National AI Strategy guides AI governance, with the public sector acting as both regulator and user. Investments in data centres and computing are accelerating AI development, yet ensuring equitable access and alignment with public needs remains challenging. South Korea's principles-based data governance framework seeks to balance innovation with privacy, while additional capacity-building and clearer procurement guidance are required for high-risk applications (Ministry of Science and ICT, 2025a).

Building on this foundation, South Korea has established policy and legal frameworks, as well as institutional bodies, to oversee AI-related risks in government. The early adoption of ethics frameworks has embedded principles of human dignity, public interest, and ethical purposefulness into public-sector AI governance. The country has invested in tools such as impact assessment frameworks and technology evaluations, and further measures are planned to improve the traceability of AI-generated content (Organisation for Economic Co-operation and Development, 2025). At a broader governance level, South Korea is implementing a structured, multi-level approach to AI governance that prioritises digital ethics and security. In 2023, the government introduced the AI Ethics Charter and the AI Governance Framework, designed to reinforce the integration of moral and social considerations into the development and deployment of AI. This approach reflects the understanding that a solitary agency cannot effectively manage the rapid evolution of AI. Instead, emphasis is placed on a collective governance system involving government, industry, and civil society to ensure compliance, transparency, and an appropriate balance between central and regional authorities in digital oversight (Busroh et al., 2025).

South Korea's digital governance model represents a distinctive hybrid system, balancing government guidance with private-sector innovation and reflecting its unique history and culture. The model prioritises strategic government involvement in building critical infrastructure, fostering

technological sovereignty, and guiding digital platforms, which has helped South Korea achieve high levels of connectivity and technological advancement (Chung et al., 2022). The focus on domestic platforms and digital sovereignty consolidates control and reduces dependence on foreign technology but also creates potential vulnerabilities. South Korea's digital governance is characterised by regulatory flexibility and active state involvement in content moderation and platform behaviour. Regulatory bodies, such as the Korea Communications Standards Commission, work closely with private platforms to implement standards and respond to crises, adopting a collaborative approach rather than rigid regulation. This allows agility in addressing challenges such as misinformation and cyber threats, but also raises concerns regarding transparency, accountability, and the balance between security and civil liberties. Overall, South Korea's digital governance constitutes a complex, adaptive system shaped by strategic priorities, cultural values, and historical experience, making it both effective and vulnerable (Merril, 2025).

As AI is increasingly deployed in the governance of smart cities, a shift from a *Netpolitik* perspective towards a *Digitalpolitik* one becomes apparent. The implementation of AI, and the manner in which it is governed, reorients analytical focus towards considerations of security, sovereignty, and control, thereby placing *Digitalpolitik* at the forefront. The concept of smart cities has evolved beyond its initial role as a governance platform and is now characterised as a strategic digital infrastructure embedded within a fragmented global digital order. This evolution is driven by the mobilisation of smart cities to enhance national competitiveness and digital sovereignty (Yoo, 2025). The growing use of AI-driven surveillance and policing technologies, alongside real-time data integration and risk management systems, exemplifies *Digitalpolitik*'s realist logic, wherein digital technologies are viewed as instruments of state power with coercive or disciplinary potential. It is important to note that this transition does not entail the dissolution of *Netpolitik*. Rather, the adoption of ethical AI frameworks, public participation mechanisms, and collaborative governance models serves to legitimise and domesticate *Digitalpolitik* practices, ensuring social acceptance and institutional stability. The following table summarises South Korea's approach to AI and smart city governance and its hybrid nature when it comes to the logic of *Netpolitik* and *Digitalpolitik*.

Table 15. South Korea's AI and Smart City Governance: Netpolitik vs Digitalpolitik

Domain	Features / Applications	Conceptual Framework
Smart Cities & Urban Safety	AI surveillance, drones, robots, IoT sensors, smart lights, Goalie Patrol, Ansimi app	***Netpolitik*** – citizen-focused, participatory, collaborative governance
Traffic & Transportation	IoT sensors, AI traffic management, public transport coordination	***Netpolitik*** – networked, data-driven urban systems for mobility and sustainability
Environmental Monitoring	AI + IoT for pollution, energy, and weather data	***Netpolitik*** – inclusive, evidence-based sustainability management
Digital Government Services	AI chatbots, mobile ID, digital document wallets, "My Data" initiative	***Netpolitik*** – citizen empowerment, transparency, ethical service delivery
Public Sector Innovation & AI Use	AI for policymaking, procurement, internal administration, fraud detection	***Digitalpolitik*** – enhances administrative control, compliance, and state authority
AI Governance & Ethics	AI Ethics Charter, Governance Framework, impact assessments	***Netpolitik*** – collaborative governance with civil society and industry; legitimises AI use
Urban Safety Infrastructure	Citywide AI cameras, emergency response platforms, integrated safety networks	***Digitalpolitik*** – strategic surveillance, real-time risk management, coercive potential
Digital Infrastructure & Sovereignty	Data centres, domestic platforms, cloud hubs	***Digitalpolitik*** – centralised control, technological sovereignty, reduced foreign dependence

Source: The candidate based on the sources above mentioned.

South Korea's development of smart cities, AI-driven urban governance, and ethical digital frameworks illustrates how the country integrates technological innovation with state coordination to enhance national competitiveness, digital sovereignty, and public service delivery (Yoo, 2025). The following section of the chapter examines how South Korea extends this strategic approach beyond its borders through international engagement, standard-setting, and partnerships in emerging digital technologies.

3.2. International Approach

South Korea's engagement with emerging technologies, global standard-setting, and multilateral cyber partnerships reflects a broader effort to consolidate its influence within the realm of international digital governance, while safeguarding national interests (Feigenbaum & Nelson, 2024). These externally oriented strategies, grounded in public–private coordination, technological innovation, and adherence to international norms, demonstrate how the country projects expertise, legitimacy, and cooperative capacity in cyberspace (Roshan, 2025). Through proactive participation in international organisations, South Korea advances norms of sovereignty, responsible state behaviour, and cooperative cyber defence (Novotná, 2025). The following segment examines how South Korea leverages technological leadership, regulatory influence, and multilateral collaboration to operationalise its international digital strategy.

3.2.1 South Korea's strategy through AI and emerging technologies

South Korea is widely recognised as a pivotal, though often understudied, actor in global standard-setting and digital transformation. The country's position as the world's thirteenth-largest economy, and fourth-largest in Asia, combined with the presence of globally competitive companies, is a primary factor contributing to this status (World Bank Group Korea Office, 2025). As South Korean ICT companies have grown into global leaders, they have increasingly engaged with international standards organisations. This shift has seen companies move beyond using national standards to protect domestic markets, instead proactively collaborating with international bodies to adopt new technologies early and derive commercial advantage. This approach has firmly established South Korea as a digital leader, particularly in the 5G sector (Feigenbaum & Nelson, 2024).

The South Korean private sector is becoming increasingly influential in global technology standards, driven by the rise of world-class ICT companies. While the government has historically dominated standard-setting, private firms are assuming a more active role in international standardisation processes. This engagement occurs primarily through corporate leaders taking positions of influence and the active participation of technical personnel in workshops and seminars (Lee, 2024). Korean companies are progressively directing efforts towards shaping the adoption of specific international standards, aiming to ensure their inclusion as key beneficiaries within the commercial context. Notable examples include leading roles in 5G standardisation and active involvement in areas such as automated vehicles, even as they continue to catch up with other global leaders in some infrastructural technologies (Nam, 2024).

ICT companies such as Samsung Electronics, SK Hynix, LG Electronics, and Naver are at the forefront of innovative technologies including advanced semiconductors, next-generation networks, artificial intelligence, big data, quantum computing, and cybersecurity. Their leadership and innovation position South Korea as a global ICT powerhouse, contributing significantly to shaping international technology trends and standards. Major Korean ICT firms are making significant investments in cutting-edge technologies. For instance, Samsung Electronics has established numerous AI centres globally, with a focus on developing AI chips and machine learning algorithms. Naver is engaged in the development of large language models and advanced AI engines, while telecommunications companies such as SK Telecom and KT Corporation are allocating substantial resources to AI and associated infrastructure (International Trade Administration, 2023). It is evident that private-sector involvement is essential not only for standard-setting but also for promoting the adoption of these standards through their integration into new products and services, thereby influencing global industry trends (Lee, 2024).

The South Korean government's economic focus has shifted towards pioneering cutting-edge emerging technologies, including AI, biotechnology, quantum computing, advanced robotics, and next-generation semiconductors. These technologies drive domestic growth while shaping South Korea's foreign policy, security, and global standing. Commitment to emerging technologies is central to the national strategy, with leaders recognising that future competitiveness, security, and international influence are closely tied to technological leadership. The government has cultivated robust public–private partnerships and developed a highly skilled workforce, positioning the nation as a leading global innovator. The Lee administration, inaugurated in June 2025, has further emphasised technological governance through strategic delegations. President Lee plans to advance AI by building infrastructure, expanding GPU access, promoting open data, and training specialists. The National Artificial Intelligence Committee, established under the previous administration, reflects a top-down approach to AI policymaking, aimed at enhancing infrastructure, promoting industrial applications, and advancing regulatory reform. The government pledged 100 trillion Korean Won towards an AI investment fund, formalised in June 2025 (Park, 2025).

At the launch ceremony of the National AI Strategy Committee, President Lee Jae-myung stated: "Advanced technologies like artificial intelligence (AI) are national power, economic strength, and ultimately, a pillar of security," adding, "the government will provide robust support through strategic investments to ensure that the private sector's creativity, dynamism, and professional capabilities are maximised" (Lee Jae-Myung, 2025). In his address, he outlined four core principles to

realise the vision of South Korea as a leading global AI power. First, he emphasised inclusive, human-centred AI, highlighting the state's role in preventing inequality and polarisation. This effort is framed as a joint public–private initiative, with strategic government support to optimise collaboration. Second, he underlined the importance of restructuring laws, institutions, and ecosystems from an AI-negative standpoint to enable technological advancement. Finally, the president called for balanced AI development, ensuring that national progress benefits society as a whole. These remarks reinforce the government's AI for All agenda, reflecting a commitment to inclusive, balanced, and socially responsible AI development (Joo, 2025).

South Korea's AI for All policy represents a strategic effort to achieve AI sovereignty and position the country among the world's leading AI powers. Following political changes in 2025, the policy prioritises expanding domestic infrastructure, developing culturally specific language models, and strengthening industrial coordination in response to demographic decline, labour shortages, and the need to sustain productivity through automation and robotics. AI development is also central to South Korea's export-oriented economy and national security strategy, with integration into defence technologies and cybersecurity enhancing responses to threats from North Korea. New institutional mechanisms have been established to implement this agenda, and leading firms coordinate domestic innovation. Despite a focus on technological sovereignty, South Korea relies on cooperation with foreign partners, particularly the US, for computing resources and advanced technologies, while seeking to stabilise relations with China due to sensitivities around defence-related collaboration. Deeper security cooperation with the US may, however, provoke renewed pressure from Beijing, requiring Seoul to balance its ambitions with careful diplomacy towards Washington and Beijing (Akhand, 2026).

President Lee's assertion that AI constitutes "national power" and a "pillar of security" (Lee Jae-Myung, 2025), together with the government's commitment to large-scale strategic investment and the pursuit of AI sovereignty, exemplifies *Digitalpolitik*'s realist logic, in which digital capabilities are regarded as strategic assets within a fragmented global digital order. The prioritisation of technological leadership as a core element of foreign policy, defence, and international standing, alongside the integration of AI into cybersecurity and military resilience, aligns with *Digitalpolitik*'s emphasis on state survival, competitive advantage, and digital sovereignty (Duarte, 2025). This Digitalpolitik orientation is reinforced by South Korea's proactive engagement in global standard-setting as a means of consolidating structural power in digital markets. The active involvement of South Korean companies in international standards bodies, particularly in sectors such as 5G and automated vehicles,

demonstrates how regulatory and technical norms are strategically leveraged to secure long-term economic and geopolitical influence. This aligns with McDonald and Mina's (2018) observation that states and corporations seek to project influence in global digital markets. Although private companies play a leading role, their activities are embedded within a nationally coordinated strategy that aligns corporate success with state interests, exemplifying *Digitalpolitik*'s fusion of market power, regulatory influence, and technological capacity.

Simultaneously, the strategy incorporates significant elements of *Netpolitik*, particularly through its emphasis on cooperation, legitimacy, and inclusive governance. South Korea's engagement in global standardisation initiatives, evidenced by active participation in workshops, seminars, and leadership roles, reflects Bollier's (2003) conceptualisation of networked influence, wherein power is exercised through professional communities, technical expertise, and transnational networks rather than direct coercion. Similarly, the AI for All agenda and the president's focus on people-centred, balanced, and socially responsible AI development align with *Netpolitik*'s emphasis on moral legitimacy, societal values, and soft power. The promotion of open data, skills development, and collaborative public-private ecosystems indicates a liberal-oriented strategy aimed at building credibility and trust both domestically and internationally. The table 16 below showcases South Korea's strategy in AI and emerging technologies and its connections with both Netpolitik and Digitalpolitik logics.

Table 16. South Korea's AI and technology strategy - Netpolitik vs Digitalpolitik

Category	Netpolitik	Digitalpolitik
Government Approach	Focus on inclusive, human-centred AI with societal balance and preventing inequality	AI and emerging tech are treated as strategic assets
International Engagement	Engagement in global standards organisations and cooperation with foreign partners	Securing a competitive economic and geopolitical edge through standard-setting
Private Sector Role	Collaborating with government on responsible AI and innovation	Drives AI innovation, early standard adoption and digital power
Strategic Objectives	Achieve domestic and international legitimacy, trust and moral authority	Enhance digital sovereignty and integration of technology into defence, security and foreign policy

Source: The candidate based on the sources above mentioned.

South Korea's strategic emphasis on AI, emerging technologies, and global standard-setting illustrates how the country leverages technological leadership to enhance economic competitiveness,

national security, and digital sovereignty (Feigenbaum & Nelson, 2024). The following subsection examines how these capabilities are operationalised in the international arena through cyberspace governance, multilateral partnerships, and the promotion of norms for responsible state behaviour.

3.2.2 Cyberspace sovereignty and partnerships

South Korea abides by international norms and laws, including those set out in the UN Charter. It asserts that the principles of sovereignty, non-intervention, the prohibition of the use of force, and self-defence apply in cyberspace. It regards cyber activities that intrude upon or gain unauthorised access to its infrastructure as violations of sovereignty. It also maintains that international laws governing territorial sovereignty apply in cyberspace. South Korea is active in international discussions and initiatives, advocating responsible state behaviour and compliance with international legal frameworks, and engaging with international organisations and forums to shape the development of global norms, while emphasising the importance of applying international law to cyberspace. South Korea also recognises the need for ongoing dialogue, participating in relevant multilateral mechanisms and articulating clearer positions through official statements (Ministry of Foreign Affairs, 2025).

South Korea's approach aims to foster trust, promote responsible behaviour, and align national and international security interests. It influences global cyberspace by engaging with international organisations such as the UN and contributes to shaping norms on sovereignty, the use of force, and state responsibility. These efforts include issuing position statements, participating in global forums, and promoting adherence to international law. South Korea's emphasis on its domestic legal framework can influence international practices by setting a precedent (Sohyun, 2025). South Korea is a key supporter of the United Nations Global Counter-Terrorism Programme on Cybersecurity and New Technologies, providing financial support and participating in key initiatives. In 2022, it funded the first Counter-Terrorism Cybersecurity Table-Top Exercise for Cities, aimed at improving preparedness against cyber-enabled terrorism. In December 2022, South Korea co-organised a panel discussion on cyber and new technologies in the context of counter-terrorism, fostering international dialogue and cooperation. Through these contributions, South Korea plays a significant role in strengthening global efforts to counter technological threats posed by terrorism (United Nations Office of Counter-Terrorism, 2023).

During the 2024-2025 UN Security Council term, South Korea, as a non-permanent member, assumed a leading role by chairing its inaugural cybersecurity-focused meeting in April 2024. The Arria-formula informal gathering, co-hosted by the US and Japan, sought to address the evolving nature of cyber threats. These threats included the use of ransomware, cryptocurrency misuse, and illicit cyber

activities by North Korea, which were identified as a significant source of funding for the development of weapons of mass destruction. South Korea's initiative reflects its commitment to enhancing international peace and security by promoting greater understanding and cooperation on cybercrime issues within the Security Council framework (Da-gyum, 2024).

