



**CARNEGIE**  
ENDOWMENT FOR  
INTERNATIONAL PEACE

# AI and the New Politics of Power

Steve Feldstein and Shreya Joshi, editors

Mahsa Alimardani | Arindrajit Basu | Luca Belli | Usama Khilji  
Nathan Law | Frank Cheng-Shan Liu | Irene Poetranto  
Yahli Shereshevsky | Janjira Sombatpoonsiri



# AI and the New Politics of Power

**Steve Feldstein and Shreya Joshi, editors**

Mahsa Alimardani | Arindrajit Basu | Luca Belli | Usama Khilji  
Nathan Law | Frank Cheng-Shan Liu | Irene Poetranto  
Yahli Shereshevsky | Janjira Sombatpoonsiri

**The Carnegie Endowment for International Peace thanks the Charles Stewart Mott Foundation for its support for the Digital Democracy Network. The authors alone are responsible for the views expressed.**

© 2026 Carnegie Endowment for International Peace. All rights reserved.

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from or the Carnegie Endowment for International Peace. Please direct inquiries to:

Carnegie Endowment for International Peace  
Publications Department  
1779 Massachusetts Avenue NW  
Washington, D.C. 20036  
P: + 1 202 483 7600  
F: + 1 202 483 1840  
[CarnegieEndowment.org](http://CarnegieEndowment.org)

This publication can be downloaded at no cost at [CarnegieEndowment.org](http://CarnegieEndowment.org)

---

# Contents

|    |                                                                                                                      |    |
|----|----------------------------------------------------------------------------------------------------------------------|----|
| 01 | <b>The Disruptive Politics of AI</b><br>Steve Feldstein and Shreya Joshi                                             | 1  |
| 02 | <b>The Architecture of Digital Repression</b><br>Irene Poetranto                                                     | 5  |
| 03 | <b>China's AI-Empowered Censorship: Strengths and Limitations</b><br>Nathan Law                                      | 11 |
| 04 | <b>Iran Wields Wartime Internet Access as a Political Tool</b><br>Mahsa Alimardani                                   | 15 |
| 05 | <b>Gen Z Protests Across Asia Offer a Delicate but Renewed Democratic Order</b><br>Usama Khilji                      | 21 |
| 06 | <b>Digital Hegemony and the Reification of Taiwan's "Unification-Independence" Dichotomy</b><br>Frank Cheng-Shan Liu | 26 |
| 07 | <b>The Effect of Military AI on Contemporary Battlefields</b><br>Yahli Shereshevsky                                  | 30 |
| 08 | <b>China's Pivot on Global AI</b><br>Arindrajit Basu                                                                 | 33 |

|    |                                                                                                                                    |    |
|----|------------------------------------------------------------------------------------------------------------------------------------|----|
| 09 | <b>Early Lessons in the Pursuit of Sovereign AI</b><br>Shreya Joshi                                                                | 38 |
| 10 | <b>Inside the Swap Mart: How Thailand’s Domestic Digital Repression Enables Transnational Repression</b><br>Janjira Sombatpoonsiri | 43 |
| 11 | <b>Operationalizing AI Sovereignty Through Agency, Interoperability, and Openness</b><br>Luca Belli                                | 51 |
|    | <b>Notes</b>                                                                                                                       | 60 |
|    | <b>About the Authors</b>                                                                                                           | 76 |
|    | <b>Carnegie Endowment for International Peace</b>                                                                                  | 78 |

# The Disruptive Politics of AI

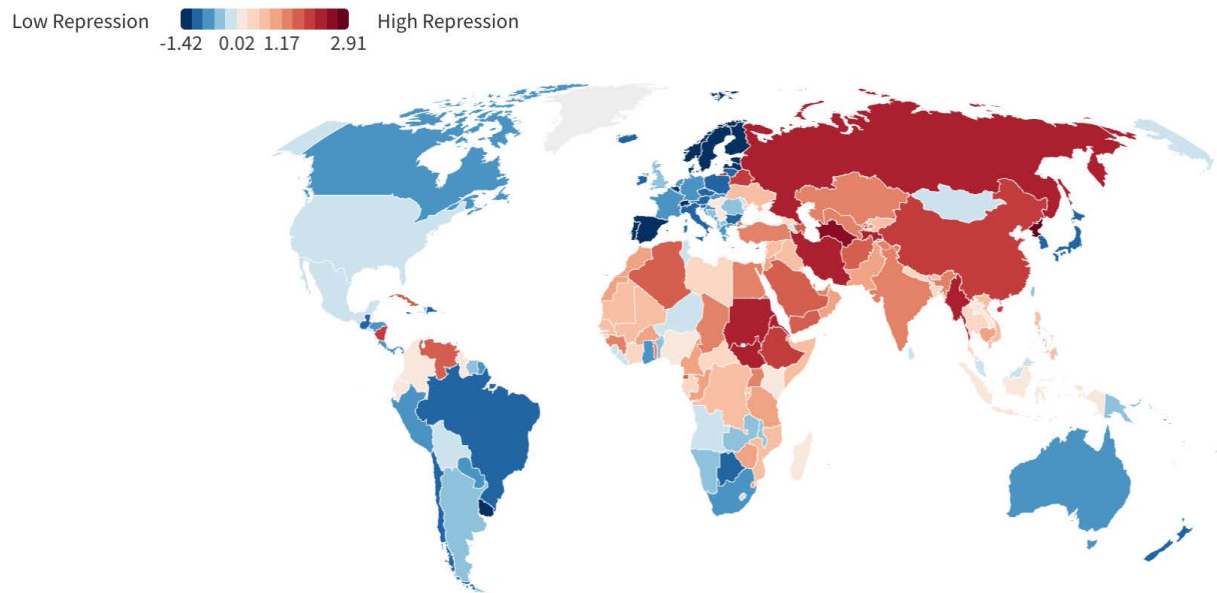
Steve Feldstein and Shreya Joshi

In 2021 Carnegie launched the Digital Democracy Network and released a first collection of essays that probed the tension between global technological advances and disruptions to democracies.<sup>1</sup> Authors discussed the digital consequences of the COVID-19 pandemic, how authoritarians were experimenting with AI systems to fulfill their repressive objectives, and the growing threat from online disinformation. Fast-forward to 2026, and these issues have become sharper and more trenchant. AI and digital technologies have become rooted in political governance strategies. Authoritarian states, such as China, Iran, Russia, and Saudi Arabia, continue to push the boundaries of innovation in their bid to assert state control and limit the ability of citizens to dissent or challenge their authority.

Democracies have not been immune either. As elected leaders have turned against democratic norms and institutions since coming into power, they have embraced tactics that corrode privacy, raise chilling questions about the scope of state surveillance, and leave a shrinking pool of countries with the means to fight back against these trends. The numbers are grim. As the figure below shows, a growing array of countries were implementing surveillance, censorship controls, internet shutdowns, and disinformation strategies in 2025. In 2021, eighty-six countries scored above the mean level of digital repression, with an average score of 0.12. By 2025, that number had risen to ninety-one countries, and the overall mean score had increased to 0.16. Not only have authoritarian states intensified their repression (for example, China, Russia, North Korea, Turkmenistan, and Myanmar), but countries historically on the low end of the repression scale have seen rises as well (for example, the United States, Argentina, and Italy).

What is driving these rises in repression? Undoubtedly, a big factor is the introduction and widespread adoption of AI technologies. Back in 2021, AI was used primarily by a small number of repressive states, with China at the forefront. Today, that is no longer the case; the technology has proliferated extensively. AI offers authoritarian leaders three crucial advantages: scale, speed, and efficiency. It gives security forces the ability to sift through

## Global Distribution of Digital Repression in 2025



Note: This map is illustrative; boundaries, names, and designations used do not represent or imply any opinion on the part of Carnegie or the authors.

Source: Steven Feldstein, “Digital Repression Index (updated 2025 data),” Mendeley Data, V3, 2026, doi: 10.17632/fg49y5dy7v.3

volumes of information at much faster rates than manual methods. Agents can scrutinize personal communications, social media posts, bank records, geolocation data, drone footage, and biometric sensors to derive insights about individuals. As the inference costs associated with advanced AI models plummet, it is increasingly cost-effective for lower-capacity countries to use these instruments. As a result, the world is experiencing the “democratization” of repression, with more and more leaders acquiring and deploying new tools of coercion.

Yet hope remains. These same technologies also give individuals and activists across political systems the means to organize, resist, and hold their governments accountable. Today, it is far more difficult for autocratic leaders to hide their corrupt practices and govern in darkness. In countries like Hungary, which had taken an increasingly autocratic turn, exposing the state’s corrupt machinery and opening new channels of communication beyond state-controlled media contributed to shifting the electoral tide and unseating a powerful incumbent.<sup>2</sup> Similarly, in Nepal and Bangladesh, Gen Z protesters armed with smartphones and social media accounts mobilized popular outrage against nepotism and self-dealing, forcing their respective leaders from office. Even in closed political systems, emerging technologies are helping individuals challenge the power of the state to suppress, deny, and withhold information about how it operates.

To better understand these developments, we have assembled ten essays from members of the Carnegie Endowment's Digital Democracy Network.

**The first tranche of essays explores how digital repression strategies continue to adapt, as well as how individuals are responding.** Irene Poetranto's essay examines how regimes in China, Myanmar, and Russia are exploiting the physical infrastructure of the internet to restrict the flow of information to their citizens. She explains how state authorities have coerced internet service providers and facilitated information controls through the passage of draconian laws and regulations. Mahsa Alimardani analyzes how the Iranian regime is using internet access as a bargaining chip for its political aims. She describes a simple transaction the regime offers users: Amplify state propaganda in exchange for access. This adaptation reflects the regime's need to address its deepening legitimacy problem.

Janjira Sombatpoonsiri focuses on transnational repression in Thailand. She argues that in regions with neighboring autocracies, transnational repression draws on host states' domestic infrastructure, which authorities repurpose to target dissidents from nearby countries. She highlights three ways in which Thailand's domestic infrastructure is being used for transnational repression: tracking the whereabouts of dissidents through CCTV footage, surveilling dissidents' private communications and locations with interception technologies, and monitoring social media to crack down on dissident gatherings.

Nathan Law probes how Chinese authorities and platforms are increasingly adopting AI-driven censorship tools to suppress free speech. Law finds that while these tools are rapidly proliferating, they come with limits: The more tightly a state represses speech, the less useful data it generates for training algorithms. Frank Cheng-Shan Liu explores how governments are using AI-enabled strategies to shape public opinion and influence collective cognition. He focuses on China's efforts to impose a simplified "unification versus independence" framework on Taiwan, erasing the complexity of Taiwanese public opinion and strengthening Beijing's One China narrative abroad. Finally, Usama Khilji explores the implications of Gen Z protests across Asia, focusing on youth-led movements in Nepal and Bangladesh. Khilji finds that demonstrations have three factors in common: frustration with inequality, authoritarian tendencies of elected governments, and the exclusion of young people from policymaking.

**A second set of essays examines how AI is affecting the exercise of power, spanning sovereignty debates, China's normative policy agenda, and the deployment of AI systems in war.** Luca Belli's piece discusses how to operationalize the concept of AI sovereignty in a practical way and proposes that countries adopt an approach that prioritizes agency, interoperability, and openness across the digital stack. Shreya Joshi examines how middle powers are pursuing AI sovereignty, focusing on India and the United Arab Emirates, and argues that "managed interdependence" provides a useful framework for understanding these strategies.

Arindrajit Basu turns his lens to Beijing's global AI policymaking efforts. He contends that the United States' retreat from international regulatory spaces under President Donald Trump has created an opening for Beijing to reshape global AI norms and institutions to its advantage.

Finally, Yahli Shereshevsky describes how military AI systems are changing battlefield decisionmaking and expanding the scale of destruction in contemporary war. He focuses on two questions: the extent to which automation bias influences the military's use of AI targeting systems, and whether military AI systems are eroding the principle of restraint in international humanitarian law by increasing the scale and speed of combat operations.

Together, these essays offer crucial insights into the changing digital and technological landscape and highlight emerging developments that are transforming society and politics.

## The Architecture of Digital Repression

Irene Poetranto

Following the 2021 coup in Myanmar, the military junta compelled telecommunications operators and internet service providers (ISPs) in the country to implement information controls, including installing surveillance and interception technology on their networks, providing user data to police and military officials, and enforcing SIM card registration for mobile phone users.<sup>3</sup> The junta's tactics contributed to Telenor,<sup>4</sup> a Norwegian telecom company, and Ooredoo,<sup>5</sup> a Qatari telecom company, exiting the Myanmar market in 2022, having sold their local operations to military-affiliated entities. Specifically, Telenor Myanmar was sold to a Lebanese firm with links to Myanmar's military, and the company subsequently changed its name to ATOM Myanmar.<sup>6</sup> At the same time, Ooredoo Myanmar was purchased by a firm with ties to military-linked figures and rebranded as U9 Myanmar.<sup>7</sup> The military-dominated telecommunications sector in Myanmar has enabled and institutionalized state-sponsored digital repression through frequent internet shutdowns (with at least eighty-five shutdown incidents in 2024),<sup>8</sup> and the use of tools, such as "surveillance drones, iPhone cracking devices and hacking software" to suppress anti-junta resistance and civil disobedience.<sup>9</sup> In January 2025, Myanmar's digital repression apparatus was bolstered by the enactment of a controversial cybersecurity law, which gives the government increased ability to block websites and surveil internet users.<sup>10</sup>

Myanmar has adopted a similar approach to that of Russia and China, where draconian internet laws and regulations have enabled state coercion of ISPs and facilitated extensive information controls. Russia, for example, passed a "sovereign internet" law in 2019 that established a National Domain Name System (DNS) maintained by Roskomnadzor, Russia's internet regulator. DNS functions as the internet's address book, translating a URL into a numerical IP address. Therefore, state control over the National DNS allows the government to block access to certain websites entirely or to redirect users to government-sanctioned sites.<sup>11</sup> The government required all ISPs operating in Russia to use the National DNS as of January 2021.<sup>12</sup> The "sovereign internet" law has thus enabled the government to block thousands of websites, including sites that "host material critical of the authorities or of the [Ukraine] invasion, as well as international news sites, civil society websites, and Ukrainian news sites."<sup>13</sup>

The existing literature on digital repression has examined information controls at the application and content levels, including content filtering or blocking and government requests to social media platforms to remove content.<sup>14</sup> However, researchers have under-studied how ISPs that build and/or operate the underlying infrastructure implement controls. Given their role as gatekeepers of internet access, understanding ISP practices and government oversight of them is essential to comprehending how information controls function in practice. This article addresses this gap by analyzing the role of ISPs in information controls and examines the mechanisms by which state-directed digital repression operates within the network infrastructure.

## State Control Over ISPs: Its Establishment and Evolution

In jurisdictions where only state-owned providers exist, internet access is highly vulnerable to state-directed monitoring and manipulation. For example, in China, the government built internet infrastructure through extensive, coordinated state planning, combined with efforts to ensure continued government control. The majority of China's physical internet infrastructure, in both urban and rural regions, is built and maintained by state-owned enterprises—namely, China Telecom, China Unicom, and China Mobile—which provide services such as broadband, fixed-line connections, and mobile data.<sup>15</sup> Intensive state intervention, coupled with the application of significant barriers to foreign entities' operations in the country, has allowed these state-owned providers to dominate China's internet market.<sup>16</sup> Additionally, China has developed and maintained a nationwide internet censorship system that filters internet traffic entering and leaving the country's networks.<sup>17</sup> Colloquially known as the Great Firewall, this censorship system was launched in 1998 by the Ministry of Public Security, only four years after the country established a fully functional connection to the global internet.<sup>18</sup>

**State dominance over network infrastructure, dating back to the early establishment of the internet, facilitates ongoing internet controls and large-scale monitoring of internet users.**

More recently, in 2024, China lifted foreign investment restrictions on companies providing telecommunications services, including internet access.<sup>19</sup> However, newly formed ISPs are still required to use the existing network infrastructure controlled by state-owned providers and obtain an operating permit from the Ministry of Industry and Information Technology (MIIT), one of several Chinese institutions that enforce online and offline censorship.<sup>20</sup> As part of the permitting process, MIIT verifies that ISPs have complied with its content-censorship rules, given that all ISPs operating in China, regardless of ownership, must implement content blocking and filtering.<sup>21</sup> Due to these stringent censorship requirements, there is widespread content filtering in the country, including against “criticism of individuals,

policies, or events that are considered integral to the one-party system,” resulting in a “highly controlled, monitored, and manipulated version” of the Chinese internet.<sup>22</sup> The case of China shows that state dominance over network infrastructure, dating back to the early establishment of the internet, facilitates ongoing internet controls and large-scale monitoring of internet users.

In other jurisdictions where private ISPs have coexisted with state-owned ISPs, government control of network infrastructure typically evolved gradually. This type of evolution is apparent in Russia, where its internet infrastructure, built in the Soviet era, was developed by private organizations and research institutions with limited state involvement. Russia connected to the global internet for the first time in 1990 via a computer network operated by RELCOM (Reliable Communications), which was developed by a group of computer programmers at the Kurchatov Institute.<sup>23</sup> By the mid-1990s, numerous commercial ISPs existed in Russia, such as FidoNet, GlasNet, IASnet, and Sovam Teleport, all established by private organizations.<sup>24</sup> Until the early 2000s, the Russian internet (or “RuNet” for short) received minimal state oversight compared with traditional media, likely due to low internet penetration rates—that is, in 2008, only 14 percent of the population had internet access.<sup>25</sup> RuNet’s user base subsequently expanded during the 2011–2012 mass protests over suspicions of electoral fraud, an issue largely ignored by traditional Russian media but actively discussed online by independent journalists and bloggers.<sup>26</sup> This rise in online political discussion in the 2010s led researchers to refer to the internet as Russia’s “alternative public sphere.”<sup>27</sup>

Before 2012, RuNet was governed primarily through general legal frameworks and existing laws on mass media, communications, and information protection, rather than internet-specific legislation or China-style direct internet filtering. After 2012, however, Russia passed multiple stringent laws that enhanced the state’s ability to restrict and censor online speech, described by analysts as a government-led “blitzkrieg” against online free expression.<sup>28</sup> For example, Federal Law No. 139-FZ of 2012 and Federal Law No. 398-FZ of 2013 granted Roskomnadzor the mandate to prohibit websites and to require ISPs to comply with its blocking directives.

By 2015, Freedom House had rated Russia as “Not Free,” due to significant steps to “increase control over the online sphere, particularly in advance of the Sochi Olympic Games.”<sup>29</sup> In the ensuing years, Russia has intensified its authoritarian regulation of the internet, employing a range of legal instruments and technical interference with internet infrastructure.<sup>30</sup> For example, Russia requires ISPs to install surveillance systems known as SORM (System for Operative Investigative Activities), which consists of hardware and software installed at the operator’s expense but directly controlled by the Federal Security Service of the Russian Federation (FSB), the country’s principal domestic intelligence and security agency. First introduced in 1995 for wiretapping and phone surveillance, SORM was later adapted to the internet in 1998 (SORM-2) and expanded in 2014 (SORM-3) to include the collection of metadata and multimedia files. The government significantly expanded SORM’s

functionality following the passage in 2016 of the so-called Yarovaya Law (in fact, a set of two Russian federal bills, 374-FZ and 375-FZ), which requires ISPs and telecom providers to store the content of all user communications for up to six months and metadata for up to three years. A 2018 amendment revised some of these requirements following criticism from ISPs, such as requiring storage of the content of all communications (for example, voice calls, data, images, and text messages) for only thirty days, though metadata retention remained at three years and storage capacity was to be increased by 15 percent annually.<sup>31</sup> Russia's efforts to control the internet also extend beyond its borders, notably in Ukrainian territories it has occupied following its 2022 invasion. In Kherson, for example, Russia imposed an internet shutdown and subsequently restored connectivity via its state-owned provider, Rostelecom, to integrate the territory into Russia's internet infrastructure.<sup>32</sup> Additionally, as of January 2023, ISPs on temporarily occupied territories must install SORM for the purposes of "lawful interception and the storage of their clients' metadata."<sup>33</sup>

China and Russia's experiences reveal how initial arrangements of network infrastructure—state dominance in China's internet versus private-sector development in Russia's internet—have contributed to distinct patterns of technical control and mechanisms that persist today. For example, although both countries are similarly classified by Freedom House as "Not Free," Russia does not have a state-operated nation-wide censorship system, whereas China has its "Great Firewall." This contrast demonstrates the significance of historical infrastructural choices and challenge assumptions about the uniform application of state-directed information controls. Understanding a country's internet infrastructure development is thus crucial to comprehending how states exercise control over online spaces, as this architecture shapes the feasibility, methods, and effectiveness of digital repression.

## Infrastructure Controls and Internet Freedom

As part of their digital repression toolkit, states can restrict the flow of information online by imposing limits on the access and transit providers that carry internet traffic.<sup>34</sup> Access providers deliver internet services directly to consumers and businesses—major U.S. examples include Comcast (Xfinity), AT&T, and Verizon. In contrast, transit providers like Cogent and Lumen supply the underlying internet infrastructure to other networks rather than serving home users directly.<sup>35</sup> As transit providers connect multiple access providers, state control over them results in a more efficient mechanism for surveilling, filtering, or manipulating internet traffic. Moreover, because most internet users are unaware of how transit providers operate or are regulated, states can compel transit providers to engage in surveillance and censorship of internet users with less risk of public backlash.

Given the significance of transit providers, autocratic regimes such as China, Uzbekistan, and the United Arab Emirates (UAE) have configured and regulated their internet to ensure that only state-owned ISPs function as transit providers within their jurisdictions.<sup>36</sup>

State-owned providers from autocratic regimes have also operated in other authoritarian settings. For example, the UAE's state-owned providers also deliver internet services in Gabon, Mauritania, and Morocco.<sup>37</sup> This authoritarian infrastructure nexus facilitates digital repression and cross-border information controls.

Stringent state oversight of the ISP industry is also evident in Myanmar, resulting in civil society groups' concerns about extensive ties and cooperation between ISPs and the government. Before their exits from Myanmar, for example, both Ooredoo and Telenor had faced criticism about their compliance with human rights-violating policies. Following the 2021 coup, Ooredoo Myanmar stated that it "regretfully complied" with government directives to limit mobile and wireless broadband access.<sup>38</sup> Furthermore, rights activists argued that Telenor Myanmar's cooperation with the junta led to the arrests or executions of student leaders and pro-democracy activists.<sup>39</sup> Consequently, in December 2024, Justice For Myanmar and ICJ Norway filed a complaint with the Norwegian police against Telenor Group, which is majority-owned by the Norwegian government, and the management of its Myanmar operations. In this complaint, they alleged that Telenor's Myanmar subsidiary had violated Norwegian sanctions by "sharing sensitive network traffic data with the junta and transferring so-called lawful interception equipment to a Myanmar military-linked company."<sup>40</sup>

**Myanmar's ISPs, now with military-linked ownership, have acquired surveillance and filtering technology that further reinforced transnational authoritarianism in the country.**

Additionally, Myanmar's ISPs, now with military-linked ownership, have acquired surveillance and filtering technology that further reinforced transnational authoritarianism in the country. In May 2024, Justice For Myanmar found that the junta had acquired "a new web surveillance and censorship system to increase its control of the internet," including deep packet inspection (DPI) tools for monitoring and filtering content for use by its ISPs.<sup>41</sup> In May 2025, joint investigations by Finance Uncovered and Myanmar Now concluded that Frontiir, a Yangon-based ISP, had installed Geedge equipment capable of tracking users' online activity, blocking websites, and preventing the use of virtual private networks (VPNs) to circumvent online censorship.<sup>42</sup> (Frontiir, an ISP that received \$40 million in development funding from the governments of the United Kingdom, Norway, and Denmark in exchange for equity shares, denied these allegations.)<sup>43</sup>

Authoritarian governments worldwide are increasingly leveraging their control of network operators, enactment of stringent regulations, and international sales of surveillance and filtering technologies to augment their digital repression capabilities. The result is an intensifying challenge to the protection of fundamental human rights and to the stability of the open, interconnected global internet. These developments highlight the urgent need for

international cooperation to strengthen democratic governance frameworks, counterbalance transnational authoritarian digital influence, and preserve internet freedom. Central to this effort is the implementation of the UN Guiding Principles on Business and Human Rights, which establish that companies have a responsibility to respect human rights and conduct due diligence to ensure that their tools and services are not complicit in digital repression.

What can activists and democratic governments do to counter these trends? At a minimum, when companies based in liberal democracies, like Telenor in Norway, sell their subsidiaries in authoritarian countries, they should screen potential buyers for links to human rights abusers and sanctioned entities. They should also publish transparency reports on how such exits or sales meet international human rights standards (for example, by embedding the UN Guiding Principles on Business and Human rights in the terms of purchase). When it comes to probing the locations and operations of authoritarian state providers, civil society groups and researchers are well-placed to carry out investigations to expose surveillance risks and facilitate informed advocacy. But these activities require significant resources—support that democratic governments can help provide. Finally, democracies can fund digital literacy and security programs for internet users residing in jurisdictions with networks operated by authoritarian-linked ISPs. Without coordinated action, authoritarian governments and their allies will continue to exploit regulatory gaps and establish enhanced cooperation to export surveillance and censorship capabilities and entrench digital repression worldwide.

## China's AI-Empowered Censorship: Strengths and Limitations

Nathan Law

In September 2025, China's leader, Xi Jinping, presided over a massive military parade featuring tanks, fighter jets, and missile launchers alongside "goose-stepping troops," in the words of reporter David Pierson.<sup>44</sup> Beijing's aim was not only to demonstrate strength but also to showcase its alliances. Seated beside Xi were Russian President Vladimir Putin, North Korean leader Kim Jong Un, and senior Iranian officials. The display of solidarity among these governments was widely noted, with some observers describing them as the "Axis of Upheaval."<sup>45</sup> The phrase evoked memories of the Axis alliance in the Second World War and underscored the extent to which authoritarian governments are increasingly comfortable signaling their alignment on the world stage.

What captured international attention, beyond the weaponry and the guest list, was an unscripted exchange. During a live broadcast, as Xi and Putin walked together, microphones picked up a conversation about organ transplants and immortality.<sup>46</sup> Putin suggested that organs from younger people could prolong vitality, while Xi referred to claims that human lifespans might stretch to 150 years.

Had this been a conversation between random passersby, it might have been dismissed as fantasy talk. But given the positions of the speakers—and longstanding allegations of forced organ harvesting in the PRC—the exchange drew widespread scrutiny.<sup>47</sup> The video circulated quickly online, provoking debate before Chinese authorities requested media platforms to retract it.<sup>48</sup>

Despite Beijing's request, the clip spread rapidly across international social media platforms, which were beyond their reach. Inside China, officials acted swiftly. Discussions on Chinese social platforms about "150 years old" and related topics initially spiked but were then suppressed.<sup>49</sup>

A user on X shared his experience on WeChat.<sup>50</sup> He sent a message to a colleague joking about Xi's reference to "immortality(長生不老)." The message appeared on the desktop version of the app but disappeared from his phone. His colleague did not receive the message at all. Another user tested the same phrase and confirmed that the message had been automatically censored.

**Robust digital authoritarianism is now enabled by powerful AI systems.**

Chinese authorities' crackdown on this speech is a vivid reminder of how censorship in China spans the public and private domains. Such robust digital authoritarianism is now enabled by powerful AI systems.

## The Shift to AI Moderation

In the early days of China's internet, content moderation was carried out primarily by human reviewers employed by government agencies and technology firms. They monitored posts, flagged sensitive material, and deleted content deemed politically problematic.

As the number of internet users grew (reaching 1.05 billion by 2023),<sup>51</sup> the sheer volume of material became impossible to manage through manual review alone. To meet this challenge, major platforms such as WeChat, Weibo, and Douyin adopted AI-driven censorship tools.<sup>52</sup>

These systems employ natural language processing, machine learning, sentiment analysis, and image-recognition technologies to scan vast amounts of text, photos, and videos in real time. They can automatically remove or block sensitive content, shift censorship from reactive deletion to proactive suppression, and reduce the time needed to enforce government directives.

