

China's Tech-Enhanced Authoritarianism

Testimony before the House Permanent Select Committee on Intelligence
Hearing on "China's Digital Authoritarianism: Surveillance, Influence, and Political Control"

Written Testimony of Dr. Samantha Hoffman¹
Fellow at The Australian Strategic Policy Institute
Fellow at The China Forum
Independent Consultant

May 16, 2019

Overall Assessment

Chairman Schiff, distinguished members of the Committee, thank you for the opportunity to testify on this subject of critical importance to the United States. I will begin with a few key observations:

- [1] The United States and other liberal democracies have massively underestimated what China would do with its vision to use technology to augment its authoritarianism. What we are seeing now is a manifestation of plans already in place and in fact public for years, even decades. We are still underestimating their potential.
- [2] The CCP uses technology to make its Gordian knot of political control inseparable from China's social and economic development. The CCP's construction of the social credit system and development of smart cities are the embodiment of this strategy, allowing the CCP to blur the line between cooperative and coercive control.
- [3] Technology already allows the CCP to expand its power in ways we have not been prepared to think about previously. The issue can only be framed through the CCP's concept of state security, which places *political security* and *ideological security* at its core. The concept is not about protecting China and the Chinese people separately from the Party's leadership.
- [4] To guarantee state security, the CCP prioritizes expanding its power. The CCP's "state security" strategy implies that the scale of the challenge is much larger than the scope of current debate. The U.S. is not simply managing a threat to national security, but also to long-term economic stability, security and the protection of civil liberties.
- [5] The CCP's power-expansion effort does not stop at China's geographic borders, largely because state security strategy is driven by the Party's political and ideological core. The CCP aims to re-shape global governance. It attempts to control international discourse on China and the channels through which individuals, businesses, and governments, can engage with China. It expects technology to enhance the sophistication of this process.

¹ In addition to new material, this testimony also uses content directly pulled from the author's previously published work and PhD thesis.

The CCP's Concept of State Security

At a rapidly increasing rate, western media is exposing the ways the Chinese Communist Party (CCP) uses or plans to use modern technology to expand its authoritarian reach. Without the ability to analyze the developments through the lens of Chinese Communist Party's state security strategy, U.S. decision-makers cannot develop strategies for responding to the ways the CCP deploys technology to augment its authoritarianism.

The problem is visible in major global debates on China, notably in the debate on whether or not to ban Huawei from participating in the construction of 5G networks. The debate tends to overly narrow the range of security threats Huawei poses because the risk of espionage is put into the context of a western liberal democratic society's version of "security". This thinking does not take into account the impact of a CCP-driven state security strategy that prioritizes the protection and expansion of the CCP's own political power above all else.

For the CCP the border that matters most is not the border between the PRC and the world, but rather the border between the Party and everybody else. The more channels that open up between China and the outside world, the more the Party has to fill in and ensure those channels are controlled. As China expands outward economically and socially the Party's political control by its own definition of security must also expand. The CCP's objective is to be the sole arbiter of what China is, and what it means to be Chinese inside or outside China.

Under Xi Jinping, numerous laws on state security have been enacted, these include: the Counter-Espionage Law (2014, which replaced the 1993 State Security Law), the State Security Law (2015), the Foreign Non-Governmental Organization Management Law (2016), the Counterterrorism Law (2015), Cyber Security Law (2016), and the Intelligence Law (2017), among others. Above all, the laws are a tool the Party uses to manage its own power.²

The laws are clear that every individual and entity is responsible for guaranteeing state security.³ The Intelligence Law, for instance, states "any organization and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of..." Not only is everyone required to participate in intelligence work when asked, but that participation must be kept secret.

Earlier this year, Huawei attempted to defend itself against international pressure using two "independent" legal opinions, which essentially claim the broad scope of the laws is a reason for the narrowest, not broadest, possible interpretation. The first document is a May 27, 2018 declaration the Beijing-headquartered Zhong Lun Law Firm provided to the US Federal Communications Commission.⁴ The second is a November 2018 review and comment backing up the Zhong Lun declaration, which London-based law firm Clifford Chance wrote for its client

² Samantha Hoffman and Peter Mattis, "Managing the Power Within: China's State Security Commission," 18 July 2016.

