JANUARY 2021

BRIEF

CHINA'S TECHNOLOGICAL RISE

IMPLICATIONS FOR GLOBAL SECURITY AND THE CASE OF NUCTECH

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

EESTI VÄLISPOLIITIKA INSTITUUT
ESTONIAN FOREIGN POLICY INSTITUTE

DIDI KIRSTEN TATLOW

China under the Chinese Communist Party (CCP) is poised to become the world's first technology-enabled totalitarian superpower. No country will be untouched by this development, including Estonia, where a Chinese state-owned technology company Nuctech specialising in "security solutions" monitors cargo crossing the NATO border with Russia using a radiation-based technology originally copied from Europe. The United States added Nuctech to its "Entity List" in December 2020, due to a range of security concerns.[1]

BECOMING A TECHNOLOGICAL POWERHOUSE

Nuctech (derived from "nuclear technology") sells widely in Europe and is one of many examples around the world of Chinese technology companies establishing a prominent presence in the open markets of democratic countries. It is a remarkable development: 40 years ago, in 1979, when post-Mao Zedong economic reforms began, China was one of the poorest countries in the world with a GDP of just $178 billion, for 970 million people. By 2019, GDP had soared to $14.3 trillion.

Especially since joining the WTO in 2001, China has produced a clutch of technology "national champions" that have quickly come to dominate life at home, and sometimes markets abroad, such as Huawei, ZTE, Datang, Tencent, Baidu, Alibaba, iFlytek and Nuctech. On its website, Nuctech says it has an "abundant product line" in public security; its parent company works with the People's Liberation Army (PLA). Repression of Uighurs, Tibetans, Mongolians and other groups in China is carried out in the name of "public security". In 2019, Nuctech announced a R&D partnership with St Petersburg State University in Russia to develop high-energy X-ray imaging technology, anti-terrorism equipment, and other technologies, all with potential for "public security" and military use.

There are several reasons for this extraordinary transformation in China. The ambition and hard work of the Chinese people is a well-known factor. But another very important one is less known because it is extremely sensitive and difficult to deal with: decades-old, large-scale, deliberate, "grey zone" technology extraction by the CCP from the world's developed economies, including but not limited to the US, Canada, Europe (principally Germany, France and the UK), Japan and South Korea.

Decades-old, large-scale, deliberate, "grey zone" technology extraction by the CCP from the world's developed economies, including but not limited to the US, Canada, Europe (principally Germany, France and the UK), Japan and South Korea

THE CHINESE SYSTEM OF TECHNOLOGY TRANSFER

This technology transfer is carried out "by many ways and means", as Chinese officials put it.[2] The phrase is deliberately ambiguous. It encompasses a range of legal, illegal and semi-legal (grey zone) activities. These include a meticulous system of open-source technology spotting carried out in multiple ways, including from research publications and PhDs around the world, knowledge transfer by tasking students going overseas to pursue certain technologies,

offering global scientists the chance to "double-dip" by taking up parallel, well-paid positions in Chinese institutions, company acquisitions overseas, venture capital funding of technology companies, and cyber and human espionage. One human example of this complex, multilayered process is "encouraging" Chinese scientists overseas to return home with their acquired skills to "repay the motherland" and "serve the country". State-run "talent plans" offering people the chance to earn more by bringing their knowledge and technology to China are another. There are probably over 200 of these, of which the best-known is the "Thousand Talents" plan, set up in 2008 and expanded to include non-Chinese in 2011. This may be illegal if the overseas scientist is the recipient of state money for research funding in the country where they live.

A clear understanding of the Chinese political system shows why there is fundamental cause for concern in all this, and why Chinese technology should not be viewed as politically neutral

Current laws in democracies, which promote open research environments and information sharing, are broadly unable to cope with most of this behaviour, partly because it is the product of an unusual, and globally unique, political and state technological system. In addition, while some of the practices may be normal—such as venture capital funding—implementing them with state- or military-building goals in mind may be less common.

According to a new book, "Since 1949, a vast, deliberate and unique system of foreign technology spotting and transfer has operated in China and overseas. Very little of it is secret. The projects are described in party and state documents, announced in the media, and executed in venues that are, broadly speaking, not hidden from the outside world".[3] They may not be hidden, but they are mostly written in Chinese.

More Modern, But Less Liberal

Two important steps have followed from this extraction, pushing China's economy to apparently ever-growing heights. The first is commercialisation at home accompanied by prompt and wide application; the second is growing indigenous innovation resulting from the transfer.

