# Written evidence supplementary to oral evidence on *Xinjiang detention camps*, HC 800, Tuesday 2 March 2021 submitted by Dr Radomir Tylecote (XIN0086)

## Introduction

The following written evidence is submitted with regard to my testimony to the Foreign Affairs Committee, in Oral evidence: Xinjiang detention camps, HC 800, Tuesday 2 March 2021.

In particular this was discussed in Q160:

Q160. Royston Smith: Dr Tylecote, did you want to add anything to that?

Dr Tylecote: Looking at this from a higher strategic level, some of the surveillance and facial recognition technologies we are describing, used in the wrong ways, have the ability to stunt the development of democracy, especially in developing countries, and harm civil society. For instance, where we see Chinese companies selling these surveillance systems to the police forces and Governments of some states in east Africa, these same technological systems appear to be used for the arrest of opposition activists. That makes clear what the dangers are, I'm afraid. In terms of what we can do about this, the first thing, as Dr Hoffman said, is to recognise and discuss the problem. Another possibility is to work through nascent associations, such as the G10 alliance of democracies, and the Commonwealth, with the United States, Five Eyes and so on, and to develop technological alternatives that various companies can purchase. We are really only at the start of recognising this problem. The first issue is to ensure that our own trade and procurement policies in the UK do not make it worse, by funding and helping the development of the corporates in question. I should be happy to provide in written evidence to the Committee further detail on the sort of purchases that I described in east Africa.

https://committees.parliament.uk/oralevidence/1768/pdf/

## Written evidence submission

The following information is adapted from my August 2020 paper with Robert Clark for the think tank Civitas, entitled *A Long March through the Institutions: Understanding and responding to China's Influence in international organisations.* Please consult this paper for full citations.

https://www.civitas.org.uk/content/files/A-Long-March.pdf

## Outline

China is pursuing a 'Sinocisation' strategy for international technology standards, which Beijing increasingly sees as 'strategic weapons'. This includes standards facilitating state control of the internet and facial recognition, which it aims to propagate through Belt and Road initiative (BRI) infrastructure.

In 2020, it also became clear that China's tactics in one standards-setting organisation (SSO) may fundamentally alter the way the internet functions, where its firms' proposed 'New IP' aims for granular control over citizens' net use, or a new 'authoritarian web architecture'. This has been described as a 'battle' for the future of the internet.

Beijing now appears to be promulgating the adoption of technical standards in the interests of its own (often state-owned) firms, which risks creating technological 'path dependency' around these companies to the detriment of their foreign competitors. This may become an impediment to growth through reducing incentives to innovate elsewhere; given these Chinese firms' links to their government, and their involvement in areas such as surveillance and facial recognition, it may also become a concern for political freedoms and sovereign polities themselves.

## The international standards institutions

Standards play a crucial role in economies and regulatory systems, demonstrating that a product meets a jurisdiction's performance or safety regulations. They are also vital to the international integration of markets.

In one recent definition: 'Technical standards are the definition of processes [or] specifications designed to improve the quality, security, and compatibility of various goods and services, for instance GSM for telecommunications or WiFi for wireless internet. They can be thought of as basic specifications or technologies on which other technologies or methods will evolve – creating lock-in effects and path-dependency for future products and technological trajectories. Defining standards [carries] significant implications for which technologies will dominate future markets' (Seaman, 2020). There is therefore some truth to the statement by Werner von Siemens in the late 1800s, that 'he who owns the standards, owns the market' (Seaman, 2020).

While some standards are voluntary, many are mandatory. Among these mandatory standards, some are determined on an entirely national level (or, within the EU, increasingly on a harmonised basis). However, many are agreed, or first agreed, in international technical-specialist standards organisations, in which China has become increasingly active. China's approach is two-fold:

• First, to pressure multinationals to use Chinese standards in China;

• Second, to 'Sinocise' international standards. This can be understood as part of a mercantilist trade policy whereby Chinese state resources are deployed to the benefit of

state-owned enterprises (SOEs) especially, in particular in higher-technology corporates and the sectors under its 'Made in China 2025' or 'Strategic Emerging Industries' strategies, to 'alter the competitive dynamics of global markets in industries essential to economic competitiveness' (US Chamber of Commerce, 2017).

On the domestic level, China's standards system is led by the Standardisation Administration of the People's Republic of China (SAC), under the State Administration for Market Regulation (SAMR), a branch of the State Council. SAC represents China at the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and other international organisations.

**Participation in international standards bodies relevant for surveillance technologies**

The Chinese government sees standards as a central component in competition, and sees becoming more influential in standards bodies as a priority, with increased participation in international SSOs. Chinese-led technical committees or subcommittees in the International Organization for Standardization (ISO), one of the largest, rose 75 percent between 2011 and 2019 (Fägersten and Rühlig, 2019). The next largest are the International Electrotechnical Commission (IEC), and the International Telecommunications Union (ITU). China's participation in all three has 'grown exponentially' in recent years (Seaman, 2020).

In 2015, Zhang Xiaogang was elected China's first President of the ISO (for a three-year term). Shu Yinbiao, Chairman of the China Huaneng Group, one of China's five largest state-owned electricity generation companies, was elected in 2019 as the IEC's President (the first among the Officers, and who is appointed by the Council). China also holds a rapidly growing number of ISO and IEC Secretariats.

