DATA-CENTRIC AUTHORITARIANISM

HOW CHINA'S DEVELOPMENT OF FRONTIER TECHNOLOGIES COULD GLOBALIZE REPRESSION

// VALENTIN WEBER

NED | NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM | INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

// **REPORT** / FEBRUARY 2025

DATA-CENTRIC AUTHORITARIANISM

HOW CHINA'S DEVELOPMENT OF FRONTIER TECHNOLOGIES COULD GLOBALIZE REPRESSION

CONTENTS

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

EXECUTIVE SUMMARY

We live in an age of increasing data-driven authoritarianism. Artificial intelligence (AI) and other technologies that collect and analyze digital data are transforming how autocrats work to stifle dissent. Today, the People's Republic of China (PRC) stands out for its quest to collect and leverage unprecedented types and volumes of data, from public and private sources and from within and beyond its borders, for social control.

This report reviews four key data-centric technologies whose development could fortify Beijing's tech-enabled efforts to control its own people and export authoritarian governance models around the world:

- **AI surveillance applications:** China is leveraging increasingly powerful AI surveillance systems, including not only facial-recognition cameras but sophisticated "city brains" that combine data streams to track and monitor urban trends. These tools create a pervasive surveillance dragnet and may be used by state authorities to quell protests before they start.
- **Neuro- and immersive technologies:** The PRC has world-class capabilities in researching and developing neurotechnologies, such as brain-computer interfaces, and has been actively investing in immersive technologies like virtual reality. Together, these technologies push the frontiers of surveillance by enabling data holders to infer, and potentially influence, people's mental states, impacting the rights to privacy and agency on which democratic citizenship depends. Chinese laws effectively ensure that data from such commercial technologies will be accessible to state authorities.
- **Quantum technologies:** China is a leader in quantum computing and quantum communications, putting it in a position to benefit down the line from advances that could render present-day encryption obsolete. These capabilities endanger independent journalists, human rights defenders, and opposition politicians, undermining the protections they enjoy in other societies.
- **Digital currencies:** The PRC has introduced its own digital currency (CBDC) run by its central bank, paving the way for frictionless state monitoring of users and control over purchases. The spread of China's CBDC would also hamper the ability of democracies to implement sanctions against authoritarian regimes.

The rapid and complex technological transition we are witnessing empowers authoritarian regimes. Thus, it is especially critical for civil society and democratic governments to identify effective, forward-looking strategies for confronting the spread of data-centric authoritarianism and mitigating its adverse impacts on human rights and democracy. To this end, this report identifies seven critical steps:

- Track and counter the diffusion of the PRC’s data-centric authoritarianism;
- Develop a roadmap for governing highly personal types of data collected by neurotechnologies and immersive interfaces;
- Keep AI systems transparent and protect them from misuse;
- Foster and support the development of privacy-preserving emerging technologies;
- Slow Beijing’s progress toward encryption-cracking quantum computing and resist the temptation to implant backdoors in new quantum communication networks;
- Accelerate civil society’s transition to quantum-resistant cryptography, especially in settings that are vulnerable to authoritarian repression;
- Engage more actively in international standard-setting fora to counter the normalization of authoritarian digital approaches.

INTRODUCTION

Data-centric technologies are transforming how autocrats relate to information. Since the days of kings, queens, tsars, and emperors, information has been crucial to authoritarian projects of crushing dissent. Indeed, their spies and police forces would regularly serve up information on clandestine meetings and opposition movements. In the dictatorial regimes of the twentieth century, such as communist East Germany, surveillance—some of it tech-assisted—took on a pervasive character, leaving no facet of social or private life fully protected from prying eyes (or ears). Despite the introduction of technological tools, however, keeping people under watch remained a profoundly human endeavor. Devices might record conversations, but human security officers would have to manually sift through and make sense of the words on tape.

Today, technological advances in areas such as Internet of Things (IoT) devices, cloud computing, and artificial intelligence (AI) help convert unprecedented volumes of information—consumer transactions, political speech, train trips or walks down the street, and even whether someone is happy or sad—into digital data.[1] Security services can still use these data the old-fashioned way, manually perusing a given individual's digital traces to build charges against a dissident or assess someone's loyalty to the state. Yet they can also feed data en masse into automated systems that categorize people or flag population-level trends. While authoritarian leaders and their security apparatuses still make public security decisions most of the time, algorithms can increasingly offer or even implement a menu of options for repression.[2]

This is the age of data-driven authoritarianism. Emerging technologies, from consumer devices that infer our innermost thoughts to quantum computers that will compromise present-day encryption, threaten to expand its global power and reach.

CHINA'S UNIQUE ROLE

Today, one country more than any other—the People's Republic of China (PRC)—is testing the boundaries of what Samantha Hoffman has described as "tech-enhanced authoritarianism."[3] Central to this system, and the focus of the present survey, is the role of digital data. The ruling Chinese Communist Party (CCP) is amassing unprecedented types and volumes of data, from both public and private sources, within and beyond PRC borders. It is leveraging cutting-edge AI systems to extract meaning from this information. Finally, it is converting this machinery into highly customized, population-wide systems of repression, manipulation, and social control.[4]

China has been, and will continue to be, at the forefront of exporting *data-centric authoritarianism*.[5] Its present-day techno-authoritarian state can be traced back to the 1998 "Golden Shield" project, a nationwide plan for integrated digital surveillance, also encompassing the censorship system that came to be known as the "Great Firewall."[6] In the mid-2000s, China reportedly exported the first radio jammers to the government of Zimbabwe, which used them to intercept citizens' communications.[7] The censorship equipment at the time was "dumb," indiscriminately blocking broadcasts at targeted times and frequencies. Increasingly, however, the PRC's digital authoritarian exports have become "smarter," including, for instance, network filtering equipment able to recognize and block specific keywords. PRC vendors also claimed a leading role in the booming global market for surveillance tools that monitor physical spaces, offering CCTV systems and eventually "smart" cameras linked to license plate readers or facial recognition technologies.[8]

Against this backdrop, the PRC's development of next-generation emerging technologies heralds a new stage for data-centric authoritarianism. **This report will explore the progress and implications of four key areas of innovation:** increasingly advanced **AI applications for surveillance**; technologies with the potential to discern our inner states from physiological cues, including **neurotechnologies and the immersive technologies that make possible the "metaverse"**; **quantum technologies** likely to render present-day encryption obsolete; and **digital currencies**. All these emerging technologies either produce new data, enable access to existing data, or facilitate the centralization and fusion of data.[9] To better prepare for this threat, the democratic community must look to the horizon and begin assessing the potential consequences for civic space.

To better prepare for the impacts of frontier technologies, the democratic community must look to the horizon and begin assessing the potential consequences for civic space.

THE DIFFUSION OF DATA-CENTRIC AUTHORITARIANISM

Before turning to a case-by-case exploration of these technologies, it is important to first consider whether the PRC's homegrown digital authoritarian strategies can realistically diffuse to other political settings. Some commentators are skeptical on this point, and they have advanced two major lines of argument.

First, **since the PRC system of digital repression rests on a costly foundation of high-tech instruments for censorship and surveillance, some have argued that it is less likely to spread globally than more wallet-friendly, legalistic approaches to digital authoritarian governance**. In 2019, analysts Alina Polyakova and Chris Meserole concluded that the equipment underpinning the "Great Firewall" and China's AI-powered surveillance dragnet would be too expensive for most regimes to import at scale. By comparison, they felt it would be cheaper to copy what they then saw as a "Russian model" built largely on legal tools for repression, intimidation of tech service providers, and control over online spaces.[10]

The subsequent evidence, however, including this author's previous research, shows that China's technologies and practices have diffused broadly. Even the most impoverished authoritarian regimes—such as Zimbabwe and Uganda, among others—manage to find money to spare for high-tech surveillance gear.[11] Infrastructure of this kind goes to the core of regime security, and it is therefore a spending priority of the CCP. Moreover, and critically, **China has implemented a variety of strategies to ensure that poorer countries can procure tech from PRC vendors**. Among these approaches are free "trials" that encourage recipients to buy in to the PRC's digital ecosystem; subsidies that ensure PRC companies can sell globally at low prices; offers of PRC state financing to cover surveillance purchases; and, finally, special deals like the one that allowed Ecuador to import surveillance gear in exchange for exports of oil.[12]

Other observers have made a different argument, **stressing that China's surveillance state rests not on technology alone but primarily on a well-organized infrastructure of informers, police, and security forces, which cannot easily be replicated abroad**.[13] On this reading, even if Chinese technologies are spreading abroad, other countries will not be able to leverage them to similar effect, since these organizational prerequisites will be absent.

Yet China is not unique when it comes to having an amply staffed and well-organized security apparatus. Think of the Yugoslav (UDBA) and East German (Stasi) secret police forces in the late twentieth century. For every 166 East Germans there was one secret police officer; if one includes regular informers and part-time spies, this ratio climbs to a staggering one agent per 6.5 citizens.[14] In China a decade ago, when the population was slightly under 1.4 billion, there were about two million uniformed police officers—a bit less than one per seven hundred people. (The numbers have most likely risen, since the PRC's security budget has increased since then.[15]) Today, Venezuela, Iran, Cuba, and many other autocracies boast expansive networks of informants and security personnel. Iran, for instance, has a multilayered repressive apparatus spanning multiple government departments and the armed forces; the paramilitary Basij force alone was estimated to comprise roughly one million of Iran's 89 million people as of 2022.[16] **China's uniqueness lies not in the fact that it has sophisticated security forces, but that it produces vast arsenals of advanced surveillance technologies.** These systems, in turn, can be exported easily.

Even while falling well short of replicating China's domestic practices, authoritarian actors can leverage digital authoritarian exports to chill civic action and meaningfully intensify tech-based manipulation and control.

It is true that PRC companies also sell surveillance technologies to **"swing states"** (those on the borderline between democracy and autocracy), which might not have invested that much into their own security apparatuses. Notably, however, exports usually come accompanied by training that PRC companies provide for local security personnel.[17] For example, Zambia, a country scored by

Freedom House as Partly Free, has imported security gear from Huawei. Huawei engineers subsequently helped local personnel to access phones of the political opposition that local officials had failed to access by themselves.[18] Another example is Meiya Pico, a digital forensics company, which has provided training to law enforcement officers in "swing states," such as Bangladesh, Indonesia, Malaysia, and Thailand.[19] These "exports" not just of technology, but also of know-how, are likely to increase the capability of local security forces in other autocratic or hybrid regimes.

Such support on its own may not be enough to offset fundamental differences in underlying security structures. Ultimately, however, "swing states" do not have to be as sophisticated as China in deploying data-driven authoritarianism in order to quell dissent on their streets. Even while falling well short of replicating China's domestic practices, authoritarian actors can leverage digital authoritarian exports to chill civic action and meaningfully intensify tech-based manipulation and control.

Finally, we should keep in mind that surveillance technologies destined for government clients are not the only instruments helping to diffuse the PRC's data-centric authoritarianism. **Consumer technologies, from the video-sharing app TikTok (with more than one billion monthly active users) and all-in-one messenger and payment app WeChat to e-commerce platforms such as Shein and Temu, also provide opportunities for the CCP to influence digital landscapes abroad.** This influence involves both manipulation of online content and digital surveillance of foreign users.[20] For instance, Temu's app was removed from the Google Play Store after it was revealed to contain malware which allowed it to read private messages and examine data from other apps. Also, Shein encourages users to share data from other apps to receive discounts. It is likely that the diffusion of PRC-sourced apps, in whatever sphere, will likely lead to an erosion of privacy until local regulatory authorities rein them in.

WHY EXPORT DATA-CENTRIC AUTHORITARIANISM?

Beyond the obvious economic gains, exporting digital authoritarian tools and know-how strengthens the CCP's grip on power and bolsters its influence in several ways. **For the CCP, one perceived benefit is likely propping up authoritarian regimes that import surveillance tools.** Researchers have found that China exports AI surveillance systems to autocratic states and weak democracies disproportionately, and that such regimes are likelier to import these technologies during periods of domestic unrest and increased repression. On this basis, they concluded that governments are turning to PRC surveillance tools to shore up political control.[21] Such impacts would be advantageous for China since autocrats and authoritarian-leaning leaders tend to be more open to close political and security relationships with Beijing—as we see in Russia, North Korea, Iran, Thailand, and Belarus. Their democratic counterparts are

Exporting digital authoritarian tools and know-how strengthens the CCP's grip on power and bolsters its influence in several ways.

likelier to resist political-security entanglements, even if they engage with China economically. Thus, helping friendly autocrats resist pressures toward democratization benefits China politically.[22]

Second, **PRC authorities view data as a "strategic resource."** China's 2017 national intelligence law compels all PRC companies, organizations, and citizens to cooperate with China's intelligence services; this requirement was reinforced in the 2021 Data Security Law. These provisions effectively mean that data collected by PRC tech vendors overseas—whether through public-security tools, social media, or e-commerce platforms—will be available to the CCP. Authorities in Beijing can glean these resources for valuable intelligence; leverage them to craft custom-tailored propaganda for foreign audiences; or update their economic strategies based on insights into foreign markets (and, potentially, companies).[23]

Third, **equipping (semi)-authoritarian governments with advanced surveillance technologies can extend the reach of Beijing's transnational repression**. A number of recipient governments, such as Thailand, are well-known to hand Chinese dissidents who have fled from the PRC back over to CCP authorities regularly.[24] Local law enforcement agencies can thus be expected to use the advanced tech tools and training they receive, in part, to target persons of interest to Beijing more effectively.