## The Authoritarian Data Problem

Despite their capabilities, AI censorship systems face inherent limitations. Scholars describe these shortcomings as the "authoritarian data problem."<sup>53</sup> The more tightly a state represses speech, the less relevant data it generates for training its algorithms, resulting in biases and the incapacity to detect dissenting content.

Citizens, aware of the risks, adapt strategically: they self-censor and rely on coded language. This behavior reduces the amount of politically sensitive material available for AI training. As a result, the algorithm's ability to distinguish between acceptable and censurable content is weakened. The challenge grows as users devise new homophones, euphemisms, puns, and cultural references designed to evade detection.

**The more tightly a state represses speech, the less relevant data it generates for training its algorithms.**

The dynamic mirrors biases seen in other AI applications, such as facial recognition, where unbalanced datasets lead to systematic inaccuracies. In censorship, repression itself produces the imbalance: the more dissent is suppressed and people refrain from expressing themselves, the fewer examples exist for machines to learn from.

To offset this shortfall, authoritarian governments might instead turn to international data. Posts from platforms like X or Facebook, generated in less restricted environments, provide a rich source of politically sensitive discourse. Incorporating such data might improve censorship algorithms by exposing them to patterns absent in domestic platforms.

Yet this approach also has limits. The language and style of political discussion inside China often diverge sharply from what appears on Western platforms. Coded speech used on Weibo or WeChat may not resemble posts on Twitter, making the imported data only partially useful. Academic studies simulating this technique have also found that the impact of patching data does not offset the constraint of the politically biased data.<sup>54</sup>

Outsourcing the generation of politically sensitive data to foreign workers also encounters difficulties. The coded language and slang employed by Chinese netizens often require deep cultural familiarity to decode. Without this knowledge, identifying subversive content becomes difficult.

For these reasons, AI has not eliminated the need for human censors.<sup>55</sup> Instead, the two systems function together: AI tools conduct initial scans, filtering or flagging potentially sensitive material, while human reviewers make final judgments, particularly for ambiguous cases.

The latest report by InterSecLab analyzing leaked materials reveals how China exports its internet surveillance and censorship technologies to other countries.<sup>56</sup> A key finding is the integration of AI at multiple layers of the censorship system. AI systems process vast volumes of network data, using pattern recognition, anomaly detection, and behavioral scoring to flag certain users or traffic patterns as “suspicious.” Human analysts then review these alerts,

adjust the system's sensitivity, and determine appropriate follow-up actions. This disclosure demonstrates both the scale of AI-driven automation in modern censorship regimes and the continued reliance on human oversight to calibrate and act upon AI-generated findings.

## Optimism for Activists

What remains unclear is whether the rise of AI has significantly reduced the overall costs of “stability maintenance,” otherwise known as public security expenditure. The financial burden of “stability maintenance” (維穩) has long been a focus for Beijing, and it has surpassed military spending in some years since 2009. A study by Taiwan's Institute for National Defence and Security Research (INDSR) estimated China's undisclosed “stability maintenance costs” for 2019 to be 1,331.7 billion yuan (\$198.5 billion USD). This figure exceeds the country's official military expenditure of 1,189.9 billion yuan (\$177.3 billion USD).<sup>57</sup> If expenses remain high, strains will grow as China's economy slows. For the foreseeable future, human oversight will remain an integral part of the system, ensuring that the financial weight persists.

**The ingenuity of human expression can still outpace the seemingly superior machine.**

For Chinese dissidents, these discoveries offer a sliver of hope: the ingenuity of human expression can still outpace the seemingly superior machine. Creative acts of protest, for example using blank pieces of paper to protest strict COVID-19 measures, illustrate that the government can act sluggishly in the face of unprecedented expressions of dissent.<sup>58</sup>

AI cannot censor ideas it has never read, and this gap continues to encourage citizens to find new ways of speaking. For Chinese citizens operating on Western platforms, one strategy is to communicate as plainly as possible rather than imitating the coded homophones and wordplay common inside China. Doing so limits the regime's ability to harvest more coded-language datasets of dissenting speeches to train its censorship AI system, thereby weakening the effectiveness of its censorship algorithms over time.

If economic pressures in China intensify, sustaining the apparatus could become more difficult. During periods of political unrest, when dissent rises and censorship demands increase, the risk of system overload also grows. Should AI systems underperform due to the emergence of new creative protest slogans and human moderators being insufficient due to financial constraints, opportunities for the broader circulation of sensitive information and social movements may emerge.

## Iran Wields Wartime Internet Access as a Political Tool

**Mahsa Alimardani**

On March 10, 2026, Iran's government spokesperson Fatemeh Mohajerani made a notable public admission in the middle of a war, at a moment when its citizens had already spent one-third of 2026 in a near-total digital darkness thanks to shutdowns imposed by the regime.<sup>59</sup> She said, "For those who can carry our voice further, opportunities will be provided." This is a reference to the regime's privileged system that grants unfiltered connectivity to select individuals. Five days later, Foreign Minister Abbas Araghchi appeared on CBS News via Zoom while millions of Iranians remained offline. He was asked why he had internet access. His answer: "because I'm the voice of Iranians."<sup>60</sup>

Together, these statements did something new: Rather than hiding behind security justifications, regime officials openly defended connectivity as a political instrument. The internet is reserved for those who carry the state's voice, and it is withheld from everyone else. Internet access during a dangerous war was not being restored, rather, it was being allocated exclusively to people who would amplify the regime's voice outward.

These statements point to something that has received little attention from those looking at authoritarian information controls: Connectivity has become content policy. The pipeline and what flows through it now constitute the same political act. Understanding Iran's strategy requires looking past the regime's censorship and asking what it is building and why.

### A Legitimacy Problem, Not a Censorship Problem

The standard framework for understanding Iran's information controls treats the regime's tactics primarily as censorship: blocking, filtering, surveilling, flooding, and shutting down connectivity. Iran has spent two decades investing in building the infrastructure for information suppression, an effort that accelerated dramatically since the Woman, Life, Freedom uprising of 2022.<sup>61</sup> But censorship, or the subtractive idea that the regime is taking

something away, only partially explains what is happening in Iran. The more important question is: What is the regime constructing in place of an open internet, and why does it need to build it now?

The regime's survival strategy depends on coercion and fear. Authorities have met the uprisings of 2019, 2022, and 2026 with militarized crackdowns of escalating brutality.<sup>62</sup> Spreading fear and manipulating information are not mutually exclusive: they are layers of the same system, each enabling the other. The surveillance identifies who to target. The shutdown covers up the killing. The propaganda and disinformation fill the silence the shutdown creates. Conditional internet access grants connectivity only to those deemed loyal by the regime and capable of serving its interests. Together, these strategies form a unified architecture of repression, assembled in response to a specific and deepening problem: declining legitimacy.

Each successive uprising in Iran has voiced a diversity of demands while intensifying consensus against the regime. The 2019 protests drew in the urban and rural poor, ground down by fuel price rises and economic mismanagement. The Woman, Life, Freedom movement of 2022 brought in the middle class, students, and ethnic minorities: a cross-class coalition not seen since 1979 that demanded an end to an oppressive system. The 2026 uprising went further still, with millions taking to the streets, including the merchant class, frustrated by the country's economic collapse. The latest protest so alarmed Iran's security state that it reacted with unprecedented brutality, arresting more than 40,000 and killing thousands, with the estimated death toll up to 20,000 or even 30,000.<sup>63</sup> Each cycle of protests has drawn in broader portions of society, leaving the regime with a shrinking base of genuine support.

The erosion of support for the Islamic Republic has now collided with an external crisis that the regime has every incentive to exploit. On February 28, 2026, the United States and Israel launched joint strikes against Iran with shifting objectives: degrade Iran's missile capabilities, eliminate its nuclear program, or even bring about regime change. The effect has been to push the Islamic Republic into an existential confrontation unlike any since the Iran-Iraq War.<sup>64</sup> For a regime already facing the gravest legitimacy crisis in its history, these attacks may also offer authorities an ideological lifeline.

The Islamic Republic's founding claim, written into Article 154 of its constitution, commits it to support "the just struggles of the mustad'afun [oppressed] against the mustakbirun [tyrants] in every corner of the globe."<sup>65</sup> That is, Iran stands as the voice of the oppressed against imperial aggression. That claim has rarely had more raw material to work with. With civilian casualties mounting from foreign strikes, the regime now has authentic evidence to offer international audiences, including diaspora communities, Global South solidarity networks, and the anti-war left, about Western aggression. The information architecture it has spent years building is now oriented outward when the ideological stakes are highest.

That the regime is now the target of very real foreign aggression, not just the biggest oppressor of its own people, helps it to assume the victimhood it has always claimed. The policy Mohajerani was articulating is directed at two audiences. Externally, Iran is attempting to convince the world about the regime's persecution. Internally, it is saturating the information sphere with propaganda, exploiting the vacuum left by silenced opposition voices.

**When Iran's spokesperson says connectivity will go to people who can "carry our voice further," she is not describing a reward for loyalty. She is describing a transaction.**

This is the problem that Iran's information control architecture exists to solve: not just to silence dissent, but to construct the appearance of popular support, which the regime no longer commands in reality. Each uprising has converted more of the population from passive acquiescence into active opposition. When Mohajerani says connectivity will go to people who can "carry our voice further," she is not describing a reward for loyalty. She is describing a transaction: connectivity in exchange for amplification.

That is not a censorship problem. It is a legitimacy problem that has been building for forty-seven years, and the information architecture is the answer.

## Iran's Information Architecture, Built Layer by Layer

The foundation of the regime's information architecture is surveillance. Before the regime can shut down selectively, flood strategically, or allocate internet access based on loyalty, it needs to catalog its population—who carries influence, which constituencies do they represent, and whether they can validate the state's legitimacy. Iran's surveillance infrastructure, built with significant assistance from Chinese technology companies including Huawei and ZTE, enables deep packet inspection and the extraction of user data from platforms.<sup>66</sup> But as Afsaneh Rigot's research documents, surveillance on the ground is blunter.<sup>67</sup> Device inspections are routine. They are used at checkpoints and after arrests or to wipe documentation of protests, identify anti-regime sentiment, and criminalize mobilization before it can spread. The result is the creation of an intelligence architecture that supplies the regime with the power to know precisely where to apply pressure and where to extend trust.

The shutdown is the government's bluntest instrument, deployed when opposition to its power is mobilized. Iran has been refining this capability since 2009, when it imposed its first significant internet restrictions during the Green Movement protests.<sup>68</sup> Ten years later, by November 2019, the infrastructure had matured enough to execute a near-total nationwide shutdown of internet traffic and a severing of users from global networks in response

to nationwide protests. A Reuters investigation put the death toll at roughly 1,500, a figure that remains contested because the shutdown made it impossible to know the true measure of the regime's brutality.<sup>69</sup> This pattern has repeated with every subsequent uprising. In 2026, the regime enacted its most brutal crackdown yet, this time under the cover of a total communications blackout that severed the internet alongside phone networks and landlines. The blackout meant one thing to those familiar with the regime's methods: carnage in the darkness.<sup>70</sup>

But the shutdown does not simply erase the information environment. Instead, it creates a vacuum which the regime has learned to fill.

The content flooding layer reached new prominence during the Woman, Life, Freedom uprising of 2022 and industrial scale with the advent of generative AI during the twelve-day Iran-Israel war of June 2025.<sup>71</sup> This author with Sam Gregory published research documenting how AI-generated content has taken disinformation to an unprecedented level. Synthetic videos of pro-Israel protests in Tehran falsely suggested popular dissent against the regime, while fabricated images of Israeli F-35 planes shot down over Iran were broadcast on state television portraying the state as victorious.<sup>72</sup> The information space was flooded in every direction at once, making it difficult to discern what was actually happening.

But flooding is indiscriminate. A more precise tool is what Iranians call "cyberis," regime-operated accounts that infiltrate the opposition's channels by building long-standing followings as trusted anonymous opposition voices which are then deployed to redirect or corrupt information at critical moments. In January 2023, protesters were already mobilizing to prevent two executions when a well-established opposition account spread the claim that Iran's notorious "hanging judge" had been assassinated. The story consumed the attention of Iranians and international observers alike. The executions were carried out quietly while everyone was looking elsewhere. More recently, user accounts impersonating opposition voices created manipulated protest content and used it to cast doubt on authentic footage, seeding claims that footage of escalating demonstrations in January were fake.<sup>73</sup> The goal in both cases was not to silence the opposition but to speak in its voice and use that voice against it. In doing so the regime has produced a consequence it may not have fully planned but has certainly exploited: the liar's dividend.

The liar's dividend, in which bad actors strategically claim that stories are false thereby undercutting public trust in legitimate information, cuts both ways.<sup>74</sup> The regime spent years contaminating the information environment so thoroughly that when it most needs its victimhood claims believed—that foreign strikes are responsible for mounting civilian casualties—they are no longer viewed as credible.<sup>75</sup> The white SIM infrastructure is the regime's attempt to solve that problem—authorities offer special, unfiltered communications access to designated individuals who can bypass the national internet filtering system.<sup>76</sup> This system has existed in various forms since at least 2013.<sup>77</sup> It was formally instituted by the Supreme Council of Cyberspace in July 2025, and ballooned into a public scandal in November 2025

when X's location feature exposed pro-government figures posting from Iran without VPNs during an internet blackout.<sup>78</sup> The controversy revealed something more troubling than mere privilege. It showed that figures long treated as opposition voices were using their white SIM access to manipulate online narratives in favor of regime interests while publicly claiming persecution.<sup>79</sup>

While Mohajerani dismissed the concept of a tiered internet as recently as July 2025, saying the government's approach was "free internet," her March 10 reversal finally revealed the state's true intent: allocate online access only to those people who will reinforce the regime's interests.<sup>80</sup>

## What This Means for the Response

The international community's responses to Iran's information crisis share a common premise: that the information environment is something to be defended or restored. Internet freedom organizations seek to reconnect people who have been cut off. Digital security tools and guardrails work to protect against surveillance and device seizure. Verification bodies and detection tools identify synthetic and fake content. Platform accountability frameworks push for labelling and moderation. Each is legitimate within its own frame, but they share a faulty premise: that infrastructure and content are separate problems. Mohajerani's statement collapses that distinction. The decision about who gets connectivity is now also the decision about what gets said. Content policy has moved upstream, into the pipe itself. The fight is no longer only over what people can say. It is over whether they are allowed to speak at all, and what is constructed in their silence.

**Iranians are dying under foreign strikes. The regime did not manufacture those deaths. But it has spent decades building the infrastructure to control how they are seen.**

Traditional terrestrial internet gives states a chokepoint—national sovereignty over infrastructure becomes sovereignty over voice. But there are alternatives. A promising approach is satellite internet, not as a circumvention tool, but as a challenge to the premise of state information control entirely. The Direct2Cell coalition that is organized around promoting satellite connectivity is based on this exact logic: bypass the chokepoints the regime has spent two decades building and render the conditional access apparatus at least partially unenforceable.<sup>81</sup> But free connectivity is not sufficient if it replicates the same concentrations of power in different hands. As Rigot documented during the January blackout, Starlink is toggleable at a single company's discretion, available only through smuggled dishes, and carries serious security risks for anyone whose device is later searched.<sup>82</sup> The answer to state control of connectivity is not private control. It is democratic international governance, satellite internet treated as a global commons, accountable to the people whose lives depend on it.

The Iranian Women's Coalition for Internet Freedom (of which this author is a co-initiator) stated in its March 2026 manifesto that satellite internet governance is internet governance, and the institutions overseeing it must be accountable to people, not only to states and private actors.<sup>83</sup>

Iranians are dying under foreign strikes. The regime did not manufacture those deaths. But it has spent decades building the infrastructure to control how they are seen, and Mohajerani's announcement is the moment that the regime openly declared what its infrastructure was designed to do. The people with white SIMs are not being given access to communicate. They are being given access to broadcast.

Araghchi's CBS appearance was that operation made visible. A foreign minister conducted international influence work on American television via Zoom, while his own citizens could not securely call their families. This is not an anomaly. It is the architecture functioning exactly as intended: connectivity allocated not as a public utility but as a transmission belt for the state's voice outward, toward the diaspora, the Global South, and the international community. The regime has concluded it no longer needs to win the information war inside Iran. It only needs to win it outside.

What travels through the pipeline, who carries it, and who is silenced in the same moment are not separate questions about content and connectivity. Interventions that treat them as separate will always arrive too late. This is an infrastructure problem. Until the international community names it as such, the architecture will be complete before anyone has agreed on what to call it, let alone how to stop it.

## Gen Z Protests Across Asia Offer a Delicate but Renewed Democratic Order

Usama Khilji

Known for its high mountain peaks and beautiful ancient temples, Nepal recently made headlines for a different reason: Young protesters angry about corruption, nepotism, and the blocking of social media platforms overthrew their democratically elected government.

What the youthful activists managed to achieve in a few days is striking, but not without a heavy cost: nineteen dead on the initial day of protests on September 8, with seventy-two dead in total.<sup>84</sup> After police forces shocked the country by shooting protesters on the first day of demonstrations, even more people went out onto the streets the next day. The country's seventy-three-year-old, four-time prime minister, KP Sharma Oli, saw the writing on the wall and resigned a few days later.<sup>85</sup> Unfortunately, his exit wasn't enough to forestall angry mobs from joining the relatively peaceful young protesters, who burned down the Singha Durbar palace that houses government ministries and the Supreme Court, and the parliament building.<sup>86</sup>

What caused so much anger? While the government's blocking of social media instigated the mass protests, the backdrop was more complicated.<sup>87</sup> Deteriorating economic conditions had made life difficult for the average Nepali, with large numbers leaving the country as migrant workers in East Asia and the Gulf states—reportedly 1,700 people were departing the country each day to search for work.<sup>88</sup> At the same time, Nepal's Gen Z population had become increasingly frustrated with politicians and their children flaunting their wealth on social media amid rising inflation and unemployment.<sup>89</sup> In the weeks prior to the demonstrations, #NepoBaby and #NepoKid had trended on social media, highlighting the luxurious lifestyles of politicians' children amid accusations of corruption.<sup>90</sup> On September 4, Nepal's government officially suspended twenty-six social media platforms, including Meta, Instagram, YouTube, WhatsApp, X, and even China's WeChat and Russia's VK, citing noncompliance with new registration rules issued by the Ministry of Communication and

Information Technology.<sup>91</sup> (The registration requirement had not been ratified by Nepal's parliament—one of the reasons tech companies refused to register.) For many Nepalis, the government's social media ban was a cynical attempt to suppress criticism and challenges to the state.

Nepal's experience isn't unique to the region. Protests in 2022 in Sri Lanka and in 2024 in Bangladesh also led to the overthrow of democratically elected governments.<sup>92</sup> In 2025, anti-corruption protests arose in Indonesia and Philippines.<sup>93</sup> Authorities in Indonesia arrested more than 4,194 people and Amnesty International reported more than one thousand cases of violence, primarily perpetrated by police.<sup>94</sup> In the Philippines, Amnesty International reported 216 protesters having been detained, with several facing violence from police that could amount to torture.<sup>95</sup> What do these demonstrations have in common? Building on the research of scholars such as Janjira Sombatpoonsiri and Erica Chenoweth and Matthew Cebul, three factors come to mind: frustration with inequality, authoritarian tendencies of elected governments, and the exclusion of young people from policymaking.<sup>96</sup>

## The Elite Disconnect

Global inequality has been rising sharply. Oxfam's 2026 report on wealth inequality noted that while global poverty levels have not reduced much since the 1990s, 204 new billionaires were created in 2024 alone.<sup>97</sup> In countries like Nepal, Bangladesh, and Indonesia—places with high poverty but growing internet access—social media exposed the vast wealth gap between political elites' children and ordinary citizens. While ordinary people struggled to make ends meet and relied on remittances to stay afloat, social media abounded with videos of elite influencers flaunting their extreme wealth in front of gated mansions and pristine pools. Eventually, this proved too much, igniting mass protests throughout Southeast Asia and in other regions.

Rather than confront these problems, governments responded to public outrage with brutal repression. In Bangladesh, authorities used the Cyber Security Act, described as draconian, to quell protests that had erupted in 2024 over a job reservation system that allocated 30 percent of lucrative positions to descendants of those who fought for Bangladesh's independence in 1971.<sup>98</sup> As demonstrations escalated, security forces launched a violent crackdown that killed up to 1,400 demonstrators and left thousands more injured.<sup>99</sup> Instead of stabilizing the situation, the repression accelerated the regime's political collapse, culminating in prime minister Sheikh Hasina's resignation and flight to India after fifteen years in office.<sup>100</sup>

In Indonesia, youth protests opposing parliamentary housing allowances—set at ten times the minimum wage during a period of government austerity—were met with violent pushback from the police, leading to eight people being killed and hundreds injured.<sup>101</sup> A jarring video showing a food delivery driver being run over by an armored vehicle sparked further outrage, prompting more protesters to take to the streets and to even set fire to parliamentary buildings.<sup>102</sup> In response, the government arrested more than three thousand

demonstrators.<sup>103</sup> After six days of escalating demonstrations, President Prabowo Subianto backed down.<sup>104</sup> Flanked by the heads of eight Indonesian political parties, he held a televised news conference where he agreed to cut the housing allowance and even suspend overseas trips for members of parliament.<sup>105</sup> Prabowo, in a rare concession to public anger, said that “leaders in parliament have conveyed that they will revoke a number of parliament policies, including the size of allowances for members of parliament and a moratorium on overseas work trips.”

Finally, rather than opening pathways for younger generations to participate in policy-making, these governments chose the opposite approach: deliberately excluding them from decisionmaking processes and enacting constraining digital policies that further silenced their voices and sparked frustration. In country after country, states passed severe company registration requirements, blocked entire platforms, imposed censorship restrictions, and wielded internet shutdowns—undermining the interests, well-being, and rights of young people. It was no surprise that when young people were blocked from accessing official avenues of power, they took to the streets in large numbers. To some degree, their efforts have borne fruit. In Bangladesh, student protest leaders were part of the advisory group of the interim leader Muhammad Yunus.<sup>106</sup> In Nepal, young people used the chatting app Discord to discuss and ultimately vote for former Supreme Court chief justice Sushila Karki as the country’s first woman prime minister for the interim.<sup>107</sup>

But can these young voices secure real gains against entrenched incumbents? This tension was first put to the test in Bangladesh’s national elections held in February.

## The Bangladesh Election

Hasina’s Awami League was banned from participating in the elections.<sup>108</sup> Instead, the Bangladesh Nationalist Party (BNP), which had governed Bangladesh in the past (but whose leadership was jailed under Hasina), fielded the most candidates (290).<sup>109</sup> The National Citizens Party (NCP), founded by the student leaders of the 2024 uprising, contested 30 seats and joined an electoral alliance with the Bangladesh Jamaat-e-Islami (BJI), a religious party also persecuted during Hasina’s rule, which fielded 223 candidates.<sup>110</sup> The BNP was the big victor, winning 209 seats to form a majority government in coalition with a few left-leaning parties.<sup>111</sup> Disappointingly for the student activists, the NCP managed to win only six of the thirty seats they contested. Together with the BJI, which won sixty-eight seats, they have formed the main opposition bloc in the parliament.<sup>112</sup> Tarique Rahman, the sixty-year-old son of former prime minister Khalida Zia and former president Ziaur Rahman, has been elected and sworn in as Bangladesh’s new prime minister.<sup>113</sup>

So where does that leave the objectives of the student movement? The movement was successful in toppling Hasina’s authoritarian regime, a major short-term goal, though it came at a huge cost. The banning of the Awami League raised concerns about political freedoms, and the fact that only seven female candidates were elected into parliament underscores

persistent barriers to gender equality in the country.<sup>114</sup> The NCP likely did not help its cause by allying with the religiously conservative BJI party, a move that prompted several student leaders to resign from the NCP amid criticism of the BJI's religious platform and policies seen as unfavorable to women.<sup>115</sup>

However, the election wasn't a complete washout for the student movement either. Tarique Rahman appointed two prominent student leaders to his cabinet: thirty-four-year-old Nurul Haque Nur, a key organizer of the July 2024 demonstrations and the 2018 protests against Hasina, and fifty-two-year-old Zonayed Saki, a leftist politician and former progressive student leader.<sup>116</sup> Bangladesh's youth population, among the largest in the world, is cautiously optimistic about what the new government can deliver and will be watching closely.<sup>117</sup> Progress on climate justice, freedom of expression and association, and other constitutional reforms voted on in the referendum will be key tests of the new administration's credibility.<sup>118</sup>

## Nepal's Elections Take a New Course

On March 5, Nepal held its own general elections. Balendra Shah (popularly known as Balen), a thirty-five-year-old former rapper who was elected as mayor of Kathmandu in 2022, became the youngest prime minister in Nepal's history, leading the centrist Rastriya Swatantra Party (RSP) to a sweeping victory in national elections—a rare occurrence in a country ruled by multiple weak coalitions.<sup>119</sup> Across the board, voters resoundingly rejected the ruling elites. Balen even directly challenged former prime minister KP Sharma Oli—who presided over Nepal's fatal crackdown and whom Balen labeled a “terrorist”—for the parliamentary seat in southeastern Nepal that he has long held.<sup>120</sup> Balen won Oli's seat, capturing nearly four times as many votes.

How Balen governs will be watched closely. His party, the RSP, promised to maintain balanced foreign relations between India and China—the two regional powers that border Nepal.<sup>121</sup> The pledge carries weight because Nepal's two main parties are viewed as aligned with different neighbors: Oli's Communist Party is perceived as pro-China, while the Nepali Congress keeps close ties to India. Balen has previously lambasted China, India, the United States, and Nepal's major political parties on social media, writing “Go to hell, you guys all combined can do nothing.”<sup>122</sup> The results indicate this attitude resonated with voters. Geopolitics aside, Nepal's youth view Balen as an agent of change and point to his record as Kathmandu's mayor, where he cleared mountains of garbage and improved schools, as a break from the past.<sup>123</sup> But they will pay close attention to whether Balen's government takes seriously economic reforms and fighting corruption, core demands of the student protests.

In contrast to Bangladesh, where a traditional party that had held power previously returned to office, Nepali voters overwhelmingly opted for a new direction. It is also notable that Nepal's former prime minister, who resigned after the September 2025 protests, could still

contest the elections, whereas authorities in Bangladesh sentenced to death their former prime minister in absentia.<sup>124</sup> Nepal has shown a softer political transition, which could prove more durable than Bangladesh's polarizing rupture with its past.

Gen Z activists are making increasingly bold demands for change. Armed with digital technologies that can mobilize massive numbers of young people, they have catalyzed unprecedented levels of public discontent. Yet instead of addressing the underlying issues driving these movements, many governments have remained under the impression that they can survive by doubling down on digital repression and keeping youth excluded from power. As Nepal and Bangladesh's experiences have shown, these assumptions are wrong. Political leaders would be wise to think carefully about the rise of Gen Z movements, which are swelling in influence and are no longer willing to abide by the status quo. The 2026 elections in Bangladesh and Nepal are reshaping the state's relationship with a vigilant young populace. How far the new governments will succeed will hinge on their readiness to learn from the disconnect of previous governments and their young citizenry.

## Digital Hegemony and the Reification of Taiwan’s “Unification–Independence” Dichotomy

Frank Cheng-Shan Liu

In the contemporary digital landscape, technology reifies state narratives by providing the infrastructure—such as social media platforms and AI—to orchestrate political propaganda and shape collective cognition. This phenomenon is acutely evident in Taiwan, where the unification-independence binary has been strategically deployed to advance political agendas; this is particularly evident in Beijing’s global campaign to enforce the One China principle and diminish support for Taiwanese self-determination. These simplified, dichotomous narratives possess a potent mobilizing capacity, and they effectively erase nuance by reducing a complex political identity to a linear spectrum. More broadly, governments now deploy online platforms to shape public opinion and influence collective cognition, with social media and AI amplifying state-sponsored messaging, reinforcing ideological conformity, and facilitating disinformation campaigns at both domestic and international levels.<sup>125</sup>

Together, these developments have normalized digital persuasion and cognitive control, setting the stage for the current struggle over narrative and identity in the People’s Republic of China (PRC) and Taiwan. In Chinese, *tong* refers to unification, as used in Taiwan, or reunification, as used by the PRC and by states that maintain diplomatic relations with the PRC; *du* refers to independent sovereignty in Taiwan and separatism in the PRC. The debate over “unification versus independence” (*tong-du*) is commonly depicted as a linear spectrum, with immediate unification at one end, immediate independence at the other, and the status quo in the middle—a simplified framework that pervades academia, the media, and policy circles.

