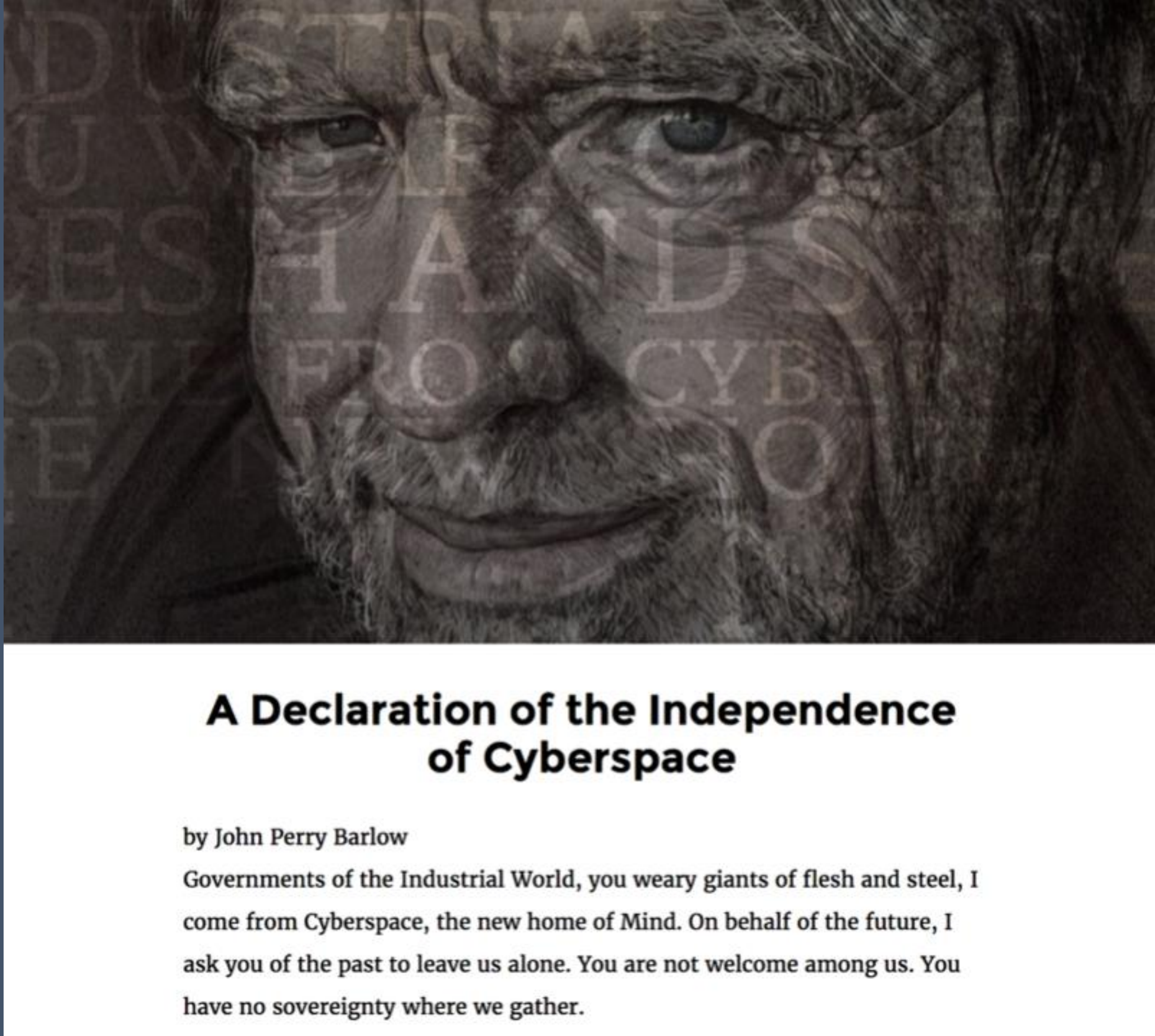
Chinese Conception of Cyber Sovereignty and its Legal Framework

