Testimony before the U.S.-China Economic and Security Review Commission

Hearing on "An Assessment of the CCP's Economic Ambitions, Plans, and Metrics of Success," Panel Four on "China's Pursuit for Leadership in Digital Currency"

15 April 2021

China's Digital Currency Electronic Payment and Surveillance[1]

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

Core Assessments

Vice-Chairman Cleveland, Commissioner Wessel, and Honourable Commissioners thank you for the opportunity to testify on this subject of emerging significance in the relationship between the United States and the People's Republic of China. I will begin with a few key points:

[1] In the Chinese party-state, everything is political, and this is exceptionally clear under Xi Jinping. DCEP will contribute to macroeconomic problem solving, but politics are also clearly embedded in DCEP's design and this political context will be a feature of DCEP's future use. These features cannot be simply removed if and when the technology is exported. Governments must be prepared to mitigate the political risks by investing in research into and the development of credible alternatives to DCEP for all key highly traded currencies.

[2] DCEP will offer no true anonymity, as the PBoC will have both complete visibility over the currency's use and the ability to confirm or deny any transaction. Even though the implications are mostly domestic for now, it's essential to act in anticipation of key shifts in global financial regulation and advances in financial technology. Policy responses cannot continue to be ad hoc and reactive as they have been in the cases of companies like Huawei. By acting now to build a baseline analysis of the DCEP project, decision-makers have an opportunity to anticipate challenges and build a consistent and coherent policy framework for managing them.

[3] The PBoC is linked to both the development of DCEP and the development of the social credit system, but a link between the two is not yet clear. The financial

[1] In addition to new material, this testimony draws heavily on the Australian Strategic Policy Institute's October 2020 publication, "The flipside of China's central bank digital currency" https://www.aspi.org.au/report/flipside-chinas-central-bank-digital-currency, edited by Dr Samantha Hoffman, and co-authored by Dr Samantha Hoffman, John Garnaut, Kayla Izenman, Dr Matthew Johnson, Alexandra Pascoe, Fergus Ryan and Elise Thomas.

transactions data DCEP generates could, in future, be ingested into big data analysis platforms associated with the social credit system. More broadly, technical assessments of risks associated with technologies like DCEP tend to be framed in ways that do not get to the core risks of how the data it generates might support other Party-state objectives or tools. To appropriately deal with these kinds of risks, the United States and others need to apply a new framework for evaluating such technologies.

Evaluating DCEP

There is increasing interest in the development of central bank digital currencies across the globe. Interest in this emerging technology is driven by a wide range of policy motivations, and the People's Republic of China (PRC) is not the only state seeking to develop a central bank digital currency. That being said, the PRC is one of the most significant actors in this space because the People's Bank of China (PBoC) is likely years ahead of other central banks in its research and development into its 'Digital Currency / Electronic Payment' project known simply as DCEP.

There are always two sides to a coin: central bank digital currencies simultaneously offer opportunities and create a threat depending on the intent of any actor who has access to the bulk data they generate. The degree of potential benefit and threat largely depends on the intent of the actor responsible for designing and deploying the technology. On the positive side, a CBDC can increase authorities' ability to understand how the economy operates and respond to problems in ways that could be beneficial to all. On the negative side, in the hands of authoritarians, the data collected can augment capabilities to surveil society and their ability to wield political power, potentially even outside their own geographic borders. With technology like DCEP, normal design features like anti-money laundering or anti-terrorism financing are politicised by default of the PRC's political system, and where those very concepts are politicised.

This testimony draws heavily on an October 2020 report I co-authored and edited for ASPI's International Cyber Policy Centre, titled "The Flipside of China's Central Bank Digital Currency". The report involved several different authors who contributed chapters. Our intention at ASPI was to improve the baseline understanding of DCEP's mechanics and place the project in its political and bureaucratic context. As a starting point, we found that existing research on DCEP did not holistically weave together the three broad categories of analysis relevant to the technology's development: finance and economics, financial technology, and Chinese politics. And in fact, politics - arguably the most important element - was the largely ignored dimension of existing DCEP analysis even though Party-state security organs, namely the Central Commission for Discipline Inspection, will be major beneficiaries of the project. The analytical framework in which we should place any technological development in the PRC, ranging from DCEP to implementing more overtly coercive surveillance tools like facial

recognition systems, should always be holistic. The nature of the Chinese Communist Party-led political system of the PRC necessitates that politics be a core feature of such analysis.

