CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

The Architecture of Digital Repression

Internet service providers can facilitate internet access but also draconian control.

By Irene Poetranto
Published on Mar 10, 2026

This essay is part of a series from Carnegie's Digital Democracy Network, a diverse group of thinkers and activists engaged in work on technology and politics. The series is produced by Carnegie's Democracy, Conflict, and Governance Program. The full set of essays is scheduled for publication in summer 2026.

Following the 2021 coup in Myanmar, the military junta compelled telecommunications operators and internet service providers (ISPs) in the country to implement information controls, including installing surveillance and interception technology on their networks, providing user data to police and military officials, and enforcing SIM card registration for mobile phone users.[1] The junta's tactics contributed to Telenor,[2] a Norwegian telecom company, and Ooredoo,[3] a Qatari telecom company, exiting the Myanmar market in 2022, having sold their local operations to military-affiliated entities. Specifically, Telenor Myanmar was sold to a Lebanese firm with links to Myanmar's military, and the company subsequently changed its name to ATOM Myanmar.[4] At the same time, Ooredoo Myanmar was purchased by a firm with ties to military-linked figures and rebranded as U9 Myanmar.[5] The military-dominated telecommunications sector in Myanmar has enabled and institutionalized state-sponsored digital repression through frequent internet shutdowns (with at least eighty-five shutdown incidents in 2024),[6] and the use of tools, such as

"surveillance drones, iPhone cracking devices and hacking software" to suppress anti-junta resistance and civil disobedience.[7] In January 2025, Myanmar's digital repression apparatus was bolstered by the enactment of a controversial cybersecurity law, which gives the government increased ability to block websites and surveil internet users.[8]

Myanmar has adopted a similar approach to that of Russia and China, where draconian internet laws and regulations have enabled state coercion of ISPs and facilitated extensive information controls. Russia, for example, passed a "sovereign internet" law in 2019 that established a National Domain Name System (DNS) maintained by Roskomnadzor, Russia's internet regulator. DNS functions as the internet's address book, translating a URL into a numerical IP address. Therefore, state control over the National DNS allows the government to block access to certain websites entirely or to redirect users to government-sanctioned sites.[9] The government required all ISPs operating in Russia to use the National DNS as of January 2021.[10] The "sovereign internet" law has thus enabled the government to block thousands of websites, including sites that "host material critical of the authorities or of the [Ukraine] invasion, as well as international news sites, civil society websites, and Ukrainian news sites."[11]

The existing literature on digital repression has examined information controls at the application and content levels, including content filtering or blocking and government requests to social media platforms to remove content.[12] However, researchers have under-studied how ISPs that build and/or operate the underlying infrastructure implement controls. Given their role as gatekeepers of internet access, understanding ISP practices and government oversight of them is essential to comprehending how information controls function in practice. This article addresses this gap by analyzing the role of ISPs in information controls and examines the mechanisms by which state-directed digital repression operates within the network infrastructure.

State Control Over ISPs: Its Establishment and Evolution

In jurisdictions where only state-owned providers exist, internet access is highly vulnerable to state-directed monitoring and manipulation. For example, in China, the government built internet infrastructure through extensive, coordinated state planning, combined with efforts to ensure continued government control. The majority of China's physical internet infrastructure, in both urban and rural regions, is built and maintained by state-owned enterprises—namely, China Telecom, China Unicom, and China Mobile—which provide services such as broadband, fixed-line connections, and mobile data.[13] Intensive state intervention, coupled with the application of significant barriers to foreign entities' operations in the country, has allowed these state-owned providers to dominate China's internet market.[14] Additionally, China has developed and maintained a nationwide internet censorship system that filters internet traffic entering and leaving the country's networks.[15] Colloquially known as the Great Firewall, this censorship system was launched in 1998 by the Ministry of Public Security, only four years after the country established a fully functional connection to the global internet.[16]

More recently, in 2024, China lifted foreign investment restrictions on companies providing telecommunications services, including internet access.[17] However, newly formed ISPs are still required to use the existing network infrastructure controlled by state-owned providers and obtain an operating permit from the Ministry of Industry and Information Technology (MIIT), one of several Chinese institutions that enforce online and offline censorship.[18] As part of the permitting process, MIIT verifies that ISPs have complied with its content-censorship rules, given that all ISPs operating in China, regardless of ownership, must implement content blocking and filtering.[19] Due to these stringent censorship requirements, there is widespread content filtering in the country, including against "criticism of individuals, policies, or events that are considered integral to the one-party system," resulting in a "highly controlled, monitored, and manipulated version" of the Chinese internet.[20] The case of

China shows that state dominance over network infrastructure, dating back to the early establishment of the internet, facilitates ongoing internet controls and large-scale monitoring of internet users.

