ADVANCING A LIBERAL DIGITAL ORDER

Retooling Democratic Good Governance

The technologies of a more open future in Southeast Asia

Coby Goldberg and Kristine Lee

EXECUTIVE SUMMARY

Online and offline, illiberal governance technologies are proliferating across Southeast Asia. From the strained democracies of Indonesia and the Philippines to the one-party electoral state of Singapore and the military-ruled kingdom of Thailand, Southeast Asian governments are harnessing emerging technologies to more effectively surveil and control their populations. As Chinese technology companies emerge as dominant players in Southeast Asian markets, both shaping and meeting the needs of consumers and their governments alike, the region as a whole is bending toward a less free and open future—one less hospitable to America's long-term commercial interests and democratic values. Yet, instead of acting as a counter-balancing force for democratic governance in the region, American companies are acting as accelerants of trends toward illiberalism and a future in which Southeast Asian governance resembles China. The controversies surrounding the 2020 American election and presidential transition, meanwhile, have undercut the credibility of the United States' ideological messaging across the globe.

Still, Chinese illiberal technology ambitions pose a real long-term threat to the United States' global standing. In order to mitigate that threat, the United States must advance a technology strategy that is not premised on theoretically pristine American systems in opposition to the straw man of Chinese illiberalism, but is instead founded in concrete offerings of competent and democratic governance. This policy brief examines the contours of the emerging digital order in Southeast Asia and, against this backdrop, identifies several notable cases in which civil society and public sector actors have leveraged digital tools to help their governments operate more effectively and transparently. It then draws out specific policy recommendations for the U.S. government to advance digital tools that can backstop both competent governance and the advancement of democracy in the region. These approaches in Southeast Asia will yield critical insights and dividends for the emerging U.S.-China technology competition across the Indo-Pacific, and for any American efforts to support democratic processes abroad, even as it focuses on fixing those processes at home.

THE STATE OF HIGH-TECH ILLIBERALISM IN SOUTHEAST ASIA

Four key trends are driving high-tech illiberalism in Southeast Asia today. First, offline, police departments and local municipalities are importing artificial intelligence-enabled (AI) precision surveillance technologies from China to better track and silence political dissidents and other persona non grata. Second, online, state and non-state actors are abusing inadequately regulated information spaces to disseminate disinformation. Third, governments are addressing the disinformation problem with remedies such as censorship and data localization that further imperil freedom in online information ecosystems. Finally, in response to the COVID-19 pandemic, governments have rolled out a host of new digital tools that, absent basic legal and regulatory frameworks for the protection of civil liberties, act as a force amplifier for illiberal governance. Collectively, these trends are shaping the future trajectory of the region's digital order.

Center for a New American Security

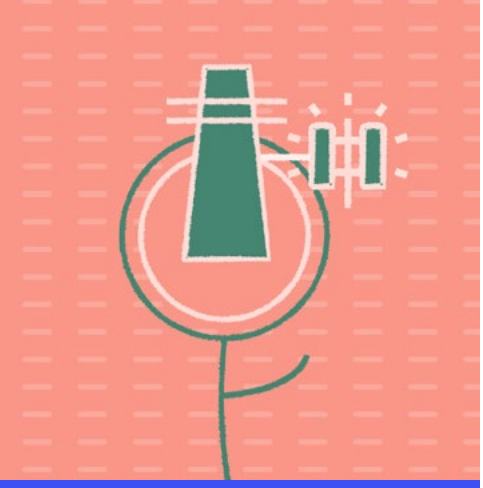
ADVANCING A LIBERAL DIGITAL ORDER

1. **Chinese companies are exporting cutting-edge surveillance technologies to Southeast Asian governments that seek to crack down on both crime and political dissidence.** Chinese facial and voice recognition startups use camera footage and voice prints from China's vast web of surveillance hardware to hone AI-enabled surveillance tools. As Chinese companies perfect these systems at home, they are looking for new markets abroad, both to fulfill commercial objectives and to create external security environments conducive to the Chinese Communist Party's longevity. The Association of Southeast Asian Nations (ASEAN) is China's largest trading partner and has emerged as a focal point of these efforts.[1] A report by the China Academy of Information and Communications Technology, a Chinese state-backed think tank, argues that "strengthening China-ASEAN cybersecurity cooperation could promote the implementation of the Belt and Road initiative while bringing new opportunities to improve the competitiveness of domestic industries."[2]

   On the receiving end of these exports are Southeast Asian governments looking to strengthen public security through enhanced state controls—primarily via Chinese surveillance technology. In Malaysia, the police partnered with Chinese startup Yitu to install facial recognition technology in body cameras.[3] The Philippines contracted China International Telecommunication Construction Corporation and Huawei to install more than 10,000 CCTV cameras across seven cities as part of a "Safe Philippines Project," despite vocal domestic opposition.[4] Nine different countries across Southeast Asia have contracted Meiya Pico, a Chinese digital forensics company, to conduct trainings for police departments.[5]

