CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Digital Democracy in a Divided Global Landscape

Steven Feldstein, editor

Arindrajit Basu | Luca Belli | McKenzie Carrier | Iginio Gagliardone | Dean Jackson | Lillian Nalwoga
Jonathan Corpus Ong | Irene Poetranto | 'Gbenga Sesan | Janjira Sombatpoonsiri | H. Akin Unver

Digital Democracy in a Divided Global Landscape

Steven Feldstein, editor

Arindrajit Basu | Luca Belli | McKenzie Carrier | Iginio Gagliardone | Dean Jackson | Lillian Nalwoga
Jonathan Corpus Ong | Irene Poetranto | 'Gbenga Sesan | Janjira Sombatpoonsiri | H. Akin Unver

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Introduction

Steven Feldstein

In February 2025, global leaders and tech moguls gathered in Paris for the Artificial Intelligence (AI) Action Summit, a confab co-hosted by French President Emmanuel Macron and Indian Prime Minister Narendra Modi meant to galvanize debate about how the world should address the growing relevance of AI technologies. Over 1,000 participants representing more than one hundred countries gathered in Paris' Grand Palais to rub shoulders, network, and debate the finer points of model weights, inference scaling, and proprietary models. It was also an opportunity for the audience to hear from U.S. President Donald Trump's administration about its vision for AI.

Vice President JD Vance did not mince his words. He delivered a tough message centered on American primacy: "The United States of America is the leader in AI, and our administration plans to keep it that way," he informed the crowd.[1] According to Vance, America under Trump's leadership would use all the tools at its disposal to preserve its technological advantages and would resist efforts by other countries and jurisdictions, such as Europe, to regulate its technology. Countries would be forced to choose between using U.S.-designed technology or siding with authoritarian competitors (namely China) that weaponize AI software to "rewrite history, surveil users, and censor speech." Leaders who were interested in making deals with Washington (and who offer concessions) would be rewarded, and those who did not play ball would face punishment. Vance's remarks represented a starkly transactional view of international relations—one in which shared values and mutual interests are cast aside for bottom-line objectives.

These ideas deviated from eighty years of alliance building adopted by multiple U.S. presidents to secure America's interests through cooperation and collaboration. As recently as last year, President Joe Biden launched a "digital solidarity" strategy intended to bind countries together, arguing that "all who use digital technologies in a rights-respecting manner are more secure, resilient, self-determining, and prosperous."[2] But while Vance's speech represented a sharp break in U.S. policy, his remarks aptly captured an emerging global reality; it is not just the United States that sees digital policymaking as an interest-based tool of

"realpolitik negotiation."[3] And it is not just Trump who is making an explicit play to put his country's interests first at the expense of the international system. Many other nations are pursuing similar measures, whether openly acknowledged or not.

Take China, for example. In contrast to Vance's remarks, Chinese Vice Premier Zhang Guoqing's address in Paris was far more conciliatory. He emphasized that Beijing wants to make sure that frontier technology is not controlled by a few corporations or a handful of countries. He outlined a vision to create "a community with a shared future for mankind," where China positions itself as a reliable partner to help countries advance their respective priorities.[4] But few people were fooled. Beijing has pumped billions of dollars into subsidizing critical industries and developing formidable tech champions, including Huawei and Alibaba. It has leveraged the Made in China 2025 program at home and the Digital Silk Road overseas to build up its technological capacities and grow its influence. When Beijing has faced resistance, its leadership has not hesitated to use coercion to get its way, whether forcing Korean conglomerate Lotte Group to exit the Chinese market after South Korea announced the deployment of America's Terminal High Altitude Area Defense (THAAD) missile defense system in 2016 or revoking the trade licenses of two leading Canadian exporters of canola seed in response to Canada's 2018 detention of Meng Wanzhou, Huawei's chief financial officer, at the urging of the United States.[5]

These changes extend beyond China; a global shift is taking place. Countries are reluctant to work across borders and in service of shared concepts and common standards relating to digital technology. The internet is fragmenting into multiple "splinternets," shifting from an open, globally connected web to a "collection of isolated networks controlled by governments."[6] Individual countries are erecting digital walls—enacting their own rules governing how platforms can operate, determining which online speech is permissible, and deciding which digital services and products are allowed. Digital solidarity is out. Tech sovereignty is in. Leaders recognize that tech innovation equals power, and they are marshaling their resources accordingly.

To make sense of these changing dynamics, the Carnegie Endowment for International Peace has assembled ten essays drawn from members of our Digital Democracy Network spanning from Thailand and Türkiye to Nigeria, South Africa, and Uganda.

A first set of essays analyzes how local actors are navigating the new tech landscape. Lillian Nalwoga explores the challenges and upsides of Starlink satellite internet deployment in Africa, highlighting legal hurdles, security risks, and concerns about the platform's leadership. As African nations look to Starlink as a valuable tool in closing the digital divide, Nalwoga emphasizes the need to invest in strong regulatory frameworks to safeguard digital spaces. Jonathan Corpus Ong and Dean Jackson analyze the landscape of counter-disinformation funding in local contexts. They argue that there is a "mismatch" between the priorities of funders and the strategies that activists would like to pursue, resulting in "ineffective and extractive workflows." Ong and Jackson isolate several avenues for structural change, including developing "big tent" coalitions of activists and strategies for localizing

aid projects. Janjira Sombatpoonsiri examines the role of local actors in foreign influence operations in Southeast Asia. She highlights three motivating factors that drive local participation in these operations: financial benefits, the potential to gain an edge in domestic power struggles, and the appeal of anti-Western narratives.

A second set of essays explores evolving applications of digital repression. Irene Poetranto argues that understanding government restrictions of online content requires looking beyond legal regulations to examine the technical aspects of internet controls. Through a study of Indonesia's content blocking requirements, she demonstrates that the different tools used by internet service providers to filter online speech implicate free expression and access to information in different ways. 'Gbenga Sesan's article tracks the harms of internet shutdowns across the globe. He argues that disconnection from the internet creates unique difficulties for populations that traditionally rely on internet access for educational, economic, and interpersonal purposes. It is critical, Sesan emphasizes, that stakeholders "pay attention to disconnected citizens" alongside broader unconnected populations. Steven Feldstein and McKenzie Carrier analyze the "AI-first" strategy of the U.S. Department of Government Efficiency (DOGE). They draw comparisons between Elon Musk's remaking of Twitter and DOGE's ongoing disruption of the U.S. federal bureaucracy. DOGE's agenda, they caution, sheds light on how the deployment of AI tools and automated technologies can "destroy institutions, wipe out accountability, and enable corruption to flourish."

A third set focuses on national strategies and digital sovereignty debates. Arindrajit Basu cautions against the Trump administration's shift away from the principle of "digital solidarity" in its foreign policy. He argues that if a key goal for the United States is to counter China's influence among developing countries, it would be sensible for the Trump administration to "pursue initiatives that resonate internationally while also advancing America's core interests." Iginio Gagliardone's examination of Kenyan gig workers and South Africa's data sovereignty debate sheds light on "pathways for resistance, negotiation, and adaptation in the pursuit of AI sovereignty." He argues in favor of "networked sovereignty"—creating cross-border collaborations and governance structures among African nations to strengthen the continent's ecosystem and trajectory.

A fourth set explores pressing tech policy and regulatory questions. Luca Belli's article examines the intersection of cybersecurity and AI. He argues that AI has transformed the cybersecurity landscape, increasing the frequency, impact, and sophistication of cyber attacks. Belli uses Brazil as a case study to explain how shortcomings in AI and cybersecurity regulations leave nations vulnerable to cyber attacks. In response, he outlines how "sound management of information and infrastructure, good stakeholder coordination, and solid capacity-building" can strengthen nations' cyber resilience. Akin Unver describes the development of the Foreign Information Manipulation and Interference (FIMI) framework, which has become the dominant method in Canada, the European Union, and the United States to analyze trends in the information space. FIMI, he argues, improved on prior methods for countering foreign influence operations by systematizing "early detection, data collection, and countermeasures architecture." However, he highlights several obstacles to further developing FIMI,

such as the mismatched threat landscape among countries, access restrictions enacted by tech platforms, and architectural differences across platforms that inhibit responses.

These viewpoints illuminate emerging questions, new debates, and unresolved dilemmas in the tech domain. They highlight the challenges new technologies pose to governance, politics, and society. And they are meant to help policymakers connect local and regional insights with international discourse.

01

Starlink Deployment and African Governments' Quest for Digital Sovereignty

Lillian Nalwoga

Satellite technology has the potential to significantly catalyze Africa's digital access landscape by providing much needed high-speed internet access across the continent. Internet connectivity is still a major concern in Africa, with only 38 percent of individuals across the continent using the internet.[7] Satellite providers like Starlink have the potential to close the digital divide in Africa by providing reliable internet connection via satellites in areas where other terrestrial providers, such as cable or fixed wireless links, are not available. However, the case of Starlink also exemplifies the ongoing challenges in closing Africa's digital divide. Starlink's deployment in Africa has not been without hurdles. These include challenges to deployment, legal and regulatory obstacles, ethical concerns around data protection and privacy, digital surveillance, and cybersecurity issues. Additionally, growing political controversy around Elon Musk, whose company SpaceX owns Starlink, raises questions about whose interests are really being served in Africa.

Starlink's Deployment Barriers

Starlink launched in Africa in 2022 and is legally operational in eighteen African countries, with several other countries set to be connected 2025.[8] Starlink is a prime option among internet service providers in Africa—reportedly cheaper than the leading alternative internet service provider in at least five of the countries in which Starlink is operational.[9] However, the high cost of purchasing installation kits continues to make Starlink deployment a financial burden within African nations.[10]

The firm provides high speed internet that does not rely on terrestrial infrastructure; instead, it uses a low earth orbiting satellite constellation. Starlink's internet speeds can reach up to 220 megabits per second (Mbps) compared to traditional satellites' 150 Mbps.[11] Such technology gives its satellites the ability to reach underserved populations, especially people living in rural areas or locations affected by natural disaster or war. However, while Starlink offers the unique ability to reach such remote regions when other providers cannot, there remain socioeconomic barriers to implementing Starlink in these rural areas.[12] For Starlink to fulfill its promise of shrinking the rural-urban digital divide through expanded coverage, these barriers must be addressed.

Legal and Regulatory Hurdles

Since its launch in Africa, Starlink has had to navigate different regulatory environments across various nations. Complications have arisen in countries such as Cameroon, the Democratic Republic of the Congo, Senegal, South Africa, and Zimbabwe.[13] Some countries have even banned the use of Starlink services for the company's failure to comply with the licensing requirements. In the case of South Africa, for example, the country's licensing regime requires foreign telecom companies to grant at least 30 percent local ownership from "historically disadvantaged groups," such as women, youth, and people living with disabilities.[14] Starlink has not met this standard, and it has been unable to acquire a license to operate in the country.

In Kenya, where Starlink launched in July 2023 and has since acquired considerable market share, similar regulatory concerns were overlooked to allow the platform to operate in the country.[15] In the same month that Starlink launched, the Communications Authority of Kenya (CA) sought to amend its 2020 National Information Communications and Technology Policy Guidelines to remove a clause that required international information and communications technology companies to have at least 30 percent local ownership.[16] The amendment came into effect in August 2023, with President William Ruto citing the country's need to boost high-speed internet access in Kenya and improve market competition and tech investment.[17] But many believed that the legal change was intended to accommodate Starlink's interests and that Ruto was exerting influence over the CA to facilitate the technology's deployment.

Despite pushback—such as when Safaricom, Kenya's leading internet service provider, challenged Starlink's blanket license to operate in the country and urged the CA to reconsider prioritizing satellite providers as direct to mobile providers[18]—the CA did not make any substantive changes that would deter Starlink from offering services. For example, the CA is considering increasing fifteen-year licensing fees for satellite internet providers from $12,302 to $115,331 and introducing an annual levy of 0.4 percent of gross turnover.[19] While this would raise costs in the country for Starlink, the new guidelines, once passed, would also

allow satellite providers to operate terrestrial cables, telemetry systems, and tracking facilities and to engage in space research—potentially "pav[ing] the way for Starlink to establish ground stations in Kenya, which has previously been delayed owing to regulatory constraints."[20] Already, there are concrete signs of Starlink's growing presence. In January 2025, the company established a Point of Presence (PoP) in Nairobi, marking only the second Starlink PoP to be placed in Africa (after Nigeria) and which has drastically reduced latency rates for users in the region.[21]

Data Protection and Privacy

Starlink is a purely commercial venture that profits from collecting its users' data. Therefore, a concern is that the absence of robust data protection and privacy laws in countries such as Burundi, Malawi, Mozambique, and South Sudan may enable Starlink to exploit and monetize Africans' personal data.[22]

One area of concern is where user data is stored and who has access to it. Although Starlink's privacy policy outlines guidelines for how the company handles user data, governments like Zimbabwe have raised questions about the potential for security issues and the loss of government control over telecommunications in countries where the platform is operating. Starlink's adherence to local requirements is another point of contention.[23] Various African countries are adopting restrictive data localization laws that prioritize national security, the promotion of the national digital economy, and the protection of user privacy.[24] Nine out of the sixteen countries in Africa with active Starlink subscriptions have data localization requirements and either consider all public data, personal data, telecom subscriber data, or consumer data as classified information, requiring prior approval before export. Yet, Starlink does not appear to be following any of these requirements—its uplink stations and satellites are located outside the continent, so every time an individual uses Starlink, the company is theoretically violating these provisions.

Digital Surveillance

SpaceX's involvement in building surveillance capabilities is another issue for consideration. News reports indicate that Starlink has helped build surveillance capabilities for U.S. government agencies. In March 2024, for example, a Reuters investigation revealed that SpaceX was building a classified spy satellite network for the National Reconnaissance Office, part of the U.S. intelligence community.[25] It also merits considering that Starlink could be used by repressive regimes in Africa as a surveillance technology. Given that digital surveillance has become a booming global industry and the current market for surveillance tools in Africa, this is not a far-fetched scenario. African governments in countries such as Ghana, Malawi, Nigeria, and Zambia are reportedly spending a collective $1 billion annually on digital

surveillance technologies, purchasing intelligence products from countries such as China, the United States, and the United Kingdom.[26] Many African states are reportedly using digital espionage tools to track or crack down on dissidents and reinforce authoritarianism.[27]

Governments can potentially leverage Starlink to expand their surveillance infrastructure domestically. In Bangladesh, for instance, the introduction of Starlink and other satellite-based internet services was accompanied with "legal surveillance capabilities and the authority to shut down services at any time."[28] There is also a heightened risk of abuse in countries where regulators lack independence from the executive. Take Zimbabwe, which already suffers from major human rights and security violations.[29] Starlink operates in Zimbabwe through IMC Communications, an entity owned by a businessman with close ties to the presidency.[30] In May 2024, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) made IMC the sole distributor of Starlink services in the country. IMC's opaque relationship with the government's senior officials raises questions about potential executive interference and surveillance authorizations targeting opposition and civil society figures.[31]

Nonetheless, Starlink might still be a preferable option to existing alternative providers. China's data governance model is expanding in Africa, but it poses major risks to digital sovereignty. In Senegal, former president Macky Sall halted the deployment of Starlink services and endorsed the Chinese model in 2021. The government migrated all government data to a China-funded national data center.[32] But there is no clarity about what type of access Chinese authorities now have to Senegalese data; there is no transparency about how Chinese agencies or companies may use this information. Given China's record on surveillance and its heavy-handedness toward embedding its own legal framework in other countries, Senegal's decision could backfire in a big way.[33]

Cybersecurity Risks

In general, satellite internet networks such as Starlink are susceptible to cybersecurity intrusions like distributed denial-of-service attacks and signal interception, threatening communication system reliability and integrity.[34] For some African countries, the combination of weaker infrastructure, fewer regulations, and widespread restrictions on technologies such as encryption that protect user data makes Starlink's operations particularly precarious.

African nations are vulnerable to cyber attacks in part because of their shortcomings in adopting cyber regulations and governance. Only 20 percent of African countries have basic legal cyber crime frameworks.[35] In the 2024 Global Cyber Security Index, which measures countries' commitments to cybersecurity across the legal, technical, organizational, capacity, and cooperation pillars, Kenya and Rwanda were the only top-performing African nations.[36] Additionally, while the 2014 African Union Convention on Cyber Security and Personal

Data Protection outlines procedures for investigating and prosecuting cyber crime, only five Starlink-serviced countries—Ghana, Mozambique, Niger, Rwanda, and Zambia—have fully ratified the convention.[37] At the same time, Ghana, Malawi, Nigeria, Rwanda, Zimbabwe, and Zambia all restrict the use of encryption, a vital tool used by Starlink to mitigate cyber attacks.[38] These factors make Starlink services acutely vulnerable to intrusion and violations on the continent, heightening the cyber risks from malicious or antidemocratic actors.

Starlink's Ownership and Geopolitical Influence

Musk, whose company SpaceX controls Starlink, is a controversial figure. He is not only one of the world's richest individuals, but he has also garnered immense political influence, overseeing the Department of Government Efficiency (DOGE) at U.S. President Donald Trump's request. In that role, he has worked to freeze U.S. foreign assistance and dismantle the U.S. Agency for International Development (USAID), which provided vital services to citizens on the continent. His false claims against the South African government, such as his accusation that Starlink cannot be deployed there because Musk is not Black, have raised concerns.[39] Musk has intervened with Starlink's deployment in the past for political reasons and there is little reason to think this wouldn't happen again. For instance, early in the war in Ukraine, Kyiv prepared a military operation that relied on Starlink services to target Russian forces in Crimea.[40] The Ukrainians thought that Starlink coverage had been activated, but it was not. They asked Musk to turn on the system, but he refused, citing concerns about Russian military escalation. This incident illustrated the depth of Kyiv's reliance on Musk; he alone was able to decide whether Ukraine's military operation could continue or had to be abandoned. Such actions could also be replicated in Africa, where politically driven decisions about access to Starlink could affect the lives of millions of people across the continent.

Conclusion

There are serious questions about the consequences of Starlink's entrance into the African market. The company's technology raises regulatory concerns pertaining to data sovereignty issues, surveillance use cases, back door data access, and its politicized ownership. African leaders should take a hard look at the security and political trade-offs involved in adopting Starlink.

As African governments consider adopting Starlink, they ought to focus on implementing forward-thinking strategies that can help them safeguard their nations' digital spaces while reaping the benefits of the technology. In particular, African governments need to proactively address Starlink's risks by adapting and implementing robust regulatory frameworks, including those related to infrastructure deployment, data governance, cybersecurity, and

data protection and privacy. The lessons that emerge from the case of Starlink also have broader applicability. As African countries seek to close the digital divide, the absence of comprehensive and enforceable laws and regulations designed to define and protect digital sovereignty leaves room for exploitation by global tech companies—not just Starlink. Before jumping on board with satellite internet technologies, African leaders would be wise to implement these protective measures.

02

"Glocalizing" Digital Propaganda: Why Domestic Influence Actors in Southeast Asia Embed Geopolitical Narratives in Their Campaigns

Janjira Sombatpoonsiri

As great power competition intensifies, information warfare has become a key component of geopolitical strategy.[41] Numerous policy papers, academic studies, and expert interviews highlight the dangers posed by malign foreign influence operations (FIOs) conducted by "threat actors" who oppose the Western-led liberal international order, such as China, Iran, and Russia.[42] While FIOs can involve a diverse set of actors, including democratic governments, this essay focuses on large-scale, covert influence efforts by foreign authoritarian states to sway public opinion, strategically disseminate disinformation, and manipulate behaviors in targeted populations.[43]

Much of what is known about FIOs comes from their role in high-profile events like the 2016 and 2020 U.S. presidential elections, the Brexit referendum, and various elections in European Union countries, where right-wing parties have gained momentum in recent years.[44] For example, in early September 2024, ahead of the November U.S. elections, the Department of Justice charged two employees working for Russian state media network RT with paying an American company to produce and spread politically divisive videos, sowing "discord and chaos in the United States."[45] Meanwhile, the China-linked influence operation known as "Spamouflage" employed inauthentic online personas to impersonate American voters to cast doubt on the legitimacy of American democracy.[46]

But FIO campaigns are also spreading hyper-partisan narratives across Africa, the Asia-Pacific, and Latin America, where geopolitical influence is also fiercely contested.[47] Specifically in Southeast Asia, Beijing-backed influence actors are reportedly active in countries involved in disputes over the South China Sea, particularly the Philippines, in part aiming to challenge U.S. influence in the Pacific.[48] These actors have also leveraged historical

ties between China and governments in Cambodia, Indonesia, Thailand, and Vietnam to shape public perceptions on multiple issues, including hailing the effectiveness of China's COVID-19 management and its vaccines and supporting Russia's war against Ukraine.[49]

A common assumption in the existing analyses of FIOs is that foreign states impose malign influence campaigns on passive local populations. This view, however, oversimplifies a complex reality. Local actors actively shape the characteristics and impact of FIOs. This author's ongoing research on conflict-driven online propaganda in Southeast Asia highlights three reasons why local influence actors and netizens exploit information drawn from geopolitical narratives.

Motivated by Financial Incentives

First, in countries such as the Philippines where the industry of online influence has flourished, domestic influencers and trolls for hire can be financially motivated to promote pro-China narratives. It is a lucrative industry: online trolls in the Philippines reportedly earn around $515 to $1,715 a month.[50] One report indicated that Beijing-funded outlets have recruited local journalists and trolls who were financially struggling.[51] Business elites who have a "dependency relationship" with Beijing have reportedly funded pro-China campaigns as well.[52]

In some cases, pro-Beijing platforms and influencers who amplify narratives aligning with China's geopolitical interests in the region may be compensated through micro-targeted ads rather than direct funding from China. After the Philippine government successfully challenged China's territorial claims in the South China Sea through the Permanent Court of Arbitration (PCA) in 2016, China rejected the ruling.[53] By 2018, pro-China fan pages on Facebook in the Philippines were pushing narratives in support of Beijing's refusal of the PCA's decision. These pages represent a network of China-backed Filipino actors: pseudo think tanks (such as the Institute for Integrated Development Studies, or IIDS), social media personalities, media outlets (such as the Manila Times and Sonshine Media Network International), and associations (such as the Philippines-China Friendship Club).[54] Together, they form a pro-China ecosystem, where geopolitical articles and opinions are published in aligned outlets and amplified across different networks.[55] Each post that goes "viral" generates between $20 and $70, depending on the number of views.[56] Not all viewers support these posts' pro-China stances, but the sensational titles, serving as "clickbait," can garner engagement even from netizens critical of China.