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

In other jurisdictions where private ISPs have coexisted with state-owned ISPs, government control of network infrastructure typically evolved gradually. This type of evolution is apparent in Russia, where its internet infrastructure, built in the Soviet era, was developed by private organizations and research institutions with limited state involvement. Russia connected to the global internet for the first time in 1990 via a computer network operated by RELCOM (Reliable Communications), which was developed by a group of computer programmers at the Kurchatov Institute.[21] By the mid-1990s, numerous commercial ISPs existed in Russia, such as FidoNet, GlasNet, IASnet, and Sovam Teleport, all established by private organizations.[22] Until the early 2000s, the Russian internet (or "RuNet" for short) received minimal state oversight compared with traditional media, likely due to low internet penetration rates—that is, in 2008, only 14 percent of the population had internet access.[23] RuNet's user base subsequently expanded during the 2011–2012 mass protests over suspicions of electoral fraud, an issue largely ignored by traditional Russian media but actively discussed online by independent journalists and bloggers.[24] This rise in online political discussion in the 2010s led researchers to refer to the internet as Russia's "alternative public sphere."[25]

Before 2012, RuNet was governed primarily through general legal frameworks and existing laws on mass media, communications, and information protection, rather than internet-specific legislation or China-style direct internet filtering. After 2012, however, Russia passed multiple stringent laws that enhanced the

state's ability to restrict and censor online speech, described by analysts as a government-led "'blitzkrieg' against online free expression."[26] For example, Federal Law No. 139-FZ of 2012 and Federal Law No. 398-FZ of 2013 granted Roskomnadzor the mandate to prohibit websites and to require ISPs to comply with its blocking directives.

By 2015, Freedom House had rated Russia as "Not Free," due to significant steps to "increase control over the online sphere, particularly in advance of the Sochi Olympic Games."[27] In the ensuing years, Russia has intensified its authoritarian regulation of the internet, employing a range of legal instruments and technical interference with internet infrastructure.[28] For example, Russia requires ISPs to install surveillance systems known as SORM (System for Operative Investigative Activities), which consists of hardware and software installed at the operator's expense but directly controlled by the Federal Security Service of the Russian Federation (FSB), the country's principal domestic intelligence and security agency. First introduced in 1995 for wiretapping and phone surveillance, SORM was later adapted to the internet in 1998 (SORM-2) and expanded in 2014 (SORM-3) to include the collection of metadata and multimedia files. The government significantly expanded SORM's functionality following the passage in 2016 of the so-called Yarovaya Law (in fact, a set of two Russian federal bills, 374-FZ and 375-FZ), which requires ISPs and telecom providers to store the content of all user communications for up to six months and metadata for up to three years. A 2018 amendment revised some of these requirements following criticism from ISPs, such as requiring storage of the content of all communications (for example, voice calls, data, images, and text messages) for only thirty days, though metadata retention remained at three years and storage capacity was to be increased by 15 percent annually.[29] Russia's efforts to control the internet also extend beyond its borders, notably in Ukrainian territories it has occupied following its 2022 invasion. In Kherson, for example, Russia imposed an internet shutdown and subsequently restored connectivity via its state-owned provider, Rostelecom, to integrate the territory into Russia's internet infrastructure.[30] Additionally, as of January 2023, ISPs on temporarily

occupied territories must install SORM for the purposes of "lawful interception and the storage of their clients' metadata."[31]

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

Infrastructure Controls and Internet Freedom

As part of their digital repression toolkit, states can restrict the flow of information online by imposing limits on the access and transit providers that carry internet traffic.[32] Access providers deliver internet services directly to consumers and businesses—major U.S. examples include Comcast (Xfinity), AT&T, and Verizon. In contrast, transit providers like Cogent and Lumen supply the underlying internet infrastructure to other networks rather than serving home users directly.[33] As transit providers connect multiple access providers, state control over them results in a more efficient mechanism for surveilling, filtering, or manipulating internet traffic. Moreover, because most internet users are unaware of how transit providers operate or are regulated, states can compel transit providers to engage in surveillance and censorship of internet users with less risk of public backlash.

