China's Tech-Enhanced Authoritarianism

Testimony before the Congressional Executive Commission on China
Hearing on "Techno-Authoritarianism: Platform for Repression in China and Abroad"

Written Testimony of Dr. Samantha Hoffman
Senior Analyst at The Australian Strategic Policy Institute
Independent Consultant

November 17, 2021

***

Chairman Merkley, Co-Chair McGovern, and members of the Commission, thank you for the opportunity to testify today on the topic of China's tech-enhanced authoritarianism.

Core Assessments

[1] **Assumptions that liberal democracy would automatically be strengthened and authoritarians weakened as the world became increasingly digitally interconnected have been proven false. Democracies are not going to self-correct in response to the problems created by authoritarian applications of technology.** Competing with China in this space is not about "winning" or "losing" a race in terms of R&D of emerging and critical technologies, such as AI or data science and storage technologies. Leadership in these R&D areas is essential, not least to guarantee supply chain resilience, but just as consequential is the competition taking place in the conceptual space. To stay ahead, the United States and like-minded countries must innovate thinking about use-cases, and set boundaries, so that these technologies positively affect society without liberal democratic values being undermined.

[2] **The ability to identify and protect strategic data will become an increasingly complex and vital national security task, especially under the conditions of China's military-civil fusion strategy.** Knowing how particular datasets are collected and used by foreign adversaries, and imagining potential use cases, will be an essential part of ranking what data sets should be prioritized for protection. Developing effective countermeasures requires understanding the implications of the fact that the Chinese party-state conceives of the usefulness of data in a strategic competition in ways that go beyond traditional intelligence collection.

[3] We cannot measure risk based on today's capabilities alone. Technology evolves on a trajectory, and to develop effective policy responses requires assuming that the challenges China faces today in realizing its optimal outcomes may not be significant in the future as concepts increasingly become capabilities.

What is Tech-Enhanced Authoritarianism?

When we talk about 'authoritarian technology", this should be defined as the uses of technology that enhance authoritarian power. The phrase "tech-enhanced authoritarianism" is a way of thinking about this concept that demystifies the phrase "techno-authoritarianism". Techno-authoritarianism connotes a vision of the future that, for most passive observers, is either like Huxley's *Brave New World* or Orwell's *1984*. The reality though is not like science fiction.

On one hand, we see the Chinese party-state deploying extremely coercive applications of technology, most notably in places like Xinjiang and Tibet and with public security surveillance projects like the "Sharp Eyes" or "Skynet".[1] But, elsewhere, it is technologies that provide services or enhance convenience and problem solving that allow the party-state to expand and reinforce its power. For example, data from IoT sensors can improve logistics and predictive analytics that increase supply chain visibility and efficiency in normal times, but in crisis those same technologies could facilitate defense mobilization capacity.

China's tech-enhanced authoritarianism is unique in a national context. When these technologies are exported globally, it is not necessarily the intent of an end user to use them in ways that enhance authoritarian power. Some fragile democracies or illiberal regimes import the technologies for coercive purposes, but others are genuinely seeking the best and most affordable technologies for problem-solving. With many technologies associated with tech authoritarianism appearing benign in their everyday end-use, problematic assumptions are made that undermine the risks they embed. For instance, one problematic claim that is made goes as follows: "[x] technology or [y] system is not inherently problematic, it is applied in ways that solve ordinary governance problems, but there is a potential that in the wrong hands that it will be misused." Following the same problematic logic, some claim that if that technology is exported, "we can control the problem because we control its end-use". The problem is analysts describing "misuse" are thinking subjectively.

For the Party-state, problem-solving technologies can also enhance authoritarian control, the two are not mutually exclusive. The tendency to compartmentalise "good" and "bad" use points to a failure to conceptualise the strategic potential value of the technologies. The Chinese Party-state sets itself apart because it is setting itself up to be able to exploit that inherent dual-use at all times. This is notable in terms of how it applies PRC law to Chinese companies and in terms of how it seeks to seize advantages in the development of technical standards.

[1] Skynet Project (天网工程) refers to video monitoring equipment, mostly at major intersections, law and order checkpoints, and other public assembly locations. It uses GIS mapping, image gathering, transmission and other technology to improve real-time monitoring and information recording. Sharp Eyes Project (雪亮工程) is an extension of the Skynet project. In addition to surveillance cameras, Sharp Eyes is focused on building video image information exchange and sharing platforms and county–village–township comprehensive management centers. It is applied to efforts including state security, anti-terrorism, enhanced logistics, security supervision, and the prevention and control of criminal activity.