Seek an Edge in Domestic Power Struggles

Second, exemplifying the concept of "glocalization," which describes the convergence of globalization and local politics, domestic influence actors often leverage geopolitical narratives to gain an edge in domestic power struggles, particularly during policy shifts, elections, and mass mobilization efforts.[57] This has been clear in the Philippines, where former president Rodrigo Duterte and his daughter, Philippine Vice President Sara Duterte, have benefited

from sophisticated influence campaigns incorporating geopolitical narratives.[58] When Duterte was president, influence actors endorsed his domestic and foreign policies, including his controversial war on drugs and his pivot toward China—a stark departure from the Philippines' traditional alliance with the United States.[59] To rally domestic support for this dramatic policy shift, pro-Duterte accounts appeared to join forces with pro-China actors to frame Duterte's pivot to China as a move promoting regional peace and independence from the United States as a former colonial power, while simultaneously attacking critics.[60] A notable example was Sass Sasot, a prominent pro-Duterte blogger who disseminated false claims that challenged the PCA's 2016 decision and aligned with China's arguments.[61]

Geopolitical narratives also played a role in the Philippines' 2022 presidential election and the subsequent power struggle among political elites. Pro-Duterte influencers weaponized pro-Russia, anti-United States, and pro-China disinformation to target opposition candidate Leni Robredo.[62] They framed her as a weak leader, in contrast to Duterte's strongman image, and as a puppet of Western powers whose pro-Ukraine stance could provoke Chinese aggression against the Philippines. As Sara Duterte was Ferdinand "Bongbong" Marcos Jr.'s running mate, his 2022 campaign aligned with the Dutertes' foreign policy stance, reinforcing skepticism toward the United States. For instance, in March 2022, an old video clip of Marcos Sr., the late dictator, resurfaced. In the clip, he expressed frustration over the mutual defense treaty with the United States, arguing that in a crisis American assistance to the Philippines would be delayed by the need for congressional approval, lamenting, "That means delay, while we are dying there."[63] However, after the election, tensions between Marcos Jr. and the Dutertes emerged, and influence actors who supported each leader began trolling one another online. In response to Marcos Jr.'s reaffirmation of Philippine ties with the United States, a domestically produced deepfake clip surfaced in July 2024, portraying Marcos's foreign policy as war-mongering.[64] (Marcos Jr. dismissed the video and countered it by launching official "anti-fake news" initiatives.)[65]

In Thailand, since the 2014 military coup, the political establishment has increasingly endorsed anti-United States, pro-Russia, and pro-China attitudes and wielded geopolitical contestation among the three countries in coordinated campaigns to discredit the opposition party and suppress dissent. Initially, coordinated fan pages framed Western criticism of the coup as foreign interference and a plot to undermine the monarchy.[66] This narrative gained traction during the youth-led protests in 2020 and 2021, with pro-establishment accounts and mainstream media alike accusing protesters of being backed by the West and calling for them to be arrested as traitors for selling out their country.[67] This rhetoric diverted attention from the domestic grievances driving the protests and stoked nationalism to justify crackdowns on activists.[68] During the 2023 election, Thai pro-establishment influencers and outlets employed the same rhetoric, accusing the opposition party, Move Forward, of receiving funding from the CIA as part of a broader effort to consolidate U.S. hegemony in Southeast Asia.[69] This conspiracy theory sought to reinforce the party's image as unpatriotic. Despite these allegations, the party secured the largest share of popular votes; however, the Thai Constitutional Court subsequently dissolved the party, ruling that it intended to topple the monarchy.[70]

In Malaysia and Indonesia, geopolitical narratives have been entangled with xenophobia. Both countries are major destinations for Rohingya refugees fleeing genocide in Myanmar. However, public sympathy toward the refugees waned during the COVID-19 pandemic, as resources became strained. In the lead-up to Indonesia's 2024 national election, "coordinated" campaigns—in the words of the UN refugee agency—circulated online rumors accusing Rohingya refugees of taking advantage of local communities, culminating in a mob attack on a refugee shelter in Aceh province in December 2023.[71] Candidates supportive of the Rohingya were also targeted online.[72] In a bizarre twist, as the unfolding Israel-Hamas conflict gained attention, some netizens in Indonesia and Malaysia began associating Rohingya refugees with "Zionists" accused of occupying native lands.[73] The irony of this conspiracy theory is glaring, given that the Rohingya are Muslim. Yet, influence accounts pushed the narrative that the Rohingya are not "real" Muslims, using this xenophobic rhetoric to stigmatize and discredit political figures who support the refugees.[74]

Appeal of Anti-Western Narratives

Third, many local actors find anti-West narratives promoted by foreign influencers appealing because they resonate with "shared sentiments" about the West's declining legitimacy.[75] In most Southeast Asian countries, which were formerly colonized by European powers or the United States, political elites and segments of the population embrace nationalism rooted in a mix of sovereignty and skepticism toward Western imperialism.[76] This sentiment grew stronger after the U.S.-led war on terror and amid ongoing support for Israel's war in Gaza, fueling anti-U.S. sentiments particularly in Muslim-majority countries such as Malaysia and Indonesia.[77]

The narrative of "Western hypocrisy" in the region aligns well with Russia's standard accusations that the West exploits human rights and democracy as a facade to entrench its global dominance.[78] This framing conveniently justifies Russia's invasion of Ukraine. Kremlin-backed online propaganda has tapped into local discontent by portraying solidarity with "Muslim victims" of Western imperialism, despite Russia's own crackdown on Muslim minorities.[79] This message has resonated with netizens in Malaysia and Indonesia, many of whom view Russia as an alternative superpower standing up to the West.[80] Rather than seeing Ukraine as a victim of Russian aggression, many netizens have adopted Russia's narrative that Ukraine provoked the conflict.[81] In Thailand, pro-establishment fan pages have reworked this narrative, portraying Ukraine as a historical part of Russia and framing the war as Russia defending its sovereignty.[82] Once again, FIOs are at play, but local discontent with the U.S.-led global order also fuels this wave of online "participatory propaganda."[83]

Conclusion

As much as foreign states orchestrate influence operations, local actors actively exploit these campaigns for their own purposes. Sometimes, their motivations are economic or political, but other times, they are ideologically driven to engage in anti-West propaganda. Analyses sounding the alarms about the dangers of FIOs often overlook these on-the-ground dynamics, mistakenly assuming that the foreign campaigns automatically translate into geopolitical setbacks. Without a preexisting ecosystem of local influence operations, domestic conditions that make populations receptive to FIO narratives, and local support or opposition to great power policies, FIOs would have less influence.[84] Tackling the impact of FIOs requires a deeper understanding of these domestic factors and the local contexts in which such campaigns operate.

03

Counter-Disinformation Funding in the Global Majority Is Broken—Here's How to Fix It

Jonathan Corpus Ong and Dean Jackson

Imagine that you lead a respected legal watchdog somewhere in the Global Majority—the countries, besides the United States, those in Europe, and several in East Asia. Like many civil society organizations in your country, you are preparing for upcoming national elections and rely on donors in the Global North for funding. To your frustration and surprise, these donors push you into supporting interventions copy-pasted from abroad, such as fact-checking and media literacy campaigns—a far cry from your bread-and-butter work on legal advocacy. What's more, they require you to share your data with other civil society organizations working in a coalition using a cumbersome tool that requires significant investments in money, time, and staff training to use. As the elections approach, it becomes clear that coalition members, instead of playing to their strengths, are engaged in redundant work that reaches the same audience but for diminishing returns. Worse still, even if the project is seen as successful, you may have to lay off staff when the grant ends because of the lack of postelection urgency from funders.

These real experiences were shared in a Global Majority knowledge exchange project organized by the Global Technology for Social Justice Lab (GloTech) at the University of Massachusetts Amherst.[85] In 2023 and 2024, the lab convened three workshops for a total of ninety-three civil society leaders in the Global Majority, interviewed seventeen key players in election counter-disinformation coalitions, and held a follow-up survey, which received twenty-five responses. The resulting report is a critical look at the top-down flow of money and ideas from North to South, alongside insights for better ways of working.[86]

The Problems with Funding Today

Too often, there is a mismatch between the priorities of Global North funders and the preferred organizational strategies of activists on the ground. Strategies cannot be operationalized without funding, and so the agendas of Northern funders too often dominate local priorities. Perhaps nowhere is this more evident than in fact-checking and media literacy initiatives, which have boomed over the past decade. For instance, according to the Duke Reporters' Lab, the number of fact-checkers around the world more than doubled between 2016 and 2023.[87] Activists in the Global Majority worry that overreliance on fact-checking and media literacy contributes to tropes about "dumb," brainwashed voters and that philanthropic support for these projects has taken too many cues from big tech companies at the expense of activist- and community-driven approaches.[88]

The resource imbalance between academic researchers in the Global Majority and their better-funded Northern counterparts also means that evidence-driven approaches reflect donor priorities, rather than local ones. Consider, for example, a July 2023 review of studies including randomized control trials (RCTs) of counter-disinformation interventions.[89] It included 155 studies, more than 80 percent of which took place in Global North countries. The authors concluded that more support is needed for empirical studies of disinformation in Global Majority countries as well as for studies comparing Northern and Majority contexts. But in the absence of such studies, funders are using this limited evidence base to inform their agendas. If funders want to see RCTs in the Global Majority, they should incorporate them into the programs they support—but they should not ignore existing scholarship that is not based on RCTs.

The power imbalance between Global North donors and aid recipients in the Global Majority is a tectonic force shaping the landscape in which activists work. This top-down arrangement traps local activists in ineffective and extractive workflows. Some interviewees in the Global Majority knowledge exchange project complained of Global North research partners poaching their staff and of grants requiring the use of software and data collection to refine approaches for use in other countries. Global Majority civil society leaders expressed wariness about extractive arrangements where local harms and horrors are collected, gathered, and decontextualized for tool development and advocacies elsewhere. As one interview participant said, "We are not your f—ing case study!"

How to Fix It

When we asked participants to envision an agenda by and for the Global Majority, the answers we received revealed common themes.

First, many observers in Global Majority countries see disinformation as an accountability issue, not a problem resulting from a deficit of good information or media literacy. They focus on accountability for players at all levels within a putrefying digital public square overrun by profit-driven clickbait and disinformation as a commercial service. This includes

tech companies, whose underinvestment in content moderation they hope to expose and reverse. It also includes politicians who have leaned into new platforms and relationships with influencers to stoke voter anger and spread anti-establishment messages. More can be done to expose the conflict entrepreneurs and shed light on the many regulatory gray areas in social media infrastructure that politicians and influencers exploit to their political and commercial advantage.

The second theme is that exposing disinformation's sources requires deep investigations, often combining online and offline methods to identify both the principals and agents of a given campaign. The focus on debunking disinformation displaces this desire for exposure and accountability, and the mostly online, open-source intelligence techniques for social media monitoring and detection of inauthentic activity which many donors encourage do not fully substitute for investigative journalism or ethnographic research.

The third theme is that many activists wish they could do more community dialogue and outreach on the ground. "It's harder to find funding for trust-building campaigns at the grassroots," one interview participant told us. "Funders are obsessed with tools that are scalable. It's not sexy to do community dialogues." But activists feel this kind of granular work is important to build trust with communities outside of major metropolitan areas and diminish the impact of disinformation in ways fact-checks from afar cannot.

More important than any one strategy or approach is the need for structural change in the way civil society coalitions are created and sustained. It is possible, through more inclusive, bottom-up approaches, to unleash the Global Majority's creative capacity. We identify three main ways that civil society in the Global Majority and their philanthropic supporters in the Global North can do so:

1. **Encourage "big tent" coalitions**. Instead of structuring coalitions around shared processes, tools, and approaches, embrace diversity and create spaces for civil society to exchange priorities and knowledge. Our research found that in the Philippines, many activists felt shoehorned into fact-checking projects that were not their specialty and that put them into competition with their peers in a crowded field. In Brazil, on the other hand, civil society entered into diverse partnerships that included issue area groups like Greenpeace and approaches ranging from community outreach to advertising reform. This allowed civil society to reach broader audiences and play to the strengths of individual coalition members.

2. **Redouble efforts to localize government-funded aid projects.** One research professional told us that technology and democracy efforts are notoriously "ten years behind" on efforts to award more projects directly to local implementing partners rather than to large international development organizations based in the Global North. A February 2024 study similarly found that the number of local awards provided by the U.S. Agency for International Development (USAID) fell "far below" its goal of 25 percent, even before the agency was dismantled by President Donald Trump's administration in early 2025.[90]

3. **Support Global Majority knowledge creation and guard against extractivism.** As mentioned above, the mismatch between research on the Global North and the Global South makes it difficult to create evidence-based programs that reflect local contexts and realities. Our work showed that activists and researchers recognize that they have much to gain by working together: researchers gain practical insights from activists, who in turn benefit from research findings when designing programs. However, this reciprocal relationship is hampered by the lack of opportunities and trust—practitioners fear extractive research arrangements, and there are too few initiatives to bring the two sides together. Funders can promote more productive, trusting relationships by supporting opportunities for repeat exposure, such as projects that integrate researchers into project implementation and academic fellowships for practitioners.

Acknowledging the Realities Under the Trump Administration

Trump's administration has not been sympathetic to the need for more localized aid and increased autonomy for Global Majority activists. On the first day of his second term, Trump issued an executive order freezing U.S. foreign development assistance and reviewing it for "consistency" with his foreign policy,[91] leading to chaos across the international development sector as career professionals struggled to determine what work could continue, what work could be salvaged with a pause, and what would happen to implementing partners who rely on program funds for their salaries. The administration subsequently dismantled USAID entirely, eliminating huge swaths of the U.S. workstreams dedicated to combating misinformation and disinformation altogether. A close reading of the Project 2025 chapter concerning USAID suggests that the administration might instead pivot to include a more securitized focus on countering "malign influence" from adversaries—a priority that has led the United States to run its own influence operations in countries where USAID funded counter-disinformation work.[92] Under the Trump administration, U.S. foundations will need to consider playing a bigger role in this space. They should start by committing to respect the viewpoints of local scholars and activists who call the U.S. focus on information integrity against foreign influence "a war that doesn't deal with our problems."[93]

In short, analysts should push back on the disempowering frames that depict the Global Majority as a digital dystopia of unfathomable and extreme technological harms that could be solved by importing tools and concepts from the Global North. Rather, partners in the Global North should engage Global Majority civil society as innovative civic entrepreneurs who are designing meaningful solutions to problems as they exist on the ground.

While the future of U.S. government aid in this area is dim and uncertain at best, other donors should commit to localizing more programs. Global Majority civil society leaders also have a chance to seize new opportunities for self-determination given the vacuum of leadership in tech accountability left wide open by the United States.

04

When AI Meets Cybersecurity: Framing Brazil's Information Security and AI Challenges

Luca Belli

Artificial intelligence (AI) has transformed the cybersecurity landscape over the past decade, leading to an increase in the frequency, impact, and sophistication of cyber attacks. While organizations can leverage AI to enhance their cyber defenses, detect cyber threats, and improve decisions about how to react, cyber criminals can also exploit the technology to launch targeted attacks at an unprecedented speed and scale, bypassing traditional detection measures.

Indeed, the increasing use of AI systems in a wide range of processes in various critical sectors—such as health, justice,[94] and autonomous vehicle management—creates numerous new, and sometimes unpredictable, risks and can open new avenues in attack methods and techniques.[95] Such risks are maximized when AI is deployed for automated decisionmaking, leading legislators around the world, including in Brazil, to consider appropriate risk regulations aimed at AI systems.[96]

This essay argues that considerable work is needed to support the implementation of existing and proposed cybersecurity and AI frameworks. Such effort is particularly necessary through the adoption of technical standards able to specify and give meaning to highly vague formulations that are typically adopted by AI regulatory frameworks to define cybersecurity risk management provisions. Notably, the essay focuses on the Brazilian context to explore how the country is dealing with the emerging threats and opportunities presented by the intersection of AI and cybersecurity, a set of issues that Brazil—and any other country—needs to consider seriously to be able to build its AI Sovereignty.[97]

AI and Cybersecurity: A Complicated Relationship

The relationship between AI and cybersecurity is dynamic, affecting defensive, offensive, or adversarial capabilities.[98] While there is already a wide body of research on the technical aspects of AI and cybersecurity, remarkably scarce research exists on the interactions of AI and cybersecurity from a regulatory and governance angle. To start, it is important to distinguish between defensive AI and offensive AI. Defensive AI usually leverages machine learning and other AI techniques to enhance the cybersecurity and resilience of computer systems, networks, and databases, and to protect individuals by shielding them against cyber threats.[99] From this perspective, AI systems can increase the effectiveness of security controls aimed at protecting specific assets, for instance through automated malware analysis, active firewalls, and automated cyber threat intelligence operations.[100]

In contrast, offensive AI, also known as AI-powered cyber attacks, involves the use of AI to launch malicious activities, enhancing attackers' ability to detect and exploit vulnerabilities, develop new cyber attack types and strategies, or automate the exploitation of existing vulnerabilities.

A Paradigm Shift

The integration of AI capabilities constitutes a watershed moment in the development of cyber threats, significantly augmenting the efficacy, scope, scale, and precision of malicious cyber operations. This evolution marks a paradigm shift in the cybersecurity landscape, fundamentally altering the nature of both offensive and defensive strategies.

First, the democratization and increased sophistication of AI tools enables cyber criminals to automate and refine their attacks, making them more effective, dynamic, and difficult to detect. Machine learning algorithms, for instance, can analyze vast amounts of data to identify vulnerabilities in systems and networks, enabling attackers to exploit these weaknesses with greater precision. Automated phishing campaigns can be tailored to individual targets based on data harvested from the target's social media accounts and other sources. This personalization increases the likelihood of the target falling for the phishing scam, as the messages appear more convincing and relevant. Critically, AI-enhanced malicious attacks now represent the top emerging risk, according to the latest version of the periodic Gartner study dedicated to risk monitoring, because "the relative ease of use and quality of AI-assisted tools, such as voice and image generation, increase the ability to carry out malicious attacks with wide-ranging consequences."[101]

Second, AI is likely to expand the scope of cyber threats by allowing attackers to increase the scale of their operations with minimal human intervention. For example, attackers can use AI-powered botnets to implement massive distributed denial-of-service (DDoS) attacks, shutting down the targeted website, server, or network with a large volume of traffic. Ransomware attacks—when an attacker infects a targeted device with malware and

threatens to deny the victim access to their device or release sensitive data if the victim does not pay the demanded ransom (although the payment does not guarantee data recovery, as obviously there is no enforceable contract with cyber criminals and data decryption entirely relies on their "good faith") are also becoming more widespread because of AI, leading to the emergence of a thriving global industry of ransomware-as-a-service (RaaS).[102] In this context, AI is lowering barriers to entry for attackers and increasing the ease and availability of ransomware, resulting in high costs associated with recovery and extended downtime.[103]

Third, AI systems can substantially increase attackers' ability to analyze complex datasets and recognize patterns, thus allowing them to execute highly targeted and precise attacks. For example, AI can be used to identify high-value targets within organizations and tailor attacks to their specific roles and responsibilities. AI can also allow cyber criminals to create realistic audio and video impersonations known as deepfakes, which can be used in social engineering attacks to manipulate individuals into divulging sensitive information or authorizing fraudulent transactions.[104] In a memorable case of an elaborate deepfake scam, a finance worker at a multinational firm was duped into paying $25 million to fraudsters who had lured him into a fake emergency call.[105]

Fourth, the increasing sophistication of deepfakes can be used to orchestrate disinformation campaigns for both financial and political purposes. These technologies pose a novel cybersecurity threat to democratic processes by enabling malicious actors to undermine information integrity at an unprecedented scale. The current democratization of AI implies much greater and easier access to AI systems that, until just a few years ago, were only accessible to researchers and highly specialized companies or governmental actors.[106] This process leads to an enormous expansion of the attack surface, both in terms of potential perpetrators and potential vulnerabilities and attack strategies that can be used.

Importantly, AI-driven cyber attacks have acquired a dynamic nature; they can adapt to changing defensive measures, making detection and mitigation more challenging. By using machine learning capabilities, attackers can alter malicious software in real time to avoid detection by traditional antivirus systems. For instance, AI-enhanced polymorphic or metamorphic malware can mutate its features or automatically "re-code" itself when it propagates to evade pattern matching detection systems that are traditionally deployed as security solutions. Furthermore, AI systems can be used to quickly identify and exploit zero-day vulnerabilities before patches can be developed and deployed.[107]

Crucially, defenders are also increasingly employing AI-based systems to detect cyber threats and vulnerabilities and rapidly respond, for instance by leveraging AI to identify software bugs and self-patch them. However, within a sort of cybersecurity arms race, attackers are also leveraging AI to outmaneuver these defenses. In a situation where both sides continuously refine their techniques, defensive AI systems must evolve rapidly to detect new attack patterns and anomalies, while policy and governance framework must be crafted to mitigate risks and facilitate communication, collaboration, and coordination among cybersecurity stakeholders.

Understanding the Brazilian Context

Despite relevant advancements in recent years, the regulation of AI and cybersecurity in Brazil is highly fragmented, limited, and poorly implemented. By adopting multiple cybersecurity-related sectoral regulations, Brazil has improved in several international rankings that assess cybersecurity readiness.[108] But regulatory oversight and cybersecurity implementation remain patchy because such processes are the responsibility of many different and uncoordinated entities, including sectoral regulators, private and public computer security incident response teams, and the military.[109]

Critically, Brazil does not have a general cybersecurity law, nor a cybersecurity agency, which represents an unforgivable deficiency, in 2025. The top institution responsible for cybersecurity governance and policy proposal is the Institutional Security Cabinet (GSI in its Portuguese acronym) of the Brazilian presidency. However, the GSI's remit is limited to the federal administration, restricting the scope of its reach. Importantly, in December 2023, Brazil adopted a new National Cybersecurity Policy and established a new multistakeholder National Cybersecurity Committee,[110] known as "CNCiber," of which the author of this essay has been appointed a member.[111] Among the tasks of CNCiber is the elaboration of a proposal for a new national cybersecurity strategy and a new body for cybersecurity governance and regulation.

Indeed, one of the reasons for Brazil's fragmented cybersecurity regulatory landscape is the lack of a unique institution responsible for coordinating the various dimensions of cybersecurity. At this moment, Brazil does not have an actionable cybersecurity strategy allowing the country to organically tackle the multiple—and mounting—cyber threats it faces nor a cybersecurity agency able to assess the ways in which AI technologies are impacting such threats.

Furthermore, only limited AI regulation exists, primarily under the purview of the Brazilian National Data Protection Authority (ANPD). In this context, the Brazilian National Congress is currently considering dedicated legislation to regulate AI, which would include cybersecurity obligations related to AI systems. (At the time of publication, legislation was still pending and the rapporteur of a new Special Commission for AI, established by the Chamber of Deputies, had promised to alter the bill.)[112]

Information Security?

Information security is an essential dimension to both AI and cybersecurity. In Brazil, the ANPD is tasked with enforcing the Brazilian General Data Protection Law (LGPD) and ensuring that organizations comply with data protection obligations.[113] Data security is a fundamental principle set by the LGPD, aimed at ensuring that personal information is protected against unauthorized access, loss, alteration, damage, or destruction. Importantly,

the LGPD explicitly establishes a security-by-design obligation for data controllers and processors, who need to implement security measures that the data subject "can expect" to demonstrate that personal data processing activities are regularly undertaken.

To comply with the LGPD, data processing agents—that is, the individuals or entities responsible for defining how personal data are processed in a given organization and implementing such decisions—are supposed to implement solid information security solutions, such as establishing an information security policy, raising awareness and capacity, and establishing technical measures to build data resilience. Without these, data processing should be considered irregular. In practice, however, data security compliance is poor at best. In the first four years after its inception, ANPD did not adopt the minimum data-security standards that it was empowered to enact in accordance with LGPD article 46.1, and its oversight is limited to receiving communications about data breaches without providing any solutions.