A clear understanding of the Chinese political system shows why there is fundamental cause for concern in all this, and why Chinese technology should not be viewed as politically neutral. All power in China belongs to the CCP. The country's system of "people's democratic dictatorship" is enshrined in Article 1 of the constitution, as well as being a practical reality since the seizure of power through revolution in 1949. Article 1 states, "The socialist system is the fundamental system of the People's Republic of China. Leadership by the Communist Party of China is the defining feature of socialism with Chinese characteristics. It is prohibited for any organisation or individual to damage the socialist system".[4] Article 2 adds, "All power in the People's Republic of China belongs to the people".[5] This is a closed circle of power with the CCP at its core.

Once completely state-controlled, China's economy remains state-driven, even among the new technology national champions. In one example, a report in 2019 assessed the total amount of government support received by Huawei Technologies Co. at $75 billion in grants, credit facilities, tax breaks and other forms of financial assistance.[6] The private economy is also influenced, and manipulated, by the state, with Xi Jinping, the CCP general secretary and Chinese leader, recently reminding private companies and entrepreneurs they must support and strengthen the party and country with their business. In September 2020, the General Office of the CCP Central Committee issued an "opinion" and a "notice" (these words in Chinese should be understood as instructions) that made clear the CCP intends to manage ever more tightly the nominally private economy sector, using its established united front strategy and the organs of the United Front Work Department, a department under the Central Committee of the Politburo. The notice is titled "Concerning the strengthening of united front work in the private economy in the New Era".[7] It instructs party committees "at all levels" and the party's united front organisations to ensure that the private economy—or the "non-state

economy", as it is often called—is "patriotic" and "in the party's orbit", "support[s] the party fully" and works towards the CCP's goal of "national rejuvenation" by 2049, when it plans for China to become the dominant technological, economic and military power in the world.

Troublingly, China's political system lacks the checks and balances of democratic societies that—ideally—work to keep technology safe for individuals. While the situation in democracies is not perfect, established separation of powers and independent judiciaries offer the possibility that technology will work for the human good, not to its detriment. In the words of Taiwan's Digital Minister, Audrey Tang, artificial intelligence (AI) should in future mean "assisted intelligence" for humans, not "authoritarian intelligence" for governments.[8] In China today, technology is widely used throughout society via surveillance and "social credit schemes" to manipulate human behaviour and support the party's power. Many reports show the impact on Chinese citizens of these technologies.[9] Overall, a tightening concentration of power enables party leadership to skew technology to support its survival.[10] That Chinese technologies—networked, cloud-based, communicating and monitoring—are spreading among overseas populations as China's economy grows ever outward creates potentially unmanageable risks for individuals there too.[11] Today, in a historical irony, China is in a position to challenge for global leadership the countries whence the technologies it has extracted came.

While the situation in democracies is not perfect, established separation of powers and independent judiciaries offer the possibility that technology will work for the human good, not to its detriment

Nuctech in Narva

An excellent example of this creep is Nuctech, operating on the Estonian—and NATO—border with Russia in Narva, scanning cargo passing between Estonia and its eastern neighbour. The company was set up in 1997 at Tsinghua University in Beijing.[12] Hu Haifeng—the son of a former general secretary of the CCP, Hu Jintao (the predecessor of Xi Jinping)—was prominent in the company in its early years before following in his father's footsteps by entering politics. Today Hu Haifeng is party secretary of Lishui, a city in Zhejiang province.[13]

In May 2018, Chinese diplomats formally delivered the large, Nuctech-made, X-ray scanning system to the Estonian customs authorities, the first "fully-automatic railway scanner" in Estonia, according to Xinhua, the Chinese state news agency. Similar deliveries had already been made to Estonia and other Baltic nations – more are under consideration, including for airports for example in Lithuania.[14] The aim of the railway scanner: to "crack down on smuggling and maintain national security", the Chinese ambassador, Li Chao, said at the ceremony.[15] This is what Tsinghua Tongfang, Nuctech's parent company, says about Nuctech's "customs container inspection comprehensive solutions":

> By using information telecommunication technology and Internet platform, Nuctech Co Ltd integrates the cloud computing, big data and Internet of Things with safety inspection technologies and products to supply the clients with hi-tech safety inspection solution. With intelligent inspection, automatic data collection and analysis, and product integration connectivity, the solution assists in anti-terrorism and fighting against illegal trades. It is widely used in various fields, such as civil aviation, customs, railways and big events in over 140 countries and regions.[16]

Estonian customs said the Chinese state-owned company won the contract due to its "favourable price and the provision of full maintenance and guarantee for ten years". It added that "the purchase of the equipment was financed in the amount of €2.55 million by the European Union Cohesion Fund and in the amount of €7.55 million by the state budget".[17]

Nuctech's price was indeed low—€10.1 million, about one-third cheaper than its competitors, Rapiscan Systems (€14.9 million) and L3Harris (€15.9 million), according to a spokeswoman for Estonian customs.

