

# Double-Edged Sword

## China's Sharp Power Exploitation of Emerging Technologies

by Samantha Hoffman



#SALMANQADIR



National Endowment  
for Democracy  
*Supporting freedom around the world*

*forum*  
International Forum for Democratic Studies

## EXECUTIVE SUMMARY

Emerging technologies offer numerous conveniences and capabilities, benefitting consumers and governments alike; however, they also carry inherent risks that can threaten liberal democracies when leveraged by powerful dictatorships that wish to reinforce and spread their authoritarianism.

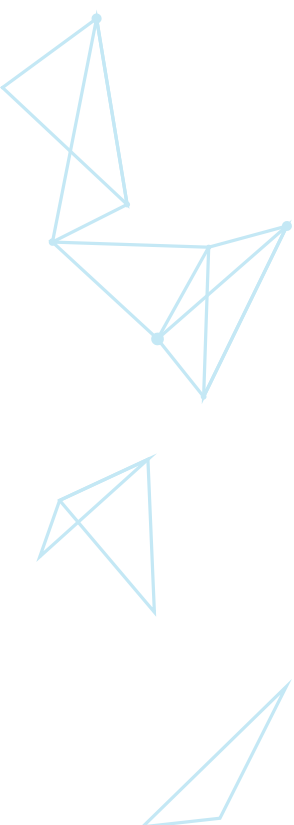
The People's Republic of China (PRC) leverages emerging technologies to undercut democracies' stability and legitimacy, while expanding its own influence. Beijing exerts "sharp power" that enables it to limit access to information, distort political environments, and undertake censorship and surveillance. In this new context, it is important to consider how Beijing seeks to harness emerging technologies as a double-edged sword to protect and expand its own power by shaping, managing, and controlling its domestic and global operating environments.

The PRC's development and global export of "smart cities" technology reveals the character of tech-enhanced sharp power and authoritarianism. The Chinese Communist Party (CCP) uses these technologies to monitor their populace and control society. It does not clearly distinguish basic public goods, for example traffic safety or the prevention of violent crime, from the authoritarian suppression of pluralism and dissent. The CCP blends the two together, prioritizing regime security over essential rights. Furthermore, governments around the world are often eager to adopt smart cities technologies, and the implications of reliance on such PRC-based, globally applicable surveillance systems are serious.

Beijing takes an active role in international standards-setting for emerging technologies. Participation in the development and design of such technologies enables the PRC to exploit emerging technologies to enhance sharp power capabilities. For instance, the China Standards 2035 plan calls for the global export of PRC standards for emerging technologies, and for PRC standards to be accepted through international standards-setting bodies. If PRC-originated technical standards are adopted internationally, PRC-made systems will enjoy greater interoperability and market access around the world, with implications for democratic integrity.

To combat PRC sharp power in the technology domain, civil society should consider the following:

- **Encourage public discourse on liberal democratic values and technology** to better understand the threat sharp power poses, including through digital literacy programs. Civil society organizations should be trained on issues related to emerging technologies, allowing them to help deliver educational programming on best practices for data security. For instance, digital literacy programs could be designed to go beyond basic personal and corporate data-management practices, to include discussion on the geopolitical dimension of the issues and the ways in which seemingly harmless data collection can be abused.
- **Civil society groups must actively participate in international standards-setting bodies**, including the ITU, ISO, and IEC, to contribute to the creation of standards for technologies like 5G and IoT devices and counter harmful PRC efforts to do the same. Civil society organizations can push for transparency around the development of technical standards for technologies that may negatively affect civil liberties, like facial- or voice-recognition systems.
- **Media and civil society organizations should coordinate to expose and amplify indicators of tech-enabled sharp power in their countries**, which would contribute to broader public awareness of the issues, encourage debate on what should be done, and pressure governments to take protective action.



**E**merging technologies are reshaping the ways in which humans interact with their environment, businesses deliver services, and governments solve problems. While these technologies—including “big data” tools, integrated urban-management systems known as smart cities, and the so-called Internet of Things (IoT)—offer a variety of conveniences and practical capabilities, they also carry inherent risks. The danger arises not just from the intent of the actor introducing the technology or its original purpose, but also from the intent of any actor who obtains access to the data that the technology generates. There is always a possibility that this information will be used for purposes beyond those for which it was initially collected, and the threat only grows in the absence of democratic oversight.<sup>1</sup> When authoritarian governments become involved, with their particular interests and legal or normative standards, emerging technologies have the potential to seriously undermine democratic practice.

The world's authoritarian regimes, while sharing key characteristics, vary significantly in their respective methods and stated aims.<sup>2</sup> Rather than attempting to describe them all, this paper focuses on the People's Republic of China (PRC) to explain the full scope of risks that emerging technologies pose to a liberal democracy when leveraged by a powerful regime with the explicit goal of transforming the world to accommodate its authoritarianism.<sup>3</sup> The national security implications of China's technological rise have been well documented,<sup>4</sup> and democratic governments have begun to take measures intended to address it, but the threat to democratic norms and institutions has not yet been fully examined. The PRC is at the forefront of global debate on the political risks associated with emerging technologies by necessity, as it is home to many leading companies that are exporting their products globally. Even though a number of these PRC-based companies are nominally private, their right to operate in China—and their success—is ultimately dependent on their willingness and ability to serve the interests of the Chinese Communist Party (CCP).<sup>5</sup>

The CCP's use of technology to expand its power and influence is best described as tech-enhanced authoritarianism. Rather than creating fundamentally new ways of controlling populations, technology augments the party's longstanding methods of exercising authoritarian dominance. To date, the global repercussions of the PRC's tech-enhanced authoritarianism have been vastly underestimated, with analysts often focusing on coercive measures and inherently invasive surveillance while failing to account for how technologies that contribute to everyday problem-solving and public service provision can simultaneously expand authoritarian power.

Overly narrow approaches to risk assessment have contributed to an equally narrow public debate in and among liberal democracies. For example, discussions about banning the Chinese telecommunications giant Huawei from constructing fifth-generation (5G) mobile networks have fixated on such companies as potential vehicles for PRC espionage. But the bulk data collection that companies like Huawei engage in as a normal business activity can facilitate a range of other practices that undermine liberal democratic interests. For instance, increased collection of high-quality data can improve the accuracy of facial- and voice-recognition systems, sentiment analysis, or relationship mapping. Authoritarian governments are not the only ones seeking to develop these capabilities, but the likelihood that a liberal democracy's regulatory system will be able to effectively police the collection and use of data is greatly diminished when the company in question is based in an authoritarian state.

In a geopolitical context, these risks are amplified by the fact that some autocracies seek to leverage technology for their wider efforts to undercut democracies' stability and legitimacy, and to expand their own global influence. In both direct and indirect ways, technology contributes to the projection of authoritarian power, which is neither clearly “soft power” nor “hard power,” but is instead best described as “sharp power.” According to Christopher Walker and Jessica Ludwig, sharp power “is not principally about attraction or persuasion; instead, it centers on distraction

and manipulation.” Unlike soft power, sharp power “pierces, penetrates, or perforates the political and information environments in the targeted countries.”<sup>6</sup> It also seeks to “limit free expression and to distort political environments.”<sup>7</sup> Technology can serve as a tool of sharp power directly when it is used for censorship and surveillance, or as a platform to conduct information operations. More indirectly, technology enhances the ability of authoritarians to understand the audiences it seeks to influence, or to project sharp power and improve other toolkits for doing so. To understand the ramifications, it is important to consider how Beijing seeks to harness emerging technologies to protect and expand its own power by shaping, managing, and controlling its domestic and global operating environments.

