EUI ROBERT SCHUMAN CENTRE

Parallel digital worlds: restrictions on anti-censorship tools as an emerging authoritarian norm

Dr Patryk Pawlak, EUI

Nils Berglund, EUI

www.eui.eu

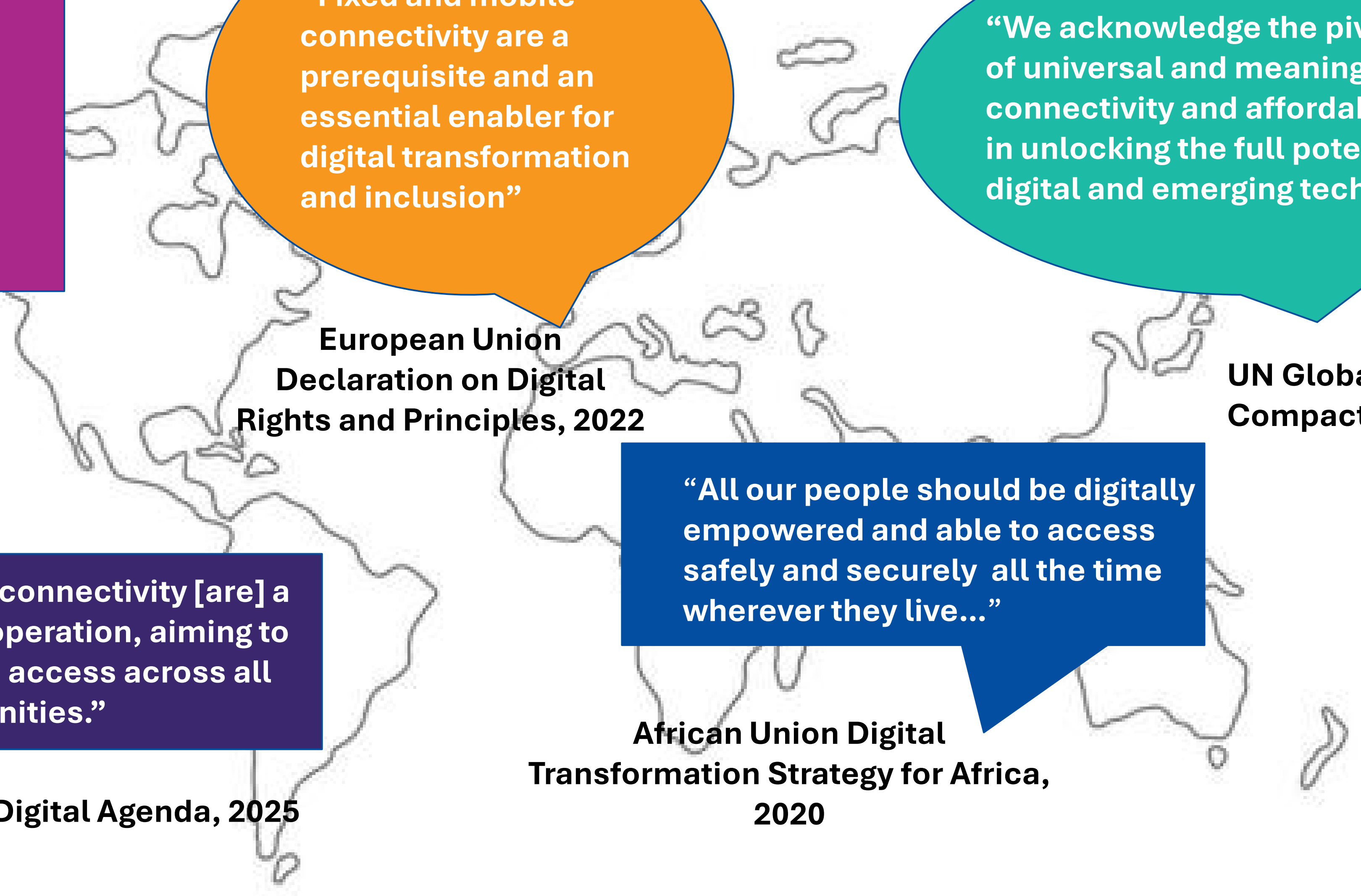
ROBERT SCHUMAN CENTRE

Structure of the presentation

1. International norm to stay online
2. Proliferation of restrictions on access to the Internet
3. Emergence of a new norm?
4. Country cases
   a) Russia
   b) Iran
   c) China
   d) India
4. UN processes

Co-funded by the Erasmus+ Programme of the European Union

Universal connectivity as an existing norm



"Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers"

World Summit of the Information Society (WSIS), 2003-2005

"Fixed and mobile connectivity are a prerequisite and an essential enabler for digital transformation and inclusion"

European Union Declaration on Digital Rights and Principles, 2022

"We acknowledge the pivotal role of universal and meaningful connectivity and affordable access in unlocking the full potential of digital and emerging technologies."