When attempting to understand the application of an emerging technology in the PRC, it is important to bear in mind that it likely will serve dual intents that at times seem contradictory. Frequently these technologies are described in a categorical, black-and-white fashion: either they are coercive, or they are problem-solving. They are described as being Orwellian if one's focus is on the coercive functions, but this often fails to take into account the technology's everyday problem-solving functions. Others might focus on the problem-solving sides of a particular technology and claim that the coercive applications of that technology are exaggerated in public discourse. Both views are misleading because the technologies in question are essentially always in a sense "dual-use".

The exact same data derived from a particular technology system can be processed to support both everyday problem-solving tools and coercive tools simultaneously. In fact, most emerging technologies deployed to support governance in PRC, such as smart cities technologies, have this dual application. Bear in mind that just because the PRC uses technology to support its everyday problem-solving does not mean that such problem solving is not also inclusive of enhancing the Party's control, like any other government authoritarian regimes rely on delivering something – or the myth that they do like Mussolini and his trains – in order to gain and maintain, or just create, the illusion of popular support.[2]

Policy Objectives

DCEP is being built to meet the party-state's specific needs. These needs are strongly linked to universal economic development and financial risk management objectives, but they also bake in the political requirements of the Party-state leadership.

As background, DCEP is a central bank digital currency. It is not a private digital token; it is a fiat currency. DCEP is a general-purpose central bank digital currency for use by both the PBoC (the central bank) and the general public. DCEP is planned to replace M0 (cash in circulation) only. DCEP will have a two-tier operational design. The first tier is the PBoC, which will handle issuance. The second tier is inclusive of commercial banks and the likes of Alipay, which will handle distribution. Finally, and most important in the context of this testimony, although DCEP is being built with a characteristic of "controlled anonymity", it does not provide true anonymity because the PBoC will have oversight into end-to-end transaction flows, as well as a register of users and institutions.

[2] Brian Cathcart. "Rear Window: Making Italy work: Did Mussolini really get the trains running on time?" The Independent, 1994. https://www.independent.co.uk/voices/rear-window-making-italy-work-did-mussolini-really-get-the-trains-running-on-time-1367688.html.

In our ASPI report, "The Flipside of China's Central Bank Digital Currency", co-authors Matthew Johnson and John Garnaut assessed the multilayered policy objectives behind DCEP.[3] They argued that at the leadership level, DCEP is being driven by the financial 'risk management and 'supervision' imperatives of Chinese Communist Party (CCP) General Secretary Xi Jinping. They described how DCEP fits within a vision of 'economic work' that Xi Jinping has developed over the past five years, noting that it puts surveillance and supervision at the core.[4] Johnson and Garnaut elaborated that as well as improving the scrutiny, and visibility, of international capital flows, and reducing the costs of printing and maintaining the circulation of cash, PBoC officials say that the data collected through DCEP will be used to improve macroeconomic policymaking.[5] And, for this purpose, the data used would be anonymised. However, Johnson and Garnaut noted, Yao said the same data would also be used for law enforcement.[6] Johnson and Garnaut importantly highlighted the increasingly prominent involvement of the CCP's top political organ for imposing political discipline internally in both promotion and policy direction of DCEP. They noted that the CCDI has promoted DCEP's potential to 'solve' the problem of terrorist financing and combat financial crimes such as bribery and embezzlement.[7] The CCDI imposes party discipline through channels that exist above and outside the formal legal apparatus, and it has served as Xi's primary organisational weapon in his ongoing campaign to combat corruption, enforce ideological unity and purge the Party of potential rivals.[8]

In "The Flipside of China's Central Bank Digital Currency", I described how the PBoC's creation of a massive repository of financial transaction data could improve both the efficiency and visibility required for the PBoC and CCDI to effectively supervise and police financial transactions. DC/EP's political-discipline-linked policy drivers—anti-money-laundering, anti-terrorist financing and anti-tax evasion—are linked to the party-state's 'social governance' process (also called 'social management). Social governance describes how the CCP leadership attempts to shape, manage and control all of society, including the Party's own members,

[3] See Dr. Matthew Johnson and John Garnaut's Chapter "Drivers of the PRC's digital currency project" in "The flipside of China's central bank digital currency" https://www.aspi.org.au/report/flipside-chinas-central-bank-digital-currency,

[4] '中央经济工作会议在北京举' [The Central Economic Work Conference is held in Beijing], *Xinhua*, 21 December 2015, online.

[5] Wolfie Zhao, 'PBoC's digital currency chief departs to lead securities clearing house', *Coindesk*, 15 October 2018, online.