## CHINA'S TECH-ENHANCED AUTHORITARIANISM: SMART CITIES TECHNOLOGIES

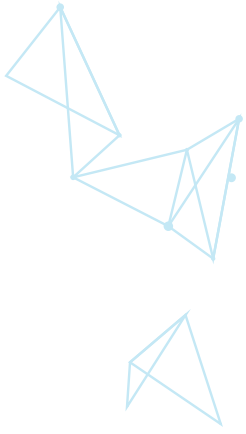
The PRC's domestic development of smart cities, and Chinese companies' global export of related products and services, show what tech-enhanced authoritarianism looks like in practice. The phenomenon is best understood through the CCP's concept of “social management” (or “social governance”). This term refers to the leadership's attempts to shape, manage, and control society—and the party's own members—using both cooperative and coercive means. Notably, the same concept can be found in the CCP's approach to global governance; under party leader Xi Jinping, the phrase “international social management” has been used to describe how the regime seeks to assert a similar level of control over its global operating environment.<sup>8</sup>

Smart cities entail the use of digital technologies like “IoT sensors, video cameras, social media, and other inputs [to] act as a nervous system, providing the city operator and citizens with constant feedback so they can make informed decisions.”<sup>9</sup> The idea behind smart cities—no matter where they are located—is to leverage existing and emerging technologies to improve the efficiency and quality of urban services. In addition to data-collection devices and surveillance cameras, smart cities technologies also include data-visualization platforms, real-time data processing tools, and cloud storage platforms.

The ability of smart cities technologies to enhance and streamline service provision can obscure their invasiveness and advancement of political control, eliciting cooperation from users who are focused on immediate and tangible benefits rather than (typically) less immediate drawbacks. In China, smart cities are the latest in a long series of e-government efforts dating back to the early 1990s, when the so-called Golden Projects were launched in order to “build and streamline information systems, and connect agencies to improve their operational capacity.”<sup>10</sup> These and other initiatives, like “grid management,” were focused not only on enhancing public security, but also on improving everyday governance, making bureaucracy more efficient, and solving problems before they emerged. All were linked more broadly to the CCP's social management concept.<sup>11</sup> Today's smart cities are also associated with two related and ongoing public security projects called Skynet, launched in 2005, and Sharp Eyes, launched in 2015.<sup>12</sup> Skynet refers to video monitoring equipment, mostly at major intersections, police checkpoints, and other public locations. It relies on the use of Geographic Information System (GIS) mapping, image gathering, transmission, and other technologies to improve real-time monitoring and information recording.<sup>13</sup> Sharp Eyes is a more advanced version of Skynet that also builds on Skynet infrastructure,<sup>14</sup> and has focused on installing platforms for the sharing of video image information and establishing rural comprehensive-management centers. Sharp Eyes feeds into work on state security, counterterrorism, enhanced logistics, security supervision, and the prevention and control of criminal activity.<sup>15</sup>

**The ability of smart cities technologies to enhance and streamline service provision can obscure their invasiveness and advancement of political control, eliciting cooperation from users who are focused on immediate and tangible benefits rather than (typically) less immediate drawbacks.**





From the standpoint of the CCP, everyday provision of basic public goods like traffic safety or the prevention of violent crime, and the projection of authoritarian power, including the suppression of dissent, operate in tandem. Concepts like social management effectively blend the two together, while prioritizing regime security over the rights and security of the public.<sup>16</sup> For instance, a smart electricity meter can improve accuracy, transparency, and reliability of readings, to the benefit of the utility and its customers.<sup>17</sup> For police, the data from that same meter may help detect “abnormal” behaviors that could be indicative of “illegal” gatherings. It is noteworthy that smart cities technologies are deployed most coercively in the Xinjiang and Tibet Autonomous Regions, where ethnic Uyghur and Tibetan populations are victims of gross human rights violations. Research from Human Rights Watch has described how authorities in Xinjiang are building the Integrated Joint Operations Platform to aggregate data on individual behaviors and flag “those deemed potentially threatening.”<sup>18</sup>

Given these abuses, it can be easy to forget that smart cities projects had emerged much earlier in other regions across the country, in a less visibly coercive form.<sup>19</sup> Beyond surveillance, smart cities technologies are designed to create a more “service-oriented” government. This remit requires improving intragovernmental coordination, with respect to both policies and technical standards, and increasing the overall functioning of government.<sup>20</sup> The CCP regime, just like any government, must solve everyday problems, and smart cities equipment contributes to this work. For instance, “city brain” systems integrate data from government departments to help improve traffic management.<sup>21</sup> Smart transportation systems seek to combine information technology, telecommunications, navigation and positioning technology, and other capabilities to improve transportation networks.<sup>22</sup> City brain systems monitoring traffic flows can even be used to improve the response times of police, paramedics, or firefighters. In addition, services like geofencing—virtual boundaries around physical locations—can be used for everything from targeted advertising to tracking the movements of a person or vehicle.<sup>23</sup> The same technology can be leveraged to help manage a natural disaster, a public health crisis, or serious civil unrest.

**From the standpoint of the CCP, everyday provision of basic public goods like traffic safety or the prevention of violent crime, and the projection of authoritarian power, including the suppression of dissent, can operate in tandem.**

Governments in developing countries are often particularly eager to adopt similar smart cities solutions as a way of both modernizing governance and enhancing security. To support the development of smart cities projects in Africa, Huawei was reported in 2018 to have set up a US\$1.5 billion fund to “improve urban traffic and air quality, promote energy efficiency in buildings, improve the management of other flows (including waste and water) and make healthcare and health services intelligent.”<sup>24</sup> In some places, Huawei’s projects have been explicitly linked to surveillance and political security. According to a 2019 *Wall Street Journal* report, Huawei helped to build eleven public security monitoring centers in Uganda, and the company’s technicians were found to have assisted with Ugandan intelligence agents’ requests to conduct surveillance targeting prominent opposition politicians.<sup>25</sup> Other smart systems are more explicitly linked to the provision of services. In Egypt, Chinese media reported in mid-2020 that Huawei was in discussions with the Ministry of Electricity on transforming the country’s electricity network into a smart grid to optimize power management.<sup>26</sup> Similarly in 2017, Nigeria’s Ministry of Communications said it would partner with Huawei on the development of smart cities to “promote open data and help manage government resources which in turn helps to get more revenue for the government.”<sup>27</sup> Regardless of their original purpose or intent, however, all of these technologies could come to serve a coercive purpose—just as they do in the PRC—if left without effective democratic oversight.

No matter where data are collected, they can support the coercive use of technology in other settings. Data analytics and artificial intelligence (AI) depend on large inputs

of high-quality data.<sup>28</sup> Facial-recognition technology, for example, grows more accurate when it is trained on a larger volume and greater diversity of facial images. In 2018, the government of Zimbabwe signed an agreement with the PRC firm CloudWalk to build a national facial-recognition database and monitoring system.<sup>29</sup> As part of the deal, Zimbabwe agreed to send biometric data of its own citizens to the PRC to improve the CloudWalk system's ability to recognize faces among different racial and ethnic groups, which in turn would make the company more globally competitive.