UN Global Digital Compact, 2024

"Infrastructure and connectivity [are] a primary pillar of cooperation, aiming to expand broadband access across all communities."

eLAC Digital Agenda, 2025

"All our people should be digitally empowered and able to access safely and securely all the time wherever they live…"

African Union Digital Transformation Strategy for Africa, 2020

Proliferation of restrictions

In at least **21** of the **72** countries covered by FOTN 2024, anti-censorship tools were blocked in the past five years.

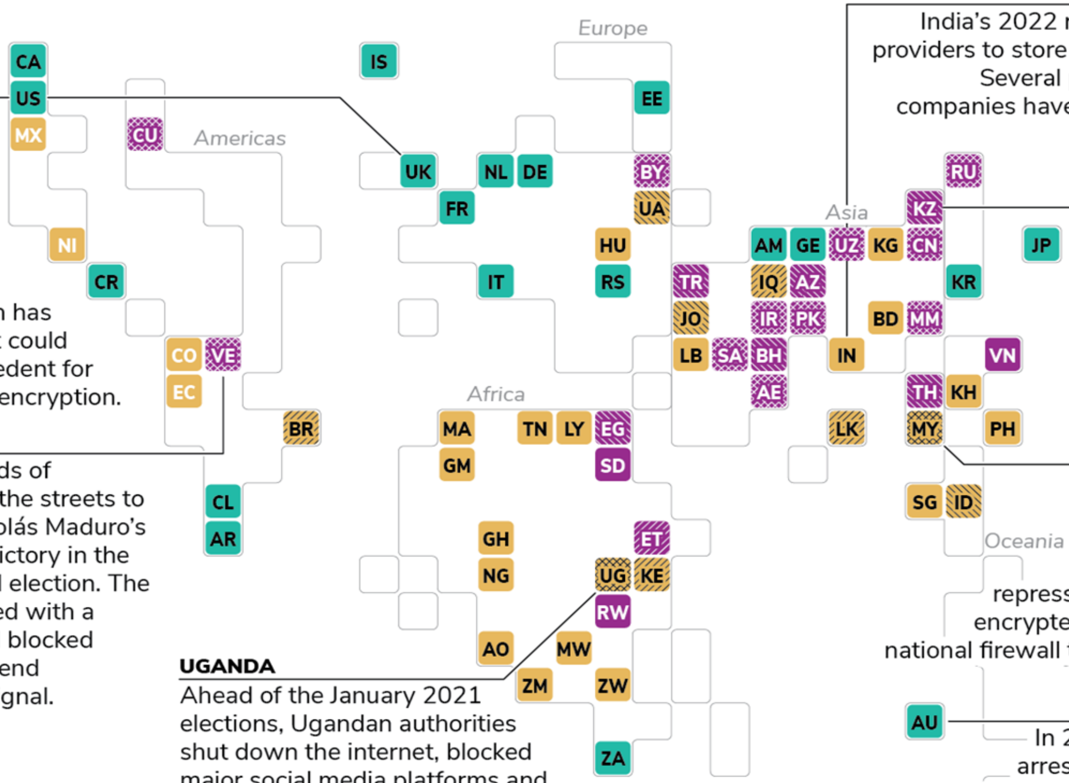
FOTN status 2024

Not Free ● Partly Free ● Free ●

Blocked 2020-2025

Anti-censorship tech ▨ E2EE messaging platforms ▨

In at least **17** of **72** countries covered by FOTN 2024, end-to-end encrypted services were blocked in the past five years.



UNITED KINGDOM

The 2023 Online Safety Act granted regulators the power to compel platforms to scan private, encrypted messages for harmful content. While implementation has been delayed, the Act could set a dangerous precedent for breaking end-to-end encryption.

VENEZUELA

In July 2024, thousands of Venezuelans flooded the streets to protest President Nicolás Maduro's fraudulent claims of victory in the July 2024 presidential election. The government responded with a brutal crackdown and blocked access to the end-to-end encrypted platform Signal.

UGANDA

Ahead of the January 2021 elections, Ugandan authorities shut down the internet, blocked major social media platforms and ordered the blocking of over 100 VPNs, limiting people's ability to share information.

INDIA

India's 2022 regulation required VPN providers to store user data for five years. Several privacy-respecting VPN companies have shut down their Indian servers in response.

KAZAKHSTAN

As of June 2024, the websites for over 70 anti-censorship tools were blocked in Kazakhstan, making it much harder for people to access their services.