While the ANPD has a potentially enormous role to play in establishing data security regulations aimed at avoiding cybersecurity incidents, it has instead spent its energies on regulating the communication of such events to the public, providing guidance only on how the tragedy must be communicated instead of about how to avoid it. Indeed, Brazil ranks second globally for cyber attacks, which have exploded in number and sophistication because of the adoption of AI systems together with frequent data leakages and a "thriving" black market for personal data.[114]

A more proactive approach has been adopted by the Ministry of Management and Innovation, through its Ordinance SGD/MGI No. 852, which established the Privacy and Information Security Program (PPSI).[115] PPSI is designed to enhance cybersecurity in the Brazilian public administration by providing guidance on data governance, encouraging projects and adaptation processes aimed at increasing cybersecurity maturity, resilience, effectiveness, collaboration, and intelligence. However, the Brazilian Court of Auditors has recently assessed that the implementation of PPSI is at an alarmingly low level, noting gross lack of compliance.[116]

While the LGPD and PPSI are essential information security pillars, they are not sufficient on their own. It is essential that a new cybersecurity strategy and a cybersecurity agency, to be proposed by the National Cybersecurity Council, provide guidance on how to specify information security criteria applicable to all entities, with particular regard to providers of essential services, critical infrastructures, and all entities managing categories of sensitive information that are not personal.[117] Furthermore, a future Brazilian cybersecurity agency should establish cooperation agreements, and ideally an effective communication and coordination mechanism, with the ANPD and the other sectoral regulators to ensure a harmonized cybersecurity approach.

What Is an "Appropriate" Way of Regulating AI?

It is important to emphasize that both cybersecurity and AI are quintessentially multidimensional. Indeed, the effective regulation of AI risks and digital technology cybersecurity relies on the understanding that both AI and digital technologies are systems based on the interconnection of data, software, and hardware. Risks and vulnerabilities are inherent to both the elements that compose the systems and the ways such elements interact. The success of both cybersecurity and AI governance depends on having a good understanding of how the different components of digital and AI technologies interplay, how they are utilized, and what are the vulnerabilities in their use and deployment.[118]

Sound management of information and infrastructure, good stakeholder coordination, and solid capacity-building are therefore essential for both AI and cybersecurity regulation. However, in Brazil, each dimension or component of both AI and cybersecurity is currently regulated by multiple entities with limited or no coordination. While Brazil is in the process of developing a new AI framework, there are several concerns about the way in which the framework proposes to regulate cybersecurity aspects of AI and foster coordination among sectoral regulators.

For one, all versions of Brazil's proposed AI framework—including the last one available at the time of this writing—have included a considerable amount of vaguely worded cybersecurity provisions, such as obligations to "perform tests to evaluate appropriate levels of security" of AI systems (see article 18.c).[119] "Appropriate" and "adequate," along with "reasonable," are every lawyer's favorite adjectives because they can mean virtually anything. While such language is essential to preserve normative flexibility, with no further guidance this can easily turn into legal uncertainty, which is the opposite of what new regulations should bring.

Clarifying and specifying these flexible provisions will require considerable technical knowledge. It is not a coincidence that the EU AI Act delegates this task to technical standardization bodies.[120] However, this solution has raised concerns from human rights advocates who claim it constitutes a delegation of regulatory power to private and poorly accountable standardization bodies with scarce knowledge about fundamental rights' risk posed by AI systems.[121]

To address these challenges, the Brazilian AI bill proposes to establish an AI governance and regulation system, where all sectoral regulators would come together under the leadership of the ANPD "to regulate and classify high risk AI systems" considering, among other things, "the high potential for systemic harms, such as to cybersecurity, and violence against vulnerable groups" (see article 15.VII that associates these two rather different risks for unspecified reasons).

The idea of a coordination system is promising, but the bill fails to articulate how it would function in practice and, most worryingly, who would deal with the cybersecurity dimensions of AI. Additionally, it seems risky to entrust the leadership of the system to an overstretched organ that barely manages to cope with fulfilling its current mission. To think that the ANPD, under its current structure, can effectively lead a new system of such relevance and magnitude, and effectively guarantee AI cybersecurity seems overly optimistic.

Conclusion

The relationship between AI and cybersecurity presents significant and transformative developments. While it has empowered malicious actors to conduct more impactful, far-reaching, and precise attacks, it has also underscored the importance of proactive and adaptive cybersecurity strategies. Indeed, the integration of AI into offensive and defensive cyber capabilities demands a fundamental shift in cybersecurity strategies.

In this context, fostering collaboration between government entities, private sector organizations, and research institutions is essential for Brazil—and all other states—to address the challenges posed by AI in the cybersecurity domain. The adoption of a multistakeholder approach is critical to understand the cyber threats landscape and develop effective regulations, standards, governance, and capacity-building mechanisms. Indeed, these elements are key to implementing robust cybersecurity measures and promoting innovation in defensive AI technologies to cope with mounting AI-driven cyber attacks.

Unfortunately, despite some advancements, the current Brazilian approach does not seem capable of confronting effectively the mounting number and complexity of cyber threats. It is vital that considerable resources be allocated to support an effective multistakeholder cooperation that need to be enshrined in the future strategic and institutional framework adopted by Brazil. This will not only increase the quality of policymaking with evidence-based solutions but, more importantly, will enable inter-stakeholder coordination to implement cybersecurity measures in an agile and effective fashion.

In this perspective, the establishment of a robustly resourced Cybersecurity Agency must be seen as an imperative for Brazil, enabling the country to comprehensively assess how both existing and emerging technologies can either bolster or compromise cybersecurity. Considering the increasing reliance of our critical infrastructure, essential services, and societal functions on AI systems, neither Brazil nor any other country can afford to operate without considering the cybersecurity of AI systems an utmost priority.

05

Toward a Transatlantic Information Defense Framework

H. Akin Unver

The Foreign Information Manipulation and Interference (FIMI) framework is starting to become the dominant method in the European Union (EU), the United States, and Canada to analyze dynamics in the information space—replacing loaded and tired terms like disinformation, propaganda, and fake news.[122] The FIMI framework was developed and systematized by the European External Action Service (EEAS) in 2022 to serve as an integrated toolbox to pool EU resources for tracking, monitoring, and mitigating foreign influence operations and channel these resources into a coherent, EU-wide defensive mechanism.[123]

FIMI refers to coordinated efforts by foreign state or non-state actors to influence political, social, or economic outcomes in a target country by deliberately manipulating or distorting information or communication processes.[124] Unlike disinformation, which focuses solely on the spread of false or misleading content, FIMI encompasses a broader range of activities, including the strategic amplification of true but contextually misleading information, suppression of critical narratives, and manipulation of social platforms to exploit existing divisions. It also differs from cyber attacks, as it primarily targets perception, trust, and decisionmaking processes rather than the integrity or functionality of digital systems. The FIMI framework is not just a new way of approaching old problems; it systematizes an elaborate and iterative early detection, data collection, and countermeasures architecture that incorporates a unified lexicon (techniques, tactics, and procedures), an integrated foreign influence monitoring and data collection interface, and a coherent repertoire of actions scalable at the EU-level and translatable across member state languages.[125]

While the FIMI framework is by no means the first attempt to address foreign information manipulation, its reach goes beyond the confines of Brussels. It is now one of the main joint frameworks used by the EEAS and the NATO Hybrid Center of Excellence (COE), with the

latter actively relying on FIMI's interface to conduct its own monitoring of foreign influence.[126] In 2024, the United States began drawing from the EEAS's FIMI framework as a model of international cooperation to counter foreign influence, including developing a pilot project between the U.S. State Department and the EEAS focusing on the Western Balkans as a flashpoint of Russian influence operations.[127] A month later, the State Department launched The Framework to Counter Foreign State Information Manipulation—a diplomatic mechanism to coordinate joint efforts with allies.[128]

In 2024, there was also greater convergence between the EEAS's and Canada's Rapid Response Mechanism (RRM), operating under the G7 framework and the 2022 Strategic Partnership Agreement.[129] The RRM has begun to adapt some of the tools from the EEAS framework, most important of which is the DISARM Framework, an information warfare escalation ladder that tracks organized manipulation before it reaches viral proportions.[130] Similar coordination mechanisms are being developed with Australia and Japan that focus on China and use the EEAS's FIMI framework for a joint defense in Southeast Asia.[131]

The current momentum of the FIMI framework across EU partner countries suggests that a broader allied information defense initiative could be in the works. Indeed, the reason why the EEAS's FIMI framework has become so popular so quickly is that it includes a robust attempt to establish a common information defense lexicon, as well as shared monitoring interfaces that are easily adaptable by allied countries.

However, 2024 also laid bare a number of obstacles to further developing FIMI. The four most difficult to resolve are discussed below.

My FIMI Is More Important Than Your FIMI

The threat landscape for FIMI varies significantly across the United States, Europe, and East Asia, reflecting each region's geopolitical priorities and constraints. As countries focus on their own imminent and pressing dangers, it becomes difficult to coordinate priorities across allies, rendering an effective prioritization of resources difficult from a diplomatic standpoint.

In Europe, the Russian FIMI threat is particularly urgent given geographical proximity and historical tensions. Russia's campaigns focus on destabilizing the EU's cohesion, challenging NATO, and influencing public opinion on energy dependency and security policy. In contrast, China's influence in Europe has primarily been economic and diplomatic, though there is growing concern about its covert influence activities. In the latest EU Disinfo Lab conference in Riga in October 2024, only one of the dozen panels had a speaker focusing on China, with the rest exclusively focusing on Russia, demonstrating the discrepancy between partners.[132]

For Japan and South Korea, FIMI threats are predominantly centered on regional tensions with North Korea and China. North Korea's tactics include cyber and influence operations targeting South Korea, while China's operations often seek to sway public opinion on security issues, maritime rights, and economic relations. These varied threat levels mean each region brings different priorities to a unified FIMI framework, potentially complicating consensus about which country's FIMI threat will be addressed first.

DIMI is Equally Important as FIMI

A significant obstacle to a unified FIMI defense framework is the presence in some countries of domestic stakeholders and interest groups that are directly connected to foreign influence actors. These actors make up a substantial portion of the domestic information manipulation and interference, or DIMI, ecosystem.

In the United States, some organizations and public figures promote narratives that align with the interests of foreign state actors, sometimes because of financial or strategic ties. For example, conservative media outlets and influencers associated with the Tennessee-based media company Tenet reportedly received funding linked to Russian state-backed media outlet RT and amplified pro-Kremlin viewpoints.[133] Similarly, groups such as the National Rifle Association (NRA) have been scrutinized for past alleged associations with Russian officials who reportedly sought to cultivate influence within conservative circles in the United States.[134]

In Europe, several political parties, especially those on the far-right, have reportedly maintained ties with Russian entities. For instance, the French National Rally, led by Marine Le Pen, reportedly received a loan from a Russian bank; critics argued that the loan contributed to the party's pro-Russia stance, especially on issues like sanctions and EU-Russia relations.[135] In Italy, the far-right League party, led by Matteo Salvini, has faced allegations of Russian connections, including that Salvini allegedly met with Russian officials to discuss potential funding.[136]

In Australia and New Zealand, economic ties with China have led to concerns about Beijing's influence over local politics and businesses. Former Australian senator Sam Dastyari resigned amid controversies surrounding his links to Chinese donors and public statements that aligned with Beijing's positions.[137] In New Zealand, the dairy and tourism sectors heavily depend on Chinese markets, leading to apparent reticence among some business leaders and political figures to publicly challenge China over disinformation and its assertive foreign policies.[138] These cases illustrate how direct and indirect ties between domestic actors and foreign states complicate efforts to form a unified framework to counter FIMI, as business or political stakeholders with interests that align with foreign governments may resist or undermine anti-FIMI measures.

Domestic entanglements with foreign actors, especially when those domestic actors gain political influence or governmental positions, complicate the creation of a joint FIMI framework. They can spark internal resistance, dilute commitments to anti-FIMI initiatives, and raise trust issues among framework members, who may be concerned about domestic actors in allied nations leaking sensitive information to foreign influence campaigns. This means that varying contours and prerogatives of DIMI can impair allied cohesion against FIMI and lead to a miscoordination of efforts and policies aimed to address foreign interference.

The API Problem and Data Unavailability

Many platforms—such as Facebook, X (formerly Twitter), and TikTok—have tightened Application Programming Interface (API) access in recent years, often citing privacy regulations, data protection concerns, or proprietary interests. These restrictions limit researchers' ability to retrieve crucial data on misinformation trends, bot activity, and network interactions in real time. Additionally, the high costs associated with API access on some platforms put it out of reach for many academic or public interest researchers.

Data availability is further restricted by platform policies that limit access to certain kinds of user-level or engagement data, particularly for researchers outside the United States. These limitations can make country-specific FIMI research exceptionally challenging. Without comprehensive datasets, researchers are often forced to rely on incomplete or inconsistent data, reducing the accuracy and impact of their findings. These limitations also make it difficult for researchers to collaborate across countries on joint FIMI projects, as data disparities can create inconsistencies in analytical methods and findings. The absence of standardized, affordable, and accessible data pipelines directly impairs the ability to detect and counteract foreign interference across diverse regions, hindering a globally unified approach to FIMI defense.

Platform Architecture

Platform architecture significantly influences the spread and success of different FIMI tactics, creating challenges for coherent, cross-platform research and response initiatives. Each social media platform has a unique architecture—encompassing content algorithms, user interaction features, and moderation policies—shaping how information is amplified or suppressed. For example, TikTok's recommendation-heavy feed and short video format make it an ideal venue for highly engaging, visually oriented disinformation, while X, with its open, real-time feed, is often used for rapid dissemination of breaking narratives or coordinated hashtag campaigns. Facebook's groups and communities foster echo chambers where disinformation can incubate within specific interest clusters, creating more isolated yet resilient pockets of influence.

This diversity in platform architectures makes it challenging for a multi-country FIMI research initiative to adopt a uniform data collection and countermeasure approach. Researchers now have to tailor their data collection techniques to each platform's unique features, making cross-platform comparisons difficult and creating methodological inconsistencies. As mentioned, platform-specific data limitations—such as closed APIs or restricted user-level data—can further fragment research efforts, leading to gaps in understanding how disinformation campaigns migrate across platforms and regions.

How to Build a Truly Transatlantic FIMI Framework

To move forward in building a cohesive transatlantic framework for countering FIMI, there are several ways to streamline operational collaboration and address existing structural obstacles.

First, given the divergent threat landscapes across the United States, Europe, and Asia, a centralized threat prioritization protocol should be implemented to identify and allocate resources to shared FIMI concerns. For example, an EU- and U.S.-led FIMI task force could systematically assess FIMI campaigns based on severity, immediacy, and cross-border impact. To enhance focus and responsiveness, the task force could leverage AI-driven analytics to classify and triage threats, identifying high-risk operations (for instance, Russian interference in EU elections or Chinese influence in the Asia-Pacific region) and deploying response teams accordingly. Under U.S. President Donald Trump, this coordination will likely be even more difficult, taking into account his ongoing policies that cut funding and data access for U.S.-based researchers and institutes working on FIMI.[139]

Second, effectively confronting domestic entanglements with foreign influence actors demands enhanced transparency alongside regulatory heft. U.S. president Joe Biden made considerable progress in this area. For example, near the end of his term, his team proposed updating the Foreign Agents Registration Act (FARA) to better track and disclose financial or ideological ties between domestic entities and foreign states.[140] Similarly, his administration robustly supported the U.S. State Department's Global Engagement Center, which was designed to serve as the hub of a global information resilience effort and funded research initiatives aimed to build synergies with Europe and beyond over countering information manipulation.[141] But Trump and his allies have taken a different tack, criticizing disinformation programs as contracting out "censoring real medical voices with real expertise that put real Americans' lives in danger."[142] Trump's reelection has imperiled these programs, resulting in their defunding and closure.[143]

Third, to address the API problem, the EU and other likeminded partner nations could establish a cooperative, standardized API access framework, with agreed-upon levels of data accessibility tailored to FIMI research needs. This could involve a data-sharing consortium involving platforms like Facebook, X, and TikTok, allowing qualified researchers and intelligence agencies access to FIMI-relevant datasets across borders. The consortium could

also negotiate reduced API access fees for approved research projects, democratizing access for academic and public-interest researchers. Princeton University's Accelerator initiative, which aims to create a joint repository of data on the information environment to foster international research on digital media, is a major step in the right direction and a model to draw from for multi-country research projects focusing on FIMI.[144]

Finally, to support cohesive transatlantic action, a formal allied information defense pact should be established, centered around a unified information manipulation detection and attribution lexicon and operational standards. This pact would require member countries to standardize key terms, methodologies, and response protocols to ensure alignment in tracking and countering FIMI threats. A common FIMI lexicon would ensure that all participants share a clear understanding of foreign adversary techniques, tactics, and procedures—making it easier to coordinate and compare data across diverse contexts. During the Trump administration, the bulk of this effort will likely fall to Europe, which will have to find ways to cooperate on research, funding, and data collection without a full contribution by the United States.

06

Techno-Legal Internet Controls in Indonesia and Their Impact on Free Expression

Irene Poetranto

Countries around the world are increasingly enacting or amending laws and regulations to control the internet. These regulations often require information intermediaries—such as internet service providers (ISPs) and social media platforms—to block or restrict access to certain types of content. Governments typically enforce these mandates through coercive mechanisms, including threats to revoke companies' licenses, arrests, or prosecutions. As ISPs and platforms operate within state jurisdictions, they must implement these controls at the behest of national governments.

Indonesia provides compelling evidence of how regulatory frameworks shape state control over online content. Similar to the trend seen in other countries, Indonesia has introduced laws and regulations that require ISPs and platforms to enforce content restrictions using broad and ambiguous criteria such as "misinformation," "fake news," and "hate speech."[145] This development has raised significant concerns about the impact of such measures on free expression.[146] In 2023, Freedom House reported that Indonesia was one of "forty-one governments [that] blocked websites with content that should be protected under free expression standards within international human rights law," highlighting the global relevance of this approach.[147]

Given the key roles of ISPs and social media platforms in internet infrastructure, understanding the full scope of state-directed internet control requires more than just analyzing legal texts. It also demands technical investigations into how these intermediaries implement laws at the infrastructural and technical levels. Such an analysis would also uncover the potential long-term consequences of internet controls on users' abilities to access information and engage in free expression.

This essay addresses that gap by examining Indonesia's use of domain name system (DNS) redirection as a method of internet censorship. By analyzing how ISPs enforce the country's internet control mandates, the essay sheds light on the broader implications of government-imposed controls, including their potential long-term effects on access to information and online freedoms.

How Indonesia Controls Internet Content

Indonesia is among many countries that control the internet through legal and technical mechanisms. For example, Russia has passed laws that facilitate state-directed internet control while imposing technical obligations on information intermediaries.[148] The country's internet regulator, Roskomnadzor, enforces these laws and has issued a detailed set of technical recommendations for ISPs to filter or block online content.[149] Noncompliance results in sanctions, such as fines.[150]

Like Russia, Indonesia has established laws and technical guidance over the years to control information online.[151] The implementation of controls, such as content blocking, in Indonesia is decentralized. That is, although the government sets guidelines about what content should be blocked—for example, through the official block list called "Trust+Positif," or "Trust Positive"—technical implementation has traditionally been left to ISPs' discretion.[152] In other words, the Indonesian government does not currently operate a nationwide technical filtering system like China's so-called "Great Firewall" filtering system.[153]

Since at least 2008, Indonesian ISPs have implemented government-directed blocking against so-called "negative" content, a term used to describe material deemed defamatory or objectionable (or violating social or moral norms).[154] Laws such as the Electronic Information and Transaction (EIT) law, which contains provisions on defamation, and the Law on Pornography are commonly cited to justify internet controls. Both laws have been criticized for being vague and overly broad and selectively enforced against human rights activists, journalists, and government critics.[155]

With over 1,000 ISPs operating in Indonesia as of 2024, many privately owned, researchers have found various internet filtering devices and software and content control practices.[156] In 2024, the Internet Monitoring Action Project (iMAP) reported over 210,000 instances of confirmed website blocking in Indonesia.[157] Then, as it is now, content targeted for blocking on the government's Trust Positive block list included those that contain political and religious issues and those related to sexuality and gender, such as LGBTQ websites.[158]

Many ISPs in Indonesia implement internet filtering by tampering with websites' domain name system (DNS), a method also employed in other Southeast Asian countries.[159] DNS is key to the internet's functioning because it translates domain names (such as carnegieendowment.org) to internet protocol (IP) addresses (such as 199.15.213.232), allowing internet-connected devices to find or communicate with one another.[160] DNS servers, such

as Google Public DNS, which, as of 2024, was the largest public DNS server available for free worldwide, perform the translation of domain names to IP addresses for the general internet globally.[161] DNS tampering is "an umbrella term used to describe various forms of DNS interference" that affect information flows online.[162] For example, Indonesian ISPs have used DNS hijacking to perform website blocking since the early 2000s.[163] When this occurs, accessing a particular domain name results in an intentionally incorrect response or IP address; for instance, instead of the page that was requested, users receive a block page or a page stating that the domain name does not exist. Internet filtering using DNS hijacking is straightforward for ISPs to implement and is therefore used widely by ISPs in Indonesia and elsewhere. In addition, testing conducted by iMAP researchers in 2023 uncovered that some Indonesian ISPs used TCP/IP and HTTP blocking methods.[164]

The deployment of various filtering systems and techniques by Indonesian ISPs in response to the country's broad and vague laws have contributed to inconsistencies in content blocking. For example, the Ministry of Communication and Digital Affairs, Indonesia's internet regulatory authority, has expressed concerns to ISPs since the early 2010s that many pornographic websites remain accessible despite the requirement to block them.[165] These concerns led the Indonesian government to announce in 2015 that ISPs must adopt specific technical requirements to filter online content. Former minister Rudiantara also declared that the government was in "the final stage" of creating its own DNS server (called the "National DNS" or "DNS Nasional"), which network operators would have to "synchronize with" to perform filtering.[166] In other words, once the National DNS was in place, Indonesian ISPs would cease using global public DNS servers like Google Public DNS.

The 2014 establishment of the National DNS, known as Trust+Positif, means that ISPs in Indonesia have to redirect all DNS traffic from their customers to that DNS, which contains a database of banned websites.[167] As a consequence, attempts by internet users to access websites listed in this database are blocked. The government argued that the mandatory use of the National DNS by Indonesian ISPs was necessary to prevent access to pornography.[168] However, the Trust Positive database included websites focused on human rights issues, LGBTQ content, and political criticism.[169] Applying content filtering through the National DNS system was tantamount to restricting freedom of expression and silencing dissent.[170]

The Citizen Lab Uncovers a New Technique: DNS Redirection

As will be shown in a forthcoming report, Citizen Lab researchers conducted a study in 2024 to uncover how Indonesian ISPs are fulfilling the government's requirement to synchronize with the National DNS. Using measurement testing, they found that two networks belonging to Telkom and Fastnet ISPs had begun the synchronization process using a technique known as DNS redirection.[171] DNS redirection is unique because, unlike other filtering methods, users can no longer use a public DNS resolver, such as Google or Cloudflare, to access restricted content. Consequently, local users seeking blocked content have far fewer circumvention options.

Although DNS redirection is a known practice in network or traffic management, the use of this technique for filtering purposes is newly discovered. For example, as of November 2024, no studies had been published about using DNS redirection for internet censorship. Furthermore, the Open Observatory of Network Interference project, which provides tools to volunteers for measuring and documenting internet filtering worldwide, did not include testing for DNS redirection on its platform as of 2024, which meant that its prevalence was unknown.

Conclusion

Indonesia's implementation of internet controls is illuminating for several reasons. First, it showcases how the Indonesian government, like the Russian government, uses legal and technical methods to harmonize controls across many information intermediaries operating in the country. This approach to internet controls presents challenges because, unlike legal frameworks that are more discernible to the public, technical methods are less visible and require specific knowledge or expertise to understand. More funding and support are needed to research these strategies and bolster collaborative efforts between digital rights groups and internet control analysts.