Han Liu

Tsinghua Law School

I.Backgrounds

Cyber Utopianism

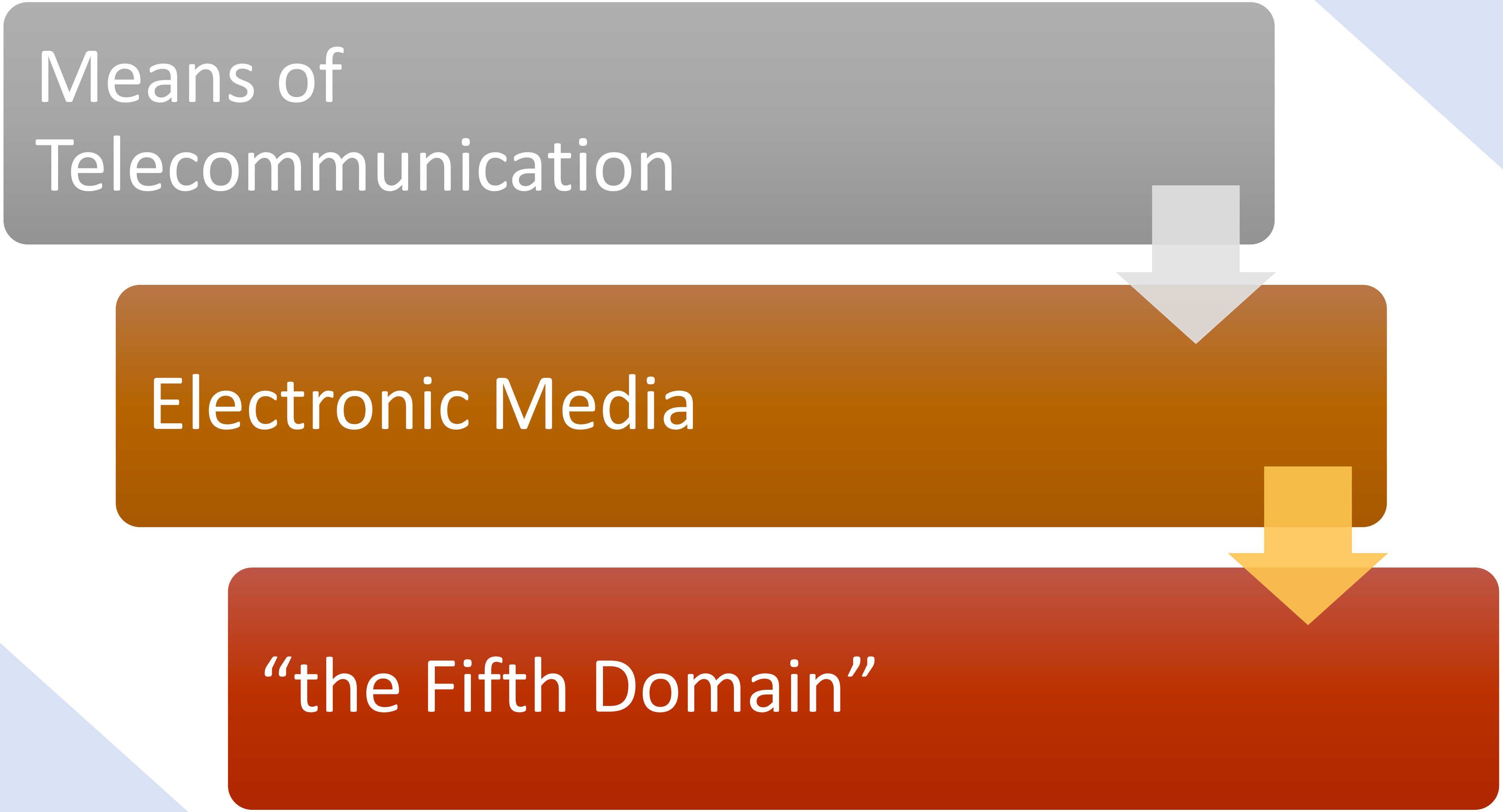


A Declaration of the Independence of Cyberspace

by John Perry Barlow

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

How China Perceives the Internet



Means of Telecommunication

Electronic Media

“the Fifth Domain”

Land

Sea

Air

Space

Cyber

Westphalian Sovereignty applies in the “fifth domain”.