MYANMAR

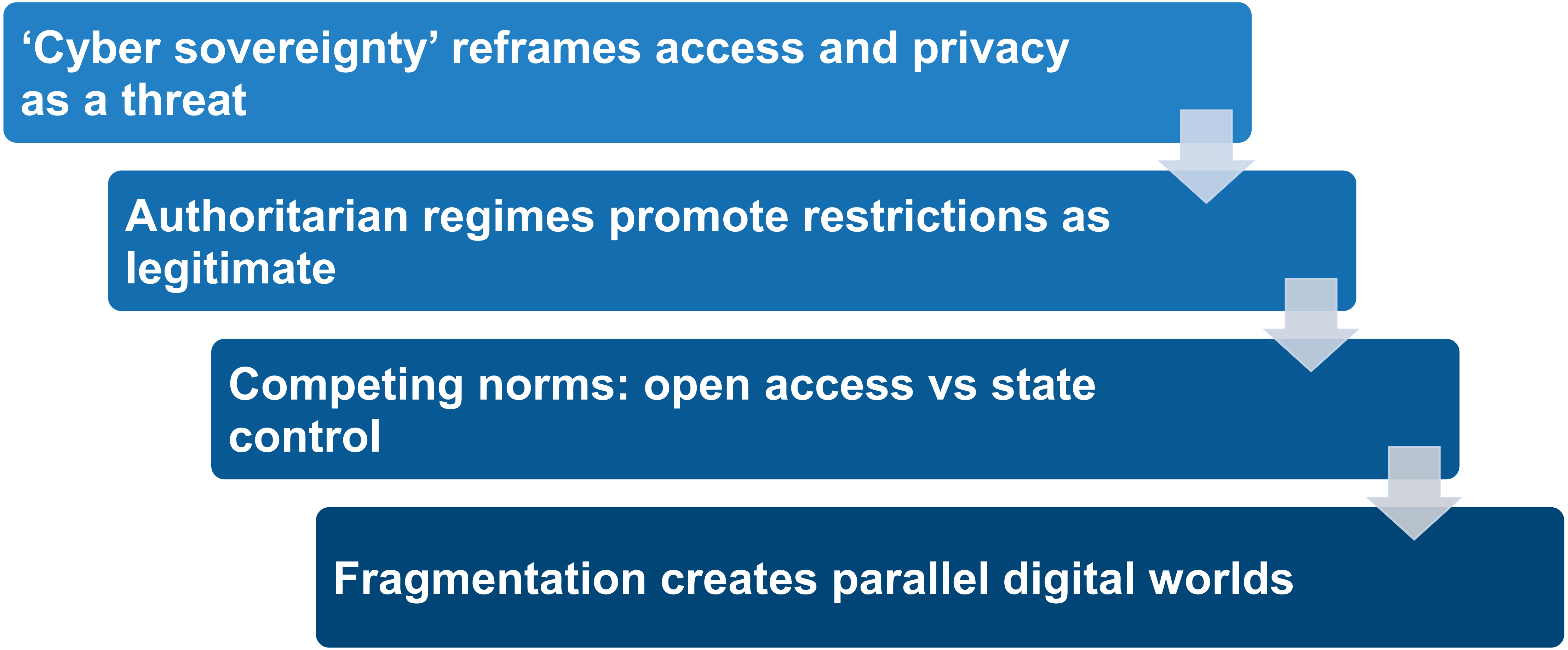
Following the 2021 coup, Myanmar's military government ramped up digital repression, blocking VPNs and encrypted apps and rolling out a national firewall to monitor online traffic.

AUSTRALIA

In 2022, climate protesters arrested for an unauthorized demonstration were barred from using encrypted messaging apps as a bail condition, marking encryption use as inherently suspicious.

Co-funded by the Erasmus+ Programme of the European Union

Restricting connectivity as a new norm?