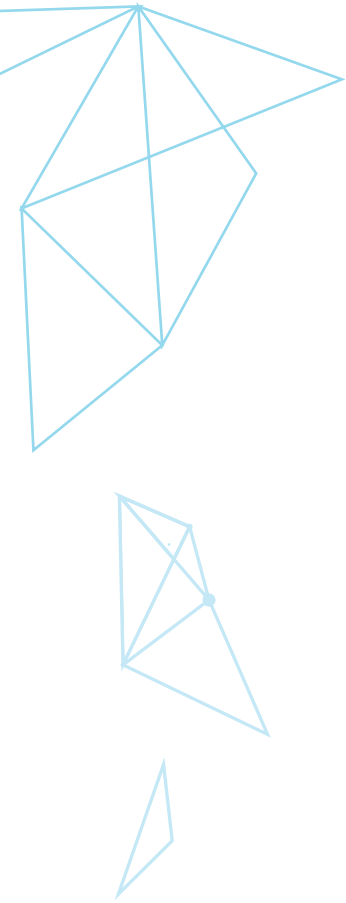
The implications of such PRC-based, globally applicable AI systems are serious, especially if the Chinese authorities work with law enforcement in other countries. Huawei has described how its project in Serbia was “inspired” by an incident in which the suspect in a deadly 2015 hit-and-run car accident in Belgrade fled to China, where he was identified and arrested within three days thanks to the PRC’s advanced facial-recognition technology.<sup>30</sup> Given that the CCP already harasses exiles and dissidents overseas and disregards the legal citizenship of Chinese-born or ethnic Chinese foreign nationals,<sup>31</sup> it is plain to see how similar law enforcement partnerships, with the aid of smart surveillance systems, could be exploited in other contexts. For instance, Huawei and leading Turkish mobile provider Turkcell have signed numerous agreements, including a smart cities urban-management cooperation agreement.<sup>32</sup> There is already notable law enforcement cooperation between Turkey and China,<sup>33</sup> and new technical links could further endanger the large population of Uyghurs living in exile in Turkey.<sup>34</sup> In many documented cases, Turkish authorities have facilitated the forced repatriation of Uyghurs to the PRC.<sup>35</sup>

Even when these technologies are exported to municipalities in established liberal democracies, such as Valenciennes in northern France or Duisburg in Germany,<sup>36</sup> where there is a lower risk of intentional misuse, there are still a number of problems associated with the acceptance of systems designed for use in an authoritarian state. Liberal democracies’ adoption of these technologies could help normalize their uptake in countries with weaker legal and regulatory safeguards. The products could also enable direct restrictions on freedom of speech by the CCP for individuals who might otherwise be protected by democratic institutions. For example, the 2020 National Security Law imposed on Hong Kong by the central government in Beijing criminalizes separatism, subversion, terrorism, and collusion with foreign powers, even if the suspect is located abroad.<sup>37</sup> This law could expose Hong Kongers, Chinese nationals, and others studying at foreign universities to criminal liability for their speech on related topics, particularly if they are forced to pursue their studies from within the PRC due to COVID-19 travel restrictions. In the United Kingdom, some universities were reported to be running a pilot project with an Alibaba Cloud online teaching tool that complies with PRC laws and regulations on content and content moderation.<sup>38</sup> Even if this specific project is not pursued further, universities in democracies must still somehow contend with PRC laws when communicating with their PRC-based students during the pandemic.

## REGIME INSECURITY: UNDERSTANDING THE MOTIVES BEHIND CCP TECH INITIATIVES

To appreciate the challenge that technology as a tool for sharp power projection represents, democratic governments must recognize that intent varies among different actors. The CCP’s strategy does not mirror Russian disinformation operations or the strategies of other authoritarian regimes, even if similar tools are being deployed. The Kremlin’s efforts are largely designed to create distrust in the states they target. The CCP’s intent is to shape, manage, and control its operating environment so that public sentiment is—or is seen to be—favorable to its interests (not simply China’s or the Chinese people’s interests). This goal is an outgrowth of the CCP’s concept of state security: its expansive threat perceptions require it to extend power beyond the PRC’s borders. There is increasingly strong evidence that the regime intends to use bulk data collection to support its efforts to control its global operating environment; among other applications, the data collected would inform the development of tools for shaping public discourse abroad.<sup>39</sup>





The kinds of crisis the Chinese party-state prepares for as part of its security strategy include everything from large-scale social unrest, natural disasters, and public health emergencies like COVID-19 to armed conflict with a foreign military, for instance over Taiwan or disputed territory in the South China Sea. But the CCP is also extremely wary of any news, information, opinion, or discussion that contradicts its own version of the truth and could delegitimize or destabilize its rule. This concern is partly why multiple defense white papers in China point to “signs of increasing hegemonism, power politics, and neo-interventionism,”<sup>40</sup> or the idea that China “faces strategic maneuvers and containment from the outside while having to face disruption and sabotage by separatist and hostile forces from the inside.”<sup>41</sup> The threat perception is magnified even further when technology is seen as a means for organizing or supporting a “color revolution”—a protest-driven civic movement calling for a transition to democracy. This perceived risk helps to explain CCP concepts such as cyberspace sovereignty, which is not just about the protection of a physical space or the domestic internet, but also amounts to control over an unbounded ideas space that transcends all borders.<sup>42</sup>

The CCP does not compartmentalize its security strategy into domestic and international components, as perceived political and ideological threats can both come from abroad. The regime sees color-revolution events as being provoked in part by “hostile forces” outside the PRC. In a 2000 speech, then PRC leader Jiang Zemin warned that “the internet has become a new important front for ideological and political work. Hostile forces at home and abroad are trying their best to use it to compete with our party and government for the masses and youth. We must study its characteristics and take effective measures to meet this kind of challenge. We must take the initiative to increase our positive propaganda and influence on the internet.”<sup>43</sup> The CCP’s online and international propaganda apparatus has greatly expanded in the years since, particularly under Xi Jinping. In essence, the PRC’s state security is really about the security of the party, regardless of state borders, and especially in the ideological and political realms.

**In essence, the PRC’s state security is really about the security of the party, regardless of state borders, and especially in the ideological and political realms.**

Illustrating the overlapping and seamless nature of these ideas within the CCP, Xi Jinping said in 2018, “People’s security is the purpose of state security, political security is the root of state security, the supremacy of national interests is the criterion of state security, realizing people’s happiness, the party’s long-term governance, and the country’s long-term stability.”<sup>44</sup> Or as one article originally published in the *People’s Liberation Army Daily* described it, political security “refers to the objective state of state sovereignty, political power, political system, political order, and ideology protected from threats, infringements, subversions, and destruction.”<sup>45</sup> Again, state security as a concept is not about protecting China and the Chinese people separate from the party’s leadership. State security is about protecting CCP rule above all else.

Shaping public perceptions effectively requires the capacity to understand public sentiment. The CCP’s methods in this regard are not very different from those seen in the global advertising industry. But instead of trying to sell a product, the party is trying to promote authoritarian control and governance beyond the PRC’s borders. In 2013, then party secretary and deputy director of the former State Administration of Press, Publication, Film, and Television Jiang Jianguo said it was necessary to understand the “psychology and acceptance habits of foreign audiences” so that the PRC could “strengthen the construction and innovation of communication content” and “realize targeted communication based on different audiences,” and “so that images, sounds, texts, and information of mainstream media of [China] can spread widely to all parts of the world.”

Emerging technologies, particularly those that utilize big data, are a critical component of the CCP's efforts to know and manipulate its international audiences. Large data sets can reveal patterns and trends in human behavior, enabling more accurate sentiment analysis, which among other things could help the party-state to disseminate propaganda more effectively.

While such data-informed propaganda strategies are still developing, the regime is already ramping up its overall efforts to shape international public opinion, demonstrating at least a political will that may soon be followed by more advanced means of carrying it out. In June 2020, for example, Twitter released information on the removal of accounts it said were part of a state-backed covert influence campaign. The company took down numerous PRC-linked accounts that mostly posted disinformation about the Hong Kong democracy movement, US-based billionaire Guo Wengui (especially his relationship with former White House adviser Steve Bannon), and to a lesser extent COVID-19 and Taiwan.<sup>49</sup> The campaign was not highly sophisticated, though there are signs of movement in that direction. Among other indicators, the CCP-controlled company Global Tone Communications Technology (see text box) has reportedly applied for patents pertaining to a machine translation method based on generative adversarial networks (GANs). GANs can be used to synthesize images based on AI, or use visual speech recognition to perform lip-reading and speech output. This is the same type of technology commonly associated with synthetic media, also referred to as “deep fakes.”