Finally, there is the question of securing wider adoption of Beijing's digital "model": **With every new country that takes up the tools and tactics of the Chinese repressive state, the world looks more and more like China**. Pakistan, Nepal, and Cambodia pursuing internet gateways that will funnel all international internet traffic through a government-controlled chokepoint is a win for China.[25] These moves enhance China's prestige, positioning the once-unique "Great Firewall" as a potential model for other countries worldwide, while also weakening the traditional democratic, decentralized approach to internet governance that Beijing views as a threat. Commercial technologies with PRC censorship and surveillance embedded may contribute in subtler ways to the global spread of PRC digital norms. Taken together, these tactics normalize PRC governance models and help to "make the world safe for the CCP."

For all these reasons, the CCP's intense investment in the global contest to dominate the field of emerging technologies demands close attention from those seeking to preserve a democratic digital future. While analysts in established democracies are scrutinizing the national security implications of the PRC's progress in emerging tech development, these capabilities are also the building blocks for a digital authoritarian ecosystem.[26] They make it easier to locate and repress dissenting opinions, identify levers of social control, and shape people's impressions of the world around them. To better understand the implications for human rights and democracy, the following sections offer a deeper dive into the trajectories of four categories of authoritarian technologies. This survey suggests that the conditions are ripe for next-generation technologies to foster innovations in digital authoritarian practice.

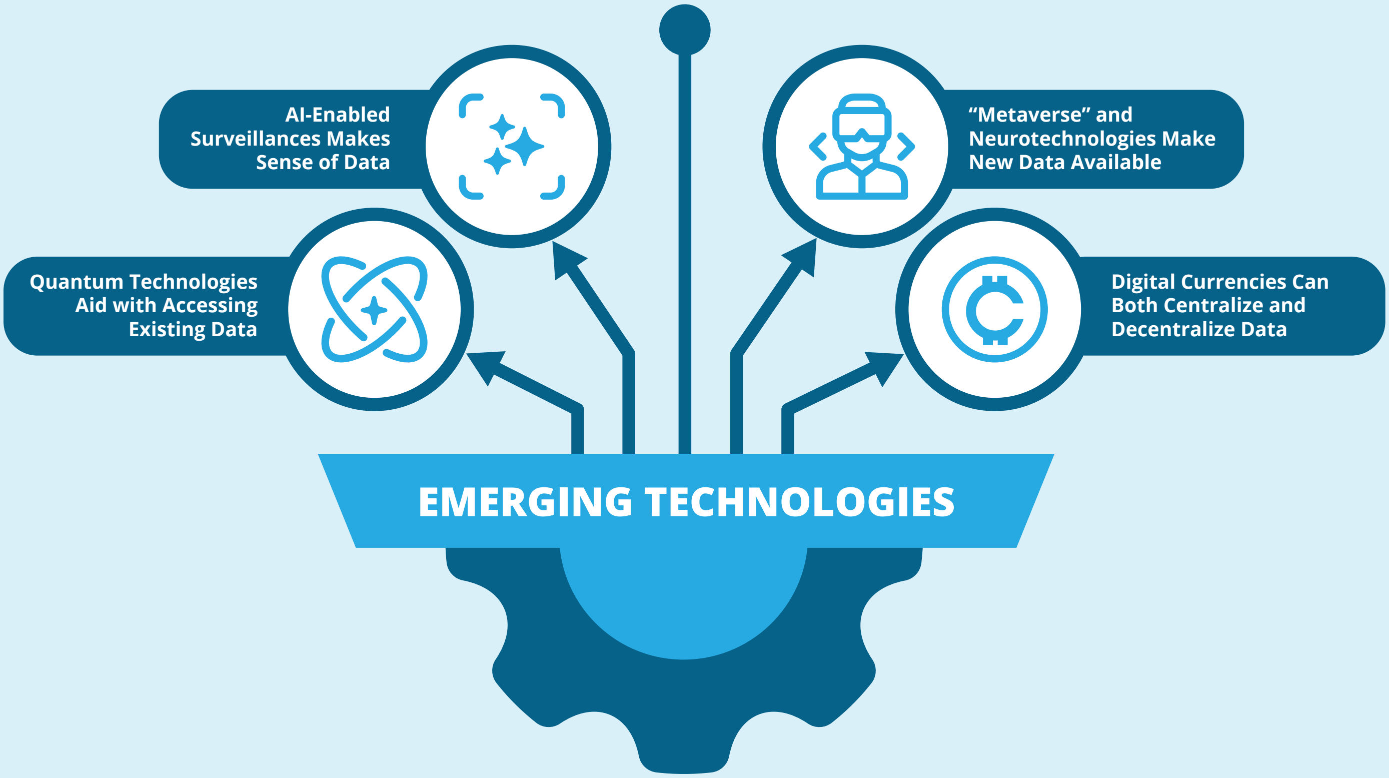
The CCP's intense investment in the global contest to dominate the field of emerging technologies demands close attention from those seeking to preserve a democratic digital future.

NEXT-GENERATION TECHNO-AUTHORITARIANISM: FOUR PATHWAYS

The field of emerging technologies is wide and evolving constantly. As a window on the future landscape, this report focuses on a selection of technologies that have drawn sustained interest from developers, figure prominently on the PRC agenda, and have clear relevance to data-centric authoritarianism. These focus areas are as follows: **AI surveillance technologies**; technologies that are changing mental privacy, particularly **neurotechnologies and the immersive world and interfaces that make up the so-called metaverse**; **quantum computing** with its potential to break present-day encryption; and **digital currencies**.

All four areas discussed are subjects of global geopolitical and economic competition, and all present risks for abuse regardless of where they are developed. New technologies to gather, centralize, access, and process data can advance medical knowledge, widen our access to new experiences, and help governance work better. As elements of a digital authoritarian ecosystem, however, they also have the potential to constrict civic space fundamentally, undermine human agency, and endanger the last bastions of personal privacy. In the coming years, even open societies will have their work cut out in thinking through the necessary guardrails to ensure that technological advances do not come at democracy's expense.[27]

Next-Generation Techno-Authoritarianism: Four Pathways


AI-Enabled Surveillances Makes Sense of Data
"Metaverse" and Neurotechnologies Make New Data Available
Quantum Technologies Aid with Accessing Existing Data
Digital Currencies Can Both Centralize and Decentralize Data
EMERGING TECHNOLOGIES

Nonetheless, **digital authoritarian risks grow more acute, and authoritarian use cases are more likely to be tested and mainstreamed, when technologies are developed in a techno-authoritarian context where meaningful checks on power are absent**. For this reason, the analysis below emphasizes China's development of emerging tech tools and the particular threats they pose in the context of the PRC's well-established, expansion-oriented system of data-centric authoritarianism. The final segment of this report offers recommendations on steps that democratic societies can take to ensure they are offering a clear alternative not only to China's brands, but also to its techno-authoritarian model.

The following section first provides an introduction to each of these technologies, considering in particular its ***relationship to data in the surveillance state***. Second, it examines ***China's progress to date*** in our four areas of focus. Third, based on current practice as well as known capacities and experimental use cases, it offers an overview of the ***mechanisms by which they might impact democratic values*** such as privacy, agency, free expression, and open civic space. Finally, it assesses the extent to which technology developed in the PRC is ***likely to diffuse and be adopted globally***—an outcome that will be influenced not only by the global ambitions of PRC companies, but also by factors such as local demand, political dynamics, and financial accessibility.[28]

This report focuses on the ways in which different emerging technologies provide state authorities with detailed digital insights into their populations. Yet it should be noted that several of these technologies will also bolster authorities' ability to shape the information environment, and thus alter how people perceive the world around them, a topic addressed by the Australian Strategic Policy Institute in its recent publication on persuasive technologies.[29] **This investigation emphasizes data collection and processing because—in addition to chilling civic action in their own right—these actions are a critical first step toward the other practices of data-centric authoritarianism.** They make it possible to refine sophisticated and targeted propaganda campaigns; carry out mass algorithmic repression and movement controls of the kind that have been implemented against the Uyghur minority community in Xinjiang; or enact social credit-style reward-penalty systems at all levels of society that incentivize conformity.[30] Whether or not the maps they create are always accurate, digital data will have enormous impact on the lives of people under techno-authoritarian rule.

AI-ENABLED SURVEILLANCE MAKES SENSE OF DATA

How does it work? AI technologies have a wide range of applications for surveillance. **Tools leveraging AI capabilities can help make sense of video, audio, and textual data, as well as process these data *en masse*** in order to map and predict individual or social behavior.

One of the most common approaches is ***biometric surveillance***, including facial, gait, and speech recognition. Algorithms determine distinctive physical characteristics—such as the shape of a person's nose, eyes, and eyebrows, the way they walk, or the sound of their voice—in order to identify a specific individual across images, audio records, or video footage automatically. Biometric surveillance technologies can be used for standard law-enforcement purposes—such as tracking a suspect's whereabouts around the time a crime took place—but they also open the door to much more pervasive forms of monitoring.

Biometric surveillance technologies can be used for standard law-enforcement purposes, but they also open the door to much more pervasive forms of monitoring.

When people and their behavior are tracked using digital tools—whether these are facial recognition cameras, social media monitoring technologies, or simply "smart" energy meters—over time, the resulting information accumulates into big data. Tapping into these troves of information, **AI tools help the state to look for deviation from "normal" behavior**—for instance, an activist leaving a geo-fenced area.

AI-powered "city brains," an innovation found in PRC "smart cities," are a striking example of surveillance via data fusion. They are an evolution of the original "smart city" concept, which provides masses of data but often lacks "intelligent" insight.[31] These systems connect different data flows (such as information from traffic cameras, energy meters, and city records), identify patterns, and construct a “digital twin” of a city, which is projected into a command center where decisions are made.[32] Pedestrians, vehicles, buildings, and police forces are visualized on a map to allow for efficient command and dispatch of forces. **“City brains” have been used “for everything from pandemic contact tracing to monitoring illegal public assemblies and river pollution.”**[33] They can automate certain tasks (particularly traffic management) and deliver quick insights that decrease police response times.[34]

Separately, large language models (LLMs), which are at their core computer programs that can engage with natural human language in nuanced ways,[35] and new multimodal foundation models that work across image, video, and textual data can contribute to China's techno-authoritarian ecosystem by enabling more fine-grained monitoring of speech. Instead of classifying online posts simply based on the presence or absence of banned keywords, for instance, **they enable authorities to identify the expression of *sentiments***, such as anger or dissatisfaction with a political system, that are deemed politically unacceptable more accurately.

China’s progress to date: China is at the frontier of both research and deployment when it comes to AI-powered governance tools, including AI surveillance systems. The Australian Strategic Policy Institute’s Critical Tech Tracker shows that from 2019-2023, the PRC led the world in the production of papers regarding AI algorithms and hardware accelerators, advanced data analytics, and several other AI linked fields by a wide margin.[36] Although a recent report by Stanford HAI underscored that the United States enjoys an overall lead in AI development,[37] **the PRC’s investment in AI is extensive and has had a clear impact**. Beijing’s advances in developing and deploying AI are particularly evident in the surveillance domain.

In 2016, the conceptualization of “city brains” ensured the central place of AI in China’s surveillance architecture. **The PRC and its companies are the global leader in smart cities technologies, as well as in the component AI systems that supply data to centralized command centers.**[38] The PRC companies CloudWalk, Megvii, and SenseTime—all companies subject to U.S. export and investment restrictions—lead the pack when it comes to algorithms for gait, object, and facial recognition. It has been estimated that half of the world’s smart cities—more than five hundred—are in the PRC,[39] and the “city brain” has been deployed to hundreds of cities across China. According to Alibaba, it is “one of the largest public artificial intelligence systems worldwide.”[40] Data-driven governance systems have often been limited by city boundaries, as their name might suggest, but more recently “megalopolis brains” have started to emerge (for example, in the Yangtze River Delta urban agglomerations or the Guangdong-Hong Kong-Macao Greater Bay Area).[41]

China is at the frontier of both research and deployment when it comes to AI-powered governance tools, including AI surveillance systems.