2. **State and non-state actors alike are manipulating social media sites to spread disinformation, to the detriment of the health of young democracies.** In Indonesia, Facebook's third largest market globally, a group called the Muslim Cyber Army used Facebook and Twitter to peddle conspiracy theories about the Christian governor of Jakarta, Basuki "Ahok" Tjahaja Purnama, which ultimately derailed his 2017 re-election bid and led to his arrest on trumped up blasphemy charges.[6] Despite the game of whack-a-mole the companies engaged in with disseminators of disinformation, fake accounts imperiled the 2019 Indonesian presidential election.[7] In the Philippines, where 97 percent of people with internet access used Facebook in 2019, fake news operations coordinated and funded by Rodrigo Duterte's PDP-Laban Party backed his presidential campaign and continued to fuel his violent anti-drug war once he took office.[8] Facebook belatedly took down hundreds of accounts with links to China, the Philippines Armed Forces, and Duterte's social media strategist in September 2020, arguing they violated its policy on "coordinated inauthentic behavior on behalf of a foreign or government entity."[9]

1. Issaku Harada, "ASEAN becomes China's top trade partner as supply chain evolves" *Nikkei Asia*, July 15, 2020, https://asia.nikkei.com/Politics/International-relations/ASEAN-becomes-China-s-top-trade-partner-as-supply-chain-evolves.
2. "Zhongguo dongmeng wangluo anquan chanye fazhan xianzhuang yanjiu baogao [China-ASEAN Cybersecurity Industry Development Status Research Report]," (zhongguo xinxi tongxin yanjiuyuan [China Academy of Information and Communications Technology], December 2019), http://www.caict.ac.cn/kxyj/qwfb/bps/201912/P020191228471585415832.pdf.
3. Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas, "Mapping China's Tech Giants," (Australia Strategic Policy Institute, April 18, 2019), https://chinatechmap.aspi.org.au/#/map/f1-Malaysia.
4. Mara Cepeda, "De Lima wants Senate probe into China-funded surveillance project," Rappler, January 5, 2020, https://rappler.com/nation/de-lima-senate-probe-china-funded-surveillance-project-philippines; Loreben Tuquero, "QC getting 1,500 CCTV cameras under 'Safe Philippines'," Rappler, December 30, 2019, https://rappler.com/nation/quezon-city-joins-safe-philippines-project-gains-cctv-cameras.
5. Cave et al., "Mapping China's Tech Giants."
6. "Facebook takes down hundreds of Indonesian accounts linked to fake news syndicate," Reuters, January 31, 2019, https://www.reuters.com/article/us-facebook-indonesia/facebook-takes-down-hundreds-of-indonesian-accounts-linked-to-fake-news-syndicate-idUSKCN1PQ3JS; Kate Lamb, "Muslim Cyber Army: a 'fake news' operation designed to derail Indonesia's leader," *The Guardian*, March 13, 2018, https://www.theguardian.com/world/2018/mar/13/muslim-cyber-army-a-fake-news-operation-designed-to-bring-down-indonesias-leader; Kharishar Kahf, "Report unveils Muslim Cyber Army's modus, purpose," *The Jakarta Post*, March 21, 2018, https://www.thejakartapost.com/news/2018/03/21/report-unveils-muslim-cyber-armys-modus-purpose.html.
7. Fanny Potkin and Agustinus Beo Da Costa, "In Indonesia, Facebook and Twitter are 'buzzer' battlegrounds as elections loom," Reuters, March 12, 2019, https://www.reuters.com/article/us-indonesia-election-socialmedia-insigh/in-indonesia-facebook-and-twitter-are-buzzer-battlegrounds-as-elections-loom-idUSKBN1QU0AS.
8. Samantha Bradshaw and Philip Howard, "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation," No. 2017.12 (Oxford Computational Propaganda Research Project, December 2017), http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf; Steven Levy, "How Facebook's News Feed Became A Political Propaganda Machine," *Science Friday*, February 28, 2020, https://www.sciencefriday.com/articles/facebook-fake-news-philippines-elections/; Interview with Mallory Knodel, Zoom, September 1, 2020.
9. Elyssa Lopez, "Philippines: fake accounts shut down by Facebook promoted Duterte and China," *South China Morning Post*, September 23, 2020, https://www.scmp.com/week-asia/politics/article/3102765/philippines-fake-accounts-shut-down-facebook-promoted-duterte; Helen Davidson and Carmela Fonbuena, "Facebook removes fake accounts with links to China and Philippines," *The Guardian*, September 23, 2020, https://www.theguardian.com/technology/2020/sep/23/facebook-removes-fake-accounts-with-links-to-china-and-philippines.