## SETTING STANDARDS DOMESTICALLY AND GLOBALLY

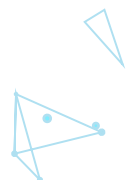
The CCP aims to reshape global governance. It expects technology to enhance the sophistication of its efforts, and it is using capitalism as a vehicle to access data that can help it disrupt democratic processes and create a more favorable global environment for its own power and security. But in addition to accumulating data, the party-state is attempting to pioneer new forms of technology and lay the technical foundations for entire industries, which the rest of the world will have to adopt. Actors in liberal democracies often assume that new technology is essentially neutral, like a simple tool, and that they can control any risk associated with adopting it. The CCP appears to understand that a technology's inherent design features cannot be removed by users, and that dominating the initial phases of development can pay dividends long into the future.

International standards for technology are typically created by countries, corporations, or nongovernmental organizations to set benchmarks for safe usage and reduce potential costs from trade and manufacturing. Because costs may increase when technologies must be adapted to comply with new rules, actors may compete to establish their standards first. Setting global technology standards through international

### Case Study: The Big Potential of Big Data

An October 2019 paper, *Engineering Global Consent*, profiled a Chinese company called Global Tone Communications Technology (GTCOM), which is controlled by the Central Propaganda Department.<sup>46</sup> As a self-described “cross-language big data” business, GTCOM says it collects bulk data globally in over 65 languages and processes the information for output into other products and services, for both government and corporate clients. In terms of scale, the firm claims to collect as much as 2 to 3 petabytes of data annually—the equivalent of about 20 billion photos on Facebook. The company's director of big data, Liang Haoyu, was quoted as saying that “GTCOM is trying to build up its recognition [capability] for objects, settings, and human faces, in conjunction with texts and voices, to provide real-time monitoring of security risks. In the future, [GTCOM] will be able to find the requested facial structure through image recognition and provide technical support and assistance for state security.”<sup>47</sup> At a presentation Liang gave in 2017, an image projected beside him read, “90 percent of military-grade intelligence data can be obtained from open data analysis.”<sup>48</sup>

It is not immediately clear what all of this collected information will eventually be used for. To a degree, the CCP amasses data in bulk and worries about what to do with it later, anticipating greater technical capacity to exploit the trove in the future. But beyond Liang's statements about potential security applications, it is revealing that GTCOM is supervised by the Central Propaganda Department. The structure suggests an intent to develop new tools—such as artificial, AI-driven social media commentary, images, and videos—that could help manipulate global public discourse and advance the CCP's sharp power agenda.





organizations, including the International Organization for Standardization, tends to encompass the establishment of “market-based de facto standards” that correspond with the goals of corporations like Huawei, and government standards such as those set domestically within the PRC or any other country.<sup>50</sup> The China Standards 2035 plan calls for the global export of PRC standards for emerging technologies, and for PRC standards to be accepted through international standards-setting bodies.<sup>51</sup> If PRC-originated technical standards—especially for key technical infrastructure—are adopted internationally, PRC-made systems will enjoy greater interoperability and market access in the rest of the world. The problem for democracies is that PRC standards were designed not simply to guarantee the quality and interoperability of various types of equipment, but also to ensure that the technology facilitates the party-state’s highly politicized social-management objectives.<sup>52</sup>

Domestically, technologies are being researched and developed to meet the needs of the CCP, which are typically set out in government standards documents. Hundreds of companies’ products are involved in smart cities projects across the PRC, making the implementation appear chaotic and uneven. Standardization is taking place at the design level, however, which indicates that seamless interoperability between smart cities systems is possible to achieve. Government and research institutes collaborate with companies on national standards technical committees to standardize equipment development and the requirements that companies must meet to successfully bid for a project. For instance, a 2015 document GA/T1334 on the technical requirements for facial recognition in security systems was drafted through the cooperation of over a dozen bodies, including research institutes, such as the Chinese Academy of Sciences, the National University of Defense Technology, and the First Research Institute of the Ministry of Public Security; technology companies, such as Hikvision and Dahua; and public security bureaus, such as the Shanxi Provincial Public Security Department and the Wuhan Public Security Bureau.<sup>53</sup> Documents like these are used as a basis for technical requirements in government procurement contracts.

In practice, local governments across the PRC have not yet achieved seamless interoperability between government departments and with other local governments using smart cities platforms, but this does not mean that it will remain out of reach. The setting of standards, and the requirement that project bidders meet those standards, makes it more likely that plans such as Skynet or Sharp Eyes will gain cohesion and be successfully implemented, despite the many players involved. The same logic applies at the international level. Although the PRC cannot force its standards on other countries, it can help to set standards that become the global norm and ease the international adoption of its technology, effectively embedding the CCP’s political values and increasing the regime’s ability to exploit this advantage and project sharp power.

It is tempting to dismiss the feasibility of the Chinese government’s plan to use smart cities technology as a tool for monitoring the movements of large populations. The problems that local governments encountered while trying to leverage these systems in response to the COVID-19 outbreak in early 2020 illustrated that their current ability to integrate data from different sources is limited. The *Financial Times* reported that some private companies refused to share users’ location data, which are considered to be of higher quality than those held by state telecommunications

**Government and research institutes collaborate with companies on national standards technical committees to standardize equipment development and the requirements that companies must meet to successfully bid for a project.**

firms, to support local governments' tracking and tracing of high-risk individuals.<sup>54</sup> However, to focus on the current flaws rather than the long-term trajectory is a mistake, not least because the gaps that the COVID-19 crisis response revealed could accelerate improvements and ultimately make the technology more effective. Technology must catch up with ideas, and once it does, enforcement of such demands for data would become increasingly automated.

Private companies do not, at the end of the day, have any genuine power to refuse to cooperate with the PRC government's demands for data.<sup>55</sup> The PRC's state security concept holds that everyone is responsible for preventing and stopping behavior that could compromise China's state security, no matter where in the world they are located.<sup>56</sup> The suite of state security-related legislation disseminated under Xi Jinping is very clear on this matter. Article 7 of the National Intelligence Law, for instance, declares that "any organization and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of." There has been a push within China for increased data security, exemplified in October 2020 by the release of the draft Personal Information Protection Law (PIPL), which proposes to adopt measures on individual rights and consent, facial recognition, responsibilities for data handlers, and limits processing of some personal information.<sup>57</sup> At the moment, it could be argued that commercial enterprises do very little to protect individuals' privacy, and therefore it is necessary that the government do more to regulate privacy protection. However, this does not mean that those protections would put limits on the Party's power. Given that the party-state describes the law as a tool for ensuring the party's political security above all else, any independence PRC companies may have to resist political pressure is obviously limited. As Xi Jinping has said, "comprehensively relying upon the law to rule the country does not at all weaken the party's leadership," but rather consolidates the party's hold on power.<sup>58</sup>

These factors will not change as Chinese companies go global, or as foreign companies continue to seek market access in the PRC. In November 2020, the *Wall Street Journal* reported that a former Airbnb executive had resigned over the company's sharing of user data with Chinese officials. The report said that in 2019, Chinese authorities had "approached Airbnb with an unwritten request for more user data, including more 'real-time data,' such as when a user first makes a reservation."<sup>59</sup> Relatedly, U.S. Department of Justice prosecutors issued a complaint in December 2020 regarding a Zoom employee who shared user information with Chinese security officials and terminated video calls organized by individuals based outside of China concerning the anniversary of the 1989 Tiananmen Square massacre.<sup>60</sup> If the PRC has the ability to coerce foreign companies into sharing data, no one should believe that companies based inside its borders have any meaningful power to push back.