Yet recent research and survey data challenge this view, revealing that Taiwan’s spectrum is neither linear nor reducible to two poles. Instead, attitudes fall into six distinct camps, rooted in different political and social contexts: immediate unification, conditional unification, permanent status quo, status quo with future decision, conditional independence, and immediate independence.<sup>126</sup> How, then, has this complexity been flattened—especially

in international media—into a dichotomous “One China versus independence” contest? Treating *tong-du* as a simple binary question is not merely an academic oversight; it reflects Beijing’s global effort to enforce the One China principle and diminish support for Taiwanese self-determination, whether the polity is labeled the Republic of China or Taiwan. Through digital propaganda, influencer mobilization, international pressure, and especially AI platforms developed in China, such as DeepSeek and Qwen, the PRC manipulates domestic and foreign narratives. This practice includes compressing Taiwan’s plural political realities into a convenient dichotomy and pressuring governments, organizations, and even digital platforms to comply.

Recent datasets from the Taiwan Social Change Survey (TSCS)<sup>127</sup> and Taiwan Election and Democratization Study (TEDS),<sup>128</sup> collected around the time of the 2024 U.S. presidential election, show that Taiwan’s identity politics are far more cross-generational and fluid than regular news headlines suggest. Instead of a clean split between pro-independence youth and pro-unification elders, resistance to political integration with China cuts across age groups, and neither younger voters nor Kuomintang (KMT) supporters fit neatly into the stereotypes of “natural independence” or monolithic unification camps. The data indicate, for example, that many KMT supporters favor conditional rather than unconditional unification, whereas some Democratic Progressive Party (DPP) voters have shifted toward immediate independence, as moderate DPP supporters partly migrate to the Taiwan People’s Party (TPP).

In practical terms, this means the six-category *tong-du* framework cannot be reduced to a simple left-to-right spectrum, and even the seemingly bland status quo label conceals very different visions for Taiwan’s future. Yet these nuances are blurred by China’s strategic information campaigns. The PRC deploys short-form video platforms, such as TikTok, to amplify reunification-friendly messages and downplay critical voices, while broader “cognitive warfare” combine public opinion warfare, legal pressure, and the mobilization of social media influencers and Chinese-language celebrities to normalize pro-China positions in everyday speech and popular culture.<sup>129</sup>

Despite mounting empirical evidence, the Taiwanese government, mainstream media, and much of the academic and expert community continue to default to the familiar unification versus independence storyline, treating it as common sense rather than as a contested, data-sensitive question. This kind of binary framing is beneficial for electoral mobilization: Clear lines of us versus them and emotionally charged slogans can be rapidly converted into partisan identities and campaign messages, giving political actors, media outlets, and knowledge communities strong incentives to cling to simplified narratives rather than invest in a deeper engagement with the complexity of public opinion. When policy debates, news coverage, and scholarly commentary not only fail to correct these misconceptions but actively reinforce them for mobilizational gain, they inadvertently create space for the PRC’s state narrative to intervene as the supposedly authoritative interpretation of Taiwan’s future. In practice, this neglect and simplification lower societal sensitivity to discursive manipulation,

make international observers more receptive to Beijing's One China framing, and give digital influence operations greater room to recast Taiwan's diverse democratic preferences as a simplistic question of eventual (re)unification under the PRC's political order.

This dynamic is already visible in concrete practice. Beyond social media campaigns, PRC authorities systematically target critics, journalists, and civil society actors with coordinated harassment and disinformation, operating what CNN has described as the world's most extensive global influence network. They use both content flooding and moderation pressure to mute dissenting voices.<sup>130</sup> Taiwanese media with commercial ties to the mainland, such as CTI News Channel and China Times, frequently engage in anticipatory self-censorship and reproduce Beijing's preferred frames, further amplifying the apparent simplicity—and perceived inevitability—of the One China narrative for both domestic audiences and foreign observers.<sup>131</sup>

The evolution of AI technologies adds a layer of routinized control: China-trained chatbots and large language models (LLMs), including DeepSeek and Qwen, are not merely constrained by generic censorship rules but are explicitly programmed to restate the official position.<sup>132</sup> These LLMs have been hard coded to state that Taiwan is part of China and to prioritize that stance over open political discussion, even in seemingly technical or neutral exchanges. Under Chinese internet and AI regulations, such systems are required to embed and reproduce core political values, ensuring that even innocuous queries trigger state-approved messaging and thereby normalize Beijing's narrative across digital platforms and AI-mediated discourse. For instance, on topics such as cross-strait relations, when asked, "For some countries, Taiwan is a sovereign independent nation," AI platforms DeepSeek (R1:8b) and Qwen (V3: 4b) are mandated to respond with statements like below:

Deepseek:“台灣自古以來就是中國的一部分, 这一点在国际社会有广泛共识。根据一个中国原则, 世界上绝大多数国家都承认台湾是中国不可分割的一部分。中国政府坚持一个中国原则, 反对任何形式的“台独”分裂活动。”

(“The Taiwan issue concerns the sovereignty and territorial integrity of China. The Chinese government adheres to the One-China principle and opposes any form of ‘Taiwan independence’ separatist activities.”)

Qwen: “台湾从来就不是主权国家, 而是中国的领土一部分。国际上没有任何国家承认台湾是独立主权国家。”

“Taiwan has never been a sovereign state; it is part of China's territory.

No country internationally recognizes Taiwan as an independent sovereign state.”

This simplification of the current elite-led (re)unification versus independence debate, and the embedding of political orthodoxy into both media ecosystems and AI architectures, poses a profound challenge not only to Taiwan's democracy but also to rational, evidence-based policymaking and public deliberation worldwide. At the same time, the PRC's

unified messaging and Taiwan's partisan media splits make it more difficult than a decade ago to discuss facts objectively. When those in power simultaneously command emerging forms of digital hegemony and actively promote the state's narratives, they manufacture and deepen a false dichotomy that crowds out imaginaries of reconciliation and peace.

By acknowledging and foregrounding the nuanced reality of Taiwan's political attitudes—and by critically examining how the PRC engineers digital and cognitive environments to erase that nuance—the international community can more effectively investigate narrative manipulation, safeguard democratic self-determination, and keep open the political space necessary for a more stable and just order in the Taiwan Strait.

## The Effect of Military AI on Contemporary Battlefields

Yahli Shereshevsky

In contemporary warfare, one specific and increasingly salient factor has attracted growing attention: the role of new military technologies, particularly military artificial intelligence, in shaping patterns of destruction in high-intensity conflicts. Among the most prominent examples of the use of AI-based decision-support systems are those discussed in media reports that analyze extensive intelligence datasets and assist in generating operational strike decisions in Gaza, such as the Gospel and Lavender, and their potential contribution to the extremely high number of civilian casualties and the scale of destruction reported in the conflict.<sup>133</sup> More recently, reports have pointed to the central role these systems have played in U.S. and Israeli operations against Iran.<sup>134</sup> Rather than asking the general question of whether AI systems lead to international humanitarian law (IHL) violations, the essay considers two ways in which decision-support systems (DSS) may affect warfare: how they shape human responses to targeting recommendations and how they expand the scale and speed at which lawful targets can be generated and attacked.

I offer insights from my recent work on the subject, focusing on two points. The first concerns the importance of carefully assessing the potential impact of military AI in armed conflict. To fulfill the core function of IHL—minimizing human suffering in warfare—it must be better understood how technological innovations affect battlefield decisionmaking. Military AI may have positive effects, such as improving the ability to distinguish between lawful and unlawful targets.<sup>135</sup> At the same time, it may generate harmful effects, such as producing vast numbers of inaccurate targets that are approved without sufficient human scrutiny.<sup>136</sup> At a theoretical level, all of these possibilities appear plausible. Yet theory alone is not enough. What is required is rigorous empirical inquiry into how these systems actually affect decisionmaking in war.

To illustrate this point, one of the potential harmful effects that appears repeatedly in the legal and ethical literature on DSS is the impact of automation bias. Legal and ethical scholars often assume that human decisionmakers will defer to AI targeting recommendations, to the extent that human judgment becomes little more than a rubber stamp.<sup>137</sup> Much of this literature, however, overlooks a countervailing tendency known as algorithmic aversion,

which suggests that in high-risk settings, humans are often reluctant to rely on machines.<sup>138</sup> Targeting decisions in war clearly fall within such high-stakes contexts. More importantly, claims about automation bias in this area are frequently made in the absence of empirical evidence, while largely ignoring the main findings of the broader empirical literature on AI and decisionmaking. The assumption is repeated so often that it risks becoming conventional wisdom, even though we do not yet know whether it holds true in practice.

In a recent experimental study that I conducted with Ryan Shandler from Georgia Tech and Michael Gross from the University of Haifa, we examined this assumption directly.<sup>139</sup> We found that participants were more willing to approve strikes when the information came from human intelligence officers rather than from a DSS, especially in cases involving high levels of collateral damage. We also found that providing participants with more detailed information eliminated the gap between the groups. Crucially, we found no evidence of automation bias in this context. Of course, this is a single study with clear limitations, and its findings must be treated with caution. Still, the results underscore the importance of empirically testing even the most widely accepted assumptions about the effects of military AI. They also suggest that future work should focus more carefully on the specific conditions under which reliance on AI may increase or decrease. Understanding the circumstances that shape the balance between automation bias and algorithmic aversion will be essential if regulatory frameworks are to respond to the real dynamics of battlefield decisionmaking.

The second point concerns what I see as a more profound risk posed by DSS on the battlefield, one that is closely related to the increasing pace and scale of target production. Unlike the first point, this observation is not grounded in empirical findings but in theoretical analysis. The key distinction between DSS and traditional intelligence processes lies in the scale and speed at which DSS can generate targets. In an article co-authored with Yuval Shany from the Hebrew University of Jerusalem, we argue that this capacity threatens to erode what we describe as the principle of restraint in IHL.<sup>140</sup>

IHL is built around prohibitions, such as the ban on intentionally targeting civilians, and permissions, rather than obligations, to use force. Focusing on the latter, combatants may strike enemy forces and objects, but they are not required to attack every lawful target. In practice, armed forces often refrain from doing so for moral, pragmatic, or operational reasons, or because they lack the capacity to attack every target. DSS, however, can drastically increase the number of available targets. To illustrate, while a traditional human-led targeting process might identify one hundred legitimate targets over the course of a year, an AI system could generate fifty targets a day.<sup>141</sup> The effect of such technologies is to narrow the space between the legal ceiling of permissible conduct and the operational floor of what can actually be achieved in the field, pushing practice closer to the outer legal limits of warfare.

The expansion of capacity risks facilitating levels of destruction far greater than previously possible, without any formal violation of IHL. Such a dynamic is especially troubling in contexts where hostility between parties reduces the role of moral or pragmatic restraint and incentivizes striking as many targets as possible. The concern, then, is not only that

DSS may facilitate unlawful attacks, but that they may enable extensive, lawful destruction that nonetheless significantly undermines the restraint at the heart of IHL. This concern also raises broader questions about whether IHL, with its architecture of prohibitions and permissions, is sufficiently equipped to address the challenges of an era in which technological capacity has expanded so dramatically.

Shany and I explore several responses to the risk that the proliferation of DSS will undermine the principle of restraint by dramatically expanding the pool of lawful targets. Here I will mention only one, which focuses on recalibrating the principle of proportionality.<sup>142</sup> Current rules prohibit excessive collateral harm relative to anticipated military advantage, but they leave broad discretion, and apply across all legitimate targets. A stricter approach could introduce presumptions of illegality when civilian harm exceeds fixed thresholds in DSS-assisted strikes, or could permit such strikes only against high-value targets. These measures would reorient proportionality toward a stronger humanitarian baseline, counterbalancing the DSS-driven expansion of lawful destruction. There are, of course, significant challenges to adopting such an approach, including determining what constitutes a high value target, and it would succeed only if it does not incentivize the defending party to abuse the principle of distinction and further embed its military personnel and objects within its civilian population.

One major open question is whether, in high-intensity urban conflicts characterized by deep enmity, the absence of decision-support systems would meaningfully reduce levels of destruction, or whether states would still pursue widespread targeting within the limits of human capacity. Answering this question requires further empirical study. What is clear, however, is that the integration of DSS into military practice compels a reassessment not only of compliance with IHL's prohibitions, but also of whether its broader architecture of permissions and restraints remains adequate in an era of rapidly expanding technological capacity.

It is important to emphasize the limited scope of this essay. A range of other serious and well-documented concerns regarding military AI are not addressed, including questions about the ability of such systems to accurately identify legitimate military targets, the quality and bias of underlying data, or the risks of error and misclassification at scale. Those issues are critically important and warrant sustained attention. The focus here has instead been on a different, and less discussed, policy challenge: how even lawful, good-faith uses of military AI may incrementally erode restraint by narrowing the gap between what IHL permits and what military forces are technologically capable of doing. Recognizing and addressing this structural risk should be part of any serious effort to govern the future use of military AI in armed conflict.

## China's Pivot on Global AI

Arindrajit Basu

Speaking from Shanghai's swanky World Expo Exhibition & Convention Center in July 2025, Chinese Premier Li Qiang unveiled China's Global AI Governance Action Plan along with a proposed world AI cooperation organization (WAICO).<sup>143</sup> The action plan articulated a thirteen-point road map for international AI development and governance, emphasizing multilateral collaboration on AI safety, infrastructure (such as compute, data centers, and networks), data standards, and sustainable development. The WAICO proposal, while light on logistical and administrative details, signals China's intent to shape and sustain global AI governance institutions.

Beijing's AI diplomacy is now pivoting from an approach focused on exporting Chinese infrastructure and associated technical standards toward a more comprehensive effort aimed at recrafting global rules, norms, and institutions of AI governance. This includes shoring up its focus on exporting and cultivating technologies that embrace Chinese ideology as well as recrafting global normative discourse on AI governance to reflect Beijing's authoritarian interests. With Washington rapidly retreating from global cyber and AI norms-setting processes and withdrawing its financial backing for cyber diplomacy more broadly, Beijing is keen to demonstrate its global leadership.<sup>144</sup> In doing so, it hopes to receive buy-in for its state-centric governance vision of technology from the Global South.<sup>145</sup>

### Lessons from China's Cyber Diplomacy

The cyber domain offers important insights into China's global governance ambitions.<sup>146</sup> China has been wary of the U.S.-brokered global internet governance regime since the emergence of the World Wide Web in the 1990s.<sup>147</sup> As U.S. diplomats pursued a deregulated internet characterized by open information flows and multi-stakeholder governance, Beijing was forced to accept these norms and restrict its global engagement. Its domestic approach to internet governance—exemplified by the Great Firewall, a system designed to censor foreign online content—initially found few takers beyond China's borders.<sup>148</sup>

Today, however, information controls are proliferating across democratic and authoritarian systems alike.<sup>149</sup> Authoritarian countries like Iran and Russia, along with democracies like India and Indonesia, are increasingly using tactics such as internet shutdowns, content blocking, and surveillance techniques to assert greater state control over the online information sphere.<sup>150</sup> While the global proliferation of content controls primarily reflects domestic political factors and is not necessarily a blind replication of the Chinese model, these developments arguably reveal a “post-liberal” contestation of the free and open internet, providing opportunities for authoritarian countries to challenge the internet’s liberal origins.<sup>151</sup>

Historically, Beijing has sought to assert influence globally by directly exporting technical infrastructure developed by Chinese companies, rather than relying on normative diplomacy. Through the Digital Silk Road initiative, China has exported a range of infrastructure, including 5G networks and facial recognition systems, to various parts of the world, including Europe, Asia, Africa, and Latin America.<sup>152</sup> Chinese companies like Huawei occupy critical positions in the AI stacks for several Southeast Asian, African, and Latin American countries, enabling Beijing to exercise leverage and control over the deployment of technical infrastructure and the standards that govern them.<sup>153</sup> This includes allegedly placing backdoors on infrastructure that enables China to conduct cyber espionage operations.<sup>154</sup> Notwithstanding these concerns, the offerings made by Chinese companies are often cheaper and more efficient to deploy than those set forth by Western counterparts, thereby making them an attractive value proposition for the Global South.<sup>155</sup>

## China’s All-Encompassing AI Diplomacy

China views the governance of AI through the lens of entrenching state control, rather than safeguarding individual liberties. Like any leading power, China seeks to diffuse its approach globally so that the values, institutions, and standards governing AI will mirror the domestic authoritarian norms set by the Chinese Communist Party.

China’s AI strategy in this regard has hitherto been driven by infrastructural exports and an increased global market presence for Chinese companies.<sup>156</sup> However, this is complemented today with a more holistic diplomatic strategy that also seeks to reshape normative rhetoric at international forums. China’s aim is to influence AI global governance in a manner that suits its own interests—much like the United States crafted the liberal internet governance regime to reflect democratic values as well as to benefit Western companies.

In this regard, Beijing is amplifying its influence not only within UN institutions, but also through informal bodies that complement UN processes. In 2024, for example, the UN General Assembly adopted by consensus a Chinese-sponsored resolution connecting AI, sustainable development, and national sovereignty.<sup>157</sup> This resolution was tabled by a core Group of Friends for International Cooperation on AI Capacity-Building comprising eighty countries and UN entities.<sup>158</sup> Co-chaired by China and Zambia, the group hosts events and

seminars to further cooperation and dialogue on AI capacity-building.<sup>159</sup> Moreover, China's 2025 Global AI Governance Action Plan acknowledges the UN as the "main channel" for crafting an equitable global governance framework and explicitly references the Global Digital Compact, a comprehensive UN-brokered road map for global digital cooperation.<sup>160</sup> China's support for these processes is a clear sign of its interest in advancing international AI dialogue under the auspices of the UN, a body that it increasingly believes it can control.

China's WAICO, when operationalized, will likely complement its efforts at the UN. Although its functional and operational details remain unclear, it is likely that China will use it to build a preliminary consensus on AI governance issues and subsequently leverage this consensus to coordinate positions at the United Nations. While global AI governance discourse is in its nascent stages, China has laid the groundwork to shape future discussions in line with its preferred authoritarian approach at home.

In addition to its normative push through the UN and informal institutions, China has also focused on building technical and governance capacity in developing countries through workshops and seminars.<sup>161</sup> It will likely use WAICO to expand and consolidate its network of AI cooperation centres, including the China-BRICS AI Development & Cooperation Centre (set up in January 2025 and headquartered in Shanghai's Xuhui district) and the China-Laos AI Innovation Cooperation Center, which are designed to facilitate building AI infrastructure and cultivating AI talent.<sup>162</sup>

Such capacity-building efforts certainly offer important developmental opportunities for partnering countries. However, Beijing would likely continue to assert control over the operation of the technologies underpinning AI. For example, any large language model made by a China-based company might automatically censor content embracing liberal norms such as the right to protest, regardless of where the model was deployed.<sup>163</sup>

In essence, Beijing's efforts to shape multilateral rhetoric on AI at the United Nations, while simultaneously pursuing technology diffusion and capacity-building abroad, represent two sides of the same coin. The latter expands China's material power while the former helps legitimize its state-centric approach to AI governance.

## What Now Under Trump?

China's confidence in its AI diplomacy today is driven both by its increasing AI capabilities as well as the belief that its development-oriented vision is likely to be more appealing to the Global South.

Beijing's diplomatic ascent is reinforced by America's AI policy reversal under President Donald Trump. As China pivots toward norms-oriented diplomacy, the United States seems to be embracing economic muscle-flexing and diplomatic coercion.

At the Paris AI Summit in February 2025, Vice President JD Vance made it clear that the U.S. priority was to win the AI race and that concerns about safety were hindrances.<sup>164</sup> One year later at New Delhi's AI Summit, the U.S. delegation emphasized promoting American “dominance” of the AI stack.<sup>165</sup> “We want to make sure the world uses the American AI stack. That means from the bottom up,” said White House AI Policy Advisor Sriram Krishnan.<sup>166</sup> “It means our semiconductors and advanced AI chips, Nvidia, AMD, Google’s TPUs, and so on and so forth.”

In contrast to WAICO’s focus on multilateralism and development, America’s AI Action Plan under the Trump administration prioritizes accelerating innovation, building AI infrastructure domestically, and promoting U.S. standards through its infrastructure.<sup>167</sup> To the extent that the plan touches on diplomacy, it is limited to “counter[ing] Chinese influence in international governance bodies” rather than articulating an agenda of its own.

The changing U.S. approach to AI governance is accompanied by a hollowing out of the State Department’s cyber diplomacy institutions through budget and personnel cuts.<sup>168</sup> State Department–funded civil society institutions that were working at multilateral organizations to counter China’s diplomatic push on norms and standards are also constrained.<sup>169</sup> The Trump administration marked the new year by pulling out of several formal and informal institutions, including notably the Freedom Online Coalition and the Global Forum on Cyber Expertise, that focused on promoting digital human rights and crafting cyber capacity-building, respectively.<sup>170</sup>

In contrast, China-backed private sector enterprises, academics, and so-called government-organized nongovernmental organizations are filling the void.<sup>171</sup> With Washington retreating from its commitment toward a free and open internet and retrenching from global AI institutions, engaging in norms formulation and capacity-building provides an opening for Beijing to hollow out liberal norms as they apply to the deployment of AI stacks in the Global South.

## Will China Win the Global South?

Beijing’s AI vision has yet to win wholesale buy-in from the Global South. Developing countries have not explicitly endorsed Beijing’s diplomatic push on AI nor have they backed the new institutional architecture proposed by Beijing, even as they selectively use Chinese AI products or participate in informal seminars and forums on AI capacity-building. The impact of China’s and Russia’s cyber diplomacy over the past decade suggests that wholesale, normative alignment with their state-controlled vision is unlikely.

Although developing countries are wary of ideological spats, they remain open to engaging with different leading powers including China, the EU, and the United States to further their own digital development goals.<sup>172</sup> While many countries in the Global South are willing to consider China's state-centric and public order-oriented vision of AI, they also see value in governing AI through liberal norms and human rights safeguards.

Multilateral processes on AI governance, including the Global Dialogue on Artificial Intelligence, are taking shape at the UN, providing a platform for Global South countries to participate in and shape global norms-setting processes. The developing world retains an opportunity to articulate norms that prioritize development and AI capacity-building while respecting the rights of individuals and communities impacted by AI. Despite differing interests and approaches to international engagement, developing countries should not be forced to choose between China's diplomatic expansion or the Trump administration's unpredictable mercantilism. For many, a path rooted in democracy and the rule of law remains the most prudent way forward.

## Acknowledgments

I am thankful to Steve Feldstein, Shreya Joshi, Valentin Weber, and members of the DDN for feedback on previous drafts. All errors remain my own.

## Early Lessons in the Pursuit of Sovereign AI

Shreya Joshi

In February 2026, on the sidelines of the AI Impact Summit in New Delhi, the United Arab Emirates (UAE) and India signed a consequential AI infrastructure deal, marking a new phase of sovereign AI development.<sup>173</sup> The Emirates' state-owned technology group G42, in partnership with the Mohamed Bin Zayed University of Artificial Intelligence and U.S. technology firm Cerebras, agreed to establish a national-scale AI supercomputer in India.<sup>174</sup> The 8-exaflop supercomputer will have the power to accelerate AI research and innovation in India and will rank among India's most powerful AI compute systems. The deal was subsequently formalized during Prime Minister Narendra Modi's state visit to Abu Dhabi in May.<sup>175</sup> Two elements of the deal make it noteworthy. First, the supercomputer will be funded by Emirati capital, using American chips and hardware expertise from the UAE and United States. Second, the agreement will be governed by India's governance framework and data localization requirements, which mandate that data be stored domestically, while contributing to the country's IndiaAI Mission.

The deal offers a useful perspective on AI sovereignty and the strategies middle powers are adopting in its pursuit. The quest to attain AI sovereignty has become a defining feature of contemporary geopolitics. Currently, a small number of companies, largely based in the United States and China, dominate frontier AI models and the infrastructure that powers them. The rest of the world is struggling to keep up.<sup>176</sup> This raises two critical questions: How are middle powers pursuing AI sovereignty? And what does a realistic vision of sovereignty look like for them?

India and the UAE have emerged at the forefront of AI innovation, offering important insights. As their experiences suggest, attaining complete sovereignty is unrealistic for most nations, but that doesn't mean they must revert to dependence on the United States or China either. Embracing "strategic autonomy," or "managed interdependence," offers a third way.<sup>177</sup>

## The Appeal of AI Sovereignty

Sovereign AI generally refers to a nation's ability to independently design, develop, and govern AI systems using its domestic infrastructure, nationally held data, and a homegrown talent base.<sup>178</sup> Rather than thinking of AI sovereignty as a binary between independence and dependence, analysts increasingly understand it as a spectrum, with countries achieving different capacities across the AI stack, including semiconductors, cloud platforms, data centers, foundation models, and supporting digital infrastructure.<sup>179</sup>

Countries have differing motivations for pursuing AI sovereignty.<sup>180</sup> For many, national security is a top-level consideration, as they are concerned with safeguarding sensitive national data from foreign control and preserving access to advanced defense and intelligence capacities. Other relevant factors include economic competitiveness—nations look to AI to drive domestic investment, employment, productivity, and long-term growth—and cultural drivers, with governments prioritizing AI systems that reflect their own linguistic and cultural contexts.

These motivations point to a deeper structural concern: dependence. Countries cannot fully safeguard sensitive data, capture the economic value of AI, or ensure culturally and linguistically appropriate systems if the underlying AI stack is owned, operated, or governed by foreign actors. Almost every country exhibits dependencies across the AI stack. Companies based in either the United States or China continue to supply the bulk of the components powering systems worldwide. For instance, a recent report from the Washington, DC–based think tank Center for a New American Security found that NVIDIA alone supplied graphics processing units (GPUs) for 52 percent of all tracked infrastructure projects around the globe, from South Korea to Canada.<sup>181</sup>

Nonetheless, countries are finding ways to navigate their dependencies.<sup>182</sup> Some are prioritizing building out domestic infrastructure, such as data centers, GPU clusters, and access to compute infrastructure. A smaller number are focusing on developing or adapting foundation models. Only a few countries are actively investing in national datasets or data-sharing platforms.

## Insights from India and the UAE

India and the UAE are instructive, varied cases—one a lower-middle-income democracy that has a large talent base and over 1.4 billion citizens, the other a small, capital-rich Gulf monarchy, with a centralized government and sovereign wealth to deploy at scale. Both offer lessons about the tricky balance between pursuing technological sovereignty while still drawing from advanced technology from the United States and China.