ADVANCING A LIBERAL DIGITAL ORDER

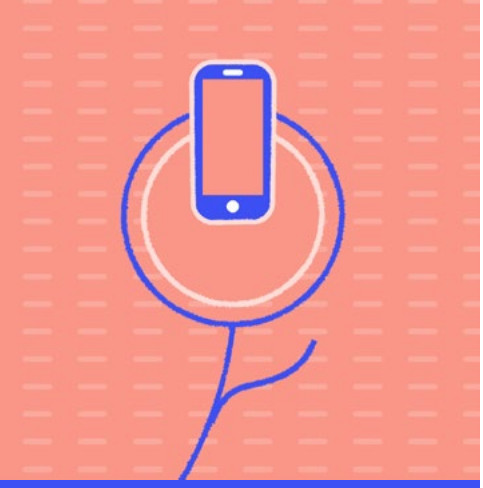
Myanmar's military abused Facebook from 2017–2018 to fuel hatred of the Rohingya, a primarily Muslim minority group that endured what the United Nations (U.N.) deemed "a textbook example of ethnic cleansing." Military personnel, some of whom had received psychological warfare training in Russia, set up fake celebrity news accounts on Facebook to attract followers, built an army of trolls to promote the accounts, and then weaponized the accounts to spread fake news about Muslim rapists and impending terrorist threats. Facebook controls 99.4 percent of the domestic social media market in Myanmar, and is thus a particularly potent means of swaying opinion.[10] By the time the company took action, fake news accounts run by the military had more than one million followers, and 700,000 Rohingya had been driven from the country.[11] U.N. Special Rapporteur on Human Rights in Myanmar Yanghee Lee noted, "I'm afraid that Facebook has now turned into a beast."[12] Disinformation and hate speech continued to flood the platform during Myanmar's 2020 election, even as Facebook increased the number of Burmese-language items it removed from its platform five times over.[13]

3. **Governments are institutionalizing online censorship through new digital norms and legal regimes.** Many governments in the region are all too ready to take advantage of opportunities for clamping down on online speech, and thus cannot be trusted to act as neutral arbiters in the fight against online disinformation. Under the guise of stopping the spread of disinformation on under-regulated online platforms, Southeast Asian governments have implemented heavy-handed digital regulations modeled on Chinese law. Malaysia and Singapore both enacted wide-ranging "fake news laws" that assigned the government the power to define and censor false online speech.[14] Myanmar's government has brought criminal charges against dissidents for critical Facebook posts.[15] Vietnam, drawing on China's concept of digital sovereignty, implemented data localization laws requiring foreign online platforms to supply the government with private user information and to support the government's censorship apparatus.[16]

   These authoritarian tendencies in digital governance have grown sharper in 2020 amid the COVID-19 pandemic. Cambodia used the pandemic as a pretense to arrest opposition lawmakers for statements on Facebook, while Thailand's military junta has invoked emergency powers to crack down on the "abuse of social media."[17]

4. **Civil liberties have atrophied amid regional governments' responses to the COVID-19 crisis.** The COVID-19 pandemic calls for the assertion of state power, but in countries with weak institutions it has allowed for the spread of surveillance technology with limited safeguards.[18] In Southeast Asia, of the six countries that released contact-tracing apps, only Singapore designed one with adequate privacy protections, according to a scorecard that MIT Technology Review developed.

10. "In Myanmar, Facebook struggles with a deluge of disinformation," *The Economist*, October 22, 2020, https://www.economist.com/asia/2020/10/22/in-myanmar-facebook-struggles-with-a-deluge-of-disinformation.
11. Paul Mozur, "A Genocide Incited on Facebook, With Posts From Myanmar's Military," *The New York Times*, October 15, 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.
12. "U.N. blames Facebook for spreading hatred against Rohingya in Myanmar," CBS News, March 13, 2018, https://www.cbsnews.com/news/facebook-un-blames-social-media-giant-for-spreading-hatred-rohingya-myanmar/.
13. "In Myanmar, Facebook struggles with a deluge of disinformation." https://www.economist.com/asia/2020/10/22/in-myanmar-facebook-struggles-with-a-deluge-of-disinformation.
14. J.C. Ong and Ross Tapsell, "Mitigating Disinformation in Southeast Asian Elections: Lessons from Indonesia, Philippines and Thailand," (NATO StratCom Centre of Excellence, May 2020), https://www.stratcomcoe.org/mitigating-disinformation-southeast-asian-elections.
15. Linda Lakhdhir, "Critics of Myanmar Government Facing Prison Time," Human Rights Watch, September 23, 2019, https://www.hrw.org/news/2019/09/23/critics-myanmar-government-facing-prison-time.
16. Dien Luong, "Vietnam's Internet is in trouble," *The Washington Post*, February 19, 2018, https://www.washingtonpost.com/news/theworldpost/wp/2018/02/19/vietnam-internet/.
17. "Cambodia: Covid-19 Spurs Bogus 'Fake News' Arrests," Human Rights Watch, April 29, 2020, https://www.hrw.org/news/2020/04/29/cambodia-covid-19-spurs-bogus-fake-news-arrests; "Thailand: Authorities using repressive laws to intensify crackdown on online critics," Amnesty International, April 23, 2020, https://www.amnesty.org/en/latest/news/2020/04/thailand-authorities-using-repressive-laws-to-intensify-crackdown-on-online-critics/.
18. Kara Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem," (Center for a New American Security, September 3, 2020), https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem.