The PRC has participated actively in global bodies that set technical standards for emerging technologies including 5G, IoT, and AI. China's engagement in this space and the relative absence of participation by liberal democracies gives PRC companies an edge over their competitors and creates an opportunity for Beijing to shape international norms that serve its political interests.<sup>61</sup> The PRC government has a strong presence in the International Telecommunication Union (ITU), which it uses to "tilt the standard-setting agenda in Huawei's favor."<sup>62</sup> China has also played a large role at the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), two of the world's largest technical standards-setting bodies. The US-China Business Council reported that PRC-occupied secretariat positions on technical committees or subcommittees had increased by 73 percent between 2011 and 2020 in the ISO, and by 67 percent between 2012 and 2020 in the IEC.<sup>63</sup> Through its presence in these bodies, the PRC is directly shaping standards on a range of issues.<sup>64</sup> Even absent this direct involvement, PRC companies set standards by default when their products are exported globally. In the security-camera industry, PRC companies like Hikvision and Dahua enjoy global market dominance, even though sales have recently declined due to U.S. sanctions related to the firms' provision of surveillance technologies that enable repression of the Uyghur population in Xinjiang.

**Liberal democracies must be able to explain clearly to their publics why China's tech-enhanced authoritarianism is a direct systemic threat, which among other things undermines individual autonomy and freedom of expression.**

The problem becomes clearer when China's tech giants are certified for meeting international standards that they helped set. For example, the company YITU, considered one of China's "AI champions," provides facial-recognition and traffic-monitoring software for Huawei smart cities projects.<sup>65</sup> A company press release from July 2020 said the British Standards Institution had confirmed that YITU met ISO/IEC 27701:2019 certification with regard to its systems for managing personally identifiable information. The company said this meant it complied with "widely accepted international certification for privacy information management systems (PIMS) that meet best practices outlined in regulations such as the [European Union's] General Data Protection Regulation (GDPR)."<sup>66</sup> But YITU is also directly involved in the Chinese party-state's system of repression in Xinjiang. According to the Australian Strategic Policy Institute's Mapping China's Technology Giants project, YITU supports Xinjiang's public security work through its Dynamic Portrait System, and it cooperates with other companies on public security in the region.<sup>67</sup> An investigation by the *New York Times* found that a YITU-generated database included code to identify Uyghurs from public security surveillance video.<sup>68</sup> This report suggests that YITU complies with standards such as GA/T1334, which assign fields for coding a person's nationality and ethnic identity. There are clear reasons to question whether the company's values actually align with the intent of regulations like the GDPR, but this problem has been largely overlooked until very recently.

## ARTICULATING DEMOCRATIC IDEAS AND VALUES FOR GOVERNING TECHNOLOGY

For decision makers, researchers, and civil society alike, it is crucial to develop a sophisticated country-specific understanding of how state actors like the PRC government project sharp power using new technologies. States act differently depending on their interests and intent, and the impact of tech-enabled sharp power will vary. Although "country-agnostic" policy approaches to decision making may feel more objective, they often obscure important realities by defining the nature of the problem inadequately. Varying intentions among authoritarian actors also affect different issue areas and require distinct responses.

At the same time, liberal democracies must be able to explain clearly to their publics why China's tech-enhanced authoritarianism is a direct systemic threat, which among other things undermines individual autonomy and freedom of expression. In doing so, liberal democracies must also be clear about why the alternative they offer is better. They should state plainly what liberal democratic values are and invest in protecting them. Given the multisectoral scope of the challenge, civil society can play a unique and critical role by coordinating with media, government, and private-sector actors to mitigate problems associated with technology and sharp power projection.

To this end, civil society should consider the following:

### 1. Strengthen public discourse on liberal democratic values and technology

- Civil society organizations should be trained on issues related to emerging technologies, allowing them to help deliver educational programming on best practices for data security. For instance, digital literacy programs could be designed to go beyond basic personal and corporate data-management practices, to include discussion on the geopolitical dimension of the issues and the ways in which seemingly harmless data collection can be abused. Digital security training should be mainstreamed into international development programs.

- Media and civil society organizations should coordinate to expose and amplify indicators of tech-enabled sharp power in their countries, which would contribute to broader public awareness of the issues, encourage debate on what should be done, and pressure governments to take protective action. Major investigative media outlets need experts on data forensics and other technical specialists as a part of their teams.
- Civil society actors should conduct research into public perceptions on digital surveillance issues and data protection, with the intent of developing a framework for the standards that liberal democratic governments should set when presenting alternatives to authoritarian initiatives. Data privacy is a common, perhaps universal value; public opinion research around it can help box in authoritarian governments with strong norms based on individual rights.
- Utilizing Chinese-language expertise, civil society organizations and journalists should pursue further research into PRC laws, regulations, and pronouncements in order to better understand how the CCP intends to shape emerging technologies, which are coming online regularly and outpacing updates to international regulations.

## 2. Develop consensus and coordinate responses among democratic partners

- Where possible, civil society organizations should coordinate with democratic governments and the private sector on finding policy solutions to the increasingly complex and fast-moving challenges posed by emerging technologies. They should engage in meaningful multilateral and Track 1.5 dialogues to generate responses to common problems associated with the projection of tech-enabled sharp power. For instance, in 2021, the Australian Strategic Policy Institute was set to host its first annual Sydney Dialogue, bringing political, business, and government leaders together with the world's best strategic thinkers to debate, generate new ideas, and work toward common understandings of the opportunities and threats presented by new technologies.<sup>69</sup>
- Civil society groups must participate actively in international standards-setting bodies, including the ITU, ISO, and IEC, to contribute to the creation of standards for technologies like 5G and IoT devices and to counter harmful PRC efforts to do the same. They need a role in these forums alongside governments and the private sector as representatives of consumers and legal entities. Civil society organizations can push for transparency around the development of technical standards for technologies that may negatively affect civil liberties, like facial- or voice-recognition systems.
- Corporate and government research-and-development technology enterprises should invite civil society groups to approach them early and often for consultation on whether their technologies meet democratic standards, and whether they should depart from PRC standards that conflict with democratic safeguards.
- Higher education institutions should be accountable for conducting their own due diligence on individuals, organizations, and end uses of academic research. Ethics review boards should engage in meaningful dialogue with human rights researchers and subject matter experts to develop guidelines on assessing and managing security, reputational, and ethical risks posed by authoritarian-linked funding sources and research collaborations.<sup>70</sup>



### 3. Address cyber insecurity in the supply chain

- Research institutions, think tanks, and other civil society organizations in democracies can support the development of effective government regulations on data privacy and protection by identifying, consolidating, reporting, and publicizing how data are collected, stored, and shared in opaque or undemocratic ways. Civil society organizations can also devote resources to investigating issues like data security and privacy breaches, especially those associated with authoritarian regimes, and publicize these widely.
- Think tank researchers should participate with cybersecurity intelligence companies and democratic governments in a multiyear research collaboration that would result in the development of a publicly accessible and intuitive database focused on tech supply chains and embedded data-collection and cybersecurity risks. This resource should be made available so that governments and private entities, such as property developers or small and medium-sized enterprises, can conduct effective due diligence on technologies they plan to procure.
- Civil society actors should help advocate for stronger legal structures around the use of equipment associated with smart cities projects. Meanwhile, they should encourage investment in research and development to offer credible alternatives to systems and services that are designed to meet the standards of authoritarian actors. For instance, they could support the development of facial-recognition and computer-vision methods that protect the rights to privacy, due process, and freedom from discrimination.<sup>71</sup>

**For decision makers, researchers, and civil society alike, it is crucial to develop a sophisticated country-specific understanding of how state actors like the PRC government exert sharp power using new technologies.**