Second, as this case study demonstrates, techniques like DNS redirection can be difficult for average users to circumvent. Digital rights activists and scholars must pay particular attention to how controls implemented through internet infrastructure or via technical means implicate free expression and access to information. Moreover, as governments experiment with different technical methods to control the internet, more research is needed to detect novel methods that inhibit online information flows and develop circumvention practices against them.

Finally, despite the guidance issued by the Indonesian government regarding its preferred use of DNS redirection, Citizen Lab research found that, as of 2024, most Indonesian ISPs implemented blocking through whichever method they saw fit. A potential reason is that DNS redirection is more costly and challenging for ISPs to implement than other forms of DNS tampering. Information intermediaries are often responsible for internet control implementation, and technical mandates to block, surveil, or reroute internet traffic may be communicated by the government only to ISPs and technical communities. Therefore, advocacy against state-directed controls should involve partnerships with ISPs and other intermediaries. As state efforts to control the internet will likely continue, examining emerging techno-legal control tactics is crucial to understanding their impact on civil liberties and developing mitigation strategies for protecting users' rights.

07

A Case for the Disconnected: Focusing on the Unconnected Alone May Not Help Bridge the Digital Divide

'Gbenga Sesan

The world is becoming more connected. As of April 2025, 5.64 billion people were connected to the internet.[172] This reflects steady increases, with the number of those online growing from 2.77 billion in 2014. However, growing global connectivity rates do not account for a troubling pattern: although people are gaining access to internet infrastructure, their ability to use it is increasingly limited by governments. State deployment of internet shutdowns is on the rise.[173] These shutdowns have significant consequences for citizens everywhere. This essay explores the impact of internet shutdowns and emphasizes the importance of accounting for disconnected people.

Shutdowns Do Not Help Anyone

The broader societal costs of internet shutdowns include economic losses; disruptions to education, healthcare, and communication; and potential human rights violations. These harms outweigh any theoretical benefits governments use to justify shutdowns.[174] Shutdowns are not merely disruptions; they are deliberate tools of control. They often serve as stark illustrations of how authoritarian regimes wield digital repression to stifle dissent, suppress information, and curtail freedoms.

For instance, Myanmar experienced significant internet restrictions following the military coup in February 2021.[175] The monthslong shutdowns targeted mobile internet services and

specific social media platforms, affecting approximately 54 million citizens.[176] The prolonged disconnection had severe implications, including hindering access to critical information, disrupting business operations, and isolating citizens from the rest of the world.[177] In 2023, the estimated cost of Myanmar's shutdowns totaled over $745 million.[178]

India has seen similar shutdowns, though with a more targeted geographic focus on conflict-prone areas like Jammu and Kashmir. In 2023, the country recorded the most internet shutdowns globally, with eighty-four incidents affecting millions of people. These shutdowns, though often justified by security concerns, resulted in disruptions to daily life, no demonstrated positive impacts on security scenarios, and significant economic losses to the tune of over $31,554,106,041 that year.[179]

The news remained grim in 2024. According to a report by the digital rights group Access Now, 2024 was the worst year on record for shutdowns.[180] The report counted "296 shutdowns in 54 countries," which "continues a sharp uptick in the number of total shutdowns after what was already a devastating, record-setting year in 2023." The leading driver of shutdowns was conflict, with "103 conflict-related shutdowns in 11 countries." In these cases, militaries "deliberately turned to internet shutdowns" both in times of active fighting and as a tactic to control populations. More than 209 shutdowns, or 71 percent of the global total, affecting millions of citizens, centered in four countries: Myanmar, India, Pakistan, and Russia.

As of December 2024, Comoros, Gabon, Mauritania, Mozambique, Mauritius, and Pakistan had restricted access to the internet because of elections. Comoros started the year with an internet disruption when violent protests followed President Azali Assoumani's reelection in January.[181] For twenty-two days in July, Mauritania blocked mobile internet access following presidential elections and protests calling for a rejection of the results.[182] Mauritius shut down the internet multiple times—on October 25, November 3, and November 4—following protests over a disputed election.[183]

Accounting for the Disconnected

Given the rise in disruptions, disconnections, and full shutdowns, it is important to be precise about three categories of people: connected, unconnected, and disconnected individuals. Connected populations enjoy regular access to the internet. Unconnected citizens have never had access because of barriers such as the lack of infrastructure, affordability, or digital literacy. The disconnected are those who once had access but are temporarily or permanently cut off from the internet. This group often faces more severe repercussions during shutoffs because their lives and livelihoods might have heavily relied on internet connectivity.

Being disconnected from the internet may be more detrimental than never having been connected, as the psychological impact of having something taken away is often more profound

than being denied access in the first place.[184] This concept can be understood through the lens of behavioral economics, particularly the theory of loss aversion, which suggests that people experience losses more intensely than gains. When individuals or communities are disconnected from the internet, they lose access to communication channels, educational resources, familial and/or social connections, and economic opportunities, leading to frustration, anxiety, and a sense of isolation.[185]

Amid the internet shutdowns in Myanmar, students could not continue their education online, businesses relying on digital platforms suffered losses, and citizens were cut off from accessing crucial information and communicating with loved ones.[186] The abrupt disconnection led to a state of uncertainty and helplessness, highlighting the impact of being disconnected compared to those who were never connected.

Economic, Developmental, and Human Rights Consequences

The economic implications of internet shutdowns are profound. Experts estimate that in 2024 alone, internet shutdowns cost the global economy over $7.69 billion in forgone revenue.[187] The Internet Society's methodology for measuring the economic impact of internet shutdowns considers the impact on gross domestic product (GDP) per capita, employment, inflation, likely foreign direct investment, the age dependency ratio, and the fraction of the population residing in urban areas, among others.[188] In Kashmir, for example, the 2019 internet shutdown led to estimated economic losses of $2.4 billion over 213 days.[189]

Shutdowns also impede development, because internet access is a critical tool for innovation, education, and healthcare. Disconnection can halt the progress of digital initiatives and set back developmental goals. During the COVID-19 pandemic, internet access became essential for remote work and online education. Shutdowns in various parts of the world during this period exacerbated the challenges faced by students and professionals, who already faced limitations in how they could access learning or perform their work. This period further highlighted the developmental setbacks caused by disconnections.

Finally, internet shutdowns raise significant human rights concerns. The right to access information is enshrined in international human rights law, and arbitrary shutdowns violate this right. The United Nations has repeatedly emphasized that restricting internet access undermines many associated rights.[190] It argues that shutdowns can suppress freedom of expression, hinder free assembly, and limit access to emergency services. Indeed, shutdowns have been used during times of political unrest to stifle dissent and control political expression, infringing on citizens' rights to information and free speech.

Conclusion

Internet shutdowns have far-reaching consequences—disrupting lives, economies, and societies. The unique harms suffered by disconnected individuals, who lose access to the services they once had, highlights the importance of preserving connectivity. As the world becomes more interconnected, ensuring consistent and equitable access to the internet should be a priority for all stakeholders. While the new Pact for the Future—approved by the United Nations during the September 2024 Summit of the Future—focuses on ensuring that the remaining 2.6 billion unconnected individuals obtain internet access, it is critical that stakeholders also pay attention to disconnected citizens.[191] If the consequences of shutdowns and the livelihoods of disconnected individuals are not recognized, well-intentioned efforts may just entail pouring water into a leaking vessel while assuming the world is on track.

08

"America First" Meets "AI First": Insights from DOGE

Steven Feldstein and McKenzie Carrier

With stunning momentum, the Donald Trump administration has initiated a deep-reaching effort to remake the U.S. government. It has dismantled long-standing government institutions, ordered mass layoffs of civil service workers, and instituted steep funding cuts across multiple sectors.

The instrument behind this institutional upheaval is the Department of Government Efficiency (DOGE). Conceived of by tech billionaire Elon Musk, DOGE is an advisory entity created by executive order at the outset of Trump's tenure. The boundaries of its influence are nebulous, and its mandate is ill-defined beyond the general notion of achieving greater efficiency in government operations.[192] In its quest to achieve this aim, DOGE is undertaking a more radical experiment—using artificial intelligence (AI) tools to supercharge the remaking of the U.S. government. Unrestrained by any clear limits on its powers, DOGE has been inserting itself across government institutions, ordering massive, invasive changes, and strong-arming any opposition to its demands.

Much of DOGE's activity is shrouded in opacity—the product of purposeful efforts to withhold information and stonewall legislative and public inquiries.[193] Nonetheless, DOGE already provides a glimpse into how AI technologies can distort governance and offers a chilling lesson for citizens in other countries about the destructive impact of powerful technologies deployed in the service of an anti-institutionalist and illiberal political agenda.

DOGE's and MAGA's Shared Ideology

It could be easy to dismiss DOGE as an instrument within the Trump administration's broader conservative agenda. But even as DOGE serves the Make America Great Again

(MAGA) movement's purposes, Musk and his team have brought their own set of motivations to Trump's remaking of the federal government.

DOGE is rooted in a techno-libertarian mindset that fundamentally believes that societies can operate better if freed from bureaucratic encumbrances.[194] The idea is not to replace one form of government power with another. Rather, the goal is to remove government restrictions as much as possible by replacing bureaucracy with machines, using algorithms and computer analysis to make rapid decisions, eliminating unnecessary regulatory barriers that hinder innovation, and promoting economic and individual liberty while scaling down human involvement to the absolute minimum.

MAGA takes a different approach. Its aim is not to free society from the government. Rather, it is to maximize executive power in service of conservative values.[195] Elite institutions should be dismantled, immigrants deported, political opponents punished, and the economy rebooted in a nationalistic and protectionist direction. (This latter aspect is antithetical to techno-libertarians and explains why in the midst of Trump's global tariff war, Musk disparaged Peter Navarro, Trump's top trade adviser, as "dumber than a sack of bricks" and called for "zero tariffs" between the United States and Europe.)[196]

The composition of DOGE's staffing reflects these distinctive camps.[197] One grouping consists of first term Trump officials and conservative lawyers deeply rooted in the MAGA agenda. They include individuals such as DOGE spokesperson Katie Miller, who, along with her husband Stephen Miller, are reportedly viewed inside Trump's inner circle "as glorified babysitters for Musk, tasked with ensuring he stays within bounds."[198] Silicon Valley figures comprise a second faction, including tech leaders, engineers, and financiers with close ties to X (formerly Twitter) and SpaceX. They have little history with the MAGA camp; instead, their involvement reflects DOGE's techno-libertarian underpinnings and the centrality of Musk's leadership.

Despite these distinctions, MAGA and DOGE overlap on many of their aims. Moreover, their deregulatory agenda is not new. Long before Trump, U.S. conservatives had formulated a right-wing agenda that hinged on slashing government agencies and curbing regulations. Trump has been a willing enabler of these ideas. At the beginning of his first term—when he promised to "drain the swamp" and kicked off a multi-month hiring freeze on federal employees—his hostility to the bureaucracy knew few bounds.[199] Later on, he dismantled institutional guardrails, demeaned the federal workforce, and used his position to enrich himself, while undermining institutional checks on his power.[200] He is following the same playbook the second time around—handing out prominent positions to political allies while ensuring that his family members reap financial rewards from the presidency.[201]

Trump has also initiated an even more sweeping deregulation agenda. The DOGE apparatus and Silicon Valley's technology have emerged as ideal instruments for implementing this vision. As Eryk Salvaggio describes in Tech Policy Press, "shifting the conversation to the technical is a way of locking policymakers and the public out of decisions and shifting that

power to the code they write."[202] By crafting a narrative that links AI technologies with greater governmental efficiency, DOGE has cleared the path for the MAGA team to run roughshod over concerns about security, privacy, and democratic accountability in favor of speed and disruption, and ultimately regulatory dismantlement.

Reports have emerged about DOGE employees feeding data on employees, civilians, and funding into AI systems for analysis to make decisions about government staffing cuts and funding.[203] Musk-affiliated political appointees are pushing to develop AI "coding agents" to automate processes such as agency finances.[204] Government agencies are reportedly using AI tools to "catch and revoke" the visas of foreign nationals who appear to support Hamas, a dramatic expansion in the machine-enabled policing of conduct and speech.[205]

These efforts reflect an emergent reality: the symbiosis between Musk's "AI-first strategy" and Trump's MAGA agenda.[206] While DOGE's tech-based dismantlement strategy appears unprecedented, this is not the first time that Musk has attempted to radically remake an organization via the deployment of powerful technologies. His experience transforming X illustrates the stakes involved.

Lessons from Twitter

In 2022, Musk sent a text message to then Twitter CEO Parag Agrawal. It read: "What did you get done this week?"[207] The message came as Musk maneuvered to join the company's board and amid a clash with Agrawal over Musk's criticisms of Twitter's operations. Just days later, Musk purchased Twitter, assumed a leadership role, and set the ball rolling for the platform's complete overhaul.

Three years later, on February 22, 2025, federal workers received an email from the U.S. Office of Personnel Management (OPM), titled simply: "What did you do last week?" The email demanded that federal workers send OPM five bullet points summarizing their accomplishments by the following Monday, or risk being fired. Musk initially warned on X that failure to respond would "be taken as a resignation."[208]

This rhetorical echo was not the only parallel between Musk's reorganization of X and the current DOGE context. After Musk completed his purchase of the company, he set out to cut its workforce. In short order, he laid off nearly 80 percent of X's 7,500 employees.[209] He warned the remaining staff that their employment was contingent on their "hardcore" participation in the company.[210] These instructions were conveyed in an email titled, "A Fork in the Road," the same subject line used in an OPM email three years later to encourage federal workers to resign from the government.[211] X reeled in the aftermath of these changes. Fired individuals sued, some remaining workers quit, and "the platform suffered numerous major outages and technical glitches."[212] It became a shell of its former self—its ad revenue fell over 55 percent between 2022 and 2023, it had lost 23 percent of its U.S. users by February 2024, and by October 2024, its stock valuation had plummeted to almost 80 percent of its

value when Musk purchased it.[213] (Its value has risen in 2025 due to Musk's pivot to AI, but it remains to be seen whether its value will hold.)

Musk's management of X reflected his belief that human oversight could be eliminated from automated tools with little drop-off in productivity and huge increases in efficiency. It was a gamble he was happy to take even if there were setbacks along the way. In late 2022, Ella Irwin—Twitter's vice president of trust and safety at the time—told the public that the company would prioritize automated content moderation.[214] She emphasized that Musk believed the company had hindered itself by relying on people and that it would reduce manual reviewing processes in favor of machine-based ones. In the ensuing years, X leaned heavily on AI systems for content moderation, but the outcomes were poor. As programs, rules, and staff dedicated to preventing violent speech and misinformation were purged, the company saw marked declines in enforcement actions against hateful speech.[215] Concerns grew about the error-prone nature of X's automated reviewers and their potential to produce biased results. Instead of changing course, Musk doubled down on AI tools. He incorporated his xAI chatbot "Grok" into the X platform, adding a direct link to allow users to conduct queries.[216] While Grok's generation of vulgar, political, or violent outputs proliferated, Musk stayed committed to the AI pivot, treating X as "a private testing ground for his AI ambition."[217]

There was also another dynamic at play. Take, for example, Musk's firing of company staff responsible for overseeing global content moderation and his dismantling of the Trust and Safety Council independent advisory group, which monitored hate speech and harassment on the platform.[218] Theodora Skeadas, who co-managed the council, told us that Musk's actions demonstrated a "lack of respect for human staffing."[219] She outlined how the changes to X undermined workers' "capacity to do work and entirely ended programs," with particularly harmful consequences for "marginalized political groups" and "civic integrity" around elections. And she described how Musk's belief that "fewer people make for more efficient systems and processes," as well as his demands for total loyalty, cultivated a "culture of intimidation and fear" within the company. DOGE, she reflected, is "absolutely a parallel" to X in its approach to staffing. For Musk, relentlessly pursuing cost-efficiency was a far greater priority than ensuring his products operated in an ethical or trustworthy manner.

Finally, Musk's leadership at X embodied his commitment to Silicon Valley's "move fast and break things" mentality. The phrase—stemming from a 2012 Mark Zuckerberg letter—champions the idea that the speed necessary for successful innovation inherently comes at the cost of breaking things along the way.[220] This concept, often linked with the process of "creative destruction," in which obsolete predecessors are dismantled in order to build from the ground up, underpinned Musk's management of his other companies.[221] When SpaceX experienced one failed launch after another in the firm's early days, Musk pushed hard to continue despite the safety risks and costs. When glitches were uncovered in Tesla's Autopilot system—resulting in at least thirteen fatal crashes—Musk was dismissive, saying he had a "moral obligation to deploy it even though you're going to get sued and blamed by a lot of people."[222] Likewise, as he reshaped X, the technical failures, operational disruptions, and backlash resulting from his widespread terminations and impractical

expectations—such as demanding the closure of an entire data center in mere months—appeared to confirm his inclination to pursue reckless change regardless of the consequences.[223]

How Is DOGE's Agenda Playing Out?

Based on Musk's stewardship of X, what can be expected from DOGE? First, Musk's team has leaned hard into Silicon Valley's creative destruction mantra in its bid to remake the federal government. Examples of this are manifest. Just as Musk purged X of most of its employees, he has been driving personnel and funding cuts throughout the federal bureaucracy. In the first months after Trump's inauguration, DOGE led efforts to institute "zero based budgeting" throughout the government, proposing to take all spending to zero and then rebuild from the ground up.[224] Under DOGE's guidance, Trump froze trillions of dollars in grants and loans, dismantled key departments and agencies, and fired thousands of workers, from probationary employees to inspectors general and senior military attorneys.[225]

These efforts have relied heavily on technological tools. At the Department of the Treasury, for example, workers are reportedly using AI filters to block grant proposals that include terminology related to diversity, equity, and inclusion (DEI).[226] The U.S. Army is deploying the "CamoGPT" AI tool to review materials for DEI-related language as it seeks to purge this content.[227] But DOGE has used AI to make far more complex and high-stakes decisions as well. At the Department of Education, the DOGE team has reportedly fed sensitive data into AI systems to make choices about which programs to slash.[228] (DOGE staff reportedly uploaded Education Department reports into its AI system and asked the algorithm to flag "inefficiencies" that were then incorporated into proposals for reducing staffing and funding.)[229] Tasking AI with such subjective tasks is unproven and risky. Not only is AI software liable to produce unpredictable errors and biased results, but these factors are compounded by DOGE's haste to generate results and its willingness to flout guardrails and established procedures.

Similar to X, DOGE's upheaval is also creating significant turbulence with few meaningful results. One former Pentagon official describing DOGE's wider involvement in the Defense Department said, "They're not really using AI, they're not really driving efficiency. What they're doing is smashing everything."[230] As a result, regular tasks require more time, eroding productivity. In the meantime, DOGE is saddling civil servants with inconsequential administrative requirements. "These new directives are not only wasting government manpower and taxpayer dollars. They're also resulting in worse services for Americans," writes Catherine Rampell for the Washington Post.[231] A good case in point is the Social Security Administration (SSA), where Trump's firing of over 12 percent of the agency's staff has sent it into a free fall.[232] Its phone lines have experienced multi-hour wait times, frequent website crashes have prevented Americans from accessing their accounts, and spending freezes have deprived the remaining workers of basic office supplies. Similar reports of beleaguered and confused operations have emerged across the government, including in the Internal Revenue Service (IRS) and the Bureau of Land Management.

As DOGE gets deeper into its dismantlement of the U.S. government, the second phase of its strategy is coming into view. Once again, Musk appears to be borrowing from his X playbook by laying the groundwork for the mass automation of scores of governmental functions previously carried out by civil servants. In a recent interview with Senator Ted Cruz, he zeroed in on the "source code" as the essential foundation of the state.[233] "Well, the government is run by computers. So you've got essentially several hundred computers that effectively run the government," Musk told him. "Because all you're doing is asking a human who will then ask another human or ask another human, and finally, usually, ask some contractor who will ask another contractor to do a query on the computer." To be sure, AI technology already plays a role in federal processes. But these tools have largely been confined to basic functions, such as using chatbots to expedite agencies' data analysis or help local governments navigate regulations.[234] Musk's vision of automation is far starker: cut human-to-human interactions to the bone and replace what he believes are redundant civil servants with AI-powered computers.

One government official told the Washington Post it may be that the "end goal is replacing the human workforce with machines" altogether.[235] Or as New Yorker writer Kyle Chayka argues, while "government run by people is cautious and slow by design," this DOGE "machine-automated version will be fast and ruthless, reducing the need for either human labor or human decision-making."[236]

Take, for instance, the General Services Administration (GSA), where Thomas Shedd, a former Tesla engineer, was installed to run the Technology Transformation Services division. He is already implementing plans to use coding agents to automate the GSA's analysis and finance functions. But Shedd aspires for more. GSA reportedly aims to expand its AI chatbot software, "GSAi," to automate functions across other federal agencies.[237] As one GSA employee suggests, the program could be "used to plan large-scale government projects, inform reductions in force, or query centralized repositories of federal data."[238] In this vision, there is little room for human input—government functions are planned, crafted, and implemented from the ground up by machine intelligence.

It remains to be seen whether DOGE will accomplish its maximalist goals, but at a minimum, it will disrupt human judgment by instilling risky and illiberal uses of technological tools. In the area of surveillance, for example, Secretary of State Marco Rubio has launched a "Catch and Revoke" effort that draws upon AI tools to evaluate the social media accounts of student visa recipients.[239] Resulting assessments have already led to erroneous deportations and punitive measures against students. The administration has also expanded its digital monitoring program, a partnership with a private prison operator and digital surveillance company GEO Group, that currently tracks 180,000 migrants and has been instrumental in the arrests of hundreds of migrants.[240] Trump's team has also proven willing to turn its AI surveillance inwards to monitor its own employees. According to Reuters, Environmental Protection Agency supervisors received information that DOGE would use AI to surveil government staff, "looking for language in communications considered hostile to Trump or Musk."[241]

DOGE's methods will likely give rise to privacy abuses and data violations as well. At OPM, reports have emerged about DOGE workers gaining "the ability to delete, modify or export the personal information of millions of federal workers and federal job applicants."[242] At the Treasury Department and the SSA, DOGE has gained access to millions of citizens' highly sensitive data, leading a federal judge to block DOGE's access to SSA systems citing privacy law concerns.[243] And, in the IRS, DOGE has reportedly brought in operatives to develop a "mega API" to consolidate the agency's data into a single place.[244] (Presently, IRS data is compartmentalized into dozens of specialized systems, and workers are only granted access on a need-to-know basis.) One IRS worker warned that this integration would create an "open door controlled by Musk for all Americans' most sensitive information with none of the rules that normally secure that data."[245]

Conclusion

The Trump administration's use of DOGE as a battering ram to carry out its goal of rapidly remaking of the federal government is a cautionary tale for other countries. While recent reports suggest that Elon Musk is taking a step back from his DOGE responsibilities, there is little question that the initiative will continue. DOGE's short track record spotlights the tremendous risks involved. AI tools can easily be instrumentalized to destroy institutions, wipe out accountability, and enable corruption. Other democracies ought to take heed of the United States' failure to insulate itself against private business interests and unregulated technological ascendency.

For countries where there already is a predisposition to abuse the instruments of government power for political or personal gain, the DOGE project presents a master class in how powerful technological tools can be deployed—in a matter of weeks—to undermine an accountable bureaucracy and replace it with something far less functional or resistant to abuse. As leaders mirror the illiberal rhetoric and far right ideological agenda coming out of the White House, it is likely that DOGE's model will be replicated in other places and states.