³ Samantha Hoffman, "'Dangerous Love': China's All-Encompassing Security Vision," 2016. ; Samantha Hoffman. "China's State Security Strategy: 'Everyone is Responsible'." *The Strategist*, 11 December 2017. <https://www.aspistrategist.org.au/chinas-state-security-strategy-everyone-is-responsible/>.

⁴ "Exhibit B: Supplemental Expert Report of Jihong Chen and Jianwei Fang ", <https://ecfsapi.fcc.gov/file/10806043972847/Huawei%20Ex%20Parte%20Written%20Submission%20Docket%20No.%2018-89%20%5BEXHIBITS%20A-M%5D.pdf>.

Huawei.⁵ Clifford Chance appears to recognize the pointlessness of its paper with the disclaimer that it “should not be construed as constituting a legal opinion on the application of PRC law.” The problem is, the *application* of law is central to the Huawei debate.

In the PRC, the law is a tool for the Chinese Communist Party to set expectations and communicate its intentions. By the Party’s own definition, the law functions to ensure the Party’s political security above everything else. In fact, as Xi Jinping said in a speech published in February, “Comprehensively relying upon the law to rule the country does not at all weaken the Party’s leadership...” but rather consolidates the Party’s hold on power. In other words, the law is a tool for making the Party’s political control more effective and the CCP can apply the law in whatever way it chooses.

At the third plenary session of the 18th Central Committee of the Chinese Communist Party (CCCPC) in November 2013, the Party’s communique announced the formation of the “Central State Security Commission” (CSSC) in a paragraph on “social governance”.⁶ The later creation of China’s Central State Security Commission in January 2014 and developments since its creation also point to the political and ideological nature of state security.

“Social governance,” also called “social management,” has its roots in the core ideology of the Chinese Communist Party. It describes Mao Zedong’s organizational guide, the “mass line”. The mass line describes how the Party leadership attempts to shape and control society as a means for expanding and protecting its power. The mass line suggests that people should be co-opted into participating in their own management. Social governance, by extension, is a pre-emptive form of state security.

Despite this relationship between social management and state security, most analysts have assessed the CSSC within a crisis management framework, as it would be understood through the example of the United States’ National Security Council.⁷ The CSSC is not a crisis management body, it is a crisis *pre-emption* body. The CSSC coordinates the work of agencies and ministries charged with ensuring state security.

Across China at local government levels, state security leading groups, now upgraded to commissions, have designated working groups within them covering areas including counter-terrorism, counter-espionage and intelligence. At local government levels these State Security

⁵ The documents have not been released publicly, but the author has obtained copies.

⁶ Samantha Hoffman and Peter Mattis, "China’s Proposed “State Security Council”: Social Governance under Xi Jinping," *China Policy Institute: Analysis*, 21 November 2013. ; Samantha Hoffman and Peter Mattis, "Inside China's New Security Council," 21 November 2013. ; Hoffman and Mattis, "Managing the Power Within: China's State Security Commission.;" "Communique of the Third Plenary Session of the 18th Central Committee of the Communist Party of China." 15 January 2014. http://www.china.org.cn/china/third_plenary_session/2014-01/15/content_31203056.htm.