## ENDNOTES

- 1 Samantha Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion," Australian Strategic Policy Institute, 14 October 2019, [www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion](http://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion).
- 2 Peter Mattis, "Russian and Chinese Political Interference Activities and Influence Operations," in Richard J. Ellings and Robert Sutter, eds., *Axis of Authoritarians: Implications of China-Russia Cooperation* (Seattle, WA: The National Bureau of Asian Research, 2018).
- 3 Nadège Rolland, "A 'China Model'? Beijing's Promotion of Alternative Global Norms and Standards," written testimony for the U.S.-China Economic and Security Review Commission, 27 April 2020, [www.nbr.org/publication/a-china-model-beijings-promotion-of-alternative-global-norms-and-standards](http://www.nbr.org/publication/a-china-model-beijings-promotion-of-alternative-global-norms-and-standards); and Liza Tobin, "Xi's Vision for Transforming Global Governance: A Strategic Challenge for Washington and Its Allies," *Texas National Security Review*, 2.1 (November 2018), <http://dx.doi.org/10.26153/tsw/863>.
- 4 Richard P. Suttmeier, "Assessing China's Technology Potential," *Georgetown Journal of International Affairs* 5.2 (Summer/Fall 2004), 97-105, [www.jstor.org/stable/43134293](http://www.jstor.org/stable/43134293); Joe McReynolds, ed., *China's Evolving Military Strategy* (Washington, DC: The Jamestown Foundation, 2017); and Marcel Anglielvi de la Beaumelle, Benjamin Spevack, and Devin Thorne, *Open Arms: Evaluating Global Exposure to China's Defense-Industrial Base*, C4ADS, October 2019, [www.c4reports.org/open-arms](http://www.c4reports.org/open-arms).
- 5 Danielle Cave et al., "Mapping China's Tech Giants," Australian Strategic Policy Institute, 18 April 2019, [www.aspi.org.au/report/mapping-chinas-tech-giants](http://www.aspi.org.au/report/mapping-chinas-tech-giants). See also company overviews on the Australian Strategic Policy Institute's Mapping China's Tech Giants website, available at <https://chinatmap.aspi.org.au/#/companies>.
- 6 Christopher Walker and Jessica Ludwig, "From 'Soft Power' to 'Sharp Power': Rising Authoritarian Influence in the Democratic World," in Christopher Walker and Jessica Ludwig eds., *Sharp Power: Rising Authoritarian Influence*, National Endowment for Democracy, December 2017, [www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf](http://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf).
- 7 Christopher Walker, "What is 'Sharp Power?'" *Journal of Democracy* 29.3 (July 2018), [www.journalofdemocracy.org/articles/what-is-sharp-power](http://www.journalofdemocracy.org/articles/what-is-sharp-power).
- 8 Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion."
- 9 "What Is a Smart City?," Cisco, [www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html](http://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html).
- 10 Samantha Hoffman, "Managing the State: Social Credit, Surveillance, and the CCP's Plan for China," *China Brief*, 17 August 2017, <https://jamestown.org/program/managing-the-state-social-credit-surveillance-and-the-ccps-plan-for-china>.
- 11 Samantha Hoffman, "Programming China: The Communist Party's Autonomic Approach to Managing State Security," University of Nottingham, 29 September 2017, <http://eprints.nottingham.ac.uk/48547/1/Hoffman%20C%20Samantha%20Student%20ID%204208393%20PHD%20THESIS>.
- 12 Dahlia Peterson, "Designing Alternatives to China's Repressive Surveillance State," CSET Policy Brief, October 2020, <https://cset.georgetown.edu/wp-content/uploads/CSET-Designing-Alternatives-to-Chinas-Surveillance-State.pdf>; and Danielle Cave, Fergus Ryan, and Vicky Xiuzhong Xu, "Mapping More of China's Tech Giants: AI and Surveillance," Australian Strategic Policy Institute, 28 November 2019, [www.aspi.org.au/report/mapping-more-chinas-tech-giants](http://www.aspi.org.au/report/mapping-more-chinas-tech-giants).
- 13 Li Zhen, "'Tianwang' jia 'xueliang' chengxiang gong ping'an" ["Skynet" Plus "Sharp Eyes" Both Cities and Rural Areas Are Safe], *People's Daily*, 11 October 2017, <http://archive.fuEMVC>.
- 14 Peterson, "Designing Alternatives to China's Repressive Surveillance State;" "Xueliang gongcheng" nongcun anfang jiankong jianshexiangmu ni zhi duoshao" [How much do you know about the construction of the "Sharp Eyes" rural security monitoring project?], *zhongguo anfang zhanlan wang* [China Security Exhibition Network], 19 December 2016, <https://archive.vn/UjkDN>.
- 15 Zhen, "'Skynet' Plus 'Sharp Eyes' Both Cities and Rural Areas Are Safe;" and Ruan Zhanjiang and Shuai Biao, "'Xueliang gongcheng' zhi mi ping'an jianshe fanghuwang" ["Sharp Eyes Project" Weaving Security Construction Net], *People's Daily*, 14 February 2019, <http://archive.fu/m6XIB>.
- 16 Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion."
- 17 "Smart Meters," Energy NSW, <https://energysaver.nsw.gov.au/households/understand-your-usage/smart-meters>.
- 18 Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, May 2019, [www.hrw.org/sites/default/files/report\\_pdf/china0519\\_web5.pdf](http://www.hrw.org/sites/default/files/report_pdf/china0519_web5.pdf).
- 19 For example, "Langchao ruanjian tiyan dianzizhengwu ji su zhilu" [Inspur experiencing a speedy journey of e-government], 28 October 2003, <https://web.archive.org/web/20190310134445/http://news.sohu.com/08/81/news214928108.shtml>; and Tian Doudou, "Huizhi 'shuzi zhongguo' (zoujin youxiu guojiazhongdianshiyanshi)—ji cehui yaogan xinxing gongcheng guojiazhongdianshiyanshi" [Painting "Digital China" (Entering the Excellent State Key Laboratory)—State Key Laboratory of Information Engineering in Surveying, Mapping, and Remote Sensing], National Natural Science Foundation of China, 30 March 2006, <http://archive.fu/bxGUW>.
- 20 Samantha Hoffman, "Grasping Power with Both Hands: Social Credit, the Mass Line, and Party Control," *China Brief*, 10 October 2018, <https://jamestown.org/program/grasping-power-with-both-hands-social-credit-the-mass-line-and-party-control>.
- 21 "Suzhou qidong jianshe 'chengshi danao'" [Suzhou starts the construction of "city brain"], *Xinhua*, 8 March 2017, <http://archive.is/wM6OE>; "Neimengguzhiqu zhongguo zhihui chengshi zaijian he xinjian ziangmu mingdan" [Inner Mongolia Autonomous Region "List of New and Under Construction Smart Cities Projects in China"], *Smart Cities Net*, 18 August 2016, <https://archive.fu/fZ7hx>; and "Wuhan jiaojing yu huaweigongsi qianshu zhihui jiaotong zhanlue hezuoxieyi" [Wuhan traffic police and Huawei signed a strategic cooperation agreement on smart transportation], ITS114.com, 24 August 2017, <http://archive.is/y6Pvs>.
- 22 Wu Lixia, "Zhihui jiaotong zai goujian zhihui chengshi zhongdi zhongyao zuoyong" [The important role of smart transportation in building a smart city], *Building Technology Research*, August 2019, [www.researchgate.net/publication/335217961\\_zhihuijiaotongzaigoujianzhihuichengshizhongdizhongyaozuoyong](http://www.researchgate.net/publication/335217961_zhihuijiaotongzaigoujianzhihuichengshizhongdizhongyaozuoyong).
- 23 Sarah K. White, "What Is Geofencing? Putting Location to Work," *CIO*, 1 November 2017, [www.cio.com/article/2383123/geofencing-explained.html](http://www.cio.com/article/2383123/geofencing-explained.html).
- 24 Jean Marie Takoulev, "Huawei Sets Up a \$1.5 Billion Fund to Boost African Smart Cities," *Afrik 21*, 2 October 2019, [www.afrik21.africa/en/africa-huawei-sets-up-a-1-5-billion-fund-to-boost-african-smart-cities](http://www.afrik21.africa/en/africa-huawei-sets-up-a-1-5-billion-fund-to-boost-african-smart-cities). See also the Australian Strategic Policy Institute's Mapping China's Tech Giants project, which documented dozens of smart cities projects around the world, led mainly by Huawei. Available at <https://chinatmap.aspi.org.au/#/map/f2-Huawei,f6-Smart%20cities>.
- 25 Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, 15 August 2019, [www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017](http://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017).
- 26 "Egypt, China's Huawei Discuss Electricity Network's Transformation to Smart Grid," *China Global Television Network*, 4 September 2020, <https://africa.cgtn.com/2020/09/04/egypt-chinas-huawei-discuss-electricity-networks-transformation-to-smart-grid>.
- 27 As Wakama, "Nigerian Government and Huawei Partner on Smart Cities Initiative," *IT News Africa*, 10 August 2017, <https://www.itnewsafrika.com/2017/08/nigerian-government-and-huawei-partner-on-smart-cities-initiative>.
- 28 For a discussion of how increased government access to combined quantitative and qualitative data erodes opportunities for ensuring democratic accountability, see Nicholas D. Wright, *Artificial Intelligence and Democratic Norms: Meeting the Authoritarian Challenge*, National Endowment for Democracy, August 2020, [www.ned.org/wp-content/uploads/2020/07/Artificial-Intelligence-Democratic-Norms-Meeting-Authoritarian-Challenge-Wright.pdf](http://www.ned.org/wp-content/uploads/2020/07/Artificial-Intelligence-Democratic-Norms-Meeting-Authoritarian-Challenge-Wright.pdf).
- 29 Danielle Cave, Fergus Ryan, and Vicky Xu, "Mapping More of China's Tech Giants: AI and Surveillance," Australian Strategic Policy Institute, 28 November 2019, [www.aspi.org.au/report/mapping-more-chinas-tech-giants](http://www.aspi.org.au/report/mapping-more-chinas-tech-giants). Note: whether or not the agreement has materialized since is unclear to the author.
- 30 "Huawei Safe City Solution: Safeguards Serbia," Huawei, 23 August 2018, <https://archive.vn/pZ9HQ>.
- 31 Lily Kuo, "Hong Kong Bookseller Gui Minhai Jailed for 10 Years in China," *Guardian*, 25 February 2020, [www.theguardian.com/world/2020/feb/25/gui-minhai-detained-hong-kong-bookseller-jailed-for-10-years-in-china](http://www.theguardian.com/world/2020/feb/25/gui-minhai-detained-hong-kong-bookseller-jailed-for-10-years-in-china); and Nate Schenkkan and Isabel Linzer, *Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression*, Freedom House, February 2021, [https://freedomhouse.org/sites/default/files/2021-02/Complete\\_FH\\_TransnationalRepressionReport2021\\_rev020221.pdf](https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf).
- 32 "Turkcell, Huawei Sign Deal on Smart Cities in Turkey," *Daily Sabah*, 23 October 2018, <https://archive.vn/6D9EG>; and Can Sezer, "UPDATE 1—Turkey's Turkcell Signs Deal to Use Huawei's Mobile Services," *Reuters*, 12 February 2020, <https://archive.vn/TYsbj>.
- 33 Asim Kashgarian and Ezel Sahinkaya, "Analysts: Extradition Treaty between Turkey, China Endangers Uighur Refugees," *Voice of America*, 7 January 2021, [www.voanews.com/east-asia-pacific/analysts-extradition-treaty-between-turkey-china-endangers-uighur-refugees](http://www.voanews.com/east-asia-pacific/analysts-extradition-treaty-between-turkey-china-endangers-uighur-refugees).
- 34 "Eradicating Ideological Viruses: China's Campaign of Repression against Xinjiang's Muslims," Human Rights Watch, 9 September 2018, [www.hrw.org/sites/default/](http://www.hrw.org/sites/default/)