The United States has long held itself out as a model of democratic norms. It is an advanced democracy and has a long history of adherence to the rule of law. But DOGE's techno-maximalist agenda is testing the limits of America's democracy.

09

Navigating AI Sovereignty in Africa: Resistance and Experimentation

Iginio Gagliardone

The concept of digital sovereignty has evolved significantly since the early days of the internet. Initially, it was associated with efforts to keep data outside a state's jurisdiction, such as censorship and firewalls, and protect the nation from external threats (what I call lock-out sovereignty).[246] The emergence of artificial intelligence (AI) has introduced a different paradigm—one in which states seek access to and control over data produced within their jurisdictions (lock-in sovereignty).[247] This shift is particularly relevant in Africa, where states are navigating the challenges of digital dependence while striving for technological autonomy.

This essay builds on and expands existing debates that have shaped the work of the Digital Democracy Network on digital sovereignty and AI sovereignty, including essays from Arindrajit Basu, Luca Belli, and myself on this topic.[248] In this piece, I examine new forms of resistance and experimentation that are emerging in Africa through two case studies: (1) Kenyan gig workers' challenge to Big Tech's labor exploitation, and (2) South Africa's evolving National Data and Cloud Policy.[249] These cases highlight pathways for resistance, negotiation, and adaptation in the pursuit of AI sovereignty, suggesting new possibilities for the cross-national networking of resources in the pursuit of an African—rather than a national vision—for the future of AI.

Contesting Digital Exploitation: The Case of Kenyan Gig Workers

Kenya has emerged as a critical site of resistance against tech giants' exploitative practices, with the country highlighting tensions between less powerful states that seek to enforce their

policies and norms and foreign companies that often take advantage of imbalances in the global labor market to their benefit. Companies such as Meta and OpenAI have outsourced AI training and content moderation to low-wage workers in Kenya and Uganda through third-party firms like Sama.[250]

For a long time, this practice of exploiting unequal distribution of labor, benefits, and responsibilities has gone unchallenged. This reality has been couched in powerful narratives that celebrate disruptive innovation, considered an inevitable feature of global capitalism, or justified through the creation of new concepts such as "impact sourcing."[251] Impact sourcing emerged in the late 2000s in opposition to traditional forms of aid. It was designed as a type of outsourcing that sought to give dignified work to the poorest people in ways that could guarantee them a living wage and possibly benefit their immediate communities.

This narrative was brought into question, however, when Daniel Motaung, a South African employee of Sama's office in Nairobi, began revealing the exploitative working conditions under which data workers in Kenya actually operated. In 2022, TIME's Billy Perrigo published a damning investigation based on Motaung's and other workers' testimonies.[252] It emerged that gig workers were reportedly paid as little as $1.50 per hour to review graphic and traumatic content, violating Sama's own purported commitment to pay living wages. These revelations received global attention, leading to discussions about fair compensation, mental health support, and labor rights in AI-related work.

Kenyan courts played a crucial role in challenging Big Tech's dominance. In a landmark ruling, the courts recognized Meta as the "true employer" of these content moderators, undermining the company's strategy of seeking immunity by outsourcing responsibility.[253] This ruling, the first of its kind in the world, could have game-changing consequences for Meta, preventing the company from claiming immunity for the dire working conditions of their moderators, just because this activity is outsourced to third parties. More broadly, it serves as a warning for other tech giants engaging in forms of exploitation of digital labor in the Global South. It challenges the idea that such companies can exploit imbalances of power and rights while facing no accountability for the dire conditions in which their outsourced employees have to operate. It also conveys an important message that highlights the plight of content moderators and data annotators in Africa and around the world, countering the process of their invisibilization and illustrating how those standing up for better working conditions and the recognition of basic rights, even against some of the world's most powerful companies, can find support in an expanding network of institutions, activists, and media.

Shifting Policies: South Africa's Data Sovereignty Debate

South Africa's evolving data sovereignty policy provides a different lens through which to understand Africa's halting efforts to navigate an independent, sovereign path toward AI. Initially, the country's 2021 Draft National Policy on Data and Cloud took a strong stance against Big Tech's data extraction practices.[254] The draft policy criticized the dominance of North American, European, and Chinese companies in Africa's cloud

infrastructure and proposed measures to ensure that data generated in South Africa remained under national control.

Three years later, when the final policy was released, these radical provisions had been significantly diluted. The final version emphasized the importance of cross-border data flows for economic growth and positioned South Africa as an attractive destination for foreign digital investments.[255] The shift from strong data localization policies to a more business friendly approach illustrates the challenges African states face in asserting data sovereignty while remaining integrated into the global economy. South African regulators reportedly faced opposition from tech giants, who leveraged their position of dominance to convince less powerful players to abandon attempts to set a different course.[256] As of 2025, South Africa is the only country in the region where all the major cloud service providers—IBM, Amazon, Microsoft, Google, Alibaba, Oracle, and Huawei—operate.[257]

While claiming greater state control over data stored on servers owned by foreign companies might have been an opportunity to cash in on the country's position as the continent's largest data warehouse, such an approach created risks. Other countries on the continent, such as Kenya, Nigeria, and Egypt, represent emerging markets with strong appeal to international tech firms; South Africa's initially proposed moves might have backfired and convinced companies to relocate elsewhere.

At a more fundamental level, the assertions of sovereignty advanced in South Africa's 2021 draft policy were built on a misleading understanding of what the government could actually do if it controlled the information produced in the country but that was stored by foreign tech companies. While it is encouraging to see how a policy document could be receptive of arguments made in critical media and AI scholarship—denouncing the concentration of tech power in the hands of a few multinational companies and their extractivist practices—the document advanced a narrow conception of the value of data. As technologist Gabriella Razzano writes in her analysis of the policy, the idea that simply gathering more data will lead to economic benefits does not recognize the microeconomic realities of data.[258] Owning more data offers scant guarantees that it will generate significant value when sold to third parties. It is the ability to use data, its resultant "network effects," that generates value. Because of economies of scale, it is mostly large firms in dominant positions that can extract value from feeding volumes of data into their own products and services.[259]

This reading highlights the limitations of using tactics that seek to beat tech giants at their own game rather than imagining different, creative strategies that better align with the distinct socio-technical conditions characterizing countries in the Global South. Many of these countries may be unable to compete in the frontier segments of AI innovation (such as the development of cutting-edge large-language models, or LLMs), but they could break new ground when it comes to national or cultural solutions, such as curating or unlocking datasets to allow new forms of imagination. (For a practical example, see the video and artwork "Noga Mo Jozi," produced by a collective of artists and architects at Wits University, which uses generative AI to build on artwork, rituals, and architecture derived from lost or partially destroyed Indigenous knowledge to create a dreamscape of a parallel Johannesburg.)[260]

Toward Networked Sovereignty

The pursuit of AI sovereignty in Africa is shaped by a complex interplay of resistance, adaptation, and strategic negotiation. The Kenyan case illustrates the potential for bottom-up mobilization to challenge Big Tech's labor practices, while South Africa's policy evolution underscores the difficulties governments face in asserting control over data without a clear and strategic understanding of how such data will be used.

Rather than adopting a purely protectionist or laissez-faire approach, African states could embrace new types of networked sovereignty to achieve AI autonomy. As Achille Mbembe explained, precolonial African political systems relied on fluid, networked governance structures that prioritized cooperation over rigid borders.[261] Applying this idea to AI sovereignty, African states could benefit from implementing collective approaches rather than engaging in nationalistic competition. Instead of creating fragmented, state-by-state policies, regional collaborations could help African nations leverage shared resources, including data, infrastructure, and talent.

By fostering regional partnerships, investing in AI education, and promoting fair labor practices, Africa can carve out a distinctive AI trajectory that prioritizes both technological advancement and social equity. The future of AI in Africa depends on whether governments, workers, and innovators can collectively navigate these challenges to build an inclusive and sovereign digital ecosystem.

10

The United States Should Re-embrace "Digital Solidarity"

Arindrajit Basu

Speaking to an audience of the world's leading cybersecurity professionals in May 2024 at a global information security conference in San Francisco, then U.S. secretary of state Antony Blinken announced that America's new "North Star" for digital and cyber foreign policy would be the principle of "digital solidarity."[262] Taking cues from a Lawfare essay by Pablo Chavez, the United States International Cyberspace and Digital Policy Strategy that was released at the RSA Conference framed digital solidarity as a "willingness to work together on share goals, help partners build capacity, and to provide mutual support" while recognizing the importance of using technology in a rights-respecting manner.[263]

Eight months and an election later, in February 2025, Vice President JD Vance struck an entirely different chord with his remarks at the Paris AI Summit.[264] While Vance's speech largely garnered attention because of its barefisted castigation of the European Union's regulatory approach, his speech also laid down the basic contours of U.S. cyber and digital foreign policy under the Donald Trump administration. In line with the administration's broader retreat from multilateral and multi-stakeholder cooperation writ large, Vance clearly signaled a shift away from digital solidarity. Straight off the block, he noted, "The United States of America is the leader in AI, and our administration plans to keep it that way," an individualistic comment that hinted at the administration's prioritization of competition over cooperation on questions of global AI governance. Like previous U.S. administrations, he highlighted the dangers of ideological bias in AI systems and their potential misuse by authoritarian countries (such as China), but rather than provide incentives for countries to partner with America, he issued a stark warning, saying, "partnering with them means chaining your nation to an authoritarian master that seeks to infiltrate, dig in, and seize your information infrastructure."

The speech envisaged a world driven by U.S. influence on account of its technological prowess and brute material power. The gloves are finally off. Engaging with the United States will happen only on America's terms and, as Ukrainian President Volodymyr Zelensky found out in the Oval Office, dissent will come with a price.[265]

At the end of the summit, the United States again grabbed headlines when it refused to sign the final declaration because of its references to regulation, again a clear body blow to international cooperation and a shift away from implementing the frame of digital solidarity.[266]

Why Digital Solidarity Works

When the Joe Biden administration first introduced the concept of digital solidarity, it marked a critical departure from prior approaches to cyber issues.[267] Fifteen years ago—as exemplified in Secretary of State Hillary Clinton's 2010 remarks on internet freedom—the United States took for granted that the pendulum of global internet governance would swing toward openness and liberal values.[268] Unsurprisingly, this vision never quite materialized. Instead of embracing openness, governments subsequently constrained internet access within their territorial boundaries through measures that restricted cross-border flows of data.[269] Nation-states weaponized the internet for electoral interference and informational manipulation purposes.[270] Domestic censorship measures also arose.[271] At the same time, geopolitical and ideological challengers like China increased their influence in the digital sphere, both through the development of global digital infrastructure and in shaping norm-making forums.[272]

The Biden administration's late 2024 refocusing of internet governance around the concept of digital solidarity offered a valuable conceptual frame to explain how U.S. thinking could evolve to respond positively and productively to the modern digital landscape. It compelled policymakers to go beyond the "democracies versus autocracies" pitch and accept that America's vision of cyberspace governance would not be adopted by all countries.[273] It was a useful way for the United States to build a larger coalition of countries against China by signaling that the United States was not coming to the table with a rigid and ideological vision of the internet but rather was willing to work on select issues, such as cybersecurity standards, secure supply chains, and capacity building, with different countries.

Just because the Trump administration is tacking in a new direction does not mean it cannot incorporate elements of the digital solidarity agenda that overlap with its own priorities. The administration should consider supporting two areas of digital policymaking: offering better and cheaper alternatives to China's products that also protect digital rights in their design; and using international institutions to shape the rules and guardrails for various technologies.

Reframing Digital Solidarity for the Trump Administration

First, as Vance articulated in Paris, a key goal for the United States is to counter China's influence among developing countries. As such, it would be sensible for the Trump administration to pursue initiatives that resonate internationally while also advancing America's core interests. Empirical research shows that the developing world's approach toward partnerships with advanced economies is pragmatically driven by domestic interests, security stakes, and developmental needs, rather than ideological or geopolitical alignment.[274] For example, India was quite comfortable acquiring information and communication technology (ICT) products from Chinese tech giant Huawei before a physical conflict occurred between Chinese and Indian soldiers on their disputed border. This caused India to reassess its strategy toward Chinese tech products and restrict Chinese applications and equipment from its core technological periphery.[275] Similarly, in Southeast Asia, Huawei leverages its capacity-building efforts and the cost effectiveness of its products to retain a significant presence in the region despite territorial disputes over the South China Sea.[276] While there are concerns over Chinese surveillance, policymakers and the general public in countries like Indonesia feel strongly that the Five Eyes are no better on this front.[277]

Amid great power competition, the overriding interest of emerging powers is to acquire necessary infrastructure, human resources, and capital from countries across the ideological spectrum based on quality, cost effectiveness, and geopolitical risk.[278] The implication is that to compete with China, at the bare minimum, the United States must provide better and cheaper alternatives that do not undermine digital rights.

America's efforts to promote the Open Radio Access Network (O-RAN) is a good illustration.[279] O-RAN is a non-proprietary telecommunications networking system that acts as an alternative to Huawei's closed models. U.S. diplomacy has focused on partnering with and providing financial resources to universities, government departments, and telecom companies in developing countries such as India, Indonesia, and the Philippines to adopt O-RAN.[280] Openness is a value that developing countries have long prioritized in building and deploying technologies. However, the jury is still out on whether O-RAN can fulfill its original vision. Some experts argue that O-RAN has underperformed and failed to make a dent in Chinese vendors' 5G market share.[281] Others maintain that O-RAN is technically sound and could become commercially viable once 6G is rolled out.[282] In short, O-RAN is an intriguing option that has made real efforts to account for and engage with the interests of the developing world. Rather than pursue coercion or one-off transactions, the Trump administration could adopt and expand upon this model, identifying rights-respecting technological solutions that offer an attractive value proposition to third countries and investing in them to drive a wedge against China's efforts.

Second, before the Trump administration fully disengages from international organizations and multilateral frameworks, it should carefully weigh the consequences of doing so. Within a rapidly evolving and contested international order, working through international institutions to set common rules of the road on the governance of cyberspace reinforces America's

interests. Trump's retreat from global governance institutions and withdrawal of funding to organizations working on digital rights and democracy issues only enables adversaries to further an alternate state-centric vision for the internet.[283] The United States would be better served continuing to find common ground with other countries and establishing technology guardrails to address global challenges, while endorsing and sustaining its own vision of the internet.

Under Biden, U.S. officials led efforts to forge consensus on global digital governance anchored by principles of fairness, accountability, transparency, safety and security, data privacy, and human oversight.[284] For instance, in 2024, the UN General Assembly adopted by consensus a U.S.-brokered resolution on forging "safe, secure and trustworthy" artificial intelligence (AI).[285] The resolution addressed not only common safeguards for AI but also spoke to closing digital divides and developing data governance—themes that appeal to developing countries.

While it is too early to make an informed assessment of the Trump administration's technology foreign policy doctrine, early signs very clearly suggest that it does not believe in the joint setting of norms and standards through multilateral processes, instead prioritizing deals-based mercantilism.[286] In the technology sphere and otherwise, this would be harmful to America's reputation and interests in the long-run.

A Word of Hope

Even if the Trump administration abandons the principles of digital solidarity, other countries must continue to respect and celebrate networks and coalitions of civil society actors who support, engage with, and demonstrate solidarity with the work of their peers worldwide. The #KeepItOn coalition coordinated by the nongovernmental organization Access Now, for example, works with civil society groups, media, and lawyers around the world to challenge internet shutdowns through litigation and raising public awareness.[287] Civil society organizations around the world, including Human Rights Watch and Amnesty International, have collaborated to resist the deployment of facial recognition technologies in public spaces to conduct surveillance.[288] Carnegie's Digital Democracy Network also provides a platform for individuals to engage with scholars and activists from other parts of the world and apply lessons learned to their own research and advocacy.

Digital solidarity through such transnational coalitions fosters mutual understanding, support, and information exchange in the service of shared goals. Even if governments neglect this vision, actors in civil society and academia should continue to build these bridges.

About the Authors

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.

McKenzie Carrier is a James C. Gaither Junior Fellow in the Democracy, Conflict, and Governance Program.

Steven Feldstein is a senior fellow at the Carnegie Endowment for International Peace in the Democracy, Conflict, and Governance Program. His research focuses on technology and geopolitics, U.S. foreign policy, and the global context for democracy. Feldstein is also the author of The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance (Oxford, 2021).

Iginio Gagliardone is an associate professor in media and communication at the University of the Witwatersrand in South Africa and an associate research fellow in new media and human rights in the Programme in Comparative Media Law and Policy at the University of Oxford.

Dean Jackson is principal of Public Circle Research & Consulting and a specialist in democracy, media, and technology. Among other positions, he was previously a project manager of the Influence Operations Researchers' Guild at the Carnegie Endowment for International Peace.

Lillian Nalwoga is a technology researcher and advocate interested in promoting and advancing the appropriate use of ICT for empowerment and development. She works as a program manager at the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) and is a co-founder and past president of the Internet Society Uganda Chapter.

Jonathan Corpus Ong is an associate professor of communication at the University of Massachusetts at Amherst and currently a research fellow at Harvard University's Shorestein Center.

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.

'Gbenga Sesan is the executive director of Paradigm Initiative, a pan-African social enterprise working on digital inclusion and digital rights, with offices in Cameroon, Kenya, Nigeria, Senegal, Zambia, and Zimbabwe.

Janjira Sombatpoonsiri is a research fellow at the German Institute for Global and Area Studies in Hamburg and an assistant professor at Chulalongkorn University, Thailand.

H. Akin Unver is an associate professor of international relations at Ozyegin University in Istanbul and the scientific coordinator for an EU grant on "Detecting and Countering Information Suppression from A Transnational Perspective."

Notes

Introduction

1 J.D. Vance, "Remarks by the Vice President at the Artificial Intelligence Action Summit in Paris, France," speech, American Presidency Project, February 11, 2025, https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france.

2 "Building Digital Solidarity: The United States International Cyberspace & Digital Policy Strategy," U.S. Department of State, May 6, 2024, https://www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy/.

3 Amber Sinha, "Trump 2.0 and the Emergence of Tech Policy as a Tool in Global Realpolitik." Tech Policy Press, April 30, 2025, https://www.techpolicy.press/trump-2-0-and-the-emergence-of-tech-policy-as-a-tool-in-global-realpolitik/.

4 "China is willing to share achievements in AI, vice premier says at Paris summit," Reuters, February 11, 2025, https://www.reuters.com/technology/artificial-intelligence/china-is-willing-share-achievements-ai-vice-premier-says-paris-summit-2025-02-11/.

5 Victor Cha, "How to Stop Chinese Coercion," *Foreign Affairs*, December 14, 2022, https://www.foreignaffairs.com/world/how-stop-china-coercion-collective-resilience-victor-cha; Kim Jae-heun, "Lotte to pull out of China, focus on Southeast Asia," *Korea Times*, May 23, 2022, https://www.koreatimes.co.kr/business/companies/20220523/lotte-to-pull-out-of-china-focus-on-southeast-asia; Drew Hinshaw, Joe Parkinson, and Aruna Viswanatha, "Inside the Secret Prisoner Swap That Splintered the U.S. and China," *Wall Street Journal*, October 27, 2022, https://www.wsj.com/articles/huawei-china-meng-kovrig-spavor-prisoner-swap-11666877779?mod=article_inline.

6 Andrew Sullivan, "A Fragmented Internet Is A Threat To The Future Of Global Business," *Forbes*, July 10, 2023, https://www.forbes.com/councils/forbestechcouncil/2023/07/10/a-fragmented-internet-is-a-threat-to-the-future-of-global-business/.

Chapter 01

7 "Measuring digital development: Facts and Figures 2024," International Telecommunication Union, 2024, https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-4/.

8 "Availability Map," Starlink, accessed May 2025, https://www.starlink.com/gb/map.

9 Khadija Alam and Damilare Dosunmu, "Starlink is now cheaper than leading internet provider in some African countries," Rest of World, January 10, 2025, https://restofworld.org/2025/starlink-cheaper-internet-africa/.

10 Joseph-Albert Kuuire, "Average Starlink Prices Across All African Countries," Tech Labari, September 10, 2024, https://techlabari.com/average-starlink-prices-across-all-african-countries/.

11 "Starlink Specifications," Starlink, accessed May 2025, https://www.starlink.com/legal/documents/DOC-1470-99699-90?regionCode=US.

12 Nkosinathi Ndlovu, "Starlink 'sold out' in major African cities – here's why," TechCentral, February 6, 2025, https://techcentral.co.za/starlink-sold-out-major-african-cities/258879/#:~:text=In%20developed%20markets%20like%20the,analogy%20of%20how%20it%20works.

13 Ephraim Modise, "Months before Starlink's Zimbabwe launch, government warns against its 'unlicensed' use," TechCabal, September 1, 2023, https://techcabal.com/2023/09/01/starlink-use-zimbabwe/.

14 "SA users of Starlink will be cut off at the end of the month," AfricaNews, August 13, 2024, https://www.africanews.com/2024/04/16/sa-users-of-starlink-will-be-cut-off-at-the-end-of-the-month//.

15 Mustapha Iderawumi, "Starlink's Internet Revolution: Becoming Kenya's 8th Largest ISP in Record Time," Space in Africa, January 24, 2025, https://spaceinafrica.com/2025/01/24/starlinks-internet-revolution-becoming-kenyas-8th-largest-isp-in-record-time/.

16 "Kenya Scraps 30% Local Equity Rule for ICT Firms," Njaga & Co. Advocates, July 24, 2023, https://njagaadvocates.com/kenya-scraps-30-local-equity-rule-for-ict-firms/.

17 "Kenya Removes the 30 per cent local shareholding requirement in the ICT Sector," UN Trade and Development, August 22, 2023, https://investmentpolicy.unctad.org/investment-policy-monitor/measures/4425/kenya-removes-the-30-per.

18 Aaron Ross, "Kenya›s Safaricom urges new requirements for satellite providers like Starlink," Reuters, August 23, 2024, https://www.reuters.com/business/media-telecom/kenyas-safaricom-urges-new-requirements-satellite-providers-like-starlink-2024-08-23/.

19 "Kenya's telecom regulator proposes 800% increase in satellite ISP licensing fees," Diplo, January 9, 2025, https://www.diplomacy.edu/updates/kenyas-telecom-regulator-proposes-800-increase-in-satellite-isp-licensing-fees/#:~:text=Kenya›s%20Communications%20Authority%20(CA)%20has,of%200.4%25%20of%20gross%20turnover.

20 Nixon Kanali, "Kenya proposes 10x fee increase for satellite ISPs," ITWeb Africa, January 9, 2025, https://itweb.africa/content/DZQ587V8YxVqzXy2.

21 Matshepo Sehloho, "Starlink doubles market share in Kenya, launches ground station," Connecting Africa, January 28, 2025, https://www.connectingafrica.com/connectivity/starlink-doubles-market-share-in-kenya-launches-ground-station; Michael Kan, "What Is a Starlink POP? How Ground Stations Improve Latency, Capacity," *PC Mag*, January 21, 2025, https://www.pcmag.com/news/what-is-a-starlink-pop-how-ground-stations-improve-latency-capacity.

22 "Which African countries have a data protection law?" Data Protection Africa, November 14, 2023, https://dataprotection.africa/which-african-countries-have-a-data-protection-law/.

23 "Privacy Policy," Starlink, last updated May 1, 2023, https://www.starlink.com/legal/documents/DOC-1000-41799-67; "Starlink Halts Service in Zimbabwe at Regulatory Request," ZimLiving, September 12, 2024, https://www.zimliving.co.zw/articles/starlink-halts-service-in-zimbabwe-at-regulatory-request.