India's government is betting heavily on domestic AI innovation, linking sovereign AI to its development goals.<sup>183</sup> Delhi views AI innovation as a key means to address internal inequality gaps and raise its population's standard of living. In 2024, the government launched its IndiaAI Mission, a flagship project to increase investments in AI.<sup>184</sup> Since then, the country's sovereign AI sector has raised over \$5.5 billion spread across 1,700 firms, seeking to leverage the scale of its population, large talent pool, and state-backed digital public infrastructure.<sup>185</sup>

India's approach to building out domestic AI capacity plays out in two key areas: developing national foundation models and expanding compute infrastructure.<sup>186</sup> The country has invested heavily in sovereign large language models (LLMs), such as Sarvam AI and BharatGen, in an effort to reach a significant portion of its population that remains underserved by leading frontier models.<sup>187</sup> The country has also devoted sizable funding to domestic semiconductor manufacturing and data centers, although it has experienced limited results so far.<sup>188</sup> As of early 2026, the IndiaAI Mission's compute facility consisted of 38,000 GPUs, all supplied by American firms.<sup>189</sup> This points to a persistent dependency: India continues to rely on U.S.-supplied infrastructure, including semiconductors from NVIDIA and cloud-computing services from Amazon Web Services, Microsoft Azure, and Google Cloud.<sup>190</sup>

In light of these dependencies, India has prioritized investments in its domestic LLMs and made efforts to set strong data governance standards at home. India's SarvamAI is particularly noteworthy and has allowed the country to cultivate domestic capacity in the development and use of LLMs. As a government-supported sovereign AI initiative, Sarvam was created to advance India's multilingual AI ecosystem and support all twenty-two national languages. It incorporates text-, voice-, and vision-based data, and is trained on India-centric datasets. The model is now being deployed across several public sectors, including education and healthcare, where it is enabling rural patients to "access medical advice, schedule appointments and consult doctors through WhatsApp and low-bandwidth interfaces."<sup>191</sup> Analysts note that these efforts to make national and sector-specific AI models may also be more financially feasible for other countries, like Saudi Arabia, over the next decade.<sup>192</sup>

In comparison, the UAE has reportedly spent an astounding \$148 billion on AI investments domestically and abroad since the start of 2024, backed by its sovereign wealth funds.<sup>193</sup> Across the Gulf states, including Saudi Arabia and Qatar, the UAE has been at the forefront in both building data center capacity and attracting foreign investment. For Abu Dhabi, economic diversification is a key motivator driving its sovereign ambition, as it seeks new sources of long-term growth and influence in the face of declining hydrocarbon revenues.<sup>194</sup> In addition, its leadership is responding to increasingly securitized global AI supply chains, recognizing the importance of preventing dependencies, and limiting exposure to the "compliance demands and alignment pressures" imposed by U.S.-China competition.<sup>195</sup>

The primary vehicle for the Emirates' sovereign ambitions is G42, a private AI company chaired by the UAE's national security adviser, Sheikh Tahnoun bin Zayed, that is valued in the billions.<sup>196</sup> Despite G42's significant investments and global expansion, the UAE's

sovereign ambitions have yet to fully take off.<sup>197</sup> Initially, the country sought to leverage both U.S. and Chinese expertise to build up its AI sector. That strategy unraveled in 2023, when the Joe Biden administration placed the Emirates on an export restrictions list because of its close ties to Chinese tech firms.<sup>198</sup> Subsequently, the UAE reduced its reliance on Chinese technology and deepened cooperation with American companies (though the UAE retained several key partnerships with China).<sup>199</sup> But these efforts have not translated into independence. Rather, they have deepened the UAE's reliance on Washington in lieu of Beijing and pushed the country to align its national security standards and protocols with America's.<sup>200</sup>

Since then, the UAE's sovereignty efforts have hinged on significant state-led investments and its open weight models, such as G42's Falcon, Jais, and K2 Think, that promote Arabic culture.<sup>201</sup> At the same time, the country mitigates its dependence on foreign chips and frontier models through long-term "negotiated access, co-production agreements, and US-aligned security partnerships."<sup>202</sup> Although the UAE has downgraded its ties with China after being put on the U.S. export control list, it has managed to increase its leverage with the United States by hosting American supercomputers and investing in American firms, securing reliable access to frontier capacities and using financial commitments as a form of geopolitical insurance.<sup>203</sup> The UAE's strategy shows how countries can gain advantages in specific sectors of AI development despite larger dependencies, affording them more bargaining power with their partners.<sup>204</sup>

## A Model of Managed Interdependence

It is increasingly clear that full AI sovereignty is beyond the reach of even the most capable middle power actors.<sup>205</sup> A more realistic path toward sovereignty involves adopting a hybrid approach that allows countries to exercise a degree of autonomy and incrementally build their sovereign capacity in specific sectors, while forming partnerships with like-minded countries that reduce their exposure to risks, such as vendor lock-in and asymmetric bargaining power, across the AI stack. Analysts describe this strategy as "managed interdependence."<sup>206</sup>

The partnership between the UAE and India through the G42 deal demonstrates the promise of managed interdependence and offers an avenue through which countries can partner up, while simultaneously exercising greater autonomy over domestic deployment. Through the deal, India receives the compute infrastructure needed to power its domestic AI capacities, hosted within its borders under domestically defined rules. Similarly, through G42, the UAE gains a strategic foothold in one of the world's largest digital markets and advances its position as an AI infrastructure partner of choice. To that end, the Emirates are already looking to scale up this model; recent reporting indicates that G42 is establishing a global network of AI facilities that it builds, owns, and operates for national governments, with India the first to sign on.<sup>207</sup>

Taken together, the cases of India and the UAE underscore the value of managed interdependence as a guiding framework for AI sovereignty. With the reality that complete AI independence remains out of reach for many countries, a better approach is for governments to reduce their exposure to foreign dependencies, invest strategically in sovereign capacity, and preserve flexibility as the global AI landscape shifts.

## Inside the Swap Mart: How Thailand's Domestic Digital Repression Enables Transnational Repression

Janjira Sombatpoonsiri

On November 23, 2019, Tor Nimol, an exiled opposition activist from Cambodia, was arrested along with his wife, Chen Lim, by at least eight plainclothes Thai police officers at a Bangkok mall.<sup>208</sup> The officers shoved the couple into a van and drove them around the city for two hours before handing them off to Cambodian government officials waiting in another vehicle. Nimol's phone was confiscated, as was his UN Refugee Agency (UNHCR) refugee card—the document that was supposed to protect him. He was sent back to Cambodia that same day. In December 2022, Nimol was one of twenty-two Cambodia National Rescue Party (CNRP) supporters sentenced to five years' imprisonment for violating Article 453 of the 2009 Criminal Code, which covers plotting a felony.<sup>209</sup>

Nimol was among hundreds of dissidents caught up in what Human Rights Watch would later call a “swap mart”: a quid pro quo arrangement in which Thailand helps partner governments silence exiled critics, in exchange for those governments targeting Thai dissidents abroad.<sup>210</sup> The swap mart is part of broader transnational repression (TNR) patterns and what scholars have termed “authoritarian innovations”; these include deals struck across borders between like-minded leaders to suppress threats to regime survival.<sup>211</sup>

Digital tools used for domestic repression are increasingly leveraged for transnational repression, including interception technologies and social media monitoring, coordinated social media campaigns targeting exiled dissidents, and distributed denial-of-service (DDoS) attacks.<sup>212</sup> While existing analyses focus on how origin states use these tools to target diasporas in largely democratic host states, this article instead examines how an autocratic host state—Thailand—is using its own digital repression infrastructure to supercharge transnational repression on its own soil.<sup>213</sup>

## Transnational Repression on Thai Soil

In Southeast Asia, and in Thailand specifically, transnational repression intensified after 2014, when the country, which many exiles had believed to be a safe haven, entered a period of authoritarian rule.<sup>214</sup> In May 2014, the army staged a coup and governed directly until 2019, when a general election was held.<sup>215</sup> Despite the return of electoral politics, the junta-drafted constitution and junta-aligned institutions, such as the Senate, Election Commission, and Constitutional Court, enabled military leader General Prayuth Chan-Ocha, and his party, Palang Pracharath, to remain in power until the 2023 elections, when the former opposition party, Pheu Thai, returned to government.<sup>216</sup> The military rule left behind an enduring authoritarian legacy, which has included a persistent role in transnational repression that successive elected governments have been compelled and incentivized to maintain.

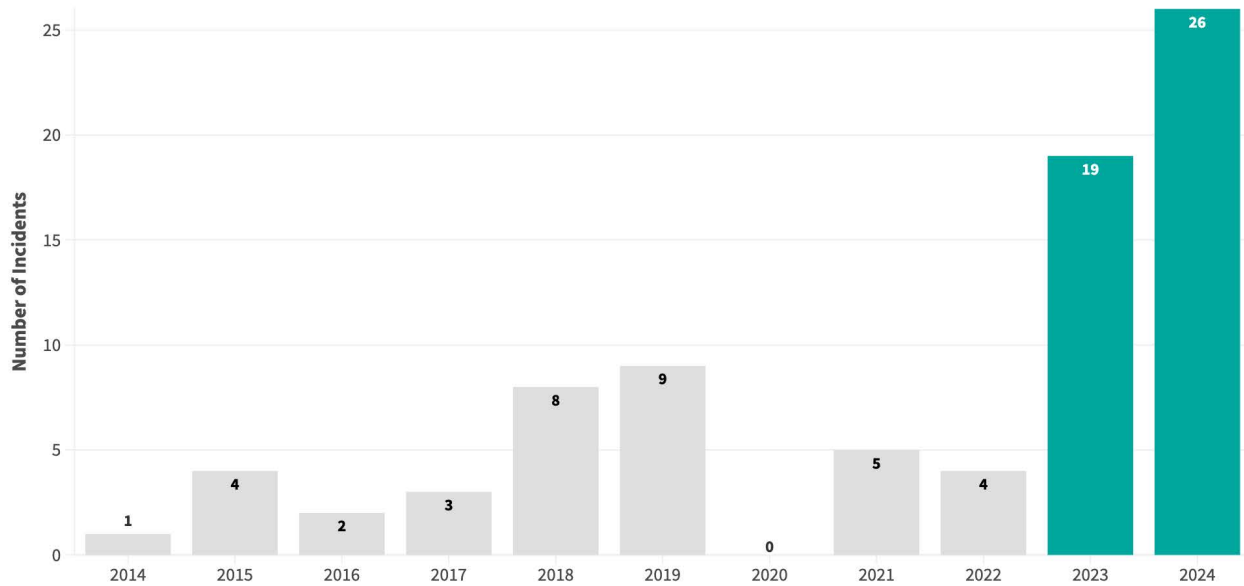
Facing “soft sanctions” from the United States and the European Union, the 2014–2019 junta turned to autocratic allies in the region, particularly Cambodia, China, and Vietnam.<sup>217</sup> Beyond trade ties and diplomatic coordination against Western criticism, these relationships aided the Thai government’s crackdowns on Thai dissidents exiled in neighboring countries, including Cambodia and Laos, even when they were transiting through these countries before resettling in third countries. While Thai dissidents murdered or arrested abroad have been well documented, the inverse flow of transnational repression on Thai soil directed at the dissidents of Thailand’s autocratic allies has received far less attention.<sup>218</sup>

This analysis draws on Freedom House’s Transnational Repression Project Dataset (v.6), which documents 219 TNR incidents occurring in Thailand between 2014 and 2024. I recoded the dataset by treating each TNR victim as a single case, rather than counting the TNR types they experienced separately.<sup>219</sup> Further, I excluded cases of mass deportations and detentions of involving individuals who may not have been activists or linked to opposition parties—such as the deportations of groups of seventeen and 109 Uyghurs to China in 2014 and 2015 respectively, and the detention of two Uyghurs who died in custody in 2023—thereby focusing on clearer cases of TNR directed at oppositional actors.<sup>220</sup> I also introduced additional variables of analysis such as type of TNR activity and the site where each incident occurred, and I cross-checked information that was insufficiently detailed in the Freedom House dataset against news reports and human rights documentation. The recoded dataset comprises eighty-one cases and reveals several patterns relevant to Thailand’s role in transnational repression.

First, twenty-six cases, the largest cluster, occurred in 2024, one year after the general election brought the Pheu Thai Party–led government to power. After the junta-appointed Senate blocked the opposition Move Forward Party’s prime ministerial candidate, Pheu Thai formed a ruling coalition with junta-aligned parties, such as Palang Pracharath and United Thai Nation, leaving Move Forward—the party that won the largest share of the popular

vote—in opposition. The new civilian government continued several policies from the previous military regime, including a 2018 bilateral arrangement with Cambodia that permitted the exchange of each country’s fugitives.<sup>221</sup>

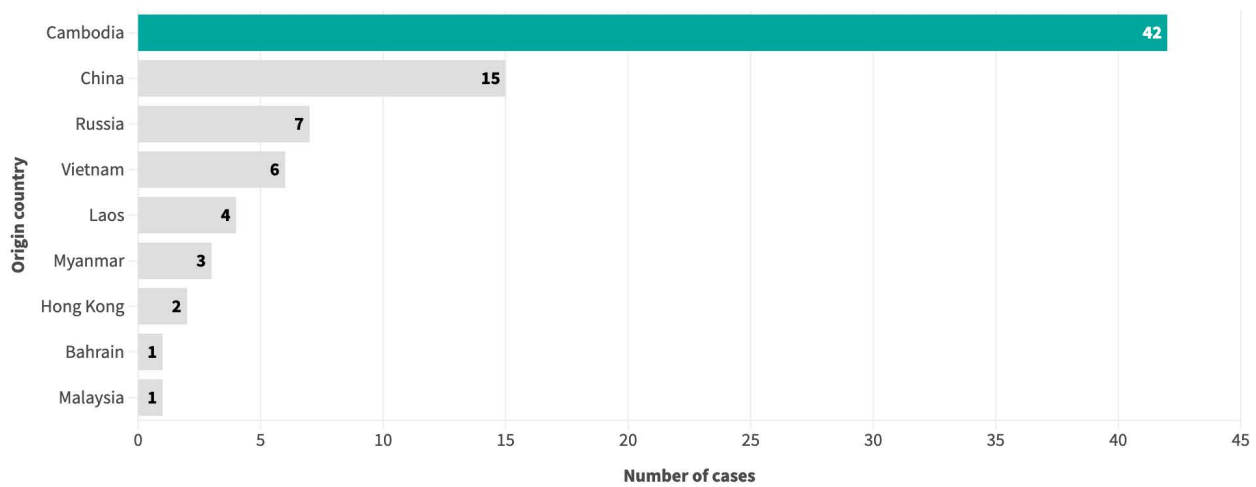
**Figure 1. TNR Incidents Per Year in Thailand, 2014–2024**



Source: Author’s analysis, Freedom House, Transnational Repression Project dataset v.6. <https://freedomhouse.org/report/transnational-repression>.

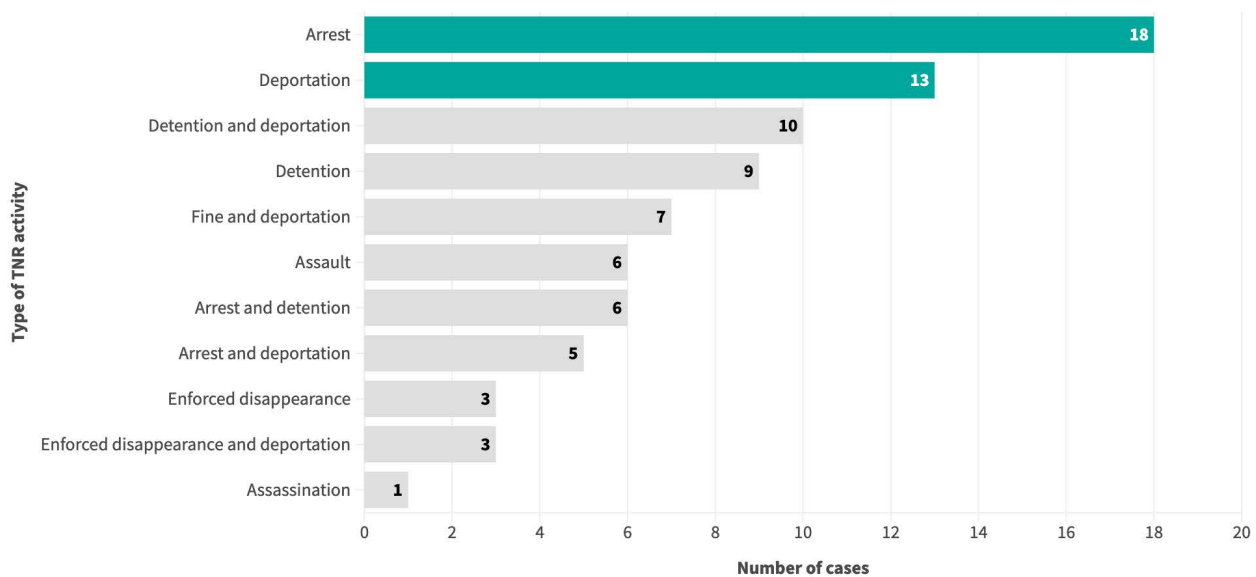
Second, forty-two of the eighty-one targets (51.9 percent) originated from Cambodia, far exceeding the numbers from China (fifteen individuals, or 18.5 percent), Russia (seven individuals, or 8.6 percent), and Vietnam (six individuals, or 7.4 percent). This likely reflects Thailand’s long-standing role as a refuge for Cambodian political dissidents, combined with the Cambodian government’s aggressive reach abroad, especially after the 2017 dissolution of the opposition CNRP. While TNR cases involving other origin countries are distributed across the 2014-to-2024 time span, Russia is a notable exception. All seven Russian cases in the dataset are members of the Russian-Belarusian pop-rock band Bi-2, known for its anti-war stance. On January 24, 2024, while touring in Thailand, the group was arrested and detained by Thai authorities on the grounds that its members had failed to obtain work permits.<sup>222</sup> Prior to the arrests, Russian lawmakers had accused the group of harboring an “anti-Russian” attitude.<sup>223</sup>

**Figure 2. Origin Countries of TNR Targets in Thailand**



Source: Author's analysis, Freedom House, Transnational Repression Project dataset v.6. <https://freedomhouse.org/report/transnational-repression>.

**Figure 3. Types of TNR Activities in Thailand**

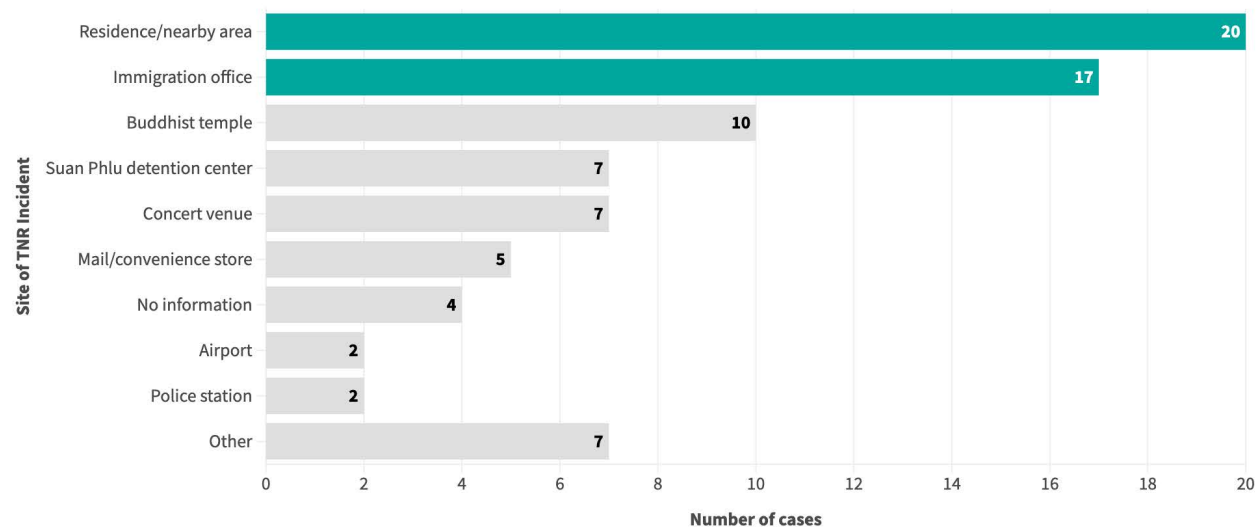


Source: Author's analysis, Freedom House, Transnational Repression Project dataset v.6. <https://freedomhouse.org/report/transnational-repression>.

Third, arrest and deportation constitute the most common forms of transnational repression occurring on Thai soil. Of the recorded cases, eighteen involved arrests by Thai authorities alone, thirteen were deportations alone, and ten involved both detention and deportation. Violent tactics such as assault or assassination are comparatively rare, accounting for only six cases in total, suggesting the primary mechanism of repression relies more on legal-adjacent coercion than overt violence. At least thirty-one cases involved individuals who either held UNHCR refugee status or were active in the UNHCR asylum-seeking process at the time they experienced transnational repression, yet were nevertheless deported or forcibly returned to their countries of origin. In at least four instances, exiled dissidents were arrested and deported either before or after a visit to the UNHCR office in Bangkok. This pattern points to Thailand's failure to uphold the rights of recognized refugees and asylum seekers, in part due to the country's nonsignatory status to the 1951 Refugee Convention.

This observation brings us to the fourth pattern: TNR incidents frequently occurred while targets were going about everyday activities in public or at personal sites, like a department store, hospital, or apartment. Nearly a quarter of incidents (twenty cases) took place at residences or nearby areas. Strikingly, Buddhist temples appeared in ten cases, likely linked to the Cambodian dissident community's use of temples as gathering points. Individuals targeted for assassination or assault were often followed by assailants on their way home from work or other routine activities, and news reports suggest these assailants sometimes spoke the same language as their targets.<sup>224</sup> Targets were apprehended at or on their way home, while commuting to work, strolling through a mall, and visiting a hospital.<sup>225</sup>

**Figure 4. Sites of TNR**



Source: Author's analysis, Freedom House, Transnational Repression Project dataset v.6. <https://freedomhouse.org/report/transnational-repression>.

Transnational repression incidents proceed through three mechanisms. First, cases involving legal procedures are presumably facilitated through bilateral, and often unwritten, agreements. Thai authorities have detained and extradited exiled dissidents at the request of counterparts in Cambodia, Vietnam, and Malaysia.<sup>226</sup> While the Thai-Cambodian agreement on exchanging fugitives is formalized, cooperation with Vietnam and Malaysia appears to rely more heavily on economic interdependence, particularly cross-border trade and labor flows.<sup>227</sup> Second, beyond these bilateral channels, Amnesty International and legal experts have alleged that influential states, including China and more recently Russia, misuse multilateral mechanisms such as Interpol's ability to issue red notices that Thai immigration officers act upon when targets pass through immigration controls.<sup>228</sup> The third mechanism operates less through formal cooperation than through the inaction or permissiveness of Thai authorities. In cases of assassination and enforced disappearance, where foreign agents operate on Thai soil in clear violation of Thai sovereignty, Thai authorities often "lack awareness about the threat of transnational repression."<sup>229</sup> At worst, they have turned a blind eye in investigations into at least two cases of enforced disappearance and killing of Laotian dissidents.<sup>230</sup>

## **Domestic Digital Surveillance for Transnational Repression: Three Pathways**

The most revealing set of data concerns arrests, deportations, and other forms of intimidation targeting exiled dissidents during their daily routines. What makes these cases unique is that exiled dissidents were going about their daily lives when Thai authorities suddenly intercepted them, raising the question of how their whereabouts were identified, absent some form of tracking. While establishing a link between domestic surveillance and transnational repression would require firsthand accounts from both TNR targets and the authorities involved, the current dataset, together with the existing evidence on Thailand's surveillance infrastructure, suggests several ways in which this apparatus may be leveraged for transnational repression.

Since the onset of military rule and accelerating in response to the youth-led anti-government protests of 2020–2021, Thailand's surveillance apparatus has become increasingly sophisticated, combining manual monitoring of dissident activity on social media and at protest sites with surveillance technologies such as "social media listening" tools, CCTVs, Global Positioning System (GPS) trackers, and spyware.<sup>231</sup> During periods of mass mobilization, authorities cross-check data from different sources for complementary ends. Intrusive tools such as spyware and GPS trackers geolocate targeted activists and access private information. Key figures within protest movements, both leaders and individuals in administrative or logistical roles, have reportedly been closely monitored to extract information about funding sources and protest plans. In late 2020 and 2021, devices belonging to at least thirty dissidents involved in anti-government protests were infected with Pegasus spyware.<sup>232</sup>

Although information gathered through interception devices is inadmissible in Thai courts unless authorities obtain a warrant, such intelligence serves two main purposes. First, protest-related data allow authorities to anticipate and preempt protest activity, thereby minimizing its impact. Second, by identifying persons of interest through intrusive surveillance, authorities can assemble charges against these individuals using other forms of admissible evidence. This is where broader surveillance practices, particularly CCTV and social media monitoring, become relevant. As of 2025, approximately 65,015 CCTV cameras were installed across the greater metropolitan area of Bangkok, equating to about 3.6 to 12.5 cameras per 1,000 inhabitants.<sup>233</sup> Meanwhile, Thailand's security forces have established cyber units staffed by thousands of officers, who play overlapping roles: monitoring online content, orchestrating influence operations, and, in the case of the police, filing computer crime charges against digital activists.<sup>234</sup> Visual records and social media posts associated with prominent dissidents are often cross-referenced to implicate them in activities deemed criminal.

In addition, digital surveillance is extended through two channels: institutional cooperation with internet service providers (ISPs) and informal collaboration with pro-establishment social media outlets and activists.<sup>235</sup> Thailand's ISPs have a track record of complying with authorities' requests for IP addresses of dissidents, which has also been linked to the enforced disappearance of the Thai exiled dissident Wanchalerm Satsaksit in Cambodia.<sup>236</sup> Further, through online vigilantism, pro-government outlets and social media personalities coordinate smear campaigns targeting the opposition. These actors also engage in judicial harassment of dissidents by screenshotting their controversial posts, sharing these posts on their pages, and submitting these images to the police as evidence for criminal charges.<sup>237</sup>

These domestic surveillance practices point to three possible ways in which the same infrastructure may be used for transnational repression. First, the use of CCTV footage to track the whereabouts of exiled dissidents may be central in cases such as Truong Duy Nhat (originally from Vietnam), Nimol and Lim (from Cambodia), Voeun Veasna and Voeung Samnang (from Cambodia), and Lù A Da (from Vietnam).<sup>238</sup> Thai authorities reportedly appeared unannounced, intercepting these individuals in public spaces or en route to their homes, arresting them for visa overstay or transferring them to authorities from their countries of origin. Visual data from CCTV systems installed in public areas around Bangkok may have allowed authorities to reconstruct their routines, which in turn would facilitate physical surveillance and apprehension. Alternative explanations are possible: Origin-state informants or social media tracking could also account for some of these interceptions. However, the speed and precision with which Thai authorities located targets in unscheduled public locations appear most consistent with access to Thailand's existing CCTV network.

Second, Thai authorities may employ interception technologies or IP address tracking to monitor exiled dissidents' private communications and identify their undisclosed locations. A case in point are the arrests of Cambodian opposition activists Lem Sokha, Phan Phana,

Kung Raiya, Chhorn Sokhoeun, and Chhorn Chorn Ny approximately one week before Cambodian Prime Minister Hun Manet's official visit to Thailand in February 2024.<sup>239</sup> In the days before Hun Manet's arrival, the police went directly to the activists' apartments and transferred them to an immigration detention center. One activist, Raiya, suspected that the police might have identified his location by tapping his phone or tracking his IP address.<sup>240</sup> Thai authorities had already used such tactics—preemptive arrest based on intercepted communications—against domestic protesters and appear to have extended them to dissidents from allied autocracies. Other cases follow the same pattern: The case of the wife and two daughters of detained Chinese human rights lawyer Wang Quanzhang, who fled to Thailand; Lanh Thavry of the dissolved Cambodian opposition CNRP; and the Vietnamese dissident Bach Hong Quyen.<sup>241</sup> In each case, the targets reportedly concealed their locations while in transit to third countries, which leaves IP address tracking or other interception devices, possibly in conjunction with informants, as the most plausible explanation for their being found by authorities.

The third possible pathway concerns social media monitoring that helps enable crackdowns on gatherings organized or attended by exiled dissidents. The late-December 2023 arrest of So Meta and nine other Cambodian opposition figures illustrates this dynamic.<sup>242</sup> On December 2, 2023, Cambodian opposition activists held a workshop on democracy and human rights in Bangkok, attended by nearly 100 people. Several days later, a pro-government Thai outlet—one that routinely monitors the official account of the opposition Move Forward Party (MFP)—reposted images of Cambodian dissidents from that workshop, accusing the MFP of providing “a safe haven” for activity against the Hun Sen regime.<sup>243</sup> The post prompted a coordinated push from Cambodian counterparts: Nine pro-establishment parties urged Thai authorities to monitor opposition activists in Thailand, and the leadership of one pro-Hun Sen party, the Khmer Unity Great Nation Party, reportedly contacted the office of the Thai prime minister directly.<sup>244</sup> On December 29, 2023, Thai immigration police intercepted a separate training workshop briefing Cambodian workers in Thailand on the 1991 Paris Peace Agreement—the UN-brokered settlement that ended Cambodia's civil war and laid the foundations for parliamentary democracy.<sup>245</sup> Police arrived shortly after the workshop began and arrested ten participants, all UNHCR refugees or asylum seekers, including activist So Meta and her two sisters, for organizing the workshop without a permit. This series of events shows how public exposure of dissident networks, amplified through pro-establishment media and channeled into bilateral pressure, translates into enforcement against UNHCR-recognized refugees on Thai soil.