[files/report\\_pdf/china0918\\_web2.pdf](#).

35 Gareth Browne, "How Turkey is Sending Muslim Uighurs Back to China without Breaking Promise," *Telegraph*, 26 July 2020, [www.telegraph.co.uk/news/2020/07/26/turkey-sending-muslim-uighurs-back-china-without-breaking-promise](http://www.telegraph.co.uk/news/2020/07/26/turkey-sending-muslim-uighurs-back-china-without-breaking-promise).

36 Matt Schrader, "Huawei's Smart Cities and CCP Influence, at Home and Abroad," *China Brief*, 19 June 2018, <https://jamestown.org/program/huaweis-smart-cities-and-ccp-influence-at-home-and-abroad>.

37 Dominic Meagher, "Has Hong Kong's National Security Law Created Secret Police with Chinese Characteristics?," *Strategist*, 14 July 2020, [www.aspistrategist.org.au/has-hong-kongs-national-security-law-created-secret-police-with-chinese-characteristics](http://www.aspistrategist.org.au/has-hong-kongs-national-security-law-created-secret-police-with-chinese-characteristics).

38 Sean Coughlan, "UK Universities Comply with China's Internet Restrictions," British Broadcasting Corporation, 9 July 2020, [www.bbc.com/news/education-53341217](http://www.bbc.com/news/education-53341217).

39 Tobin, "Xi's Vision for Transforming Global Governance: A Strategic Challenge for Washington and Its Allies."

40 "Zhongguo wuzhuanglilang de duoyanghua yunying" [The Diversified Employment of China's Armed Forces], Information Office of the State Council of the People's Republic of China, 2013; and "Zhongguo de guofang (2000)" [China's National Defense in 2000], Information Office of the State Council of the People's Republic of China, October 2000.

41 "Zhongguo de junshizhanlue (2008)" [China's National Defense in 2008], Information Office of the State Council of the People's Republic of China, January 2009.

42 Samantha Hoffman, "China's Tech-Enhanced Authoritarianism," written testimony for the U.S. House Permanent Select Committee on Intelligence for the hearing "China's Digital Authoritarianism: Surveillance, Influence, and Political Control," 16 May 2019.

43 "Jiang Zemin: zai zhongyang sixiangzhengzhi gongzuo huiyi shang de jianghua" [Jiang Zemin: Remarks at the Central Ideological and Political Work Conference], China Reform Information Database, 28 June 2000, [www.reformdata.org/2000/0628/5849.shtml](http://www.reformdata.org/2000/0628/5849.shtml).

44 "Zhenghi anquan shi guojia'anquan de genben" [Political security is the root of state security], Qstheory, 20 April 2018, [https://web.archive.org/web/20180420123613/http://www.qstheory.cn/defense/2018-04/20/c\\_1122716581.htm](https://web.archive.org/web/20180420123613/http://www.qstheory.cn/defense/2018-04/20/c_1122716581.htm).

45 Ibid.

46 Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion."

47 "Liang Haoyu: zhongyiyutong 'quanqiu gongkai dashuju' zhu fang anquan fengxian" [Liang Haoyu: GTCOM "global public big data" helps to prevent security risks], Global Tone Communication Technology Co. Ltd. (GTCOM), 20 September 2017, <https://archive.vn/FVJHM>; and Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion."

48 Ibid.

49 Jake Wallis et al., "Retweeting through the Great Firewall," Australian Strategic Policy Institute, June 2020, [https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Retweeting%20through%20the%20great%20firewall\\_1.pdf](https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Retweeting%20through%20the%20great%20firewall_1.pdf).

50 See for instance, Justus Baron and Daniel F. Spulber, "Technology Standards and Standards Organizations: Introduction to the Searle Center Database," Northwestern University, 8 September 2015, [www.law.northwestern.edu/research-faculty/clbe/innovationeconomics/documents/Baron\\_Spulber\\_Searle%20Center\\_Database.pdf](http://www.law.northwestern.edu/research-faculty/clbe/innovationeconomics/documents/Baron_Spulber_Searle%20Center_Database.pdf).

51 "Chinese Standards Going Global an Unavoidable Trend," *Global Times*, 28 April 2020, <https://archive.is/kfUDG>.