One of the lessons China has taken from its experience in these organisations is the importance of first-mover advantage, especially from China's 2006 attempt to propagate its own WLAN Authentication and Privacy Infrastructure (WAPI) standard. China designed its own standard to close perceived security loopholes of the existing WiFi standard (ISO/IEC 8802-11 or IEEE 802.11) and to facilitate state oversight of wireless networks. However, an ISO Technical Review established that the two standards were competing and, because an international WiFi standard had already been established, China's WAPI could not be. This was an early example of China's strategy of attempting to permeate its own standards for state technological control.

China is now attempting first-mover advantage in another sphere, internet of things (IoT). As of 2019, of China's 11 proposed standards within the ISO/IEC framework, 5 have been adopted and published and 6 are being reviewed. Under Chinese leadership, the IEC has also begun coordinating standards for Global Energy Interconnection, a concept of China's State Grid Corporation for massive intercontinental smart grids. In facial recognition, in conjunction with a group of 27 Chinese firms who are developing national standards, the Chinese companies ZTE, China Telecom and Dahua appear to have been establishing positions at the ITU in facial recognition and other surveillance technologies (Seaman, 2020).

At the IEEE, Huawei, Tencent and Baidu all became active corporate members after around 2010, with seats in all major decision-making panels, while IEC President and State Grid Chairman Shu Yinbiao is an IEEE senior member. Huawei dedicates around fifteen percent of its revenues to standards (Seaman, 2020).

After a career in China's Ministry of Post and Telecommunications, Zhao Houlin was elected Secretary-General of the ITU in 2014. Under his leadership, the organisation has seen increasing cooperation with China and promoting China's BRI programme at global events. ITU Vice-Chair posts are now held by employees of the China Academy of Information and Communications Technology (CAICT), Alibaba, ZTE, Huawei, China Mobile and China Telecom.

China's ITU activity became clearer in 2019 in China's framing of facial recognition policies. Huawei, Hikvision, ZTE, Dahua, and China Telecom are involved in international standard-setting for these technologies, to the extent that Chinese firms have made every submission to the ITU on surveillance technology standards over the last three years (December 2019 data). Most submissions related to the storage and analysis of facial recognition data, where European and US submissions have been relatively light.

According to 2019 analysis by the Financial Times, 'one proposal [from] China Telecom and ZTE outlines how a surveillance system can trigger alarms and automatically "deploy personnel" if conditions set by its user are met.' ITU delegates state that China now uses the large corporate membership of its delegations to push through standards. A UK delegate stated: 'I've sat in the room and watched half of a delegation say they don't agree, and [a standard] has passed anyway', describing one 2017 meeting in which Chinese companies made 24 sequential proposals on the surveillance of individuals within cities. The delegate stated that China '[uses] volume of contributions [so] that it's difficult for meetings not to reflect theirs as a dominant view.' (Financial Times, 2019)

The BRI also incorporates infrastructure intended to feature facial recognition technologies, including for African and Asian countries. Chinese firms already provide AI surveillance technologies to 63 countries (Huawei alone supplies 50 countries, by far the world's largest supplier). Analysts find that without their own standards organisations, developing countries often follow the standards set at international organisations, the ITU included.

In March 2020, it became apparent that Chinese strategy at the ITU included a more radical tactic that could fundamentally alter the way the internet functions. With China's Ministry of Industry and Information Technology (MIIT), Huawei, China Unicom and China Telecom proposed a new core network technology standard called 'New IP', which scholars have stated threatens to create granular control over citizens' internet use, describing a new 'authoritarian architecture' for the web (Oxford Innovation working paper 2020, in Financial Times, 2019).

**Impact to date in developing countries**

Beijing's exports to BRI partner states, including through the Digital Silk Road, create challenges for the freedom and openness of internet use in the developing world, including in states with fragile democratic institutions.

Tanzania's May 2018 Electronic and Postal Communications (Online Content) Regulations force content creators to pay around two million Tanzanian shillings ($930) to a central register (Tanzania's per capita GDP is $879). A few months before the bill was introduced, the Cyberspace Administration of China chaired meetings with Tanzania's Deputy Minister for Communications, to discuss collaboration on social media censorship.

Despite less than 1 percent of Ethiopia's population having mobile internet access at the time, in 2013 Addis Ababa signed an $800m deal for China's telecom giant ZTE to help modernise state telecommunications infrastructure, widely acknowledged to strengthen the Ethiopian government's internet censorship capacity. In 2017 Ethiopia used a state of emergency to intermittently ban social media platforms including WhatsApp, Twitter, and Facebook. In Uganda, the Chinese state-owned company China National Electronics Import & Export Corporation (CEIEC) was awarded a deal to 'build the capacity' of the Communications Commission, Police, and the Ministry of Internal Affairs.

**Proposals**

Domestically, the UK should assess those companies active in pursuing a technological agenda that diverges from the UK's and that are implicated in the development of cyber technologies, mass surveillance, and facial recognition technologies, to the extent that these pose threats to UK security and civil liberties elsewhere.

The UK should act in concert with the US and willing Commonwealth partners, and potentially others, in a 'strategic planning group' to form common positions, and put forward more candidates for positions in the organisations discussed (proposed centrally by the UK government itself). The UK should also use this group to be more vocal about abuses. Related UK membership – and funding – of the Asian Infrastructure Investment Bank (AIIB) should cease.

Failure to take action is likely to lead to technological 'lock-in' around Chinese technologies and standards, which, as the analysis of internet and facial recognition standards has demonstrated, implies grave consequences for innovation, wealth generation, and civil liberties.

***8th March 2021***