[6] '姚前: 中国法定数字货币原型构想' [Yao Qian: Prototype conception of China's legal digital currency], *China Finance*, issue 17, 2016, online. On the use of DC/EP in conjunction with big data and AI for prevention and targeting of illegal behaviour, including money laundering, terrorist financing, and tax evasion see also '范一飞：关于数字人民币M0定位的政策含义分析' [Fan Yifei: analysis on the policy implications of digital RMB position as M0], China Financial News Net/Financial Times via Yicai, 14 September 2020, online.

[7] '观察丨央行数字货币如何影响你我' [Observer: How does central bank digital currency affect you and me?], Central Commission for Discipline Inspection (CCDI) website, 7 June 2020, online. The article quoted the PBoC Digital Currency Research Institute head, Mu Changchun, to make the following points: DC/EP is a response to the impact of bitcoin and crypto-assets on China's currency and monetary sovereignty; anonymity would be provided for 'reasonable and legal' micropayments; DC/EP would be a tool to prevent asset loss and embezzlement; a real-name wallet would be required for any large transaction, and the PBoC's goal was to strike a balance between protecting personal privacy and preventing crime.

[8] In 2018, CCDI secretary Zhao Leji signalled his intentions to move into the financial system by dispatching permanent anti-corruption teams to banks, insurers and other state-owned financial conglomerates, likening the new policy to 'installing surveillance cameras' aimed at top institutional leadership. 'Anti-corruption teams to be installed at China's state banks and insurance companies, acting like "human surveillance cameras"', *South China Morning Post*, 6 November 2018, online.

through a process of co-option and coercion.[9] DCEP helps solve legitimate problems, but that problem solving also acts as a tool for enhancing control. For instance, a local PBoC official described 'anti-money laundering' as an 'important means to prevent and defuse financial risks and consolidate social governance.'[10] Similarly, an article by Deputy Governor of the PBoC Liu Guoqiang published in the *People's Daily* said:

> In recent years, the scope of anti-money laundering work has become increasingly diverse and has expanded to many areas such as anti-terrorist financing, anti-tax evasion and anti-corruption. Anti-money-laundering work has strengthening modern social governance as its goal through guiding and requiring anti-money-laundering agencies to effectively carry out customer identification, discovering and monitoring large-value transactions and suspicious transactions, timely capturing abnormal capital flows, and enhancing the standardisation and transparency of economic and financial transactions to weave a 'security net' for the whole society to protect normal economic and financial activities from infringement …[11]

More specifically, the connection of DCEP's policy drivers to social management is indicative of how DCEP would ultimately serve the Party's needs in practice. Through the PRC's global Operation Skynet, which seeks to 'track down fugitives suspected of economic crimes and confiscate their ill-gotten assets', the PBoC cooperates directly with the Ministry of Public Security because of the role of the PBoC as an anti-money-laundering authority.[12] Genuinely corrupt officials are certainly caught up in the campaign, but who gets accused of corruption is the result of a political decision linked to power politics. Likewise, the crime of 'terrorist financing' is defined by the Chinese party-state's version of 'terrorism', and it's been directly linked to the PRC's campaign against the Uyghurs in Xinjiang. For instance, in July 2020, Australian media reported on an Uyghur woman who has been arrested on charges of financing terrorism for sending money to her parents in Australia, who used it to purchase a house.[13]

These drivers can also be seen in conjunction with two others that Johnson and Garnaut highlighted in their chapter: competing with the US financial-led global financial system (and in particular combatting Libra) and competing globally. They described China's finance and banking officials have repeatedly expressed concern at the prospect of a supranational stablecoin, namely Facebook's Libra, which Chinese authorities perceive as being tied to the

---

[9] Samantha Hoffman, 'Programming China: the Communist Party's autonomic approach to managing state security', PhD thesis, University of Nottingham, 29 September 2017.

[10] '关于反洗钱工作 中国人民银行长春中心支行组织召开了这个会……' [Regarding anti-money-laundering work, the People's Bank of China Changchun Branch organised this meeting …], Jinlin Province Financial Supervision Administration, 29 April 2019, online.

[11] Liu Guoqiang, '人民日报：维护国家金融安全 全面推进反洗钱事业' [*People's Daily*: Maintain national financial security and comprehensively promote anti-money-laundering], *People's Daily*, 15 July 2019, online.