Although there has been some pushback against tech-enabled surveillance by private companies in the PRC—such as a successful lawsuit against a zoo’s use of facial recognition, followed by adoption of the Personal Information Protection Law (PIPL)—state surveillance activities remain legally unconstrained.[42]

The picture is somewhat different when we turn to AI language-processing. Leveraging data from censored homegrown platforms such as WeChat and Sina Weibo,[43] PRC engineers have developed domestic LLMs (such as Baidu's Ernie) which refuse to provide any information on topics such as Xi Jinping or the CCP.[44] Some analysts have speculated that the impacts of censorship—including limits on training data as well as the challenge of ensuring that models will not give politically unacceptable answers—is slowing PRC companies' progress in generative AI.[45] Yet various evidence, most notably the January 2025 release of the widely-discussed DeepSeek R1 model, strongly suggests that PRC companies are catching up in this area of AI development.[46] A November 2024 report by ASPI described China as "the world leader in adopting generative AI," with key public-sector applications including social media surveillance and "public opinion management."[47]

Implications for data-driven authoritarianism: While some forms of AI-powered surveillance (such as traffic monitoring systems) can be benign tools for improving governance, **the use of these tools to track people directly impacts civilian rights to privacy, freedom of assembly, and freedom of movement**. In democracies, debates are taking place around the acceptable use of AI image recognition capabilities; they were used during the 2024 Paris Olympic Games, for instance, to monitor the density and movement of crowds, but not to identify faces.[48]

In closed settings, however, there is little space for civil society to challenge or constrain government use of AI surveillance tools. In China's "smart cities," data is constantly fed into the cloud infrastructure.[49] There, it is processed by AI algorithms, which advise police on where to deploy forces more efficiently and help, for instance, to differentiate between protests that can be safely ignored and those that constitute a genuine threat to regime security. In Hangzhou, the city brain algorithms and infrastructure reduce emergency services' response times—for example, by creating a free passage for police vehicles.[50] This shift speeds up the response to genuine crises, but it also means that protests have less time to form before being quelled. **In Xinjiang, digital surveillance tools including facial recognition cameras are linked to draconian algorithmic controls on people's movements.**[51] Interlinked "city brains" will make it increasingly difficult for China's citizens to travel to other cities to raise complaints with the government in a process commonly known as petitioning.[52]

In China's "smart cities," AI algorithms help ensure that protests have less time to form before being quelled.

The global spread of AI-enabled surveillance may also impact public participation in government decision making. Josh Chin and Liza Lin have demonstrated how PRC authorities view data surveillance as an alternative to relying on feedback from below to understand social trends and optimize governance.[53] Whether or not this technocratic approach proves effective, it is a tempting offer for authoritarian-minded political actors.[54]

The democracy impacts of *generative* AI tools, such as ChatGPT, require a broader assessment that lies beyond the scope of this analysis. For propagandists, they are a clear asset, making it possible to produce more convincing and customized messages at a wider scale.[55] In chatbot form, they may frustrate censors by producing unpredictable text responses. Yet custom tools that leverage AI language processing for censorship can instead speed up their work, making it possible to automate complex moderation tasks.[56] Notably, in semi-open settings, LLM-based social media-monitoring tools could also be used simply to keep tabs on dissent. **The application of LLMs and other generative AI tools to stifle regime critics or enforce political orthodoxy erodes the fundamental democratic right to freedom of expression.**

The global outlook: PRC-sourced AI-for-surveillance solutions have already diffused to over eighty authoritarian and democratic countries worldwide.[57] According to JVSG, a video surveillance software tool provider, as of the first through third fiscal quarters of 2024, Hikvision and Dahua jointly made up roughly 34 percent of the global market for surveillance cameras.[58] Since systems from different companies are not interoperable and it is expensive to change suppliers—the so-called **lock-in effect**—countries that have come to be reliant on China-produced surveillance tools will likely stick with PRC providers for the near future. Kuala Lumpur, the first municipality to have imported a city brain (focused on traffic surveillance) from Alibaba in 2018, has since then increased cooperation with China in related technology fields, such as digital twins.[59]

PRC-sourced AI-for-surveillance solutions have already diffused to over eighty countries worldwide, and countries that have come to be reliant on these China-produced surveillance tools will likely stick with PRC providers.

It is also likely that many existing Chinese smart city projects will be updated to become city brains. In November 2024, Lenovo (a Hong Kong–based multinational firm with a PRC company as its largest shareholder) announced that it would introduce generative AI to the city of Barcelona and other municipalities via its Lenovo VINA solution.[60] VINA, in turn, relies on the NVIDIA Metropolis and NVIDIA AI Blueprint for video search and summarization, which allows city operators to query large amounts of video footage quickly and extract information of interest. The system can prioritize among data flows and highlights those that are most critical to city operations. Even though Lenovo does not label its product as such, these capabilities introduce actionable intelligence into smart city products in much the same manner as AI “city brains.” Also, in November 2024, Lenovo announced a strategic cooperation agreement with Hongxin Electronics Technology Group on developing AI city brains.[61]

Advanced surveillance systems can be found in countries across the political spectrum, from established democracies like the United Kingdom—where it can be hoped that privacy regulations and rule-of-law safeguards will help to mitigate excessive data fusion—to autocratic settings such as Cambodia. In these latter settings, they are likely to face few legal or normative roadblocks, although practical and logistical constraints may still mean that their deployment will look different than China’s domestic approach. For instance, in some countries where authorities have managed to construct vast surveillance infrastructures, the data is not being used to draw conclusions at a population level. Rather, it is stored up and then used haphazardly and inefficiently to target specific individuals of interest to the state.[62]

The PRC companies currently engaged in LLM production are now eying the prospects for expansion abroad,[63] although entering new language markets presents technical challenges.[64] In some markets, domestic alternatives such as the United Arab Emirates' Jais or Falcon (whose creator G42 has a highly publicized partnership with Microsoft) have a competitive advantage in vying for the public-security market.[65] Competition appears to be lighter in Southeast Asia, where Alibaba Group Holding has launched its SeaLLM, which is tailored to the local languages in Malaysia, Laos, Vietnam, Indonesia, Cambodia, the Philippines, and Burma.[66] It is conceivable that China's domestic experience will put PRC vendors in a position to advise other governments in highly repressive settings (such as Burma, Venezuela, or Cuba) on tailoring generative AI to meet censorship goals.

NEURO- AND IMMERSIVE TECHNOLOGIES MAKE NEW DATA AVAILABLE

How does it work? Though distinct, technologies related to the metaverse and neurotechnologies are notable for their capacity to provide access to previously untapped types of data. Specifically, they can offer digital readouts that speak not only to subjects' outward behavior, but also their inner mental and emotional states.

The "metaverse" is a loose term generally used to describe digital spaces where users can interact while experiencing persistent virtual worlds. Although some have used this concept to refer to traditional, screen-based online gaming platforms, speaking of the metaverse often implies the use of **virtual reality** (headsets completely immerse users in a virtual world) or **augmented reality** (users see a virtual world projected onto the real world through a phone, a headset, or "smart glasses").[67] In order to situate the user in immersive experiences, virtual reality headsets must collect data on pupil dilation, eye movement, and other subtle physical reactions (some "smart glasses" do the same, albeit to a lesser extent).

These subtle physical cues can provide information that would be invisible to a human observer regarding users' medical conditions and mental states. For instance, advertisers could track physiological reactions to determine whether someone found the sight of a passing car appealing.[68] With these kinds of tracking capabilities, immersive technologies could serve as something of a more effective cousin of emotion recognition technology, which makes similar inferences generally on the basis of video data.[69] System operators can draw inferences about metaverse users' intended actions, based on their previous decision making, and draw on distinctive behavior patterns to track specific individuals across platforms.[70]

"Metaverse" and neurotechnologies can offer digital readouts that speak not only to subjects' outward behavior, but also their inner mental and emotional states.

While metaverse technologies monitor subtle physiological cues, **neurotechnologies consist of devices that monitor or intervene in brain activity directly**.[71] They can be either **invasive** (implants that require surgically cutting into someone's skull) or **non-implantable devices** (headsets or wearables). Experimental uses have shown that **brain-computer interfaces (BCIs)** and other neurotechnologies can be used to monitor brain activity (for example, they have succeeded in producing rough verbal renditions of a story that a user imagines telling);[72] to help a user control a computer cursor or prosthetic limb;[73] or, most invasively, to "remote control" behavior by activating specific parts of the brain. U.S. and Brazilian researchers have conducted experiments where invasive BCIs were used to force mice to eat, even if they did not want to, and to insert artificial memories of fear.[74] Although the term may make us think of cutting-edge experimental applications such as the chip-based Neuralink, neurotechnologies are already in wider use than many people realize. Wearable neurotechnologies, for instance, are already being used by employers to monitor fatigue,[75] marketed as remedies for depression,[76] and explored by gamers as alternatives to traditional controllers.[77]

China's progress to date: Compared to other technologies covered in this report, China's research and deployment of technologies associated with the metaverse is less striking. In neurotechnologies, however, it has world-class capabilities.

While the PRC is a major global market for VR sales, experiencing the metaverse via augmented or virtual reality is still quite rare relative to the size of the country's population. In 2022, around one million headsets enabling such immersive experiences were shipped within the country.[78] With the recent wave of global attention to AI, industry giants such as Baidu have refocused on developing LLMs.[79] Nonetheless, Beijing is avid to get ahead of the curve. **Indeed, CCP ideologues have speculated about using the metaverse as an educational tool to immerse school children in compulsory ideological material.**[80] Chinese tech companies have developed VR products that either explicitly provide ideological instruction or simply reinforce themes and values favored by CCP leadership—for example, through scenes set in ancient China.[81]

From 2019 onward, the PRC has led globally in producing publications on brain-computer interfaces, even as U.S. publications began to drop off.[82] Shanghai academics have worked at the intersection of the metaverse and neurotechnologies: They have conducted experiments using **electroencephalography** (EEG, a technique wherein a tool is placed on the scalp to measure brain waves) to assess people's emotional reactions as they experience 3D worlds.[83] According to researchers at Georgetown's CSET, China has achieved world-class capabilities in BCIs; PRC developers have traditionally focused on wearable BCI devices, although they are turning more attention to implants.[84] Chinese researchers have experimented with the introduction of neurotechnologies in classrooms to monitor student performance,[85] as well as contemplated law-enforcement applications (see more below). Party ethical guidelines anticipate the use of BCIs for cognitive enhancement.[86]

Neurotechnologies are already in wider use than many people realize, and the PRC has world-class capabilities in this domain.

Implications for data-driven authoritarianism: Although still limited in their uptake, both neuro- and immersive technologies represent a sea change in terms of the types of personal data that can be accessed. Technologies that infer, and potentially influence, mental states have vast implications for democracy, primarily impacting the right to privacy (intimate tracking of behavior) and the right to agency on which democratic citizenship depends.

> Technologies that infer, and potentially influence, mental states have vast implications for democracy, primarily impacting the rights to privacy and agency on which democratic citizenship depends.

One critical question is whether authorities will leverage neurotechnologies or body-based data to make determinations about suspects' thoughts and feelings in courts or at police stations.[87] This possibility is not mere science fiction: In December 2023, a researcher from the Graduate School of the People's Police University of China, Langfang, Hebei, examined the possible use cases for BCIs in police work—for instance, **the use of brainwave monitors as a kind of next-level polygraph during interrogation** to help gauge whether the interrogee is experiencing fear or anxiety.[88] While current BCI technologies, which rely on external non-surgical methods, are very low in accuracy, PRC companies are working on implantable devices (such as NeuraMatrix) to obtain more accurate results.[89] Furthermore, in 2023, one vendor at a Dubai surveillance expo offered a headset marketed as a brain wave reader able to discern when subjects under interrogation are lying.[90]

Virtual legal proceedings, meanwhile, may be marketed as a way to make justice more efficient or accessible, but they will open the door to highly intrusive surveillance. The Siming District Court in Xiamen, China, has for instance already experimented with holding trials in the metaverse.[91] A court in democratic Colombia has done the same.[92] Notably, emotion-recognition technologies—generally considered unreliable—were already being marketed in the PRC for purposes of interrogation and threat detection, suggesting that authorities will likely be eager to leverage data from emerging neuro- and immersive technologies for similar ends.[93]

The prospect of security forces accessing *private consumer data* from the metaverse and neurotechnologies presents even wider concerns. For example, police might try to access the phone or cloud-based apps with which neurotechnologies are synchronized. **Data laws in the PRC effectively ensure that data from neurotechnologies or "commercial" metaverse providers would be accessible to state authorities,** enabling them to make determinations about users' personal associations, political attitudes, and psychological vulnerabilities.