Data Security and Digital Supply Chain Security

Technologies that collect, store and transfer data facilitate the delivery of wide range of services on which society is becoming increasingly dependent. In a June 2021 report, "Mapping China's Technology Giants: Supply chains and the global data collection ecosystem"[2], we found that existing global policy debates and subsequent policy responses concerning security in the digital supply chain miss the bigger picture because they typically prioritize the potential for disruption or malicious alterations of the supply chain. Yet, digital supply-chain risk starts at the design level. Not all methods used to acquire data need to be intrusive, subversive, covert or even illegal—they can be part of normal business data exchanges. Figure 1 illustrates how a digital supply chain can be compromised without a malicious intrusion or alteration. The data-sharing relationships that bring commercial advantages are also the same ones that could compromise an organization.

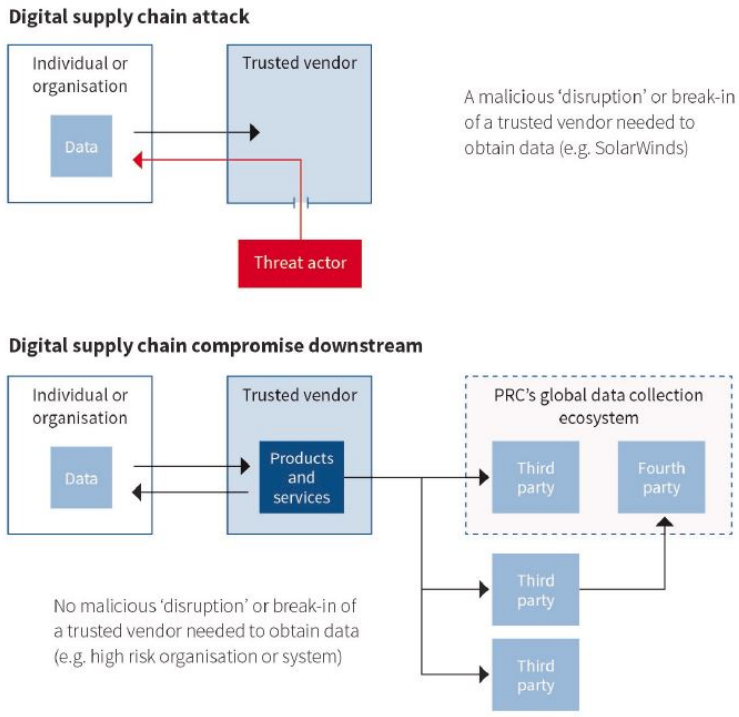

Figure 1: Dr Samantha Hoffman and Dr Nathan Attrill, "Mapping China's Tech Giants: Supply chains & the global data collection ecosystem," Australian Strategic Policy Institute, 8 June 2021: https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem

My October 2019 ASPI report, *Engineering Global Consent*, provided a case study describing what this problem can look like in reality. The report identified and described a machine-

[2] Samantha Hoffman and Nathan Attrill, *Mapping China's Technology Giants: Supply chains and the global data collection ecosystem*, Australian Strategic Policy Institute (8 June 2021), https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem.

translation company controlled by the Central Propaganda Department, Global Tone Communications Technology (GTCOM), which engages in global bulk data collection.[3]

GTCOM claims that one of its many platforms, *InsiderSoft*, accumulates about 2–3 petabytes of data per year, including from Twitter and Facebook.[4] The company feeds the data it aggregates into various tools, some linked to state security. For instance, in 2017, GTCOM's Big Data Director, Liang Haoyu said: Through the real-time listening and interpretation of cross-language data, the company has established information security systems for countries and regions, and ultimately finds relevant security risks in targeted areas through open channels … [Only with] image recognition on top of text and voices, can [we] better prevent security risks.[5]

There are strong indications that GTCOM generates military and other state security intelligence out of the data it collects (and not only because an image from GTCOM Big Data Director Liang Haoyu's aforementioned speech shows a screen claiming '90% of military-grade intelligence data can be obtained from open data analysis'). GTCOM runs the 2020 Cognitive Research Institute (the 2020 Institute), which is a mechanism through which the company does R&D to enhance 'machine learning, deep neural networks, natural language processing, speech recognition, AI chips, data mining, distributed computing'. The 2020 Institute has numerous NLP (natural language processing) algorithms, including for automatic text identification, sentiment analysis, event element extraction, sensitivity determination (whether text contains 'violent, reactionary, pornographic or other sensitive information'), relation extraction, and 'military text classification'. The 'military text classification' algorithm classifies text according to subfields such as nuclear, shipping, aviation, electronic and space.