[12] Zhang Yan, 'Skynet launches new fugitive hunt', *China Daily*, 29 January 2019, online; '央行"天网行动"挖出洗钱四大秘密通道' [Central Bank 'Skynet Operation' found four secret channels for money laundering], *jrj.com.cn*, 8 November 2008, online.

[13] Lin Evlin, 'This Uighur woman sent money to her parents in Australia. China accuses her of financing terrorism', *SBS News*, 18 July 2020, online.

US dollar. They equate US digital currencies with US dollar hegemony and say that it reinforces the need to decouple the renminbi from the US-dollar-led global financial system.[14] In my research, I've noted how more broadly, the Party-state has described the concept of credit as being one politicised by powerful competitors, namely the US, as a potential threat.[15] For instance, leading international credit agencies—Moody's Investors Service, Standard & Poor's and Fitch have been described as having the capacity to "destroy a nation by downgrading their credit score, utilising the shock power of 'economic nukes'".[16] The problem has also been tied to the Belt and Road Initiative because participant countries accept the current international rating system, and a solution would be to increase the 'discourse power [that China's] credit agencies possess on the international credit evaluation stage'.[17]

Surveillance Features[18]

DC/EP does not create surveillance practices that didn't already exist. Rather, its digital nature and centralised supervision facilitate the aggregation and bulk analysis of user and financial data to more easily meet those objectives.

The PBoC's Digital Currency Research Institute director Mu Changchun has attempted to make assurances that DCEP will provide users with greater privacy than commercial payment systems.[19] But DCEP will offer no true anonymity, as the PBoC will have both complete visibility over the use of the currency, and the ability to confirm or deny any transaction. There are design features that allow users to be more anonymous with more limits on transactions. Though a basic account does not need to be bound to a bank account but rather to a phone number, the increasingly effective implementation of regulations like "real-name" registration to purchase a SIM card mean those individuals are ultimately traceable even if initially transactions appear anonymous.

PBoC officials will conduct monitoring using big data analytics that flag unusual activity that might indicate illegal activity (as defined in the PRC, not the definition of "terrorism" above). The PBoC might also seek to monitor more closely a specific subset of individuals and entities, just like domestic smart cities solutions for policing like the Police Geographic Information

[14] '中联部原副部长预警，积极应对六大外部环境恶化的准备' [Former deputy minister of the International Liaison Department gives a warning, (make) preparations for actively responding to six major deteriorations in the external environment], Chongyang Institute for Financial Studies, Renmin University of China, 29 June 2020, online; 中钞区块链技术研究院 [China Banknote Printing and Minting Corp. Blockchain Technology Research Institute]; '中共中央党校《学习时报》：积极谋划我国数字货币发展' [CCP Central Party School *Study Times*: Actively plan the development of China's digital currency], China Banknote Printing and Minting Corp. Blockchain Technology Research Institute, 16 August 2019, online.

[15] See, Samantha Hoffman, "Social credit: Technology-enhanced authoritarian control with global consequences," ASPI, 28 June 2018: https://www.aspi.org.au/report/social-credit .

[16] Zhengzhong Xu, Hongwei Du, '世界格局变迁中的战略主动权之争' ('The struggle for strategic initiative amid changing patterns of the world)', People's Forum, 16 April 2015, online

[17] '宁夏：抢抓发展机遇 打造"丝路信用之城"' ('Ningxia: Grab hold of developmental opportunities and construct the "Silk Road City of Credit"'), People's Daily Online (Ningxia Channel), 28 September 2016, online.

[18] See Samantha Hoffman's chapter "DC/EP and Surveillance" in "The flipside of China's central bank digital currency" https://www.aspi.org.au/report/flipside-chinas-central-bank-digital-currency,

[19] https://www.coindesk.com/peoples-bank-of-china-official-says-fully-anonymous-digital-yuan-not-feasible

Systems that feed into the "Sharp Eyes" and "Skynet" surveillance projects.[20] For instance, these systems seek to monitor in real-time particular lists of individuals considered "key personnel". Maya Wang's work for Human Rights Watch has described key personnel tracking systems, which focus on "seven categories" of people, included petitioners, those who "undermine stability," those who are involved in "terrorism," major criminals, those involved with drugs, wanted persons, and those with mental health problems who "tend to cause disturbances."[21] Chinese publications have described the "key personnel early warning system" as involving relationship mining algorithms applied to collected data to locate 'criminal' networks, including political dissidents.[22]

There are also no express limits on the information-access powers of the party-state's political security or law enforcement agencies, such as the Central Commission for Discipline Inspection (CCDI), which has a keen interest in the technology. While DCEP could enable more effective financial supervision and risk management that any government might seek to embed in a central bank digital currency, the PRC's authoritarian system embeds political objectives within economic governance and otherwise reasonable objectives. Terms such as 'anti-terrorist financing', for instance, take on a different definition in the PRC that is directed at the CCP's political opponents, as the previous section elaborated.