The collaboration between the European Union (EU) and South Korea is grounded in shared universal values and interests, with a strong emphasis on upholding the principles of international law and the UN Charter. At the Seoul Summit on 22 May 2023, the Joint Statement acknowledged threats to global peace and security and called for the development of a security partnership, including the establishment of a Strategic Dialogue at the Foreign Ministerial level to strengthen cooperation. The summit underlined the importance of enhanced collaboration across a range of areas, including cybersecurity. Both parties committed to building on existing momentum to intensify cooperation and address shared security challenges. Accordingly, the EU and South Korea aim to expand and strengthen dialogue and cooperation across the full spectrum of security and defence issues through existing frameworks. In the cyber domain, the EU and South Korea agreed to deepen their Cyber Policy Consultations through regular exchanges on the threat landscape, policy frameworks, and practical cooperation. This includes coordinating diplomatic responses to malicious cyber activities and aligning cyber capacity-building efforts. They will continue to cooperate at multilateral, regional, and bilateral levels, particularly in promoting the UN framework on responsible state behaviour in cyberspace and supporting the establishment of a UN Cyber Programme of Action. Their cooperation also addresses North Korea's illicit cyber activities that fund weapons of mass destruction and ballistic missile programmes and supports the development of cyber confidence-building measures within the ASEAN Regional Forum, especially regarding the protection of critical infrastructure (European External Action Service, 2024).

In 2016, South Korea launched the Cybersecurity Alliance for Mutual Progress (CAMP), a global network aimed at enhancing international cooperation and information sharing to address cyber threats. CAMP facilitates coordination and collaboration in responding to cyber incidents, promotes best practices, and supports capacity building. By providing a platform for dialogue and joint efforts, CAMP helps to strengthen collective cybersecurity resilience, particularly in developing regions. With over 59 members from around 45 countries, it exemplifies South Korea's proactive approach to fostering global cybersecurity partnerships (Wood, 2024). More recently, in late 2024, South Korea and NATO launched the High-Level Cyber Dialogue. This initiative aims to improve international cooperation against cyber

threats by facilitating the sharing of threat intelligence and joint cyber defence strategies. The partnership reflects the commitment of South Korea and NATO to strengthening cyber resilience through cooperation and underscores the importance of multilateral efforts in addressing cyberspace security and countering cyber activities originating from state and non-state actors (Roshan, 2025).

South Korea is an active participant in the ASEAN Regional Forum (ARF), a key forum for security cooperation in the Asia-Pacific. Within the ARF, it engages in discussions on cybersecurity, confidence-building measures, and capacity-building to address emerging threats. South Korea's involvement reflects its commitment to regional stability and its recognition of the importance of multilateral collaboration in managing cybersecurity challenges. By participating in the ARF's working groups on cybersecurity and confidence-building measures, South Korea helps to establish a stable regional security environment. Its active engagement also supports bilateral and trilateral initiatives, providing a broader framework for international cooperation and the development of shared norms and standards in cyberspace (Roshan, 2025).

Within the regional context, South Korea's cybersecurity engagement extends beyond broader multilateral forums. South Korea and Japan share strong concerns about North Korea's cyber capabilities, particularly its use of cyberattacks to fund weapons programmes and target critical sectors in both countries. Both states are frequent targets of North Korean state-sponsored cyber operations, creating a common security interest in the cyber domain. Despite this shared threat perception, bilateral cybersecurity cooperation between Japan and South Korea has been limited, with few sustained mechanisms. Instead, most cooperation has occurred within trilateral frameworks involving the US. Since 2014, Japan and South Korea have participated in the Trilateral Cyber Policy Consultations and the Experts Meeting on Cybersecurity of Critical Infrastructure, together with the US. However, these mechanisms have been infrequent, with irregular meetings and limited continuity. More recently, in 2023, the three countries agreed at ministerial and leaders' levels to counter North Korea's cyber activities that fund its weapons programmes. This led to the creation of a new trilateral working group and the establishment of a high-level consultative group, which committed to closer cooperation on incident response, threat intelligence sharing, and cyber defence strategies (Vosse, 2025).

South Korea's relationship with the G7 has evolved from informal participation to a structured and pragmatic engagement, reflecting Seoul's broader strategy of navigating a fragmented and uncertain international environment. While not a member, South Korea has become a regular and valuable partner in G7 processes, leveraging the forum's informal nature for agenda-setting, political

signalling, and coalition-building. This engagement complements Seoul's alliance with the US, its partnerships with NATO and the EU, and its efforts to normalise relations with Japan. The G7 serves as a stabilising external platform, helping to depersonalise bilateral tensions and promote cooperation on shared global challenges (Novotná, 2025).

President Lee Jae-myung's inaugural attendance at the G7 Summit in June marked a pivotal moment in South Korea's evolving foreign policy. His participation indicated a shift towards pragmatic multilateralism, flexible diplomacy, and broader international engagement. Despite limited prior experience in major multilateral forums and the ongoing formation of his foreign policy team, Lee adopted a cautious and measured approach rather than pursuing a dramatic policy shift. His engagement signalled a recalibration from rigid alignment toward interest-based diplomacy, emphasising economic nationalism, dialogue over deterrence, and expanded multilateral outreach beyond traditional Western partners. It also suggested an effort to move beyond a strictly US-centric framework and to navigate complex regional and global dynamics more flexibly. Although not indicative of a sudden transformation, his participation established the foundations for a new trajectory, aimed at aligning South Korea's international role with its growing capabilities and long-term aspirations (Singh, 2025).

This approach aligns closely with the logic of *Netpolitik*, being primarily cooperative, norm-oriented, and multilateral in its cybersecurity governance. The focus on international law, sovereignty, non-intervention, and responsible state behaviour demonstrates a commitment to legitimacy and norms through international institutions such as the UN. This emphasis on multilateral mechanisms corresponds to Bollier's (2003) conception of *Netpolitik*. South Korea's efforts to shape global cyber norms through statements, forums, and legal precedents reflect *Netpolitik*'s reliance on persuasion, credibility, and cooperation. Its active involvement in cooperative security frameworks further reinforces *Netpolitik*, prioritising information sharing, confidence-building, capacity-building, and collective resilience. Digital networks and institutions are employed to manage cooperation and interdependence, embodying *Netpolitik*'s liberal emphasis on networked governance, coalition-building, and soft power through institutional embeddedness. At the same time, elements of *Digitalpolitik* are evident, particularly its strong focus on sovereignty, territorial integrity in cyberspace, and national security interests. Cyber intrusions are framed as violations of sovereignty, reflecting *Digitalpolitik*'s security-centred worldview, in which digital space is seen as an extension of geopolitical competition. The following table 17 illustrates South Korea's hybrid approach to its cybersecurity strategy.

Table 17. South Korea's Hybrid Cybersecurity Strategy

Category	Netpolitik	Digitalpolitik
Legal /Norms	International law, UN Charter, legitimacy	Sovereignty, security, territorial integrity
International Engagement	UN, ASEAN, EU, G7, trilateral forums, dialogue and cooperation	Counter threats, strategic positioning, North Korea cyber threats
Multilateral Initiatives	CAMP, UN Counter-Terrorism Programme, NATO Cyber Dialogue, info-sharing & capacity-building	Shape global cyber norms, advance national influence
Government Approach	Inclusive, cooperative, human-centred AI	Security focus
Private Sector	Ethical & responsible AI, collaboration in networks	Tech innovation, standard adoption
Objectives	Build trust, cooperation, resilience	Digital Sovereignty

Source: The candidate based on the sources above mentioned.

In summary, South Korea's strategy reflects a hybrid approach that integrates multilateral cooperation, norm-setting, and technological innovation to promote international legitimacy while securing national interests. Domestically, the government emphasises inclusive, human-centred AI policies, robust public–private partnerships, and technological sovereignty, supported by investments in AI, semiconductors, next-generation networks, and cybersecurity infrastructure (Joo, 2025). Internationally, South Korea engages actively in multilateral forums such as the UN, ASEAN Regional Forum, G7, NATO, and EU consultations, shaping global cyber norms, promoting responsible state behaviour, and participating in initiatives like CAMP and the UN Counter-Terrorism Programme on Cybersecurity (Roshan, 2025). Through these combined domestic and international efforts, South Korea balances *Netpolitik*, emphasising cooperation, legitimacy, and soft power, with *Digitalpolitik*, prioritising sovereignty, security, and strategic influence, thereby constructing a distinctive model of cyberspace governance that advances both national resilience and global engagement. The last chapter will compare both China's and South Korea's approaches and analyse the similarities and differences between their strategies.

4. Comparing the Chinese and South Korean models

This chapter compares the digital governance models of China and South Korea, analysing how both states regulate cyberspace, AI, and digital infrastructure while pursuing national security, economic competitiveness, and technological influence. The first subsection examines the main similarities between the two cases, focusing on state-led cybersecurity governance, the integration of legal and institutional frameworks, and the role of public-private collaboration in developing emerging technologies and cyber capabilities. It also considers how both countries engage internationally to shape digital standards and AI governance. The second subsection analyses the key differences between the two models, particularly in data governance, legal frameworks, surveillance practices, and international digital strategies. While China emphasises state sovereignty, centralised control, and data-driven governance, South Korea adopts a more regulatory, rights-based approach that balances technological innovation, democratic oversight, and international cooperation.

4.1. Similarities

The following subsection examines the key similarities between China and South Korea in their approaches to digital governance, focusing on how both states prioritise cybersecurity, AI, and digital infrastructure as instruments of national power and strategic influence. Both countries implement state-led frameworks that integrate legal, institutional, and technological mechanisms to secure cyberspace and critical infrastructure, while fostering collaboration with private-sector actors to advance innovation and enhance cyber capabilities (Paz et al., 2024). This subsection also highlights how China and South Korea engage internationally to shape AI governance, set standards, and promote digital norms, reflecting a shared understanding of digital technologies as central to economic competitiveness, national security, and global influence.

4.1.1 State-led cybersecurity governance and Integration of law, technology, and institutions

China's cybersecurity approach is characterised by a centralised legal and institutional framework emphasising state-led governance. Specialised agencies and mechanisms operate under central government departments to ensure coherent policymaking, enforcement, and coordination across different sectors and levels of government. This approach integrates top-down coordination with international cooperation, maintaining strict control over cyberspace while engaging in global dialogue. Cybersecurity efforts align with national security and law-based governance objectives, reinforcing the state's dominant role in cyberspace regulation (State Council, 2023a). Since Xi Jinping took office, China has seen a shift towards centralisation. This has been further fuelled by the response to the trade war with the US and Xi's Maoist style of governing. Xi has strengthened his authority in areas including

national security, cybersecurity, and military reform. In the face of rising tensions with the US, China's recentralisation is particularly pronounced in science and technology (Xiao & Xu, 2024).

China's cyberspace governance is explained by its combination of capitalism, authoritarianism, and Confucianism, or "authoritarian informationalism" (Murniasari, 2024, p. 4). This model suggests that the internet poses a threat to the regime, however, challenges have been mitigated by promoting growth, stability, and identity. The government seeks to use the internet to strengthen its control over society and bolster legitimacy. Cybersecurity is viewed as part of national security, involving the minimisation of risks and threats to a reference object arising from activities in cyberspace. Structural changes following President Xi Jinping's directive were driven by insecurity. Insecurity has long been a concern for political leaders in China, and information and communication technologies have heightened this concern, as society now has greater opportunities to create, discover, and disseminate contradictory narratives (Murniasari, 2024). Xi envisions legislation to protect national security and ensure economic and social stability. This requires making cyberspace more manageable and building China's digital resilience to support the country's transition from an industrial to an information era (Descamps, 2020).

The policy context for this activity was guidance from China's political leaders that the expanded application of ICT was a national priority. In 2015, the State Council promoted the “deep integration” of the internet with all aspects of the economy and society, as well as the “Made in China 2025” guidelines to help Chinese industry reach the technological frontier in various sectors, with ICT-related industries featuring prominently (Lee, 2022, p. 11). The CCP's theoretical justification for its policies identifies informatisation as a global trend that China must keep pace with to modernise and protect itself against foreign powers. This policy framework has been matched by measures to develop and deploy ICT technologies and infrastructure. A 2021 study by the International Institute for Strategic Studies judged that China's cyber defences were weak and that the country was still in the early stages of building resilience into its critical infrastructure. These insecurities have been exacerbated by the US targeting China's foreign dependencies in essential technologies, notably semiconductors, in a context of worsening relations. This has led to a policy and regulatory push by Chinese authorities to gain visibility and control over cyberspace, even as they seek to exploit it for development goals (Lee, 2022).

China is strengthening protection over CII by establishing security measures, including monitoring, defence against cyber threats, and legal responsibilities for operators. It requires security management institutions to be set up within relevant organisations, with clearly defined responsibilities

for ensuring network safety. It also promotes information sharing among government departments, operators, and cybersecurity agencies to facilitate a timely response to threats, vulnerabilities, and incidents. The regulation emphasises the importance of securing the energy and telecommunications sectors, encouraging technological innovation and talent training in cybersecurity. It stipulates legal liabilities for operators, including corrective actions and penalties for non-compliance, thereby reinforcing accountability. Overall, China's strategy combines regulatory oversight, technological advancement, talent cultivation, and interdepartmental cooperation (State Council, 2021).

China's regime regarding CII is characterised by a top-down approach with strict oversight, clearly defined responsibilities, and severe penalties for non-compliance. Since September 2021, the Chinese government has demanded specific cybersecurity measures and the reporting of system anomalies from CII operators, who are required to implement security protocols. The regulations mandate that regulatory authorities identify and designate CII operators based on the importance of their network systems to national security, the potential harm caused by security breaches, and their cross-sector impacts. Designated operators must then establish and maintain security measures, conduct risk assessments, and report incidents. The government enforces oversight through multiple levels of administration, including the CAC and the National Security Bureau. Penalties for violations range from warnings to hefty fines, with personal liability also possible. The regime allows for the designation of foreign companies as CII operators, requiring them to comply with Chinese cybersecurity standards and reporting obligations, ensuring control over critical data. China's regime emphasises oversight, compliance, and accountability (Huld, 2021).

China's centralised internet governance heavily influences its tech companies by establishing strict regulatory controls and oversight through agencies such as the CAC. The CAC has absolute authority over internet infrastructure and enforces legal frameworks, including audits, warnings, penalties, and censorship. This system emphasises compliance with government directives and aligns private-sector activities with state policies, promoting a top-down control approach. Enforcement methods ensure companies adhere to China's rules on information security, data management, and ideological standards, shaping how tech companies operate both domestically and internationally. China uses technology to centrally control cyberspace, integrating infrastructure, law, and ideology. It employs tools such as the Great Firewall to regulate content and activities online. The CAC implements these controls by coordinating with internet providers and operators, using fines and content removal. These measures maintain control, ensure compliance, and suppress dissent (Mok, 2025).

In the case of South Korea cybersecurity is also vital for national security and economic growth. President Lee views strong and systematic information protection as essential to support AI development and technological innovation. He advocates closer cooperation between the public and private sectors to enhance cybersecurity capabilities, improve resilience, and create a safe digital environment for citizens. He also underscores the importance of transforming cybersecurity into a core national strategy, supporting industry growth, and cultivating security talent. The government is taking several specific steps to boost cybersecurity, including reorganisation, setting clear security benchmarks, and raising cyber protection standards for regional and small-scale businesses. Plans also include expanding cybersecurity events and improving legislation. President Lee emphasises the importance of developing the information protection industry for national security and economic growth, advocating support for the industry's transformation into a strategic sector (Kim, 2025).

South Korea's centralised cyber governance system is structured around a three-layer security monitoring framework, consisting of agency-level, sector-level, and national-level monitoring, which detects and responds to cyber threats and disseminates threat detection techniques to lower-level centres. Central administrative agencies operate 44 network security monitoring centres that provide continuous protection for information and communications networks. Additionally, the system incorporates cybersecurity control and monitoring for e-government, safeguards against exposure, falsification, and damage of electronic documents, and guarantees official identification and document integrity. The system also ensures the security of electronic documents and the integrity of official identification (Paz et al., 2024). South Korea prioritises the security of its critical ICT infrastructure, recognising its importance to citizens' safety and well-being. Korean law requires all critical ICT infrastructures to confirm the implementation of security measures at least once a year to protect against cyber threats. The government has also taken steps to enforce compliance, including publishing guidelines for assessing security measures. These infrastructures span multiple sectors and are managed by numerous organisations under various administrative departments (Ministry of Science and ICT, 2025a). South Korea enforces annual security checks for critical ICT infrastructures, revises guidelines to address emerging problems and evolving technologies, and involves infrastructure operators and security experts to improve and validate these guidelines, ensuring robust protection (Park & Kim, 2025).