Given the significance of transit providers, autocratic regimes such as China, Uzbekistan, and the United Arab Emirates (UAE) have configured and regulated

their internet to ensure that only state-owned ISPs function as transit providers within their jurisdictions.[34] State-owned providers from autocratic regimes have also operated in other authoritarian settings. For example, the UAE's state-owned providers also deliver internet services in Gabon, Mauritania, and Morocco.[35] This authoritarian infrastructure nexus facilitates digital repression and cross-border information controls.

Stringent state oversight of the ISP industry is also evident in Myanmar, resulting in civil society groups' concerns about extensive ties and cooperation between ISPs and the government. Before their exits from Myanmar, for example, both Ooredoo and Telenor had faced criticism about their compliance with human rights-violating policies. Following the 2021 coup, Ooredoo Myanmar stated that it "regretfully complied" with government directives to limit mobile and wireless broadband access.[36] Furthermore, rights activists argued that Telenor Myanmar's cooperation with the junta led to the arrest or executions of student leaders and pro-democracy activists.[37] Consequently, in December 2024, Justice For Myanmar and ICJ Norway filed a complaint with the Norwegian police against Telenor Group, which is majority-owned by the Norwegian government, and the management of its Myanmar operations. In this complaint, they alleged that Telenor's Myanmar subsidiary had violated Norwegian sanctions by "sharing sensitive network traffic data with the junta and transferring so-called lawful interception equipment to a Myanmar military-linked company."[38]

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

Additionally, Myanmar's ISPs, now with military-linked ownership, have acquired surveillance and filtering technology that further reinforced transnational authoritarianism in the country. In May 2024, Justice For

Myanmar found that the junta had acquired "a new web surveillance and censorship system to increase its control of the internet," including deep packet inspection (DPI) tools for monitoring and filtering content for use by its ISPs.[39] In May 2025, joint investigations by Finance Uncovered and Myanmar Now concluded that Frontiir, a Yangon-based ISP, had installed Geedge equipment capable of tracking users' online activity, blocking websites, and preventing the use of virtual private networks (VPNs) to circumvent online censorship.[40] (Frontiir, an ISP that received $40 million in development funding from the governments of the United Kingdom, Norway, and Denmark in exchange for equity shares, denied these allegations.)[41]

Authoritarian governments worldwide are increasingly leveraging their control of network operators, enactment of stringent regulations, and international sales of surveillance and filtering technologies to augment their digital repression capabilities. The result is an intensifying challenge to the protection of fundamental human rights and to the stability of the open, interconnected global internet. These developments highlight the urgent need for international cooperation to strengthen democratic governance frameworks, counterbalance transnational authoritarian digital influence, and preserve internet freedom. Central to this effort is the implementation of the UN Guiding Principles on Business and Human Rights, which establish that companies have a responsibility to respect human rights and conduct due diligence to ensure that their tools and services are not complicit in digital repression.

What can activists and democratic governments do to counter these trends? At a minimum, when companies based in liberal democracies, like Telenor in Norway, sell their subsidiaries in authoritarian countries, they should screen potential buyers for links to human rights abusers and sanctioned entities. They should also publish transparency reports on how such exits or sales meet international human rights standards (for example, by embedding the UN Guiding Principles on Business and Human rights in the terms of purchase). When it comes to probing the locations and operations of authoritarian state providers, civil society groups and researchers are well-placed to carry out investigations to expose surveillance risks and facilitate informed advocacy. But

these activities require significant resources—support that democratic governments can help provide. Finally, democracies can fund digital literacy and security programs for internet users residing in jurisdictions with networks operated by authoritarian-linked ISPs. Without coordinated action, authoritarian governments and their allies will continue to exploit regulatory gaps and establish enhanced cooperation to export surveillance and censorship capabilities and entrench digital repression worldwide

About the Author

Irene Poetranto

Senior Researcher, Citizen Lab

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. She has a PhD in Political Science from the University of Toronto. Her research interests include the politics of internet regulation, surveillance technology and gendered digital repression, and the geopolitical implications of platform regulation and data sovereignty.