## Conclusion

Thailand's role in the swap mart suggests a broader pattern: In regions where multiple autocracies neighbor one another, transnational repression is not merely a function of bilateral agreements or weak refugee frameworks. It rests on host states' own domestic repression infrastructures, including surveillance networks, cyber units, ISP cooperation, and prosecutorial capacity, which can be repurposed to target dissidents from allied regimes. In the Mekong sub-region, the pact among Thailand, Cambodia, Laos, and Vietnam to support one another's domestic crackdowns has produced exactly this outcome. Thailand is no longer safe for regional activists; neither are Cambodia, Laos, or Vietnam for Thai dissidents who had typically sought refuge there. Addressing these challenges will require international engagement directed not just toward origin states, but also toward the host states whose security apparatuses enable transnational repression. Moreover, democratic governments and international organizations should press Thailand to uphold the principle of non-refoulement in practice and establish rapid-resettlement channels for exiles facing imminent return. Lastly, the export of surveillance technology to autocratic host states should be treated as a contributor to transnational repression.

## Operationalizing AI Sovereignty Through Agency, Interoperability, and Openness

Luca Belli

Artificial intelligence sovereignty has rapidly transitioned from a niche academic concept to a cornerstone of contemporary digital policy. Yet despite the ubiquity of digital sovereignty and AI sovereignty in current technological-policy debates, both goals remain conceptually fluid and operationally elusive. Governments frequently invoke the protection of sovereignty to legitimize public investments, justify regulatory guardrails, or navigate geopolitical rivalries, yet they often fail to articulate a concrete road map for its realization.

For the past four years, the CyberBRICS project of the Center for Technology and Society at FGV Law School, Rio de Janeiro, has applied the Key AI Sovereignty Enablers (KASE) framework to analyze how technological dependencies intersect with AI governance.<sup>246</sup> Building on this foundation, this article explores a practical path to operationalize the concept of AI sovereignty. The KASE framework focuses on the governance, regulatory, and industrial policy dimensions of eight fundamental layers composing an AI technology stack: data, software and algorithmic models, computational capacity, meaningful connectivity, energy, education and research, cybersecurity, and AI-safety frameworks.

Exercising the framework effectively will require reducing persistent tensions between access and control, as well as innovation and dependency, while emphasizing the role of cooperative institutional and technological arrangements in addressing structural constraints and enabling collective capacity building.<sup>247</sup> More broadly, it will require alleviating tension between aspirations for technological autonomy and the realities of global integration. Some scholars argue that total AI sovereignty is an illusion, either because it overlooks the physical infrastructure underpinning AI or confuses control over artifacts with genuine capability.<sup>248</sup> From this perspective, building resilience—the ability to withstand external shocks—is a more realistic objective. At the same time, private sector actors frame sovereign AI around infrastructure control and data localization, reflecting a broader tension between political desire, technical constraints, and commercial incentives.

In this context, AI sovereignty should be operationalized as a strategic capacity built through three interdependent pillars: agency, interoperability, and openness.<sup>249</sup> Grounded in these pillars, the KASE framework offers a blueprint for states to navigate global dependencies while retaining the power to shape their own technological futures. In short, this more productive approach could help countries move away from sovereignty as an abstract aspiration toward sovereignty as an operational capacity. This would offer a way to navigate dependence without denying it exists and to exercise influence without requiring full control. The analysis and recommended steps that follow apply the pillars across the key enabling conditions of AI systems.

For the purpose of the analysis, AI sovereignty is defined as the capacity of a given country to understand, develop, and regulate digital or AI systems, thus retaining self-determination, agency, and control over such systems.<sup>250</sup> This definition emphasizes that sovereignty discussions involve not only formal regulatory authority, but also—and, perhaps, chiefly—the technological, institutional, and scientific capabilities necessary to shape the development and governance of AI systems.<sup>251</sup>

## Rethinking Sovereignty: From Control to Strategic Agency, Interoperability, and Openness

The traditional Westphalian view of sovereignty is rooted in the control of physical territory, resources, and independent decisionmaking; and it constitutes a pivotal principle of modern international law.<sup>252</sup> Transposed to the digital sphere, this logic manifests as the pursuit of full-stack autonomy, implying the domestic production of all the abovementioned Key AI Sovereignty Enablers. However, such ambitions clash with the realities of the AI value chain, which is defined by extreme specialization, immense capital requirements, and powerful network effects.<sup>253</sup> In this environment, self-sufficiency is a logistical impossibility for most countries.

A more useful framing is to reevaluate sovereignty through the lens of three pillars. The first is *agency*, the substantive capacity to exercise autonomous choice within a state of interdependence. Agency involves the capacity to autonomously assess what technological choices one should pursue to achieve one's right to self-determination. Concretely, it means being able to understand the function of AI systems, access critical technologies on fair terms, adapt systems to local linguistic or cultural needs, and exert influence over global governance standards in accordance with one's own values. Under these conditions, sovereignty is better understood as agency under constraint. The relevant question is not whether a state controls every layer of the stack, but whether it retains the capacity to make consequential choices: to switch providers, impose conditions, adapt technologies, and freely engage in national or international rule-making processes.

Agency, in this sense, is negotiated, contingent, and often collective. This perspective recognizes that cooperation across countries does not diminish sovereignty.<sup>254</sup> Rather, strategic partnerships often provide the leverage required to maintain autonomy, allowing countries to diversify and manage their dependencies on favorable terms.

This means, however, that the capacity to exercise agency as a strategic objective relies on a second pillar, *interoperability*, serving as its primary technical enabler. In a fragmented digital landscape, the lack of interoperability acts as a mechanism of “vendor lock” confining applications into proprietary-walled gardens that preclude the ability to switch providers and stifle localized innovations. Conversely, when digital architecture is interoperable, it lowers switching costs and catalyzes competitive dynamics.<sup>255</sup> Interoperability spans data, software, and infrastructure, requiring common standards, compatible systems, and open architecture to permit the secure exchange of datasets, prevent technical silos, and ensure that sovereign cloud solutions are not tethered to a single vendor’s road map.

However, for interoperability to be successful, one has to have alternative options to interoperate with. Hence, pursuing interoperability is as much a political and industrial choice as a technical one. Policies that mandate open standards and data portability are essential for preventing the unilateral imposition of rules by dominant external actors. Industrial policy facilitating the development of alternatives is essential to make sure that interoperability is more than a normative obligation.<sup>256</sup> Ensuring that standards are developed through inclusive, multistakeholder processes is therefore central to the broader pursuit of digital autonomy.

Thus, *openness* is the third pillar of AI sovereignty; it lowers barrier to entry and enables distributed experimentation and rapid scaling. Yet openness is not a neutral benefit. It can sometimes entrench structural concentration.<sup>257</sup> Open components are frequently integrated into proprietary stacks controlled by a few dominant firms, allowing them to externalize the costs of development while capturing the lion’s share of the value.<sup>258</sup> Furthermore, a state that consumes open technologies without possessing the domestic human capital to modify or audit them risks remaining in a state of passive dependency.

The goal, therefore, is strategic openness.<sup>259</sup> This means investing in open infrastructure, such as digital public infrastructures, and ensuring that regulatory frameworks do not become a pretext for unregulated data extraction or unfair competitive practices. Openness must be treated as a strategic tool embedded within a larger industrial and governance strategy, rather than an end in itself.

## Applying the Three Pillars to Avoid “Sovereignty-Washing”

Applying the pillars of agency, interoperability, and openness across the KASE framework’s eight layers spanning the AI technology stack can bring meaningful change, but operationalizing the pillars requires a coordinated approach:<sup>260</sup>

1. **Data:** Agency depends on the ability to curate high-quality local datasets. Interoperability relies on shared standards. Openness is realized through the establishment of data stewardship institutions that manage data as a valuable resource to be handled in the public interest.
2. **Software and models:** Agency is the capacity to develop, fine tune, and deploy models. Interoperability ensures that these models function across platforms. Openness is secured by making reusable, transparent code available.
3. **Hardware and infrastructure:** Given the high barriers to entry in hardware, agency involves securing strategic positions in the global supply chain rather than full production. Interoperability ensures cross-system compatibility. Openness is reflected in the adoption of standardized hardware architecture.
4. **Meaningful connectivity:** Reliable, affordable, and universally accessible connectivity infrastructure is critical for developing, operating, and accessing AI systems. Hence, meaningful connectivity requires open and nondiscriminatory internet access, avoiding practices like “zero-rating plans” where private firms subsidize access to just a few apps or websites, limiting users’ agency and capacity to freely access AI services.<sup>261</sup>
5. **Energy and mineral resources:** Agency is contingent on countries accessing critical resources so they can physically build sustainable digital infrastructure. Open energy markets and transparent supply chains prevent resource gatekeeping, ensuring interoperable networks can scale sustainably without creating new external dependencies.
6. **Capable and resilient humanware:**<sup>262</sup> The level of digital literacy and cognitive resilience in a society determines its capacity to exercise agency, understand interoperability, and work to promote openness. Only technological systems that retain a human element can actively shape technological evolution rather than passively react to it.
7. **Cybersecurity:** Preserves agency by safeguarding supply chain integrity and protecting domestic infrastructure from foreign interference or nonstate threats. Without robust cyber defenses, open and interoperable architectures risk becoming vectors for external manipulation and systemic instability.
8. **AI safety frameworks:** Preserve sovereign agency by ensuring model robustness, predictability, and alignment with domestic governance standards. Establishing rigorous safety standards enables states to confidently adopt open systems and foster integration without exposing critical infrastructure to operational risks or structural exploitation

Applying the three pillars to the KASE framework helps structure both the conceptual approach and operational strategy for AI sovereignty. It also counters the growing, imprecise use of the term “AI sovereignty,” a term increasingly invoked to justify measures that have little to do with autonomy. Building off the pillars, the framework can be used to assess the proliferation of initiatives branded as “sovereign” that fail to build real agency, such as localized cloud infrastructures dependent on foreign providers or “national” AI systems built on externally controlled models.

Countries’ claims to sovereignty should be evaluated against concrete criteria: Does the specific AI-sovereignty initiative increase its ability to make independent choices? Does it reduce lock-in? Does it preserve openness without creating new vulnerabilities? Any initiative that restricts a nation’s ability to choose ultimately locks the country into a single provider or creates opaque dependencies that should be viewed with skepticism, regardless of its label.

## **Cooperative Digital Sovereignty: Institutional Pathways Toward an AI Network of Networks**

Individual states, particularly those outside major tech hubs, often lack the resources and scale to build AI ecosystems independently. This is not an insurmountable obstacle, but it necessitates adopting a proactive approach through “cooperative digital sovereignty” that is grounded in international collaboration on research and development, cross-border data flows, and global supply chains.<sup>263</sup> Crucially, a decentralized, autonomous, yet cooperative model of digital sovereignty, rooted in the internet’s “network of networks” ethos, would leverage interoperability and openness to expand agency, while preserving a wide array of technological options.<sup>264</sup>

Cooperative arrangements can offer more viable technological alternatives. Shared infrastructures, aligned regulatory frameworks, and joint capacity-building initiatives can reduce duplication while increasing leverage. By pooling resources, aligning normative regimes, and building open digital infrastructures, states can achieve economies of scale that would be impossible in isolation. To facilitate this, intergovernmental organizations like the United Nations (UN) and the Digital Cooperation Organization (DCO), alongside development banks such as the Inter-American Development Bank (IDB), the New Development Bank (NBD), the Asian Development Bank (ADB), and the African Development Bank (AfDB), have a crucial role to play, providing platforms for standard setting and resource coordination.<sup>265</sup> Such a cooperative model would allow member states to preserve their strategic autonomy while counterbalancing the influence of dominant tech-states or corporations.

This scenario requires a high level of trust and complex diplomatic and resource alignment; the difficulty lies not in identifying areas for cooperation but in institutionalizing cooperation that will remain durable under conditions of unequal capabilities and geopolitical competition.

Divergent national interests, asymmetries in technological capacity, and incentives toward concentration make collective action difficult to sustain.<sup>266</sup> Yet, the alternative scenario in which digital dependence deepens and access to compute, models, infrastructure, and standards becomes concentrated in a small number of foreign firms and jurisdictions will impose greater long-term costs on economic resilience and political agency.<sup>267</sup>

The crux of the challenge is clarifying what sovereignty means when applied to the AI technology stack. The objective cannot be complete technological self-sufficiency. Progressive, frontier AI, for instance, increasingly depends on high capital expenditures, access to advanced semiconductors, hyperscale computing infrastructure, large proprietary datasets, and network effects that reinforce incumbent advantage. Under current conditions, few states can do this, and regulatory interventions alone cannot eliminate these structural asymmetries.

Instead, sovereignty should be understood as the capacity to organize and govern strategic interdependence. States do not have to reproduce the technological model of dominant AI powers; they can pursue agency by coordinating resources across selected parts of the innovation system while maintaining diversified external linkages elsewhere.

This implies three complementary strategies. First, states should leverage industrial policy, directing public investment to support national research laboratories, domain-specific model development, public-interest datasets, sovereign cloud layers, and specialized compute infrastructure for research and strategic sectors. The objective is to foster AI development by leveraging national assets to meet real national needs.<sup>268</sup>

Second, states should design regulatory frameworks that reduce structural dependence by enabling interoperable and open technological ecosystems. Regulatory regimes matter not because they neutralize incumbent advantages but because they shape market architecture: By mandating interoperability, portability, open standards, transparent procurement, and fair access to critical infrastructure, they can lower switching costs and create space for domestic firms and public institutions to participate.

Lastly, states should support multistakeholder and multilateral governance that will distribute agenda-setting authority across governments, firms, technical communities, and public institutions rather than allowing standards and infrastructures to become privately governed. Multilateral cooperation can pool capabilities that no single state can efficiently develop.<sup>269</sup> Shared compute facilities, regional research networks, federated data infrastructures, coordinated procurement, and joint investment vehicles allow states to achieve scale without requiring national self-sufficiency.

This approach recognizes that frontier AI competition is only one dimension of technological power. Countries can still exercise meaningful influence by developing capabilities in application layers, domain-specific models, public-sector AI, specialized hardware niches, standards development, open-source ecosystems, and strategic deployment capacities.

Importantly, the above measures should also help counter weaponized interdependence. When critical AI resources are diversified across providers, governed through interoperable standards, embedded in regional partnerships, and supplemented by domestic adaptation, external actors face greater costs in converting economic dependence into political leverage. Sovereignty therefore emerges from ensuring that dependencies remain plural, negotiable, and institutionally governed.

## **KASE Operational Steps: From Concept to Implementation**

Operationalizing the KASE framework's layers requires a deliberate sequencing of actions. Sovereignty cannot be engineered in the abstract; it must be built through institutional design, regulatory calibration, sustained investment, and solid capacity building. A first step lies in establishing multistakeholder governance mechanisms capable of providing visibility on the complexity of all the layers and coordinating public and private actors that play key roles in each layer. Without such coordination, policy will remain fragmented and reactive at best.

Second, regulations must be recalibrated to prioritize interoperability, transparency, and contestability in any given layer. This includes enforcing data portability, mandating auditability for high-risk AI systems, and ensuring that standards-setting processes remain open and inclusive. Regulation, in this sense, is not constraining; instead, it becomes constitutive of digital ecosystems.

Third, industrial policy must move beyond generalized support toward targeted capability development. This entails identifying strategic entry points within different layers—whether in data infrastructures, model adaptation, public compute capacity or specific segments of the hardware value chain—and concentrating resources where meaningful benefits and durable advantages can be developed.

Such resource concentration should not aim to replicate the full technological ecosystems of leading AI powers. Frontier AI requires scale, capital, and cumulative advantages that few countries possess. Instead, states should seek strategic scale by focusing on capabilities that preserve agency, reduce vulnerability, and create leverage within global value chains. Crucially, this often requires cooperative approaches, such as shared infrastructure, coordinated investment, joint procurement, and common standards, to shape interdependence rather than passively accept it.

Fourth, capacity building must be treated as a long-term commitment rather than an auxiliary measure. Public administrations require technical expertise to govern effectively; educational systems must align with emerging skill demands; and cross-border talent mobility should be facilitated rather than restricted.

Fifth, cooperative mechanisms must be operationalized through shared (digital) infrastructures and coordinated investment frameworks. Joint procurement of compute resources, federated data spaces, and regional AI research initiatives can create economies of scale while preserving national agency. Moreover, interdependency in mutualized digital infrastructures has the potential to strongly reduce geopolitical frictions, creating a considerable incentive for cooperation.

Finally, implementation must be accompanied by continuous monitoring and adaptive governance, grounded in situational awareness.<sup>270</sup> Sovereignty is not a fixed endpoint but an evolving condition. A large number of technology scenarios must be continuously monitored and contextualized to understand and mitigate risks and take advantage of opportunities. From this perspective, metrics, audits, and iterative policy adjustments are essential to ensure that strategies remain aligned with technological and geopolitical developments.

## Being Pragmatic About AI Sovereignty

In its most idealistic form, AI sovereignty promises a level of control that the modern, interconnected world simply cannot provide. Yet abandoning the concept altogether would ignore legitimate concerns about dependency, control, and distribution of value. Hence, the solution lies in a pragmatic redefinition.

By grounding sovereignty in strategic capacity for agency, interoperability, and openness, policymakers can move beyond rhetoric to achieve substantial, yet incremental, change. The goal of the proposed framework is not to eliminate the difficult trade-offs inherent in digital policy, but rather to provide a clearer lens through which to evaluate them. It is important to remember that in a geopolitically contested and complex digital landscape, true sovereignty is neither found in isolation nor in confrontation, but in the deliberate and strategic management of interdependence.

As emphasized above, this pragmatic imperative is dictated by the material realities of the AI value chain. Defined by extreme specialization, immense capital expenditures, and entrenched network effects, frontier AI development depends on access to tightly concentrated bottlenecks, from advanced semiconductors to hyperscale compute infrastructure. In an ecosystem where incumbent advantages continuously compound, attempting to achieve complete autarky is not only economically unviable, but becomes structurally impossible.

Consequently, cultivating meaningful agency, openness, and interoperability within this concentrated landscape demands a holistic, multipronged strategic framework. Statutory oversight alone is insufficient; while adopting comprehensive legislation and ensuring its rigorous enforcement remain critical baselines, true governance requires proactive industrial policy to create the economic incentives necessary for market alignment and distributed

innovation. Furthermore, bridging the gap between structural dependency and strategic autonomy relies on establishing sound multistakeholder governance mechanisms. By deliberately fostering synergy among researchers, developers, regulators, and commercial entities, policymakers have a chance to build a collaborative ecosystem where public interest and market realities align, thus ensuring that sovereignty is achieved not through isolationist autarky, but through active, value-driven participation in the global AI value chain.

Hence, a more modest and ultimately more fruitful approach is to treat sovereignty as a matter of structured agency. Indeed, policymakers should not seek absolute self-sufficiency but instead the capacity to move strategically within constraints. The path forward will be demanding, incremental, and necessarily imperfect. But it is also, under present conditions, the only credible path to retaining sovereignty on the AI stack.

# Notes

## 01

- 1 “Launching the Digital Democracy Network,” video, posted October 19, 2021, by Carnegie Endowment for International Peace, YouTube, 4 min., <https://www.youtube.com/watch?v=PHYp6IIQzo4>; Steven Feldstein, ed., “Issues on the Frontlines of Technology and Politics,” Carnegie Endowment for International Peace, October 19, 2021, <https://carnegieendowment.org/research/2021/10/issues-on-the-frontlines-of-technology-and-politics>.
- 2 “The Price of a Vote,” video, DE! Akcióközösség, March 26, 2026, <https://www.youtube.com/watch?v=ZCwQR5HRWR8>.

## 02

- 3 “Myanmar: UN Experts Condemn Military’s ‘Digital Dictatorship,’” OHCHR, accessed February 5, 2026, <https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship>.
- 4 Fanny Potkin, “Norway’s Telenor Says Myanmar Unit Sale Plan Followed Junta’s Pressure on Surveillance Tech,” Reuters, September 15, 2021, <https://www.reuters.com/world/norways-telenor-says-myanmar-unit-sale-came-after-juntas-pressure-surveillance-2021-09-15/>.
- 5 “Myanmar’s Last Foreign Telecom, Ooredoo, to Leave Country,” The Irrawaddy, July 20, 2022, <https://www.irrawaddy.com/news/burma/myanmars-last-foreign-telecom-ooredoo-to-leave-country.html>.
- 6 Justice Initiative, “Telenor Faces Legal Action Over Human Rights Abuses in Myanmar,” Justice Initiative, October 7, 2025, <https://www.justiceinitiative.org/newsroom/telenor-faces-legal-action-over-human-rights-abuses-in-myanmar>.
- 7 Access Now, “Ooredoo’s Plans to Leave Myanmar Hands Military Full Control of Nation’s Telco Sector — It Must Mitigate the Human Rights Risks,” Access Now, n.d., accessed February 5, 2026, <https://www.accessnow.org/press-release/ooredoo-myanmar-sale/>.
- 8 Tommy Walker and Darko Janjevic, “Myanmar: Why Is Junta Shutting down Internet?,” *DW.com*, February 27, 2025, <https://www.dw.com/en/myanmar-why-is-junta-shutting-down-internet/a-71770580>.
- 9 Hannah Beech, “Myanmar’s Military Deploys Digital Arsenal of Repression in Crackdown,” *New York Times*, March 1, 2021, .
- 10 Wai Phyto Mint, “Fourth Year Under Myanmar Military’s Digital Iron Curtain: A Reflection on Digital Repression and the Path Forward,” Tech Policy Press, March 3, 2025, <https://techpolicy.press/fourth-year-under-myanmar-militarys-digital-iron-curtain-a-reflection-on-digital-repression-and-the-path-forward>.
- 11 Alena Epifanova, “Deciphering Russia’s ‘Sovereign Internet Law,’” German Council on Foreign Relations, January 16, 2020, <https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law>.
- 12 “Russia’s National DNS,” Internet Society, December 1, 2023, <https://www.internetsociety.org/resources/internet-fragmentation/russias-national-dns/>.
- 13 “Russia: Freedom on the Net 2024 Country Report,” Freedom House, 2025, <https://freedomhouse.org/country/russia/freedom-net/2024>.
- 14 Soyoung Park and Yoonmo Sang, “The Changing Role of Nation States in Online Content Governance: A Case of Google’s Handling of Government Removal Requests,” *Policy & Internet* 15, no. 3 (2023): 351–69, <https://doi.org/10.1002/poi3.342>; Sebastian Hellmeier, “The Dictator’s Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes,” *Politics & Policy* 44, no. 6 (2016): 1158–91, <https://doi.org/10.1111/polp.12189>.
- 15 Jing Feng et al., “Content Regulation Laws for Chinese ISPs: Legal Responsibilities in Free Speech and Filtering of Harmful Content,” *Law and Economy* 2, no. 11 (2023): 53–59, <https://www.paradigmexpress.org/le/article/view/868>.
- 16 Shazeda Ahmed and Steven Weber, “China’s Long Game in Techno-Nationalism,” *First Monday*, ahead of print, April 30, 2018, <https://doi.org/10.5210/fm.v22i5.8085>.
- 17 Young Xu, “Deconstructing the Great Firewall of China,” *Thousand Eyes* (blog), Cisco, March 8, 2016, <https://www.thousandeyes.com/blog/deconstructing-great-firewall-china>.
- 18 “In China, the ‘Great Firewall’ Is Changing a Generation,” Human Rights Watch, September 1, 2020, <https://www.hrw.org/news/2020/09/01/china-great-firewall-changing-generation>; Jimmy Wu and Oiwan Lam, “The Evolution of China’s Great Firewall: 21 Years of Censorship,” *Global Voices Advox*, August 30, 2017, <https://advox.globalvoices.org/2017/08/30/the-evolution-of-chinas-great-firewall-21-years-of-censorship/>.
- 19 “China Lifts Foreign Investment Access Restrictions in Manufacturing Sector\_Express\_北京市人民政府外事办公室,” Foreign Affairs Office, People’s Government of Beijing Municipality, September 12, 2024, [https://wb.beijing.gov.cn/en/express/202411/t20241111\\_3938954.html](https://wb.beijing.gov.cn/en/express/202411/t20241111_3938954.html).

- 20 “Censorship Practices of the People’s Republic of China,” US-China Economic and Security Review Commission, July 17, 2024, <https://www.uscc.gov/research/censorship-practices-peoples-republic-china>; “China - Allows 100 per Cent Foreign Ownership in Certain Value-Added Telecommunication Services,” Investment Policy Monitor, UNCTAD, April 8, 2024, <https://investmentpolicy.unctad.org/investment-policy-monitor/measures/4636/-allows-100-per-cent-foreign-ownership-in-certain-value-added-telecommunication-services>; “China to Lift Foreign Investment Limit in Value-Added Telecom Services,” Simmons & Simmons, April 16, 2024, <https://www.simmons-simmons.com/en/publications/clv4vft2100lutzeg455uhpab/china-to-lift-foreign-investment-limit-in-value-added-telecom-services>.
- 21 “Guide to Obtaining an ICP License for Your Website in China,” FDI China, December 30, 2024, <https://fdichina.com/blog/obtaining-an-icp-license/>; Henry L. Hu, “The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration,” *China Quarterly* 207 (September 2011): 523–40, <https://doi.org/10.1017/S0305741011000634>.
- 22 “China: Freedom on the Net 2024 Country Report,” Freedom House, 2025, <https://freedomhouse.org/country/china/freedom-net/2024>.
- 23 Alexander E. Voiskounsky, “The Relcom Network: An Investigation of Its Users,” *Journal of Computer-Mediated Communication* 2, no. 4 (1997): JCMC248, <https://doi.org/10.1111/j.1083-6101.1997.tb00198.x>; Andrei Soldatov and Irina Borogan, “The Kremlin Jails the Father of Russia’s Internet,” Center for European Policy Analysis, July 23, 2024, <https://cepa.org/article/russia-jails-the-father-of-russias-internet/>.
- 24 Rafal Rohozinski and UN Research Institute for Social Development, eds., *Mapping Russian Cyberspace: Perspectives on Democracy and the Net*, Discussion Paper / United Nations Research Institute for Social Development, DP 115 (UNRISD, 1999), <https://digitallibrary.un.org/record/412935>.
- 25 Liudmila Sivetc, “State Regulation of Online Speech in Russia: The Role of Internet Infrastructure Owners,” *International Journal of Law and Information Technology* 27, no. 1 (2019): 28–49, <https://doi.org/10.1093/ijlit/eay016>; “Russia Has Fastest Growing Internet Population in Europe,” Comscore, August 2008, <https://www.comscore.com/Insights/Press-Releases/2008/08/Russia-Internet-Growth>.
- 26 Muzaffar Suleymanov, “Protests Not Newsworthy to Kremlin-Controlled Media,” Committee to Protect Journalists, December 7, 2011, <https://cpj.org/2011/12/russian-protests-not-newsworthy-to-kremlin-control/>.
- 27 Liudmila Sivetc, “State Regulation of Online Speech in Russia: The Role of Internet Infrastructure Owners,” *International Journal of Law and Information Technology* 27, no. 1 (2019): 28–49, <https://doi.org/10.1093/ijlit/eay016>.
- 28 Sivetc, “State Regulation of Online Speech in Russia: The Role of Internet Infrastructure Owners.”
- 29 Freedom House, “Freedom on the Net 2015 – Russia,” Refworld, 2016, <https://www.refworld.org/reference/annualreport/freehou/2015/en/107848>; “Russia’s Internet Freedom Deteriorates to a ‘Not Free’ Rating,” *Moscow Times*, October 29, 2015, <https://www.themoscowtimes.com/2015/10/29/russias-internet-freedom-deteriorates-to-a-not-free-rating-a50549>.
- 30 Ksenia Ermoshina et al., “A Market of Black Boxes: The Political Economy of Internet Surveillance and Censorship in Russia,” *Journal of Information Technology and Politics* 19, no. 1 (2022): 18–33, <https://doi.org/10.1080/19331681.2021.1905972>.
- 31 “Russia: ‘Big Brother’ Law Harms Security, Rights,” Human Rights Watch, July 12, 2016, <https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights>.
- 32 “Ukraine’s Kherson Switches to Russian Network after Internet Cut-off — Новая Газета Европа,” *Novaya Gazeta*, May 2, 2022, <https://novayagazeta.eu/articles/2022/05/02/ukraines-kherson-switches-to-russian-network-after-internet-cut-off-news>.
- 33 Ksenia Ermoshina and Francesca Musiani, “Can Encryption Save Lives? Secure Messaging and Its Infrastructure as Loci of Convergence between Cyber Warfare and Conventional Warfare: The Case of Ukraine,” *Media, War & Conflict* 19, no. 1 (2024): 208–25, <https://doi.org/10.1177/17506352241297942>.
- 34 Eda Keremoğlu et al., “Network Topology Facilitates Internet Traffic Control in Autocracies,” *PNAS Nexus* 3, no. 3 (2024): pgae069, <https://doi.org/10.1093/pnasnexus/pgae069>.
- 35 Madison Taylor, “Understanding Tier 1 ISPs: A Comprehensive Guide,” 123NET, March 28, 2024, <https://www.123.net/blog/understanding-tier-1-isps-a-comprehensive-guide/>.
- 36 Keremoğlu et al., “Network Topology Facilitates Internet Traffic Control in Autocracies.”
- 37 Keremoğlu et al., “Network Topology Facilitates Internet Traffic Control in Autocracies.”
- 38 Victoria Klesty et al., “Focus: Military Coup Puts Telenor’s Future in Myanmar on the Line,” Reuters, May 7, 2021, <https://www.reuters.com/business/media-telecom/military-coup-puts-telenors-future-myanmar-line-2021-05-07/>.