⁷ Andrew S. Erickson and Adam P. Liff, "Installing a Safety on the ‘Loaded Gun’? China’s Institutional Reforms, National Security Commission and Sino–Japanese Crisis (In)stability," *Journal of Contemporary China* 25, no. 98 (2016); Weixing Hu, "Xi Jinping’s ‘Big Power Diplomacy’ and China’s Central National Security Commission " *Journal of Contemporary China* 25, no. 98 (2016); David M. Lampton, "Xi Jinping and the National Security Commission: Policy Coordination and Political Power," *Journal of Contemporary China* 24, no. 95 (2015); Joel Wuthnow, "Decoding China's New 'National Security Commission'," *CNA Brief* (2013); Joel Wuthnow. "China’s Much-Heralded NSC Has Disappeared." *Foreign Policy*, 2016. <http://foreignpolicy.com/2016/06/30/chinas-much-heralded-national-security-council-has-disappeared-nsc-xi-jinping>; Samantha Hoffman, "Programming China: The Communist Party’s Autonomic Security Approach to Managing State Security," in *MERICCS China Monitor* (Mercator Institute for China Studies, 12 December 2017).

Work Leading Small Groups were established mostly between the 1 July 2015 passage of the State Security Law and the first annual “State Security Education Day” on 15 April 2016, according to publicly available sources. Since November 2018, many if not most of these leading groups have been upgraded to the status of “commission”.⁸

Political and Legal Affairs committees (comprising of the judiciary and public security organs) are partly subordinate to this system. They are also central to the development of China’s surveillance state. According to regulations effective in January 2019, the Party’s Political and Legal Affairs Committees across China are required to implement state security decision-making of central and local state security leading mechanisms (referring directly to the Central State Security Commission and local level state security leading groups and state security commissions) while prioritizing political security.⁹

The centrality of politics in state security work highlights the fact that the CCP’s version of state security seeks to prevent perceived threats to state security, especially in the realm of political and ideological security, from having the opportunity to emerge.

Tech-Augmented Control

The Chinese Communist Party’s effort to use technology to expand its power is best described as “tech-enhanced” or “tech-augmented” authoritarianism. It describes processes the CCP has been engaged in for decades augmented through technology.

The coercive nature of the CCP’s tech-enhanced authoritarianism is on full display through the construction of a police state in Xinjiang, where an estimated 1.5-million Muslims, predominately members of the Uyghur ethnic group, are suffering in extra-judicial internment camps on the basis of their ethnic identity.¹⁰ Early forms of smart cities (or “safe cities”) ecosystem, which include invasive monitoring including facial recognition and mobile applications, are deployed to support the suppression of an entire population.¹¹

Smart cities projects are being developed on the basis of a range of government plans including but not limited to the “3111 Project”, Document No. 996, the Skynet Project and the *Xueliang* Project. Hundreds of projects exist and are at various stages of development. The technology is not trialed in Xinjiang with the possibility that it might spread elsewhere, instead the initial development of the systems began elsewhere in China. Their visibility and intrusiveness is more distinct in Xinjiang.

⁸ "林铎在省委国家安全委员会第一次会议上强调全面贯彻落实总体国家安全观 努力推动国家安全工作上台阶 唐仁健出席." *Gansu Daily*, 29 December 2018. http://www.gansu.gov.cn/art/2018/12/29/art_4422_415654.html; "河南省级机构改革: 设党委机构 18 个 政府机构 42 个." *Henan Daily*, 6 November 2018. http://www.ha.xinhuanet.com/news/2018-11/06/c_1123668742.htm.

⁹ "全民国家安全教育日 这 20 个法律知识你懂吗? (National State Security Education Day: Do You Understand These 20 Legal Trivia?)." *The People's Liberation Army Daily*, 7 April 2017. http://www.81.cn/2017gjaqjyr/2017-04/07/content_7553451.htm; "中共中央印发《中国共产党政法工作条例》." *Xinhua*, 18 January 2019. http://www.xinhuanet.com/politics/2019-01/18/c_1124011592.htm.

¹⁰ Chris Buckley and Amy Qin. "Muslim Detention Camps Are Like 'Boarding Schools,' Chinese Official Says." *The New York Times*, 12 March 2019. <https://www.nytimes.com/2019/03/12/world/asia/china-xinjiang.html>.

¹¹ Earlier this month, Human Rights Watch published a groundbreaking report after ‘reverse-engineering’ an app authorities in Xinjiang use to assist its effort to monitor and control all aspects of people’s lives, see: Maya Wang, "China’s Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," (Human Rights Watch, May 2019).