Data and the information it helps generate can also support the party-state's development of tools for shaping public discourse. Separately from GTCOM, research funded by the National Natural Science Foundation of China, the National Key R&D Program of China and a key project of the 'National Society Science Foundation of China' has worked specifically on automatic news comment generation; that is, synthetic comments on news articles. The methodology is based on NLP and large-scale datasets of real comments in Chinese and English. Given GTCOM's Propaganda Department ownership, its state security role and the fact that it collects bulk data in 65 languages, the research indicates a potential tool that a state-controlled company such as GTCOM could use, especially given that the research was funded with national-level grants. It's also simply indicative of how GTCOM's bulk data may be used

[3] Samantha Hoffman, *Engineering global consent: The Chinese Communist Party's data-driven power expansion*, Australian Strategic Policy Institute (2019), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-10/Engineering%20global%20consent%20V2.pdf?VersionId=eIvKpmwu2iVwZx4o1n8B5MAnncB75qbT.

[4] "7*24 小时实时监测," InsiderSoft, https://archive.vn/jJeJ0.

[5] ""梁浩宇：中译语通"全球公开大数据"助防安全风险" ", GTCOM, 2017, http://archive.is/FVJHM.

by others who have access to it, such as researchers working in cooperation with GTCOM's 2020 Institute. Other R&D associated with GTCOM may also have security implications, even if it's not immediately obvious. For instance, among GTCOM's patent applications is a machine translation method based on generative adversarial networks (GANs). GAN can be used to synthesise images based on AI or use visual speech recognition to perform lip-reading and speech output (it's the same type of technology commonly associated with synthetic media, meaning 'fake news' and 'deep fakes'). It's an intriguing patent not because of the technology itself, but because GTCOM is controlled by the Propaganda Department. The department's intent isn't simply to use GTCOM to provide language services, but to shape global public discourse.

Future Trajectory

Sometimes that control might just be about improved information integration and sharing. Integrated Joint Operations Platform, which is designed to help with the integration and sharing of data on citizens across multiple government agencies.[6] One metric used to identify threats is energy usage from smart electricity meters: abnormally high energy use could indicate 'illegal' activity, but such meters in their normal use would also improve the accuracy of meter readings.[19] Another example is building datasets for use in the PRC's 'national defence mobilisation system' (a crisis response platform) using data sourced from a variety of government cloud networks, from smart cities to tourism-related cloud networks (Figure 2).[20]

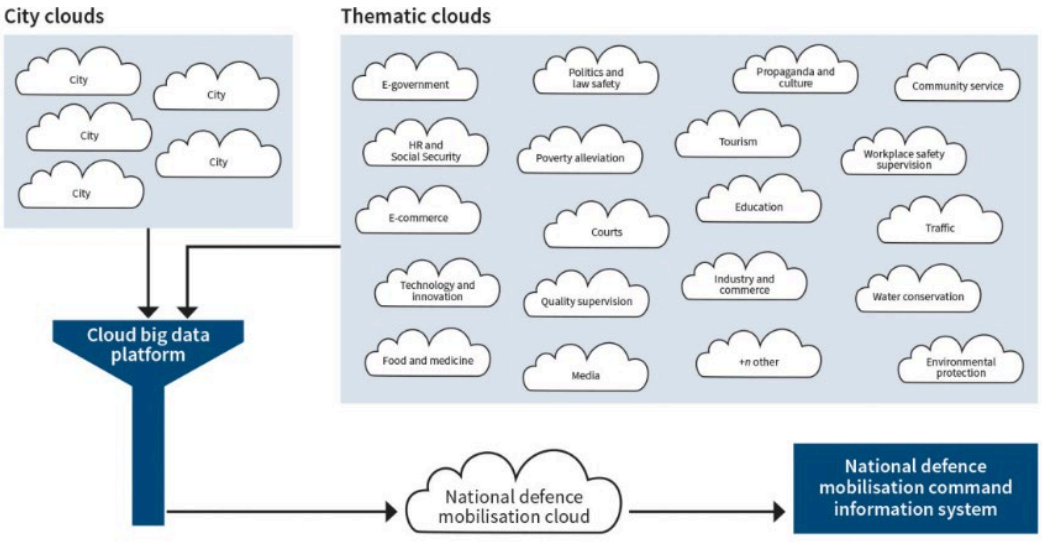

Figure 2 The concept of defence mobilisation and smart cities data integration and processing from Mapping China's Technology Giants: Supply chains and the global data collection ecosystem.