These developments reflect the logic of *Digitalpolitik,* understood as the strategic projection of state power into the digital sphere and the treatment of digital infrastructure as a site of geopolitical and

domestic control. In line with McDonald and Mina's (2018) argument that states seek to influence global digital markets and construct national digital regimes, China's cybersecurity framework demonstrates how regulation, surveillance, and governance are mobilised to secure regime stability and national security. The "authoritarian informationalism" model (Murniasari, 2024, p.165) illustrates how digital technologies are used to manage narratives and consolidate authority, reinforcing a worldview centred on security. Measures such as protecting critical information infrastructure and enforcing compliance show how digital networks function as instruments of governance, consistent with the emphasis on digital power as an extension of authority. South Korea's systems demonstrate how resilience, infrastructural control, and technological competitiveness are embedded in national strategy (Kim, 2025). In both cases, external pressures intensify perceptions of vulnerability and state oversight of cyberspace. This reinforces the claim that *Digitalpolitik* is driven by and leads to fragmentation and nationalisation. The cases illustrate how China and South Korea prioritise sovereignty, security and technological supremacy over openness and individual autonomy. This is done by integrating instruments into strategies of power projection and digital sovereignty in a contested international order. Table 18 below summarises the connection between both countries and *Digitalpolitik*.

Table 18. China and South Korea's Cyber Governance through the Lens of Digitalpolitik

Dimension	China	South Korea	Digitalpolitik
Governance	Highly centralised, CAC-led control	Centralised, multi-level monitoring	State-led digital governance
Security Focus	Regime and national security	National safety and resilience	Cyberspace as security domain
Infrastructure	Strict CII oversight	Mandatory ICT audits	Control enables sovereignty
Regulation	Censorship, heavy penalties	Compliance guidelines	Law as power instrumen
Ideology	Authoritarian informationalism	Developmental security	Security-centred worldview
Main Goal	Stability and control	Security and growth	Power and sovereignty

Source: The candidate based on the sources above mentioned.

The next subsection aims to analyse how public-private collaboration and international engagement shape national cyber and technological strategies. In a digitalised geopolitical environment,

states rely on governmental institutions and private technology firms to develop cyber capabilities, drive innovation and expand influence in global digital governance frameworks (Aitel et al., 2025). It explores how both countries mobilise their private sectors to strengthen cyber capabilities and advance strategic interests. It also examines how these domestic collaborations extend into the international sphere, particularly through initiatives related to artificial intelligence governance, digital standards, and development cooperation.

4.1.2 Public-Private collaboration and international engagement

Private sector companies in China play a significant role in the country's cyber strategies. These firms serve both as innovative developers of cybersecurity technologies and as instruments of state interests. They operate under strict government regulation and act as extensions of Chinese national security objectives. Many of these companies, such as Tencent, ByteDance, and Xiaomi, have garnered international influence through their products and services, which can be leveraged for cyber espionage, intellectual property theft, or influence operations. The Chinese government has encouraged domestic cybersecurity firms to contribute to national security by fostering innovation within the private sector and integrating these companies into broader military-civil fusion efforts (Klyman, 2022). These firms conduct research and development that supports both commercial interests and intelligence activities. They often share vulnerabilities and facilitate access to global digital infrastructure. Moreover, regulatory measures now require these companies to share zero-day vulnerabilities with the government, which can then be exploited for cyber operations. Overall, private sector companies are vital to China's cyber capabilities, providing technological innovation, talent, and infrastructure that support both defensive and offensive cyber efforts (Aitel et al., 2025).

The Chinese government and technology firms have collaborated to develop cyber capabilities rapidly, giving state institutions access to advanced technologies and talent. This cooperation has focused on AI, data analysis, 5G, and cloud computing, strengthening China's cyber-offensive capabilities and capacity for state-sponsored cyber operations. Access to private company data enhances intelligence gathering, facilitating more accurate and effective cyberattacks. Innovations from the private sector are integrated into state capabilities, reinforcing China's technological and cyber strength. China's cyber operations model involves government and private companies collaborating to conduct cyberattacks on targets deemed important to Beijing. Large technology firms play a central role in this regard, with several leading Chinese technology companies functioning as major cyber contractors for the state. Firms such as ThreatBook, Qihoo360, and Qi An Xin provide defensive cybersecurity services to public agencies but are also believed to support offensive operations.

Alongside these major firms, numerous SMEs (small and medium-sized enterprises) operate within the same ecosystem, often as subcontractors providing specialised services. One example is i-Soon, a Shanghai-based firm with 72 employees, whose connections to the Chinese government became public following a data leak in early 2024 (Vijayan, 2024).

China's socialist market economy combines private entrepreneurship with political control by the CCP. Xi has publicly reaffirmed the importance of private enterprise for growth, but his governance has strengthened Party oversight and embedded political authority within corporate structures. This arrangement positions private firms as key drivers of development while subjecting them to close supervision by the CCP. Market activity is permitted only if it aligns with Party priorities, and the state can intervene when firms diverge from national objectives. The CCP implements this system through Party cells, oversight mechanisms, and state capital, aiming to leverage market dynamism while maintaining firm political control (Dohr, 2025).

Concerning AI, China has become a major player in global AI governance, reflecting its status as the world's second-largest economy. In October 2023, Xi Jinping proposed the Global Artificial Intelligence Governance Initiative, presenting AI as a critical domain for humanity's future and outlining China's approach to global governance in this field. Subsequent statements emphasised expanding international cooperation in AI, strengthening technological capacities in countries of the Global South, and contributing to the reduction of the global digital divide. China also advocates stronger alignment of development strategies, governance rules, and technical standards in order to establish a global governance framework and standards based on broad international consensus (Ping, 2026). The Global Artificial Intelligence Governance Initiative sets out China's principles for developing, securing, and regulating AI. These include a people-centred approach to AI that benefits humanity, respecting mutual respect and cooperation, opposing ideological division and exclusive blocs, and implementing risk assessment and testing to improve safety, reliability, controllability, and fairness. It emphasises international cooperation to reduce digital and governance gaps (Ministry of Foreign Affairs, 2023).

The Global AI Governance Action Plan, published in July 2025 proposes international action guided by the principles of AI for the benefit of humanity, national sovereignty, alignment of AI development with other objectives, safety, inclusiveness, and cooperation. It stresses participation from governments, international organisations, enterprises, research institutions, and civil society in developing and governing AI (Ministry of Foreign Affairs, 2025). Priorities include expanding infrastructure, encouraging innovation through cooperation, reducing barriers, and promoting adoption

to support economic and social development and the 2030 United Nations Agenda for Sustainable Development (United Nations in China, 2025). The plan promotes the broad application of AI across various sectors, emphasising cooperation, best practices, and intelligent infrastructure. It highlights the importance of open and innovative technological ecosystems, including open-source collaboration, resource sharing, and interoperability. It underlines the need for international standards and norms, the role of public institutions in deploying and regulating AI in public services, and strengthened governance through risk assessment systems, transparency measures, and safeguards against misuse. Finally, it emphasises the central role of the United Nations in global digital governance, calls for international cooperation to bridge the digital divide, and supports an inclusive multi-stakeholder governance model (People's Republic of China UN Mission, 2025).

China's approach to AI governance involves selective shaping, prioritising areas where it has strategic advantages. Key priority areas include technical standards, AI safety, data governance, environmental sustainability, and capacity building. This allows China to maximise its influence in emerging governance areas. It targets regions and contexts with regulatory gaps, particularly in developing countries, where its initiatives can have greater impact. China's strategy for shaping international AI governance involves soft-law instruments, partnerships, channels, regional organisations, and collaborations. It promotes technologies and standards in developing countries before international rules are finalised, including through joint AI centres and infrastructure. China regularly updates governance frameworks and adjusts its positions on sensitive issues. Overall, China uses selective domains, institutions, and partnerships to promote preferred norms and governance arrangements (Wang, 2025). China has become increasingly proactive in promoting global AI engagement, particularly through multilateral diplomacy. Its approach to global AI governance is largely based on its domestic strategy, which integrates development and security, with economic development taking priority. AI is viewed pragmatically, emphasising its role in economic growth and industrial modernisation. Growing ethical and security concerns have led China to support safeguards and accountability mechanisms to ensure safe, reliable, and controllable AI. China aims to shape global AI governance and align the international environment with its own development goals, while protecting its technological competitiveness. Concerned about inequalities in the global technology landscape, particularly Western domination of rules, standards, and frameworks, China seeks to expand its influence in global institutions to counter this. (Qiao-Franco & Van Beek, 2025).

When it comes to South Korea, the government's ministries have emphasised the potential economic benefits for companies participating in development cooperation. To fulfil this role, companies must align their activities with the development goals of partner countries (Kim, 2024). In November 2022, the South Korean government introduced a strategy to encourage private investment and support corporate participation through Official Development Assistance (ODA), including plans for blended finance and impact investment. The strategy also sought to connect companies' ESG (environmental, social, and governance) activities with ODA initiatives and improve consultation between the government and businesses. The Korea International Cooperation Agency (KOICA), central to partnerships with the private sector, is promoting new models linked to development cooperation projects and companies' business strategies (Government of Korea, 2022). An example of this is a vocational training project for women in Ghana's electronics sector by Samsung Electronics. Since 2022, development cooperation has included both large corporations and SMEs. For example, Samsung Electronics launched a smartphone upcycling project in Uganda, while SK Forestry initiated a project in northern Vietnam that reduces forest degradation and greenhouse gas emissions. The Export-Import Bank of Korea has also promoted private sector participation through public-private partnership projects (Kim, 2024).

South Korea's public-private collaboration in smart technologies is characterised by a strong, integrated approach that leverages the strengths of both sectors. The government plays a pivotal role by providing significant funding and strategic direction to nurture the country's New Generation Technologies (NGT) capabilities. In 2024, South Korea announced a substantial fund to boost technologies such as AI, semiconductors, batteries, and robotics. These funds are offered at low interest rates to private companies and facilitated through partnerships with major corporations, thereby fostering growth and innovation in the private sector. Essential to South Korea's strategy is the establishment of consultative bodies that bridge the government, industry, academia, and manufacturers. These platforms provide channels for ongoing feedback and joint strategising to strengthen local industries, particularly in semiconductor development and AI security (Sharma, 2025). Large conglomerates, such as Hyundai, Samsung, and Hanwha, are key partners in this ecosystem. They proactively invest in and adopt emerging smart technologies, frequently expanding their capabilities through acquisitions and collaborations. The acquisition of Boston Dynamics by Hyundai in June 2021 signifies the company's dedication to robotics, while Samsung provides financial support to robotics startups such as Rainbow Robotics, whose products are currently undergoing trials by the Korean Army. Furthermore, the government recognises innovative startups specialising in niche areas,

such as quantum technologies and AI semiconductors. These startups are designated as national strategic technologies, positioning them for both domestic and international opportunities (Helman, 2025).

South Korea has successfully led the development of international standards for AI safety and trustworthiness. These standards provide a framework for assessing and managing data quality to ensure AI models are safe, reliable, and unbiased. This achievement marks the world's first standard to address AI safety from a data quality perspective. It tackles critical challenges in AI development and helps to ensure compliance with international regulations. By focusing on data quality, the standards promote risk management and interoperability across AI systems globally. They create a common language and best practices that can be adopted internationally, fostering trust in AI systems by enhancing model accuracy and reliability. Furthermore, South Korea leads international standardisation efforts, shaping digital and AI regulations and innovations. It collaborates with major technological powers to drive consensus on AI governance and safety worldwide. South Korea's contribution impacts the global AI community by establishing a foundation for safe and trustworthy AI development based on high-quality data, encouraging innovation, compliance, and interoperability. This paves the way for reliable AI-integrated services and strengthens global efforts to manage risks from sophisticated AI technologies (Ministry of Science and ICT, 2025b).

As a signatory of the Seoul Declaration, South Korea plays a significant role in advancing AI safety on the international stage. Through its AI Safety Institute (AISI) and participation in the International Network of AISIs, South Korea collaborates closely with other like-minded countries, including the US, members of the EU, Japan, and others, to develop harmonised AI safety standards. This collective endeavour seeks to establish process, management, and product testing standards that emphasise responsible AI development and deployment, human rights, and civil liberties. The government of South Korea has leveraged its technical expertise and convening power within its domestic AI ecosystem to contribute effectively to the creation of coherent, safety-focused international standards. These standards have the potential to inspire broader global adoption (Fort, 2024).

The 2025 International AI Standards Summit in Seoul saw the joint release of the Seoul Statement on AI Standards by the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunication Union (ITU). This historic declaration reflects South Korea's commitment to trustworthy, human-centric AI technologies by emphasising socio-technical considerations, human rights, multistakeholder collaboration, and capacity

building. Although the Seoul Statement is a policy document rather than a technical standard, it strategically directs global AI standardisation efforts, including Korea's domestic AI governance framework. South Korea's leadership in fostering international cooperation and AI innovation helps ensure AI benefits society equitably and responsibly, positioning the country as a global advocate for ethical and sustainable AI development (International Organisation for Standardisation, 2025).

The relationship between the state and private technology firms in China and South Korea reflects the core logic of *Digitalpolitik*. As McDonald and Mina (2018) argue, *Digitalpolitik* involves states using regulatory authority, market leverage, and technological capabilities to advance national power through the digital domain. In China, private technology companies are integrated into national cyber strategies, supporting innovation, intelligence activities, and cyber operations. Through military-civil fusion and CCP oversight, the state leverages commercial innovation to strengthen its cyber capabilities. South Korea follows a different but related model, in which the government coordinates closely with large corporations and startups through funding, policy direction, and innovation platforms in AI, semiconductors, and robotics (Helman, 2025). Both countries also attempt to shape global digital governance, with China promoting the Global Artificial Intelligence Governance Initiative and South Korea leading international AI safety and standardisation efforts. These strategies illustrate *Digitalpolitik*'s premise that technological ecosystems, corporate actors, and digital standards have become key instruments through which states pursue influence and strategic advantage in the global digital order. Table 19 below summarises how both countries' approaches are similar to one another in the logic of *Digitalpolitik*.

Table 19. State-Private Sector Collaboration in the Logic of Digitalpolitik

Dimension	China	South Korea	Digitalpolitik
Public-Private collaboration	Tech firms integrated into national cyber strategy	Government–chaebol collaboration in NGT sectors	States mobilise corporate innovation
Governance	Strong CCP oversight of private firms	Strategic funding and policy guidance	State direction of digital ecosystems
Cyber capabilities	Firms support cyber operations and intelligence	Investment in cybersecurity and defence tech	Digital tech integrated into security
Global AI governance	Global AI Governance Initiative	Leadership in AI safety standards	Norm-setting as geopolitical influence

Source: The candidate based on the sources above mentioned.

The following subsections aim to analyse the differences between both states in their approaches to digital governance. Although China and South Korea both recognise the strategic importance of digital technologies, their governance models reflect different political systems, legal frameworks, and policy priorities. China's model emphasises strong state sovereignty, centralised control, and the use of regulatory and technological systems to manage information and maintain political stability. In contrast, South Korea adopts a more regulatory and rights-based approach that seeks to balance data protection, privacy, and technological innovation within a democratic governance framework. By examining governance models, legal frameworks, and technological strategies, the following subsections highlight how these differences shape each country's approach to digital governance and the broader management of cyberspace.

4.2. Exploring the differences

China's model emphasises state sovereignty, centralised control, and extensive surveillance, integrating legal regulation and AI-driven monitoring to maintain political stability and manage information flows. In contrast, South Korea adopts a more rights-based, regulatory approach that balances data protection, citizen privacy, and technological innovation, while promoting transparency and international cooperation in cyberspace governance. This subsection underscores how these divergent strategies reflect broader differences in national priorities, governance structures, and approaches to digital sovereignty.