Notes

1 "Myanmar: UN Experts Condemn Military's 'Digital Dictatorship,'" OHCHR, accessed February 5, 2026, https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship.

2 Fanny Potkin, "Norway's Telenor Says Myanmar Unit Sale Plan Followed Junta's Pressure on Surveillance Tech," Reuters, September 15, 2021, https://www.reuters.com/world/norways-telenor-says-myanmar-unit-sale-came-after-juntas-pressure-surveillance-2021-09-15/.

3 "Myanmar's Last Foreign Telecom, Ooredoo, to Leave Country," The Irrawaddy, July 20, 2022, https://www.irrawaddy.com/news/burma/myanmars-last-foreign-telecom-ooredoo-to-leave-country.html.

[4] Justice Initiative, "Telenor Faces Legal Action Over Human Rights Abuses in Myanmar," Justice Initiative, October 7, 2025, https://www.justiceinitiative.org/newsroom/telenor-faces-legal-action-over-human-rights-abuses-in-myanmar.

[5] Access Now, "Ooredoo's Plans to Leave Myanmar Hands Military Full Control of Nation's Telco Sector — It Must Mitigate the Human Rights Risks," Access Now, n.d., accessed February 5, 2026, https://www.accessnow.org/press-release/ooredoo-myanmar-sale/.

[6] Tommy Walker and Darko Janjevic, "Myanmar: Why Is Junta Shutting down Internet?," DW.com, February 27, 2025, https://www.dw.com/en/myanmar-why-is-junta-shutting-down-internet/a-71770580.

[7] Hannah Beech, "Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown," *New York Times*, March 1, 2021, https://www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html.

[8] Wai Phyo Mint, "Fourth Year Under Myanmar Military's Digital Iron Curtain: A Reflection on Digital Repression and the Path Forward," Tech Policy Press, March 3, 2025, https://techpolicy.press/fourth-year-under-myanmar-militarys-digital-iron-curtain-a-reflection-on-digital-repression-and-the-path-forward.

[9] Alena Epifanova, "Deciphering Russia's "Sovereign Internet Law," German Council on Foreign Relations, January 16, 2020, https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

[10] "Russia's National DNS," Internet Society, December 1, 2023, https://www.internetsociety.org/resources/internet-fragmentation/russias-national-dns/.

[11] "Russia: Freedom on the Net 2024 Country Report," Freedom House, 2025, https://freedomhouse.org/country/russia/freedom-net/2024.

[12] Soyoung Park and Yoonmo Sang, "The Changing Role of Nation States in Online Content Governance: A Case of Google's Handling of Government Removal Requests," *Policy & Internet* 15, no. 3 (2023): 351–69, https://doi.org/10.1002/poi3.342; Sebastian Hellmeier, "The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes," *Politics & Policy* 44, no. 6 (2016): 1158–91, https://doi.org/10.1111/polp.12189.

[13] Jing Feng et al., "Content Regulation Laws for Chinese ISPs: Legal Responsibilities in Free Speech and Filtering of Harmful Content," *Law and Economy* 2, no. 11 (2023): 53–59, https://www.paradigmpress.org/le/article/view/868.

[14] Shazeda Ahmed and Steven Weber, "China's Long Game in Techno-Nationalism," *First Monday*, ahead of print, April 30, 2018, https://doi.org/10.5210/fm.v22i5.8085.

[15] Young Xu, "Deconstructing the Great Firewall of China," *Thousand Eyes* (blog), Cisco, March 8, 2016, https://www.thousandeyes.com/blog/deconstructing-great-firewall-china.