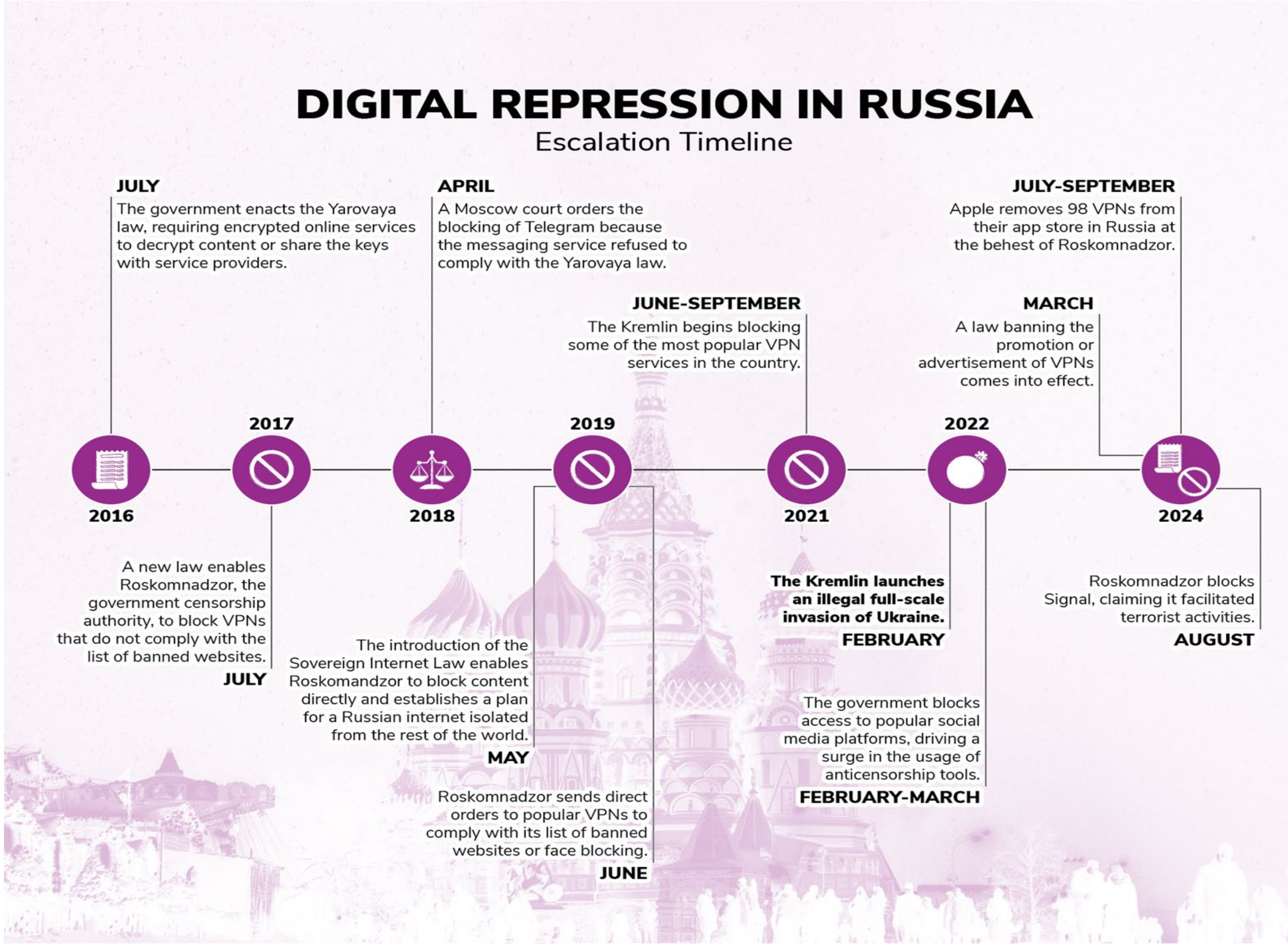
‘Cyber sovereignty’ reframes access and privacy as a threat

Authoritarian regimes promote restrictions as legitimate

Competing norms: open access vs state control

Fragmentation creates parallel digital worlds

Russia: Proliferation of restrictions



DIGITAL REPRESSION IN RUSSIA

Escalation Timeline

2016

JULY
The government enacts the Yarovaya law, requiring encrypted online services to decrypt content or share the keys with service providers.

2017

JULY
A new law enables Roskomnadzor, the government censorship authority, to block VPNs that do not comply with the list of banned websites.

2018

APRIL
A Moscow court orders the blocking of Telegram because the messaging service refused to comply with the Yarovaya law.

2019

MAY
The introduction of the Sovereign Internet Law enables Roskomandzor to block content directly and establishes a plan for a Russian internet isolated from the rest of the world.

JUNE
Roskomnadzor sends direct orders to popular VPNs to comply with its list of banned websites or face blocking.

2021

JUNE-SEPTEMBER
The Kremlin begins blocking some of the most popular VPN services in the country.

2022

FEBRUARY
The Kremlin launches an illegal full-scale invasion of Ukraine.

FEBRUARY-MARCH
The government blocks access to popular social media platforms, driving a surge in the usage of anticensorship tools.