4.2.1 Governance Models and Legal Frameworks in Data Governance

China's conception of cyberspace differs fundamentally from Western approaches. Western perspectives treat the internet primarily as a technological environment governed through technocratic management. China conceptualises it as an information space that must be tightly regulated to prevent threats to state power, national unity, and national interests. Within this framework, the Chinese government asserts its sovereign right to control and organise cyberspace, while formally acknowledging citizens' rights. The principle of internet sovereignty serves as the foundation for China's comprehensive system of digital regulation and censorship. The country has developed one of the most sophisticated technological and legal frameworks for information control, commonly known as the Great Firewall. This system has undergone substantial expansion and reinforcement, particularly during the leadership of Xi Jinping (Kaska & Tolpa, 2020).

Xi Jinping has highlighted the central role of cyberspace governance within China. During a study session in November, he emphasised the need to improve governance mechanisms to maintain a clean and orderly online environment. Cyberspace governance requires coordinated implementation under the Party's leadership, with particular emphasis on strengthening the supervision and guidance of online entities. The internet is regarded as important for ideological guidance and cultural transmission. Xi emphasised the importance of combating harmful or unethical online content, arguing that it can damage public interests and social morality. Authorities should take action against problematic content and the networks that support its production and distribution. Emerging technologies present both challenges and opportunities for cyberspace governance, with an emphasis on encouraging technological development while strengthening regulatory capacity (Xi, 2025).

In April 2025, China's Internet Governance Development Report, published by the CAC, revealed China's internet governance system in action. Addressing the domestic and international legal framework as well as strategies for promotion, it demonstrates the CAC's extensive authority over China's internet infrastructure and its role in digital and online affairs. The report emphasises that China's internet governance system is aligning with international practices while retaining national characteristics. It reiterates directives from July 2023, when Xi Jinping stated that the internet must be regulated, operated, and used in accordance with the law. The structure of the report delineates five core components of China's internet governance model: accelerating legislation, ensuring effective regulatory implementation, strengthening judicial enforcement, expanding education and propaganda related to internet governance policies, and promoting China's approach to internet governance beyond its borders. While the first three components correspond to the functions of legislative, executive, and

judicial institutions, the framework emphasises coordination among these bodies rather than the democratic principle of separation of powers (Mok, 2025).

China's data governance system is comprehensive and evolving. It promotes data sharing and utilisation while ensuring security, privacy, and compliance, particularly in healthcare and medical research. The system integrates policy guidance, legal regulations, institutional establishment, and ethical standards. Key institutions include the Big Data Bureau and related national data centres. These institutions coordinate the collection, management, and sharing of large datasets, underpinning China's aims to use data as a driver for technology and the economy. The legal framework is central to data governance in China, securing data privacy and security, regulating data ownership and sharing, and defining the responsibilities and rights of data processors. China's dual governance strategy combines legal and ethical oversight for scientific and big data sharing, particularly in healthcare. Regulations mandate ethical reviews for research involving human data. Transparency, fairness, risk control, and respect for individual rights are required. This ethical governance framework ensures that data sharing complies with legal requirements and upholds societal values and human dignity (Guan, 2025).

The government's approach to data governance is state-centred and treats data rights as a component of broader cyber sovereignty, blurring the lines between individual and state data control. Rights are defined and limited by the overarching principle of state sovereignty, conceptualised not as inherent to individuals but as granted and structured by the state, and function as communication rights. This framework reflects a divergence from Western individualist conceptions of human rights, emphasising that rights derive from the Party and state rather than from individuals. The result is a distinctive data governance model in which individual rights are subordinated to state interests (Liu, 2025).

Since 2015, data has been recognised as a production and strategic resource for both the digital economy and traditional industries. The legal framework establishes strict regulations on data classification, localisation, and the protection of critical data for national security. Personal data is protected, but the government retains unrestricted access to all data, prioritising national security. Large digital platforms are regulated as critical infrastructure and are expected to comply with data security rules while supporting economic development. Cross-border data flows face stringent controls to prevent security risks, with government access to data remaining largely unregulated. China's state-centric approach contrasts sharply with Western models, raising concerns about surveillance and global

data fragmentation. China's data governance prioritises state control and security, often at the expense of personal data protection, shaping both domestic policies and global digital governance (He, 2023).

Authoritarian regimes increasingly use data-driven technologies to control and suppress populations. China stands out for aggressively collecting and leveraging data to enforce social control and extend its model of governance. Its authoritarianism is profoundly data-centric, integrating advanced technologies that gather, fuse, and analyse data to monitor and manage society. This system builds on decades of surveillance infrastructure, beginning with the 1998 Golden Shield or, more commonly addressed, Great Firewall (Weber, 2025). China has evolved its tools from basic censorship equipment to sophisticated systems capable of keyword filtering and AI-enhanced facial recognition. Its digital governance model relies on several emerging technologies, notably AI-based surveillance systems, for enhanced state oversight. These include facial recognition networks and platforms that integrate pedestrian and vehicle data. The systems enable real-time monitoring and rapid law-enforcement responses while analysing large volumes of digital information. The government is also investing in neurotechnology and immersive systems, including brain–computer interfaces and VR (Virtual Reality), which could allow authorities to infer or potentially influence individuals' cognitive and emotional states, raising privacy and personal autonomy concerns. Existing legal frameworks facilitate state access to commercial neurotechnology data, and experiments with brainwave monitoring in police interrogations have been reported (Yang, 2022).

China is advancing quantum technologies, such as quantum computing and communications, which could compromise encryption standards, increasing the vulnerability of confidential communications. It is also exploring the international diffusion of these technologies through the BRICS framework. Furthermore, China has introduced a central bank digital currency that allows state authorities to monitor financial transactions and user behaviour. The global expansion of such digital currency systems could also affect international financial governance. These technologies form a data-driven authoritarian ecosystem. Data fusion allows authorities to create "digital twins" of cities and populations, facilitating precise governance and repression (Weber, 2023, p.4). China is exporting these technologies and influencing other states. Its data-centric authoritarianism represents a new frontier in state control, challenging privacy, free speech, and democratic agency. It is crucial for democracies and civil society to develop strategies to counter China’s approach (Weber, 2023).

South Korea has established itself as a leader in data protection legislation among Asian democracies. The PIPA covers both the public and private sectors and introduces a broad

understanding of personal data, ensuring protections extend beyond a strict government/private sector divide. South Korea's approach focuses on the nature of data processing activities rather than the status of the entity involved, applying obligations to all "personal information controllers," whether state or non-state actors (Duessel, 2020, p.18). This reflects a shift towards aligning domestic data protection frameworks with international norms, influenced by the EU's General Data Protection Regulation (GDPR). PIPA grants data subjects extensive rights, although some newer rights, such as data portability, are still evolving. Importantly, the country has established an independent data protection authority, tasked with enforcing the law and maintaining oversight of compliance (Marda, 2020).

This institutional design fosters trust in data governance and is crucial for securing international adequacy decisions, facilitating cross-border data flows that are essential to South Korea's participation in the global digital economy. South Korea's data protection regime is a prominent model in the Asian digital landscape, contributing to discussions on cybersecurity, international data governance, and digital trade. The country balances the need for state sovereignty in cyberspace with the economic imperatives of facilitating free and secure cross-border data flows. Within the context of Asia's evolving digital constitutionalism, South Korea represents a pragmatic and advanced model for the governance of personal data (Ray, 2020). South Korea balances economic growth, privacy rights, and platform regulation in its approach to data protection. It treats personal data as a valuable asset for economic development, particularly for domestic companies and platforms. The law restricts cross-border data transfers, requiring companies to notify users and designate local agents if they are foreign entities operating in South Korea. There are no strict data localisation mandates; regulations primarily aim to govern companies that handle personal data within its jurisdiction. This approach reflects a nuanced understanding of privacy, emphasising the importance of safeguarding individual interests while supporting innovation. The law also contemplates exceptions for government or public security purposes and specific categories of data use, such as employment. Overall, South Korea's data governance strategy is shaped by an intent to promote economic growth, control platform influence, and balance privacy concerns within its sociotechnical and geopolitical context (Grover et al., 2024).

South Korea's strategy for managing legal protections in the metaverse involves a hybrid model, combining strict data privacy regulations with a proactive virtual asset regulatory framework. Central to this approach is PIPA, which enforces rigorous obligations on data controllers. Violations under PIPA can result in significant sanctions, emphasising the country's commitment to protecting individuals' digital rights in the metaverse. Complementing this, South Korea has launched initiatives such as the

Korea Digital Bill of Rights, which underscores user-centric principles. This promotes a safe and trustworthy environment for users by embedding rights-based protections within digital services (Kandrina et al., 2025). South Korea is progressing towards a comprehensive regulatory framework for the oversight of cryptocurrency and digital assets. The government has passed legislation to protect consumers, combat money laundering, and ensure transparency in transactions, especially cross-border ones. This regulation aims to prevent market manipulation, insider trading, and fraud, which are critical for a stable virtual economy within the metaverse. South Korea's regulatory stance reflects an understanding that the security of digital assets and personal data are closely intertwined (Andersen et al., 2024).

The country's model seeks to ensure that the metaverse remains a protected space where individual rights are respected while supporting digital innovation and economic growth. The careful balance between strict data privacy, proactive virtual asset regulation, and fostering an environment conducive to technological advancement underscores South Korea's position as a pioneering digital nation in metaverse governance. Overall, South Korea's approach exemplifies a user-focused, comprehensive legal framework that actively addresses the protection of personal data and the regulation of virtual assets, emphasising public trust, safeguarding users, and enabling sustainable digital economic development within the metaverse (Kandrina et al., 2025). South Korea's approach to social media regulation is linked to its democratic evolution and unique political context. Since 1987, the country has made significant strides towards establishing a full democracy, characterised by free political speech, fair elections, and the rule of law. Several distinctive features influence how social media is regulated. North Korea remains an ongoing national threat, leading to limits on political rights, particularly regarding communist ideology. South Korea prohibits the communist party and restricts speech praising North Korea, with authorities removing content that promotes the regime (Yu, 2025).

Confucian cultural values also shape South Korea's political and media environment, favouring harmony and respect for hierarchy and elites, which constrains the political diversity seen in Western democracies. Decades of authoritarian rule have left deep social divisions and influenced media and speech regulation. While democratisation restored some freedoms, controls remain, especially concerning national security (Im, 2020). South Korea's regulatory framework is further influenced by tensions between traditional media oversight and the demands of the digital age. The establishment of the Korea Communications Commission (KCC) in 2008 aimed to adapt media regulation to contemporary digital realities, balancing democratic freedoms with concerns over security, defamation,

privacy, and social harms. South Korea's approach to social media regulation reflects its journey towards democracy, cultural factors, and national security considerations, seeking to protect democratic values while maintaining restrictions due to geopolitical and historical circumstances. This balancing act illustrates the country's ongoing efforts to reconcile democratic ideals with practical challenges in the digital era (Yu, 2025).

The governance of data and cyberspace in China and South Korea illustrates two different, yet overlapping, logics of *Digitalpolitik* and *Netpolitik*. China's model emphasises strong state sovereignty over cyberspace, where data governance, surveillance technologies, and regulatory frameworks are designed to preserve political stability, national security, and ideological control (He, 2023). Through systems such as the Great Firewall, extensive data regulation, and AI-enabled monitoring infrastructures, the state employs digital technologies as instruments of strategic power and social control, reflecting the core logic of *Digitalpolitik*, whereby digital infrastructures and data become tools of geopolitical and domestic state power. This arrangement exemplifies *Digitalpolitik*'s emphasis on state dominance over digital infrastructures and the use of technological ecosystems to consolidate geopolitical power.

By contrast, South Korea's governance approach places greater emphasis on regulatory frameworks, international data flows, and rights-based protections. Legislation such as PIPA establishes strong privacy safeguards and an independent data protection authority, while enabling cross-border data exchanges crucial for the digital economy (Marda, 2020). South Korea also seeks to regulate emerging digital environments, such as the metaverse and digital assets, while maintaining democratic accountability and fostering market innovation (Andersen et al., 2024). This reflects a closer alignment with *Netpolitik*, which focuses on governance norms, legal frameworks, and institutional coordination to shape the digital ecosystem. At the same time, South Korea's regulation of platforms, security-driven speech restrictions linked to geopolitical tensions, and economic use of data demonstrate elements of *Digitalpolitik*, as digital governance intersects with national security and economic strategy. Table 20 below shows the difference in approaches from both states and how they connect to the logics of *Digitalpolitik* and *Netpolitik*.

Table 20. Cyberspace and Data Governance in China and South Korea through the Logics of Digitalpolitik and Netpolitik

Dimension	China	South Korea	Digitalpolitik vs Netpolitik
Cyberspace governance	Controls information flows and asserts cyber sovereignty via the Great Firewall	Democratic oversight of digital platforms and social media balanced with security concerns	**China:** Digitalpolitik – cyberspace used as a tool of state control and sovereignty. **Korea:** Netpolitik – governance through regulatory institutions and rules.
Data governance	Data is a strategic national resource, strictly controlled and accessed by the state	Data protection under PIPA overseen by an independent authority	**China:** Digitalpolitik – data strengthens national power and security. **Korea:** Netpolitik – legal frameworks and rights shape the digital environment.
Cross-border data & digital economy	Control data exports to safeguard security and strategic interests	Support cross-border data flows for digital economy participation	**China:** Digitalpolitik – economic and security autonomy in data. **Korea:** Netpolitik – integration through international regulatory alignment.
Normative orientation	Individual data rights are secondary to state sovereignty and Party authority	Balances privacy, innovation and regulation within a democratic framework	**China:** Digitalpolitik – state interests dominate digital governance. **Korea:** Netpolitik – governance based on legal norms and institutional checks.

Source: The candidate based on the sources above mentioned.

The next subchapter examines how China and South Korea differ in their use of surveillance technologies, artificial intelligence, and international digital strategies. It explores how China integrates AI-driven surveillance and information control into its broader governance and security framework, while South Korea emphasises regulatory oversight, responsible AI governance, and international cooperation in emerging technologies.

4.2.2 Surveillance, AI and International strategy

China's SCS demonstrates how principles of information warfare are applied in domestic governance. The system is part of a broader digital governance architecture that collects data and employs laws and administrative measures to monitor, reward, or sanction individuals and firms. Discussions of China's information warfare often emphasise external influence operations, but a significant domestic dimension exists, whereby surveillance technologies and data-driven governance are used to shape behaviour, enforce conformity, and suppress dissent. Surveillance forms the operational backbone of information control. Technologies such as facial recognition and content filtering enable the government to manage information within its governance framework. The SCS uses data to measure trustworthiness, linking individuals' and firms' activities to political reliability and moral conformity. This integrates management, discipline, and control into a single digital architecture, blurring the boundaries between national security, social regulation, and information governance. China's surveillance ecosystem combines both physical and digital monitoring. This includes closed-circuit television networks, mandatory identification for mobile phones, online platforms, financial transactions, and biometric databases. Authorities can link online speech, consumption patterns, and social interactions to individuals, thereby enabling extensive control over information and behaviour (Awasthi, 2026).

AI is a key component of the Chinese government's control strategy, helping to monitor and manage populations both domestically and abroad. The CCP uses AI to automatically censor politically sensitive content, including text and images, embedding ideological conformity into the technology itself. AI is employed throughout the criminal justice process, from surveillance and policing to court hearings and prison monitoring, increasing efficiency but reducing transparency and enabling repression. The government encourages companies to develop and supply censorship tools to other firms, integrating political control into the digital economy. AI also targets minority populations, analysing specific languages and deploying advanced technologies in regions such as Xinjiang, thereby extending control beyond national borders. China's AI initiatives propagate party-approved messages, while predictive policing uses AI to prevent dissent and manage behaviour. Overall, AI provides the CCP with a more automated, pervasive, and adaptive system of control that shapes information, suppresses dissent, enforces repression, and projects influence internationally, posing significant human rights risks (Ryan et al., 2025).

China's global surveillance network, once focused solely on domestic monitoring, now targets Chinese citizens living abroad, challenging international norms of sovereignty and human rights. The world's largest surveillance system, with over 500 million cameras, enables continuous monitoring and

data-sharing across networks. China is further enhancing these capabilities through AI and cyber-operations, analysing social media and exploiting devices to identify potential dissidents abroad. The adoption of quantum computing and advanced AI models, such as the DeepSeek model, could further expand these monitoring capacities, undermine current encryption standards and increase the vulnerability of individuals outside China (Ankit, 2025).