Two Visions of Internet Governance

Cosmopolitan

1. US Rules as Blueprint
2. Internet Freedom As Banner
3. Free Speech Laws As Content
4. Dark Side: Hegemonic Americanism

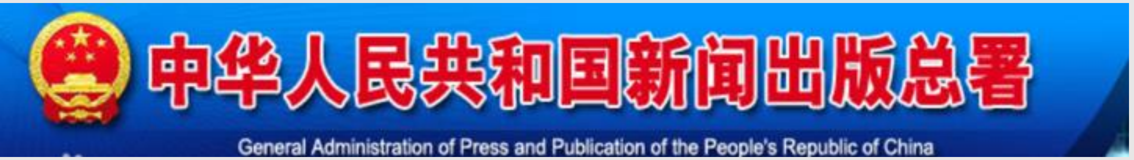
Sovereign-Difference

1. Diversified System Based on Sovereignty
2. Each Country Regulating the Internet According to its Own Laws
3. Dark Side: Internet Fragmentation

II.Chinese Practice

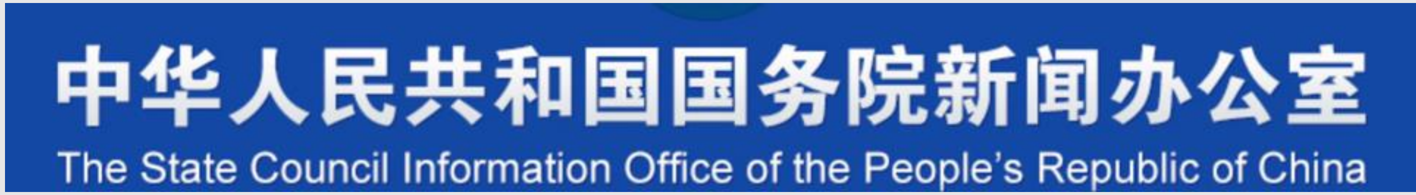
(1)
Internally

a. Centralizing Regulatory Power



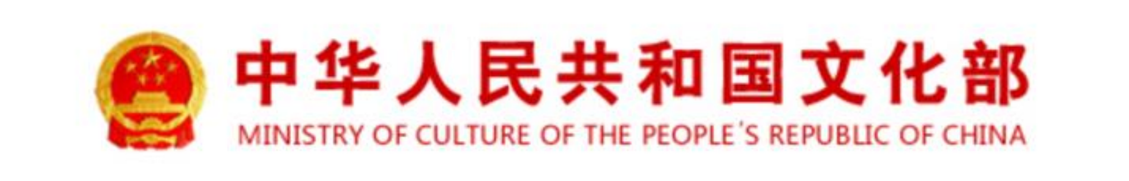
中华人民共和国新闻出版总署

General Administration of Press and Publication of the People's Republic of China