2024

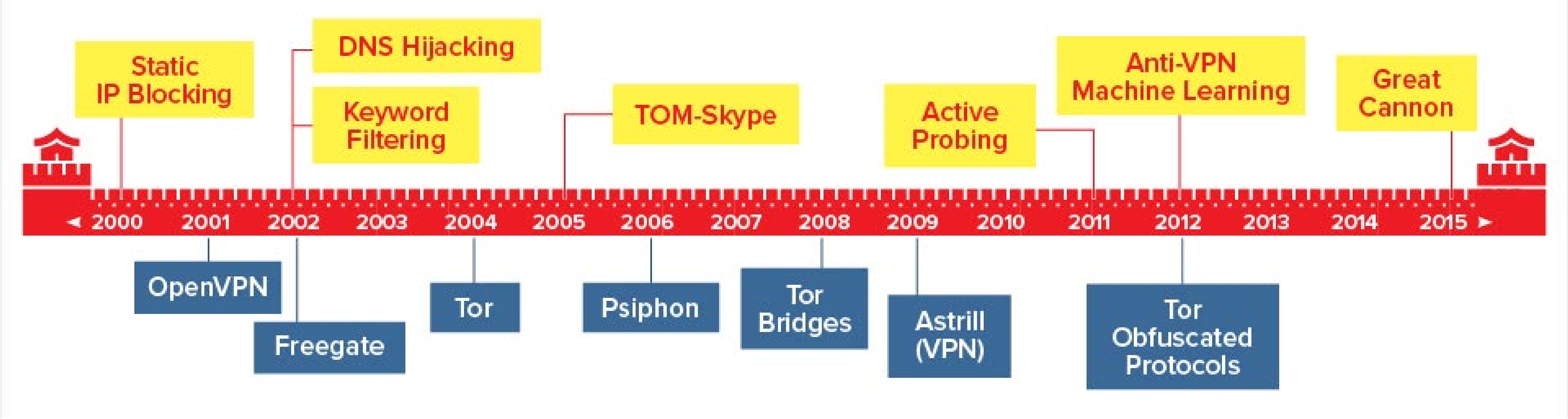
MARCH
A law banning the promotion or advertisement of VPNs comes into effect.

JULY-SEPTEMBER
Apple removes 98 VPNs from their app store in Russia at the behest of Roskomnadzor.

AUGUST
Roskomnadzor blocks Signal, claiming it facilitated terrorist activities.

Co-funded by the Erasmus+ Programme of the European Union

China: The Great Firewall & New Architecture

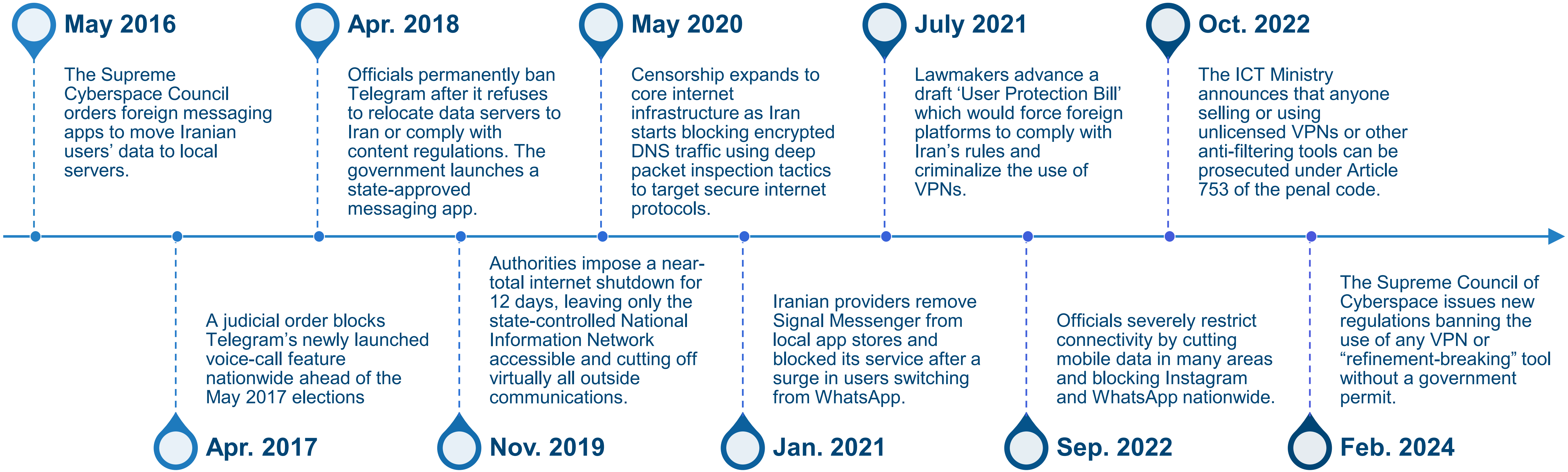


Co-funded by the Erasmus+ Programme of the European Union

Source: Thousand Eyes (Cisco)

ROBERT SCHUMAN CENTRE

Iran: co-opting privacy infrastructure



May 2016
The Supreme Cyberspace Council orders foreign messaging apps to move Iranian users' data to local servers.