The Chinese government's approach to foreign social media platforms reflects a deliberate security strategy, portraying services such as Facebook, Twitter, and Instagram as existential threats to national stability and sovereignty. By framing these platforms as conduits for foreign influence, dissent, or destabilising narratives, the government justifies extraordinary measures, including widespread censorship, legal restrictions, and technological barriers such as the Great Firewall. This security narrative is reinforced through state media and official discourse, encouraging citizens to perceive overseas platforms as threats to collective security and ideological unity. China restricts access to foreign social media and monitors users employing VPNs (Virtual Private Network), using AI and data tracking to identify and penalise subversive content. Legal frameworks, including cybersecurity laws, institutionalise these measures, obliging compliance from foreign platforms and consolidating state oversight. This strategy cultivates public support for strict regulation, presenting censorship and surveillance as protective rather than coercive. China's security of social media challenges norms of a free and open internet, attracting criticism from governments and organisations advocating digital freedom. The Chinese model provides a template for other authoritarian regimes, potentially contributing to a more fragmented and polarised global internet. By linking digital sovereignty to national security, China advances both domestic control and influence over international internet governance debates (Agustine, 2024).

China's social media ecosystem is largely dominated by domestic technology firms. This structural feature provides the CCP with a significant advantage in regulating online discourse. The government can implement censorship measures rapidly, reliably, and selectively because major platforms are locally controlled. This enables authorities to remove specific pieces of content without resorting to broad censorship, while targeted moderation undermines the appearance of a digital public sphere. In other countries, multinational technology companies dominate the social media landscape, and governments lack the authority or technical access to directly remove content, often having to submit requests to platform operators, which can take days or weeks. Beyond censorship, the CCP seeks to shape public opinion through direct participation in the online information environment. Rather

than disguising state-produced content, authorities frequently use accounts that openly indicate their affiliation with government institutions (Pan, 2022).

The CCP requires local governments and administrative agencies at various levels to maintain official social media accounts, enabling direct communication with citizens. This effort spans both established and emerging platforms. For example, Douyin facilitates rapid content creation and distribution through vertically oriented, full-screen videos optimised for mobile consumption. Unlike traditional social media platforms that emphasise networks of friends or followers, Douyin's algorithmic feed provides content to users even before they follow any accounts, meaning visibility is driven more by recommendation systems than by social connections. Similarly, live-streaming platforms such as Kuaishou allow users to broadcast content in real time to large audiences while interacting with viewers during the broadcast. These technological features create additional opportunities for state-affiliated actors to disseminate information widely and shape online discourse (Lu & Pan, 2022).

Chinese cybersecurity firms enhance China's global operations, visibility, and capabilities. By expanding their international customer base, these firms gain access to more endpoints and telemetry, providing insight into cyber-attacks worldwide and strengthening China's cyber defences. The Ministry of Industry and Information Technology's platform collects vulnerability reports, further improving national understanding. Chinese firms also allow security services to operate on their protected networks, enabling China's offensive cyber teams to access foreign networks more readily, reducing the need to evade defences. Partnerships with foreign CERTs (Computer Emergency Response Team) involve intelligence-sharing, further boosting China's cyber-intelligence efforts. These companies supply technologies to authoritarian regimes, strengthening China's geopolitical influence. By providing these tools, China supports allied governments in maintaining political control and securing its strategic interests abroad. Chinese cybersecurity firms thus serve as critical enablers of China's cyber strategy, improving defensive visibility, facilitating offensive operations, sharing intelligence, and supporting authoritarian partners. This multifaceted role significantly advances China's global cyber influence (Cary, 2023).

The DSR is shaping global influence through key digital infrastructure projects involving AI, 5G, and telecommunications systems. By providing affordable digital infrastructure and financing through a partnership between the Chinese state and major tech companies such as Huawei, Tencent, and Alibaba, China is embedding its technology deeply into developing countries' digital ecosystems, amplifying Beijing's influence. This model differs from Western approaches by centralising decision-

making and aligning corporate strategies with national objectives, allowing Chinese firms to offer competitive pricing and financing options that appeal to developing nations (Wiater, 2025).

While this facilitates rapid modernisation and economic development, it also increases dependence on Chinese technology, data centres, and financing, raising concerns about digital sovereignty, debt, and potential limitations on alternative partnerships. Although digital infrastructure such as 5G networks forms the backbone of the DSR, AI provides the analytical and operational capacity necessary to fully utilise these systems across borders. It facilitates economic modernisation, enhanced digital services, and technological integration among participating countries, supporting China's expanding digital infrastructure across regions such as Eurasia and Africa. The rapid growth and global attention of DeepSeek, a leading Chinese AI model, demonstrate China's growing competitiveness in AI. DeepSeek is an attractive option for countries with limited resources to develop advanced AI technologies independently, owing to its efficient architecture and open-source design (Au & Chen, 2025).

This soft power strategy, which leverages attraction through technology and infrastructure rather than coercion, positions China as a model of digital modernisation while subtly expanding its geopolitical leverage and reinforcing domestic priorities abroad. While the DSR undoubtedly cultivates goodwill by providing essential digital infrastructure, critics have raised concerns that it may lead to instances of digital coercion. Increasing reliance on Chinese technology could restrict partner nations' digital sovereignty and their freedom to select alternative suppliers, complicating the balance between benefiting from and being dependent on China's global soft power (Wiater, 2025).

South Korea is transitioning from a traditional e-government model to a digital platform government approach that prioritises openness, connectivity, and collaboration with citizens and businesses. The strategy focuses on high-quality, interoperable open data, supported by robust legal and institutional frameworks to facilitate AI adoption in the public sector. The government relies on private-sector innovations, particularly cloud infrastructure and shared generative AI platforms, to deliver integrated, personalised, and proactive public services. The approach also encourages cross-agency data integration and public–private cooperation, enabling AI-driven applications in areas such as public safety, health, welfare, and transportation. Recent initiatives have applied AI to large-scale data analysis in citizen-focused sectors, aiming to improve service delivery and expand the practical use of AI across government operations (Thian, 2025).

South Korea's AI Basic Act, which came into force on 22 January 2026, establishes a comprehensive regulatory framework for artificial intelligence, analogous to the EU Artificial Intelligence Act. It introduces transparency and governance requirements for high-risk AI systems, delegating the development of detailed technical rules to the MSIT. The AI Basic Act imposes specific obligations on generative AI and its high impact in critical sectors, as well as high-performance AI systems exceeding a defined computational threshold. It includes transparency measures, user notification, explainability requirements, and impact assessments. Draft enforcement decrees define high-performance AI as systems trained with at least 10 floating-point operations (FLOPs), requiring risk-management and safety measures. The Act also applies extraterritorially to AI systems affecting the South Korean market, obliging foreign companies to appoint local representatives for regulatory communications. Overall, the legislation strengthens national AI governance and supports research, infrastructure, and development (Cooley, 2026).

The AI Basic Act ensures ethical AI practices and transparency. AI businesses using high-impact or generative AI must inform users in advance about AI involvement, with various notification methods permitted to facilitate compliance. For AI-generated outputs, clear and age-appropriate labelling is required to help users recognise AI involvement. For other AI-generated content, both visible labels and digital identifiers such as watermarks are allowed, with notifications deliverable via pop-up messages or user interface features. The Act also establishes obligations relating to AI ethics, verification and certification, transparency, safety, and the management of high-impact AI systems, further detailed in the Enforcement Decree and corresponding guidelines. The MSIT provides detailed guidance and an AI Basic Act Support Desk to assist compliance and address concerns. Watermarks on AI-generated content are emphasised to prevent misuse. Collectively, these measures promote ethical AI use and transparency, contributing to a safe and trustworthy AI ecosystem in South Korea (Ministry of Science and ICT, 2025b).

The Korean government's comprehensive approach to supporting AI development includes the AI Basic Act, which aims to enhance national competitiveness and public trust in AI technologies. AI innovation is a key initiative within the Five-Year Policy Blueprint, facilitated through public-private partnerships. Strategic collaborations are central to Korea's AI ambitions. Partnerships between Samsung, SK, and OpenAI seek to expand AI infrastructure globally, positioning Korean companies as leaders in frontier AI development. Infrastructure development remains a government priority, with the MSIT signing memoranda with OpenAI to establish AI data centres across South Korea, including

regions outside the Seoul Metropolitan Area, to promote balanced growth and job creation. The government's dual-track AI strategy both advances an independent domestic ecosystem and encourages global partnerships. This balance of sovereignty and innovation is complemented by modernised regulation and expanded public data access. The overarching goal is to foster innovation within a predictable and adaptive legal environment that is also safe and trusted. Sector-specific initiatives, such as Dr. Answer 3.0 in healthcare, address challenges including an ageing population and strain on the healthcare system. National strategies are coordinated through policy planning to build a robust ecosystem capable of overcoming challenges such as fragmented data governance. With the appropriate combination of legislation, investment, partnerships, infrastructure, strategy, and initiatives, South Korea is poised to become a global leader in AI (OpenAI, 2025).

At the APEC Leaders' Summit in Gyeongju on October 31st and November 1st, Lee Jae-myung utilised the multilateral forum to advance a pragmatic foreign policy linking trade strategy with technological leadership. The summit produced cross-regional commitments under the APEC Artificial Intelligence Initiative, highlighting South Korea's growing role in shaping international AI governance. Domestically, the government is promoting a sovereign AI strategy and supporting national companies and workforce development to strengthen AI innovation capacity. Internationally, South Korea has positioned itself as a leader in responsible AI through participation in various forums, including the Summit for Democracy, the AI Seoul Summit, and the Responsible AI in the Military Domain Summit. Outcomes from the summit included agreements on semiconductor supply chains, AI innovation frameworks, and cooperation on low-carbon energy and digital technologies, reinforcing South Korea's role in shaping regional technology governance and economic resilience in the Indo-Pacific. The long-term impact of these initiatives will depend on the effective implementation of bilateral and multilateral trade and technology agreements (Orta, 2025).

South Korea's smart city development emphasises aligning policies and investments with citizens' preferences and needs, improving quality of life and sustainability. Researchers and policymakers are re-evaluating top-down initiatives. The citizen-centric smart city strategy invests in accordance with citizen benefits and optimises government resources through a bottom-up approach, incorporating collaboration with local communities. The aim is to build inclusive smart cities with active engagement from residents. Citizen preferences are integrated into planning and resource allocation to bridge the gap between projects and actual demands. This ensures that smart city developments enhance quality of life, sustainability, and competitiveness (Kim et al., 2025).

South Korea's smart city policies have evolved from a technology-centric to a citizen-centric focus. Early initiatives, such as the U-City project, emphasised integrating advanced ICT infrastructure into urban environments. However, these technology-driven strategies were limited in embodying core social values and fostering sustainable urban development. The focus has shifted towards smart cities that prioritise residents' quality of life and active participation. Civic engagement is central to this approach, residents' real needs are identified through active participation, contributing to more inclusive urban services. This fosters trust and ensures smart city projects meet public expectations. South Korea's smart city policies advocate a phased approach to goal-setting. While infrastructure development is expected to be completed by 2030, full integration of smart city services into citizens' daily lives is projected for around 2035. This shift involves moving from supplier-driven to citizen-centred models, prioritising citizen satisfaction and empowerment alongside technological innovation. South Korea's citizen-centric smart city strategy combines technology and human values, focusing on sustainable urban development, public participation, and improving quality of life. The objective is to create socially inclusive, technologically advanced, and responsive smart cities (Shin et al., 2025).

South Korea prioritises national control and strategic independence over global integration in its approach to digital sovereignty. Home bias, the preference for domestic platforms and software, is reinforced by policies promoting local tech companies and standards. This has resulted in a concentrated digital ecosystem dominated by domestic firms such as Naver and Kakao, which are closely integrated with government services. This strategic choice reflects a balance between national control and cultural sovereignty versus openness to global platforms (Merril, 2025). More recently, however, this approach has evolved. After years of restrictions, South Korea approved Google's export of national mapping data, subject to strict conditions, including the exclusion of certain information such as contour lines. Export was approved only after processing on domestic servers and authorisation by the government, with satellite images of military and sensitive sites deliberately blurred. Previously, similar requests from foreign technology firms had been rejected due to national security concerns, particularly the risk of exploitation by North Korea, and to protect domestic mapping platforms operated by Naver and Kakao. This decision reflects an effort to improve navigation services for international users while maintaining control over sensitive geographic information (Kim, 2026).

The Chinese approach is clearly aligned with the logic of *Digitalpolitik*, in which digital technologies, data infrastructures, and information systems are strategically employed as instruments of political authority, national security, and geopolitical influence. Domestically, systems such as the

SCS integrate surveillance technologies, data collection, and administrative sanctions into a unified digital governance architecture that monitors behaviour and enforces political and social conformity (Awasthi, 2026). The integration of AI into these systems serves to automate the enforcement of ideological standards and social management, thereby further reinforcing the model. These mechanisms are complemented by strict control of information flows through systems such as the Great Firewall, where foreign platforms are securitised as threats to national stability and sovereignty (Agustine, 2024). At the international level, China extends this *Digitalpolitik* logic through initiatives such as the DSR, exporting digital infrastructure, surveillance technologies, and AI capabilities to partner countries. This approach embeds Chinese standards and expands geopolitical influence through technological ecosystems.

In contrast, South Korea's digital governance model is more closely aligned with *Netpolitik*, emphasising regulatory frameworks, institutional governance, and the development of digital ecosystems. The country's transition to a digital platform government prioritises open data, interoperability, and cooperation with the private sector to deliver public services through AI-enabled platforms (Thian, 2025). Regulatory initiatives, such as the AI Basic Act, establish transparency, accountability, and safety requirements for high-impact AI systems, while supporting innovation and competitiveness (Cooley, 2026). South Korea's smart city policies focus on citizen participation, public trust, and quality of life in the deployment of digital technologies (Shin et al., 2025). At the same time, elements of *Digitalpolitik* are evident in efforts to secure technological sovereignty, promote domestic platforms such as Naver and Kakao, and protect sensitive national data from external actors. This is exemplified by the government's cautious approval of national mapping data exports to Google, granted only under strict conditions. The decision illustrates how South Korea seeks to balance openness to global digital services with continued state oversight of strategically sensitive digital information. Table 21 below summarises the difference in both approaches and shows the hybrid nature of the South Korean model, along with the solid logic of China’s Digitalpolitik approach.

Table 21. Digital Governance Approaches of China and South Korea through the Logics of Digitalpolitik and Netpolitik

Dimension	China	South Korea	Digitalpolitik vs Netpolitik
Domestic digital governance	The SCS uses surveillance and data collection to enforce conformity	The digital government uses data, AI and cooperation to improve services and governance	**China** → Digitalpolitik (digital systems used for state control). **South Korea** → Netpolitik (governance through digital platforms and institutions).
AI governance	AI is used for censorship, predictive policing and ideological monitoring	The AI Basic Act establishes requirements for AI systems	**China** → Digitalpolitik (technology strengthens political authority). **South Korea** → Netpolitik (rule-based regulation of technology).
Information control & social media	State platforms and censorship infrastructure regulate and securitise online discourse	Digital platform regulation balances freedom with security concerns and oversight	**China** → Digitalpolitik (control of information space). **South Korea** → Netpolitik (regulated digital public sphere).
Global digital influence	The DSR is a project to export Chinese technology and influence	Shapes global AI standards through forums and partnerships	**China** → Digitalpolitik (technology as geopolitical leverage). **South Korea** → Netpolitik (norm-setting and cooperation).
Digital sovereignty	Surveillance prioritises state authority over data and information	Promotion of domestic platforms and conditional sharing of data show efforts to protect digital assets	**China** → Digitalpolitik (state-centric sovereignty). **South Korea** → Hybrid (Netpolitik governance with Digitalpolitik sovereignty measures).

Source: The candidate based on the sources above mentioned.

The comparison drawn between China and South Korea reveals two distinct yet partially converging models of digital governance, both of which have been shaped by strategic imperatives of

security, economic competitiveness, and technological influence. China's system is centralised, state-centric, and integrates legal frameworks, surveillance technologies, and data governance into a model of control. Digital infrastructures are instruments of political authority and geopolitical power (Liu, 2025). South Korea's approach is hybrid, combining regulatory institutions, rights-based data protection, and international cooperation with targeted measures to secure technology and national resilience. Both countries demonstrate elements of *Digitalpolitik* through their emphasis on security, innovation and control of digital ecosystems. South Korea is more aligned with *Netpolitik* through commitment to legal norms, governance and global standard-setting. These approaches illustrate how differing political systems and frameworks shape cyberspace governance, showing growing global digital order fragmentation and the existence of competing digital sovereignty and international models.