52 "Shehui zhili zhinenghua de fazhi lujing" [The Legal Pathway of Social Governance Intelligence], Law Science Journal, 9 October 2020, [www.fxcw.org.cn/dyna/content.php?id=14294](http://www.fxcw.org.cn/dyna/content.php?id=14294).

53 Full list: Tsinghua University, First Research Institute of the Ministry of Public Security, Hikvision, Institute of Automation, Chinese Academy of Sciences, National University of Defense Technology, Computing Institute of Chinese Academy of Sciences, Beijing Haixin Kejin High-Tech Co., Ltd., Guangzhou Pixel Data Technology Development Co., Shanghai Yinchen Intelligent Identification Technology Co., Ltd., Zhejiang Dahua, Shenzhen Zhongkong Biometrics Co., Ltd., Guangdong Boya Information Technology Co., Ltd., Sichuan Chuanda Zhisheng Co., Ltd., Shanxi Provincial Public Security Department, Jiangsu Provincial Public Security Department, and Wuhan Public Security Bureau.

54 Yuan Yang, Nian Liu, Sue-Lin Wong, and Qianer Liu, "China, Coronavirus, and Surveillance: The Messy Reality of Personal Data," *Financial Times*, 2 April 2020, [www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca](http://www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca).

55 Zach Dorfman, "Tech Giants Are Giving China a Vital Edge in Espionage," *Foreign Policy*, 23 December 2020, <https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies>.

56 Samantha Hoffman, "China's State Security Strategy: 'Everyone Is Responsible,'" *Strategist*, 11 December 2017, [www.aspistrategist.org.au/chinas-state-security-strategy-everyone-is-responsible](http://www.aspistrategist.org.au/chinas-state-security-strategy-everyone-is-responsible).

57 "Zhonghuarenmingongheguo geren xinxu baohufa (caoan)" [Personal Information Protection Law of the People's Republic of China (Draft)], *NPC Observer*, October 2020, <https://npcobserver.files.wordpress.com/2020/10/personal-information-protection-law-draft.pdf>.

58 "Xi Jinping tan fazhi zuixin jin ju pouxu gaoji ganbu zoushang fanzui daolu yuanyin" [The latest quotes from Xi Jinping on rule of law, an analysis of the reasons why senior cadres have committed crimes], CPC News, 15 February 2019, <http://archive.fo/gnXxA>.

59 Dustin Volz and Kirsten Grind, "Airbnb Executive Resigned Last Year over Chinese Request for More Data Sharing," *Wall Street Journal*, 20 November 2020, [www.wsj.com/articles/airbnb-executive-resigned-last-year-over-chinese-request-for-more-data-sharing-11605896753](http://www.wsj.com/articles/airbnb-executive-resigned-last-year-over-chinese-request-for-more-data-sharing-11605896753).

60 Drew Harwell and Ellen Nakashima, "Federal Prosecutors Accuse Zoom Executive of Working with Chinese Government to Surveil Users and Suppress Video Calls," *Washington Post*, 18 December 2020, [www.washingtonpost.com/technology/2020/12/18/zoom-helped-china-surveillance](http://www.washingtonpost.com/technology/2020/12/18/zoom-helped-china-surveillance).

61 Anna Gross and Madhumita Murgia, "China Shows Its Dominance in Surveillance Technology," *Financial Times*, 27 December 2019, [www.ft.com/content/b34d8ff8-21b4-11ea-92da-f0c92e957a96](http://www.ft.com/content/b34d8ff8-21b4-11ea-92da-f0c92e957a96).

62 Melanie Hart and Jordan Link, "There Is a Solution to the Huawei Challenge," Center for American Progress, 14 October 2020, [www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge](http://www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge).

63 "China in International Standards Setting," U.S.-China Business Council, February 2020, [www.uschina.org/sites/default/files/china\\_in\\_international\\_standards\\_setting.pdf](http://www.uschina.org/sites/default/files/china_in_international_standards_setting.pdf).

64 Haley Wu, "ISO/IEC Approved China's Standards Proposal on IoT," Seconded European Standardization Expert in China (SESEC), 22 February 2019, [www.sesec.eu/iso-iec-approved-chinas-standards-proposal-on-iot](http://www.sesec.eu/iso-iec-approved-chinas-standards-proposal-on-iot).

65 Danielle Cave, Fergus Ryan, and Vicky Xu, "Mapping More of China's Tech Giants: AI and Surveillance," Australian Strategic Policy Institute, 28 November 2019, [www.aspi.org.au/report/mapping-more-chinas-tech-giants](http://www.aspi.org.au/report/mapping-more-chinas-tech-giants).

66 YITU Technology, "YITU Technology Received ISO/IEC 27701:2019 Certification from BSI, Becomes the First Chinese AI Company to Obtain It," CISION PR Newswire, 1 July 2020, [www.prnewswire.com/news-releases/yitu-technology-received-isoiec-277012019-certification-from-bsti-becomes-the-first-chinese-ai-company-to-obtain-it-301086961.html](http://www.prnewswire.com/news-releases/yitu-technology-received-isoiec-277012019-certification-from-bsti-becomes-the-first-chinese-ai-company-to-obtain-it-301086961.html); and "ISO/IEC 27701:2019 Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines," International Organization for Standardization, August 2019, [www.iso.org/standard/71670.html](http://www.iso.org/standard/71670.html).

67 See YITU company overview on the Australian Strategic Policy Institute's Mapping China's Tech Giants website, available at <https://chinatechmap.aspi.org.au/#/company/yitu>.

68 Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *New York Times*, 14 April 2019, [www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html](http://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html).

69 Danielle Cave, "Introducing a New Global Technology Initiative: The Sydney Dialogue," *Strategist*, 23 December 2020, [www.aspistrategist.org.au/introducing-a-new-global-technology-initiative-the-sydney-dialogue](http://www.aspistrategist.org.au/introducing-a-new-global-technology-initiative-the-sydney-dialogue).

70 Kara Frederick, "Democracy by Design: An Affirmative Response to the Illiberal Use of Technology for 2021," Center for a New American Security, 15 December 2020, [www.cnas.org/publications/reports/democracy-by-design](http://www.cnas.org/publications/reports/democracy-by-design).

71 Peterson, "Designing Alternatives to China's Repressive Surveillance State."







**National Endowment  
for Democracy**

*Supporting freedom around the world*

*forum*  
International Forum for Democratic Studies

## ABOUT THE NATIONAL ENDOWMENT FOR DEMOCRACY

The National Endowment for Democracy (NED) is a private, nonprofit foundation dedicated to the growth and strengthening of democratic institutions around the world. Each year, NED makes more than 1,700 grants to support the projects of nongovernmental groups abroad who are working for democratic goals in more than 90 countries. Since its founding in 1983, the Endowment has remained on the leading edge of democratic struggles everywhere, while evolving into a multifaceted institution that is a hub of activity, resources, and intellectual exchange for activists, practitioners, and scholars of democracy the world over.

## ABOUT THE FORUM

The International Forum for Democratic Studies at the National Endowment for Democracy (NED) is a leading center for analysis and discussion of the theory and practice of democracy around the world. The Forum complements NED's core mission—assisting civil society groups abroad in their efforts to foster and strengthen democracy—by linking the academic community with activists from across the globe. Through its multifaceted activities, the Forum responds to challenges facing countries around the world by analyzing opportunities for democratic transition, reform, and consolidation. The Forum pursues its goals through several interrelated initiatives: publishing the *Journal of Democracy*, the world's leading publication on the theory and practice of democracy; hosting fellowship programs for international democracy activists, journalists, and scholars; coordinating a global network of think tanks; and undertaking a diverse range of analytical initiatives to explore critical themes relating to democratic development.

1201 Pennsylvania Ave, NW, Suite 1100 | Washington, DC 20004 | (202) 378-9700 | [ned.org](http://ned.org)



ThinkDemocracy



@thinkdemocracy