These intimate (if sometimes flawed) mental portraits could help authorities to single out potential dissenters for targeting. They could also enable next-generation influence operations—including manipulation of user experiences in virtual worlds themselves, which will further blur the boundaries between reality and fiction. Finally and most speculatively, neurotechnologies could shake the fundaments of democracy if malicious actors acquired the ability to alter voters' memories or incentives through engaging in "brainjacking," which is defined as the unapproved control of another subject's electronic brain implant.[94]

As the range of technologies with the potential to encroach on mental privacy widens, **the expert community has begun debating how to guard against the novel human rights threats they present**. Some argue for the elaboration of new **"neuro-rights,"** while others contend that the focus should be on thinking through how established rights, such as the rights to privacy and mental integrity, apply in the context of neurotechnologies.[95]

The global outlook: Currently, PRC companies are still second-tier players in the global market for AR/VR interfaces. As of the first fiscal quarter of 2024, China's most successful AR/VR company PICO (owned by ByteDance) had a global market share of 7 percent, compared to Meta's 64 percent.[96] It has multiple partnerships, including with Palo Alto–based neurotechnologies company SyncThink to introduce eye tracking for medical purposes to PICO XR devices.[97] PICO is also collaborating with Wisear, a Paris-based startup, to integrate earphones which are controlled by facial expressions with PICO's headset.[98] Until at least 2030, the AR/VR market is anticipated to see its strongest growth in the Asia-Pacific region, North America, and Europe.[99] While most AR/VR sets, including those produced in China, will be bought in those regions, growing sensitivities around PRC-sourced technology might hamper adoption of Chinese AR/VR systems down the road. PRC immersive technologies could also find promising markets in the Middle East, where governments are enthusiastic about the metaverse and sales are expected to rise from US $4 billion to US $69 billion by 2031.[100] Compared to established democracies, Beijing's digital authoritarian practices may raise fewer red flags in the affluent but undemocratic Gulf States.[101] The trends in neurotechnologies are broadly similar.[102]

QUANTUM TECHNOLOGIES AID WITH ACCESSING EXISTING DATA

How does it work? Quantum computers leverage the properties of quantum mechanisms to solve certain types of mathematical problems much faster than traditional computers. Using specialized hardware, they perform operations with ***qubits***, which can exist in more than one state at a time, as opposed to traditional bits that represent only either 1 or 0. This capability provides an advantage for certain computing tasks—which happens to include cracking the public-key encryption that keeps most of today's online communication safe from prying eyes. If a state were to build sufficiently powerful quantum computers, it could theoretically **decrypt large amounts of online data** (whether enterprise data or private communications) currently stored on the internet and protected by encryption. Moreover, the speed and power of quantum computers enable them to **perform data-intensive tasks much more quickly than traditional computers**, meaning that they could support advances in the use at scale of the AI surveillance techniques described above.[103] Thus, quantum computing is yet another way to access and make sense of data.

Quantum computers that are powerful enough to decrypt large amounts of encrypted online data could be available in the early 2030s.

Though quantum computers are not yet at the stage of development where they would be useful to crack encryption, the current estimate is that such computers could be available in the early 2030s.[104] Therefore, **states and private companies have already started developing quantum-proof cryptography algorithms and protocols** as well as special quantum communications technology that is resilient against decryption via quantum computers.

China's progress to date: The PRC is a leader in quantum computing (used to decrypt communications), quantum communications (the use of novel quantum hardware to relay information, in theory offering foolproof encryption), and designing approaches to quantum-proof encryption that can be implemented on present-day computers.[105] China has dedicated significant resources in quantum technology research and development, investing four times the amount of planned governmental spending in the United States as of 2023.[106] PRC researchers have also published intensively in various fields related to quantum, taking the lead in the subfields of post-quantum cryptography (33.9 percent vs. a mere 12.1 for the United States, the next closest contender) and quantum communication (33.6 percent vs. 16.8 percent for the U.S. share).[107] With a research budget in the billions of dollars, the Hefei National Laboratory for Physical Sciences is responsible for most of China's achievements in this area.[108] Origin Quantum and QuantumCTek, both based in Hefei, are among the PRC's leading quantum companies.[109]

Implications for data-driven authoritarianism: While there are numerous reasons for Beijing to pursue advances in quantum—they will, for instance, help the PRC to shield its own information from other state actors—the prospects for accessing encrypted communications are one key factor.[110] The advent of quantum technologies presents two major threats to privacy, and thus to global democratic and human-rights norms.

First, **quantum computing is expected to eventually enable any state or non-state actor that possesses this technology to circumvent encryption that protects communications**. Second, if the quantum communications providers who are first-movers in this space adopt cryptography standards and equipment that include backdoors for official government use, information conveyed over quantum networks will be vulnerable to state surveillance—potentially either by the governments that import these technologies, or by the home countries of companies that provide quantum services. (Although quantum communications are believed to be invulnerable to compromise, the same is not true of the "nodes" currently needed to enable quantum communication over long distances.)[111] Therefore, control over quantum communications and cryptography is likely to prove a new sphere of interstate competition, with autocracies as well as democracies potentially seeking the advantage by building backdoors into quantum-proof encryption and subverting quantum communications infrastructure.

China has dedicated significant resources in quantum technology research and development, investing four times the amount of planned governmental spending in the United States as of 2023.

This geopolitical contest will impact the rights to privacy and free expression of independent journalists, human rights defenders, and opposition politicians who rely on encryption to keep their communications or identities private from authoritarian state actors. Of particular note, some authoritarian (and possibly also democratic) regimes are believed to be collecting and storing encrypted data now with the expectation that in the future, they will be able to access this saved-up data using quantum computers. Autocrats could then scan through the past digital messages of their political opponents and leverage the information they find for blackmail, doxing, or even prosecution.[112]

Given that many governments' digital surveillance systems currently collect more data than security services are actually able to process—even with the help of advanced technologies[113]—improvements in the processing power of AI surveillance tools will also affect the human rights landscape. Notably, Chinese tech platform Origin Quantum states on its website that its quantum computing technology can aid with speech and image recognition and processing as well as pattern matching more broadly, underscoring the potential symbiotic relationship between quantum computing and AI-powered surveillance.[114]

Some governments are believed to be collecting encrypted data now with the expectation that they will be able to access it in the future using quantum computers.

The global outlook: PRC quantum technology is likely to spread to Russia, with which Beijing has tested quantum communications via China's quantum satellite Mozi.[115] A next step that has been envisioned is establishing **a quantum communication network among the so-called BRICS countries**, whose members have recently expanded from the titular cohort of Brazil, Russia, India, China, and South Africa to include Egypt, Ethiopia, Iran, and the United Arab Emirates. Among these countries, **China is the leader when it comes to quantum technologies and would thereby be in a position to shape encryption standards and export technologies**. In 2019, the BRICS STI Framework Programme selected a project which aims to establish quantum communication channels utilizing the Chinese satellite Mozi and special fiber optics to link Russia, India, China, and South Africa.[116] Its current status is unclear.[117] In many free countries, PRC encryption standards are unlikely to be adopted, as there will be significant national security concerns regarding the use of Chinese encryption algorithms and quantum communication technologies.

DIGITAL CURRENCIES CAN BOTH CENTRALIZE AND DECENTRALIZE DATA

How does it work? **Digital currencies are assets used for payment that are native to digital form** (in contrast, for instance, to credit card–based online payments that technically represent a transfer of rights to physical fiat currency). Many, though not all, of these currencies rely on a **blockchain**, meaning transactions are recorded on an inalterable digital ledger stored across a network of computers. Digital currencies take two main forms, with starkly opposite implications for state power.

Cryptocurrencies, such as Bitcoin, rely on a decentralized system that records transactions without having to rely on a central issuing authority. Their value may or may not be pegged to an official state currency (as with so-called stablecoins). These currencies tend to dilute the state's power over financial transactions. Moreover, while cryptocurrencies' reliance on blockchain ensures an immutable record of transactions, users seeking to avoid scrutiny have been able to cover their traces by using tactics such as mixing services that pool and repeatedly transfer funds to hide their origins, or by mining new coin.[118] These qualities have made such features appealing to a range of actors—from nation-states or companies under U.S. sanctions and transnational criminal networks or political dissidents in authoritarian settings.[119]

Central bank digital currencies (CBDCs), in contrast, are—like traditional physical currencies—issued and controlled directly by official central banks. Unlike cash, however, they leave a digital trail. By removing the digital middlemen (such as banks, credit card providers, or mobile payment apps) between users and state authorities, CBDCs can make transactions more susceptible to state scrutiny and control.

While the PRC's central bank digital currency (CBDC) is not widely adopted either within the country or abroad, China has gone farther than most countries in experimenting with this technology.

China's progress to date: While the PRC's CBDC (which has come to be known variously as the digital renminbi, digital yuan, or e-CNY) is not widely adopted either within the country or abroad, China has gone further than most countries in experimenting with this technology.

PRC ambitions in this space can be traced back to the mid-2010s. CCP authorities envisioned their state-issued digital currency as a more centralized alternative to the two commercial payment platforms currently favored overwhelmingly by PRC citizens: Alipay and WeChat Pay, operated respectively by the private tech giants Alibaba and Tencent. Meanwhile, **cryptocurrencies, which are decentralized payment systems—and thus outside of the CCP's control—remain outlawed in China**.[120]

To date, many e-commerce (for example, JD.com) and transportation providers (for instance, Meituan) have started accepting e-CNY as a form of payment.[121] Its centralizing features, however, may be less than appealing to the Chinese public. E-CNY adoption among individuals has been lackluster, with most consumers thus far content to stick with WeChat Pay and AliPay.[122]

Implications for data-driven authoritarianism: Digital currencies impact both the **right to privacy** and citizens' **susceptibility to government financial control**.[123] In closed settings, the decentralization of financial data can empower opposition movements: Burma's shadow National Unity Government, for example, launched a cryptocurrency bank last year.[124] The bank (Spring Development Bank) enables it to continue raising money for its resistance against the military junta, which operates its own financial system led by the state central bank.

CBDCs are more appealing to authoritarian regimes, which—from Russia to China and Iran—have started to launch state-backed digital currencies. With a direct link between central banks and individuals, governments can immediately access and monitor user data, rather than having to request it from third-party financial intermediaries.[125] **Adoption of these currencies centralizes financial data—along with adjacent behavioral and geo-location data, which can be inferred from a user's financial transactions.** They also make it relatively straightforward for governments to penalize what they see as bad behavior by constricting or cutting off purchases.[126]

Central bank digital currencies make it easier for governments to immediately access and monitor user data, as well as to constrict or cut off purchases.

The e-CNY's design, in particular, increases the legibility of transactions to state authorities. PRC citizens can get an e-CNY account only through their mobile phone numbers, which ensures that every transaction can be traced back to an individual.[127] While users can access the e-CNY via commercial bank apps, they also have the option of downloading an app developed by China's central bank.[128] For children or elderly people who do not have smartphones, digital currency accounts are integrated into a person's physical ID card, giving state authorities insight into the whereabouts of individuals who were previously harder to trace.[129] Although the e-CNY allegedly features "managed anonymity," its implementation depends on a government that has an insatiable need for control and surveillance.[130]

As highly centralized currencies such as the e-CNY come into use internationally, anonymity will be compromised. In settings like the PRC, where authorities could previously requisition information from private financial service providers like Alipay fairly easily, a shift to CBDCs would mainly **remove friction from state financial surveillance and coercion efforts.**[131] They would make it possible, for instance, to deliver user data instantaneously and directly into state-controlled information systems, where it might be fed into AI-powered analytical tools. In open societies, legal and privacy safeguards could be established to guard against these abuses. On the other hand, in settings where private financial institutions enjoy relative autonomy but political leaders have authoritarian tendencies, CBDCs could represent a leap forward for state control.

The one area of overlap between authoritarian CDBCs and cryptocurrencies is that they represent an alternative to existing, Western-dominated financial systems and institutions. Specifically, they make foreign governments less dependent on SWIFT, a messaging system currently needed to make international payments which has been used to implement economic sanctions against Belarus, Iran, North Korea, and Russia. Thus, authoritarian regimes may find cryptocurrencies more appealing when operating outside their own borders. For example, cryptocurrencies—stolen or demanded as a ransom by hackers—are a major source of revenue for North Korea's diplomatically isolated regime.[132] The wide adoption of currencies such as Russia's digital ruble or China's digital renminbi may also hamper the ability of democracies to implement sanctions against authoritarian regimes.[133]

The global outlook: The PRC has started diffusing the e-CNY by engaging in a range of partnerships to facilitate cross-border payments. One of those initiatives is the mBridge project, a blockchain-based platform for large cross-border transactions between financial institutions, which was spearheaded by the Bank for International Settlements (BIS) together with the central banks of China, Hong Kong, Saudi Arabia, Thailand, and the United Arab Emirates.[134] The BIS dropped out of the project in November 2024, stating that the other partners were able to continue it themselves.[135] The e-CNY has quickly assumed a dominant role in transactions on this "multi-CBDC common platform," with nearly 50 percent carried out in Beijing's digital currency.[136] **There is not yet extensive uptake among individuals outside PRC borders**, however; for example, on the Google Play Store, the e-CNY app appears to have been downloaded only a bit over ten thousand times.[137] For comparison, the payment app Venmo has been downloaded more than fifty million times, and Google's app (for its relatively new generative AI tool, Gemini) has been downloaded over ten million times.

The wide adoption of currencies such as Russia's digital ruble or China's digital renminbi may also hamper the ability of democracies to implement sanctions against authoritarian regimes.