Conclusion

Drawing on the dichotomy between the theoretical frameworks of *Netpolitik* and *Digitalpolitik*, this dissertation has attempted to answer the research question previously stated: How do China and South Korea navigate the tensions between openness and control in cyberspace governance within the frameworks of *Netpolitik* and *Digitalpolitik*? To clarify the research question we began the dissertation by defining the concepts of cyberspace, cyber sovereignty, internet fragmentation, data governance and AI, focusing on their definitions and overarching importance to understand both countries' models. By applying a dual theoretical lens, the study progressively mapped the normative and practical dimensions of digital governance policies in both countries, thereby uncovering the underlying dynamics of their cyberspace security models and international digital strategies.

This study has conducted an extensive analysis of the national and international approaches to cyberspace governance, cybersecurity, AI, and digital infrastructure, with a view to highlighting the broader geopolitical dynamics that are shaping the contemporary digital landscape. The digital governance models of China and South Korea reflect distinct yet interconnected approaches that have been shaped by their unique political systems, legal frameworks and strategic priorities. It is evident that both countries recognise digital technologies, including but not limited to cybersecurity, AI, and digital infrastructure, as being central to national power, economic competitiveness, and geopolitical influence. Nevertheless, the strategies employed by these countries are underpinned by divergent logics of *Digitalpolitik* and *Netpolitik*, giving rise to disparate governance paradigms.

The first major conclusion of the dissertation pertains to the characterisation of China's cyberspace governance model as a highly centralised, state-centric system firmly rooted in the logic of *Digitalpolitik*. China's approach is marked by a comprehensive legal and institutional infrastructure designed to assert and maintain cyber sovereignty, which is a cornerstone of its *Digitalpolitik* paradigm. Legislation such as the Cybersecurity Law, Data Security Law, and Personal Information Protection Law underscores the prioritisation of state authority over data flows, digital infrastructures, and information dissemination. The concept of authoritarian informationalism integrates surveillance technologies, AI-driven monitoring, and the Great Firewall censorship system to exercise comprehensive control over digital narratives and social behaviour. This enables the maintenance of regime stability and the reinforcement of political legitimacy. The deployment of advanced, AI-driven surveillance technologies forms a critical component of this governance model. Surveillance here is not merely a tool of security, but also an instrument of information control and regime legitimisation. In the contemporary geopolitical landscape, characterised by a heightened focus on security concerns, initiatives such as the DSR have emerged as significant factors. This initiative serves to embed Chinese standards within the global digital ecosystem, thereby shaping the international technological landscape. The prioritisation of regime security and sovereignty gives rise to a governance paradigm that perceives cyberspace as a contested terrain, thus necessitating strict control to mitigate internal vulnerabilities and external threats, particularly in the context of escalating US-China technological rivalry. The Chinese model contrasts sharply with more decentralised and cooperative paradigms, embodying the fundamental principles of *Digitalpolitik*, as outlined in the dissertation's theoretical framework.

The second major conclusion of the dissertation focuses on South Korea's digital governance model, which represents a hybrid approach, combining elements of both *Netpolitik* and *Digitalpolitik*. This model is characterised by regulatory flexibility, rights-based data governance, and active public-private collaboration within a democratic political framework. South Korea's approach emphasises balancing technological innovation and economic competitiveness with the protection of digital rights and privacy, reflecting principles aligned with *Netpolitik*. The government encourages multilateral engagement and aligns closely with Western normative frameworks, particularly those emphasising democratic oversight and user rights. At the national level, South Korea's legal framework supports a rights-based approach to data governance that prioritises individual privacy and data protection. Furthermore, South Korea actively participates in international forums and alliances, shaping global norms around AI, governance, and cybersecurity in ways consistent with its hybrid model. It seeks to promote interoperability, cooperation and standards that reflect democratic principles, while also

reinforcing digital sovereignty and national security through domestic platform development and strategic technological investments. Despite these liberal-democratic traits, South Korea also exhibits nuanced characteristics of *Digitalpolitik*, such as emphasising state security and strategic governance of digital technologies. This blend creates a distinctive model that navigates between state-centric control and networked, pluralistic governance, reflecting the complexities of balancing national sovereignty with global digital cooperation. South Korea's dual approach reflects a unique political context, legal frameworks, and strategic priorities, illustrating an alternative paradigm in cyberspace governance that contributes to the broader phenomenon of global digital order fragmentation.

Moreover, we can also conclude that a fragmented global digital order has emerged, featuring competing ideas of sovereignty, governance, and technology. Previous notions of a borderless, open internet are now challenged by nation strategies focusing on digital sovereignty and control. China's model shows this fragmentation with its authoritarian approach, where data, infrastructure and information are controlled to secure regime stability and influence. On the one hand, there is increasing state-driven emphasis on asserting sovereign control over digital ecosystems to protect national security, cultural identity, and political authority. On the other hand, there is the normatively informed aspiration for openness, multilateral cooperation, participatory governance, and rights protection, increasingly embraced, although with caveats, by states like South Korea. The differences between China and South Korea's models reflect their underlying political systems and strategic priorities. The present research also underscores the increasing centrality of AI and data governance as strategic domains within state digital governance. Both countries invest heavily in AI research and deployment, though their governance logics differ. The findings demonstrate the increasing intricacy of digital sovereignty as a contested and multifaceted concept. The dynamics of competition and cooperation between states, such as China and South Korea, contribute to the fragmentation and pluralisation of the global digital ecosystem. It is imperative for policymakers, scholars and practitioners seeking to navigate the dilemmas of power, ethics and rights in international digital policy to understand these diverse governance models and their underpinning theoretical frameworks.

In conclusion, this dissertation has attempted to highlight potential research opportunities in the evolving cyberspace governance, in which the existing literature remains relatively limited, particularly with regard to Asian governance models, as evidenced in the case of South Korea. Moreover, the emergence of new technologies, most notably AI, introduces additional layers of complexity that have yet to be thoroughly explored. In particular, the regulatory and ethical challenges posed by AI and

automated systems require detailed assessment to understand how different political regimes might approach their governance and implications. Another critical domain for future research is the evolution of global governance mechanisms for cyberspace. As it becomes increasingly fragmented due to competing national models, exploring how international institutions, multilateral forums, and standard-setting bodies can adapt or respond to this pluralisation is essential. Analysing other countries' strategies could reveal how political, cultural, and regional contexts influence the balance between *Netpolitik* and *Digitalpolitik*. This would enhance our understanding of how states navigate the sometimes conflicting demands of democracy, innovation, sovereignty, and cybersecurity in their digital policymaking. Methodological innovation is necessary to keep pace with the rapid and complex evolution of digital governance. Future studies should explore new approaches including big data analysis, network mapping, and interdisciplinary frameworks.

Bibliography

Primary Sources

Act on the Promotion of Smart City Development and Industry (2026). Act No. 21381, Feb. 19 (S. Kor.). [online] National Laws and Regulations Information Center. Available at: https://www.law.go.kr/lsInfoP.do?lsId=010730#0000

Cyberspace Administration of China (2023). 2022 internet ecological governance situation. [online] Available at: http://www.cac.gov.cn/

European External Action Service (EEAS) (November, 2024). Security and defence partnership between the European Union and the Republic of Korea. [online] Available at: https://www.eeas.europa.eu/eeas/security-and-defence-partnership-between-european-union-and-republic-korea_en

International Trade Administration (December, 2023). South Korea – Information and communication technology. U.S. Department of Commerce. [online] Available at: https://www.trade.gov/country-commercial-guides/south-korea-information-and-communication-technology

OECD (2023). Share of businesses making e-commerce sales that sell across borders. Going Digital Toolkit. [online] Available at: https://goingdigital.oecd.org/en/indicator/72

OECD (October, 2025). Digital Government Review of Korea: Harnessing digital and data to transform government. OECD Digital Government Studies. [online] Available at: https://doi.org/10.1787/9defc197-en

Korea Information Society Development Institute (2021). 2022 ICT Industry Outlook of Korea. [online] Available at: https://mediasvr.egentouch.com/egentouch.media/apiFile.do?action=view&SCHOOL_ID=1007002&URL_KEY=22ed8f99-548d-424c-a1de-7acfdfb1944b

Korea Internet & Security Agency (2024). National cybersecurity white paper. [online] Available at: https://www.scribd.com/document/806005024/KISA-2024-National-Cybersecurity-White-Paper

Korea Internet & Security Agency (2026). Korea Internet & Security Agency (Business – Korea Internet Security). [online] Available at: https://www.kisa.or.kr/EN/101

Lee Jae-myung (September, 2025). Lee vows to develop AI into next-generation growth engine. Yonhap News Agency. [online] Available at: https://en.yna.co.kr/view/AEN20250908007800315

Ministry of Foreign Affairs People's Republic of China (March, 2015). Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road. [online] Available at: https://www.mfa.gov.cn/eng/zy/jj/2015zt/xjpcxbayzlt2015nnh/202406/t20240606_11381659.html

Ministry of Foreign Affairs People's Republic of China (October, 2023). Global AI Governance Initiative. [online] Available at: https://www.mfa.gov.cn/eng/zy/gb/202405/t20240531_11367503.html

Ministry of Foreign Affairs People's Republic of China (July, 2025). Global AI Governance Action Plan. [online] Available at: https://www.fmprc.gov.cn/mfa_eng/xw/zyxw/202507/t20250729_11679232.html

Ministry of Foreign Affairs, Republic of Korea (July, 2025). The Government of the Republic of Korea announces its position on application of international law in cyberspace. [online] Available at: https://www.mofa.go.kr/eng/brd/m_5674/view.do?seq=321145

Ministry of the Interior and Safety (2025). Digital Government Innovation. [online] Available at: https://www.mois.go.kr/eng/sub/a03/digitalGovInnovation/screen.do

Ministry of Land, Infrastructure and Transport (2023). Smart City Pilot Projects in Sejong and Busan. Smart City Korea. [online] Available at: https://smartcity.go.kr/en/

Ministry of Land, Infrastructure and Transport (December, 2021). MOLIT picks 13 cities as beneficiaries of smart service projects. [online] Available at: https://www.molit.go.kr/english/USR/BORD0201/m_28286/DTL.jsp?idx=3003&mode=view

Ministry of Legislation (February, 2026). Korean Smart City Act. [online] Available at: https://www.law.go.kr/lsInfoP.do?lsId=010730#0000

Ministry of Science and ICT (October, 2025a). Government announces comprehensive information security measures. [online] Available at: https://english.msit.go.kr/eng/bbs/view.do?sCode=eng&nttSeqNo=1181&bbsSeqNo=42&mId=4&mPid=2

Ministry of Science and ICT of the Republic of Korea (November, 2025b). Government policy on AI and digital technologies. [online] Available at: https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mPid=2&mId=4&bbsSeqNo=42&nttSeqNo=1058

National Intelligence Service (2026). National Cyber Security Center. [online] Available at: https://eng.nis.go.kr/EID/1_7_1.do

OpenAI (2025). *AI in South Korea—OpenAI's economic blueprint*. [online] Available at: https://cdn.openai.com/global-affairs/f9361fe7-e452-4c78-94dc-e6946c73c858/openai-south-korea-economic-blueprint-october-2025.pdf

Permanent Mission of the People's Republic of China to the United Nations (July, 2025). Statement on international cooperation in artificial intelligence governance. [online] Available at: https://un.china-mission.gov.cn/eng/zgyw/202507/t20250729_11679232.htm

Seoul Metropolitan Government (2025). Smart Public Safety. [online] Available at: https://english.seoul.go.kr/seoul-policy-archive/smart-public-safety/

Smart City Korea (2024). Towards a sustainable future: K-Smart City. [online] Available at: https://smartcity.go.kr/wp-content/uploads/2024/10/Towards-a-Sustainable-Future-K-Smart-City_EN.pdf

The State Council Information Office of the People's Republic of China (January, 2017). China's policies on Asia-Pacific security cooperation (White paper). [online] Available at: https://english.www.gov.cn/archive/white_paper/2017/01/11/content_281475539078636.htm

The State Council of the People's Republic of China (August, 2021). Regulations on the security protection of critical information infrastructure. [online] Available at:

https://english.www.gov.cn/policies/latestreleases/202108/17/content_WS611b8062c6d0df57f98de907.html

The State Council Information Office of the People's Republic of China (April, 2016). Press conference on achievements in building China's strength in cyberspace in the new era. [online] Available at: http://www.scio.gov.cn/news_0/202209/t20220921_414321.html

The State Council of the People's Republic of China (October, 2022). Report to the 20th National Congress of the Communist Party of China. [online] Available at: https://english.www.gov.cn/news/topnews/202210/25/content_WS6357df20c6d0a757729e1bfc.html

The State Council Information Office of the People's Republic of China (March, 2023a). Press conference on the development of cyberspace in the new era. [online] Available at: http://www.scio.gov.cn/zfbps/ndhf/49551/202303/t20230320_709284.html

The State Council Information Office of the People's Republic of China (July, 2023b). Xi stresses advancing high-quality development of cybersecurity, informatization work. [online] Available at: https://english.www.gov.cn/news/202307/15/content_WS64b28bf2c6d0868f4e8ddcea.html

United Nations in China (2026). Our work on the Sustainable Development Goals in China.. [online] Available at: https://china.un.org/en/sdgs

United Nations Office of Counter-Terrorism (2023). Cybersecurity and new technologies programme. United Nations. [online] Available at: https://www.un.org/counterterrorism/en/cct/programme-projects/cybersecurity

Xi, J. (February, 2014). Build our country from a large cyber country into a strong cyber country. Xinhua News Agency. [online] Available at: http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm

Xi, J. (April, 2016). Speech at the work conference for cybersecurity and informatization. China Copyright and Media. [online] Available at: https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/

Xi, J. (May, 2017a). Work Together to Build the Silk Road Economic Belt and The 21st Century Maritime Silk Road. Belt and Road Forum for International Cooperation. [online] Available at: https://2017.beltandroadforum.org/english/n100/2018/0306/c25-1038.html

Xi, J. (August, 2017b). Xi delivers speech at the Brazilian National Congress. ChinaDaily. [online] Available at: https://www.chinadaily.com.cn/world/2014xibricssummit/2014-07/17/content_17820460.htm

Xi, J. (August, 2018). Xi stresses ideological work to keep the Party's leadership firm. Xinhua News Agency. [online] Available at: http://www.xinhuanet.com/english/2018-08/22/c_137410956.htm

Xi, J. (December 2025). Xi: Strengthen cyberspace governance framework. ChinaDaily. [online] Available at: https://www.chinadaily.com.cn/a/202512/01/WS692c6f2ca310d6866eb2c21e.html

Xinhua Net (2014). Address of President Xi Jinping in the Brazil Congress. [online] Available at: http://news.xinhuanet.com/world/2014

Secondary Sources

Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, 49(2), 187–212. Doi: 10.1080/03085147.2019.1690275

Aitel, D., d'Antoine, S., DeSombre, W., Garcia-Camargo, I., Roos, I., Rostow, N., Smith, J., Strongwater, A., Wagner, A. and Work, J.D. (2024). China's cyber operations: The rising threat to American security. *Margin Research*. [online] Available at: https://margin.re/chinas-cyber-operations-the-rising-threat-to-american-security/

Agustine, M.P.D. (2024). A review of China's restrictions and surveillance of foreign social media platforms. *Modern Diplomacy*. [online] Available at: https://moderndiplomacy.eu/2024/11/07/a-review-of-chinas-restrictions-and-surveillance-of-foreign-social-media-platforms/

Akhand, A. (2026). South Korea's AI revolution is forcing a US–China balancing act. *East Asia Forum*. [online] Available at: https://eastasiaforum.org/2026/01/17/south-koreas-ai-revolution-is-forcing-a-us-china-balancing-act/

Akhtar, N. and Iqbal, A.R. (2025). Cyber Sovereignty: National Security in the Digital Age. *Lahore Institute for Research and Analysis Journal, 3,* pp. 87–104.

Andersen, K.N., Lee, J. and Kim, S. (2024). MetaVerse+ in South Korea and Denmark: Snapshots from two leading digital nations. In: *Proceedings of the 25th Annual International Conference on Digital Government Research*, pp.827–831. Doi: 10.1145/3657054.3657149

Ankit, K. (2025). China's surveillance state watches everyone, everywhere. *The Irrawaddy*. [online] Available at: https://www.irrawaddy.com/opinion/guest-column/chinas-surveillance-state-watches-everyone-everywhere.html

Assad, D. (2025). China's Digital Silk Road and cyber diplomacy: Building influence in the cyber sphere. *Contemporary Journal of Social Science Review*, 3(2), 528–537.