Smart cities are not solely about enhanced policing. Smart cities also support service allocation and resource management. The conceptual and technical groundwork for smart cities technology was laid in areas such as e-governance projects and later “grid policing” and “grid management”.

Between 1984 and 1990, the State Council approved of plans to develop national information systems covering about a dozen areas, including the economy, banking, electrical power, civil aviation, statistics, taxation, customs, meteorology and disaster mitigation.¹² By 1993, these early e-government plans turned into projects initially known as the “Three Golden” projects. Golden Shield, initiated sometime around 1998 or 1999, is the most well-known of these, and involved connecting the Ministry of Public Security with its local-level bureaus, and it was already widely employed at provincial and city levels by 2002.¹³

Efforts like Golden Shield supported grid policing programs initiated around 2001 and 2002 in separate localities across the country, initially in Shanghai.¹⁴ In this early stage, it was characterized mostly by enhanced monitoring and surveillance and more efficient data sharing within a designated area and within public security bureaus. Projects that began as grid policing in the early 2000s gradually expanded to a broader “grid management” concept. Grid management enabled the organization of data to generate better situational awareness and predictive capacity, as well as enhanced tracking and monitoring of individuals.¹⁵ The effort involves physically and virtually separated areas into grids for surveillance and knowledge building to serve both cooperative and coercive functions.

Smart cities are a natural progression from this early effort. Their current development across China is in various stages depending on locality, but my research shows that it is also far more coherent than is often assumed. The kinds of smart cities surveillance systems recently exposed through data breaches, such as one near the U.S. Embassy in Beijing, are already operational, though the operability certainly varies, across China.¹⁶

China’s widely-discussed Social Credit System overlaps with smart cities projects and tech surveillance. Commercial social credit apps, for instance, share data with police and vice-versa. The data collected may be vast and not entirely usable at present, but as advances in big data

¹² Yu Xu and Hongren Zhou, *中国信息化形势分析和预测(2010) (Analysis and Forecast on China's Informatisation (2010))*, 信息化蓝皮书 (Blue Book of Informatisation) (Beijing: Social Sciences Academic Press, 2010), 8.

¹³ Peter Mattis, "China's Adaptive Approach to the Information Counter-Revolution," *China Brief* 11, no. 10 (2011); Yu Jijun, "公安部推广使用“城市公安综合信息系统” (Ministry of Public Security to Promote the Use of "Urban Public Security Comprehensive Information Systems")," *The People's Daily*, 26 April 2002.

¹⁴ Lei Mao, "社会治安保持平稳防控能力得到提高上海严重刑事犯罪发案数下降 (Social Security and Order Remain Steady; the Prevention and Control Capacity has Improved; the Number of Serious Criminal Cases in Shanghai have Decreased)," *The People's Daily*, 3 August 2001. ; Jinyi Zhao, "上海治安启示录 (The Revelation of Shanghai's Public Security)," *The People's Daily*, 22 August 2001. ; Ye Yang, "严密治安防控的成功实践——上海警方打击街面“两抢”犯罪纪实 (Successful Implementation of Strict Law and Order Prevention and Control -- Accounts of Shanghai Police Striking the Streetside "Two [kinds of] Robberies")," *The People's Daily*, 14 August 2002.

¹⁵ Jie Li and Changrong Qu, "警力下沉 网格布警 科技强警 郑州筑牢社会治安防控体系 今年前八月各类刑事案件同比下降两成多 (The Police Force Goes Grassroots; Grid Deployment of the Force; Scientifically Strengthen the Force; Zhengzhou Building a Sturdy Social Security Prevention and Control System, For the First Eight Months This Year, Criminal Cases Have Declined by Twenty Percent)," *The People's Daily*, 15 October 2006.