The CCP has some levers at its disposal to increase uptake of the e-CNY: For instance, netizens might be encouraged to embrace China's CBDC if its use is linked to special discounts on internationally popular Chinese shopping or social media apps. With the broad global trend toward online payments, and away from cash, **the e-CNY has an opportunity to gain traction, but only if China can propose practical use cases to induce people to adopt it**.[138] Adoption might be further limited if some countries start restricting the availability of the e-CNY for national security reasons.[139]

CONFRONTING THE SPREAD OF DATA-CENTRIC AUTHORITARIANISM

A survey of the emerging tech landscape shows how overt systems of state surveillance, highly invasive consumer technologies, and fundamental advances in computing are poised to shape the evolution of data-centric authoritarianism over the coming decade. **Together, they lay the groundwork for a system that can monitor our actions and attitudes in minute detail and then leverage that information to induce conformity.**

Across all four domains under scrutiny, Beijing has invested intensively in research that is positioning PRC developers to shape the trajectory of emerging tech development globally. As seen with Chinese companies' facial-recognition cameras, "safe cities," and other current-generation surveillance packages, it is very difficult if not impossible to prevent the cross-border diffusion of technologies outside the military sphere. Although governments are growing more concerned about PRC surveillance tools, it remains to be seen to what extent such retroactive concerns (such as the U.K. government's 2023 announcement on removing PRC-linked cameras from sensitive government sites) will alter the landscape.[140] **The diffusion of newer systems with clear state and security connections (such as quantum technologies and potentially CBDCs) may be limited by national security considerations**

in many, but not all, democracies—the BRICS grouping, notably, includes several Free states. Consumer technologies, such as wearable neurotech, have more potential to fly under the radar. Across various technological domains, PRC developers enjoy a cost advantage if favored by the state-directed economy, and their products offer the world's many autocratic and autocratizing states a way around even the limited rights-based export controls that might constrain vendors in democratic settings.

In this challenging context, it is critical for civil society and democratic governments to identify effective, forward-looking strategies for confronting the spread of data-centric authoritarianism and mitigating adverse impacts on human rights and democracy. In particular, they should build up a technological ecosystem infused with democratic values that can serve as an alternative to PRC offerings. To this end, there are seven critical steps they should consider.

It is critical for civil society and democratic governments to identify effective, forward-looking strategies for confronting the spread of data-centric authoritarianism and mitigating adverse impacts on human rights and democracy.

First, in order to confront data-centric authoritarianism, it will be critical to track its diffusion. Several research centers have started commendable efforts to map the diffusion of PRC surveillance technologies, but their data is stored in siloes across different institutions, and many have not been updated for some time.[141] Journalists, civil society activists, and researchers need to consult dozens of websites and research papers for insight into China's surveillance technology capabilities and exports. A central platform where data is collected and updated regularly would be valuable to not only get snapshots of projects such as PRC-built smart cities in Barcelona and elsewhere, but to track how they are evolving.

Second, open societies—including both established democracies and democrats in partly open "swing states"—need a roadmap for governing previously untapped, highly personal types of data collected by neurotechnologies and immersive interfaces. In a not too distant future, tapping into neurological and physiological cues on a person's mental state could become a regular practice of security services in authoritarian settings such as China and Russia. In democracies, real-time law enforcement access to brain-related data or personal data collected through immersive systems should be banned.

Third, as AI algorithms complicate the relationship between digital data sources and sensitive information about people, democracies and the democratic tech ecosystem have an obligation to keep those systems transparent. Building AI systems that are transparent should be a minimal baseline to help ensure that these systems do not inject bias into decisions which affect people's rights; that there are controls on fusing and integrating data in ways that could enable sensitive inferences about individuals or populations; and that the people whose data are being processed have avenues to hold the developers and deployers of AI systems accountable for their use.

Fourth, governments should foster, and civil society should push for, the development of privacy-preserving emerging technologies, building up a technological ecosystem infused with democratic values that can serve as an alternative to PRC offerings. For instance, central banks in open societies that opt to create CBDCs should build privacy protections into their design. In the case of the digital euro, the European Central Bank (ECB) is attempting to achieve this objective through pseudonymization of data regarding online transactions, as well as by enabling people in physical proximity to perform offline transactions via "wallets" stored on mobile devices, replicating the anonymity of cash.[142] (The e-CNY also has an offline option but little information has been provided about how anonymity would be upheld for those using it, in contrast to the ECB proposal.)[143] Democratic governments have also promoted exploration of privacy-preserving AI techniques such as federated machine learning, where training data is processed locally across different machines rather than centralized in one system.[144]

Civil society and democratic governments should build up a technological ecosystem infused with democratic values that can serve as an alternative to PRC offerings.

Fifth, democratic governments must resist the temptation to implant backdoors own quantum-proof encryption algorithms, just as they have resisted calls from law-enforcement agencies to mandate backdoors in traditional end-to-end encryption. Simultaneously, they should continue to take measures to delay China's progress toward developing quantum computers that are able to break encryption. In this vein, several countries as part of the Wassenaar Arrangement have already started to impose export controls on certain quantum computers.[145]

Sixth, civil society, especially groups working in Unfree and Partly Free settings, should speed their transition to quantum-resistant cryptography. States are already storing data now in order to decrypt it later when they have the quantum computers to do so. They are surely also harvesting data related to dissidents. While there are post-quantum cryptographic algorithms that have been vetted thoroughly, their relative novelty leaves some room for uncertainty. As a result, entities transiting to post-quantum cryptography usually add post-quantum encryption on top of traditional encryption, which means there is a fallback mechanism if vulnerabilities are found in post-quantum encryption. The private messenger Signal is among the early adopters of this approach.[146] Yet large parts of civil society's communications—including those over Viber, WeChat, Line, WhatsApp, Proton Mail, and Gmail—are still exposed to harvest-now, decrypt-later attacks.[147]

Finally, democratic governments and civil society should engage in international standard-setting fora to counter the normalization of authoritarian digital approaches. As PRC companies gain sway in various emerging tech markets, they are also in a position to influence the technical standards that shape the development of these systems globally—an explicit goal of CCP leadership.[148] For example, Beijing has proposed the creation of a

Digital Identity System that would link people's participation in the metaverse with records of their real identity and social characteristics (such as occupation status and social media handles).[149] This fundamental challenge to online anonymity would standardize surveillance on a global level. Prodemocratic actors should monitor and push back against the adoption of standards that will turn emerging tech tools into promising instruments of data-driven authoritarianism.

CONCLUSION

After the end of the Cold War, democratic nations—in both the East and the West—played the leading role in technological innovation and development. This state of affairs has changed markedly with China's rise as a major technological power. Previously, Beijing had to repurpose externally designed technologies to fit its public-security environment. **PRC companies can now design AI systems with authoritarian characteristics built in from the outset,** as with facial recognition capabilities intended to detect Uyghurs and other targeted ethnic minorities.[150] The diffusion of these authoritarian approaches presents grave concerns for democracy and human rights worldwide.

While each emerging technology in itself presents challenges for human rights and democratic values, the full stakes become clear only when all of these new capabilities are analyzed together. In the coming years, data on thoughts and emotions will become widespread. The quantum transition might provide a window of opportunity for law enforcement across the globe to install backdoors, not to mention freely access communications protected by pre-quantum encryption. These capacities will intersect with others, such as advances in genomics, that lie beyond the scope of this report. Furthermore, the growing opacity of data streams and the AI systems that process them is slowly eroding democratic accountability, even as these technologies strengthen the hand of autocrats seeking to rule through manipulation and repression.

The rapid and complex technological transition we are witnessing suits authoritarian regimes, and Beijing in particular. It presents a window of opportunity not only to challenge the technological edge of democratic states, but also to weaken the established rights to privacy, anonymity, and freedom of expression and assembly. The danger of data-driven authoritarianism can only be mitigated if democracies recognize the centrality of data in today's governance systems and work consciously to present an alternative to authoritarian approaches. It is high time that democratic societies double down on building data and technological ecosystems that are transparent, accountable, and infused with democratic values. **Leveraging their robust innovation ecosystems in tandem with the power of vibrant, pluralistic civil societies, democracies must chart a rights-respecting path to unlock the benefits of emerging technologies for people around the globe.**

> The danger of data-driven authoritarianism can only be mitigated if democracies recognize the centrality of data in today's governance systems and work consciously to present an alternative to authoritarian approaches.

ENDNOTES

[1] For instance, please see: *Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights*, Article 19, January 2021, www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf; and Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy*, 30:1 (January 2019): 53-67, https://muse.jhu.edu/article/713722.

[2] China's Algorithms of Repression," Human Rights Watch, 1 May 2019, www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

[3] Samantha Hoffman, *Double-Edged Sword: China's Sharp Power Exploitation of Emerging Technologies*, National Endowment for Democracy, April 2021, www.ned.org/wp-content/uploads/2021/04/Double-Edged-Sword-Chinas-Sharp-Power-Exploitation-of-Emerging-Technologies-Hoffman-April-2021.pdf.

[4] For more information, please see: Josh Chin and Liza Lin, *Surveillance State: Inside China's Quest to Launch a New Era of Social Control* (New York: MacMillan, 2022); and Samantha Hoffman, "China's Tech-Enhanced Authoritarianism," *Journal of Democracy,* 33:2 (April 2022): 76-89, www.journalofdemocracy.org/articles/chinas-tech-enhanced-authoritarianism/.

[5] *The Digital Silk Road: China and the Rise of Digital Repression in the Indo-Pacific*, Article 19, March 2024, www.article19.org/wp-content/uploads/2024/04/DSR_final.pdf; and *The Global Expansion of PRC Surveillance Technology,* International Republican Institute, 10 July 2024, www.iri.org/resources/the-global-expansion-of-prc-surveillance-technology/.

[6] Greg Walton, *China's Golden Shield Corporations and the Development of Surveillance Technology in the People's Republic of China*, (Montreal: International Centre for Human Rights and Democratic Development), 2001, https://ora.ox.ac.uk/objects/uuid:084840ac-b192-407b-ab6c-f8f810310369.

[7] Valentin Weber, *The Diffusion of Cyber Norms: Technospheres, Sovereignty, and Power*, submitted doctoral thesis, Oxford University, 2021, https://ora.ox.ac.uk/objects/uuid:57f267fa-777d-41c7-a238-3b9dcd42e5f6/files/dn296wz44p.

[8] Zeyi Yang, "The World's Biggest Surveillance Company You've Never Heard Of," *MIT Technology Review*, 22 June 2022, www.technologyreview.com/2022/06/22/1054586/hikvision-worlds-biggest-surveillance-company/; and Simon Migliano and Samuel Woodhams, "Global Locations of Hikvision & Dahua Surveillance Cameras," Top10VPN, 16 November 2021, www.top10vpn.com/research/hikvision-dahua-surveillance-cameras-global-locations/.

[9] Dahlia Peterson, "How China Harnesses Data Fusion to Make Sense of Surveillance Data," Brookings Institution, (blog commentary), 23 September 2021, www.brookings.edu/articles/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/.

[10] Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models*, Brookings Institution, 26 August 2019, www.brookings.edu/research/exporting-digital-authoritarianism/. It bears noting that technological tools for repression (including deep-packet inspection to enable fine-grained filtering of online content, efforts to create a "sovereign internet" that can be isolated from the global network, and facial-recognition cameras that have been used to target antiwar protesters and draft dodgers) have come to play an increasingly significant role in Russia's own repressive model since 2019.

[11] Weber, *The Diffusion of Cyber Norms: Technospheres, Sovereignty, and Power.*

[12] Valentin Weber, *The Diffusion of Cyber Norms; The Global Expansion of PRC Surveillance Technology: Implications for Human Rights and International Governance*, International Republican Institute, 2024, www.iri.org/wp-content/uploads/2024/07/IRI-TextOre-PRC-Export-of-Surveillance-and-Security-Technologies-and-Its-Impact-on-Human-Rights-Globally.pdf; and Gaspar Pisanu and Veronica Arroyo, "Surveillance Tech in Latin America: Made Abroad, Deployed at Home," Access Now, 13 January 2023, www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home/.

[13] Minxin Pei, "Why China Can't Export Its Model of Surveillance," *Foreign Affairs*, 6 February 2024, www.foreignaffairs.com/china/why-china-cant-export-its-model-surveillance.

[14] John O. Koehler, Stasi: *The Untold Story of the East German Secret Police*, (Boulder, Colorado: Westview Press), 1999, https://archive.nytimes.com/www.nytimes.com/books/first/k/koehler-stasi.html?_r=1.

[15] Pei, "Why China Can't Export Its Model of Surveillance."

16 Precise numbers vary, with some estimates falling lower than one million, and many others being significantly higher. For additional context, please see: "What We Know About the Basij," ABC News, 13 October 2022, www.abc.net.au/news/2022-10-13/what-we-know-about-the-basij-in-iran/101534184; Morad Vaisibiame, "Anatomy Of Suppression In Iran: The Institutions & Tactics That Repeatedly Quash Dissent," Radio Free Europe/Radio Liberty, 21 August 2018, https://en.radiofarda.com/a/layers-of-suppression-in-Islamic-republic-Iran/29437016.html; Tara Kangarlou, "The Brutal Militia Trained to Kill for Iran's Islamic Regime," *Time*, 5 December 2022, https://time.com/6238623/iran-basij-militia-meaning-mahsa-amini/; and Saied Golkar, "Iran's Coercive Apparatus: Capacity and Desire," Washington Institute for Near-East Policy, 5 January 2018, www.washingtoninstitute.org/policy-analysis/irans-coercive-apparatus-capacity-and-desire.