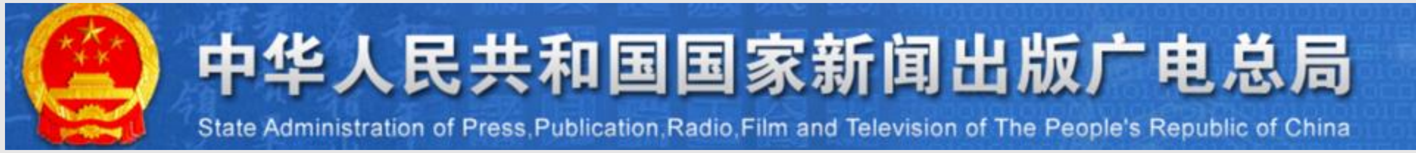
中华人民共和国国务院新闻办公室

The State Council Information Office of the People's Republic of China



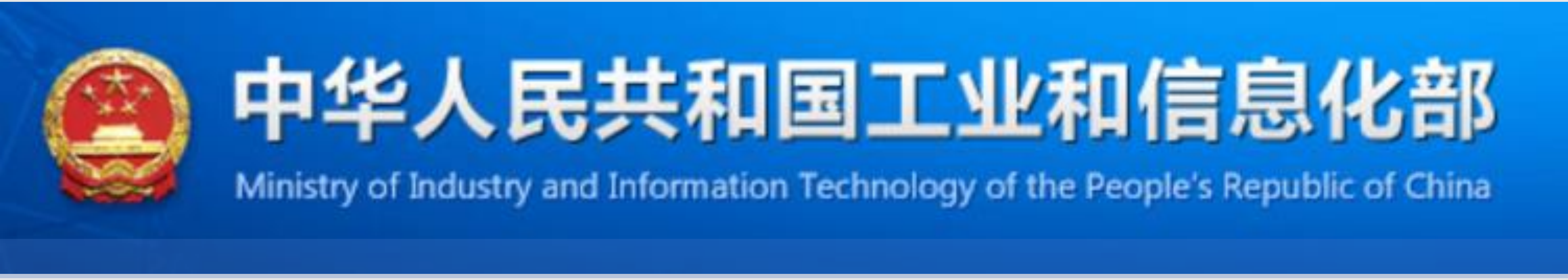
中华人民共和国文化部

MINISTRY OF CULTURE OF THE PEOPLE'S REPUBLIC OF CHINA



中华人民共和国国家新闻出版广电总局

State Administration of Press,Publication,Radio,Film and Television of The People's Republic of China



中华人民共和国工业和信息化部

Ministry of Industry and Information Technology of the People's Republic of China

Chinese Internet Regulation Erstwhile: “Nine Dragons Tame the Flood.”

cac.gov.cn

CYBERSPACE ADMINISTRATION OF CHINA

CAC (2014)

中共中央网络安全和信息化领导小组办公室

Office of the Central Leading Group for Cyberspace Affairs

b. Making Pillars of Cyber Law

Framework Laws

Cyber Security Law (2016)

- Critical Information Infrastructure’ s Data Transfer must get approval
- Data localization requirements for personal information and “important data”

Data Security Law (2021)

- Data Security Review before transfer of important data
- Export control over important data
- Against Long-Arm Jurisdiction

Personal Information Law (2021)

(2) Externally

Call for the Idea of Cyber Sovereignty and Global Response

III.Global Response

EU: Embracing Digital Sovereignty

European Institute of Innovation & Technology Report (2020)