¹⁶ Zack Whittaker, "Security lapse exposed a Chinese smart city surveillance system: Thousands of facial recognition scans were matched against Chinese police records," 3 May 2019. <https://techcrunch.com/2019/05/03/china-smart-city-exposed/>.

analysis and decision-making technologies improve, currently unusable data will contribute to improved predictive applications, which is the Party's clear intent.

The Party describes social credit as a system to build trust, but the trust is CCP-defined. The system is not about improving trust between individuals and trust between entities subject to the system. Instead it is about the Party trusting society, and its members, to uphold its power. The CCP's political control itself sets the parameters for what is normal or acceptable behavior. Social credit aims to normalize the decision-making behaviors of individuals and entities by discouraging any deviation from the ill-defined grey space of acceptable and unacceptable behavior.

Social credit relies on enhanced interagency information sharing. The integration of data supports the CCP's ability to analyze, monitor, shape and rate the behaviour of individuals and entities. It involves cooperative and coercive tactics and improving government services as a way of exerting control through convenience.

The system's complexity and the difficulty of integrating its many components does not indicate the absence of clear intentions. The best research on earlier versions of the Party-state's tech-enhanced authoritarianism was published in 2001 by Gregory Walton, who wrote at the time: "Ultimately the [CCP's] aim is to integrate a gigantic online database with an all-encompassing surveillance network – incorporating speech and face recognition, closed-circuit television, smart cards, credit records, and Internet surveillance technologies."¹⁷ At the time, his assessment was often dismissed as science fiction, perhaps the problem these critics had was the failure to imagine the CCP could succeed. Now under 20 years later, Walton has been proven startlingly accurate.

Global Consequences

Many of China's surveillance technologies are exported overseas to both liberal and illiberal regimes. In April, the Australian Strategic Policy Institute published a report Mapping China's technology giants and corresponding Mapping China's Tech Giants website.¹⁸

Through this research and as of April 2019, we mapped 75 Smart City-Public Security projects, most of which involved Huawei. Those projects—also euphemistically referred to as 'safe city' projects—include the provision of surveillance cameras, command and control centers, facial and license plate recognition technologies, data labs, intelligence fusion capabilities and portable rapid deployment systems for use in emergencies. Turkey, for instance, is a country where at least 10,000 Uyghurs live in exile according to Human Rights Watch Figures.¹⁹ From afar, they still struggle to escape the CCP's authoritarian reach, yet in 2018, Turkish mobile operator Turkcell signed an agreement to collaborate with Huawei on 5G and smart cities development. How would a deal like this coming to fruition be leveraged to increase the Party's capacity for control over its political opponents and victims?

¹⁷ Greg Walton, "China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China," International Centre for Human Rights and Democratic Development, 2001. <http://publications.gc.ca/collections/Collection/E84-7-2001E.pdf>.

¹⁸ Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas, "Mapping China's Technology Giants," in *Issues Paper No. 15* (The Australian Strategic Policy Institute, April 2019). Website: <https://chinatechmap.aspi.org.au/>
¹⁹ "Eradicating Ideological Viruses": China's Campaign of Repression Against Xinjiang's Muslims," 9 September 2018. https://www.hrw.org/sites/default/files/report_pdf/china0918_web2.pdf.

The Party's far-reaching efforts to manage its power points to its wide-range of perceived threats. The emergencies China prepares for range from isolated but large-scale unrest events, to massively destabilising unrest events. They also include wars, not just over disputed territory like the South and East China Seas, but also an attack on the Chinese mainland by a foreign military, particularly in a scenario like the Kosovo War where a domestic conflict could be a justification for outside interference.²⁰

It may seem far-fetched to an outsider, but the ideas have clear importance in the CCP's thinking on state security. It is part of why multiple defence white papers point to "signs of increasing hegemonism, power politics and neo-interventionism."²¹ Others have claimed: "[China] faces strategic manoeuvres and containment from the outside while having to face disruption and sabotage by separatist and hostile forces from the inside."²² The perception is magnified where technology is seen as a means for supporting a Colour Revolution or Jasmine Revolution-like event or movement. This integrated perception of threat also helps to explain concepts such as cyberspace sovereignty. Cyberspace sovereignty is not just about the protection of a physical space, but is the protection of an unbounded ideas space that transcends all borders.