[16] "In China, the 'Great Firewall' Is Changing a Generation," Human Rights Watch, September 1, 2020, https://www.hrw.org/news/2020/09/01/china-great-firewall-changing-generation; Jimmy Wu and Oiwan Lam, "The Evolution of China's Great Firewall: 21 Years of Censorship," Global Voices Advox, August 30, 2017, https://advox.globalvoices.org/2017/08/30/the-evolution-of-chinas-great-firewall-21-years-of-censorship/.

[17] "China Lifts Foreign Investment Access Restrictions in Manufacturing Sector_Express_北京市人民政府外事办公室," Foreign Affairs Office, People's Government of Beijing Municipality, September 12, 2024, https://wb.beijing.gov.cn/en/express/202411/t20241111_3938954.html.

[18] "Censorship Practices of the People's Republic of China," US-China Economic and Security Review Commission, July 17, 2024, https://www.uscc.gov/research/censorship-practices-peoples-republic-china; "China - Allows 100 per Cent Foreign Ownership in Certain Value-Added Telecommunication Services," Investment Policy Monitor, UNCTAD, April 8, 2024, https://investmentpolicy.unctad.org/investment-policy-monitor/measures/4636/-allows-100-per-cent-foreign-ownership-in-certain-value-added-telecommunication-services; "China to Lift Foreign Investment Limit in Value-Added Telecom Services," Simmons & Simmons, April 16, 2024, https://www.simmons-simmons.com/en/publications/clv4vft2100lutzeg455uhpab/china-to-lift-foreign-investment-limit-in-value-added-telecom-services.

[19] "Guide to Obtaining an ICP License for Your Website in China," FDI China, December 30, 2024, https://fdichina.com/blog/obtaining-an-icp-license/; Henry L. Hu, "The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration," *China Quarterly* 207 (September 2011): 523–40, https://doi.org/10.1017/S0305741011000634.

[20] "China: Freedom on the Net 2024 Country Report," Freedom House, 2025, https://freedomhouse.org/country/china/freedom-net/2024.

[21] Alexander E. Voiskounsky, "The Relcom Network: An Investigation of Its Users," *Journal of Computer-Mediated Communication* 2, no. 4 (1997): JCMC248, https://doi.org/10.1111/j.1083-6101.1997.tb00198.x; Andrei Soldatov and Irina Borogan, "The Kremlin Jails the Father of Russia's Internet," Center for European Policy Analysis, July 23, 2024, https://cepa.org/article/russia-jails-the-father-of-russias-internet/.

[22] Rafal Rohozinski and UN Research Institute for Social Development, eds., *Mapping Russian Cyberspace: Perspectives on Democracy and the Net*, Discussion Paper / United Nations Research Institute for Social Development, DP 115 (UNRISD, 1999), https://digitallibrary.un.org/record/412935.

[23] Liudmila Sivetc, "State Regulation of Online Speech in Russia: The Role of Internet Infrastructure Owners," *International Journal of Law and Information Technology* 27, no. 1 (2019): 28–49, https://doi.org/10.1093/ijlit/eay016; "Russia Has Fastest Growing Internet Population in Europe," Comscore, August 2008, https://www.comscore.com/Insights/Press-Releases/2008/08/Russia-Internet-Growth.

[24] Muzaffar Suleymanov, "Protests Not Newsworthy to Kremlin-Controlled Media," Committee to Protect Journalists, December 7, 2011, https://cpj.org/2011/12/russian-protests-not-newsworthy-to-kremlin-control/.

[25] Liudmila Sivetc, "State Regulation of Online Speech in Russia: The Role of Internet Infrastructure Owners," *International Journal of Law and Information Technology* 27, no. 1 (2019): 28–49, https://doi.org/10.1093/ijlit/eay016.

[26] Sivetc, "State Regulation of Online Speech in Russia: The Role of Internet Infrastructure Owners."

[27] Freedom House, "Freedom on the Net 2015 – Russia," Refworld, 2016, https://www.refworld.org/reference/annualreport/freehou/2015/en/107848; "Russia's Internet Freedom Deteriorates to a 'Not Free' Rating," *Moscow Times*, October 29, 2015, https://www.themoscowtimes.com/2015/10/29/russias-internet-freedom-deteriorates-to-a-not-free-rating-a50549.