24 "Which Way for Data Localisation in Africa?" CIPESA, November 2022, https://cipesa.org/download/briefs/Which_Way_for_Data_Localisation_in_Africa___Brief.pdf.

25 Joey Roulette and Marisa Taylor, "Musk›s SpaceX is building spy satellite network for US intelligence agency, sources say," Reuters, March 16, 2024, https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16/.

26 Tony Roberts et al., "Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia," Institute of Development Studies, September 24, 2023, https://opendocs.ids.ac.uk/articles/online_resource/Mapping_the_Supply_of_Surveillance_Technologies_to_Africa_Case_Studies_from_Nigeria_Ghana_Morocco_Malawi_and_Zambia/26431414.

27 Nathaniel Allen and Matthew La Lime, "How digital espionage tools exacerbate authoritarianism across Africa," Brookings, November 19, 2021, https://www.brookings.edu/articles/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/.

28 "Starlink will have surveillance capabilities in Bangladesh, can be shut down at any time," *Financial Express*, March 27, 2025, https://thefinancialexpress.com.bd/national/starlink-will-have-surveillance-capabilities-in-bangladesh-can-be-shut-down-at-any-time#google_vignette.

29 "Zimbabwe: Events of 2024," Human Rights Watch, 2025, https://www.hrw.org/world-report/2025/country-chapters/zimbabwe.

30 "President Mnangagwa Misled World, Starlink Not Yet Licenced," *Zimbabwean*, May 26, 2024, https://www.thezimbabwean.co/2024/05/president-mnangagwa-misled-world-starlink-not-yet-licenced/#google_vignette.

31 "Zimbabwe: Freedom on the Net 2024," Freedom House, 2024, https://freedomhouse.org/country/zimbabwe/freedom-net/2024#footnote4_wzdF38ogUPjf1Tr9zd4R4rTEnasvCknls0O05tC26xM_aQci00O5Jwvr.

32 Jason Warner and Toyosi Ajibade, "Navigating Digital Sovereignty and its Impact on the Internet," Internet Society, December 2022, https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf.

33 "China's Smart Cities in Africa: Should the United States Be Concerned?" CSIS, November 18, 2024, https://www.csis.org/analysis/chinas-smart-cities-africa-should-united-states-be-concerned.

34 Tom Barrett, "Looking to the skies: The importance of satellite cybersecurity," United States Studies Centre, November 11, 2024, https://www.ussc.edu.au/the-importance-of-satellite-cybersecurity.

35 "Overview," Cybersecurity Multi-Donor Trust Fund, accessed May 2025, https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview.

36 "Global Cybersecurity Index 2024," International Telecommunication Union, 2024, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.

37 "African Union Convention on Cyber Security and Personal Data Collection," African Union, 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

38 "World map of encryption laws and policies," Global Partners Digital, accessed May 2025, https://www.gp-digital.org/world-map-of-encryption/; Elton Chang, "Starlink's Network Security and Privacy," TelecomWorld101, January 7, 2025, https://telecomworld101.com/starlinks-network-security-and-privacy/.

39 Khanyisile Ngcobo, "Racially charged row between Musk and South Africa over Starlink," BBC, April 16, 2025, https://www.bbc.com/news/articles/cly3d8gd8mno.

40 Christian Davenport and Joseph Menn, "Musk refused to allow Ukraine's military to use Starlink to attack Russian fleet," *Washington Post*, September 11, 2023, https://www.washingtonpost.com/technology/2023/09/07/ukraine-starlink-musk-biography/.

Chapter 02

41 Dani Madrid-Morales, Herman Wasserman, and Saifuddin Ahmed, "The Geopolitics of Disinformation: Worldviews, Media Consumption and the Adoption of Global Strategic Disinformation Narratives," *International Journal of Public Opinion Research* 36, no.3 (2024), https://academic.oup.com/ijpor/article-abstract/36/3/edad042/7709016.

42 Jon Bateman and Dean Jackson, "Countering Disinformation Effectively: An Evidence-Based Policy Guide," Carnegie Endowment for International Peace, January 31, 2024, https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en; "GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem," U.S. Department of State, August 2020, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

43 Kamya Yadav et al., "What Makes an Influence Operation Malign?" Carnegie Endowment for International Peace, August 7, 2023, https://carnegieendowment.org/research/2023/08/what-makes-an-influence-operation-malign?lang=en; Filippo Menczer, "How foreign operations are manipulating social media to influence your views," The Conversation, October 8, 2024, https://theconversation.com/how-foreign-operations-are-manipulating-social-media-to-influence-your-views-240089; Hedvig Ördén and James Pamment, "What Is So Foreign About Foreign Influence Operations?" Carnegie Endowment for International Peace, January 26, 2021, https://carnegieendowment.org/research/2021/01/what-is-so-foreign-about-foreign-influence-operations?lang=en.

44 "Malign Foreign Influence," in "Final Report of the Select Committee to Investigate the January 6th Attack on the United States Capitol," H.R. Rep No. 117-663 (December 22, 2022), https://www.govinfo.gov/content/pkg/GPO-J6-REPORT/pdf/GPO-J6-REPORT-4-4.pdf; Donatienne Ruy, "Did Russia Influence Brexit?" CSIS, July 21, 2020, https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit; Nicolas Hénin, FIMI: Towards a European Redefinition of Foreign Interference," EU Disinfo Lab, April 7, 2023, https://www.disinfo.eu/publications/fimi-towards-a-european-redefinition-of-foreign-interference/.

45 Sarah N. Lynch, Andrew Goudsward, and Christopher Bing, "US charges employees of Russia›s RT network in crackdown on election influence efforts," Reuters, September 4, 2024, https://www.reuters.com/world/us/us-accuse-russia-effort-influence-2024-election-cnn-2024-09-04/.

46 "Chinese State-Linked Influence Operation Spamouflage Masquerades as U.S. Voters to Push Divisive Online Narratives Ahead of 2024 Election," Graphika, September 3, 2024, https://www.graphika.com/reports/the-americans.

47 Madrid-Morales, Wasserman, and Ahmed, "The Geopolitics of Disinformation: Worldviews, Media Consumption and the Adoption of Global Strategic Disinformation Narratives"; Julia Voo, "Driving Wedges: China's Disinformation Campaigns in the Asia-Pacific" in *Asia-Pacific Regional Security Assessment* (London: IISS, May 2024), https://www.iiss.org/publications/strategic-dossiers/asia-pacific-regional-security-assessment-2024/chapter-5/; Celina Realuyo, "The competition for influence in the Americas is now online," Atlantic Council, February 12, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-competition-for-influence-in-the-americas-is-now-online/.

48 Pauline Macaraeg, "How pro-China propaganda is seeded online in the Philippines," Rappler, November 1, 2023, https://www.rappler.com/newsbreak/investigative/ways-how-china-propaganda-seeded-online-philippines/; Gregory Winger, "China's Disinformation Campaign in the Philippines," *The Diplomat*, October 6, 2020, https://thediplomat.com/2020/10/chinas-disinformation-campaign-in-the-philippines/.

49 Olga Dror, "Weaponising Ho Chi Minh in Vietnamese Discourse on the War in Ukraine," Fulcrum, June 17, 2022, https://fulcrum.sg/weaponising-ho-chi-minh-in-vietnamese-discourse-on-the-war-in-ukraine/; Audrye Wong, "COVID-19 and China's information diplomacy in Southeast Asia," Brookings, September 3, 2020, https://www.brookings.edu/articles/covid-19-and-chinas-information-diplomacy-in-southeast-asia/; Darren Cheong, "Unpacking Russia's Twitter Disinformation Narratives in Southeast Asia," Fulcrum, April 8, 2022, https://fulcrum.sg/unpacking-russias-twitter-disinformation-narratives-in-southeast-asia/.

50 Derrick A. Paulo, "Trolls for hire in Philippines: The concealed political weapon used in a social media war," Channel News Asia, September 4, 2022, https://www.channelnewsasia.com/cna-insider/paid-troll-army-hire-philippines-social-media-elections-influencers-2917556.

51 Christina Chi, "Filipino influencers, troll farms tapped for pro-China narratives — study," *Philstar*, September 11, 2024, https://www.philstar.com/headlines/2024/09/11/2384510/filipino-influencers-troll-farms-tapped-pro-china-narratives-study.

52 Alvin A. Camba, "Countering China›s Information Manipulation A Framework for Understanding and Action," International Republican Institute, 2023, https://www.researchgate.net/profile/Alvin-Camba/publication/375185974_Countering_China%27s_Information_Manipulation_A_Framework_for_Understanding_and_Action/links/654334be3cc79d48c5c6a2bf/Countering-Chinas-Information-Manipulation-A-Framework-for-Understanding-and-Action.pdf.

53 "The South China Sea Arbitration (The Republic of Philippines v. The People›s Republic of China)," Permanent Court of Arbitration, 2016, https://pca-cpa.org/cn/cases/7/; Tom Phillips, Oliver Holmes, and Owen Bowcott, "Beijing rejects tribunal›s ruling in South China Sea case," *Guardian*, July 12, 2016, https://www.theguardian.com/world/2016/jul/12/philippines-wins-south-china-sea-case-against-china.

54 "Nexus of Manipulation: Anatomy of Influence Operations in the Philippines," Internews, August 12, 2024, https://internews.org/resource/nexus-of-manipulation-anatomy-of-influence-operations-in-the-philippines/; Macaraeg, "How pro-China propaganda is seeded online in the Philippines"; BC Han and Camille Elemia, "Beijing›s Global Media Influence 2022: Philippines," Freedom House, 2022, https://freedomhouse.org/country/philippines/beijings-global-media-influence/2022; Billy Begas, "Lawmakers worried about SMNI potential collab with China's TV network," Politiko, December 11, 2023, https://politiko.com.ph/2023/12/11/lawmakers-worried-about-smni-potential-collab-with-chinas-tv-network/politiko-lokal/.

55 "Nexus of Manipulation: Anatomy of Influence Operations in the Philippines," Internews.

56 "Philippines, China clashes trigger money-making disinformation," France 24, November 26, 2024, https://www.france24.com/en/live-news/20241126-philippines-china-clashes-trigger-money-making-disinformation.

57 Victor N. Roudometof, "Glocalization," Oxford Bibliographies, January 15, 2020, https://www.oxfordbibliographies.com/display/document/obo-9780199756841/obo-9780199756841-0241.xml.

58 Aries A. Aruga and Fatima Gaw, "Like, Subscribe and Vote: The Role of Political Influencers in the 2022 Philippine Elections and Beyond," Fulcrum, April 5, 2024, https://fulcrum.sg/like-subscribe-and-vote-the-role-of-political-influencers-in-the-2022-philippine-elections-and-beyond/.

59 Fatima Gaw et al., "Covert political campaigning: Mapping the scope, scale, and cost of cross-platform election influence operations," New Media & Society, January 12, 2025, https://journals.sagepub.com/doi/abs/10.1177/14614448241312191; Jinhyun Lee, "Duterte's 'Pivot to China' and the Influence of the Public," *Asia-Pacific Social Science Review* 20, no. 1 (2020): 53-65, https://www.dlsu.edu.ph/wp-content/uploads/pdf/research/journals/apssr/2020-March-vol20-1/6-dutertes-pivot-to-china-and-the-influence-of-the-public.pdf.

60 Sebastian Strangio, "Parsing the Philippines' 'Pivot' to China Under Rodrigo Duterte," *The Diplomat*, September 24, 2024, https://thediplomat.com/2024/09/parsing-the-philippines-pivot-to-china-under-rodrigo-duterte/; Macaraeg, "How pro-China propaganda is seeded online in the Philippines"; Christina Chi, "Anonymous accounts flood WPS discourse with 'CIA agent' accusations vs PCG spox," *Philstar*, December 4, 2023, https://www.philstar.com/headlines/2023/12/04/2316405/anonymous-accounts-flood-wps-discourse-cia-agent-accusations-vs-pcg-spox/amp/.

61 "VERA FILES FACT CHECK: Pro-Duterte blogger makes multiple inaccurate claims on West Philippine Sea, arbitral ruling," VERA Files, April 28, 2021, https://verafiles.org/articles/vera-files-fact-check-pro-duterte-blogger-makes-multiple-ina.

62 Aries A. Arugay, "Foreign Policy & Disinformation Narratives in the 2022 Philippine Election Campaign," *ISEAS Perspective* 59 (June 6, 2022), https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-59-foreign-policy-disinformation-narratives-in-the-2022-philippine-election-campaign-by-aries-a-arugay/.

63 Arugay, "Foreign Policy & Disinformation Narratives in the 2022 Philippine Election Campaign."

64 "Deepfake audio falsely portrays Marcos as confrontational," Indo-Pacific Defense Forum, May 12, 2024, https://ipdefenseforum.com/2024/05/deepfake-audio-falsely-portrays-marcos-as-confrontational/.

65 Julie M. Aurelio, "'Deepfake': PCO disowns clip of Marcos 'attack order' vs China," *Philippine Daily Inquirer*, April 25, 2024, https://globalnation.inquirer.net/233290/deepfake-pco-disowns-clip-of-marcos-attack-order-vs-china; "PCO to designate 'fact-check officers' in state media to fight fake news," Presidential Communications Office, September 9, 2024, https://pco.gov.ph/news_releases/pco-to-designate-fact-check-officers-in-state-media-to-fight-fake-news/.

66 Janjira Sombatpoonsiri, "Manipulating Civic Space: Cyber Trolling in Thailand and the Philippines," GIGA Focus no. 3 (June 2018), https://www.giga-hamburg.de/assets/pure/21580615/web_asien_2018_03_english.pdf.

67 Rebecca Ratcliffe, "Amnesty faces pressure to leave Thailand amid 'growing intolerance,'" *Guardian*, February 17, 2022, https://www.theguardian.com/world/2022/feb/17/amnesty-faces-pressure-to-leave-thailand-amid-growing-intolerance; "'ดร.เสรี' ซัด 'ลัทธิชังชาติ' ปลุกปั่นอ้างถูกจับเพราะ 'คิดต่าง' แท้จริง 'ชักน้ำเข้าลึก ชักศึกเข้าบ้าน' (Dr. Seri slams 'national hatred' for inciting people to be arrested for 'different thinking', in reality 'draws water deeper, invites war into the house')," *Siam Rath*, March 19, 2022, https://siamrath.co.th/n/332435.

68 Janjira Sombatpoonsiri, "Intersectional Powers of Digital Repression: How Activists are Digitally Watched, Charged, and Stigmatized in Thailand," *International Journal of Communication* 18 (2024): 1611-1633, https://ijoc.org/index.php/ijoc/article/view/21411/4526.

69 "'พิธา-ก้าวไกล' จิ๊กซอว์ตัวใหม่ Hybrid Warfare ของมะกันในอินโดแปซิฟิก ("Pita-Move Forward," the New Piece of the US's Hybrid Warfare Puzzle in the Indo-Pacific), MGR Online, May 13, 2023, https://mgronline.com/onlinesection/detail/9660000044395.

70 "Thai Constitutional Court dissolves election-winning Move Forward Party," Al Jazeera, August 7, 2024, https://www.aljazeera.com/news/2024/8/7/thai-constitutional-court-dissolves-progressive-move-forward-party.

71 Rebecca Ratcliffe, "The online hate campaign turning Indonesians against Rohingya refugees," *Guardian*, January 17, 2024, https://www.theguardian.com/world/2024/jan/18/the-online-hate-campaign-turning-indonesians-against-rohingya-refugees.

72 Muhammad Haziq Bin Jani, "Transnational Hate Speech and Disinformation: Anti-Rohingya Sentiments in Indonesia," RSIS, January 24, 2024, https://rsis.edu.sg/rsis-publication/idss/ip24008-transnational-hate-speech-and-disinformation-anti-rohingya-sentiments-in-indonesia/.

73 Benjamin Y. H. Loh and Sarah Ali, "Rhetorical Sympathy for the Palestinian Struggle in Malaysia and the Poignant Misuse of 'Zionism,'" *ISEAS Perspective*, January 22, 2024, https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2024-5-rhetorical-sympathy-for-the-palestinian-struggle-in-malaysia-and-the-poignant-misuse-of-zionism-by-benjamin-y-h-loh-and-sarah-ali/.

74 Chris Chaplin, "Rohingya, politics and disinformation in Indonesia," Indonesia at Melbourne, January 23, 2024, https://indonesiaatmelbourne.unimelb.edu.au/rohingya-politics-and-disinformation-in-indonesia/.

75 Jason Vincent A. Cabañes, "Digital Disinformation and the Imaginative Dimension of Communication," *Journalism and Mass Communication Quarterly* 97, no.2 (April 2020), https://journals.sagepub.com/doi/abs/10.1177/1077699020913799.

76 "A UN vote on Palestine underlines America's weakening clout," *Economist*, September 18, 2024, https://www.economist.com/international/2024/09/18/a-un-vote-on-palestine-underlines-americas-weakening-clout.

77 Shannon Teoh and Nirmal Ghosh, "Washington 'risks losing the street' in Muslim S-E Asia as Gaza war stirs anti-US sentiments," *Straits Times*, November 11, 2024, https://www.straitstimes.com/asia/se-asia/washington-risks-losing-the-street-in-muslim-s-e-asia-as-gaza-war-stirs-anti-us-sentiments.

78 "A UN vote on Palestine underlines America's weakening clout," Economist.

79 "Pro-Russian Narratives on the Israel-Hamas War in Indonesia on YouTube," Ukraine Crisis Media Center, May 31, 2024, https://uacrisis.org/en/pro-russian-narratives-on-the-israel-hamas-war-in-indonesia-on-youtube; Nataliya Vasilyeva, "Russian crackdown on Muslims fuels exodus to Daesh," *Arab News*, November 26, 2015, https://www.arabnews.com/node/840806/%7B%7B.

80 Sebastian Strangio, "Why Are Indonesian Netizens Expressing Support for Russia's Invasion of Ukraine?" *Diplomat*, March 9, 2022, https://thediplomat.com/2022/03/why-are-indonesian-netizens-expressing-support-for-russias-invasion-of-ukraine/.

81 Benjamin Y.H. Loh and Munira Mustaffa, "Social Media Discourse in Malaysia on the Russia-Ukraine Conflict: Rationales for Pro-Russia Sentiments," ISEAS Perspective, April 22, 2022, https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-41-social-media-discourse-in-malaysia-on-the-russia-ukraine-conflict-rationales-for-pro-russia-sentiments-by-benjamin-y-h-loh-and-munira-mustaffa/.

82 Janjira Sombatpoonsiri, "In Denial Against Democracy: Thailand's Royalists see Putin as a 'Decoloniser,'" Fulcrum, May 11, 2022, https://fulcrum.sg/in-denial-against-democracy-thailands-royalists-see-putin-as-a-decoloniser/.

83 Alicia Wanless and Michael Berk, "Participatory Propaganda: The Engagement of Audiences in the Spread of Persuasive Communications" in *Social Media and Social Order* (Berlin: De Gruyter, 2022), https://www.degruyterbrill.com/document/doi/10.2478/9788366675612-009/html?lang=en.

84 James Andrew Lewis, "Advice for Successful Influence Operations: Recruit the Discontented," CSIS, March 28, 2024, https://www.csis.org/blogs/working-papers/advice-successful-influence-operations-recruit-discontented.

Chapter 03

85 "GloTech," GloTech, accessed May 2025, https://glotechlab.net/.

86 Jonathan Corpus Ong et al., "Custom Built / Feito Sob Medida: Reforming Tech & Democracy Programs for the Global Majority," Global Technology for Social Justice Lab at UMass Amherst, 2024, https://glotechlab.net/wp-content/uploads/2024/10/custom-built-exec-summary-pre-final.pdf.

87 Mark Stencel, Erica Ryan, and Joel Luther, "Misinformation spreads, but fact-checking has leveled off," Duke Reporters' Lab, June 21, 2023, https://reporterslab.org/2023/06/21/misinformation-spreads-but-fact-checking-has-leveled-off/.

88 Jonathan Corpus Ong et al., "Parallel Public Spheres: Influence Operations in the 2022 Philippine Elections," Internews and Harvard Kennedy School Shorenstein Center, https://mediamanipulation.org/research/unmasking-influence-operations-in-the-philippines; Odanga Madung, "Platforms, Promises and Politics," Mozilla Foundation, February 27, 2024, https://www.mozillafoundation.org/en/campaigns/platforms-promises-and-politics/.

89 Robert A. Blair et al., "Interventions to Counter Misinformation: Lessons from the Global North and Applications to the Global South," USAID, archived September 10, 2024, Internet Archive, https://web.archive.org/web/20240910163028/https:/pdf.usaid.gov/pdf_docs/PA0215JW.pdf.

90 Patrick Fine, "USAID can't go it alone on localization," Brookings, February 5, 2024, https://www.brookings.edu/articles/usaid-cant-go-it-alone-on-localization/.

91 "Reevaluating and Realigning United States Foreign Aid," The White House, January 20, 2025, https://www.whitehouse.gov/presidential-actions/2025/01/reevaluating-and-realigning-united-states-foreign-aid/.

92 Paul Dans and Steven Groves, eds., "Mandate for Leadership: The Conservative Promise," The Heritage Foundation, 2023, archived October 26, 2023, DocumentCloud, https://www.documentcloud.org/documents/24088042-project-2025s-mandate-for-leadership-the-conservative-promise/; Chris Bing and Joel Schectman, "Pentagon ran secret anti-vax campaign to undermine China during pandemic," Reuters, June 14, 2024, https://www.reuters.com/investigates/special-report/usa-covid-propaganda/.

93 Nina Santos, "Why Do We Need to Discuss So-called 'Information Integrity'?" Tech Policy Press, March 4, 2024, https://www.techpolicy.press/why-do-we-need-to-discuss-socalled-information-integrity/.

Chapter 04

94 See also Luca Belli et al., "Courting AI: How Brazilian Courts are Using and Regulating AI," in Monika Zalnieriute and Agne Limante, *Cambridge Handbook of Courts and AI* (forthcoming).

95 Luis Felipe Salomão, "Artificial Intelligence: Technology Applied to Conflict Management within the Brazilian Judiciary," Fundação Getulio Vargas, 2022, https://repositorio.fgv.br/items/89149bfb-04df-4260-8a6c-6d5729cd622a; Luca Belli et al., "Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano (Cybersecurity: A Systemic Vision Towards a Regulatory Framework Proposal for a Digitally Sovereign Brazil)," Fundação Getulio Vargas, June 14, 2023, https://repositorio.fgv.br/items/4814c750-6b42-4d48-b8bb-302ce467b4ea; Apostolos Malatras and Georgia Dede, eds., "Artificial Intelligence Cybersecurity Challenges," *ENISA*, December 15, 2020, https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

96 This article adopts the definition of AI system offered by article 4 of the latest version of Brazilian Bill No. 2338/2023 on the development, promotion, ethical and responsible use of artificial intelligence based on the centrality of the human person, which is largely based on the definitions offered by the EU AI Act and the Organisation for Economic Co-operation and Development. See Stuart Russell, Karine Perset, and Marko Grobelnik, "Updates to the OECD's definition of an AI system explained," OECDA, November 29, 2023, https://oecd.ai/en/wonk/ai-system-definition-update.

97 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, May 25, 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4465501.

98 Belli et al., "Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano (Cybersecurity: A Systemic Vision Towards a Regulatory Framework Proposal for a Digitally Sovereign Brazil)"; Malatras and Dede, eds., "Artificial Intelligence Cybersecurity Challenges."