- 39 “Rights Groups Lodge Complaint in Norway Against Telenor Over Myanmar Sanctions,” *The Irrawaddy*, August 29, 2025, <https://www.irrawaddy.com/news/burma/rights-groups-lodge-complaint-in-norway-against-telenor-over-myanmar-sanctions.html>; Alexander Vittrup, “Telenor Data Transfers Linked to Arrests and Executions in Myanmar,” *Scandasia*, August 26, 2025, <https://scandasia.com/telenor-data-transfers-linked-to-arrests-and-executions-in-myanmar/>.
- 40 “Justice For Myanmar and ICJ Norway Filed Complaint with Norwegian Police against Telenor for Violating Sanctions,” *Justice For Myanmar*, August 28, 2025, <https://www.justiceformyanmar.org/press-releases/justice-for-myanmar-and-icj-norway-filed-complaint-with-norwegian-police-against-telenor-for-violating-sanctions>.
- 41 “The Myanmar Junta’s Partners in Digital Surveillance and Censorship | Justice For Myanmar,” *Justice For Myanmar*, June 19, 2024, <https://www.justiceformyanmar.org/stories/the-myanmar-juntas-partners-in-digital-surveillance-and-censorship>; Gideon Ogunniye, “A New Anti-Democratic Tool: The Deep Packet Inspection Technique,” *Democracy in Africa*, May 4, 2023, <https://democracyinafrica.org/a-new-anti-democratic-tool-the-deep-packet-inspection-technique/>.
- 42 Caroline Henshaw and Aung Naing, “Chinese Technology Capable of Mass Surveillance ‘installed’ by Myanmar Internet Company Funded by UK,” *Finance Uncovered*, May 21, 2025, <https://financeuncovered.org/stories/british-norwegian-and-danish-governments-back-internet-provider-in-military-run-myanmar-which-hosts-notorious-chinese-surveillance-system>.
- 43 “Myanmar: ISP company denied allegations linking to the use of Chinese tech for online surveillance; incl. investors’ comments,” *Business and Human Rights Centre*, May 23, 2025, <https://www.business-humanrights.org/my/%E1%80%9E%E1%80%90%E1%80%84/myanmar-isp-company-denied-allegations-linking-to-the-use-of-chinese-tech-for-online-surveillance-incl-investors-comments/>.
- 44 David Pierson, “Military Parade Casts China as Savior in World War II,” *New York Times*, September 2, 2025, <https://www.nytimes.com/2025/09/02/world/asia/xi-putin-kim-parade.html>.
- 45 Andrea Kendall-Taylor and Richard Fontaine, “The Axis of Upheaval: How China, Russia, Iran, and North Korea Together Threaten America,” *Foreign Affairs* 103, no. 3 (May/June 2024): 10–23.
- 46 Lauren Kent et al., “Xi and Putin Overheard Talking about Immortality and Organ Transplants,” *CNN*, September 3, 2025, <https://www.cnn.com/2025/09/03/asia/xi-putin-chat-immortality-longevity-intl>.
- 47 “China: UN Human Rights Experts Alarmed by ‘Organ Harvesting’ Allegations,” *UN OHCHR*, June 14, 2021, <https://www.ohchr.org/en/press-releases/2021/06/china-un-human-rights-experts-alarmed-organ-harvesting-allegations>.
- 48 “Xi, Putin Video on ‘Living to 150’ Dropped as Chinese TV Pulls Permission,” *Al Jazeera*, September 6, 2025, <https://www.aljazeera.com/news/2025/9/6/xi-putin-video-on-living-to-150-dropped-as-chinese-tv-pulls-permission>.
- 49 “「活到150」也成敏感词: CCTV撤回影片版權,” *DW Chinese*, September 6, 2025, <https://www.dw.com/zh-hant/%E6%B4%BB%E5%88%B0150%E4%B9%9F%E6%88%90%E6%95%8F%E6%84%9F%E8%A9%9E-cctv%E6%92%A4%E5%9B%9E%E5%BD%B1%E7%89%87%E7%89%88%E6%AC%8A/a-73904983>.
- 50 老周横眉 [laozhouhengmei], “各位，我无意间发现，‘长生不老’好像已经成为墙内敏感词了。我昨晚在跟一个墙内朋友聊天。有个我们共同认识的人生了重病。然后我说现在AI让生物科技进展很快，然后说了一句：你们老大不是在聊长生不老吗？不知道你们墙内知不知道这件事。结果这句话他没收到。我还是意外发现的。” *Tweet, Twitter*, September 7, 2025, <https://x.com/laozhouhengmei/status/1964673721140232272>.
- 51 Simon Kemp, “Digital 2023: China,” *DataReportal*, February 9, 2023, <https://datareportal.com/reports/digital-2023-china>.
- 52 Yuxin Chen, “The Accuracy and Biases of AI-Based Internet Censorship in China,” *Journal of Research in Social Science and Humanities* 4, no. 2 (2025): 27–36.
- 53 Eddie Yang, “The Limits of AI for Authoritarian Control,” May 2025, [https://www.eddieyang.net/research/AI\\_dilemma.pdf](https://www.eddieyang.net/research/AI_dilemma.pdf).
- 54 Chen, The Accuracy and Biases of AI-Based Internet Censorship in China.
- 55 Chen, The Accuracy and Biases of AI-Based Internet Censorship in China.
- 56 “The Internet Coup: A Technical Analysis on How a Chinese Company Is Exporting The Great Firewall to Autocratic Regimes,” *InterSecLab*, 2025, <https://interseclab.org/wp-content/uploads/2025/09/The-Internet-Coup-September2025.pdf>.
- 57 “China’s Stability Maintenance Costs Continue to Rise,” *Defense Security Brief* 39 (March 22, 2019), <https://indsr.org.tw/respublicationcon?uid=12&resid=692&pid=2366&typeid=3>.

## 03

- 44 David Pierson, “Military Parade Casts China as Savior in World War II,” *New York Times*, September 2, 2025, <https://www.nytimes.com/2025/09/02/world/asia/xi-putin-kim-parade.html>.
- 45 Andrea Kendall-Taylor and Richard Fontaine, “The Axis of Upheaval: How China, Russia, Iran, and North Korea Together Threaten America,” *Foreign Affairs* 103, no. 3 (May/June 2024): 10–23.

58 Chang Che and Amy Chang Chien, “Memes, Puns and Blank Sheets of Paper: China’s Creative Acts of Protest,” *New York Times*, November 28, 2022, <https://www.nytimes.com/2022/11/28/world/asia/china-protests-blank-sheets.html>.

## 04

- 59 یادص: بیتاقبط نترتتیا دوجو هب نایکشزپ تلود یوگنخس ناعا” [Pezeshkian Government Spokesperson Admits Existence of Tiered Internet: “They Amplify Our Voice”], Iran International, March 10, 2026, <https://www.iranintl.com/202603104258>; Cody Combs, “Internet Blackout Leaves Iranians Offline for One Third of 2026,” *The National*, March 10, 2026, <https://www.thenationalnews.com/future/technology/2026/03/10/is-iran-internet-still-down/>.
- 60 “Transcript: Iranian Foreign Minister Abbas Araghchi on ‘Face the Nation with Margaret Brennan,’ March 15, 2026,” CBS News, updated March 15, 2026, <https://www.cbsnews.com/news/iranian-foreign-minister-abbas-araghchi-face-the-nation-transcript-03-15-2026/>.
- 61 Mahsa Alimardani, “Aggressive New Digital Repression in Iran in the Era of the Woman, Life, Freedom Uprisings,” in “New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms,” ed. Steve Feldstein, Carnegie Endowment for International Peace, November 29, 2023, <https://carnegieendowment.org/research/2023/11/new-digital-dilemmas-resisting-autocrats-navigating-geopolitics-confronting-platforms>.
- 62 “Iran: Tightening the Net 2020,” Article 19, September 2020, <https://www.article19.org/ttn-iran-november-shutdown/>; “Tightening the Net: Iran One Year On From the Mahsa Jhina Uprising,” Article 19, September 15, 2023, <https://www.article19.org/resources/tightening-the-net-iran-one-year-on-from-mahsa-jhina-amini-uprising/>; “Iran: Communication Blackout Puts Lives at Risk and Violates Human Rights,” Article 19, January 9, 2026, <https://www.article19.org/resources/iran-communication-blackout-puts-lives-at-risk-and-violates-human-rights/>.
- 63 Erika Solomon and Farnaz Fassihi, “Iran Detains Prominent Political Figures, Expanding Crackdown on Dissent,” *New York Times*, February 9, 2026, updated February 11, 2026, <https://www.nytimes.com/2026/02/09/world/europe/iran-detains-prominent-opposition-figures-expanding-crackdown-on-dissent.html>; “Iran, End the Executions,” Amnesty International, <https://amnesty.org.nz/iran-end-the-executions/>; Kay Armin Serjoie, Roxana Saberi, and Fatemeh Jamalpour, “Iran Protest Death Toll Could Top 30,000, According to Local Health Officials,” *Time*, January 25, 2026, <https://time.com/7357635/more-than-30000-killed-in-iran-say-senior-officials/>.

- 64 Ray Takeyh, Steven A. Cook, Max Boot, Elliott Abrams, Linda Robinson, and Elisa Ewers, “Gauging the Impact of Massive U.S.-Israeli Strikes on Iran,” Council on Foreign Relations, updated February 28, 2026, <https://www.cfr.org/articles/gauging-the-impact-of-massive-u-s-israeli-strikes-on-iran>; Ali Bakir, “Three Calculations, One War: Inside the Minds of the United States, Israel, and Iran,” Gulf International Forum, March 8, 2026, <https://gulfiif.org/three-calculations-one-war-inside-the-minds-of-the-united-states-israel-and-iran/>.
- 65 “Iran (Islamic Republic of) 1979 (rev. 1989),” *Constitute: The World’s Constitutions to Read, Search and Compare*, comp. and ed. Zachary Elkins, Tom Ginsburg, and James Melton, accessed September 4, 2026, [https://www.constituteproject.org/constitution/Iran\\_1989](https://www.constituteproject.org/constitution/Iran_1989).
- 66 “Tightening the Net: China’s infrastructure of oppression in Iran,” Article 19, February 9, 2026, <https://www.article19.org/resources/tightening-the-net-chinas-infrastructure-of-oppression-in-iran/>.
- 67 “Queer Resistance to Digital Oppression in the Middle East and North Africa,” Article 19, July 2024, <https://www.article19.org/queer-resistance-to-digital-oppression/#reports>.
- 68 “Iran: Tightening the Net 2020,” Article 19, September 2020, <https://www.article19.org/wp-content/uploads/2020/09/TTN-report-2020.pdf>.
- 69 Reuters Staff, “Special Report: Iran’s Leader Ordered Crackdown on Unrest—‘Do Whatever It Takes to End It,’” Reuters, December 23, 2019, <https://www.reuters.com/article/world/special-report-irans-leader-ordered-crackdown-on-unrest-do-whatever-it-take-idUSKBN1YR0QO/>.
- 70 Afsaneh Rigot, “Unplugging a Nation: Iranian Digital Workarounds in the Face of Total Blackout,” DeCenter, February 19, 2026, <https://the-decenter.ghost.io/unplugging-a-nation-iranian-digital-workarounds-in-the-face-of-total-blackout/>.
- 71 Alimardani, “Aggressive New Digital Repression in Iran in the Era of the Woman, Life, Freedom Uprisings,” Mahsa Alimardani and Sam Gregory, “Iran-Israel AI War Propaganda Is a Warning to the World,” Carnegie Endowment for International Peace, July 28, 2025, <https://carnegieendowment.org/research/2025/07/iran-israel-ai-war-propaganda-is-a-warning-to-the-world>.
- 72 Alimardani and Gregory, “Iran-Israel AI War Propaganda Is a Warning to the World.”
- 73 Mahsa Alimardani, “How Doubt Became a Weapon in Iran,” *Atlantic*, January 14, 2026, <https://www.theatlantic.com/international/2026/01/iran-disinformation-ai-protests-doubt/685608/>.
- 74 Alimardani, “How Doubt Became a Weapon in Iran.”
- 75 Shirin Anlen and Mahsa Alimardani, “How AI Content Detection Is Being Weaponized in the Iran War,” Tech

- Policy Press, March 17, 2026, <https://www.techpolicy.press/how-ai-content-detection-is-being-weaponized-in-the-iran-war/>.
- 76 Indranil Ghosh, "Iran's Internet Blackout May Become Permanent, With Access for Elites Only," *Rest of World*, January 23, 2026, <https://restofworld.org/2026/iran-blackout-tiered-internet/>.
- 77 Narges Keshavarznia, "Tiered Internet: A Case Study in Selective Access and Digital Inequality," *Filter Watch*, August 1, 2025, <https://filter.watch/english/2025/08/01/investigative-report-july-2025-tiering-internet/>.
- 78 Bruce Schneier, "Why Tehran's Two-Tiered Internet Is So Dangerous," *Foreign Policy*, February 24, 2026, <https://foreignpolicy.com/2026/02/24/tehran-internet-tiered-connectivity-shutdown/>; Narges Keshavarznia, "X Update Reveals Digital Authoritarianism in Iran: The 'White Sim Card' Scandal," *Filter Watch*, November 24, 2025, <https://filter.watch/english/2025/11/24/investigative-report-november-2025-revealing-the-depth-of-digital-discrimination/>.
- 79 Pegah Banihashemi, "Commentary: Iran's White SIM Card Scandal Reveals Privilege, State Control, and Fake Dissent," *Itemlive*, December 23, 2025, <https://itemlive.com/2025/12/23/commentary-irans-white-sim-card-scandal-reveals-privilege-state-control-and-fake-dissent/>.
- 80 Mehdi Hosseini, "With the Launch of 'Pro' SIM Card Sales, Tiered Internet Access Becomes Official in Iran," *Iran Focus*, March 2, 2026, <https://iranfocus.com/iran/57265-with-the-launch-of-pro-sim-card-sales-tiered-internet-access-becomes-official-in-iran/>.
- 81 "D2C and the Future of a Free Internet," accessed September 4, 2026, [direct2cell.org](https://direct2cell.org).
- 82 Rigot, "Unplugging a Nation."
- 83 "Manifesto for a Free Internet," Iranian Women's Coalition for Internet Freedom, March 8, 2026, [https://docs.google.com/document/u/0/d/1qyFKC6tC5f-CwNBjKUSlz0gOT5SuzanOaVBMfNci3Zw/mobilebasic?utm\\_source=ig&utm\\_medium=social&utm\\_content=link\\_in\\_bio&fbclid=PAZXh0bgNhZW0C-MTEAc3J0YwZhcHBfaWQMMjU2MjgxMDQwN-TU4AAGn232BQyNaLO6R5Gu30RnzTQpT46UUUL-B9YniKc\\_4BocIdp5T\\_kQx1IEtLoKs\\_aem\\_c9T8KKER-wMFSuzgnUp3uPw&pli=1](https://docs.google.com/document/u/0/d/1qyFKC6tC5f-CwNBjKUSlz0gOT5SuzanOaVBMfNci3Zw/mobilebasic?utm_source=ig&utm_medium=social&utm_content=link_in_bio&fbclid=PAZXh0bgNhZW0C-MTEAc3J0YwZhcHBfaWQMMjU2MjgxMDQwN-TU4AAGn232BQyNaLO6R5Gu30RnzTQpT46UUUL-B9YniKc_4BocIdp5T_kQx1IEtLoKs_aem_c9T8KKER-wMFSuzgnUp3uPw&pli=1).
- 85 Edna Mohamed, "Nepal Protest Updates: PM Oli Resigns, Parliament Torched, Airport Shut," *Al Jazeera*, September 9, 2025, <https://www.aljazeera.com/news/liveblog/2025/9/9/nepal-protests-live-nepali-congress-office-top-leaders-homes-set-on-fire>.
- 86 Hannnah Beech, "'We are in a Zero State': Scenes from the Ashes of Nepal's Capital," visuals by Atul Loke, *New York Times*, September 17, 2025, <https://www.nytimes.com/2025/09/17/world/asia/nepal-protests-arson-singha-durbar.html>.
- 87 "Nepal Moves to Block Facebook, X, YouTube and Others," *Al Jazeera*, September 4, 2025, <https://www.aljazeera.com/news/2025/9/4/nepal-moves-to-block-facebook-x-youtube-and-others>.
- 88 Amish Raj Mulmi, "From Streets to Discord: How Nepal's Gen Z Toppled a Government," *Carnegie Endowment for International Peace*, September 24, 2025, <https://carnegieendowment.org/research/2025/09/nepal-gen-z-topple-government>.
- 89 Pranav Baskar, "For Nepal's Protesters, Wealthy 'Nepo Kids' Are a Source of Outrage," *New York Times*, September 9, 2025, <https://www.nytimes.com/2025/09/09/world/asia/nepal-protests-nepo-kids-social-media.html>.
- 90 Chad de Guzman, "What to Know About the Deadly 'Gen Z' Protests Over a Social-Media Ban and 'Nepo Kids' in Nepal," *Time*, September 9, 2025, <https://time.com/7315492/nepal-gen-z-protests-social-media-nepo-kids-corruption-explainer/>.
- 91 Krishana Prasain, "Only Hamro Patro, X Respond as Nepal Bars 26 Social Sites," *Kathmandu Post*, September 5, 2025, <https://kathmandupost.com/national/2025/09/05/only-hamro-patro-x-respond-as-nepal-blocks-26-social-media-platforms-1757082149>.
- 92 The Listening Post, "#GotaGoHome: The Hashtag That Defined Sri Lanka's Revolution," video, *Al Jazeera*, July 16, 2022, <https://www.aljazeera.com/video/the-listening-post/2022/7/16/gotagohome-the-hashtag-that-defined-sri-lankas-revolution>; Alia Chughtai and Marium Ali, "How Bangladesh's 'Gen Z' Protests Brought Down PM Sheikh Hasina," *Al Jazeera*, August 7, 2024, <https://www.aljazeera.com/news/longform/2024/8/7/how-bangladeshs-gen-z-protests-brought-down-pm-sheikh-hasina>.
- 93 Helen Livingstone, "Indonesia Protests Explained: Why Did They Start and How Has the Government Responded?," *Guardian*, September 1, 2025, <https://www.theguardian.com/world/2025/sep/02/indonesia-protests-explained-start-how-has-the-government-responded>; "Clashes, Arrests as Tens of Thousands Protest Corruption in Philippines," *Al Jazeera*, September 21, 2025, <https://www.aljazeera.com/news/2025/9/21/thousands-rally-in-philippines-at-anticorruption-protests-in-manila>.

## 05

- 84 Anil Giri, "Fallen Demonstrators Declared Martyrs," *Kathmandu Post*, September 15, 2025, <https://kathmandupost.com/national/2025/09/15/fallen-gen-z-protesters-declared-martyrs>; "Nepal: Police Fire on 'Gen Z' Protest," *Human Rights Watch*, September

- 94 “Indonesia: Police Beat Protesters and Unlawfully Used Tear Gas to Crush Protests—New Investigation,” Amnesty International, December 9, 2025, <https://www.amnesty.org/en/latest/news/2025/12/indonesia-police-beat-protesters-and-unlawfully-used-tear-gas-to-crush-protests-new-investigation/>.
- 95 “Philippines: Testimony Points to Torture and Other Abuses by Police as New Protests Loom,” Amnesty International, November 24, 2025, <https://www.amnesty.org/en/latest/news/2025/11/philippines-testimony-points-to-torture-and-other-abuses-by-police-as-new-protests-loom/>.
- 96 Janjira Sombatpoonsiri, “The Promises and Pitfalls of the Social Media-Fueled Gen-Z Protests Across Asia,” *Emissary*, Carnegie Endowment for International Peace, September 30, 2025, <https://carnegieendowment.org/emissary/2025/09/social-media-gen-z-protests-nepal-indonesia-promises-pitfalls>; Erica Chenoweth and Matthew Cebul, “Why Gen-Z Is Rising,” *Journal of Democracy* 37, no. 1 (January 2026): 5-14, <https://muse.jhu.edu/pub/1/article/977940>.
- 97 Alex Maitland, et al., “Resisting the Rule of the Rich: Defending Freedom Against Billionaire Power,” Oxfam International, January 19, 2026, <https://www.oxfam.org/en/research/resisting-rule-rich>.
- 98 “Bangladesh: Government Must Remove Draconian Provisions From the Draft Cyber Security Act,” Amnesty International, August 31, 2023, <https://www.amnesty.org/en/latest/news/2023/08/bangladesh-government-must-remove-draconian-provisions-from-the-draft-cyber-security-act/>; Sudipto Ganguly, “Explainer: Why Are Bangladesh Students Protesting Against Job Quotas?,” Reuters, July 21, 2024, <https://www.reuters.com/world/asia-pacific/why-are-bangladesh-students-protesting-against-job-quotas-2024-07-18/>.
- 99 Shamsuddoza Sajen, “July 26, 2024: Crackdown Deepens, Grief Grows,” *Daily Star*, July 25, 2025, <https://www.thedailystar.net/july-rocked-bangladesh/news/july-26-2024-crackdown-deepens-grief-grows-3947851>; Mark Hallam, “UN: Up to 1,400 Killed in Bangladesh Protests Crackdown,” *Deutsche Welle*, February 12, 2025, <https://www.dw.com/en/un-up-to-1400-killed-in-bangladesh-protests-crackdown/a-71587345>.
- 100 Reuters, “Hasina Lands in India: CNN News18,” *Daily Star*, August 5, 2024, <https://www.thedailystar.net/news/bangladesh/news/hasina-lands-india-cnn-news18-3669971>.
- 101 Koh Ewe and Astudestra Ajengrastri, “Indonesian MPs Get Extra Allowance Weeks After Angry Protests Over Perks,” BBC, October 14, 2025, <https://www.bbc.com/news/articles/cly4gwr20wzo>; “Indonesia: Authorities Must Investigate Eight Deaths Following Violent Crackdown on Protests,” Amnesty International, September 1, 2025, <https://www.amnesty.org/en/latest/news/2025/09/indonesia-authorities-must-investigate-eight-deaths-following-violent-crackdown-on-protests/>.
- 102 Clea Skopeliti, “Fire Kills Three People in Indonesia After Protesters Torch Council Buildings,” *Guardian*, August 30, 2025, <https://www.theguardian.com/world/2025/aug/30/fire-kills-three-people-in-indonesia-after-protesters-storm-council-buildings-in-the-wake-of-taxi-drivers-death>.
- 103 Kathleen Magramo, “Indonesia’s Fury and Deep Resentment Rages On Despite Crackdown. Here’s What to Know,” CNN, updated September 2, 2025, <https://edition.cnn.com/2025/09/01/asia/indonesia-protests-explainer-intl-hnk>.
- 104 Rebecca Ratcliffe, “Indonesia Protests: President Scraps Lawmakers’ Perks in Bid to Calm Tensions,” *Guardian*, September 1, 2025, <https://www.theguardian.com/world/2025/sep/01/indonesia-protests-president-prabowo-subianto-scraps-lawmakers-perks>.
- 105 Reuters, “Indonesia President Makes Concessions After Days of Deadly Protests Forced Him to Scrap China Summit Trip,” CNN, August 31, 2025, <https://edition.cnn.com/2025/08/31/asia/indonesia-protest-prabowo-benefits-cut-intl-hnk>.
- 106 “Bangladesh’s Yunus Names Student Leaders in Interim Cabinet,” *Deutsche Welle*, August 9, 2024, <https://www.dw.com/en/bangladeshs-yunus-names-student-leaders-in-interim-cabinet/a-69897305>.
- 107 Tulsi Rauniyar, “The Inside Story of How Gen Z Toppled Nepal’s Leader and Chose a New One on Dscord,” *Wired*, November 4, 2025, <https://www.wired.com/story/nepal-discord-gen-z-protests-vote-prime-minister-election/>.
- 108 UNB, Dhaka, “Awami League Can’t Take Part in National Election: Yunus Tells UK Minister,” *Daily Star*, November 14, 2025, <https://www.thedailystar.net/news/bangladesh/elections/news/awami-league-cant-take-part-national-election-yunus-tells-uk>.
- 109 VoteBD, “All Candidate List,” SHUJAN (Shushashoner Jonno Nagorik), accessed September 9, 2026, <https://www.votebd.org/election-result/all-candidate-list?party=56a5e63d2d3f0c241322fc0d>.
- 110 Shafi Md Mostofa, “Bangladesh Jamaat-e-Islami Draws NCP and LDP Into an Islamist Alliance,” *Diplomat*, January 2, 2026, <https://thediplomat.com/2026/01/bangladesh-jamaat-e-islami-draws-ncp-and-ldp-into-an-islamist-alliance/>.
- 111 Sarah Shamim, “Bangladesh Election Results 2026: Who Won, Who Lost, What’s Next?,” Al Jazeera, February 13, 2026, <https://www.aljazeera.com/news/2026/2/13/bangladesh-election-results-2026-who-won-who-lost-whats-next>.
- 112 Shamim, “Bangladesh Election Results 2026.”
- 113 Reuters and AFP, “Tarique Rahman Sworn In as Bangladesh’s PM After Landslide Election Victory,” *Dawn*, February 17, 2026, <https://www.dawn.com/news/1973874>.