Yao Qian (the PBoC's primary patent author on DCEP) described DCEP as having an 'anonymous front end, real-name backend'.[23] There's an element of anonymity through a characteristic of DCEP called 'controlled anonymity', but true anonymity doesn't exist, as currency registration and traceability are built into DCEP's transaction process. That process, augmented by data mining and big-data analysis, provides the PBoC with the ability to have complete oversight over the use of the currency. That functionality is provided through DCEP's "three centres". These are an "Authentication Centre" for recording and managing the identities of institutional and individual users; a "Registration Centre" for recording users' ownership of digital currency and history of transactions; and a "Big Data Analytics Centre" for analysing how money is being used, transacted and stored, supporting tracking and surveillance using static and real-time data, providing data and analysis inputs for monetary policy, and flagging financial fraud.

The term 'controlled anonymity' within the operation of DCEP means that the PBoC has complete supervision over the digital currency but has afforded users some anonymity for their transactions and protection of their personal information from other third parties besides PBoC.

---

[20] See also my new paper for the National Endowment for Democracy, "Double-Edged Sword China's Sharp Power Exploitation of Emerging Technologies," National Endowment for Democracy, April 2021: https://www.ned.org/wp-content/uploads/2021/04/Double-Edged-Sword-Chinas-Sharp-Power-Exploitation-of-Emerging-Technologies-Hoffman-April-2021.pdf and Dahlia Peterson, "Designing Alternatives to China's Repressive Surveillance State," CSET Policy Brief, October 2020, https://cset.georgetown.edu/research/designing-alternatives-to-chinas-repressive-surveillance-state/

[21] Maya Wang, "China: Police 'Big Data' Systems Violate Privacy, Target Dissent," *Human Rights Watch*, 19 November 2017, online.

[22] Gong Chunqiang, "Design and Implementation of Key Personnel Early Warning System Based On Telecommunication Data," (2015) Shanghai Jiaotong University.

[23] '姚前：中国法定数字货币原型构想' [Yao Qian: Prototype conception of China's legal digital currency], *China Finance*, issue 17, 2016, online.

DCEP has been designed such that, even if commercial banks and merchants were to collude, users' purchase history couldn't be determined by them or any other third party, except, crucially, the currency issuer (the PBoC).[24] PBoC Deputy Governor Fan Yifei has explained that full anonymity won't be implemented through DCEP in order to discourage crimes such as tax evasion, terrorism financing and money laundering.[25] All central banks would need to ensure that their digital currency meets anti-money laundering and countering terrorism financing rules. Central bank digital currencies would allow for better digital records and traces, but it's been suggested in a report by the Bank of International Settlements that such gains may be minimal because the illicit activity is less likely to be conducted over a formal monetary system that's fully traceable.[26]

DCEP is designed so it can be used without the need for a bank account, but digital wallets have a grading system such that wallets that are loosely bound to a real-name account have transaction size limits. A user can attain the lowest grade of digital wallet—with the transaction limits—by registering their wallets with a mobile number only (of course, phone numbers are required to be registered to an individual's real name in the PRC). Users can access higher grade digital wallets by linking to an ID or bank card. Through the Agricultural Bank of China, for instance, users are encouraged to upgrade their digital wallets to a 'Level 2 digital wallet' by registering with their name and national ID details.[27] If a user registers in person at a counter, there are no restrictions on their digital wallet.[28]

The integration of DCEP into third-party applications does not make users' transactions on those applications more private, but the underlying digital currency system is designed to provide privacy from third parties (except, of course, the central bank). That being said, practicalities when implementing any payment system mean that in practice, there is little anonymity for the individual from any app because the app will already know the user, and when transacting will need the user to identify the recipient of the funds and the transaction amount. Therefore, the implementation of DCEP into mobile applications, such as DiDi Chuxing, BiliBili and Meituan Dianping, that are in partnership negotiations with PBoC.[29] It doesn't change the amount of information those apps, and by extension, their linked platforms, are able to collect on the user.

DC/EP and the Social Credit System

[24] Patent application 201610179712.3 'Digital Currency System', online.