99 B. Geluvaraj, P. M. Satwik, and T. A. Ashok Kumar, "The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace," *International Conference on Computer Networks and Communication Technologies* 15 (2019), https://link.springer.com/chapter/10.1007/978-981-10-8681-6_67.

100 Ramanpreet Kaur, Dušan Gabrijelčič, and Tomaž Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion* 97 (September 2023), https://www.sciencedirect.com/science/article/pii/S1566253523001136.

101 "2Q24 Emerging Risk Report," Gartner, June 24, 2024, https://www.gartner.com/en/documents/5529395.

102 "Ransomware Attacks 2024: A Look Back at the Top Ransomware Headlines," Sanfor Technologies, January 19, 2025, https://www.sangfor.com/blog/cybersecurity/ransomware-attacks-2024-top-ransomware-headlines.

103 Syed Minhaj Ul Hassan Minhaj, "Study of Artificial Intelligence in Cyber Security and the Emerging Threat of AI-Driven Cyber Attacks and Challenge," *Journal of Aeronautical Materials* 43, no.1 (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4652028.

104 "Preparing for AI-enabled cyberattacks," MIT Technology Review, April 8, 2021, https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/.

105 Heather Chen and Kathleen Magramo, "Finance worker pays out $25 million after video call with deepfake 'chief financial officer'," CNN, February 4, 2024, https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html.

106 Lorenzo Pupillo et al., "Artificial Intelligence and Cybersecurity," Centre for European Policy Studies, May 2021, https://www.ceps.eu/wp-content/uploads/2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf.

107 Malatras and Dede, eds., "Artificial Intelligence Cybersecurity Challenges."

108 Most notably, in 2020, Brazil jumped up fifty-three positions, from seventy-first to eighteenth, in the Global Cybersecurity Index elaborated by the International Telecommunications Union. In the Americas region, Brazil reached the third position and is considered a "Tier 1—Role-modelling" country. See "Global Security Index 2024," International Telecommunication Union, 2024, https://www.itu.int/epublications/publication/global-cybersecurity-index-2024.

109 Belli et al., "Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano (Cybersecurity: A Systemic Vision Towards a Regulatory Framework Proposal for a Digitally Sovereign Brazil)."

110 The CNCiber is composed of representatives from thirteen ministries, the Brazilian Central Bank, the telecoms regulator, the Brazilian Internet Steering Committee, three representatives civil society, three private sector representatives, and three academic community representatives. See "Decreto Nº 11.856, de 26 de Dezembro de 2023 (Decree No. 11856, of December 26, 2023)," Diário Oficial da União, December 27, 2023, https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289#wrapper.

111 "Portaria Nº 6, de 9 de Fevereiro de 2024 (Ordinance No. 6, of February 9, 2024)," Diário Oficial da União, February 14, 2024, https://www.in.gov.br/en/web/dou/-/portaria-n-6-de-9-de-fevereiro-de-2024-542752145; " Professor Luca Belli appointed member of the new Brazilian Cybersecurity Committee," CyberBRICS, February 16, 2024, https://cyberbrics.info/professor-luca-belli-appointed-member-of-the-new-brazilian-cybersecurity-committee/.

112 Levy Teles, "'Câmara terá protagonismo na regulação da IA', diz presidente de comissão especial ('Chamber will play a leading role in regulating AI,' says president of special committee)," *Estadão*, April 24, 2025, https://www.estadao.com.br/politica/coluna-do-estadao/camara-tera-protagonismo-na-regulacao-da-ia-diz-presidente-de-comissao-especial/.

113 "Lei Nº 13.709, de 14 de Agosto de 2018 (Law No. 13,709, of August 14, 2018)," Presidência da República, August 14, 2018, https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

114 João Nakamura, "Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes por minuto, aponta estudo (Brazil is runner-up in cyber attacks, with 1,379 attacks per minute, study finds)," CNN Brasil, October 30, 2024, https://www.cnnbrasil.com.br/economia/negocios/brasil-e-vice-campeao-em-ataques-ciberneticos-com-1-379-golpes-por-minuto-aponta-estudo/; Luca Belli, "The largest personal data leakage in Brazilian history," Open Democracy, February 3, 2021, https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history/.

115 The ordinance was issued by the Secretariat of Digital Government of the Ministry of Management and Innovation in Public Services. See "Privacidade e Segurança (Privacy and Security)," Ministério da Gestão e da Inovação em Serviços Públicos, accessed May 2025, https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca.

116 "Auditoria constata falta de entidade responsável pela segurança cibernética nacional (Audit finds lack of entity responsible for national cybersecurity)," Tribunal de Contas da União, November 26, 2024, https://portal.tcu.gov.br/imprensa/noticias/auditoria-constata-falta-de-entidade-responsavel-pela-seguranca-cibernetica-nacional.

117 Such specification is utilized, for example, by the Chinese Cybersecurity Law and Data Security Law, which prescribe the adoption of specific measures to protect "important" or "core" data whose security is essential for the well-functioning of national critical infrastructure. See Luca Belli, "Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation," *African Journal of Information and Communication* 28 (2021), https://journals.assaf.org.za/index.php/ajic/article/view/12944.

118 Muhammad Fakhrul Safitra, Muharman Lubis, and Hanif Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," *Sustainability* 15, no.18 (2023), https://www.mdpi.com/2071-1050/15/18/13369.

119 "Disposições Preliminares (Preliminary Provisions)," Senado Federal, 2023, https://legis.senado.leg.br/sdleg-getter/documento?dm=9881643&ts=1738762541678&disposition=inline.

120 According to recital 61 of the EU AI Act, "Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation." In this respect, in December 2022, the European Commission adopted the "Draft standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence." See "Regulation (EU) 2024/1689 of the European Parliament and of the Council," European Union, June 13, 2024, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng; "Draft standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence," European Commission, May 12, 2022, https://ec.europa.eu/docsroom/documents/52376?locale=en.

121 Christine Galvagna, "Inclusive AI governance," Ada Lovelace Institute, March 30, 2023, https://www.adalovelaceinstitute.org/report/inclusive-ai-governance/.

Chapter 05

122 "Beyond Disinformation - What is FIMI?" European External Action Service, February 6, 2023, https://www.eeas.europa.eu/eeas/beyond-disinformation-what-fimi_en.

123 "1st EEAS Report on Foreign Information Manipulation and Interference Threats." European External Action Service, February 7, 2023, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en.

124 "1st EEAS Report on Foreign Information Manipulation and Interference Threats." European External Action Service.

125 "DISARM Red Framework," DISARM Foundation, accessed May 2025, https://www.disarm.foundation/framework; "opencti," OpenCTI-Platform, accessed May 2025, https://github.com/OpenCTI-Platform/opencti; "Introduction to STIX," STIX, last updated July 24, 2024, https://oasis-open.github.io/cti-documentation/stix/intro.html.

126 Hadley Newman, "Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM' (prepared in cooperation with Hybrid COE)," NATO Strategic Communications Centre of Excellence, November 29, 2022, https://stratcomcoe.org/publications/foreign-information-manipulation-and-interference-defence-standards-test-for-rapid-adoption-of-the-common-language-and-framework-disarm-prepared-in-cooperation-with-hybrid-coe/253.

127 "U.S., EU launch coordination mechanism against disinformation in Western Balkans," Federal Newswire, May 23, 2024, https://thefederalnewswire.com/stories/659508688-u-s-eu-launch-coordination-mechanism-against-disinformation-in-western-balkans.

128 Jacob Katz Cogna, ed., "The Department of State Announces Initiatives to Counter Foreign State Information Manipulation," *AJIL Contemporary Practice of the United States* 118, no.3 (July 2024): 533-539, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/department-of-state-announces-initiatives-to-counter-foreign-state-information-manipulation/FC0924C7866F4446525638491E071EED.

129 "Rapid Response Mechanism Canada: Global Affairs Canada," Government of Canada, last updated March 13, 2025, https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng.

130 "Welcome to DISARM," DISARM Framework Explorer, accessed May 2025, https://disarmframework.herokuapp.com/.

131 "Chapter 3 - International issues" in Senate Select Committee on Foreign Interference through Social Media, report, Parliament of Australia, August 2023, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_through_Social_Media/ForeignInterference47/Report/Chapter_3_-_International_issues; "Security and Defence Partnership between the European Union and Japan," European External Action Service, November 1, 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EU-Japan%20Security%20and%20Defence%20Partnership.pdf.

132 "EU DisinfoLab 2024 Annual Conference," EU Disinfo Lab, 2024, https://www.disinfo.eu/conference-2024/.

133 Evan Mealins, "What to know about Tenet Media, Tennessee company linked to Russian propagandists," Tennessean, September 4, 2024, https://www.tennessean.com/story/news/crime/2024/09/04/tenet-media-what-to-know-russian-election-interference/75077703007/; Steven Lee Myers, Ken Bensinger, and Jim Rutenberg, "Russia Secretly Worms Its Way Into America's Conservative Media," *New York Times*, September 7, 2024, https://www.nytimes.com/2024/09/07/business/media/russia-tenet-media-tim-pool.html.

134 Tim Mak, "NRA Was ‹Foreign Asset› To Russia Ahead of 2016, New Senate Report Reveals," NPR, September 27, 2019, https://www.npr.org/2019/09/27/764879242/nra-was-foreign-asset-to-russia-ahead-of-2016-new-senate-report-reveals.

135 Paul Sonne, "A Russian bank gave Marine Le Pen's party a loan. Then weird things began happening," *Washington Post*, December 27, 2018, https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a50422_story.html.

136 "Italy's Salvini under scrutiny over Russia ties in wake of government collapse," France 24, June 28, 2022, https://www.france24.com/en/europe/20220728-italy-s-salvini-under-scrutiny-over-russia-ties-in-wake-of-government-collapse.

137 Amy Remeikis, "Sam Dastyari quits as Labor senator over China connections," *Guardian*, December 11, 2017, https://www.theguardian.com/australia-news/2017/dec/12/sam-dastyari-quits-labor-senator-china-connections.

138 Tess McClure, "New Zealand intelligence report accuses China of 'foreign interference,'" *Guardian*, August 11, 2023, https://www.theguardian.com/world/2023/aug/11/new-zealand-intelligence-report-accuses-china-of-foreign-interference.

139 Hannah Murphy, "Donald Trump's return sends shivers through the anti-misinformation world," *Financial Times*, November 24, 2024, https://www.ft.com/content/bfb404e8-aa7e-4795-a60c-454a310293cc.

140 Caitlin Oprysko and Dana Nickel, "Experts mull what Trump means for FARA," *POLITICO*, December 6, 2024, https://www.politico.com/newsletters/politico-influence/2024/12/06/experts-mull-what-trump-means-for-fara-00193113.

141 Dina Sadek, "FIMI 101: Foreign information manipulation and interference targeting the 2024 US general election," DFR Lab, September 26, 2024, https://dfrlab.org/2024/09/26/fimi-101/.

142 "The Cover Up: Big Tech, the Swamp, and Mainstream Media Coordinated to Censor Americans' Free Speech," House Committee on Oversight and Government Reform, February 8, 2023, https://oversight.house.gov/release/the-cover-up-big-tech-the-swamp-and-mainstream-media-coordinated-to-censor-americans-free-speech-%EF%BF%BC/.

143 Michael R. Gordon and Dustin Volz, "State Department Division That Battles Foreign Disinformation Faces Closure," *Wall Street Journal*, November 10, 2024, https://www.wsj.com/politics/national-security/state-department-division-that-battles-foreign-disinformation-faces-closure-315e58b7.

144 "Accelerator," Accelerator, accessed May 2025, https://researchaccelerator.org/.

Chapter 06

145 Matthew Carrieri et al., "IGF 2013: Analyzing Content Controls in Indonesia (Part 2 of 4)," Citizen Lab, October 25, 2013, https://citizenlab.ca/2013/10/igf-2013-analyzing-content-controls-indonesia/.

146 Kamya Yadav et al., "Countries have more than 100 laws on the books to combat misinformation. How well do they work?" Bulletin of the Atomic Scientists, May 13, 2021, https://thebulletin.org/premium/2021-05/countries-have-more-than-100-laws-on-the-books-to-combat-misinformation-how-well-do-they-work/.

147 Allie Funk, Adrian Shahbaz, and Kian Vesteinsson, "The Repressive Power of Artificial Intelligence," Freedom House, 2023, https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence.

148 Miriam Elder, "Russia adopts stringent internet controls amid censorship concerns," *Guardian*, July 11, 2012, https://www.theguardian.com/world/2012/jul/11/russia-internet-censorship.

149 Ksenia Ermoshina, Benjamin Loveluck, and Francesca Musiani, "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://www.tandfonline.com/doi/full/10.1080/19331681.2021.1905972.

150 "How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine," Open Observatory of Network Interference, February 24, 2023, https://ooni.org/post/2023-russia-a-year-after-the-conflict/.

151 "Freedom on the Net 2024: Indonesia," Freedom House, 2024, https://freedomhouse.org/country/indonesia/freedom-net/2024.

152 Berita Komdigi, "TRUST+POSITIF," KOMDIGI, October 23, 2013, https://www.komdigi.go.id/berita/pengumuman/detail/trust-positif.

153 Mingshi Wu et al., "How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic," USENIX, August 2023, https://www.usenix.org/conference/usenixsecurity23/presentation/wu-mingshi.

154 "Freedom on the Net 2024: Indonesia," Freedom House.

155 Adi Renaldi, "Queer Indonesians Are Being Arrested Under a Vague Anti-Porn Law," Vice, May 31, 2017, https://www.vice.com/en/article/queer-indonesians-are-being-arrested-under-a-vague-anti-porn-law/; Cornelius Hanung, "Indonesia: restrictive laws used to target activists, journalists and government critics," speech, Civicus, March 27, 2023, https://www.civicus.org/index.php/media-resources/news/united-nations/geneva/6329-indonesia-restrictive-laws-used-to-target-activists-journalists-and-government-critics.

156 "Indonesia: Number of Internet service providers (ISPs)," DataHub, 2024, https://datahub.itu.int/data/?e=IDN&i=19174; Carrieri et al., "IGF 2013: Analyzing Content Controls in Indonesia (Part 2 of 4).

157 "iMAP Indonesia 2024 Internet Censorship Report," iMAP, 2024, https://imap.sinarproject.org/reports/2024/imap-indonesia-2024-internet-censorship-report.

158 "iMAP Indonesia 2024 Internet Censorship Report," iMAP, 2024; Carrieri et al., "IGF 2013: Analyzing Content Controls in Indonesia (Part 2 of 4); Jakub Dalek et al., "No Access: LGBTIQ Website Censorship in Six Countries," Citizen Lab, August 31, 2021, https://citizenlab.ca/2021/08/no-access-lgbtiq-website-censorship-in-six-countries/#indonesia.

159 "2024 Internet Censorship Report," iMAP, 2024, https://imap.sinarproject.org/reports/2024.

160 "What is DNS? | How DNS works," Cloudflare, accessed May 2025, https://www.cloudflare.com/learning/dns/what-is-dns/.

161 Aurelija Einorytė, "What is Google DNS, and how do you start using it?" NordVPN, November 19, 2024, https://nordvpn.com/blog/what-is-google-dns/.

162 "DNS tampering" in "OONI Glossary," Open Observatory of Network Interference, last updated July 3, 2023, https://ooni.org/support/glossary/#dns-tampering.

163 "DNS hijacking" in "OONI Glossary," Open Observatory of Network Interference, last updated July 3, 2023, https://ooni.org/support/glossary/#dns-hijacking.

164 "iMAP Indonesia 2024 Internet Censorship Report," IMAP; "TCP/IP blocking" in "OONI Glossary," Open Observatory of Network Interference, last updated July 3, 2023, https://ooni.org/support/glossary/#tcpip-blocking; "HTTP blocking" in "OONI Glossary," Open Observatory of Network Interference, last updated July 3, 2023 https://ooni.org/support/glossary/#http-blocking.

165 "Situs Porno Bocor, Provider Internet Ditegur (Porn Site Leaks, Internet Providers Reprimanded)," KOMDIGI, May 4, 2012, https://www.komdigi.go.id/berita/sorotan-media/detail/situs-porno-bocor-provider-internet-ditegur.

166 "Kominfo Finalisasi DNS Nasional (Kominfo Finalizes National DNS)," KOMDIGI, August 26, 2020, https://www.komdigi.go.id/berita/pengumuman/detail/kominfo-finalisasi-dns-nasional.

167 Herman and Dames Alexander Sinaga, "Gov't Launches 'Web Crawler' to Seek Out Negative Internet Content," Jakarta Globe, January 11, 2018, https://jakartaglobe.id/context/govt-launches-web-crawler-to-seek-out-negative-internet-content; "Freedom on the Net 2016: Indonesia," Freedom House, 2016, https://freedomhouse.org/country/indonesia/freedom-net/2016#B.

168 Herman and Sinaga, "Gov't Launches 'Web Crawler' to Seek Out Negative Internet Content."

169 "iMAP Indonesia 2023 Internet Censorship Report," iMAP, 2023, https://imap.sinarproject.org/reports/2023/imap-indonesia-2023-internet-censorship-report.

170 Wahyudi Djafar, "Human rights and Internet governance," ELSAM, October 23, 2013, https://www.elsam.or.id/en/business-and-human-rights/human-rights-and-internet-governance.

171 Baojun Liu, "Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path," USENIX, August 2018, https://www.usenix.org/conference/usenixsecurity18/presentation/liu-baojun.

Chapter 07

172 "Digital Around the World," DataReportal, last updated April 2025, https://datareportal.com/global-digital-overview.

173 "Internet Shutdowns," Internet Society, accessed May 2025, https://pulse.internetsociety.org/en/shutdowns/.

174 Steven Feldstein, "Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?" Carnegie Endowment for International Peace, March 31, 2022, https://carnegieendowment.org/research/2022/03/government-internet-shutdowns-are-changing-how-should-citizens-and-democracies-respond?lang=en.

175 "Myanmar: UN experts condemn military's 'digital dictatorship,'" United Nations, June 7, 2022, https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship.

176 Andrea Januta and Minami Funakoshi, "Myanmar's internet suppression," Reuters, April 7, 2021, https://www.reuters.com/graphics/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo/.

177 Surachanee Sriyai, "Myanmar's Internet Shutdowns: Silencing Resistance in the Battle for Connectivity," Fulcrum, January 24, 2025, https://fulcrum.sg/myanmars-internet-shutdowns-silencing-resistance-in-the-battle-for-connectivity/.

178 "Netloss Calculator: Myanmar 01/01/2023-12/31/2023," Internet Society, accessed May 2025, https://pulse.internetsociety.org/en/netloss/?country_code=MM&start_date=2023-01-01&end_date=2023-12-31&shutdown_type=shutdown.

179 "Netloss Calculator: India 01/01/2023-12/31/2023," Internet Society, accessed May 2025, https://pulse.internetsociety.org/en/netloss/?country_code=IN&start_date=2023-01-01&end_date=2023-12-31&shutdown_type=shutdown.

180 Zach Rosson et al., "Lives on hold: internet shutdowns in 2024," Access Now, February 23, 2025, https://www.accessnow.org/internet-shutdowns-2024/.

181 Abdullahi Jimoh, "Comoros Shutdown Internet Following Protests Against President's Re-Election," News Central, January 19, 2024, https://newscentral.africa/comoros-shutdown-internet-following-protests-against-presidents-re-election/.

182 "Mauritania Mobile Internet Shutdown Amidst Protests," Internet Society, July 26, 2024, https://pulse.internetsociety.org/en/shutdowns/mauritania-mobile-internet-shut-down-amidst-protests/.

183 "Internet Shutdowns – Acts of Defiance!" Paradigm Initiative, November 18, 2024, https://paradigmhq.org/internet-shutdowns-acts-of-defiance/.

184 Wei Hong et al., "Reduced loss aversion in value-based decision-making and edge-centric functional connectivity in patients with internet gaming disorder," *Journal of Behavioral Addictions* 12, no.2 (2023): 458-470, https://pmc.ncbi.nlm.nih.gov/articles/PMC10316170/.

185 Shelia R. Cotton, William A. Anderson, and Brandi M. McCullough, "Impact of Internet Use on Loneliness and Contact with Others Among Older Adults: Cross-Sectional Analysis," *Journal of Medical Internet Research* 15, no.2 (2013), https://www.jmir.org/2013/2/e39/.

186 "Myanmar: Internet shutdowns shrouding torchings and killings," Article 19, June 23, 2022, https://www.article19.org/resources/myanmar-internet-shutdowns-torchings-killings/.

187 Simon Migliano, "Government Internet Shutdowns Cost $7.69 Billion in 2024," Top10VPN, January 2, 2025, https://www.top10vpn.com/research/cost-of-internet-shutdowns/.

188 "Internet Society Pulse NetLoss Calculator: Methodology for Measuring the Economic Impact of Internet Shutdowns," Internet Society, June 2023, https://pulse.internetsociety.org/wp-content/uploads/2023/06/Methodology_Internet-Society-Pulse-NetLoss-Calculator_June-2023.pdf.

189 Fayaz Bukhari, "Indian Kashmir sees more than $2.4 billion losses since lockdown – group," Reuters, December 18, 2019, https://www.reuters.com/article/world/indian-kashmir-sees-more-than-24-billion-losses-since-lockdown-group-idUSKBN1YM0SJ/; Majid Maqbool, "I›m a journalist who lived through Kashmir›s traumatic internet blackout, which started one year ago. Here›s what it›s like to have your freedoms ripped away for 213 days," Business Insider, August 5, 2020, https://www.businessinsider.com/india-kashmir-internet-blackout-anniversary-i-lived-through-it-2020-8.

190 "Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights - Report of the Office of the United Nations High Commissioner for Human Rights," UN Office of the High Commissioner for Human Rights, May 13, 2022, https://www.ohchr.org/en/documents/thematic-reports/ahrc5055-internet-shutdowns-trends-causes-legal-implications-and-impacts.

191 "Pact for the Future," United Nations, September 2024, https://www.un.org/en/summit-of-the-future/pact-for-the-future.

Chapter 08

192 Alex Nowrasteh and Ryan Bourne, "Six Ways to Understand DOGE and Predict Its Future Behavior," Cato Institute, March 17, 2025, https://www.cato.org/blog/six-ways-understand-doge-predict-its-future-behavior.

193 Nicole Alvarez, "How Is DOGE Abusing Its Power?" Center for American Progress, March 10, 2025, https://www.americanprogress.org/article/how-is-doge-abusing-its-power/.

194 Jill Lepore, "The Failed Ideas That Drive Elon Musk," *New York Times*, April 4, 2025, https://www.nytimes.com/2025/04/04/opinion/elon-musk-doge-technocracy.html.

195 David Remnick, "At the Smithsonian, Donald Trump Takes Aim at History," *New Yorker*, April 6, 2025, https://www.newyorker.com/magazine/2025/04/14/at-the-smithsonian-donald-trump-takes-aim-at-history.

196 Tyler Pager, "Musk Disparages Trump's Trade Adviser, Exposing Rift in President's Inner Circle," *New York Times*, April 8, 2025, https://www.nytimes.com/2025/04/08/us/politics/musk-navarro-tariffs-fight.html.

197 Vittoria Elliott, "We Mapped DOGE's Silicon Valley and Corporate Connections," *WIRED*, March 28, 2025, https://www.wired.com/story/elon-musk-doge-silicon-valley-corporate-connections/.