[28] Ksenia Ermoshina et al., "A Market of Black Boxes: The Political Economy of Internet Surveillance and Censorship in Russia," *Journal of Information Technology and Politics* 19, no. 1 (2022): 18–33, https://doi.org/10.1080/19331681.2021.1905972.

[29] "Russia: 'Big Brother' Law Harms Security, Rights," Human Rights Watch, July 12, 2016, https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

[30] "Ukraine's Kherson Switches to Russian Network after Internet Cut-off — Новая Газета Европа," *Novaya Gazeta*, May 2, 2022, https://novayagazeta.eu/articles/2022/05/02/ukraines-kherson-switches-to-russian-network-after-internet-cut-off-news.

[31] Ksenia Ermoshina and Francesca Musiani, "Can Encryption Save Lives? Secure Messaging and Its Infrastructure as Loci of Convergence between Cyber Warfare and Conventional Warfare: The Case of Ukraine," *Media, War & Conflict* 19, no. 1 (2024): 208–25, https://doi.org/10.1177/17506352241297942.

[32] Eda Keremoğlu et al., "Network Topology Facilitates Internet Traffic Control in Autocracies," *PNAS Nexus* 3, no. 3 (2024): pgae069, https://doi.org/10.1093/pnasnexus/pgae069.

[33] Madison Taylor, "Understanding Tier 1 ISPs: A Comprehensive Guide," 123NET, March 28, 2024, https://www.123.net/blog/understanding-tier-1-isps-a-comprehensive-guide/.

[34] Keremoğlu et al., "Network Topology Facilitates Internet Traffic Control in Autocracies."

[35] Keremoğlu et al., "Network Topology Facilitates Internet Traffic Control in Autocracies."

[36] Victoria Klesty et al., "Focus: Military Coup Puts Telenor's Future in Myanmar on the Line," Reuters, May 7, 2021, https://www.reuters.com/business/media-telecom/military-coup-puts-telenors-future-myanmar-line-2021-05-07/.

[37] "Rights Groups Lodge Complaint in Norway Against Telenor Over Myanmar Sanctions," The Irrawaddy, August 29, 2025, https://www.irrawaddy.com/news/burma/rights-groups-lodge-complaint-in-norway-against-telenor-over-myanmar-sanctions.html; Alexander Vittrup, "Telenor Data Transfers Linked to Arrests and Executions in Myanmar," *Scandasia*, August 26, 2025, https://scandasia.com/telenor-data-transfers-linked-to-arrests-and-executions-in-myanmar/.

[38] "Justice For Myanmar and ICJ Norway Filed Complaint with Norwegian Police against Telenor for Violating Sanctions," Justice For Myanmar, August 28, 2025, https://www.justiceformyanmar.org/press-releases/justice-for-myanmar-and-icj-norway-filed-complaint-with-norwegian-police-against-telenor-for-violating-sanctions.

[39] "The Myanmar Junta's Partners in Digital Surveillance and Censorship | Justice For Myanmar," Justice For Myanmar, June 19, 2024, https://www.justiceformyanmar.org/stories/the-myanmar-juntas-partners-in-digital-surveillance-and-censorship; Gideon Ogunniye, "A New Anti-Democratic Tool: The Deep Packet Inspection Technique," Democracy in Africa, May 4, 2023, https://democracyinafrica.org/a-new-anti-democratic-tool-the-deep-packet-inspection-technique/.

[40] Caroline Henshaw and Aung Naing, "Chinese Technology Capable of Mass Surveillance 'installed' by Myanmar Internet Company Funded by UK," Finance Uncovered, May 21, 2025, https://financeuncovered.org/stories/british-norwegian-and-danish-governments-back-internet-provider-in-military-run-myanmar-which-hosts-notorious-chinese-surveillance-system.

[41] "Myanmar: ISP company denied allegations linking to the use of Chinese tech for online surveillance; incl. investors' comments," Business and Human Rights Centre, May 23, 2025, https://www.business-humanrights.org/my/%E1%80%9E%E1%80%90%E1%80%84/myanma

r-isp-company-denied-allegations-linking-to-the-use-of-chinese-tech-for-online-surveillance-incl-investors-comments/.

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