ADVANCING A LIBERAL DIGITAL ORDER

The Indonesian government's PeduliLindungi app, which had been downloaded 4.6 million times as of July, does not have an open source codebase, has no transparency policies in case of data breaches, and lacks restrictions on the type of data collected and the ways in which its data is used.[19] In Malaysia—where the government launched three different contact-tracing apps, in addition to deploying a fleet of drones to enforce stay-at-home orders—similar concerns about data privacy and protection for contact-tracing apps have gone unanswered by the government.[20] In Thailand, the contact-tracing app MorChana accesses data, including from the phone's camera and device history, that serves no clear contact-tracing function.[21]

Evaluating the data collection practices of Southeast Asian contract-tracing apps

	Voluntary	Limitations on data use	Destruction of data after certain time	Data collection is minimized	Transparent code
Indonesia	Yes	No	No	No	No
Malaysia	Yes	No	Yes	No	No
The Philippines	Yes	No	No	No	No
Singapore	Yes	Yes	Yes	Yes	Yes
Thailand	No	No	No	No	No
Vietnam	Yes	No	No	No	Yes

This table uses the scorecard developed by MIT Technology Review, with supplementary information collected from the Global Privacy Enforcement Network.[22] The MIT Technology Review scorecard looks at the following five measures: (1) Is the app voluntary to download? (2) Are there limits on how the collected data is used? (3) Is the data deleted after a certain timeframe? (4) Does the app only collect data that is directly used for the app's stated purposes? (5) Is the underlying code base transparent?

As these measures indicate, only Singapore's TraceTogether app provides sound protections for civil liberties.

Implications for U.S. interests

As governments across Southeast Asia harness technology toward illiberal ends, the region's strategic environment may grow unfavorable to American values and interests. Chinese technology champions are particularly valuable vectors of geopolitical influence, as they give Beijing significant political leverage and advance the narrative that China's development model is superior to that of free and open systems. Already, citizens of ASEAN states view China as more geopolitically and economically important than the United States, leaving values and ideology as the primary domains in which America holds an edge.[23] Because the 2020 election has undermined faith in the United States' ability to set an example for democracies abroad, the next administration cannot expect a return to the old messaging around democratic ideals to gain traction. Instead, it should

19. Trevor Williams, "Asian Diplomats: Contact-Tracing Apps, Tech Solutions Play Key Role in COVID-19 Fight," Global Atlanta, August 13, 2020, https://www.globalatlanta.com/asian-diplomats-contract-tracing-apps-tech-solutions-play-key-role-in-covid-19-fight/; "Open Letter to KOMINFO Requesting for Strong User Privacy Protections in the PeduliLindungi App," Lembaga Studi and Advokasi Masyarakat [Institute for Studies and Community Advocacy], June 26, 2020, https://elsam.or.id/open-letter-to-kominfo-requesting-for-strong-user-privacy-protections-in-the-pedulilindungi-app/.

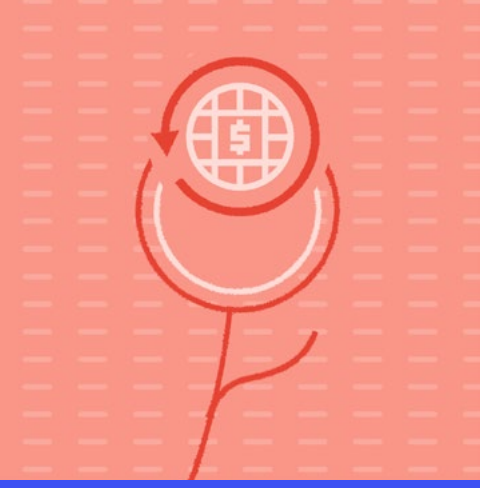
20. Moonyati Mohd Yatid, "Vulnerabilities during pandemic show need for heightened Internet governance," *New Strait Times*, July 22, 2020, https://www.nst.com.my/opinion/columnists/2020/07/610793/vulnerabilities-during-pandemic-show-need-heightened-internet; Moonyati Yatid, Farlina Said, and Tengku Nur Qistina, "Digital surveillance: Privacy, data ecosystem and effectiveness," Malay Mail, May 17, 2020, https://www.malaymail.com/news/what-you-think/2020/05/17/digital-surveillance-privacy-data-ecosystem-and-effectiveness-moonyati-yati/1867050.

21. "Contact tracing apps in Thailand," (Norton Rose Fulbright, May 11, 2020), https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/thailand-contact-tracing.pdf?revision=dd60dd88-ca93-4c6d-bccd-7e24ca41ea0e&la=en; Husai Chantarawirod, "Temporary measure or a long-term violation?," Friedrich Naumann Stiftung, July 31, 2020, https://asia.fnst.org/content/temporary-measure-or-long-term-violation.

22. Patrick Howell O'Neill, Tate Ryan-Mosley, and Bobbie Johnson, "A flood of coronavirus apps are tracking us. Now it's time to keep track of them," *MIT Technology Review*, May 7, 2020, https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/; Kevin Shepherdson, "How intrusive are contact-tracing apps in ASEAN?," Tech in Asia, June 23, 2020, https://www.techinasia.com/intrusive-asean-contacttracing-apps.

23. Michael Green and Amy Searight, "Powers, Norms, and Institutions: The Future of the Indo-Pacific from a Southeast Asia Perspective," (Center for Strategic and International Studies, June 9, 2020), https://www.csis.org/analysis/powers-norms-and-institutions-future-indo-pacific-southeast-asia-perspective.