17 *The Global Expansion of PRC Surveillance Technology*.

18 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.

19 Weber, *The Diffusion of Cyber Norms: Technospheres, Sovereignty, and Power.*

20 For more information, please consult: Nicholas Kaufman, "Shein, Temu, and Chinese e-Commerce," U.S.-China Economic and Security Review Commission, 14 April 2023, www.uscc.gov/research/shein-temu-and-chinese-e-commerce-data-risks-sourcing-violations-and-trade-loopholes; Seth Kaplan "China's Censorship Reaches Globally Through WeChat," *Foreign Policy*, 28 February 2023, https://foreignpolicy.com/2023/02/28/wechat-censorship-china-tiktok/; and Jeffrey Knockel et al., "We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus," Citizen Lab, 7 May 2020, https://citizenlab.ca/2020/05/we-chat-they-watch/.

21 Martin Beraja et al., "Exporting the Surveillance State via Trade in AI," NBER Working Paper 31676, 2-3, September 2023, https://www.nber.org/papers/w31676.

22 Weber, *The Diffusion of Cyber Norms: Technospheres, Sovereignty, and Power.*

23 For additional context, please see: "National Intelligence Law of the People's Republic of China," the National People's Congress of the People's Republic of China, 27 June 2017, https://web.archive.org/web/20190216061930/http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm (original source material in Mandarin Chinese); and Matthew Johnson, *China's Grand Strategy for Global Data Dominance*, Hoover Institution, April 2023, www.hoover.org/sites/default/files/research/docs/Johnson_ChinasGrandStrategy_Web.pdf.

24 Oliver Holmes and Tom Phillips, "Gui Minhai: The Strange Disappearance of a Publisher Who Riled China's Elite," *Guardian*, 7 December 2015, www.theguardian.com/world/2015/dec/08/gui-minhai-the-strange-disappearance-of-a-publisher-who-riled-chinas-elite.

25 For more information, please reference: "Nepal Has a Lot to Gain from the Open, Global Internet. So Why Is the Country Closing the Doors on It?," Internet Society, 1 December 2023, www.internetsociety.org/resources/internet-fragmentation/nepals-national-internet-gateway/; and Sarah Zaman, "Pakistani Minister Confirms Internet Firewall, Rejects Censorship Concerns," Voice of America, 26 July 2024, www.voanews.com/a/pakistani-minister-confirms-internet-firewall-rejects-censorship-concerns/7714552.html.

26 For further context, please consult: Jamie Gaida et al., "ASPI's Critical Technology Tracker," March 2023, www.aspi.org.au/report/critical-technology-tracker; Owen Daniels, *The PRC's Efforts Abroad: CSET Analyses of China's Technology Policies and Ecosystem*, Center for Security and Emerging Technology (CSET), September 2023, https://cset.georgetown.edu/publication/the-prcs-efforts-abroad/; and "Vision for Competitiveness Mid-Decade Opportunities for Strategic Victory," Special Competitive Studies Project (SCSP), May 2024, www.scsp.ai/reports/vision/.

27 For the Forum's prior work on these issues, please see: Krzysztof Izdebski, Teona Turashvili, and Haykuhi Harutyunyan, *The Digitalization of Democracy: How Technology is Changing Government Accountability*, National Endowment for Democracy, 27 March 2023, www.ned.org/digitalization-democracy-technology-changing-government-accountability/; and Beth Kerley, *Setting Democratic Ground Rules for AI: Civil Society Strategies*, National Endowment for Democracy, 19 October 2023, www.ned.org/setting-democratic-ground-rules-for-ai-civil-society-strategies/.

28 On the importance of demand-side factors in the surveillance market, please consult: Sheena Chestnut Greitens, *Dealing with Demand for China's Global Surveillance Exports*, Brookings Institution, April 2020, www.brookings.edu/articles/dealing-with-demand-for-chinas-global-surveillance-exports/.

29 Daria Impiombato et al., "Persuasive Technologies in China: Implications for the Future of National Security," Australian Strategic Policy Institute, 26 November 2024, www.aspi.org.au/report/persuasive-technologies-china-implications-future-national-security.

30 On the range of ways in which autocrats can use the "data exhaust" produced by tech exports to project power across borders, please reference: Christopher Walker, Shanthi Kalathil, and Jessica Ludwig, "The Cutting Edge of Sharp Power," *Journal of Democracy*, 31:1 (January 2020): 124-137, www.ned.org/wp-content/uploads/2020/01/Cutting-Edge-Sharp-Power-Walker-Kalathil-Ludwig.pdf.

31 Joss Wright, Valentin Weber, and Gregory Finn Walton, "Identifying Potential Emerging Human Rights Implications in Chinese Smart Cities via Machine-Learning Aided Patent Analysis," *Internet Policy Review*, 12:3 (28 July 2023), https://policyreview.info/articles/analysis/identifying-potential-human-rights-implications-in-chinese-smart-cities.

32 Wright, Weber, and Walton, "Identifying Potential Emerging Human Rights Implications in Chinese Smart Cities via Machine-Learning Aided Patent Analysis."

33 For more information, please see: Stephen Chen, "Across China, 'City Brains,' Are Changing How the Government Runs," *South China Morning Post*, 10 June 2021, www.scmp.com/news/china/science/article/3136661/across-china-ai-city-brains-are-changing-how-government-runs; and Valentin Weber, "China's Smart Cities and the Future of Geopolitics," German Council on Foreign Relations (DGAP), 11 May 2023, https://dgap.org/en/research/publications/chinas-smart-cities-and-future-geopolitics.

34 Valentin Weber, "China's Smart Cities and the Future of Geopolitics."

35 For more information about Large Language Models (LLMs), please reference Cloudflare's definition, cited here: "What Is a Large Language Model (LLM)?," Cloudflare, www.cloudflare.com/learning/ai/what-is-large-language-model/.

36 For more information, please consult ASPI's Critical Technology Tracker, accessible here: https://techtracker.aspi.org.au/tech/adversarial-ai/research-contribution/?c1=us&c2=cn.

37 For additional context, please see Stanford University's Global AI Vibrancy Tool, accessible here: https://aiindex.stanford.edu/vibrancy/.

38 On the global proliferation of PRC smart cities, please see: Beth Kerley et al., *Smart Cities and Democratic Vulnerabilities*, National Endowment for Democracy, 15 December 2022, www.ned.org/smart-cities-and-democratic-vulnerabilities/.

39 For more information, please consult: Katherine Atha et al., "China's Smart Cities Development," U.S.-China Economic and Security Review Commission, 29 April 2020, www.uscc.gov/research/chinas-smart-cities-development; and Valentin Weber, "China's Smart Cities and the Future of Geopolitics."

40 Wright, Weber, and Walton, "Identifying Potential Emerging Human Rights Implications in Chinese Smart Cities via Machine-Learning Aided Patent Analysis."

41 Stella Chen, "Petitioning," China Media Project, 20 May 2022, https://chinamediaproject.org/the_ccp_dictionary/petitioning/. Weber, "China's Smart Cities and the Future of Geopolitics."

42 Amy Qin, John Liu, and Amy Chang Chien, "China's Surveillance State Hits Rare Resistance From Its Own Subjects," *New York Times*, 14 July 2022, www.nytimes.com/2022/07/14/business/china-data-privacy.html.

43 Tao Zhu et al., "The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions," USENIX Security Symposium, Washington, D.C., August 2013, www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/zhu.

44 Information taken from National Endowment for Democracy Workshop in Palo Alto, April 2024. For more information, please see: Ryan McMorrow and Tina Hu, "China Deploys Censors to Create Socialist AI," *Financial Times*, 17 July 2024, www.ft.com/content/10975044-f194-4513-857b-e17491d2a9e9; and Stephen McDonnell, "Elusive Ernie: China's New Chatbot Has a Censorship Problem," BBC, 8 September 2023, www.bbc.com/news/world-asia-66727459.

45 For additional information, please reference: Nicholas Welch and Jordan Schneider, "China's Censors Are Afraid of What Chatbots Might Say," *Foreign Policy*, 3 March 2023, https://foreignpolicy.com/2023/03/03/china-censors-chatbots-artificial-intelligence/. Among other challenges, the PRC's own prior success in censoring Mandarin-language digital environments may also, paradoxically, have left its engineers with little training data available to "teach" LLMs what kind of expression they ought to censor. For further reading on this topic, please consult: Eddie Yang and Margaret E. Roberts, "The Authoritarian Data Problem," *Journal of Democracy*, 34:4 (October 2023): 141-150, www.journalofdemocracy.org/articles/the-authoritarian-data-problem/.

46 Britney Nguyen, "9 of China's Top AI Models and Startups," Quartz, 19 September 2024, https://qz.com/china-top-ai-models-startups-baidu-alibaba-bytedance-1851563639.

47 Impiombato et al., "Persuasive Technologies in China."

48 Théophane Hartmann, "Paris Olympic Games Are a Test for AI Video Surveillance," Euractiv, 24 July 2024, www.euractiv.com/section/artificial-intelligence/news/paris-olympic-games-are-a-test-for-ai-video-surveillance/.

49 Weber, “China’s Smart Cities and the Future of Geopolitics.”

50 For more information, please see: “How ET City Brain Is Transforming the Way We Live – One City at a Time,” Alibaba Cloud Community, 11 June 2018, www.alibabacloud.com/blog/how-et-city-brain-is-transforming-the-way-we-live-one-city-at-a-time_593745.

51 Ross Andersen, “The Panopticon Is Already Here,” *Atlantic*, September 2020, www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

52 Stella Chen, “Petitioning.”

53 Chin and Lin, *Surveillance State.*

54 Some commentators have speculated that such approaches will entrap governments in a dangerous feedback loop of distorted information. For more information, please see: Henry Farrell, Abraham Newman, and Jeremy Wallace, “Spirals of Delusion: How AI Distorts Decision-Making and Makes Dictators More Dangerous,” *Foreign Affairs*, 31 August 2022, www.foreignaffairs.com/world/spirals-delusion-artificial-intelligence-decision-making.

55 For additional context, please reference the Forum’s recent report on gen AI and information manipulation: Beatriz Saab, *Manufacturing Deceit: How Generative AI Supercharges Information Manipulation*, National Endowment for Democracy, 18 June 2024, www.ned.org/manufacturing-deceit-how-generative-ai-supercharges-information-manipulation/. Furthermore, scholars have warned of the potential for mass-produced authoritarian propaganda, if picked up in training data, to skew the output of AI tools in free societies. For more information on this topic, please consult: Yang and Roberts, “The Authoritarian Data Problem.”

56 Freedom House’s 2023 “Freedom on the Net” report notes that some governments have, either directly or implicitly by demanding rapid takedowns, forced online platforms to apply AI content moderation tools (which or may not involve LLMs specifically). Please see the “Freedom on the Net” report for more information, accessible here: https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.

57 Beraja et al., “Exporting the Surveillance State via Trade in AI.”

58 For more information, please see: “Popular CCTV Camera Brands – JVSG Ratings,” JVSG, 2024, www.jvsg.com/ipica-ratings/.

59 Hazel Moises, “China and Malaysia Collaborate on ‘Digital Twin Cities’ Project to Drive Data Innovation,” W.Media, 12 July 2024, https://w.media/china-and-malaysia-collaborate-on-digital-twin-cities-project-to-drive-data-innovation/.

60 Jeff Esposito, “Lenovo Expands Generative AI Solutions for Smart Cities and Spaces Using NVIDIA AI Enterprise and NVIDIA AI Blueprints,” Lenovo StoryHub, 5 November 2024, https://news.lenovo.com/lenovo-expands-generative-ai-solutions-for-smart-cities/.

61 “[Win-Win Cooperation] Three-Party Alliance! This FPC Company Opens a New Chapter in AI Strategy,” PCB Network City ISPCAIGPCA, Weixin Official Accounts Platform, 2 December 2024, http://mp.weixin.qq.com/s?__biz=MjM5MTI3NzY2Mg==&mid=2651630891&idx=2&sn=07b04bc5f912d34e08ebf2af1b80381d&chksm=bc0e41265c2f4fbdb1bf77c2187dee6705a7106487173278265c143013bb58ea1b9a2469ed07#rd. (Original source material in Mandarin Chinese).

62 “Getting Ahead of Digital Repression: Authoritarian Innovation and Democratic Response,” Stanford University, 12 September 2024, https://fsi.stanford.edu/publication/getting-ahead-digital-repression-authoritarian-innovation-and-democratic-response.

63 Wency Chen, “Chinese AI Apps Eye Overseas Markets for Growth amid Tough Competition, Regulation at Home,” *South China Morning Post*, 25 August 2024, www.scmp.com/tech/tech-trends/article/3275747/chinese-ai-apps-eye-overseas-markets-growth-amid-tough-competition-regulation-home.