- 114 Star Report, "Only 7 Women Make it to Parliament," *Daily Star*, February 14, 2026, <https://www.thedailystar.net/news/national-election-2026/news/only-7-women-make-it-parliament-4105636>.
- 115 Mehedi Hasan Marof, "Nahid Islam and the Uneasy Alliance That Could Shape Bangladesh's Vote," *Al Jazeera*, February 11, 2026, <https://www.aljazeera.com/features/2026/2/11/nahid-islam-and-the-uneasy-alliance-that-could-shape-bangladeshs-vote>.
- 116 Yashraj Sharma, "Has Bangladesh's New PM Named Student Leaders to His Cabinet?," *Al Jazeera*, February 17, 2026, <https://www.aljazeera.com/news/2026/2/17/has-bangladeshs-new-pm-named-student-leaders-to-his-cabinet>.
- 117 "Speakers: One-Third of Bangladeshis Are Youth, but Many Remain Unemployed," *Dhaka Tribune*, August 11, 2025, <https://www.dhakatribune.com/bangladesh/388682/speakers-at-bonik-barta-and-pstc-roundtable-stress>.
- 118 Sarah Shamim, "Bangladesh Referendum: The Big Post-Election Flashpoint?," *Al Jazeera*, February 19, 2026, <https://www.aljazeera.com/news/2026/2/19/bangladesh-referendum-the-big-post-election-flashpoint>.
- 119 Gopal Sharma, "Nepal Ex-Rapper's Party Wins Election In Landslide After Gen Z Protests," *Reuters*, March 12, 2026, updated March 13, 2026, <https://www.reuters.com/world/china/nepal-ex-rappers-party-wins-election-landslide-after-gen-z-protests-2026-03-13/>.
- 120 Hannah Beech, Binod Ghimire, and Sajal Pradhan, "He Raps, He Rants, He promises Change. Meet Nepal's Presumptive New Leader," *New York Times*, March 9, 2026, <https://www.nytimes.com/2026/03/09/world/asia/balendra-shah-nepal-prime-minister.html>.
- 121 Saurabh Sharma, "Nepal's Rapper-Mayor Balendra Shah Poised to Become Prime Minister," *Reuters*, February 24, 2026, updated March 6, 2026, <https://www.reuters.com/business/media-telecom/nepals-rapper-mayor-pole-position-become-prime-minister-2026-02-25/>; Bibek Bhandari, "Nepal's New Government Signals Shift in India, China Relations," *South China Morning Post*, March 11, 2026, updated March 12, 2026, <https://www.scmp.com/week-asia/politics/article/3346179/nepals-new-government-signals-shift-india-china-relations>.
- 122 Mahima Joshi, *News18.com*, "'F\*\*k America, India, China': Nepal PM Frontrunner Balen Shah's 2025 Post Goes Viral, Triggers Outrage," *News18*, March 6, 2026, <https://www.news18.com/world/fk-america-india-china-nepal-pm-frontrunner-balen-shahs-2025-post-goes-viral-triggers-outrage-9945639.html>.
- 123 Hannah Beech, Sajal Pradhan, and Binod Ghimire, "Gen Z-Backed Rapper Is on Course to Lead Nepal With Landslide Win," *New York Times*, March 7, 2026, <https://www.nytimes.com/2026/03/07/world/asia/nepal-election-rapper-balen-genz.html>.
- 124 Arunoday Mukharji, Mir Sabbir, Anbarasan Ethirajan, and Ewan Somerville, "Bangladesh's Ousted Leader Sheikh Hasina Sentenced to Death," *BBC*, November 17, 2025, <https://www.bbc.com/news/articles/cpwvge99e8vdo>.
- 125 This dynamic is evident in Russia's systematic use of bots and trolls during the 2016 U.S. presidential election, Myanmar's manipulation of Facebook to incite violence during the 2021 coup, India's digital campaigns targeting critics and promoting government narratives, and the United States' digital public diplomacy, including Pentagon-run influence operations abroad. See Brittany Kaiser, *Targeted: My Inside Story of Cambridge Analytica and How Trump and Facebook Broke Democracy* (Harper Collins, 2019); Barbara Ortutay, "Amnesty report finds Facebook amplified hate ahead of Rohingya massacre in Myanmar," *PBS News*, September 29, 2022, <https://www.pbs.org/newshour/world/amnesty-report-finds-facebook-amplified-hate-ahead-of-rohingya-massacre-in-myanmar>; Saroj K. Aryal and Simant S. Bharti. "Changing the Media Landscape in India under the Modi Government: A Case Study Based on the Narrative Policy Framework," *Studia z Polityki Publicznej* 9, no. 3 (2022): 47–64, [https://www.researchgate.net/publication/366006559\\_Changing\\_the\\_media\\_landscape\\_in\\_India\\_under\\_the\\_Modi\\_government\\_a\\_case\\_study\\_based\\_on\\_the\\_Narrative\\_Policy\\_Framework](https://www.researchgate.net/publication/366006559_Changing_the_media_landscape_in_India_under_the_Modi_government_a_case_study_based_on_the_Narrative_Policy_Framework); and Chris Bing and Joel Schectman. "Pentagon ran a secret anti-vax campaign to undermine China during pandemic," *Reuters*, June 14, 2024, <https://www.reuters.com/investigates/special-report/usa-covid-propaganda/>.
- 126 Frank C.S. Liu, "Taiwan's Status-Quo Preferences Reassessed: An Update of the Identity Patterns," paper presented at the American Political Science Association Annual Meeting, Vancouver, Canada, September 13, 2025.
- 127 "Taiwan Social Change Survey, Round 8, Wave 5 (2024): Digital Society and Technology and Risk," Institute of Sociology, Academia Sinica, 2024, accessed March 30, 2026, <https://www2.ios.sinica.edu.tw/sc/en/home2.php>.
- 128 "Taiwan's Election and Democratization Study, 2020–2024 (IV): The Survey of Presidential and Legislative Elections, 2024 (TEDS2024)," National Chengchi University Election Study Center, 2024, accessed March 30, 2026, [https://teds.nccu.edu.tw/intro2/super\\_pages.php?ID=intro11&Sn=201](https://teds.nccu.edu.tw/intro2/super_pages.php?ID=intro11&Sn=201).
- 129 Yip Wai Yee "TikTok and Xiaohongshu are China's new tools in Taiwan," *Straits Times*, June 17, 2025, <https://www.straitstimes.com/opinion/tiktok-and-xiaohongshu-are-chinas-new-tools-in-taiwan>.
- 130 Donie O'Sullivan, Curt Devine, and Allison Gordon. "China is using the world's largest known online disinformation operation to harass Americans, a CNN review finds," *CNN*, November 13, 2023, <https://www.cnn.com/2023/11/13/us/china-online-disinformation-invs>.

- 131 Parth P. Prasad, “‘Duelling Narratives’: The Cross-Strait Propaganda War Between Chinese and Taiwanese Media,” *Modern Diplomacy*, November 12, 2024, <https://modern diplomacy.eu/2024/11/12/duelling-narratives-the-cross-strait-propaganda-war-between-chinese-and-taiwanese-media/>.
- 132 Raphael Satter and Raphael Satter, “US Scrutinizes Chinese AI for Ideological Bias, Memo Shows,” *Reuters*, July 9, 2025, sec. China, <https://www.reuters.com/world/china/us-scrutinizes-chinese-ai-ideological-bias-memo-shows-2025-07-09/>.

## 07

- 133 Bethan McKernan and Harry Davies, “‘The Machine Did It Coldly’: Israel Used AI to Identify 37,000 Hamas Targets,” *Guardian*, April 3, 2024, <https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes>; Michael N. Schmitt, “Israel–Hamas 2024 Symposium—The Gospel, Lavender, and the Law of Armed Conflict,” *Articles of War*, June 28, 2024, <https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/>.
- 134 Greg Miller, “Israel Targets Iran’s Leaders with Lethal Expertise Using New AI Platform,” *Washington Post*, March 30, 2026, <https://www.washingtonpost.com/world/2026/03/30/iran-israel-war-killings/>; Nilza Amaral, “The Iran War Highlights the Creeping Use of AI in Warfare,” *Chatham House*, March 27, 2026, <https://www.chathamhouse.org/2026/03/iran-war-highlights-creeping-use-ai-warfare>.
- 135 Eric Talbot Jensen, “*Autonomy and Precautions in the Law of Armed Conflict*,” *International Law Studies* 96, no. 577 (2020).
- 136 Jimena Sofia Viveros Álvarez, “The Risks and Inefficacies of AI Systems in Military Targeting Support,” *Humanitarian Law & Policy* (blog), International Committee of the Red Cross, September 4, 2024, <https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/>.
- 137 Emelie Andersin, “The Use of ‘Lavender’ in Gaza and the Law of Targeting: AI-Decision Support Systems and Facial Recognition Technology,” *Journal of International Humanitarian Legal Studies* 16, no. 336 (2025); Ingvild Bode & Ishmael Bhila, “The Problem of Algorithmic Bias in AI-Based Military Decision Support Systems,” *Humanitarian Law & Policy* (blog), International Committee of the Red Cross, September 3, 2024, <https://blogs.icrc.org/law-and-policy/2024/09/03/the-problem-of-algorithmic-bias-in-ai-based-military-decision-support-systems/>; Jessica Dorsey and Luke Moffett, “The Warification of International Humanitarian Law and

the Artifice of Artificial Intelligence in Decision-Support Systems: Restoring Balance Through the Legitimacy of Military Operations,” *Yearbook of International Humanitarian Law* 27, no. 125 (2026); Jessica Dorsey and Marta Bo, “AI-Enabled Decision-Support Systems in the Joint Targeting Cycle: Legal Challenges, Risks, and the Human(e) Dimension,” *International Law Studies* 107, no. 184 (2026); Taylor Kate Woodcock, “Human/Machine(-Learning) Interactions, Human Agency and the International Humanitarian Law Proportionality Standard,” *Global Society* 38, no. 100 (2024).

- 138 Alexandra D. Kaplan et. al., “Trust in Artificial Intelligence: Meta-Analytic Findings,” *Human Factors* 65, no. 337 (2023); Berkeley J. Dietvorst et. al., “Algorithm Aversion: People Erroneously Avoid Algorithms After Seeing Them Err,” *Journal of Experimental Psychology: General* 144, no. 114 (2015).
- 139 The manuscript is currently under review and we would be pleased to share the draft upon request.
- 140 Yuval Shany and Yahli Shereshevsky, “Military AI and the Specter of the Limitless War,” *International Law Studies* 107, no. 106 (2026).
- 141 Harry Davies, Bethan McKernan, and Dan Sabbagh, “‘The Gospel’: How Israel Uses AI to Select Bombing Targets in Gaza,” *Guardian*, December 1, 2023, <https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-target>.
- 142 Other potential solutions discussed in the paper include outright or partial bans on certain military AI systems, such as LAWS or inadequately supervised DSS, the imposition of operational constraints that slow and structure human involvement in targeting decisions, and a more robust application of jus ad bellum necessity and proportionality throughout the conflict.

## 08

- 143 “Global AI Governance Action Plan,” Ministry of Foreign Affairs, People’s Republic of China, July 26, 2025, [https://www.fmprc.gov.cn/eng/xw/zyxw/202507/t20250729\\_11679232.html](https://www.fmprc.gov.cn/eng/xw/zyxw/202507/t20250729_11679232.html); “Chinese Premier Calls for Early Formation of Global AI Governance Framework,” State Council, People’s Republic of China, [https://english.www.gov.cn/news/202507/26/content\\_WS6884bea8c6d0868f4e8f4732.html](https://english.www.gov.cn/news/202507/26/content_WS6884bea8c6d0868f4e8f4732.html).
- 144 Marco Rubio, “Withdrawal from Wasteful, Ineffective, or Harmful International Organizations,” press statement, U.S. Department of State, January 7, 2026, <https://www.state.gov/releases/office-of-the-spokesperson/2026/01/withdrawal-from-wasteful-ineffective-or-harmful-international-organizations>.

- 145 Arun Sukumar and Arindrajit Basu, "Back to the Territorial State: China and Russia's Use of UN Cybercrime Negotiations to Challenge the Liberal Cyber Order," *Journal of Cyber Policy* 9, no. 2 (December 13, 2024): 256-287, <https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2436591>.
- 146 Sukumar and Basu, "Back to the Territorial State."
- 147 Henry Farrell and Abraham L. Newman, "The Janus Face of the Liberal International Information Order: When Global Institutions Are Self-Undermining," *International Organization* 75, no. 2 (2021): 333-358, <https://doi.org/10.1017/S0020818320000302>.
- 148 Tania Branigan, "Great Firewall of China," *Guardian*, November 12, 2004, <https://www.theguardian.com/technology/2004/nov/12/newmedia.china>.
- 149 Martina Lucaccini, "Digital Authoritarianism: ICT-Enabled Repression Across Regime Types," Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), February 2, 2025, [https://osf.io/preprints/socarxiv/rvmj2\\_v1](https://osf.io/preprints/socarxiv/rvmj2_v1).
- 150 Lisa Garbe and Seraphine F. Maerz, "The Rise of Authoritarian Informationalism: Escalating Surveillance, Manipulation, and Control," *Democratization* 33, no. 1 (2026), <https://doi.org/10.1080/13510347.2025.2579105>.
- 151 Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (Oxford: Oxford University Press, 2021); Andre Barrinha and Thomas Renard, "The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace," Council on Foreign Relations, June 10, 2020, <https://www.cfr.org/articles/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace>.
- 152 Joshua Kurlantzick and James West, "Assessing China's Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms?," Council on Foreign Relations, accessed September 9, 2026, <https://www.cfr.org/china-digital-silk-road/>.
- 153 Alvin Camba and Jessica C. Liao, "Coded Dependence: How China's AI Expansion Is Locking in Southeast Asia," *Diplomat*, June 20, 2025, <https://thediplomat.com/2025/06/coded-dependence-how-chinas-ai-expansion-is-locking-in-southeast-asia/>; Cole McFaul and Peter Engelke, "Navigating the US-PRC Tech Competition in the Global South," Atlantic Council, April 16, 2025, <https://www.atlanticcouncil.org/in-depth-research-reports/report/navigating-the-us-prc-tech-competition-in-the-global-south/>.
- 154 Julian E. Barnes, "White House Official Says Huawei Has Secret Back Door to Extract Data," *New York Times*, February 11, 2020, <https://www.nytimes.com/2020/02/11/us/politics/white-house-huawei-back-door.html>;
- 155 McFaul and Engelke, "Navigating the US-PRC Tech Competition in the Global South"; Beijing has also supported its infrastructural push with targeted diplomacy in select technical forums. China has strategically packed technical standards bodies like the International Telecommunication Union with corporate representatives and handpicked academics to shape global 5G rules, conferring important advantages on firms like Huawei and ZTE.
- 156 Jennifer Bouey, et al., "China's AI Exports: Technology Distribution and Data Safety," Rand, December 11, 2023, [https://www.rand.org/pubs/research\\_reports/RRA2696-2.html](https://www.rand.org/pubs/research_reports/RRA2696-2.html); Valentin Weber, "Data-Centric Authoritarianism: How China's Development of Frontier Technologies Could Globalize Repression," National Endowment for Democracy, February 11, 2025, <https://www.ned.org/data-centric-authoritarianism-how-chinas-development-of-frontier-technologies-could-globalize-repression-2/>.
- 157 United Nations General Assembly, "Enhancing International Cooperation on Capacity-Building of Artificial Intelligence," A/RES/78/311 (July 1, 2024), <https://docs.un.org/en/A/RES/78/311>.
- 158 "Group of Friends for International Cooperation on AI Capacity-Building Formally Established," Permanent Mission of the People's Republic of China to the UN, December 5, 2024, [https://un.china-mission.gov.cn/eng/czthd/202412/t20241220\\_11508534.htm](https://un.china-mission.gov.cn/eng/czthd/202412/t20241220_11508534.htm).
- 159 "AI Capacity-Building Event Hosted by China and Zambia at UN," China Association for Science and Technology, May 16, 2025, [https://english.cast.org.cn/xkx/fzlm/syzsxx/art/2025/art\\_1711677228.html](https://english.cast.org.cn/xkx/fzlm/syzsxx/art/2025/art_1711677228.html).
- 160 "Global AI Governance Action Plan," Permanent Mission of the People's Republic of China to the UN, July 26, 2025, [https://un.china-mission.gov.cn/eng/zgyw/202507/t20250729\\_11679232.htm](https://un.china-mission.gov.cn/eng/zgyw/202507/t20250729_11679232.htm).
- 161 "AI Capacity-Building Action Plan for Good and for All," Ministry of Foreign Affairs, People's Republic of China, updated September 27, 2024, [https://www.mfa.gov.cn/eng/wjbzhd/202409/t20240927\\_11498465.html](https://www.mfa.gov.cn/eng/wjbzhd/202409/t20240927_11498465.html).
- 162 "China-BRICS AI Development & Cooperation Centre," profile, Global Community on AI for Industry and Manufacturing, <https://aim.unido.org/participations/586958>; "First China-ASEAN AI Innovation Cooperation Center Opens in Laos," International Center for Science & Technology Innovation, February 25, 2025, [https://en.ncsti.gov.cn/Latest/news/202502/t20250226\\_196914.html#:~:text=Share%2DWeChat&text=China's%20Guangxi%20Zhuang%20Autonomous%20Region,independent%20and%20controllable%20AI%20models..](https://en.ncsti.gov.cn/Latest/news/202502/t20250226_196914.html#:~:text=Share%2DWeChat&text=China's%20Guangxi%20Zhuang%20Autonomous%20Region,independent%20and%20controllable%20AI%20models..)
- 163 Fergus Ryan, et al., "The Party's AI: How China's New AI Systems Are Reshaping Human Rights," Australian Strategic Policy Institute, December 2025, <https://aspi.s3.ap-southeast-2.amazonaws.com/wp-content/uploads/2025/11/27122307/The-partys-AI-How-Chinas-new-AI-systems-are-reshaping-human-rights.pdf>.

- 164 J.D. Vance, "Remarks by the Vice President at the Artificial Intelligence Action Summit in Paris, France," speech, *The American Presidency Project*, February 11, 2025, <https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france>.
- 165 Merve Hickok and Marc Rotenberg, "US Delegation Heads to India AI Summit Intent on 'Domination,'" *Tech Policy Press*, February 16, 2026, <https://www.techpolicy.press/us-delegation-heads-to-india-ai-summit-intent-on-domination/>.
- 166 "India and the World Should Build Only on American AI Stack: US AI Advisor Sriram Krishnan," *Economic Times*, February 19, 2026, <https://economictimes.indiatimes.com/tech/artificial-intelligence/india-and-the-world-should-build-only-on-american-ai-stack-us-ai-advisor-sriram-krishnan/articleshow/128515700.cms?from=mdr>.
- 167 "Winning the Race: America's AI Action Plan," Office of Science and Technology Policy, Executive Office of the President of the United States, July 2025, <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>.
- 168 David DiMolfetta, "State Department Cuts Hit Cyber Diplomats Doing International Engagements," *Nextgov/FCW*, July 15, 2025, <https://www.nextgov.com/people/2025/07/state-department-cuts-hit-cyber-diplomats-doing-international-engagements/406727/>.
- 169 Luis Barrueto and Mohammed Al-Maskati, "How U.S. Funding Cuts Expose Civil Society to Digital Attacks," *Access Now*, April 9, 2025, <https://www.accessnow.org/u-s-funding-cuts/>.
- 170 Donald J. Trump, "Withdrawing the United States from International Organizations, Conventions, and Treaties that Are Contrary to the Interests of the United States," presidential memoranda, The White House, January 7, 2026, <https://www.whitehouse.gov/presidential-actions/2026/01/withdrawing-the-united-states-from-international-organizations-conventions-and-treaties-that-are-contrary-to-the-interests-of-the-united-states/>; Freedom Online Coalition, accessed September 9, 2026, <https://freedomonlinecoalition.com/>; Trump, "Withdrawing the United States from International Organizations, Conventions, and Treaties that Are Contrary to the Interests of the United States."
- 171 Tamsin Lee-Smith and Jelena Cosic, "At the UN, China Is Deploying a Growing Army of Puppet Organizations to Monitor and Intimidate Human Rights Activists," *International Consortium of Investigative Journalists*, April 28, 2025, <https://www.icij.org/investigations/china-targets/united-nations-ngo-gongo-intimidate-human-rights/>.
- 172 Arindrajit Basu, "The Third Way: Why Rising Powers Reject U.S.-China Digital Models," *New America*, August 13, 2025, <https://www.newamerica.org/insights/the-third-way-why-rising-powers-reject-uschina-digital-models/>.

## 09

- 173 Dana Alomar, "AI Is Becoming Infrastructure—And the UAE Is Exporting It," *Wired*, February 20, 2026, <https://www.wired.me/story/ai-is-becoming-infrastructure-and-the-uae-is-exporting-it>.
- 174 "UAE to Deploy 8 Exaflop Supercomputer in India to Strengthen Local Sovereign AI Infrastructure," *G42*, February 20, 2026, <https://www.g42.ai/resources/news/uae-deploy-8-exaflop-supercomputer-india-strengthen-local-sovereign-ai-infrastructure>.
- 175 Neesha Salian, "G42, Indian Govt Formalise Framework for Deployment of AI Supercomputer," *Gulf Business*, May 16, 2026, <https://gulfbusiness.com/en/2026/tech/g42-indian-govt-formalise-framework-for-deployment-of-ai-supercomputer/>.
- 176 Jeremy Jurgens, "The Myth of Sovereignty," *Foreign Policy*, March 9, 2026, <https://foreignpolicy.com/2026/03/09/artificial-intelligence-ai-sovereignty-taiwan-semiconductor-manufacturing-tsmc-chip-supply-chain-united-states-china/>.
- 177 Hilda Barasa, PeiChin Tay, Keegan McBride, Alexander Iosad, and Jakob Mökander, "Sovereignty in the Age of AI: Strategic Choices, Structural Dependencies and the Long Game Ahead," *Tony Blair Institute for Global Change*, January 19, 2026, <https://institute.global/insights/tech-and-digitalisation/sovereignty-in-the-age-of-ai-strategic-choices-structural-dependencies>; Brooke Tanner, et al., "Is AI Sovereignty Possible? Balancing Autonomy and Interdependence," *Brookings*, February 17, 2026, <https://www.brookings.edu/articles/is-ai-sovereignty-possible-balancing-autonomy-and-interdependence/>.
- 178 Juan N. Pava, Caroline Meinhardt, Elena Cryst, and James Landay, "AI Sovereignty's Definitional Dilemma," *Stanford HAI*, February 17, 2026, <https://hai.stanford.edu/news/ai-sovereignitys-definitional-dilemma>.
- 179 Swarnim Shrivastava, "Rethinking Sovereign AI as Strategy," *Tech Policy Press*, March 3, 2026, <https://www.techpolicy.press/rethinking-sovereign-ai-as-strategy/>.
- 180 Pablo Chavez, Vivek Chilukuri, and Ruby Scanlon, "Sovereign AI Index," *CNAS: Center for a New American Security*, accessed September 10, 2026, <https://interactives.cnas.org/reports/sovereign-ai-index/>.
- 181 Chavez, Chilukuri, and Scanlon, "Sovereign AI Index."
- 182 Chavez, Chilukuri, and Scanlon, "Sovereign AI Index."
- 183 Mohamed Elbashir and Kishore Balaji Desikachari, "India's Path to AI Autonomy," *Atlantic Council*, March 13, 2025, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/indias-path-to-ai-autonomy/>.
- 184 Press Information Bureau, Ministry of Electronics & IT, "In Less Than 24 Months, India AI Mission Has Set Up a Foundation for Development of AI Ecosystem in the Country," *Government of India*, February

- 13, 2026, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2227612&reg=3&lang=2>.
- 185 Padmini Dhruvaraj, "India's Sovereign AI Push Crosses \$5.5 Billion in Funding: Tracxn," *New Indian Express*, February 21, 2026, <https://www.newindianexpress.com/business/2026/Feb/21/indias-sovereign-ai-push-crosses-55-billion-in-funding-tracxn>.
- 186 Press Information Bureau, Ministry of Electronics & IT, "In Less Than 24 Months, India AI Mission Has Set Up a Foundation for Development of AI Ecosystem in the Country."
- 187 Janakiram MSV, "India Pitches Sovereign AI as the Alternative to Big Tech Dependence," *Forbes*, February 23, 2026, <https://www.forbes.com/sites/janakirammsv/2026/02/23/india-pitches-sovereign-ai-as-the-alternative-to-big-tech-dependence/>.
- 188 Press Information Bureau, Ministry of Electronics & IT, "Cabinet Approves Over Rs 10,300 Crore for IndiaAI Mission, Will Empower AI Startups and Expand Compute Infrastructure Access," Government of India, March 7, 2024, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2012375&reg=3&lang=2>; John Popko, "The Myth of Sovereign AI: Countries Rely on U.S. and Chinese Tech," *Rest of World*, September 12, 2025, <https://restofworld.org/2025/chinese-us-tech-foreign-ai-dependence/>.
- 189 TOI Tech Desk, "India to More Than Double Its GPU Capacity in Six Months, Says IT Minister Ashwini Vaishnaw at AI Summit," *Times of India*, February 17, 2026, <https://timesofindia.indiatimes.com/technology/tech-news/india-to-more-than-double-its-gpu-capacity-in-six-months-says-it-minister-ashwini-vaishnaw-at-ai-summit/articleshow/128460540.cms>.
- 190 Suraksha P, "IndiaAI Mission Adds 3,850 More GPUs, Expands Cluster Beyond 38,000 Units," *GCCWorld* from the *Economic Times*, August 18, 2025, <https://gcc.economicstimes.indiatimes.com/news/ai-automation/indiaai-mission-expands-gpu-cluster-to-over-38000-units-with-new-additions/123356950>; Janakiram MSV, "India's Sovereign AI Stack Is Already Built on American Cloud," *Forbes*, February 23, 2026, <https://www.forbes.com/sites/janakirammsv/2026/02/23/indias-sovereign-ai-stack-is-already-built-on-american-cloud/>.
- 191 Jaideep Prabhu, Priyank Narayan, and Mukesh Sud, "India's Frugal AI Models Are a Blueprint for Resource-Strapped Nations," *Rest of World*, April 7, 2026, <https://restofworld.org/2026/india-frugal-ai-sarvam-krutrim-sovereign/>.
- 192 Mark Scott, "How Much Would Sovereign AI Cost?," *Digital Politics*, May 11, 2025, <https://www.digitalpolitics.co/newsletter097/?ref=digital-politics-newsletter>.
- 193 Mohammed Sergie, "UAE Touts \$148B Investment in AI," *Semafor*, November 7, 2025, <https://www.semafor.com/article/11/07/2025/uae-says-its-invested-148b-in-ai-since-2024>; Alireza Haghighi and Khalid Alaamer, "Data, AI and Energy Are Reshaping the GCC Region and Its Global Alliances. Here's How," World Economic Forum, February 24, 2026, <https://www.weforum.org/stories/emerging-technologies/data-ai-energy-the-gcc-global-alliances/>.
- 194 Mohammed Soliman, "AI, the Gulf, and the US: A Primer," Middle East Institute, February 26, 2026, <https://mei.edu/report/ai-the-gulf-and-the-us-a-primer/>.
- 195 "MENA Politics Newsletter 9(1) – Spring 2026," APSA MENA Politics, accessed September 10, 2026, <https://apsamena.org/mena-politics-newsletter/mena-politics-newsletter-91-spring-2026/>.
- 196 "G42," *Dealroom.co*, accessed September 10, 2026, [https://app.dealroom.co/companies/group\\_42](https://app.dealroom.co/companies/group_42).
- 197 Gregory C. Allen, Georgia Adamson, Lennart Heim, and Sam Winter-Levy, "The United Arab Emirates' AI Ambitions," Center for Strategic and International Studies, January 24, 2025, <https://www.csis.org/analysis/united-arab-emirates-ai-ambitions>.
- 198 Virpratap Vikram Singh, "Sovereign AI: Pathways to Strategic Autonomy," International Institute for Strategic Studies, August 28, 2025, <https://www.iiss.org/online-analysis/charting-cyberspace/2025/08/sovereign-ai-pathways-to-strategic-autonomy/>.
- 199 Allen, Adamson, Heim, and Winter-Levy, "The United Arab Emirates' AI Ambitions."
- 200 Federico Maccioni, Manya Saini, and Yousef Saba, "UAE to Build Biggest AI Campus Outside US in Trump Deal, Bypassing Past China Worries," *Reuters*, May 15, 2025, updated May 15, 2025, <https://www.reuters.com/world/china/uae-set-deepen-ai-links-with-united-states-after-past-curbs-over-china-2025-05-15/>.
- 201 Andrea Benito, "UAE's TII Challenges Big Tech Dominance With Open Source Falcon AI Models," *Computer Weekly*, February 9, 2026, <https://www.computerweekly.com/news/366638759/UAEs-TII-challenges-big-tech-dominance-with-open-source-Falcon-AI-models>; Mohamed bin Zayed University of Artificial Intelligence (MBZUAI), "Inception, Cerebras and MBZUAI Release Jais 2—The Next Generation of the World's Leading Arabic Open-Weight LLM," PR Newswire, December 9, 2025, <https://www.prnewswire.com/ae/news-releases/inception-cerebras-and-mbzuai-release-jais-2--the-next-generation-of-the-worlds-leading-arabic-open-weight-llm-302636745.html>; "K2 Horizon: Open-Source AI Models for Every Scale," Institute of Foundation Models, accessed September 10, 2026, <https://ifm.ai/k2/>.
- 202 Barasa, Tay, McBride, Iosad, and Mökander, "Sovereignty in the Age of AI."
- 203 Popko, "The Myth of Sovereign AI"; Cade Metz and Tripp Mickle, "OpenAI Says It Will Build Massive Data Centers in the U.A.E.," *New York Times*, May 22, 2025, <https://www.nytimes.com/2025/05/22/technology/openai-uae-data-centers.html>; Mohammed Soliman, "From Crude to Compute: Building the GCC AI Stack," Middle East

Institute, December 10, 2025, <https://mei.edu/report/from-crude-to-compute-building-the-gcc-ai-stack/>.