Center for a New American Security



ADVANCING A LIBERAL DIGITAL ORDER

adopt a practical, technology-driven approach to supporting electoral processes and good government.

The spread of digital authoritarianism also threatens the prospects of American technology companies operating in ASEAN, America's fourth largest trading partner.[24] In the long-term, the commercial success of American technology companies operating in the region is contingent on the presence of open digital ecosystems and the prevalence of liberal norms around the use of technology. As Chinese-style digital sovereignty gains currency, more American companies will be forced to choose between their bottom lines and their values. The United States should seek to prevent such a future.

FOUR SNAPSHOTS OF LIBERAL USES OF TECHNOLOGY

Although technology is undoubtedly being applied toward illiberal ends in Southeast Asian governance, there are bright spots, too. In some cases, governments, civil society, and citizens within these countries have deployed select technologies to bolster competent and more democratic governance. The cases offer insights into the ways in which the United States and its allies can partner with stakeholders in Southeast Asia to advance an alternative, more open vision of technology-enabled governance in the region.

1. Crowdsourcing election transparency: Indonesia

The challenge: Building trust in electoral outcomes in a young, sprawling democracy.

With 193 million voters using 810,000 polling stations across hundreds of islands, Indonesian elections are the most complex in the world.[25] The official election results take two weeks to process, as tallies from local polling stations gradually work their way up the chain to the regional and, finally, national counting systems.[26] During this period after election night, conspiracy theories abound. Candidates in a closely contested vote are liable to cry foul play. In 2014, when both of the leading presidential candidates claimed victory on election night, the country's young democracy seemed on the brink of crisis.[27]

The solution: Use a crowdsourced data analysis system to provide live election results.

In response to the claims of miscounts on both sides, an Indonesian data engineer working for a Singapore-based tech company created Kawal Pemilu, or "guard the election." Kawal Pemilu's team of volunteers digitized the raw vote totals coming in from local polling stations to provide an independent means of verifying the numbers reported by local election officials as tallies were slowly sent up the chain of command.

Keys to success:

— Open information laws allowed for independent vote tallies to be conducted using raw data.

— Organizers drew on the human capital that multinational tech companies provided to bring a large group of coders together.

24. Jack Myint, "Annual US Exports in Goods and Services to ASEAN Total over $105 Billion," US-ASEAN Business Council, July 22, 2019, https://www.usasean.org/why-asean/trade-and-investment.
25. Ben Bland, "The World's Most Complicated Single-Day Election Is a Feat of Democracy," *The Atlantic,* April 15, 2019, https://www.theatlantic.com/international/archive/2019/04/indonesias-elections-are-feat-democracy/587143/.
26. Arie Purwanto, Anneke Zuiderwijk, and Marijn Janssen. "Citizen engagement in an open election data initiative: a case study of Indonesian's 'Kawal Pemilu'," *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age,* 62 (May 2018), https://dl.acm.org/doi/10.1145/3209281.3209305.
27. "Election dispute emerges as serious test for Indonesia," *The Financial Times,* July 14, 2014, https://www.ft.com/content/d14ad11c-0b1e-11e4-9e55-00144feabdc0.

2. Democratizing information access: Malaysia

The challenge: Providing trusted alternative information platforms to state media.

For a long time, Malaysian elections offered voters a choice at the ballot without giving them real say over who held power. Extreme gerrymandering ensured that even if the opposition won the majority of votes, the ruling party could hold on to 60 percent of the seats in parliament.[28] Tight control over the state television broadcasters and newspapers, which 57 percent and 41 percent of Malaysians, respectively, turned to for news in 2018, kept the opposition out of the spotlight.[29] The 2018 elections were expected to be no different.[30] When the results came in, the opposition and ruling party alike were shocked to find that after 60 years in power, the ruling Barisan Nasional coalition had been swept out of office.

The solution: Democratize information access in rural areas outside of the digital divide.

The result was, in large part, due to increased mobile phone penetration in rural areas that were traditional strongholds of government support. By 2018, 77 percent of Malaysians said that their primary news access came via smartphone, mostly through Facebook or WhatsApp.[31] Using these apps, habitual government supporters could watch opposition rallies or become consumers of information about government corruption.[32] Though the disinformation risks present in open online information ecosystems are well-documented, when put in the hands of traditionally disenfranchised groups living under tightly controlled media and political systems, basic information access technologies have the potential to be a democratizing force.

Key to success:

— A well-established technology was put in the hands of people long left outside of digital divides.

3. Open data for transparent government: Indonesia

The challenge: Using open data laws to make government more accountable.

Indonesia and the Philippines are both founding members of the Open Government Partnership (OGP), and as such are officially committed to making government data freely accessible to the public. Theoretically, such commitments enable watchdog groups to monitor government spending. In practice, however, government departments have a tendency to adhere to these programs in letter rather than in spirit, flooding the public with data that is not easily turned into actionable information.

The solution: Work with civil society and government to align on open data needs.