To prevent this kind of infiltration requires a constant expansion of power, meaning domestic stability is not the only priority. State security strategy is projected outward to shape the way external actors engage with the Chinese Communist Party. Writing for the Texas National Security Review Liza Tobin, noted that at the United Nations in January 2017, Xi Jinping gave a speech likening the CCP's framing for global governance (the community of common destiny) to a Swiss army knife — a Chinese-designed multifunctional tool for solving the world's problems. On both occasions, he proposed the concept as a better model for global governance in five dimensions: politics, security, development (economic, social, technological, etc.), culture, and the environment. In sum, the five dimensions reflect the extraordinarily wide range of arenas in which Beijing believes it must restructure global governance to enable China to integrate with the world while at the same time achieving global leadership."²³

Realizing this objective necessitates a long-term process of creating feedback loops, as if the concept of "social governance" or "social management" was internationalized. In fact, the term "international social management" has on occasion been used, including by Xi Jinping, to describe China's concept of global governance. Technology-enhanced authoritarianism, including the social credit system and smart cities technology, can help support this goal.

²⁰ Hoffman, "China's State Security Strategy: 'Everyone is Responsible'."

²¹ "中国武装力量的多样化运用 (The Diversified Employment of China's Armed Forces)," (Information Office of the State Council, The People's Republic of China, 2013); Information Office of the State Council of the People's Republic of China, "2000年中国的国防 (China's National Defence in 2000)," October 2000.

²² Information Office of the State Council of the People's Republic of China. "中国的军事战略《2008》 (China's National Defence in 2008)," January 2009.

²³ Liza Tobin, "Xi's Vision for Transforming Global Governance: A Strategic Challenge for Washington and Its Allies," *Texas National Security Review* 2, no. 1 (2018).

An overlooked purpose of the social credit system is to strengthen [the PRC's] "discourse power" or "right to speak" (话语权).²⁴ This can also be understood as building the CCP's narrative control. Discourse power "is an extension of soft power, relating to the influence and attractiveness of a country's ideology and value system".²⁵ Discourse power allows a nation to shape and control its internal and external environment.

In the hands of political opponents, discourse power is a potential threat. According to the CCP, "hostile forces" can incite and exploit economic and social disorder in other countries.²⁶ This threat has been tied directly to leading international credit agencies – namely Moody's Investors Service, Standard and Poor's, and Fitch Ratings – are seen as potential threats to China. One article claimed the agencies can "destroy a nation by downgrading their credit score, utilising the shock power of 'economic nukes'." ²⁷ Another article tied the problem to One Belt One Road (OBOR), because participant countries accept the current international ratings system. For the CCP, the solution is to increase the "discourse power [China's] credit agencies possess on the international credit evaluation stage."²⁸

Preventing this sort of crisis requires the CCP to have control over the narrative to prevent a political opponent from taking over the narrative – in other words it requires the CCP to strengthen its "discourse power". Discourse power is directly embedded in the trust and morality social credit is supposed to create in Chinese society, and not only because trust and morality help with everyday social and economic problem-solving. This linkage is traced to at least the early 1980s with a propaganda effort related to "spiritual culture", which responded to "popular disillusionment with the CCP" and the promotion of western politics as "superior" to China's.²⁹

One reason social credit contributes to strengthening the CCP's discourse power is that the system relies on the collection and integration of data to improve the CCP's awareness of its internal and external environments. In, 2010, Lu Wei described in detail the meaning of "discourse power" as not only referring to the "right to speak", but also to guarantee the "effectiveness and power of speech".³⁰ He elaborated that for China to have discourse power requires both collection power

²⁴ For example, see: "被低估的中国信用." *Globe Biweekly*, 20 September 2017. http://www.xinhuanet.com/globe/2017-09/18/c_136618566.htm.