[25] '范一飞：关于央行数字货币的几点考虑' [FAN Yifei, Several considerations about the central bank's digital currency], *China Business Network app*, 2018, online.

[26] Committee on Payments and Market Infrastructures and Markets Committee, 'Central bank digital currencies', Bank of International Settlements, 2018, online.

[27] Agricultural Bank of China DCEP test app manual. '重磅！央行数字货币DCEP在农行内测（附测试链接）' [Huge! The Central Bank's digital currency DCEP is tested internally in the Agricultural Bank of China (with test link)], *Sina Finance*, 15 April 2020, online.

[28] Mu Changchun, '科技金融前沿：Libra 与数字货币展望', [Frontiers of technology and finance: Libra and digital currency outlook], *DeDao App*, August 2019, online.

[29] Hu Yue, Denise Jia, 'Didi partners with Central Bank on digital currency trial', *Caixin*, 9 July 2020, online.

I have been asked to specifically address the potential linkage between DCEP and China's social credit system. My assessment is based on my research on both of these separate topics, but it should be noted that there is no publicly available authoritative sourcing that specifically addresses the link between the social credit system and DCEP. At this point, understanding of how the two systems might interact is at best extremely vague. Further research is required to better articulate how this potential future interaction would look in practice.

The People's Bank of China and the National Development and Reform Commission are the key central institutions responsible for the construction of the social credit system (though the actual system requires a whole of government approach).[30] It is logical to assume that financial transactions data derived from DCEP transactions might play into the social credit system given the PBoC's direct role in both. This is especially true if we take into account the disciplinary policy drivers behind DCEP, which, at least conceptually, are similar to the kinds of data that would indicate the trustworthiness or honesty of an individual or entity being evaluated using the social credit system.

According to PBoC data, the social credit system covered 1.1 billion individuals and over 60 million enterprises and organisations at the end of 2020.[31] The financial transactions data DCEP generates could, in future, be ingested into big data analysis platforms associated with the social credit system. DCEP would most likely support aspects of the social credit system related to the development and sharing of financial credit information. The PBoC's 'credit reference' system, covering financial credit data, is a core part of the social credit system. Even though this deals with financial information, it is neither completely separate nor completely distinct from the "social credit system" as a whole. The social credit system combines both social integrity and financial credit – these are distinct in some areas, but ultimately overlapping parts of the larger "social credit" construct.

Functionally, if a link exists between DCEP and the social credit system, this does not necessarily imply that in the future the data generated through DCEP would in real time and automatically feed into or be reflected in a financial credit record or other social credit-linked output directly. It does, however, mean that either real-time or non-real-time data could be ingested into credit platforms. Such data could be processed into information that would support the generation of social credit-linked outputs. We know there are already three data centres being established in association with DCEP, so transaction data is already going to a big data analysis platform. Hypothetically, the big data analysis centre would streamline the information that would feed into another platform like a social credit linked big data information centre. [32]

[30] '社会信用体系建设工作由发展改革委、人民银行牵头进行' [The construction of the social credit system is led by the National Development and Reform Commission and The People's Bank of China], *China Government Net*, 23 July 2014, online.

[31] 'China's social credit system covers 1.1 billion people by end 2020', *Global Times*, 26 January 2021, online.

[32] Based on research I've done on other systems, specifically some linked to smart cities, data from various cloud platforms like "public security" or "traffic" clouds is integrated into a larger pool of data and then processed for specific outputs.

For instance, streamlined information could include data specific to KYC, anti-money laundering and anti-terrorist financing requirements. An article published through the Development and Research Centre of the State Council in April 2020, for instance, suggested that the Authentication Centre and Big Data Analytics Centre of DCEP's "Three Centres" would "enhance the central government's ability to control the monetary system such as KYC, anti-money laundering, and anti-terrorist financing. It said that "the central bank's credit reference advantage and KYC and AML capabilities can be communicated to commercial banks through the combination of traditional accounts and digital currency wallets."[33]

Bear in mind the political implications of concepts like "anti-terrorist" financing as they affect the kinds of credit information the credit reference centre holds and shares. In 2014, deputy director of the PBoC Pan Gongsheng said that "establishing a credit information sharing mechanism was one of the important tasks to promote the construction of China's social credit system." Pan added:

> "Carrying out information collection cooperation is conducive to realizing the interconnection of credit information between government departments and credit institutions, helping credit institutions to effectively prevent credit risks, and reducing risks in the entire financial system. [Carrying out information collection cooperation] is conducive to establishing a joint disciplinary mechanism and improving the efficiency of administrative law enforcement by government agencies, realizing the coordinated supervision of untrustworthy behaviour. [Carrying out information collection cooperation] is conducive to enhancing the credit awareness of information subjects, forming a systemic arrangement of "[if one] keep one's promise, then [they will] be provided incentives; if [one] breaks one's promise, then [they will] be punished, improving the social credit environment and accelerating the construction of the social credit system."[34]

For as hypothetical as the above technical aspects of this system might appear, it is important to emphasise that technologies -- like social credit big data analysis platforms -- are being researched and developed to meet the needs that are typically set out in government standards documents. Dozens of companies' products are involved in social credit platforms across the PRC, making the implementation appear chaotic. Yet, there are also national standards being developed for the social credit system. The National Social Credit Standardisation Technical Committee, which held its inaugural meeting in 2016, oversees the research and development of standards. [35] Application of standards like these should be universal for any social credit big data platform that wins a contract no matter what company is involved. The current or future implementation of standardised database schema creates a trajectory whereby the seamless

[33]杨荣、陈翔：央行数字货币对商业银行的影响' [Yang Rong and Chen Xiang: The Impact of DCEP on Commercial Banks], *China Thinktanks, Development Research Center of the State Council*, 23 April 2020, online.

[34] '人民银行与环保部、税务总局等单位签署征信系统信息采集合作文件' [The People's Bank of China, the Ministry of Environmental Protection, the State Taxation Administration and other units signed a cooperation document on credit information collection], Credit Reference Center, The People's Bank of China, 11 December 2014, online.

[35] For example, '公共信用信息分类与编码规范' [Classification and coding specifications of public credit information], *National Public Service Platform For Standards Information*, 29 December 2018, online.

integration of information from across local platforms to national platforms is far more achievable than might meet the eye at a surface level evaluation of the sheer number of companies involved.

In a new report for the National Endowment for Democracy's Sharp Power series, I describe how standardisation of emerging technologies is taking place at the design level.[36] Contrary to arguments that fragmentation is a significant barrier to the success of the Party-state's tech-enhanced authoritarianism, there are strong indicators that the groundwork has been laid for seamless interoperability between smart cities systems to be achieved, and it is reasonable to assume the same is possible with social credit-linked platforms. Government and research institutes collaborate with companies to standardise equipment development and the requirements that companies must meet to successfully bid for a project. For instance, a 2016 document entitled "GA/T1334: Technical Requirements of Facial Recognition Application in Security and Face Image Extraction from Videos—Application Programming Interface of Facial Recognition in Security System" was drafted by 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; tech companies, such as Hikvision and Dahua; and public security bureaus, such as the Shanxi Provincial Public Security Department and the Wuhan Public Security Bureau.[37] Documents like these are used as a basis for technical requirements in government procurement contracts. A new report by IPVM has separately made a very similar case using the same kinds of documents.[38]

Future extraterritorial implications?

To project future extraterritorial implications of DCEP, one must assume that the project will first succeed domestically and then be exported globally. There are channels through which this might take place or where certain activities might assist this future uptake. China has a clear ambition to shape global technological and financial standards. As Matt Johnson and John Garnaut highlighted in their contribution to the ASPI report, with China Standards 2035 on the horizon, DCEP and its related technologies are likely to be an important component in China's push to establish a comprehensive alternative to the dollar system. The liberalisation of China's current account is not required for the export of the DC/EP technology stack to other countries. China's ability to develop new financial technology that embeds authoritarian norms of control and surveillance may affect global standards and financial infrastructure well before the internationalisation of the renminbi is achieved.

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

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

[38] 'Dahua and Hikvision Co-Author Racial And Ethnic PRC Police Standards', *IPVM*, 30 March 2021, online.

Conceptually, the political motives for tools of power expansion are clear. As I highlighted in my contribution to the ASPI report, under Xi Jinping, the concept of social management has expanded to specifically include 'international social management.[39] Something to consider is the fact that Hong Kong's new state security law criminalises separatism, subversion, terrorism, and collusion in and support for any of those activities by anyone in the world, no matter where they are located.[40] This means that journalists, human rights advocacy groups, researchers or anyone else accused of undermining the party-state and advocating for Hong Kong democracy could be accused of those four types of crime. By extension, anyone financing those individuals or entities (such as funding a research group) could potentially be linked to the accusations. If DCEP is successfully rolled out and adopted in the distant future, then the world would have to be prepared to contend with a PRC in possession of information that would also allow it to enforce its definitions of the activities that it's monitoring (anti-corruption and anti-terrorism, for instance) globally, thus potentially allowing it to implement PRC standards and definitions of illegality beyond its borders with greater effectiveness.