The World Wide Web Foundation created the Open Data Lab in Jakarta to serve both as an incubator for startups that make use of government data, and as a training hub for established civil society groups to learn how to make use

28. "What's Malay for gerrymandering?," *The Economist*, August 9, 2014, https://www.economist.com/asia/2014/08/09/whats-malay-for-gerrymandering.
29. Ross Tapsell, "The Smartphone as the 'Weapon of the Weak': Assessing the Role of Communication Technologies in Malaysia's Regime Change," *Journal of Current Southeast Asian Affairs*, 37 no. 3 (2018), https://journals.sagepub.com/doi/pdf/10.1177/186810341803700302.
30. "How Malaysia's next election will be rigged," *The Economist*, March 8, 2018, https://www.economist.com/asia/2018/03/08/how-malaysias-next-election-will-be-rigged; Trinna Leong and Nadirah Rodzi, "Electoral maps for upcoming Malaysia election passed in Parliament," *The Straits Times,* March 28, 2018, https://www.straitstimes.com/asia/se-asia/malaysian-premier-najib-razak-presents-highly-criticised-new-electoral-maps.
31. Nic Newman, "Reuters Institute Digital News Report 2018," (Reuters Institute, 2018), http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf.
32. Tapsell, "The Smartphone as the 'Weapon of the Weak': Assessing the Role of Communication Technologies in Malaysia's Regime Change."

of data. The Open Data Lab also launched a program with U.S Agency for International Development (USAID) support that brings local governments available for the latter's purposes.[33]

Keys to success:

— Existing civil society groups were retooled through capacity building initiatives to serve as data watchdogs.

— New programs were established to build innovation ecosystems responsive to publicly available government data.

— Local governments were targeted as stakeholders in a win-win data publication process, allowing for progress despite a recalcitrant national government.

4. Fighting COVID-19 without violating privacy: Singapore

The challenge: Tracking people's movement to prevent COVID-19 transmission without violating civil liberties.

A strong government response to COVID-19 need not mean an authoritarian government response to COVID-19, but authoritarian countries have tried to conflate the two. China's Health Code app, for example, was mandatory to download, shared information with the police, and might become a permanent feature of public health ecosystems in some municipalities.[34] China has sought to cast such a response as the most effective means of controlling COVID-19.[35]

The solution: An open source, voluntary use contact-tracing app.

In March, Singapore released TraceTogether, the world's first Bluetooth-enabled contact-tracing app. The app would notify people if they had crossed paths with someone who later tested positive for COVID-19, but did so without violating civil liberties. Indeed, it drew praise for being voluntary to download, destroying its data after a pre-set amount of time, and running on an open source software made available on GitHub.[36]

Keys to success:

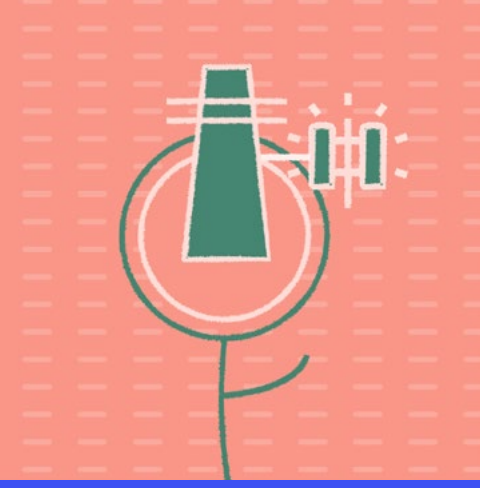
— An open-source code base.

— Strict privacy rules paired with explicit limits on the type of data collected and on how that data can be used and shared.

RECOMMENDATIONS FOR THE U.S. GOVERNMENT

These four cases demonstrate how local innovation is rising to meet the technological needs of the region in ways that also support more democratic and competent governance. Washington can use these technologies to work with the private sector and partner countries to set the Indo-Pacific on the path to a more free and open future. Doing so requires that the U.S. government advance a strategy that is informed by facts on the ground and offers concrete alternatives to Chinese illiberal technology ambitions with attractive upside value for local governments that will be more interested in performance outcomes than democratic outcomes.

33. "Starting Conversations Between Citizens and the State with Open Data," (The World Wide Web Foundation, August 20, 2015), http://labs.webfoundation.org/wp-content/uploads/2015/09/Lessons-Learned-FOIODAceh.pdf.
34. Paul Mozur, Raymond Zhong, and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags," *The New York Times*, March 1, 2020, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html; Liza Lin, "China's Plan to Make Permanent Health Tracking on Smartphones Stirs Concern," *The Wall Street Journal*, May 25, 2020, https://www.wsj.com/articles/chinas-plan-to-make-permanent-health-tracking-on-smartphones-stirs-concern-11590422497?mod=tech_lead_pos4.
35. Vivian Wang, "China's Coronavirus Battle is Waning. Its Propoganda Fights is Not," *The New York Times*, April 8, 2020, https://www.nytimes.com/2020/04/08/world/asia/coronavirus-china-narrative.html.
36. Mary Hui, "Singapore wants all its citizens to download contact tracing apps to fight the coronavirus," Quartz, April 21, 2020, https://qz.com/1842200/singapore-wants-everyone-to-download-covid-19-contact-tracing-apps/; "OpenTrace," GitHub, https://github.com/opentrace-community.



The following principles and recommendations outline ways for American policymakers to engage key allies and stakeholders to advance a more liberal vision for the region's digital future.