64 Abbas Raza Ali et al., “A Large and Diverse Arabic Corpus for Language Modeling,” *Procedia Computer Science*, Volume 225 (8 December 2023): 12–21, https://doi.org/10.1016/j.procs.2023.09.086.

65 For more information, please see: “Abu Dhabi-Based Technology Innovation Institute Introduces Falcon LLM: Foundational Large Language Model (LLM) Outperforms GPT-3 with 40 Billion Parameters,” Technology Innovation Institute, 15 March 2023, www.tii.ae/news/abu-dhabi-based-technology-innovation-institute-introduces-falcon-llm-foundational-large; and Ali Dalloul, “Introducing JAIS: Arabic-Centric Large Language Model on Azure,” Microsoft Tech Community, 21 May 2024, https://techcommunity.microsoft.com/t5/ai-ai-platform-blog/introducing-jais-arabic-centric-large-language-model-on-azure/ba-p/4137329.

66 Aaron Raj, “Alibaba DAMO Academy Introduces SeaLLMs, Inclusive AI Language Models for SEA” Tech Wire Asia, 13 December 2023, https://techwireasia.com/2023/12/will-alibaba-damo-academy-seallms-inclusive-ai-language-models-work-for-sea/.

67 Ashley Belanger, “Meta Smart Glasses Can Be Used to Dox Anyone in Seconds, Study Finds,” Ars Technica, 2 October 2024, https://arstechnica.com/tech-policy/2024/10/harvard-students-make-auto-doxxing-smart-glasses-to-show-need-for-privacy-regs/.

68 Brittan Heller, “Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law,” *Vanderbilt Journal of Entertainment & Technology Law*, 23:1 (1 December 2020): 1, https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1/; and Daniel Berrick and Jameson Spivack, “Understanding Extended Reality Technology & Data Flows: Privacy and Data Protection Risks and Mitigation Strategies,” Future of Privacy Forum, 17 November 2022, https://fpf.org/blog/understanding-extended-reality-technology-data-flows-privacy-and-data-protection-risks-and-mitigation-strategies/.

69 Tate Ryan-Mosley, “AI Isn’t Great at Decoding Human Emotions. So Why Are Regulators Targeting the Tech?,” *MIT Technology Review*, 14 August 2023, www.technologyreview.com/2023/08/14/1077788/ai-decoding-human-emotions-target-for-regulators/.

70 Dilshani Kumarapeli, Sungchul Jung, and Robert W. Lindeman, “Privacy Threats of Behaviour Identity Detection in VR,” *Frontiers in Virtual Reality*, 5 (28 January 2024), https://doi.org/10.3389/frvir.2024.1197547.

71 “Protecting Cognition: Background Paper on Neurotechnology,” Australian Human Rights Commission, 12 March 2024, https://humanrights.gov.au/our-work/technology-and-human-rights/publications/protecting-cognition-background-paper.

72 Oliver Whang, “A.I. Is Getting Better at Mind-Reading,” *New York Times*, 1 May 2023, www.nytimes.com/2023/05/01/science/ai-speech-language.html.

73 Emily Mullin, “Neuralink Plans to Test Whether Its Brain Implant Can Control a Robotic Arm,” *WIRED*, 25 November 2024, www.wired.com/story/neuralink-robotic-arm-controlled-by-mind/.

74 Fernando M. C. V. Reis et al., “Control of Feeding by a Bottom-up Midbrain-Subthalamic Pathway,” *Nature Communications*, 15:1 (7 March 2024), https://doi.org/10.1038/s41467-024-46430-5.

75 Nita A. Farahany, “Neurotech at Work,” *Harvard Business Review*, March-April 2023, https://hbr.org/2023/03/neurotech-at-work.

76 Natasha Lomas, “What Is Wearable Neurotech and Why Might We Need It?,” TechCrunch, 12 October 2024, https://techcrunch.com/2024/10/12/what-is-wearable-neurotech-and-why-might-we-need-it/.

77 Michael Nolan, “This Gamer Turned EEG Tech Into a Game Controller: Questioning through *Elden Ring* on the Power of Thought Alone,” *IEEE Spectrum*, 24 May 2023, https://spectrum.ieee.org/elden-ring-hands-free-controller.

78 For more information, please see: “More Than 1 Million XR Headsets Shipped in China in 2022, Pico Number 1,” Counterpoint, 15 March 2023, www.counterpointresearch.com/insights/1-million-xr-headsets-shipped-china-2022-pico-number-1/.

79 Liao Shumin, “Head of Baidu’s Metaverse App Xirang Moves On as Focus Shifts to Chatbots,” Yicai Global, 19 May 2023, www.yicaiglobal.com/news/2023051920-head-of-baidus-metaverse-app-xirang-moves-on-as-focus-shifts-to-chatbots.

80 Eduardo Baptista, “A Metaverse with Chinese Characteristics Is a Clean and Compliant Metaverse,” Reuters, 25 January 2022, www.reuters.com/markets/funds/metaverse-with-chinese-characteristics-is-clean-compliant-metaverse-2022-01-25/.

81 For instance, please reference Baidu’s “VR Party Building” information webpage, accessible here: https://vr.baidu.com/solution/partybuildingeducation. Also, please see this resource for more information: Tom Wang, “Baidu Unveils China’s First Metaverse Platform ‘Xi Rang,’” *South China Morning Post*, 24 December 2021, www.scmp.com/video/technology/3160931/baidu-unveils-chinas-first-metaverse-platform-xi-rang.

82 Baraka Maiseli et al., “Brain–Computer Interface: Trend, Challenges, and Threats,” *Brain Informatics*, 10:1 (4 August 2023): 20, https://doi.org/10.1186/s40708-023-00199-3.

83 Minchang Yu et al., “EEG-Based Emotion Recognition in an Immersive Virtual Reality Environment: From Local Activity to Brain Network Features,” *Biomedical Signal Processing and Control*, 72, Part A (February 2022): https://doi.org/10.1016/j.bspc.2021.103349.

84 William Hannas et al., “Bibliometric Analysis of China’s Non-Therapeutic Brain-Computer Interface Research,” Center for Security and Emerging Technology (CSET), March 2024, https://cset.georgetown.edu/publication/bibliometric-analysis-of-chinas-non-therapeutic-brain-computer-interface-research/; and Emily Mullin, “China Has a Controversial Plan for Brain-Computer Interfaces.”

85 *Emotional Entanglement: China’s Emotion Recognition Market and Its Implications for Human Rights*; and Bruce E. Wexler, “Mind Control in China’s Classrooms,” YaleGlobal Online (Yale University), 3 December 2019, https://archive-yaleglobal.yale.edu/content/mind-control-chinas-classrooms.

86 Emily Mullin, “China Has a Controversial Plan for Brain-Computer Interfaces.”

87 Sjors Ligthart et al., “Minding Rights: Mapping Ethical and Legal Foundations of ‘Neurorights,’” *Cambridge Quarterly of Healthcare Ethics*, 32:4 (15 May 2023): 461–81, https://doi.org/10.1017/S0963180123000245.

88 For more information, please see: Xuebin Zhou, “Application Prospects and Challenges of Brain-Computer Interface Technology in the Field of Police Work,” Baidu, December 2023, https://wenku.baidu.com/view/645e36cfbb4ae45c3b3567ec102de2bd9605debb.html?wkts_=1719990490993&bdQuery=%22%E8%84%91%E6%9C%BA%E6%8E%A5%E5%8F%A3%22+%22%E8%AD%A6%E5%AF%9F%22&needWelcomeRecommand=1. (Original source material in Mandarin Chinese.)

89 Hannas et al., “Bibliometric Analysis of China’s Non-Therapeutic Brain-Computer Interface Research.”

90 Paul Mozur and Adam Satariano, “A.I., Brain Scans and Cameras: The Spread of Police Surveillance Tech,” *New York Times*, 30 March 2023, www.nytimes.com/2023/03/30/technology/police-surveillance-tech-dubai.html.

91 “‘Metaverse + Court Trial + Classroom Teaching’ Xiamen Siming Court Promotes Judicial Digitalization and Intelligence,” People’s Daily, 23 September 2022, http://fj.people.com.cn/n2/2022/0923/c181466-40137243.html. (Original source material in Mandarin Chinese.)

92 Marialejandra Portal, “Moving to the Metaverse: First Trial Held in the Metaverse,” Miami Law, *International and Comparative Law Review*, 32:1 (3 March 2023), https://international-and-comparative-law-review.law.miami.edu/moving-to-the-metaverse-first-trial-held-in-the-metaverse/.

93 Article 19, *Emotional Entanglement: China’s Emotion Recognition Market and Its Implications for Human Rights.*

94 Jonathan Pugh et al., “Brainjacking in Deep Brain Stimulation and Autonomy,” *Ethics and Information Technology*, 20 (30 July 2018): 219–232, https://doi.org/10.1007/s10676-018-9466-4.

95 Bojana Bellamy and Eduardo Bertoni, “Neurodata – the New Epicenter of Data Protection,” Tech Policy Press, 17 September 2024, https://techpolicy.press/neurodata-the-new-epicenter-of-data-protection.

96 “Global VR Market Slips 4% YoY in Q3 2024, AR Glasses Set to Grow in 2025,” Counterpoint, 27 December 2024, www.counterpointresearch.com/insight/post-insight-global-vr-market-slips-4-yoy-in-q3-2024-ar-glasses-set-to-grow-in-2025/. Moreover, Meta has partnered with Tencent to offer its products in the PRC as well. For more information, please see: “Meta Strikes Deal with Tencent to Sell VR Headset in China,” Reuters, 10 November 2023, www.reuters.com/technology/meta-strikes-deal-sell-vr-headset-china-wsj-2023-11-10/.

97 “SyncThink and Pico Extend Partnership,” Med-Tech Innovation News, 14 March 2022, www.med-technews.com/api/content/eb58e442-a3a8-11ec-bba9-12f1225286c6/. In addition, "SyncThink" is now known as "NeuroSync."

98 Sam Sprigg, “Wisear Partners with PICO to Bring Neural-Based Hands & Voice-Free Controls to VR,” Auganix, 30 May 2023, www.auganix.org/vr-news-wisear-partners-with-pico-to-bring-neural-based-voice-and-hands-free-controls-to-vr/.

99 “Augmented Reality And Virtual Reality Market Size — Global Industry, Share, Analysis, Trends and Forecast 2022-2030,” Acumen Research and Consulting, December 2022, www.acumenresearchandconsulting.com/augmented-reality-and-virtual-reality-market.

100 “Middle East And Africa Virtual Reality Market Size Analysis By 2031,” Data Bridge, April 2024, www.databridgemarketresearch.com/reports/middle-east-and-africa-virtual-reality-market; and Arushi Singh, “Gulf States Pioneer the Implementation of Metaverse Technology,” Fair Observer, 22 July 2023, www.fairobserver.com/world-news/gulf-states-pioneer-the-implementation-of-metaverse-technology/.

101 On deepening technical-scientific cooperation between China and the Gulf States, please see: Mohammed Al-Sudairi, Steven Jiawei Hai, and Kameal Alahmad, *How Saudi Arabia Bent China to Its Technoscientific Ambitions,* Carnegie Endowment for International Peace, 1 August 2023, https://carnegieendowment.org/research/2023/08/how-saudi-arabia-bent-china-to-its-technoscientific-ambitions?lang=en.

102 “Neurotechnology Market — Growth, Trends, and Forecasts (2025-2030),” Mordor Intelligence, 2024, www.mordorintelligence.com/industry-reports/neurotechnology-market.

103 Daniel Duke and Lorri Anne Meils, “Are We Ready for the Quantum Age? Preparing for the Risks of Quantum Technologies with Rights-Respecting Policy Frameworks,” Tech Policy Press, 5 March 2024, https://techpolicy.press/are-we-ready-for-the-quantum-age-preparing-for-the-risks-of-quantum-technologies-with-rightsrespecting-policy-frameworks.

104 “Quantum-Safe Cryptography – Fundamentals, Current Developments and Recommendations,” German Federal Office for Information Security, 18 May 2022, www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=132646.

105 Holly Chik, “Scientists Install Encryption to Protect Advanced Chinese Quantum Computer from Attack,” *South China Morning Post*, 12 April 2024, www.scmp.com/news/china/science/article/3258787/scientists-install-encryption-shield-protect-advanced-chinese-quantum-computer-attack; and Valentin Weber, “The New Quantum Technology Race,” *Internationale Politik Quarterly*, 22 March 2024, https://ip-quarterly.com/en/new-quantum-technology-race.

106 For more information, please see: Jakub Pii, “Chinese Quantum Companies and National Strategy 2023,” Quantum Insider, 13 April 2023, https://thequantuminsider.com/2023/04/13/chinese-quantum-companies-and-national-strategy-2023/.

107 For additional context, please consult ASPI’s “Quantum Computing” Techtracker, available here: https://techtracker.aspi.org.au/tech/quantum-computing/research-contribution/?c1=us&c2=cn.