198 Jake Lahut, "Elon Musk's Takeover Is Being Aided by a Trumpworld Power Couple," *WIRED*, February 27, 2025, https://www.wired.com/story/katie-stephen-miller-elon-musk-takeover/.

199 Lisa Rein, "Trump has a plan for government workers. They're not going to like it.," *Washington Post*, November 21, 2016, https://www.washingtonpost.com/news/powerpost/wp/2016/11/21/trump-republicans-plan-to-target-government-workers-benefits-and-job-security/.

200 Rebecca Jacobs and Robert Maguire, "Trump made up to $160 million from foreign countries as president," Citizens for Responsibility and Ethics in Washington, April 13, 2023, https://www.citizensforethics.org/reports-investigations/crew-investigations/trump-made-up-to-160-million-from-foreign-countries-as-president/.

201 Eric Lipton, Theodore Schleifer, and Zolan Kanno-Youngs, "Trump Family's Cash Registers Ring as Financial Meltdown Plays Out," *New York Times*, April 5, 2025, https://www.nytimes.com/2025/04/05/us/politics/trump-family-saudi-golf.html?smid=nytcore-ios-share&referringSource=articleShare.

202 Eryk Salvaggio, "Anatomy of an AI Coup," Tech Policy Press, February 9, 2025, https://www.techpolicy.press/anatomy-of-an-ai-coup/.

203 Will Oremus, "Concerns about DOGE's data grab fuel push to update privacy law," *Washington Post*, March 18, 2025, https://s2.washingtonpost.com/camp-rw/?trackId=596e8f25ae7e8a614b2f3241&s=67d97001c7d02e51222398ac&utm_campaign=wp_the_technology_202&utm_medium=email&utm_source=newsletter&linknum=5&linktot=72.

204 Makena Kelly, "Elon Musk Ally Tells Staff 'AI-First' Is the Future of Key Government Agency," *WIRED*, February 3, 2025, https://www.wired.com/story/elon-musk-lieutenant-gsa-ai-agency/.

205 Marc Caputo, "Scoop: State Dept. to use AI to revoke visas of foreign students who appear 'pro-Hamas,'" Axios, March 6, 2025, https://www.axios.com/2025/03/06/state-department-ai-revoke-foreign-student-visas-hamas.

206 Kelly, "Elon Musk Ally Tells Staff 'AI-First' Is the Future of Key Government Agency."

207 Miranda Bryant, "Elon Musk and Twitter boss's messages show how pair fell out," *Guardian*, October 1, 2022, https://www.theguardian.com/technology/2022/oct/01/elon-musk-and-twitter-boss-parag-agrawal-messages-show-blossoming-relationship.

208 Rebecca David O'Brien, "Some Trump Officials Push Back Against Musk's Ultimatum to Workers," *New York Times*, February 23, 2025, https://www.nytimes.com/live/2025/02/23/us/trump-news; Elon Musk (@elonmusk), "Consistent with President @realDonaldTrump's instructions, all federal employees will shortly receive an email requesting to understand what they got done last week. Failure to respond will be taken as a resignation.," X, February 22, 2025, 2:46 p.m., https://x.com/elonmusk/status/1893386883444437415.

209 Derek Saul, "Here's What Happened After Elon Musk Cut 80% Of X's Employees—As He Eyes Reshaping Federal Workforce," *Forbes*, February 5, 2025, https://www.forbes.com/sites/dereksaul/2025/02/05/heres-what-happened-after-elon-musk-cut-80-of-xs-employees-as-he-eyes-reshaping-federal-workforce/.

210 Shannon Bond, "Twitter employees quit in droves after Elon Musk›s ultimatum passes," NPR, November 17, 2022, https://www.npr.org/2022/11/17/1137413251/twitter-employees-quit-elon-musk.

211 Chris Cameron, Madeleine Ngo, and Erica L. Green, "Trump Administration Entices Millions of Federal Workers to Resign," *New York Times*, January 28, 2025, https://www.nytimes.com/2025/01/28/us/politics/trump-buyouts-federal-workers.html?smid=url-share.

212 Clare Duffy and Hadas Gold, "They lived through Elon Musk's Twitter takeover. Now, they have advice for federal government employees," CNN, February 5, 2025, https://www.cnn.com/2025/02/05/tech/musk-x-twitter-takeover-us-government-employee-advice/index.html.

213 Sheila Dang, "US ad revenue at Musk›s X declined each month since takeover - data," Reuters, October 4, 2023, https://www.reuters.com/technology/us-ad-revenue-musks-x-declined-each-month-since-takeover-data-2023-10-04/; Alex Hern, "Twitter usage in US 'fallen by a fifth' since Elon Musk's takeover," *Guardian*, March 26, 2024, https://www.theguardian.com/technology/2024/mar/26/twitter-usage-in-us-fallen-by-a-fifth-since-elon-musks-takeover; Matt Egan, "Elon Musk's X is worth nearly 80% less than when he bought it, Fidelity estimates," CNN, October 2, 2024, https://www.cnn.com/2024/10/02/business/elon-musk-twitter-x-fidelity/index.html.

214 Katie Paul and Sheila Dang, "Exclusive: Twitter leans on automation to moderate content as harmful speech surges," Reuters, December 5, 2022, https://www.reuters.com/technology/twitter-exec-says-moving-fast-moderation-harmful-content-surges-2022-12-03/#:~:text=Dec%202%20(Reuters)%20%2D%20Elon,trust%20and%20safety%20told%20Reuters.

215 Anisha Sircar, "X's Latest Content Findings Reveal Troubling Trends In AI Moderation," *Forbes*, October 18, 2024, https://www.forbes.com/sites/anishasircar/2024/10/18/xs-latest-content-findings-reveal-troubling-trends-in-ai-moderation/.

216 Kylie Robison, "How Elon Musk's xAI is quietly taking over X," Verge, January 10, 2025, https://www.theverge.com/2025/1/10/24339249/elon-musk-xai-x-twitter.

217 Soutik Biswas, "Why Elon Musk›s Grok is kicking up a storm in India," BBC, March 20, 2025, https://www.bbc.com/news/articles/cd65p1pv8pdo; Kelsey Piper, "The AI that apparently wants Elon Musk to die," Vox, February 28, 2025, https://www.vox.com/future-perfect/401874/elon-musk-ai-grok-twitter-openai-chatgpt; Robison, "How Elon Musk's xAI is quietly taking over X."

218 "Musk fires outsourced content moderators who track abuse on Twitter," CBS News, November 14, 2022, https://www.cbsnews.com/news/elon-musk-twitter-layoffs-outsourced-content-moderators/; Matt O'Brien and Barbara Ortutay, "Musk's Twitter disbands its Trust and Safety advisory group," Associated Press, December 13, 2022, https://apnews.com/article/elon-musk-twitter-inc-technology-business-a9b795e8050de12319b82b5dd7118cd7.

219 Authors' interview with Theodora Skeadas, over Zoom, on April 15, 2025.

220 Josh Constine, "Facebook's S-1 Letter From Zuckerberg Urges Understanding Before Investment," TechCrunch, February 1, 2012, https://techcrunch.com/2012/02/01/facebook-ipo-letter/.

221 Paul O'Brien, "Silicon Valley's Culture of Creative Destruction," Medium, January 3, 2025, https://seobrien.medium.com/silicon-valleys-culture-of-creative-destruction-4ff2a06aed1a; Calder McHugh, "Elon Musk's 'Move Fast and Break Things' Attitude Clashes with Washington," *POLITICO*, December 24, 2024, https://www.politico.com/news/magazine/2024/12/24/elon-musk-washington-congress-00196006.

222 Aarian Marshall, "Tesla Autopilot Was Uniquely Risky—and May Still Be," *WIRED*, April 26, 2024, https://www.wired.com/story/tesla-autopilot-risky-deaths-crashes-nhtsa-investigation/; Faiz Siddiqui and Jeremy B. Merrill, "17 fatalities, 736 crashes: The shocking toll of Tesla's Autopilot," *Washington Post*, June 10, 2023, https://www.washingtonpost.com/technology/2023/06/10/tesla-autopilot-crashes-elon-musk/.

223 David Paul Kirkpatrick, "Elon Musk and the Art of Controlled Demolition," Medium, February 3, 2025, https://thegoodage.medium.com/elon-musk-and-the-art-of-controlled-demolition-115902e36b81.

224 Jeff Stein et al., "In chaotic Washington blitz, Elon Musk's ultimate goal becomes clear," *Washington Post*, February 8, 2025, https://www.washingtonpost.com/business/2025/02/08/doge-musk-goals/.

225 Jeff Stein, Jacob Bogage and Emily Davies, "White House pauses all federal grants, sparking confusion," *Washington Post*, January 28, 2025, https://www.washingtonpost.com/business/2025/01/27/white-house-pauses-federal-grants/; Ivan Pereira and Emily Chang, "Here are all the agencies that Elon Musk and DOGE have been trying to dismantle so far," ABC News, February 27, 2025, https://abcnews.go.com/Politics/elon-musks-government-dismantling-fight-stop/story?id=118576033; Ashley Wu et al., "Where Trump, Musk and DOGE Have Cut Federal Workers So Far," *New York Times*, last updated March 12, 2025, https://www.nytimes.com/interactive/2025/02/11/us/politics/trump-musk-doge-federal-workers.html.

226 Kyle Chayka, "Elon Musk's A.I.-Fuelled War on Human Agency," *New Yorker*, February 12, 2025, https://www.newyorker.com/culture/infinite-scroll/elon-musks-ai-fuelled-war-on-human-agency.

227 Jared Keller, "The US Army Is Using 'CamoGPT' to Purge DEI From Training Materials," *WIRED*, March 6, 2025, https://www.wired.com/story/the-us-army-is-using-camogpt-to-purge-dei-from-training-materials/.

228 Matteo Wong, "DOGE's Plans to Replace Humans With AI Are Already Under Way," *Atlantic*, March 10, 2025, https://www.theatlantic.com/technology/archive/2025/03/gsa-chat-doge-ai/681987/.

229 Gerald E. Connolly to Howard Lutnick, March 12, 2025, in Committee on Oversight and Government Reform, https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025-03-12-gec-to-24-agencies-re-doge-ai.pdf.

230 Mohar Chatterjee, "Pentagon's 'SWAT team of nerds' resigns en masse," *POLITICO*, April 15, 2025, https://www.politico.com/news/2025/04/15/pentagons-digital-resignations-00290930.

231 Catherine Rampell, "How DOGE is making government almost comically inefficient," *Washington Post*, March 21, 2025, https://www.washingtonpost.com/opinions/2025/03/21/doge-government-efficiency-federal-workers/?utm_source=substack&utm_medium=email.

232 Lisa Rein and Hannah Natanson, "Long waits, waves of calls, website crashes: Social Security is breaking down," *Washington Post*, March 25, 2025, https://www.washingtonpost.com/politics/2025/03/25/social-security-phones-doge-cuts/.

233 Ezra Klein, "What Is DOGE's Real Goal?" *New York Times*, March 25, 2025, https://www.nytimes.com/2025/03/25/opinion/ezra-klein-podcast-santi-ruiz.html.

234 Geoffrey A. Fowler, "The truth about DOGE's AI plans: The tech can't do that," *Washington Post*, March 3, 2025, https://www.washingtonpost.com/technology/2025/03/03/doge-ai-government-automation/.

235 Stein et al., "In chaotic Washington blitz, Elon Musk's ultimate goal becomes clear."

236 Chayka, "Elon Musk's A.I.-Fuelled War on Human Agency."

237 Kelly, "Elon Musk Ally Tells Staff 'AI-First' Is the Future of Key Government Agency."

238 Wong, "DOGE's Plans to Replace Humans With AI Are Already Under Way."

239 Caputo, "Scoop: State Dept. to use AI to revoke visas of foreign students who appear 'pro-Hamas.'"

240 Paul Mozur, Adam Satariano, and Aaron Krolik, "This Company's Surveillance Tech Makes Immigrants 'Easy Pickings' for Trump," *New York Times*, April 14, 2025, https://www.nytimes.com/2025/04/14/technology/trump-immigration-tech-geo-group.html.

241 Alexandra Ulmer et al., "Musk›s DOGE using AI to snoop on U.S. federal workers, sources say," Reuters, April 8, 2025, https://www.reuters.com/technology/artificial-intelligence/musks-doge-using-ai-snoop-us-federal-workers-sources-say-2025-04-08/.

242 Stein et al., "In chaotic Washington blitz, Elon Musk's ultimate goal becomes clear."

243 Eryk Salvaggio, "The AI State is a Surveillance State," Tech Policy Press, March 12, 2025, https://www.techpolicy.press/the-ai-state-is-a-surveillance-state/; Lindsay Whitehurst, "Federal judge blocks DOGE from accessing Americans' personal Social Security data, for now," PBS, March 20, 2025, https://www.pbs.org/newshour/politics/federal-judge-blocks-doge-from-accessing-americans-personal-social-security-data-for-now.

244 Makena Kelly, "DOGE Is Planning a Hackathon at the IRS. It Wants Easier Access to Taxpayer Data," *WIRED*, April 5, 2025, https://www.wired.com/story/doge-hackathon-irs-data-palantir/.

245 Kelly, "DOGE Is Planning a Hackathon at the IRS. It Wants Easier Access to Taxpayer Data."

Chapter 09

246 Iginio Gagliardone, "Lock-out, lock-in, and networked sovereignty. Resistance and experimentation in Africa's trajectory towards AI," *Liincem Revista* 20, no.2 (December 2024), https://revista.ibict.br/liinc/article/view/7319/7074.

247 Gagliardone, "Lock-out, lock-in, and networked sovereignty. Resistance and experimentation in Africa's trajectory towards AI."

248 Arindrajit Basu, "Defending the 'S Word': The Language of Digital Sovereignty Can be a Tool of Empowerment," 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?lang=en#defending-the-s-word-the-language-of-digital-sovereignty-can-be-a-tool-of-empowerment; 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?lang=en#to-get-its-ai-foothold-brazil-needs-to-apply-the-key-ai-sovereignty-enablers-kase; Iginio Gagliardone, "A Postcolonial Perspective on Digital Sovereignty," 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?lang=en#a-postcolonial-perspective-on-digital-sovereignty.

249 "National Policy on Data and Cloud," Government Gazette, May 31, 2024, https://www.gov.za/sites/default/files/gcis_document/202406/50741gen2533.pdf.

250 "Sama," Sama, accessed May 2025, https://www.sama.com/.

251 Leila janah, *Give Work: Reversing Poverty One Job at a Time* (New York: Portfolio/Penguin, 2017), https://www.penguinrandomhouse.com/books/546305/give-work-by-leila-janah/.

252 Billy Perrigo, "Inside Facebook's African Sweatshop," Time, February 17, 2022, https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/.

253 "Huge ruling in Kenyan court threatens global model of outsourced content moderation – and says that Facebook is the 'true employer' of its key safety workers," Foxglove, June 6, 2023, https://www.foxglove.org.uk/2023/06/06/kenyan-court-ruling-outsourced-content-moderation-facebook/.

254 "Draft National Policy on Data and Cloud," *Government Gazette*, April 1, 2021, https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf.

255 "National Policy on Data and Cloud," *Government Gazette*, May 31, 2024, https://www.gov.za/sites/default/files/gcis_document/202406/50741gen2533.pdf.

256 Sibahle Malinga, "Several flaws in SA's draft data and cloud policy, say experts," IT Web, June 11, 2021, https://www.itweb.co.za/article/several-flaws-in-sas-draft-data-and-cloud-policy-say-experts/xA9PO7NZ46Z7o4J8.

257 William King and Christian Tshishiku, "Africa's Key Data Centre Markets," DCByte, 2023, http://africadca.org/wp-content/uploads/2023/07/Title_Africas-Key-Data-Centre-Markets.pdf.

258 Gabriella Razzano, Data Localisation in South Africa: Missteps in the Valuing of Data," Mandela Institute, December 2021, https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/mandela-institute/documents/research-publications/800482%20PB6%20Missteps%20in%20valuing%20data_REV%20Dec2021.pdf.

259 Antonio García Martínez, "No, Data Is Not the New Oil," *WIRED*, February 26, 2019, https://www.wired.com/story/no-data-is-not-the-new-oil/.

260 "Noga Mo Jozi Loop of Dreams," video, Authentic Studio, September 26, 2023, https://vimeo.com/868332312/2f837b5f9b?share=copy.

261 Achille Mbembe, "Scrap the borders that divide Africans," *Mail and Guardian*, March 17, 2017, https://mg.co.za/article/2017-03-17-00-scrap-the-borders-that-divide-africans/.

Chapter 10

262 "RSA Conference 2024: San Francisco," RSAC, 2024, https://www.rsaconference.com/events/2024-usa; Anthony J. Blinken, "2024 RSA Conference Address: Technology and the Transformation of U.S. Foreign Policy," speech, RSAC, May 6, 2024, archived, American Rhetoric, https://www.americanrhetoric.com/speeches/antonyblinkenrsa2024.htm.

263 Pablo Chavez, "Toward Digital Solidarity," Lawfare, June 28, 2022, https://www.lawfaremedia.org/article/toward-digital-solidarity; "United States International Cyberspace & Digital Policy Strategy," U.S. Department of State, last updated May 2024, https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.

264 J.D. Vance, "Remarks by the Vice President at the Artificial Intelligence Action Summit in Paris, France," speech, Artificial Intelligence Action Summit, February 11, 2025, archived, The American Presidency Project, https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france.

265 Kevin Liptak, Samantha Waldenberg, and Oren Liebermann, "Trump pauses military aid to Ukraine after Oval Office argument with Zelensky, White House official says," CNN, March 3, 2025, https://edition.cnn.com/2025/03/03/politics/trump-administration-ukraine-aid/index.html.

266 Zoe Kleinman and Liv McMahon, "UK and US refuse to sign international AI declaration," BBC, February 11, 2025, https://www.bbc.com/news/articles/c8edn0n58gwo.

267 Tianyu Fang and Tim Hwang, "Digital Solidarity in U.S. Foreign Policy," New America, September 5, 2024, https://www.newamerica.org/oti/reports/digital-solidarity-in-us-foreign-policy/.

268 Hillary Rodham Clinton, "Remarks on Internet Freedom," speech, U.S. Department of State, January 21, 2010, https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm; Matt Perault, "Internet Freedom 10 Years In," Lawfare, January 21, 2020, https://www.lawfaremedia.org/article/internet-freedom-10-years.

269 Milton Mueller, "Internet Fragmentation Exists, But Not In the Way That You Think," Council on Foreign Relations, June 12, 2017, https://www.cfr.org/blog/internet-fragmentation-exists-not-way-you-think.

270 "Safeguarding Democracy: Navigating the Complex Landscape of Foreign Interference in Elections," Kofi Annan Foundation, September 1, 2023, https://www.kofiannanfoundation.org/news/foreign-interference-in-elections-how-to-define-it/.

271 "The State Internet Censorship: A Global Overview," Go-Globe, July 1, 2024, https://www.go-globe.com/the-state-internet-censorship-a-global-overview/.

272 Xiao Qiang, "China's Role in Global Digital Repression," Global Policy, March 28, 2023, https://www.globalpolicyjournal.com/blog/28/03/2023/chinas-role-global-digital-repression; Mark Raymond and Justin Sherman, "Authoritarian multilateralism in the global cyber regime complex: The double transformation of an international diplomatic practice," *Contemporary Security Policy* 45, no.1 (October 2023), https://www.tandfonline.com/doi/full/10.1080/13523260.2023.2269809.

273 Tom Temin, "State Department pursues digital solidarity with like-minded countries," Federal News Network, May 17, 2024, https://federalnewsnetwork.com/management/2024/05/state-department-pursues-digital-solidarity-with-like-minded-countries/.

274 Gatra Priyandita, Dirk van der Kley, and Benjamin Herscovitch, "Localization and China's Tech Success in Indonesia," Carnegie Endowment for International Peace, July 11, 2022, https://carnegieendowment.org/research/2022/07/localization-and-chinas-tech-success-in-indonesia?lang=en.

275 Gautam Chikermane, "Excluding Huawei from India is part of a policy continuum," Observer Research Foundation, May 7, 2021, https://www.orfonline.org/expert-speak/excluding-huawei-from-india-is-part-of-a-policy-continuum.

276 "The Intricacies of 5G Development in Southeast Asia," *ISEAS Perspective* 130 (November 2020), https://www.iseas.edu.sg/wp-content/uploads/2020/11/ISEAS_Perspective_2020_130.pdf.

277 Priyandita, van der Kley, and Herscovitch, "Localization and China's Tech Success in Indonesia."

278 Christopher S. Chivvis and Beatrix Geaghan-Breiner, "Emerging Powers and the Future of American Statecraft," Carnegie Endowment for International Peace, April 9, 2024, https://carnegieendowment.org/research/2024/04/emerging-powers-and-the-future-of-american-statecraft?lang=en.

279 Eva Dou, "Trump dreamt of a 'Huawei killer.' Biden is trying to unleash it," *Washington Post*, February 12, 2024, https://www.washingtonpost.com/technology/2024/02/12/oran-biden-china-huawei-technology/.

280 Gagandeep Kaur, "India, US formulate open RAN roadmap," Light Reading, January 18. 2024, https://www.lightreading.com/open-ran/india-us-formulate-open-ran-roadmap; "USTDA, Indonesia Partner on Next Generation Network Deployment," USTDA, February 22, 2024, https://www.ustda.gov/ustda-indonesia-partner-on-next-generation-network-deployment/; "United States, Philippines Step Closer to Launching First Open RAN Laboratory in Manila," U.S. Embassy Manila, June 5, 2024, https://ph.usembassy.gov/united-states-philippines-step-closer-to-launching-first-open-ran-laboratory-in-manila/.

281 Manoj Harjani, "O-RAN is overhyped as avoiding Chinese 5G influence," ASPI, May 29, 2024, https://www.aspistrategist.org.au/o-ran-is-overhyped-as-avoiding-chinese-5g-influence/.

282 Emil Björnson, "Open RAN: Success or Failure?" Wireless Future, October 23, 2024, https://ma-mimo.ellintech.se/2024/10/23/open-ran-success-or-failure/.

283 Ramsha Jahangir and Justin Hendrix, "With US Commitment to Internet Freedom in Jeopardy, China and Russia Set to Gain," Tech Policy Press, February 6, 2025, https://www.techpolicy.press/with-us-commitment-to-internet-freedom-in-jeopardy-china-and-russia-set-to-gain/; 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 (2024): 256-287, https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2436591.

284 Emma Klein and Stewart Patrick, "Envisioning a Global Regime Complex to Govern Artificial Intelligence," Carnegie Endowment for International Peace, March 21, 2024, https://carnegieendowment.org/research/2024/03/envisioning-a-global-regime-complex-to-govern-artificial-intelligence?lang=en.

285 Vibhu Mishra, "General Assembly adopts landmark resolution on artificial intelligence," United Nations, March 21, 2024, https://news.un.org/en/story/2024/03/1147831.

286 Raj Bhala, "The New Age of Global Trade: Aggressive Neo-Mercantilism," *The Diplomat*, March 1, 2025, https://thediplomat.com/2025/03/the-new-age-of-global-trade-aggressive-neo-mercantilism/.

287 "#KeepItOn," Access Now, accessed May 2025, https://www.accessnow.org/campaign/keepiton/.

288 "Global statement: Stop facial recognition surveillance now!" joint letter, European Digital Rights and Big Brother Watch, et al., September 2023, https://edri.org/wp-content/uploads/2023/09/Global-statement-Stop-facial-recognition-now.pdf.

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 170 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.

CarnegieEndowment.org