Principle 1: Foster civic technology innovation both domestically and in contested spaces.

Leverage public research funding to design privacy-protecting technology alternatives to the Chinese technology toolkit. Government research dollars—namely from the Defense Advanced Research Projects Agency, the Intelligence Advanced Research Projects Activity, and In-Q-Tel—should fund preliminary research into privacy-by-default technologies.[37] To best target such funding toward developing alternatives to Chinese surveillance technology, these agencies could draw on existing government mechanisms for tracking Chinese technology transactions abroad, and, when a transaction is identified for a tool without a clear safer option, fund research into privacy-protecting alternatives. For example, by funding basic research into technological detection solutions to online disinformation campaigns that program ethics into online content moderation, the government could help kickstart greater efforts from industry to build tools that combat disinformation without recourse to heavy handed Chinese norms.

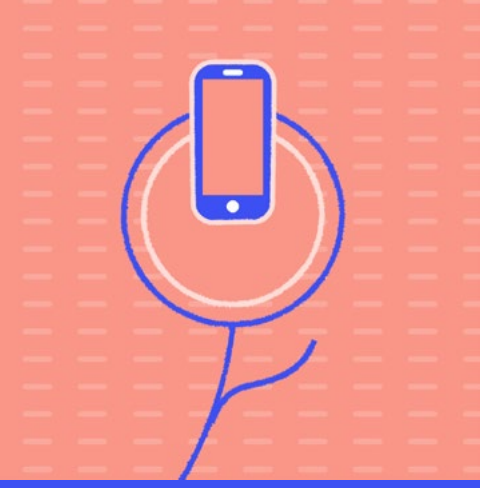
Work with key allies to foster innovation within partner markets to meet particular regional, national, and local civic technology needs. Working with the Taiwanese Digital Ministry to replicate the model of the Taiwanese Presidential Hackathon, the State Department Bureau of Global Public Affairs should build out civic tech hackathons in Southeast Asian technology hubs to promote and amplify civic technology entrepreneurship in the region. The U.S. International Development Finance Corporation should partner with the European Union's GovStart to establish social impact startup incubators in key contested technology ecosystems. It could also build on American private sector projects already underway in the region, for example by partnering with Google's Southeast Asia Startup Accelerator, in order to use American private sector investments as a conduit for shaping open, socially minded innovation ecosystems.

Principle 2: Work with American social media companies to protect democracy abroad.

Partner with Facebook on combating disinformation in fragile democracies. In the run-up to elections in young democracies abroad, the Department of Commerce's Digital Attachés and other consulate representatives should organize regular meetings between regional Facebook offices and local civil society groups or academics. Use these dialogues, which would marry Facebook's access to high level views of its own platform with local representatives' understanding of the online information ecosystem, to identify key nodes in local disinformation systems.[38] Facebook has begun to take its role in elections and information ecosystem integrity more seriously, everywhere from the United States to Myanmar.[39] But in order to make American social media platforms forces for democracy abroad, the U.S. government should play a more active role in working with them to prevent platform abuse.

Develop a sharper understanding of the impact Facebook and Twitter have on young democracies through future congressional hearings. Washington and Brussels understandably focus their attention more squarely on social media's role in established, Western democracies, but this has been to the neglect of an easier and potentially more impactful opportunity to combat disinformation in some of the world's most fragile democracies. Policymakers should leverage congressional briefings to ask what steps leading technology companies are taking to ensure

37. Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem."
38. Interview with Ross Tapsell, Zoom, August 19; Interview with Mallory Knodel, Zoom, September 1.
39. Rafael Frankel, "How Facebook Is Preparing for Myanmar's 2020 Election," Facebook, August 31, 2020, https://about.fb.com/news/2020/08/preparing-for-myanmars-2020-election/.



that their platforms cannot be abused by malign forces as they were during the Rohingya genocide. These instances of digitally enabled hate should not be addressed on a case-by-case basis. Instead, tech companies should adopt comprehensive action plans for preempting future crises.

Principle 3: Use multilateral governance bodies and broadened alliance frameworks to build out shared norms with allies and key digital swing states.

Identify priority partners for making coordinated investments in building more open digital ecosystems in contested spaces like Southeast Asia on a country-by-country basis. India, France, Germany, Japan, South Korea, Taiwan, the Netherlands, and the United Kingdom all have or are developing strategies for engaging the Indo-Pacific. Partnerships will not be one size fits all. For example, while India's relationship with the military makes it a valuable partner in Myanmar, South Korea's burgeoning ties with Vietnam make it the most suitable partner for digital initiatives there.[40]

Double down on investments in regional cybersecurity initiatives that can shape emerging regulatory systems. Through partnership with the ASEAN-Singapore Cybersecurity Centre of Excellence, for example, create a center which regional policymakers can use to design and implement digital regulations.