²⁵ Peter Mattis, "An American Lens on China's Interference and Influence-Building Abroad," *The Asan Forum*, 30 April 2018. <http://www.theasanforum.org/an-american-lens-on-chinas-interference-and-influence-building-abroad/>; Peter Mattis, "China's International Right to Speak," *China Brief* XII, no. 20 (19 October 2012).

²⁶ Titus C. Chen, "China's Reaction to the Color Revolutions: Adaptive Authoritarianism in Full Swing," *Asian Perspective* 34, no. 2 (2010).

²⁷ Zhengzhong Xu and 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. http://www.cssn.cn/zxx/gjzxx_zxx/201504/t20150416_1589558_3.shtml.

²⁸ "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. <http://nx.people.com.cn/n2/2016/0928/c378047-29074734.html>.

²⁹ Anne-Marie Brady, *Marketing dictatorship : propaganda and thought work in contemporary China*, Asia/Pacific/perspectives (Lanham, Md. ; Plymouth: Rowman & Littlefield, 2007), 26. ²⁹ An example from the time period is the controversial television show "He Shang" (River Elegy)", see: Xiaomei Chen, *Occidentalism : a theory of counter-discourse in post-Mao China* (New York ; Oxford: Oxford University Press, 1995), 28-29. This is also an explanation for why "cultural security" (文化安全) is part of the CCP's "holistic" state security concept.

³⁰ Lu Wei is the now jailed former Publicity Department and Cyberspace Administration of China head, who in 2010 was then deputy director of Xinhua News Agency. The article added, in the phrase discourse power/ right to speak (话语权) "quan"

and communication power. Collection power is the ability to “collect information from all areas in the world in real time.” Communication power, which “decides influence” meanwhile, becomes stronger with more timely collection power.

Data collection supporting this environmental awareness does not stop at China’s borders. Social credit requires real-time monitoring through big data tools that can inform decision-making and the implementation of the credit system. A magazine affiliated with the International Liaison Department, “Contemporary World”, published an article focused on big data collection associated with OBOR.³¹ It said data could be used to inform diplomatic and economic decision making, as well as emergency mobilisation capacity. “Data courier stations” within foreign countries would send data via back-ends to a centralised analysis centre in China. Data collection would come from legal information mining, such as the internet and database purchases, and from market operations. “Data courier stations” would include, “e-commerce (platforms), Confucius Institutes, telecoms, transportation companies, or chain hotels, financial payment institutions and logistics companies.”³²

The CCP’s development of the ‘social credit’ system is another step in the Party’s long exploration of ways to fuse political control and economic prosperity. The expanding global reach of China’s economy means that social credit’s fusion of social and political control will also be used to bend entities outside China’s borders towards the Party’s political objectives. It might seem abstract, but last year dozens of international airlines, including four US airlines, recently discovered what this can mean in practice.

The Civil Aviation Administration of China (CAAC) sent dozens of international airlines letters demanding their websites be changed to show Taiwan as a part of the People’s Republic of China. The letter the CAAC sent to United Airlines was made public, it read:

[We] now request that your company, in accordance with the above requirements, complete the changes and submit the rectification report within 30 days from the date of this letter. If it is not corrected within this period, our bureau will take further measures according to the regulations, including on the basis of Article 8, Section 11 of the “Civil Aviation Industry Credit Management Measures (Trial Measures)”, and make a record of your company’s serious dishonesty and take disciplinary actions against your company in accordance with Chapter 3 of the Measures. At the same time, [we will] transfer your company’s violation of Chinese laws to the State Internet Information Office and other law enforcement agencies to take administrative penalties according to the law.

(权)” means both “right” and “power” in the law.“ See: Lu Wei. “经济全球化背景下的国家话语权与信息安全 (National Discourse Power and Information Security against the Background of Economic Globalization).” *People’s Daily*, 18 July 2010. <https://chinacopyrightandmedia.wordpress.com/2014/12/21/national-discourse-power-and-information-security-against-the-background-of-economic-globalization/>.