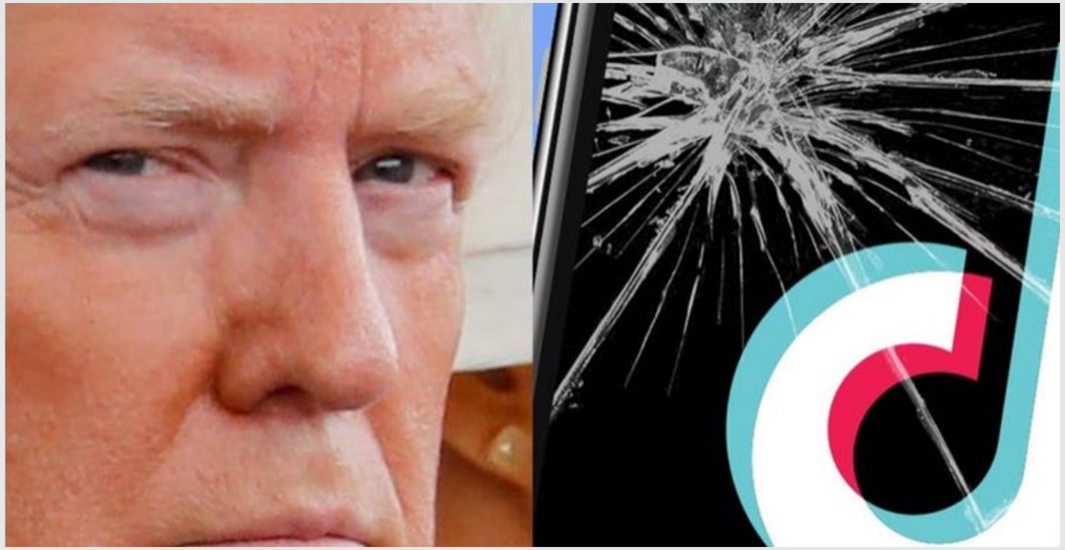
EUROPEAN DIGITAL INFRASTRUCTURE AND DATA SOVEREIGNTY

A POLICY PERSPECTIVE

Europe should have its own data platform, rather than relying on Google’s or Microsoft’s cloud services, to ensure “digital sovereignty” (2019).

US: Defending National Security and Tech overeignty

TikTok and Huawei Cases



Russia: Sovereign Internet

The Global South: Avoiding Data Colonialism & Protect Digital Sovereignty

The Global South: Avoiding Data Colonialism

Digital Transformation Strategy for Africa (2020-2030): “Even though Africa is at the moment less restrictive, soon it will be necessary to ensure localization of all personal data of Africa’s citizens.”

In Senegal, President Macky Sall hopes to protect “Senegalese digital Sovereignty” by building a data center within the country with the help of Huawei in 2021.

In 2021, South Africa published a draft National Data and Cloud Policy, seeking to “promote South Africa’s data sovereignty.”

the Māori Data Sovereignty Network seeks to ensure that Māori peoples have sovereignty over the “data produced by Māori or that is about Māori and the environments we have relationships with.”

Two
Historical Phases

- First generation of Internet control tried to keep information out.
- Next generation of Internet border control try to keep data within.

Data Localization Laws in Global Perspectives

Strong Protection

Local Storing

China
Russia

Weak Protection

Conditional Transfer

EU
Brazil
South Africa

1. Brazil and South Africa allow transborder data flow only if backed up and retained within the country.
2. China and Russia requires data collected by foreign companies to be retained locally.
3. Canada and Australia implement classified protection: e.g., personal health information not allowed to leak.

IV.Our Project

Initiative on the New Rules

Internationalizing Governance Subjects

- Strengthen the role of UN as the main channel
- Enhancing Degree of Participation of ICANN

Systematizing Governance Rules: Combining Law and Tech

- Meta-Rules
- Enforcement Rules
- Adjudication Rules
- Technical Standards

Deepening Security Cooperation Mechanisms

- Shaping“Hard and Soft Laws”under UN Framework
- Classification of Data Security Management and Cross-Border Flows
- Improving International Cooperation Mechanisms for Managing Basic Internet Resources

Promoting Development Benefits Sharing

- Transnational Digital Divide Management Organization within OBOR Initiative
- "Digital Silk Road" and Improve Cooperation Mechanisms, Governance Rules and Technical Standards

Application :Draft of Regional Governance Rules for IPv6 Cyberspace in Belt and Road Countries (Scholars' Proposal)

Table of Contents

[Highlights]

Chapter IV Network Governance Enforcement Mechanism and Credit system

Article 24 [Purpose of Network Credit System Construction]

Article 25 [Recognition of Credit Standing]

Article 26 [Credit Information Management]

Article 27 [Regional Credit Early Warning Platform]

Article 28 [Incentive to Keep Faith and Constraints on Faith Breaking]

Article 29 [Credit Repair]