Policy Responses

We cannot keep treating technology as neutral when it is intertwined with the ambitions of the Party-state, which go beyond normal problem-solving to include the protection and expansion of the Party's power. These ambitions cannot simply be removed or ignored when technology is researched and developed to meet those political needs.

Our previous ad hoc approaches to Huawei and Tik Tok were reactive, coming after they had already entered the market. Countries that have chosen to act against Huawei, Tik Tok, and other PRC-developed technology have done so in large part because of the ways Beijing can exert power over companies or companies that might comply with those demands. While these are solid arguments, they do not address the inevitable vulnerabilities in any software or hardware given the politics driving the development of PRC tech standards they meet or help establish or the intended problems the technologies are designed to solve (when the Party's problem-solving efforts often drive the R&D itself). The technology itself isn't agnostic, and technical assessments tend to be framed in ways that do not get to the core design risks that explain why.

Take, for instance, the issue of supply chain security. Often, conversation on supply chain security is focused on logistics or physical elements of the supply chain. When this is inclusive of risks to the digital supply chain, namely data security, cyber security experts tend to focus on the ways threat actors can exploit hardware and software vulnerabilities. They do not focus on how data harvesting through the supply chain as part of business activity is part of what the

[39] Liqun Wei, '党的十八大以来社会治理的新进展' [New progress of social governance since the 18th Party Congress], *Guangming Daily*, 7 August 2017, online. The author, Wei Liqun, is a former Director of the State Council Research Office and former Deputy Director of the National School of Administration.

[40] Dominic Meagher, 'Has Hong Kong's national security law created secret police with Chinese characteristics?', *The Strategist*, 14 July 2020, online.

Party-state uses or exploits to meet political needs that global bulk data collection and processing can support.[41]

To appropriately deal with these kinds of risks, the United States and others need to apply a new framework for evaluating such technologies as to their suitability that explicitly includes the actors who maintain control over their functioning and the data they collect. Below are some of the key issues that I think need to be addressed:

- The US government and others cannot stop the development of DCEP within the PRC and cannot change DCEP's policy drivers. Governments must be prepared to mitigate the political risks by investing in research into and developing credible alternatives to DCEP for all key highly traded currencies.

- Governments must attempt to understand emerging technologies more proactively and seek to develop better ways of regulating financial technology. When Congress investigates the risks associated with Financial Technology – and develops laws and regulations to address specific issues like data privacy – the assessment of risk needs to be more holistic and inclusive or varying political intent of different actors. It must be sophisticated enough to address those variations at a core level. Right now, conversations on policy responses for dealing with such risks are still very surface level because our framework of responses has not adjusted to meet the challenge.

- Beijing has repeatedly broken its agreements on issues large and small, ranging from intellectual property rights protections to the Sino-British Joint Declaration related to Hong Kong. Given this track record and the CCP's explicit ambitions for the use of DCEP and other technologies, the presumption should be that the party-state will exploit the technology's potential international reach. What concrete protections are embedded that prevent Beijing from misusing the access and data that it gains?

DCEP's rollout is likely to have notable ramifications for governments, investors and companies, including China's own tech champions. More analysis is needed before prescriptive policy solutions can be developed for the political and financial oversight challenges DCEP could create. At the same time, it's important to act in anticipation of key shifts in global financial regulation and advances in financial technology so that governments don't end up trying to reverse course when it's too late to deal with the systemic risks DCEP could create. Below are a few starting points:

- A clear domestic authority for financial technology regulation should be designated, but this must take place under the aforementioned condition that our framework for understanding the problem is also adjusted to meet political challenges embedded in financial technologies like DCEP.

[41] The GTCOM case study in my 2019 report Engineering Global Consent helps to illustrate this risk, see: Samantha Hoffman, 'Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion,' the Australian Strategic Policy Institute, 14 October 2019, online.

- Early efforts to establish and coordinate norms, rules and standards will reduce any subsequent need to resort to blunt and arbitrary measures that are economically, socially and diplomatically disruptive. Although democracies should develop a set of standards and norms, Beijing's willingness to adhere to those agreements when its political priorities lead in a different direction also has to be considered.

- Decision-makers in liberal democracies must develop a clear strategy for detecting flaws in and improving the existing system for global financial governance and work to improve international coordination among each other to achieve those strategic outcomes.