³¹ “陆钢：大数据时代下“一带一路”决策系统的构建 (Lu Gang: Construction of the One Belt, One Road Decision Making System in the Era of Big Data).” *People’s Daily* 8 July 2015. <http://cpc.people.com.cn/n/2015/0708/c191095-27273055.html>.

³² Ibid.

Unlike the majority of international airlines, four US carriers delayed implementing the changes until just before a deadline in late July.³³ The US airlines found a compromise and removed references to Taiwan, but did not add “People’s Republic of China/China” after the names of Taiwanese cities. This compromise was reached only after Chinese authorities rejected other efforts, including, for instance, a proposal for the airlines to create separate China-specific websites.

The CAAC used trial Civil Aviation Industry Credit Measures, written specifically to support the construction of China’s social credit system, to force airlines to comply with its political demands. The Civil Aviation Industry Credit Measures were written to implement the spirit of two key plans related to social credit, according to the first paragraph of the measures: the “Social Credit System Construction Planning Outline (2014-2020)” and the “Guiding Opinion from the State Council Relating to the Construction and Perfection of the System for Collective Encouragement of Honesty and Collective Punishment of Dishonesty, in order to Accelerate the Construction of Social Trust”. If the airlines did not accommodate the demands, their “act of serious dishonesty” for failing to comply would have been recorded on their credit records (according to Article 8, Section 11).³⁴

The social credit system is also extending to overseas Chinese. The MPS is developing a unified social credit code for overseas Chinese linked to their overseas Chinese code—for instance when an overseas Chinese national returns to China, his or her records would automatically be integrated with other identifying records attached to the social credit code, instead of those records being in multiple places the codes allow data to be more easily shared. Social credit codes are being developed for overseas Chinese federations, which would certainly include their China-based organizations and presumably extend to include their overseas branches.

Recommendations for U.S. Policy

The U.S. government must find short term solutions to the problems at hand but not at the expense of committing to long-term strategy for dealing with China’s tech enhanced authoritarianism. How precisely China’s tech-enhanced authoritarianism will evolve cannot be fully known, but the CCP’s objectives are known. These should be taken seriously as if the CCP might succeed. If there is one point you take away from my testimony, I hope it is that the U.S. government needs to quickly reframe the way it thinks about the Chinese Communist Party’s strategy secure and expand its power. If we cannot properly frame the issues, the debate will not move past false binary policy choices we are often presented with today, for instance, the idea that the only choices we have are cooperation or confrontation.

- [1] The U.S. must develop a long-term strategy for dealing with the CCP’s authoritarianism. Bipartisan consensus needs to move beyond the simple recognition that there is a problem in U.S.-China relations. A comprehensive and long-term strategy should not focus on national security alone. It should cover a wide range of domains not focused on national security alone, such as but not limited to the economy, technology, education, human rights protection.

³³ The four US airlines were Delta, American, United and Hawaiian.

³⁴ “关于印发《民航行业信用管理办法（试行）》的通知 (Civil Aviation Industry Credit Management Measures (Trial Measures)).” 7 November 2017.

- [2] Long-term strategy requires strengthening America's competitiveness. The United States must leverage the strengths and address the weaknesses of its own political, legal, economic and social systems. In foreign policy, this means that first and foremost the United States must also seek to improve, maintain, and respect long-standing alliances.
- [3] The U.S. government should use its existing regulatory toolkit to force U.S. businesses and research institutes to increase their risk calculus before becoming entangled in projects that put at risk civil liberties or long-term economic security or national security.
- [4] The U.S. government should review export controls on emerging technologies with respect to the CCP's tech-enhanced authoritarianism, and place organizations involved in tech-enabled human rights abuses on the entity list.
- [5] The Global Magnitsky Act should be used to hold companies and entities accountable for enabling the Chinese party-state's human rights violations.
- [6] The U.S. must strengthen its data privacy standards. A crucial step is to limit the way data can be exported, used and stored overseas.