Apr. 2017
A judicial order blocks Telegram's newly launched voice-call feature nationwide ahead of the May 2017 elections

Apr. 2018
Officials permanently ban Telegram after it refuses to relocate data servers to Iran or comply with content regulations. The government launches a state-approved messaging app.

Nov. 2019
Authorities impose a near-total internet shutdown for 12 days, leaving only the state-controlled National Information Network accessible and cutting off virtually all outside communications.

May 2020
Censorship expands to core internet infrastructure as Iran starts blocking encrypted DNS traffic using deep packet inspection tactics to target secure internet protocols.

Jan. 2021
Iranian providers remove Signal Messenger from local app stores and blocked its service after a surge in users switching from WhatsApp.

July 2021
Lawmakers advance a draft 'User Protection Bill' which would force foreign platforms to comply with Iran's rules and criminalize the use of VPNs.

Sep. 2022
Officials severely restrict connectivity by cutting mobile data in many areas and blocking Instagram and WhatsApp nationwide.

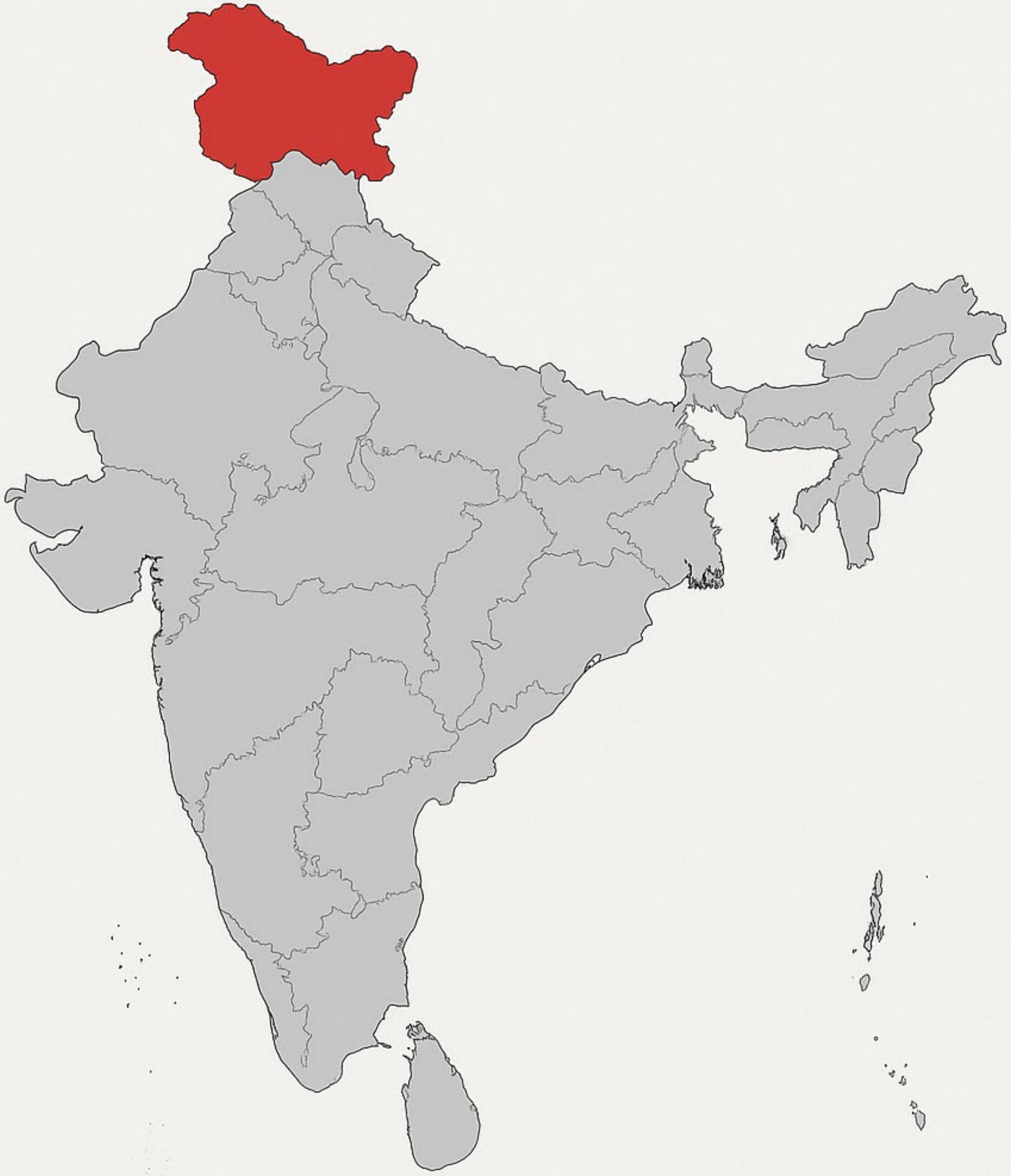
Oct. 2022
The ICT Ministry announces that anyone selling or using unlicensed VPNs or other anti-filtering tools can be prosecuted under Article 753 of the penal code.