Atkinson, R. D. (2021). A U.S. grand strategy for the global digital economy. *Social Science Research Network*. Available at: https://ssrn.com/abstract=3773652.

Au, A. and Chen, F.F. (2025). China expands AI globally through the Digital Silk Road. *EABC*. Doi:10.59425/eabc.1744365600

Awasthi, S. (2026). China's social credit system and information control regime. *Observer Research Foundation*. [online] Available at: https://www.orfonline.org/english/expert-speak/china-s-social-credit-system-and-information-control-regime

Ayeola, F. (2025). AI-Driven Anomaly Detection and Data Governance: Securing Financial Systems, Cybersecurity Networks, and Regulatory Compliance in Multicultural Digital Ecosystems. *SSRN*. Doi:10.2139/ssrn.5439102

Baker McKenzie (2026). Key data and cybersecurity laws: South Korea. *Global Data and Cyber Handbook Lite*. [online] Available at: https://resourcehub.bakermckenzie.com/pl-pl/resources/global-data-and-cyber-handbook-lite/asia-pacific/south-korea/topics/key-data-and-cybersecurity-laws

Bartlett, B. G. (2018). Institutional determinants of cybersecurity promotion policies: Lessons from Japan, the U.S., and South Korea. [online] Available at: https://escholarship.org/uc/item/02f4879m

Bartley, A. S. R. (2025). China's AI development trajectory: From fragmented authoritarianism to securitisation. *Journal of East Asia Security*, 1(3), 55–61. Doi: 10.53300/001c.144339

Bokhari, S. A. A., & Myeong, S. (2022). Artificial intelligence-based technological-oriented knowledge management, innovation, and e-service delivery in smart cities: Moderating role of e-governance. *Applied Sciences*, 12(17), Article 8732. Doi: 10.3390/app12178732

Bokhari, S. A. A., & Myeong, S. (2023). The impact of AI applications on smart decision-making in smart cities as mediated by the Internet of Things and smart governance. *IEEE Access*, 11, 120827–120844. Doi:10.1109/ACCESS.2023.3327174

Bollier, D. (2003). The rise of Netpolitik: How the internet is changing international politics and diplomacy. The Aspen Institute. [online] Available at: https://www.bollier.org/pdf/Netpolitik.pdf

Busroh, F. F., Khairo, F., Niravita, A., & Nunna, B. P. (2025). Digital transformation with the impact of AI in government decision making. *Journal of Law and Legal Reform*, 6(4), 1839–1874. Doi: 10.15294/jllr.v6i4.30339

Cabestan, J.-P. (2020). The state and digital society in China: Big Brother Xi is watching you! *Issues & Studies*, 56(1), 2040003. Doi: 10.1142/S1013251120400032

Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). *Smart Cities*, 5(3), 1129–1150. Doi: 10.3390/smartcities5030057

Cary, D. (2023). Community watch: China's vision for the future of the internet. *Atlantic Council*. [online] Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/

Chan, K., Smith, G., Goodrich, J., et al. (2025). Full Stack: China's Evolving Industrial Policy for AI. RAND Corporation. [online] Available at: https://www.rand.org/pubs/perspectives/PEA4012-1.html

Chang, Y. (2023). China beyond China: Establishing a digital order with Chinese characteristics. *Politics & Policy*, 51(2). Doi: 10.1111/polp.12524

Chaskes, W. (2022). The three laws: The Chinese Communist Party throws down the data regulation gauntlet. Washington and Lee University School of Law. [online] Available at: https://scholarlycommons.law.wlu.edu/wlulr/vol79/iss3/10/

Chen, D., & Zhan, J. V. (2025). When does surveillance trigger resistance? *Journal of Chinese Political Science*. Doi: 10.1007/s11366-025-09918-5

Chen, J., & Sun, J. (2021). Understanding the Chinese data security law. *International Cybersecurity Law Review*, 2. Doi:10.1365/s43439-021-00038-3

Chen, Y., & Cheung, A. S. Y. (2017). The transparent self under big data profiling. *SSRN Electronic Journal*. Doi: 10.2139/ssrn.2992537

Chen, Y.-J., Lin, C.-F., & Liu, H.-W. (2018). "Rule of trust": The power and perils of China's social credit megaproject. *Social Science Research Network*. Doi: 10.2139/ssrn.2992537

Cheney, C. (2019). China's Digital Silk Road: Strategic technological competition and exporting political illiberalism. *Issues & Insights*, Vol. 19, WP 8. Pacific Forum. [online] Available at: https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf

Chung, C.-S., Choi, H., & Cho, Y. (2022). Analysis of digital governance transition in South Korea: Focusing on the leadership of the president for government innovation. *Journal of Open Innovation: Technology, Market, and Complexity*, 8(1), Article 2. Doi: 10.3390/joitmc8010002

Cooley (2026). South Korea's AI Basic Act: Overview and key takeaways. [online] Available at: https://www.cooley.com/news/insight/2026/2026-01-27-south-koreas-ai-basic-act-overview-and-key-takeaways

Creemers, R. J. E. H. (2020). China's approach to cyber sovereignty. Konrad-Adenauer-Stiftung. [online] Available at: https://www.kas.de/en/single-title/-/content/china-s-approach-to-cyber-sovereignty

Creemers, R. (2023). Cybersecurity law and regulation in China. *China Law & Society Review*, 6(2), 111–145. Doi:10.1163/25427466-06020001

Da-gyum, J. (2024). S. Korea to chair first UN Security Council meeting with focus on cyber threats. *The Korea Herald*. [online] Available at: https://www.koreaherald.com/article/3364172

Diab, R. S. (2017). Becoming-infrastructure: Datafication and the social credit system. *Journal of Critical Library and Information Studies*, 1(1). Doi: 10.24242/jclis.v1i1.19

DLA Piper (2025). Law in China. In *Global data protection laws of the world*. [online] Available at: https://www.dlapiperdataprotection.com/

Dohr, P. (2025). China's weaponization of global cyber supply chains. *Center for Strategic and International Studies*. [online] Available at: https://www.csis.org/blogs/strategic-technologies-blog/chinas-weaponization-global-cyber-supply-chains

Duarte, P. A. B. (2025). The hybrid panda: China's sea and digital achievements. *(1st ed.). 5 Livros Publishing*.

Duarte, P. A. B., Tavares, A., Mosavi, N., & Amorim, F. P. L. (2024). The security dimension of the Digital Silk Road. In M. Sahakyan (Ed.), *Routledge handbook of China's Belt and Road Initiative in Eurasia* (pp. 135–149). Routledge. Doi; 10.4324/9781003513872-11

Elsner, G. and Natarajan, A. (n.d.). Regulating the cyberspace. *Konrad-Adenauer-Stiftung*. [online] Available at: https://www.kas.de/documents/278334/8513721/Regulating+The+Cyberspace.pdf

Ezenwaka, C.P. (2025). Digital sovereignty and the use of competitive intelligence to understand the race for technological dominance. *International Journal of Science and Research Archive,* 17(1), pp. 459–471. Doi: 10.30574/ijsra.2025.17.1.2774

Feigenbaum, E. A., & Nelson, M. R. (2024). Korea's path to digital leadership: How Seoul can lead on standards and standardization. Carnegie Endowment for International Peace. [online] Available at: https://carnegieendowment.org/research/2024/02/koreas-path-to-digital-leadership-how-seoul-can-lead-on-standards-and-standardization

Fort, K. (2024). Artificial intelligence governance and global policy. Doi: 10.48550/arXiv.2409.11314

Fung, C. J. (2022). China's use of rhetorical adaptation in development of a global cyber order: A case study of the norm of the protection of the public core of the internet. *Journal of Cyber Policy*, 7(3), 256–274. Doi: 10.1080/23738871.2023.2178946

Gao, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the Western model. *The International Spectator*, 57(3), 15–30. Doi: 10.1080/03932729.2022.2074710

Ghiasy, R., & Krishnamurthy, R. (2020). China's Digital Silk Road—Strategic implications for the EU and India. Special Report 208. [online] Available at: http://www.ipcs.org/issue_select.php?recNo=6153

Gida, J., Leung, J. W., Robin, S., & Cave, D. (2023). Critical technology tracker. Australian Strategic Policy Institute. [online] Available at: https://www.aspi.org.au/report/critical-technology-tracker/

Gosling, J. (2021). Maximising soft power: The role of digital diplomacy. *Global Affairs Review*, 1(2), 1–19.

Greenleaf, G. (2021). China's completed Personal Information Protection Law. *SSRN Electronic Journal*. Doit: 10.2139/ssrn.3989775

Griffiths, J. (2019). *The great firewall of China*. Zed Books.

Grover, R., Jang, K. and Su, L.W. (2024). Beyond digital protection(ism): Comparing data governance frameworks in Asia. *Journal of Information Policy*, 14, pp.161–193. Doi: 10.5325/jinfopoli.14.2024.0005

Guan, J. (2026). China's data sharing practice and data governance and legal exploration. In: *Governance and Management of Medical Scientific Data Sharing and Application*. Springer, Singapore. Doi: 10.1007/978-981-95-2806-6_4

Gul, S., Malik, W. and Qureshi, G. (2025). Cybersecurity and sovereignty: The role of international law in governing state behavior in cyberspace. *ResearchGate.* [online] Available at: https://www.researchgate.net/publication/392373086_cybersecurity_and_sovereignty_the_role_of_international_law_in_governing_state_behavior_in_cyberspace

He, A. (2023). State-centric data governance in China. *CIGI Papers No. 282*. Centre for International Governance Innovation. [online] Available at: https://www.cigionline.org/documents/2409/no.282.pdf

Helman, C. (2025). How South Korea's chaebols are pushing the robotics revolution. *Forbes*. [online] Available at: https://www.forbes.com/sites/christopherhelman/2025/06/12/how-south-koreas-chaebols-are-pushing-the-robotics-revolution/

Heydon, K. (2023). High digital stakes in new China–ASEAN new agreement. *East Asia Forum*. [online] Available at: https://eastasiaforum.org/2023/08/06/high-digital-stakes-in-new-china-asean-new-agreement/

Hoffman, S. (2017). Managing the state: Social credit and surveillance. *China Brief*, 17(11), 21–27. [online] Available at: https://jamestown.org/

Horsley, J. P. (2025). China's data dilemma. *SSRN Electronic Journal*. Doi: 10.2139/ssrn.5674524

Hu, J., & Rossi, J. (2025). Control through the state of exception. *World Comparative Law*. [online] Available at: https://www.researchgate.net/

Huang, J., & Tsai, K. S. (2022). Securing authoritarian capitalism. *The China Journal*, 88(1). Doi: 10.1086/720144

Huáng, M. (2025). Regulating personal data protection in China: Practices and future directions. *International Journal of Law and Criminology*, 5(2), 48–50.

Huang, Y. (2019). Analysis of internet censorship in mainland China. Lahti University of Applied Sciences. [online] Available at: https://www.theseus.fi/

Huld, A. (2023). Critical information infrastructure: China's new regulations. *China Briefing*. [online] Available at: https://www.china-briefing.com/news/critical-information-infrastructure-chinas-new-regulations/

Hung, H. T. (2025). Exploring China's cyber sovereignty concept and artificial intelligence governance model: A machine learning approach. *Journal of Computational Social Science*, 8(1), Article 24. Doi:10.1007/s42001-024-00346-8

Ijaz, S. (2024). Cybersecurity and Sovereignty: The Conflict among States in Governing Cyberspace. *Pakistan Social Sciences Review, 8(4),* pp. 706–714.

International Institute for Strategic Studies (2021). Cyber capabilities and national power: A net assessment. [online] Available at: https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power

International Organization for Standardization (2025). AI standards summit. [online] Available at: https://www.iso.org/news/2025/12/ai-standards-summit

International Telecommunication Union (2025). Key international organizations align on AI standards. [online] Available at: https://www.itu.int/hub/2025/12/key-international-organizations-align-on-ai-standards/

Ivanova, K.A., Myltykbaev, M.Zh. and Shtodina, D.D. (2022). The concept of cyberspace in international law. *Law Enforcement, 6(4),* pp. 32–44. Doi: 10.52468/2542-1514.2022.6(4).32-44

Jin, D. Y. (2024). The rise of digital platforms as soft power. *Communication and the Public*, 9(2). Doi: 10.1177/20570473241234204

Jing Cheng & Zeng, J. (2023). "Digital Silk Road" as a Slogan Instead of a Grand Strategy. *Journal of Contemporary China*. Doi:10.1080/10670564.2023.2222269

Joo, H.-y. (2025). President Lee Jae-myung: AI is national power, security pillar. *Chosun Ilbo*. [online] Available at: https://www.chosun.com/english/national-en/2025/09/08/MQPF3GDIC5HINPDKH6ZJ4WWSVI/

Kaska, K. and Tolppa, M. (2020). China's sovereignty and internet governance. ICDS. [online] Available at: https://icds.ee/wp-content/uploads/2020/06/ICDS_EFPI_Brief_Chinas_Sovereignty_and_Internet_Governance_Kadri_Kaska_Maria_Tolppa_June_2020.pdf

Khan, A. M. (2025). China's digital Silk Road and cyber diplomacy: Building influence in the cyber sphere. *Contemporary Journal of Social Science Review*, 3(2).

Kim, E. (2024). Cyber governance and international security. In: *Springer*. Doi: 10.1007/978-3-031-65671-2_11

Kim, I. S. (2025). 2025 comprehensive national cybersecurity strategy and initiatives. *EnkiWhiteHat*. [online] Available at: https://www.enki.co.kr/en/media-center/blog/2025-comprehensive-national-cybersecurity-strategy-and-initiatives

Kim, K., Seung, H., Kim, J. and Kim, J. (2025). Citizen-centric smart city strategies: Analyzing public demand and economic value in South Korea. *Cities*, 165, 106032. [online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0264275125003324

Kim, S. (2014). Cyber security and middle power diplomacy. *Korean Journal of International Studies*, 12(2), 323. Doi:10.14731/kjis.2014.12.12.2.323

Kim, T.-H. (2026). South Korea allows Google to export map data after years of frustration over Google Maps. *Associated Press*. [online] Available at: https://apnews.com/article/south-korea-google-maps-export-data-74d8c4d3e041a055f0bf1524ebdb9149

Klyman, K. (2022). China's tech crackdown could give it an edge. *The Diplomat*. [online] Available at: https://thediplomat.com/2022/04/chinas-tech-crackdown-could-give-it-an-edge/

Koepp, R. (2020). Locating the Digital Silk Road in the Belt and Road Initiative. *Adelphi Series*, 60(487–489), 37–50. Doi: 10.1080/19445571.2020.2151124

Kostka, G. (2019). China's social credit systems and public opinion. *New Media & Society*, 21(7), 1565–1593. Doi: 10.1177/1461444819826402

Krasikov, D.V. and Lipkina, N.N. (2020). Proceedings of the XIV European-Asian Law Congress "The Value of Law" *(EAC-LAW 2020)*. *Advances in Social Science, Education and Humanities Research.* Doi:10.2991/assehr.k.201205.028

Krishna (2023). Digital Sovereignty and Cybersecurity Governance: Legal Implications of State Control in a Fragmented Internet. *Innovative Research Thoughts,* 9(3), pp. 199–209. Doi: 10.36676/irt.v9.i3.1648

Lale, A. (2020). The soft power of South Korea. *Asya Studies*, 4(13), 63–74. Doi: 10.31455/asya.615427

Lee, D. (2024). Korea's path to digital leadership: How Seoul can lead on standards and standardization. Chapter 2: The Role of South Korea's Private Sector in Setting Technology Standards. Carnegie Endowment for International Peace. [online] Available at: https://carnegieendowment.org/research/2024/02/koreas-path-to-digital-leadership-how-seoul-can-lead-on-standards-and-standardization

Lee, J. (2022). Cyberspace governance in China. IFRI. [online] Available at: https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/lee_cyberspace_governance_china_2022.pdf

Lee, K., Rasser, M., Fitt, J., & Goldberg, C. (2020). Digital entanglement. Center for a New American Security. [online] Available at: https://www.cnas.org/

Lee, Y., Han, S., & Cho, Y. (2025). Navigating the path to smart and sustainable cities: Insights from South Korea's National Strategic Smart City Program. *Land*, 14(5), Article 928. Doi: 10.3390/land14050928

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, 10(4), 415–453. Doi: 10.1002/poi3.183

Lim, Y., Edelenbos, J., & Gianoli, A. (2022). Dynamics in the governance of smart cities: Insights from South Korean smart cities. *International Journal of Urban Sciences*, 27(1), 1–22. Doi: 10.1080/12265934.2022.2063158

Liu, L. (2025). China and global human rights in the digital age. *Arizona State University*. [online] Available at: https://newcollege.asu.edu/global-human-rights-hub/fellows-program/ghr-fellows-blog/liming

Lu, Y. (2022). Digital governance and regulatory frameworks. *Chinese Journal of Communication Review*, 2(2). Doi: 10.5117/CCR2022.2.002.LU

Lu, W. (2015). Lu Wei urges China and Europe to deepen cooperation and build a "Digital Silk Road." *Guancha*. [online] Available at: https://www.guancha.cn/strategy/2015_07_07_325897.shtml

Lynch, T.F. III (2024). Cyberspace: Great Power Competition in a Fragmenting Domain. *Orbis, 68(4), pp. 607–623*. Doi:10.1016/j.orbis.2024.09.007

MA, H., & DU, X. (2025). Digital Economic Integration Under RCEP: China-ASEAN Collaboration Opportunities, Challenges, and Pathways. *International Relations and Diplomacy*, 13(2), 96–106.