[6] Maya Wang, "China: Big Data Fuels Crackdown in Minority Region," (2018). https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region.

This is partly tied to administrative efficiency objectives set over two decades ago, before current technical capabilities existed. I noted in a 2018 article for *China Brief*[7] that in his report to the 15th Party Congress in 1997, then-CCP General Secretary Jiang Zemin noted that a bloated, inefficient bureaucracy hampers economic development, and the Party's ability to manage both itself and its relationship with society. His prescription was the establishment of a "highly efficient, well-coordinated and standardized administrative system".[8] Streamlining administration does more than improve the government's capacity to provide advertised administrative services, it improves the Party-state's overall visibility and, if effective, ability to predict and respond to problems (both "normal" governance problems and authoritarian control).

Current public conversation on China's capabilities among China analysts can often, misleadingly, focus on PRC discussion on its challenges with the integration and processing of data. Hundreds of companies' products are involved in smart cities projects across the PRC, making the implementation appear chaotic and uneven. Standardization is taking place at the design level, however, which indicates that seamless interoperability between smart cities systems is possible to achieve. While these capabilities are not currently at an optimal state, the trajectory appears to be in the Party-state's favor and levels of standardization across database schema for tools like Facial Recognition Systems improve. There is a constant evolution with digital technology. We must imagine technology's trajectory and future use cases to adequately develop policies governing their use. For now, the critical domains of influence are in possessing infrastructure, the storage, processing capacity and the data contained within it. If they invest the time and cost into doing so, the actor that controls those means can later control much more in terms of how technologies or the data derived from and passing through them are used.

In a report earlier this year for the National Endowment for Democracy, I highlighted how domestically, technologies are being researched and developed to meet the needs of the CCP, which are typically set out in government standards documents.[9] Government and research institutes collaborate with companies on national standards technical committees to standardize equipment development and the requirements that companies must meet to successfully bid for a project. For instance, a 2015 document GA/T1334 on the technical requirements for facial recognition in security systems was drafted through the cooperation of over a dozen bodies, including research institutes, such as the Chinese Academy of Sciences, the National University of Defense Technology, and the First Research Institute of the Ministry of Public Security; technology companies, such as Hikvision and Dahua; and public security bureaus, such as the Shanxi Provincial Public Security Department and the Wuhan Public Security Bureau. Documents like these are used as a basis for technical requirements in government procurement contracts.

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

[8] Jiang Zemin, Hold High the Great Banner of Deng Xiaoping Theory for an All-round Advancement of the Cause of Building Socialism With Chinese Characteristics' Into the 21st Century: Report Delivered at the 15th National Congress of the Communist Party of China on September 12, 1997, (Beijing Review, 1997).

[9] Hoffman, *Double-Edged Sword: China's Sharp Power Exploitation of Emerging Technologies*.

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

Recommendations for U.S. Policy

Recalibrate data security policy and privacy frameworks to account for the Chinese state's use of data to reinforce its political monopoly. Companies and governments too often assume that other governments' data and privacy regulations share the same goals as their own. That isn't true when it comes to the Chinese party-state and PRC-based companies, even if common vocabularies are used or if some policy drivers are similar. In the PRC, unlike in liberal democracies, data security and privacy concepts (including draft legislation) reinforce the party-state's monopoly power. Companies and governments need to recognize this risk and calibrate their policies to account for it.

Collaborate with like-minded countries to develop systems for improving risk-based approaches to improving the regulation of data transfers. Organizations must assess the value of their data, as well as the value of that data to any potential party in their supply chain that may have access to it or that might be granted access. In an age in which information warfare and disinformation campaigns occur across social media platforms and are among the greatest threats to social cohesion, data that's about public sentiment is as strategically valuable as data about more traditional military targets. Risk needs to be understood in a way that keeps up with the current threat landscape, in which otherwise innocuous data can be aggregated to carry meaning that can undermine a society or individuals.

Take a multidisciplinary approach to due diligence. Governments, businesses and other organizations need to develop frameworks for conducting supply-chain reviews that take into account country-specific policy drivers. Developing such a framework shouldn't be limited to just assessing a vendor's risk of exposure to political risk. It should also include detailed analysis of the downstream actors who have access to the vendor's data (and must include analysis of things such as the broader data ecosystem they're a part of and the obligations those vendors have to their own governments). Taking this more holistic approach to due diligence will better ensure that data can be protected in an effective way.