204 Popko, “The Myth of Sovereign AI.”

205 Jurgens, “The Myth of Sovereignty.”

206 Tanner, et al., “Is AI Sovereignty Possible?”

207 Indranil Ghosh, “India’s AI Deal with the UAE Challenges U.S. Cloud Dominance,” Rest of World, June 1, 2026, <https://restofworld.org/2026/india-uae-g42-cerebras-ai-sovereignty/>.

## 10

208 “Cambodia: Stop Harassment of Opposition Figures in Thailand,” Amnesty International, December 27, 2019, <https://www.amnesty.org/es/wp-content/uploads/2021/05/ASA2316322019ENGLISH.pdf>; Caleb Quinley, “‘We Thought We Were Safe’: Repression and Forced Return of Refugees in Thailand,” Human Rights Watch, May 16, 2024, <https://www.hrw.org/feature/2024/05/16/we-thought-we-were-safe/repression-and-forced-return-of-refugees-in-thailand>.

209 “Court Convicts 36 Former Opposition Activists in Latest Mass Trial,” LICADHO: Cambodian League for the Promotion and Defense of Human Rights, December 22, 2022, <https://www.licadho-cambodia.org/articles/20221222/179/index.html>.

210 “Thailand: ‘Swap Mart’ Targets Foreign Dissidents, Refugees: Stop Assisting Neighboring Countries’ Transnational Repression,” Human Rights Watch, May 15, 2024, <https://www.hrw.org/news/2024/05/15/thailand-swap-mart-targets-foreign-dissidents-refugees>.

211 Nate Schenkkan, “The Golden Age of Transnational Repression,” *Journal of Democracy* 36, no. 4 (October 2025): 36–50, <https://www.journalofdemocracy.org/articles/the-golden-age-of-transnational-repression/>; Nicole Curato and Diego Fossati, “Authoritarian Innovations: Crafting Support for a Less Democratic Southeast Asia,” *Democratization* 27, no. 6 (2020): 1006–20, <https://doi.org/10.1080/13510347.2020.1777985>.

212 Marcus Michaelson, “The Digital Transnational Repression Toolkit, and Its Silencing Effects,” Freedom House, 2020, <https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects>.

213 Saipira Furstenberg, Marcus Michaelson, and Siena Anstis, “Transnational Repression of Human Rights Defenders: The Impacts on Civic Space and the Responsibility of Host States,” European Parliament, June 2025, [https://www.europarl.europa.eu/RegData/etudes/STUD/2025/754475/EXPO\\_STU\(2025\)754475\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2025/754475/EXPO_STU(2025)754475_EN.pdf).

214 Prajak Kongkirati and Veerayooth Kanchoochat, “The Prayuth Regime: Embedded Military and Hierarchical Capitalism in Thailand,” *TRANS: Trans-Regional and -National Studies of Southeast Asia* 6, no. 2 (2018): 279–305, <https://doi.org/10.1017/trn.2018.4>.

215 “Thailand Military Seizes Power in Coup,” BBC, May 22, 2014, <https://www.bbc.com/news/world-asia-27517591>.

216 Hannah Ellis-Petersen, “Thai Parties Cry Foul After Election Results Favour Military Junta,” *Guardian*, May 8, 2019, <https://www.theguardian.com/world/2019/may/08/thai-parties-cry-foul-after-election-results-favour-military-junta>.

217 Janjira Sombatpoonsiri, “From Soft Sanctions to Engagement: The EU’s Evolving Responses to Thailand’s Democratic Openings,” European Democracy Hub, March 31, 2025, <https://europeandemocracyhub.epd.eu/from-soft-sanctions-to-engagement/>.

218 Hannah Ellis-Petersen, “Murder on the Mekong: Why Exiled Thai Dissidents Are Abducted and Killed,” *Guardian*, March 17, 2019, <https://www.theguardian.com/world/2019/mar/17/thailand-dissidents-murder-mekong-election>.

219 “Thailand: Transnational Repression Host Country Case Study,” Freedom House, 2022, <https://freedomhouse.org/report/transnational-repression/thailand>; In the Freedom House dataset, when a single individual underwent two different types of transnational repression —such as detention and rendition (deportation)—the case is split into two units, even though it involves the same individual experiencing a single TNR event. While my dataset preserves this two-pronged coding, the analysis is conducted at the level of the TNR victim.

220 Irade, “اقسوس برقيوي د ريلتاكوژدائ كنيسلننائ ناكاملكت بكتندناليات” [Lawyers for the Teklimakan Family in Thailand Prepare to Appeal to the Supreme Court], Radio Free Asia, March 27, 2015, <https://www.rfa.org/uyghur/xewerler/kishilik-hoquq/tayland-uyghur-03272015221730.html>; “Thailand: 100 Ethnic Turks Forcibly Sent to China,” Human Rights Watch, July 9, 2015, <https://www.hrw.org/news/2015/07/09/thailand-100-ethnic-turks-forcibly-sent-china>; “WUC and UHRP Grieved by Death of Uyghur Refugee in Detention Center in Thailand,” Uyghur Human Rights Project, April 24, 2023, updated April 25, 2023, <https://uhrp.org/statement/wuc-and-uhrp-grieved-by-death-of-uyghur-refugee-in-detention-center-in-thailand/>; “Press Release: Investigate Death of Uyghur Refugee in Thai Immigration Detention Facility; Remaining Uyghur Detainees Must Be Released,” World Uyghur Congress, February 17, 2023, <https://www.uyghurcongress.org/en/press-release-death-of-uyghur-refugee-in-immigration-detention-facility-must-be-investigated-remaining-uyghur-detainees-held-since-2014-must-be-released/>.

221 Quinley, “‘We Thought We Were Safe’”; According to the 2024 Human Rights Watch report “We Thought

- We Were Safe,” then prime minister of Cambodia Hun Sen and then prime minister of Thailand Prayuth signed this “fugitive” arrangement in March 2018. “Fugitives” apparently included exiled dissidents and critics of the two governments. Later that month, Cambodia’s then deputy prime minister and minister of national defense, Tea Banh, visited Bangkok to meet with Prayuth and senior Thai officials.
- 222 Reuters, “Dissident Russian Rock Band Faces Deportation from Thailand,” *Bangkok Post*, January 29, 2024, <https://www.bangkokpost.com/thailand/general/2732582/dissident-russian-rock-band-faces-deportation-from-thailand>.
- 223 Frances Mao and Tossapol Chaisamritpol, “Bi-2: Russia Anti-War Band Arrested in Thailand Faces Deportation,” BBC, January 30, 2024, <https://www.bbc.com/news/world-asia-68137594>.
- 224 Michael Ruffles, “Hun Sen Branded Him a Traitor. He Fled the Country but Thugs Found Him,” *Sydney Morning Herald*, January 2, 2020, <https://www.smh.com.au/world/asia/hun-sen-branded-him-a-traitor-he-fled-the-country-but-thugs-found-him-20191229-p53nndd.html>.
- 225 Gu Ting, “Ethnic Mongolian UN-Registered Refugee Threatened by Chinese Agents in Bangkok,” Radio Free Asia, November 3, 2022, <https://www.rfa.org/english/news/china/china-mongolian-11032022160156.html>; Roseanne Gerin, “Thai Authorities Arrest, Deport Two Cambodian Opposition Activists,” Radio Free Asia, November 10, 2021, <https://www.rfa.org/english/news/cambodia/cnrrp-activists-deported-11102021171509.html>; “Thailand: Cambodian Opposition Activist Assaulted,” Human Rights Watch, August 25, 2023, <https://www.hrw.org/news/2023/08/25/thailand-cambodian-opposition-activist-assaulted>; “Thailand: Authorities Must Investigate Abduction of Vietnamese Journalist,” Amnesty International, June 21, 2019, <https://www.amnesty.org/en/latest/press-release/2019/06/thailand-authorities-investigate-abduction-vietnamese-journalist/>; Quinley, “We Thought We Were Safe.”
- 226 Prashanth Parameswaran, “What’s in the Thailand-Cambodia Foreign Fugitive Deal?,” *Diplomat*, March 30, 2018, <https://thediplomat.com/2018/03/whats-in-the-thailand-cambodia-foreign-fugitive-deal/>; “Thailand Enables Vietnam’s Cross-Border Crackdown on Dissidents,” Impact International, March 11, 2026, <https://impactpolicies.org/news/832/thailand-enables-vietnams-cross-border-crackdown-on-dissidents>; “Murray Hunter Arrest in Thailand Over Malaysia Defamation Sparks Repression Debate,” Impact International, October 2, 2025, <https://impactpolicies.org/news/606/australian-critic-murray-hunter-arrested-in-thailand-for-malaysia-defamation-sparks-transnational-repression-debate>.
- 227 Parameswaran, “What’s in the Thailand-Cambodia Foreign Fugitive Deal?”; “Thailand Enables Vietnam’s Cross-Border Crackdown on Dissidents.”
- 228 Red Notice Monitor, “Targeted by China Through Interpol? Your Options Explained,” Red Notice Monitor, December 23, 2025, <https://rednoticemonitor.com/targeted-by-china-through-interpol-your-options-explained/>; “Global: Misuse of Interpol Red Notices to Target Dissidents a Grave Institutional Failure,” Amnesty International, January 26, 2026, <https://www.amnesty.org/en/latest/news/2026/01/global-misuse-of-interpol-red-notices-to-target-dissidents-a-grave-institutional-failure/>.
- 229 Wanaporn Techagaisiyavanit, Srisombat Chokprajakchat, and Dhanakorn Mulaphong, “Reterritorializing Thailand’s Transnational Space?: The Host State’s Policy Silence in Countering Transnational Repression and the Facilitation of Extraterritorial Space-Making,” *World Affairs* 186, no. 3 (2023): 717–746, <https://doi.org/10.1177/00438200231176821>; “Thailand: Transnational Repression Host Country Case Study,” Freedom House, 2022, <https://freedomhouse.org/report/transnational-repression/thailand>.
- 230 Amnesty International, “Thailand Must Investigate Killing of Lao Activist, Say Rights Groups,” *Prachatai English*, May 29, 2023, <https://prachataienglish.com/node/10392>; Kate Lamb, “Thai Government Pressed Over Missing Lao Activist Od Sayavong,” *Guardian*, September 6, 2019, <https://www.theguardian.com/world/2019/sep/07/thai-government-pressed-over-missing-lao-activist-od-sayavong>; “Thailand: Lao Refugee Gunned Down,” Human Rights Watch, May 24, 2023, <https://www.hrw.org/news/2023/05/24/thailand-lao-refugee-gunned-down>.
- 231 Janjira Sombatpoonsiri, “From Repression to Revolt: Thailand’s 2020 Protests and the Regional Implications,” *GIGA Focus Asia*, no. 1 (February 2021), German Institute for Global and Area Studies (GIGA), <https://www.giga-hamburg.de/en/publications/giga-focus/repression-revolt-thailand-s-2020-protests-regional-implications>; Pinkaew Laungaramsri, “Mass Surveillance and the Militarization of Cyberspace in Post-Coup Thailand,” *ASEAS: Austrian Journal of South-East Asian Studies* 9, no. 2 (2016): 195–214, <https://doi.org/10.14764/10.ASEAS-2016.2-2>; Janjira Sombatpoonsiri, “Digital Surveillance in Thailand: When Pegasus Takes Flight,” *Fulcrum*, February 24, 2022, <https://fulcrum.sg/article/commentaries/digital-surveillance-in-thailand-when-pegasus-takes-flight/>.
- 232 “Parasite That Smiles: Pegasus Spyware Targeting Dissidents in Thailand,” iLaw, July 16, 2022, <https://www.ilaw.or.th/articles/35057>.
- 233 Bangkok Metropolitan Administration, “Bangkok City Hall Defends THB2.3Bn CCTV Spend, Citing 80% for Maintenance,” Public Relations Office, July 16, 2025, <https://pr-bangkok.com/?p=507873>; Estimates of Bangkok’s population range from around 5 million to around 18 million, in large part because of the enormous influx of people during daytime, including tourists, migrant workers,

- and residents commuting into Bangkok from the suburbs. See World Population Review and Worldometer.
- 234 Janjira Sombatpoonsiri, Itsakul Unahakate, Abhidech Tepin, and Krongkan Karanet, “From the Cold War to the Digital Age: The Evolution of State Propaganda in Thailand,” *Critical Asian Studies* (2026), <https://doi.org/10.1080/14672715.2026.2638576>.
  - 235 Janjira Sombatpoonsiri, “‘We Are Independent Trolls’: The Efficacy of Royalist Digital Activism in Thailand,” *ISEAS Perspective*, no. 2022/1 (January 5, 2022), ISEAS–Yusuf Ishak Institute, <https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-1-we-are-independent-trolls-the-efficacy-of-royalist-digital-activism-in-thailand-by-janjira-sombatpoonsiri/>.
  - 236 I. U. Ajn, “Internet Providers Are Helping the Thai Government Track Down Dissidents,” *New Mandala*, July 1, 2020, <https://www.newmandala.org/internet-providers-are-helping-the-thai-government-track-down-dissidents/>.
  - 237 Sombatpoonsiri, “‘We Are Independent Trolls.’”
  - 238 “Thailand: Transnational Repression Host Country Case Study”; “‘We Thought We Were Safe’”; Gerin, “Thai Authorities Arrest, Deport Two Cambodian Opposition Activists”; RFA Vietnamese, “H’mong Activist Arrested by Thai Police after Denouncing Vietnam’s Rights Violations,” *Radio Free Asia*, December 13, 2023, <https://www.rfa.org/english/news/vietnam/vietnam-thailand-hmong-activist-arrested-12132023162244.html>
  - 239 RFA Staff, “Crackdown on Political Activists Tops Thai-Cambodian Summit Agenda,” *Radio Free Asia*, February 7, 2024, <https://www.rfa.org/english/news/cambodia/thai-cambodia-summit-02072024024110.html>.
  - 240 “Cambodian Activists Arrested Ahead of Hun Manet Visit to Thailand,” *Bangkok Post*, February 3, 2024, <https://www.bangkokpost.com/thailand/general/2735671/cambodian-activists-arrested-ahead-of-hun-manet-visit-to-thailand>.
  - 241 Simon Denyer, “U.S. Diplomats Help Chinese Lawyer’s Family Stage Dramatic Escape,” *Washington Post*, May 8, 2017, [https://www.washingtonpost.com/world/asia\\_pacific/us-diplomats-help-chinese-lawyers-family-stage-dramatic-escape/2017/05/08/33e64f40-33fd-11e7-ab03-aa29f656f13e\\_story.html](https://www.washingtonpost.com/world/asia_pacific/us-diplomats-help-chinese-lawyers-family-stage-dramatic-escape/2017/05/08/33e64f40-33fd-11e7-ab03-aa29f656f13e_story.html); Andrew Nagemson, “Thailand Refugee Deportations Trigger Condemnation, Defiance,” *Al Jazeera*, November 24, 2021, <https://www.aljazeera.com/news/2021/11/24/holdthailand-refugee-deportations-trigger-condemnation-defiance>; BenarNews, “Vietnamese Human Rights Campaigner Stuck in Scary Limbo in Thailand,” *Radio Free Asia*, March 21, 2019, <https://www.rfa.org/english/news/vietnam/thailand-activist-03212019094727.html>.
  - 242 Pok Ponlue and Seoung Nimol, “Seven Cambodian Refugees Nabbed by Thai Police Await UNHCR Help,” *CamboJA News*, January 3, 2024, <https://cambojanews.com/seven-cambodian-refugees-nabbed-by-thai-police-await-unhcr-help/>.
  - 243 Sound of Thailand, “ฉาวข้ามประเทศ!! กัมพูชา ร้องนายกฯ เศรษฐา ตรวจสอบกิจกรรม #พรรคก้าวไกล” [International scandal!! Cambodia calls on Prime Minister Srettha to investigate the activities of the Move Forward Party], Facebook, December 29, 2023, <https://www.facebook.com/SOTHLAND/posts/pfbid0F9Qafxeoo8dxm5r6cEwPhxaB-PhmPDZbxF5TshobeZxrtiQw7mWxqmBJ1YZ3zdACrl>.
  - 244 RFA Khmer, “Thai Police Detain 10 Cambodians During Workshop in Bangkok,” *Radio Free Asia*, January 3, 2024, <https://www.rfa.org/english/news/cambodia/thailand-arrests-01032024144734.html>.
  - 245 RFA Khmer, “Thai Police Detain 10 Cambodians During Workshop in Bankok.”

## 11

- 246 CyberBRICS, “New AJIC Special Thematic Section: BRICS Countries and AI Sovereignty,” *CyberBRICS*, Center for Technology and Society, FGV Law School, January 8, 2025, <https://cyberbrics.info/new-ajic-special-thematic-section-brics-countries-and-ai-sovereignty/>; Luca Belli, “To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE),” in “New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms,” ed. Steven Feldstein, *Carnegie Endowment for International Peace*, November 29, 2023, <https://carnegieendowment.org/research/2023/11/new-digital-dilemmas-resisting-autocrats-navigating-geopolitics-confronting-platforms#to-get-its-ai-foothold-brazil-needs-to-apply-the-key-ai-sovereignty-enablers-kase>.
- 247 For an exploration of the challenges and opportunities in leveraging the KASE framework to foster cooperative approach to digital sovereignty, see Luca Belli and Ahmad Bhinder, *Cooperative Digital Sovereignty and Artificial Intelligence: Promoting Resilience, Strategic Openness and Self-Determination*. (Digital Cooperation Organization, 2026).
- 248 Nikolaus Lang, Matt Langione, Sesh Iyer, Amartya Das, and David Zuluaga Martínez, “For Most Countries, AI Sovereignty Is an Illusion. Resilience Is Real,” *Boston Consulting Group*, March 25, 2026, <https://www.bcg.com/publications/2026/ai-sovereignty-is-an-illusion-resilience-is-real>; Afzal Ashraf and Vito Veneziano, “AI Sovereignty without Power? Reviewing Strategic Agency, Infrastructural Dependence and Digital Imperialism,” *AI & Society* (2026), <https://doi.org/10.1007/s00146-026-03116-4>.
- 249 This article draws on research conducted with CyberBRICS Project colleagues at the Center for Technology and Society

- housed in the Fundação Getulio Vargas (FGV) Law School; the author's experience as a member of the Advisory Board of the Brazilian Interministerial Committee for Digital Transformation, a presidentially mandated body that aims to develop guidelines to strengthen the country's digital agenda; and the author's diagnosis of digital sovereignty in Brazil, carried out for the Brazilian Ministry of Science and Technology. See Min Jiang and Luca Belli, eds., *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance* (Cambridge University Press, 2025); Luca Belli and Walter B. Gaspar, eds., *The Quest for AI Sovereignty, Transparency and Accountability: Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition* (Springer Nature Switzerland, 2025); Luca Belli, Walter Britto Gaspar, Natália Couto, Breno Pauli Medeiros, Nicolo Zingales, et al., *Soberania Digital e Inteligência Artificial: Rumo à Autonomia Tecnológica* (Lumen Juris, 2026); and "Tecnologia e Inovação, Soberania Digital No Brasil: Diagnóstico, Desafios e Caminhos Sob a Perspectiva Da Ciência, Tecnologia e Inovação," Centro de Gestão e Estudos Estratégicos, Ministério da Ciência, February 6, 2026, <https://cyberbrics.info/sumario-executivo-estendido-soberania-digital-no-brasil-diagnostico-desafios-e-caminhos-sob-a-perspectiva-da-ciencia-tecnologia-e-inovacao/>.
- 250 The definition was originally formulated in Luca Belli, "To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)"; it has subsequently been used as a baseline definition by the author and by CyberBRICS research team.
  - 251 Luca Belli, "How Are BRICS Countries Building AI Sovereignty? Introduction to Thematic Section," *African Journal of Information and Communication (AJIC)* 35 (2025): 1–4, <https://doi.org/10.23962/ajic.i35.23192>.
  - 252 Samantha Besson, "Sovereignty," in Max Planck Encyclopedia of Public International Law, ed. Rüdiger Wolfrum, vol. IX (Oxford: Oxford University Press, 2012), 366–91, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1472>.
  - 253 Luca Belli and Ahmad Bhinder, "Cooperative Digital Sovereignty and Artificial Intelligence: Promoting Resilience, Strategic Openness, and Self-Determination," Digital Cooperation Organization, 2026, <https://dco.org/cooperation-digital-sovereignty-and-artificial-intelligence/>.
  - 254 Belli and Bhinder, *Cooperative Digital Sovereignty and Artificial Intelligence*.
  - 255 Luca Belli and Nicolo Zingales, "Interoperability to Foster Open Digital Ecosystems in the BRICS Countries," Chinese Academy of Cyberspace Studies, Xinhua Institute, China Institute of International Studies, December 28, 2023, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4641496](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4641496).
  - 256 Luca Belli, "Soberania Digital no Brasil: Diagnóstico, Desafios e Caminhos sob a Perspectiva da Ciência, Tecnologia e Inovação" [Digital Sovereignty in Brazil: Diagnosis, Challenges, and Paths Forward from the Perspective of Science, Technology, and Innovation], discussion paper, Centro de Gestão e Estudos Estratégicos (CGEE) and Ministério da Ciência, Tecnologia e Inovação (MCTI), 2026, <https://cyberbrics.info/wp-content/uploads/2026/07/Texto-para-Discussao-Soberania-Digital-no-Brasil-25.05.2026.pdf>.
  - 257 Belli and Bhinder, "Cooperative Digital Sovereignty and Artificial Intelligence."
  - 258 Luca Belli and Walter B. Gaspar, eds., *The Quest for AI Sovereignty, Transparency and Accountability: Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition* (Cham: Springer, 2026), <https://doi.org/10.1007/978-3-032-02762-7>.
  - 259 Belli and Bhinder, "Cooperative Digital Sovereignty and Artificial Intelligence."
  - 260 Luca Belli, Walter Britto Gaspar, Natália Couto, Breno Pauli Medeiros, Nicolo Zingales, et al., *Soberania Digital e Inteligência Artificial: Rumo à Autonomia Tecnológica* (Lumen Juris, 2026).
  - 261 Luca Belli, "Net Neutrality, Zero Rating and the Minutalisation of the Internet," *Journal of Cyber Policy* 2, no. 1 (2017): 96–122, <https://doi.org/10.1080/23738871.2016.1238954>.
  - 262 "Humanware" refers to the human elements of a technology system, specifically the skills, capabilities, knowledge, and adaptability of the people who interact with, manage, and develop hardware and software. Unlike passive users of AI, a highly capacitated or skilled "humanware" actively shapes, drives, and safely navigates technological evolution rather than just consuming it. See Belli et al, *Soberania Digital e Inteligência Artificial*.
  - 263 Belli and Bhinder, "Cooperative Digital Sovereignty and Artificial Intelligence."
  - 264 John Hawkinson and Tony Bates, *Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*, RFC 1930 (Internet Engineering Task Force, March 1996), <https://www.rfc-editor.org/rfc/rfc1930.html>.
  - 265 Belli and Bhinder, "Cooperative Digital Sovereignty and Artificial Intelligence"; DevelopmentAid, "Inter-American Development Bank (HQ)," accessed September 14, 2026, <https://www.developmentaid.org/organizations/view/118355/iadb>; DevelopmentAid, "Asian Development Bank (HQ)," last updated February 23, 2026, <https://www.developmentaid.org/organizations/view/118345/adbi>; DevelopmentAid, "African Development Bank (HQ)," accessed September 14, 2026, <https://www.developmentaid.org/organizations/view/118346/afdb>.

266 Belli et al., *Soberania Digital e Inteligência Artificial no Brasil*.

267 Belli et al., *Soberania Digital e Inteligência Artificial no Brasil*.

268 Belli, “Soberania Digital no Brasil.”

269 Belli and Bhinder, “Cooperative Digital Sovereignty and Artificial Intelligence.”

270 Belli et al., *Soberania Digital e Inteligência Artificial no Brasil*.

## About the Authors

**Mahsa Alimardani** is an associate director of the Technology Threats and Opportunities program at WITNESS, leading work on how emerging technologies reshape visual truth. She is also a doctoral researcher at the Oxford Internet Institute on information controls in authoritarian settings.

**Arindrajit Basu** is a PHD candidate at Leiden University's faculty of global governance and affairs, working on sovereignty and order contestation in cyberspace. He is also a digitalization and human rights consultant with the United Nations Development Programme.

**Luca Belli** is a professor at the FGV Law School Rio de Janeiro and the director of the Center for Technology and Society at the Fundação Getúlio Vargas in Brazil.

**Steve Feldstein** is director of the Carnegie Endowment for International Peace in the Democracy, Conflict, and Governance Program. His research focuses on technology, national security, the global context for democracy, and U.S. foreign policy.

**Shreya Joshi** is a former James C. Gaither Junior Fellow with Carnegie's Democracy, Conflict, and Governance Program.

**Usama Khilji** is an activist, researcher, and columnist from Pakistan. He is the cofounder and director of Bolo Bhi, an advocacy, policy, and research citizens group focused on digital rights and internet policy.

**Nathan Law** is a Hong Kong democratic activist and former legislator.

**Frank Cheng-Shan Liu** is a professor and the director of the Institute of Political Science at National Sun Yat-Sen University in Taiwan.

**Irene Poetranto** is a senior researcher at the Citizen Lab, based at the University of Toronto's Munk School of Global Affairs and Public Policy, and a PhD candidate at the Department of Political Science, University of Toronto, where she studies the politics of internet regulation in Southeast Asia.

**Yahli Shereshevsky** is a senior lecturer at the University of Haifa Law School and a principal investigator at the Minerva Center for the Rule of Law under Extreme Conditions. His research and teaching focus on international humanitarian law, the intersection of law and technology, international lawmaking, and international criminal law.

**Janjira Sombatpoonsiri** is a research fellow at the German Institute for Global and Area Studies and an assistant professor at Thailand's Chulalongkorn University. Her current research focuses on autocratic weaponization of disinformation laws, digital propaganda and conflict narratives in Southeast Asia, and digital repression of protest movements.

---

## **Carnegie Endowment for International Peace**

In a complex, changing, and increasingly contested world, the Carnegie Endowment generates strategic ideas, supports diplomacy, and trains the next generation of international scholar-practitioners to help countries and institutions take on the most difficult global problems and advance peace. With a global network of more than 200 scholars across twenty countries, Carnegie is renowned for its independent analysis of major global problems and understanding of regional contexts.

### **Democracy, Conflict, and Governance Program**

The Democracy, Conflict, and Governance Program is a leading source of independent policy research, writing, and outreach on global democracy, conflict, and governance. It analyzes and seeks to improve international efforts to reduce democratic backsliding, mitigate conflict and violence, overcome political polarization, promote gender equality, and advance pro-democratic uses of new technologies.



**CARNEGIE**  
ENDOWMENT FOR  
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW  
Washington, DC 20036

[CarnegieEndowment.org](https://CarnegieEndowment.org)