Mark Raymond & Sherman, J. (2024). Authoritarian multilateralism in the global cyber regime complex: The double transformation of an international diplomatic practice. *Contemporary Security Policy*, 45(1), 110–140. Doi: 10.1080/13523260.2023.2269809

Mayer, M. and Nock, P.J. (2024). Digital fragmentations, technological sovereignty and new perspectives on the global digital political economy. *Global Political Economy,* pp. 1–12. Doi: 10.1332/26352257Y2024D000000029

McDonald, S. M., & Mina, A. X. (2018). The war-torn web. *Foreign Policy*. [online] Available at: https://foreignpolicy.com/

Meaghan, T. (2025). How China is spending heavily to build an AI superpower. *New York Times Chinese Version*. [online] Available at: https://cn.nytimes.com/technology/20250717/china-ai/

Meissner, M. (2017). China's social credit system: A big-data enabled approach to market regulation with broad implications for doing business in China. *MERICS*. [online] Available at: https://merics.org/en/report/chinas-social-credit-system

Merrill, N. (2025, April). The South Korean digital paradox: How South Korea's internet development model creates unique cybersecurity vulnerabilities (White Paper). Center for Long-Term Cybersecurity, UC Berkeley. [online] Available at: https://cltc.berkeley.edu/publication/the-south-korean-digital-paradox-how-south-koreas-internet-development-model-creates-unique-cybersecurity-vulnerabilities/

Mirza, M. N., Ali, L. A., & Qaisrani, I. H. (2021). Conceptualising cyber sovereignty. [online] Available at: https://www.researchgate.net/

Misra, S., Barik, K. and Kvalvik, P. (2025). Digital Sovereignty in the Era of Industry 5.0: Challenges and Opportunities. *Procedia Computer Science,* 254, pp. 108–117. Doi: 10.1016/j.procs.2025.02.069

Mok, C. (2025). How China governs its internet and plans to export its model. *Tech Policy Press*. [online] Available at: https://www.techpolicy.press/how-china-governs-its-internet-and-plans-to-export-its-model/

Murniasari, M. (2024). China's cyber security governance as part of foreign and security policy. *Security Intelligence Terrorism Journal (SITJ)*, 1(2), 164–177. Doi: 10.70710/sitj.v1i2.23

Mutingwende, B. A. (2022). Huawei's Seeds for the Future Program 2023 Trains Students in Cutting-Edge Technologies. *Spiked Media*. [online] Available at: https://spikedmedia.co.zw/huaweis-seeds-for-the-future-program-2023-trains-students-cutting-edge-technologies/

Nam, S. (2024). The Republic of Kakao goes on hiatus: The public cost of platform monopolies in South Korea. *Communication and the Public*, 9(1), 84–99. Doi: 10.1177/20570473231224818

Naughton, B. (2021). What's behind China's regulatory storm? *Wall Street Journal*. [online] Available at: https://www.wsj.com/

Nocetti, J. (2024). A splintered internet? *IFRI*. [online] Available at: https://www.ifri.org/

Novotná, T. (2025). Beyond the pivot: Expanding South Korea's global role and G7 cooperation in a new era (IAI Papers No. 25|38). *Istituto Affari Internazionali*. [online] Available at: https://www.iai.it/en/publications/c03/beyond-pivot-expanding-south-koreas-global-role-and-g7-cooperation-new-era

Nye, J. S. (2010). *Cyber power*. Belfer Center. [online] Available at: https://www.belfercenter.org/

Niu, J. (2025). The sovereignty exception: China's state-centric approach to national security in cross-border data flows. *Lecture Notes in Education Psychology and Public Media*, 107(1), 60–66. Doi: 10.54254/2753-7048/2025.ld27192

Orta, K.T. (2025). How South Korea advanced its trade and technology agenda at the APEC summit. *Atlantic Council*. [online] Available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/how-south-korea-advanced-its-trade-and-technology-agenda-at-the-apec-summit/

Oscar Borgogno & Zangrandi, M. S. (2024). Chinese Data Governance and Trade Policy: From Cyber Sovereignty to the Quest for Digital Hegemony? *Journal of Contemporary China*, 33(148), 578–602. Doi: 10.1080/10670564.2023.2299961

Olson, S. (2020). Are private Chinese companies really private? *The Diplomat*. [online] Available at: https://thediplomat.com/

Pan, J. (2022). Controlling China's digital ecosystem: Observations on Chinese social media. *PRC Leader*. [online] Available at: https://www.prcleader.org/post/controlling-china-s-digital-ecosystem-observations-on-chinese-social-media

Park, J. (2025). The development of emerging technologies in South Korea and its impact on international relations. *Korea On Point*. [online] Available at: https://koreaonpoint.org/articles/article_detail.php?idx=440

Park, J., & Kim, D. (2025). Forging forward: South Korea's proactive cyber defense and strategic cooperation with the United States. *Center for Strategic and International Studies*. [online] Available at: https://www.csis.org/analysis/forging-forward-south-koreas-proactive-cyber-defense-and-strategic-cooperation-united

Paudel, P. (2025). Connecting Asia: The rise of China's Digital Silk Road in ASEAN countries. *Realism: Law Review*, 3(2). Doi: 10.71250/rlr.v3i2.75

Paz, S., Tejerina, L., & Kang, D. (2024). National Cybersecurity Law, Governance, and Infrastructure in the Republic of Korea. *Inter-American Development Bank*. [online] Available at: https://publications.iadb.org/publications/english/document/National-Cybersecurity-Law-Governance-and-Infrastructure-in-the-Republic-of-Korea.pdf

Perarnaud, C., Rossi, J., Musiani, F., & Castex, L. (2022). 'Splinternets'. *European Parliamentary Research Service*. [online] Available at: https://www.europarl.europa.eu/

Ping, L. (2026). The global governance of artificial intelligence: Progress, challenges, and China's role. *China-CEE Institute*. [online] Available at: https://china-cee.eu/2026/02/12/the-global-governance-of-artificial-intelligence-progress-challenges-and-chinas-role/

Prüfer, J., Graef, I., & Jeon, D.-S. (2024). Regulation of digital platforms and the state's use of platform technologies in China. *Social Science Research Network*. Doi: 10.2139/ssrn.4852160

Qiang, X. (2019). The road to digital unfreedom. *Journal of Democracy*, 30(1), 53–67. Doi: 10.1353/jod.2019.0004

Qiao-Franco, G. (2024). An Emergent Community of Cyber Sovereignty: The Reproduction of Boundaries? *Global Studies Quarterly, 4(1).* Doi: 10.1093/isagsq/ksad077

Qiao-Franco, G. and van Beek, A. (2025). China's strategy for global AI governance. *Leiden Asia Centre*. [online] Available at: https://leidenasiacentre.nl/publication-chinas-strategy-for-global-ai-governance

Rahman, A. (2025). The Digital Silk Road. *Asian Journal of Political Science*, 1–21. Doi: 10.1080/02185377.2025.2489375

Rajgopal, P.R. and Yadav, S. (2025). *The Role of Data Governance in Enabling Secure AI Adoption*. *IJSIE,* 3(1). Doi: 10.56830/IJSIE202501

Ramadhan, I. (2023). ASEAN-China Cybersecurity Cooperation: Challenges and Opportunities. *Journal of Social and Political Sciences*, 6(4), 1–10. Doi: 10.31014/aior.1991.06.04.440

Roberts, H., Hine, E. and Floridi, L. (2023). Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance. In: M. Timoteo, B. Verri and R. Nanni (eds), Quo Vadis, Sovereignty? *Philosophical Studies Series,* vol. 154. Doi: 10.1007/978-3-031-41566-1_4

Roberts, M. E. (2018). *Distraction and diversion inside China's great firewall*. Princeton University Press.

Roshan, P. (2025). The evolving cyber landscape: Capabilities and cyber diplomatic efforts of the Korean Peninsula. *Journal of Regional Studies Review*, 4(1), 1–14.

Rothschild, V. (2024). Protest and repression in China's digital surveillance state. *Journal of Information Technology & Politics*, 1–16. Doi: 10.1080/19331681.2024.2326464

Ryan, F., Allen, B., Shih, S., Robin, S., Attrill, N., Alpert, J., Young, A. and Hoja, T. (2025). The party's AI: How China's new AI systems are reshaping human rights. *Australian Strategic Policy Institute (ASPI)*. [online] Available at: https://www.aspi.org.au/report/the-partys-ai-how-chinas-new-ai-systems-are-reshaping-human-rights/

Sacks, S., & Sherman, J. (2019). China's cybersecurity legislation: Paper tiger or institutionalised theft? Institute for Security and Development Policy. [online] Available at: https://www.isdp.eu/publication/chinas-cybersecurity-legislation-paper-tiger-institutionalized-theft/

Sharma, A. (2025). Mapping South Korea's defence industrialisation in the age of smart technologies. *Observer Research Foundation*. [online] Available at: https://www.orfonline.org/research/mapping-south-korea-s-defence-industrialisation-in-the-age-of-smart-technologies

Sheehan, M. (2023). China's AI Regulations and How They Get Made. Carnegie Endowment for International Peace. [online] Available at: https://carnegieendowment.org/files/202307-Sheehan_Chinese%20AI%20gov.pdf

Shen, H. (2018). Building a digital Silk Road? Situating the Internet in China's Belt and Road Initiative. *International Journal of Communication*, 12, 2683–270.

Shen, Y., Zhang, S., & Oliveira, I. T. (2025). China's approach to cybersecurity and information integrity. *Liinc em Revista*, 21(1). Doi: 10.18617/liinc.v21i1.7537

Shin, S.-Y., Lee, A. and Chung, C.-S. (2025). Blueprints for tomorrow's smart cities in South Korea: Conceptual definition and timeline forecast from a policy Delphi study. *Journal of Political Studies*. Doi:10.52372/jps.e680

Singh, L. (2025). President Lee Jae-myung's G7 Debut and the Recalibration of South Korean Foreign Policy. *The Diplomat*. [online] Available at: https://thediplomat.com/2025/06/president-lee-jae-myungs-g7-debut-and-the-recalibration-of-south-korean-foreign-policy/#:~:text=The%20strategic%20contours%20of%20Lee%E2%80%99s%20emerging%20doctrine%20%E2%80%93,reorientation%20of%20South%20Korea%E2%80%99s%20traditionally%20U.S.-centric%20foreign%20policy.

Sohyun, S. (2025). National Position of the Republic of Korea on the Application of International Law in Cyberspace: Present and Future. *Asan Institute for Policy Studies*. [online] Available at: http://www.jstor.org/stable/resrep72581

Srivastava, S. and Bullock, J. (2024). AI, Global Governance, and Digital Sovereignty. [online] Available at: https://www.convergenceanalysis.org/research/ai-global-governance-and-digital-sovereignty

Svanadze, V., Iavich, M. and Lukashenko, V. (2024). Geopolitical and Technical Dimensions of Internet Fragmentation. *CEUR Workshop Proceedings*. [online] Available at: https://ceur-ws.org/Vol-3991/short3.pdf

Thian, S.Y. (2025). Robust, open data foundations power South Korea's AI digital government vision. *GovInsider*. [online] Available at: https://govinsider.asia/intl-en/article/robust-open-data-foundations-power-south-koreas-ai-digital-government-vision

Tiwari, R. (2025). The Geopolitics of Digital Sovereignty and Artificial Intelligence (AI). *Episteme Journal,* 14(3), p. 66.

Torrisi, R. (2023). China's new personal information protection law (PIPL): Implications for companies and human resources management. Master's thesis, *Università Ca' Foscari Venezia*. [online] Available at: https://unitesi.unive.it/bitstream/20.500.14247/17888/1/890721-1281615.pdf

Vagianos, D., & Stavrou, G. (2023). Surveillance infrastructure and artificial intelligence: Challenging democracy and human rights in China. [online] Available at: https://www.researchgate.net/publication/370941029

Vijayan, J. (2024). Private firms and academia in China's cyber offense strategy. *Dark Reading*. [online] Available at: https://www.darkreading.com/cyber-risk/private-firms-academia-china-cyber-offense-strategy

Vosse, W. (2025). Prospects of closer Japan-Korea cybersecurity cooperation. *The Ritsumeikan Journal of International Studies*, 37(3), 63–70. Doi: 10.34382/0002001856

Wang, A. (2020). Cyber sovereignty at its boldest: A Chinese perspective. *The Ohio State Technology Law Journal*, 16(2), 395–466. [online] Available at: https://docslib.org/doc/9069500/cyber-sovereignty-at-its-boldest-a-chinese-perspective

Wang, H. (2025). China's approach to international AI governance: Selective shaping. *ResearchGate*. [online] Available at: https://www.researchgate.net/publication/397796651_China's_Approach_to_International_AI_Governance_Selective_Shaping

Wang, Z. (2024). China's Digital Silk Road (DSR) in Southeast Asia: Progress and challenges. *ISEAS Perspective*, No. 2024/1. *ISEAS – Yusof Ishak Institute*. [online] Available at: https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2024-1-chinas-digital-silk-road-dsr-in-southeast-asia-progress-and-challenges-by-wang-zheng/

Weber, V. (2023). China's smart cities and the future of geopolitics. *German Council on Foreign Relations (DGAP)*. [online] Available at: https://dgap.org/en/research/publications/chinas-smart-cities-and-future-geopolitics

Wiater, D. (2025). China's AI soft power play: How is the Digital Silk Road shaping global influence? [online] Available at: https://ipr.blogs.ie.edu/wp-content/uploads/sites/574/2025/01/IPR-ARTICLE-second-draft.pdf

Wood, N. (2024). South Korea's 2024 Cyber Strategy: A Primer. *CSIS*. [online] Available at: https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer

Woods, A.K. (2023). Digital Sovereignty + Artificial Intelligence. In: A. Chander and H. Sun (eds), Data Sovereignty: From the Digital Silk Road to the Return of the State. *New York: Oxford Academic.* Doi: 10.1093/oso/9780197582794.003.0006

Woods, D. (2025). AI as a tool for surveillance. *Journal of Chinese Political Science*. Doi:/10.1007/s11366-025-09907-8

Xiao, Y. (2024). Recentralisation and China's evolving cyber governance. UC Institute on Global Conflict and Cooperation. [online] Available at: https://ucigcc.org/wp-content/uploads/2024/03/Xiao-Recentralization-03.19.24.pdf

Yang, Z. (2022). Hikvision: The world's biggest surveillance company. *MIT Technology Review*. [online] Available at: http://technologyreview.com/2022/06/22/1054586/hikvision-worlds-biggest-surveillance-company/

Yilmaz, C. (2026). The Geopolitics of Artificial Intelligence: Power, Regulation, and Global Governance. *FIU Journal of Social Sciences and Humanities,* 2(3), 39–70.

Yu, J.S. (2025). Regulating social media in a democracy: The case of South Korea. PhD thesis. University of Otago. [online] Available at: https://hdl.handle.net/10523/45570