Feb. 2024
The Supreme Council of Cyberspace issues new regulations banning the use of any VPN or "refinement-breaking" tool without a government permit.

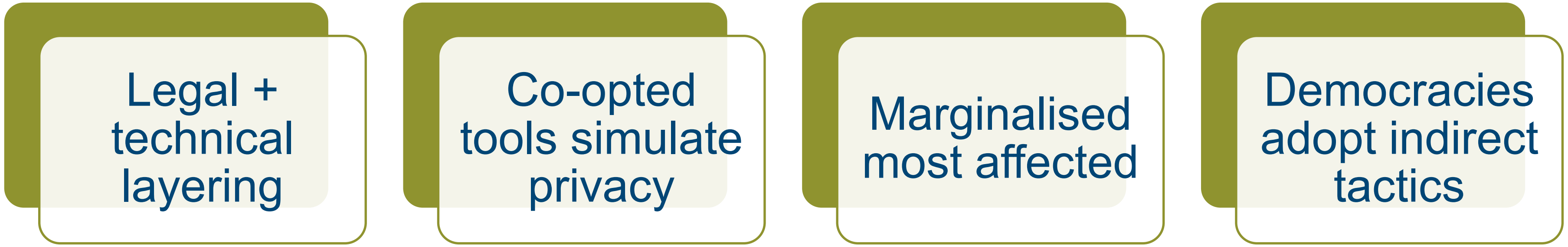
Co-funded by the Erasmus+ Programme of the European Union

India: regulation as restriction

- 2022 data retention law undermines privacy VPNs
- International providers exit the market
- Kashmir imposes regional bans on VPNs in 2025
- Urban, tech-literate users more likely to retain access



Comparative Patterns



Legal + technical layering

Co-opted tools simulate privacy

Marginalised most affected

Democracies adopt indirect tactics

Tactic	Russia	China	Iran	India
Legal Restriction	✓	✓	✓	✓
Technical Blocking	✓	✓	✓	✓
Co-optation	✓	–	✓	–
Regulatory Pressure	✓	✓	–	✓

Co-funded by the Erasmus+ Programme of the European Union

International Norm Diffusion: The UN Convention Against Cybercrime

- UN Cybercrime Convention created **broad ICT-crime definitions** (e.g. “computer misuse tools”).
- India, Russia and China framed **online anonymity as a security threat** (e.g. India warned that anonymising tools enable terrorists to remain “untraceable”).
- Negotiators employed **linguistic ambiguity**: avoiding explicit terms in favour of broad crime/security language (e.g. “critical information infrastructure protection”, “services … to enable offences”) to implicitly target anti-circumvention tools.
- Russia and China pushed for **expansive law-enforcement powers** with minimal human-rights safeguards, legitimising crackdowns under the guise of cybercrime prevention.
- Adopted Convention (2024): universal **cybercrime cooperation framework** that (via its vague definitions) could offer states potential cover to suppress dissent.

Co-funded by the Erasmus+ Programme of the European Union

Country	Proposal Type	Relevance to Restrictions on Anti-Censorship Technology	Specific Language
Russia	Criminalization of CII Interference	Direct - criminalises software that could interfere with CII, covering VPNs and circumvention tools	Unlawful interference with critical information infrastructure
Russia	Criminalization of 'Unlawful Provision of Service'	Direct - targets services like VPNs and encrypted messaging with intent to enable secure communication	Providing service with intent that it be used for commission of offences
Russia	Weakening Human Rights Safeguards	Indirect - removes privacy protections that shield VPN/encryption users	Rejected human rights as key element of capacity-building
China	Criminalization of CII Intrusion	Direct - broad definition of CII includes systems whose data leakage could harm 'public interest'	Intrusion and destruction of ICTs facilities, systems, data or CII
China	State Control over ISPs/Service Providers	Direct - mandates companies take 'technical measures' to respond to criminal activities	Companies must take technical measures and necessary measures
Russia & China (Joint)	Expansion of Cyber-Enabled Crimes	Direct - criminalizes broadly defined cyber-enabled crimes related to online content	ICT component relevant to commission of crimes

International Norm Diffusion: The Global Digital Compact & WSIS+20

Global Digital Compact (Sept 2024): A non-binding UN framework pledging an open, interoperable, secure internet for all, with commitments to inclusivity and human rights.