108 Edward Parker, “The Chinese Industrial Base and Military Deployment of Quantum Technology,” (testimony before the U.S.-China Economic and Security Review Commission on 1 February 2024), RAND Corporation, 1 February 2024, www.rand.org/pubs/testimonies/CTA3189-1.html.

109 For more information, please consult: “QuantumCTek– Cases,” QuantumCTek, www.quantum-info.com/English/#cases; and “Origin Quantum - Crunchbase Company Profile & Funding,” Crunchbase, www.crunchbase.com/organization/origin-quantum.

110 Valentin Weber and Joss Wright, “(Quantum) Encryption: Europeans Need to Come Down in Favor,” German Council on Foreign Relations (DGAP), 20 June 2023, https://dgap.org/en/research/publications/quantum-encryption-europeans-need-come-down-favor.

111 For more information, please see: “Position Paper on Quantam Key Distribution,” German Federal Office for Information Security (BSI), www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4.

112 David Lague, “U.S. And China Race to Shield Secrets from Quantum Computers,” Reuters, 12 December 2024, www.reuters.com/investigates/special-report/us-china-tech-quantum/.

113 Information taken from National Endowment for Democracy Workshop in Palo Alto, April 2024.

114 For more information, please consult: “Artificial Intelligence Solution | OriginQ Cloud,” Origin Quantum, https://qcloud.originqc.com.cn/en/solution/ai.

115 Victoria Bela, “China and Russia Test ‘Hack-Proof’ Quantum Communication Link for BRICS Countries,” *South China Morning Post*, 30 December 2023, www.scmp.com/news/china/science/article/3246752/china-and-russia-test-hack-proof-quantum-communication-link-brics-countries.

116 For additional information, please see: “BRICS STI Framework Programme,” BRICS, 3 December 2019, http://brics-sti.org/?p=new/25; “Policy and R&D Trends of Quantum Technology in the Leading Countries of the Asia and Pacific Regions,” Japan Science and Technology Agency, March 2023, https://spap.jst.go.jp/investigation/downloads/2022_rr_01_en.pdf; and view Yaseera Ismail’s bio page online at the University of Kwazulu-Natal’s website, accessible here: https://wp-scp.ukzn.ac.za/yaseera-ismail/.

117 The project, led in the PRC by the University of Science and Technology of China, was initially planned to start in 2019-20 and take approximately three years; the last mention of it that can be identified dates to 2021. For this last reference, please see: "Quantum Satellite and Fibre Communication (QuSAF) - BRICS Workshop," BRICS, 25 January 2021, http://lsits.psuti.ru/arc/BRICS%20Workshop%202021.pdf. More recently, the researchers involved in the BRICS project have been collaborating on quantum papers. For instance, please see: Shweta Mittal et al., "Design and Performance Analysis of a Novel Hoop-Cut SPR-PCF Sensor for High Sensitivity and Broad Range Sensing Applications," *IEEE Sensors Journal*, 24:3 (February 2024): 2,697-2,704, https://ieeexplore.ieee.org/abstract/document/10355908/; and Akshat Agarwal et al., "A Six-Core Microstructured Fiber for Sensing Applications," in *Optica Imaging Congress 2024*, *Technical Digest Series*, Optica Publishing Group, 2024, https://opg.optica.org/abstract.cfm?uri=3D-2024-JD6A.1.

118 Mining new Bitcoin is believed to be a popular strategy in the Russian-occupied territories in Georgia, Ukraine, and Moldova. For more information, please see: Neil Barnett, *The Other Bitcoin Boom: Crypto Mining in Russia's Shadow Territories,* Royal United Services Institute, 12 December 2024, www.rusi.org/explore-our-research/publications/commentary/other-bitcoin-boom-crypto-mining-russias-shadow-territories.

119 Sandra Waliczek, "How Are CBDCs Different from Cryptocurrencies and Stablecoins?," World Economic Forum, 9 November 2023, www.weforum.org/agenda/2023/11/cbdcs-how-different-cryptocurrency-stablecoin/#:~:text=The%20main%20difference%20between%20a,White%20Paper%20Series%20points%20out.

120 Marco Quiroz-Rodriguez, "Crypto Is Fully Banned in China and 8 Other Countries," *Fortune*, 4 January 2022, https://fortune.com/2022/01/04/crypto-banned-china-other-countries/.

121 Zhiyuan Sun, "China Begins Next Phase of CBDC Testing with E-CNY Payment for Public Transport," Cointelegraph, 23 August 2022, https://cointelegraph.com/news/china-begins-next-phase-of-cbdc-testing-with-e-cny-payment-for-public-transport.

122 Pratham Rawat, "The Lackluster Past and Promising Future of China's Central Bank Digital Currency," Cornell University, 17 April 2024, https://business.cornell.edu/hub/2024/04/17/lackluster-past-promising-future-chinas-central-bank-digital-currency/.

123 For more information, please see the *Journal of Democracy's* webpage on bitcoin and its potential impact on democracy, accessible here: https://www.journalofdemocracy.org/news-and-updates/is-bitcoin-good-for-democracy/.

124 "Myanmar's Shadow Government Sets up Crypto Bank to Block Money Flow to Junta," Radio Free Asia, 21 July 2023, www.rfa.org/english/news/myanmar/crypto-bank-07212023164817.html.

125 For additional information, please consult the Human Rights Foundation's CBDC Tracker, accessible here: https://cbdctracker.hrf.org/cbdc-101.

126 Darrell Duffie and Elizabeth Economy (eds.), *Digital Currencies: The US, China, and the World at a Crossroads*, Hoover Institution, 2022, www.hoover.org/sites/default/files/research/docs/duffie-economy_digitalcurrencies_web_revised.pdf.

127 Mike Orcutt, "What's Next for China's Digital Currency?," *MIT Technology Review*, 3 August 2023, www.technologyreview.com/2023/08/03/1077181/whats-next-for-chinas-digital-currency/.

128 One can see the app developed by the People's Bank of China available for download on the "E-CNY - Apps on Google Play," webpage, available here: https://play.google.com/store/apps/details?id=cn.gov.pbc.dcep&hl=en.

129 "Will a Digital RMB Coin Coin Wallet Used by One Card Be the Future Trend?," Mpaypass, 27 July 2022, www.mpaypass.com.cn/news/202207/27101419.html. (Original source material in Mandarin Chinese.)

130 "China Central Bank Governor Says Digital Yuan Has 'Managed Anonymity,'" PYMNTS, 31 October 2022, www.pymnts.com/cryptocurrency/2022/china-central-bank-governor-digital-yuan-managed-anonymity/.

131 Information taken from National Endowment for Democracy Workshop in Palo Alto, April 2024.

132 Choe Sang-Hun and David Yaffe-Bellany, "How North Korea Used Crypto to Hack Its Way Through the Pandemic," *New York Times*, 30 June 2022, www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html.

133 Jonathan Movroydis, "What the Rise of China's Digital Currency Could Mean for the U.S.," Stanford University, 23 March 2022, www.gsb.stanford.edu/insights/what-rise-chinas-digital-currency-could-mean-us.

134 "Project mBridge Reaches Minimum Viable Product Stage," Bank for International Settlements, 11 November 2024, www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.

135 "BIS to Leave China-Backed Central Bank Digital Currency Project," Reuters, 31 October 2024, www.reuters.com/business/finance/bis-leave-cross-border-payments-platform-project-mbridge-2024-10-31/.

136 Ananya Kumar, "Practice Makes Perfect: What China Wants from Its Digital Currency in 2023," Atlantic Council, 24 April 2023, www.atlanticcouncil.org/blogs/econographics/practice-makes-perfect-what-china-wants-from-its-digital-currency-in-2023/.

137 For more information, please visit the Google Play webpage that lists the People's Bank of China's app on the "E-CNY - Apps on Google Play."

138 Stefan Ingves, "Going Cashless," IMF Finance & Development (F&D) Magazine, International Monetary Fund, June 2018, www.imf.org/en/Publications/fandd/issues/2018/06/central-banks-and-digital-currencies-point.

139 Tom Keatinge and Joshua Tjeransen, *Central Bank Digital Currencies and National Security: Policy Considerations*, Royal United Services Institute, 18 December 2023, www.rusi.org/explore-our-research/publications/emerging-insights/central-bank-digital-currencies-and-national-security-policy-considerations.

140 For more information, please consult: Emma Woollacott, "U.K. Government May Still Use Chinese Surveillance Kit Well Into Next Year," *Forbes*, 30 April 2024, www.forbes.com/sites/emmawoollacott/2024/04/30/uk-govt-may-still-use-chinese-surveillance-kit-well-into-next-year/; and "Britain to Remove Chinese Surveillance Gear from Government Sites," *Guardian*, 7 June 2023, www.theguardian.com/world/2023/jun/08/britain-to-remove-chinese-surveillance-gear-from-government-sites.

141 For additional context, please see: 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; Steven Feldstein, *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, 17 September 2019, https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en; Valentin Weber, "The Worldwide Web of Chinese and Russian Information Controls," Open Technology Fund, September 2019, https://public.opentech.fund/documents/English_Weber_WWW_of_Information_Controls_Final.pdf; and Sheena Chestnut Greitens, "Dealing With Demand for China's Global Surveillance Exports."

142 Maarten G. A. Daman, "Making the Digital Euro Truly Private," The European Central Bank (ECB), The ECB Blog, 13 June 2024, www.ecb.europa.eu/press/blog/date/2024/html/ecb.blog240613~47c255bdd4.en.html.

143 Du Chuan, "E-Yuan App Adds Payment Function for When Mobiles Are Offline, Out of Power," Yicai Global, 11 January 2023, www.yicaiglobal.com/news/e-yuan-app-adds-payment-function-for-when-mobiles-are-offline-out-of-power.

144 For more information, please visit the Privacy-Enhancing Technologies Prize Challenges "U.K.-U.S. Prize Challenges" webpage, accessible here: https://petsprizechallenges.com/.

145 Matthew Sparkes, "Multiple Nations Enact Mysterious Export Controls on Quantum Computers," *New Scientist*, 3 July 2024, www.newscientist.com/article/2436023-multiple-nations-enact-mysterious-export-controls-on-quantum-computers/.

146 Ehren Kret, "Quantum Resistance and the Signal Protocol," Signal Messenger, 19 September 2023, https://signal.org/blog/pqxdh/.

147 Valentin Weber and Maria Pericàs Riera, "How Germany Can Improve Its Standing in Post-Quantum Cryptography," German Council on Foreign Relations (DGAP), 26 November 2024, https://dgap.org/en/research/publications/how-germany-can-improve-its-standing-post-quantum-cryptography.

148 For more information, please see: "Will China Set Global Tech Standards?," ChinaFile, 22 March 2022, www.chinafile.com/conversation/will-china-set-global-tech-standards; and Samantha Hoffman, *Double-Edged Sword: China's Sharp Power Exploitation of Emerging Technologies.*

149 Gian Volpicelli, "Beijing Is Coming for the Metaverse," *Politico*, 20 August 2023, www.politico.eu/article/china-beijing-designing-metaverse-proposal-social-credit-system-un-itu/.

150 "Patenting Uyghur Tracking - Huawei, Megvii, More," IPVM, 12 January 2021, https://ipvm.com/reports/patents-uyghur.

ABOUT THE AUTHOR

Valentin Weber is a senior research fellow at the German Council on Foreign Relations (DGAP). His research covers the geopolitics of cyberspace, as well as surveillance and emerging technologies. In 2019, he analyzed Chinese and Russian information controls as an Open Technology Fund Senior Fellow with the Berkman Klein Center for Internet & Society at Harvard University. Weber has contributed to major news outlets including *Die Zeit*, Deutsche Welle, *the Globe and Mail*, *South China Morning Post*, and the Associated Press. He holds a PhD in cybersecurity from the University of Oxford. Follow him on X @weberv_.

ACKNOWLEDGMENTS

The author appreciates the contributions of the International Forum's staff and leadership, including Christopher Walker, John K. Glenn, Kevin Sheives, John Engelken, and Maya Recanati, all of whom played important roles in the editing and publication of this report. The author also wishes to thank this report's peer reviewers for lending their expertise and knowledge to further sharpen and refine the analysis. Particular acknowledgment goes to Beth Kerley whose support and vision for this project were vital to its completion. Finally, the Forum wishes to acknowledge Factor3 Digital for their efforts and invaluable support in designing this report for publication.

PHOTO CREDITS

Cover image: Photo by janiecbros/iStock (by Getty Images)

Page 8: Photo by Getty Images for Unsplash

Page 23: Photo by Jason marz/Getty Images

Page 27: Photo by Getty Images for Unsplash

FORUM

INTERNATIONAL
FORUM FOR
DEMOCRATIC
STUDIES

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.

NED

NATIONAL
ENDOWMENT
FOR
DEMOCRACY

SUPPORTING FREEDOM AROUND THE WORLD

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.

1201 Pennsylvania Avenue, NW
Suite 1100
Washington, DC 20004
(202) 378-9700
ned.org

@thinkdemocracy

ThinkDemocracy

International Forum for Democratic Studies