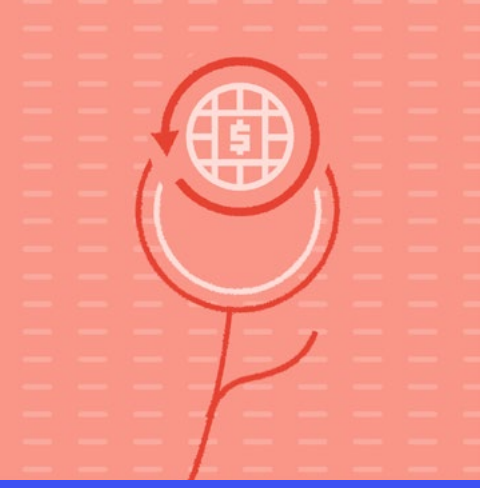
Build mechanisms into any future D-10 grouping for engaging key digital swing states on building shared norms and platforms. The U.S. government should use the OGP's Peer Learning and Exchange Subcommittee and the 2021 OGP Summit to advance formal processes for technology exchanges between young democracies.[41] These efforts could then seek to create a more united front with countries like Indonesia, Malaysia, the Philippines, and Singapore, which can, in turn, form the base of a broader coalition at international standards bodies, such as the International Telecommunication Union, and can advance shared principles at the regional level through programs like the ASEAN Smart City Initiative.

Principle 4: Digitally empower the traditionally disempowered.

Establish a standalone Digital Rights Fund to build digital capacity among civil society groups. A whole-of-government technology diplomacy program will, by necessity, require that the United States engage governments without strong democratic institutions. A Digital Rights Fund, run through USAID, would empower local civil society groups to play watchdog roles, keeping checks on expanded digital governing powers.[42] The Digital Rights Fund can also support programs, modeled on the Open Data Lab in Jakarta, that bring a broader range of community stakeholders into government deliberations on digital programs to maximize programmatic impact. As governments seek to roll out new financial technologies for reaching unbanked communities, for example, civil society organizations will play a pivotal role between the government and local communities, ensuring that civil liberties are adequately protected and that local needs are effectively met as governments expand their digital footprints.[43]

Bring new technologies and innovation capacity to non-urban communities. Through the State Department's Bureau of Democracy, Human Rights, and Labor or the Global Engagement Center, work with initiatives like the U.S. Open Technology Fund to get digital tools into the hands of people traditionally outside of the digital divide and, in countries with more closed information ecosystems, support technologies of free information access like VPNs.

40. Interview with John Dale, Zoom, September 4.
41. Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem."
42. We are indebted to Steve Feldstein for this point; see also, Siddharth Mohandas, Kristine Lee, Joshua Fitt, and Coby Goldberg, "Designing a U.S. Digital Development Strategy," CNAS, September 10, 2020, https://www.cnas.org/publications/commentary/designing-a-u-s-digital-development-strategy/.
43. Julianna Lai, "On the Fast Track: The Rise of Digital Welfare States in the Philippines and Indonesia," (Center for Strategic and International Studies, September 22, 2020), https://www.csis.org/blogs/new-perspectives-asia/fast-track-rise-digital-welfare-states-philippines-and-indonesia.



CONCLUSION

If current trends in Southeast Asian governance continue to accelerate, allowing Chinese surveillance technologies to proliferate and freedom of the net to wither, the United States will find its star fading not only among the ASEAN states, but across the Indo-Pacific. The United States needs to work with allies and key stakeholders in the private sector and civil society to advance alternative technologies that support good governance and shape the region's strategic environment to its advantage. No silver bullet technology will make the region as a whole more democratic—nor is it entirely productive to frame U.S. engagement with the region in terms that pit democracy against authoritarianism. But with a more calibrated and holistic strategy for promoting the technologies of effective and open government, the United States can help build a freer and more open future for the Indo-Pacific.

ABOUT THE AUTHORS

Coby Goldberg is the Joseph S. Nye Intern with the Asia-Pacific Security Program at CNAS. He recently graduated summa cum laude and Phi Beta Kappa from Princeton University, with a BA in East Asian studies. Goldberg spent one semester in the philosophy department at Tsinghua University, Beijing, and previously interned with a China-cross border strategic advisory firm in New York and a migrants' rights organization in Thailand.

Kristine Lee is an Associate Fellow with the Asia-Pacific Security Program at CNAS, where her research focuses on U.S.-China relations, U.S. alliances and partnerships in the Indo-Pacific region, and managing the North Korean nuclear threat. Lee was granted a Fulbright fellowship and earned a BA in history and literature with a language citation in Mandarin Chinese from Harvard College, where she served as the editor-in-chief of the *Harvard International Review*. She also earned an MPP degree from the Harvard Kennedy School. In June 2019, Lee was named as a recipient of the 1LT Andrew J. Bacevich Jr., USA Award.

This policy brief was made possible by support from the Open Society Foundations and the Quadrivium Foundation. The authors are grateful to John Dale, Mallory Knodel, Glenn Maail, and Ross Tapsell for sharing their perspectives in interviews. We are particularly indebted to Hunter Marston for his review of this paper. Finally, this paper would not have been possible without assistance from a variety of CNAS colleagues, including Melody Cook, Joshua Fitt, Allison Francis, Daniel Kliman, Maura McCarthy, Jake Penders, Ely Ratner, and Emma Swislow. The views presented here do not represent those of CNAS or any other organization, and the authors are solely responsible for any errors in fact, analysis, or omission.