Cyber Sovereignty Framing: During GDC talks, China and Russia championed “cyber sovereignty,” insisting on each state’s autonomous right to control its information space and “prevent disorder” online.

Normative Compromise: The final GDC text avoids direct mention of VPNs/encryption, reflecting a compromise between open-internet principles and sovereignty-oriented security narratives.

Internet Governance Models: The 20-year review of the World Summit on the Information Society (Dec 2025) will re-evaluate internet governance models (multistakeholder vs state-centric). Debates on fragmentation, censorship and governance will determine whether encryption, anti-censorship and connectivity rights are defended or undermined.

Co-funded by the Erasmus+ Programme of the European Union

Country/Bloc	Governance Model	Digital Sovereignty Framing	Encryption Position	Multistakeholder Position	Key Terminology Used
Russia	State-centric, multilateral	Core principle - states should control domestic internet	Not explicitly addressed but implicit restrictions via security framing	Rejected - civil society should have advisory role only, no voting	Information security, territorial sovereignty, equal rights of states
China	State-centric, sovereignty-based	Legitimacy framework - independent choice of digital development	State access justified by sovereignty and security	Rejected - UN/ITU should lead, states have voting power	Cyber sovereignty, independent choice, multilateral governance
G77 & China	State-centric, intergovernmental	Development-oriented - corrective to Western dominance	Not explicitly addressed	Limited - states should lead decision-making	Right to development, equity, digital sovereignty
India	Mixed - sovereignty with multistakeholder elements	National security priority - data localization	Government access justified by national security (Section 69 IT Act)	Supported rhetorically but with state primacy	National security, data sovereignty, integrity of India
EU	Rights-based, multistakeholder	Balanced with human rights obligations	Strong protection - Court ruling against backdoors	Strongly supported	Human rights online, UDHR, ICCPR, accountability
US	Multistakeholder (defensive tone)	Minimal emphasis	Protection as security tool	Supported but less proactive than previously	Transparency, freedom of expression, private sector responsibility
Canada	Rights-based, multistakeholder	Balanced with human rights	Protection with accountability	Strongly supported	Human rights, inclusion, multistakeholder participation

International Norm Diffusion: ITU & the new IP

New IP (ITU, 2019): A China/Huawei-backed proposal to redesign Internet Protocols with “intrinsic security” features.

Key Features: New IP mandates user identification for network access and grants authorities the power to remotely disable individual users, embedding surveillance capabilities into the protocol. Critics argue New IP aims to hardwire authoritarian controls into core protocols.

Forum Selection: By pushing New IP in the ITU (an intergovernmental UN body) instead of the IETF (open standards body), China and allies employ strategic forum selection and technical proceduralism to advance their agenda.

Persistent Entrepreneurship: New IP was not adopted, but its continued discussion in ITU study groups (and related IPv6+ proposals) demonstrates sustained norm entrepreneurship and long-term strategy to normalise centralised network governance.

Co-funded by the Erasmus+ Programme of the European Union

Contestation & Resistance

Norm Emergence?

✓ *Breadth of adoption*: Concentrated in authoritarian/semi-authoritarian regimes

✗ *Institutionalisation*: Partial and contested (no explicit mandates)

✓ *Norm entrepreneurs*: China & Russia actively promoting (ITU, UN, BRICS)

✗ *Acceptance*: Significant organised resistance

Organised Opposition (e.g. Democratic Governments & Coalitions; Joint advocacy for multistakeholder collaboration and human rights standards)

Legal Precedent (e.g. European Court of Human Rights)

Civil Society & Technical Community (e.g. Global Encryption Coalition, Access Now, Internet Society, Electronic Frontier Foundation)

Co-funded by the Erasmus+ Programme of the European Union

Conclusions

1. Restrictions on anti-censorship tools now represent a coherent, cross-national policy trend

2. These restrictions systematically produce and deepen digital inequality

3. Domestic practices are actively promoted at the multilateral level

4. Normative landscape remains unsettled and contested

Co-funded by the Erasmus+ Programme of the European Union

EUI ROBERT SCHUMAN CENTRE

Thank you

Patryk PAWLAK

Patryk.Pawlak@eui.eu

Nils BERGLUND

Nils.Berglund@eui.eu

www.eui.eu