Yet it is perhaps curious that Nuctech's parent company has been in so much financial trouble that in early 2020 it was formally taken over by the asset management wing of China National Nuclear Corporation (CNNC). CNNC belongs to the State-owned Assets Supervision and

Administration Commission of the State Council of China (SASAC), and thus is one of the "crown jewels" of the state. The move undoubtedly reflects the priority the Chinese state accords to Tsinghua Tongfang and Nuctech itself, one of the profitable companies in Tsinghua Tongfang's stable, according to the company's 2018 report.

State-sponsored Foreign Aid Work in Politically Sensitive Regions

Nuctech sells and operates cargo- and people-scanning systems around the world and has won security contracts for major sporting events such as the Summer Olympics in Rio de Janeiro (2016), the Wimbledon tennis championships, the Milan Expo (2015) and the Military World Games held in 2019 in Wuhan, China. The company says it contributes to China's "national security", as well as its "national military strategy of border construction". Tsinghua Tongfang runs large data storage banks (大数据库) and provides technology and maintenance for the PLA, as well as technologies such as RFID cards. These capabilities are part of growing population surveillance systems being built by the state in China and—via "smart cities" using, for example, Huawei technology—around the world, too.

Nuctech has donated, or offered cheap loans for, its equipment in politically sensitive regions such as Serbia and the western Balkans.[18] During a visit to Nuctech company headquarters in Beijing by Ministry of Commerce officials in August 2019, its senior vice president, Miao Qitian, made clear the connection between Nuctech's commercial ventures (it has a factory in Poland, which supplied the Baltic equipment) and China's state-sponsored foreign aid work. (In Chinese the company is known as "Tongfang Weishi".) Miao said:

> Foreign aid projects are of profound and far-reaching importance to Tongfang Weishi's expansion in the international market, its effort for Chinese manufacturing to "go global", and to spread Chinese culture. Tonfgang Weishi acts on the orders of "supporting science and technology to make the world a safer place". Tongfang Weishi is a bright and beautiful calling card for China's foreign aid work, it is a vanguard example of foreign aid work that helps Chinese companies globalize.[19]

Nuctech has donated, or offered cheap loans for, its equipment in politically sensitive regions such as Serbia and the western Balkans

In late 2017, not long before the Nuctech's new scanner arrived in Narva, the company set up a new CCP committee. At its first meeting, on Dec. 28 of that year, Zhou Liye, the party secretary of Tsinghua Tongfang, congratulated Nuctech on the step, and noted new "hopes and expectations" for the company which included, "seriously implement the spirit of the party's 19th Congress [held in Oct. 2017], clearly support the party leadership and party-building … continuously push forward and develop Nuctech's party-building and business activities".[20] Since coming to power in 2012, Xi Jinping has pushed the development of a Chinese "national security state", with the CCP making renewed inroads into society.[21]

The U.S. is concerned about the security implications of Nuctech operating at sensitive border crossings (including ports, airports and railways and roads), as well as other surveillance functions. Yet there is an additional aspect that led directly to its placement on the U.S. Entity List in December 2020: nuclear smuggling. After tests by the U.S. Department of Energy, it decided "Nuctech's lower performing equipment impair U.S. efforts to counter illicit international trafficking in nuclear and other radioactive materials. Lower performing equipment means less stringent cargo screening, raising the risk of proliferation".[22]

Given all that, it seems almost an afterthought that Nuctech was founded following an act of copying: scientists at Tsinghua University were ordered by the government to develop the radiation-based scanning equipment that had just begun operating in Europe and created by French, German and British companies. So says a Chinese-language book published by Tsinghua University Press that describes the creation of the high-grade equipment, and multiple Chinese-langue media reports. The story is given in more detail in *China's Quest for Foreign Technology: Beyond Espionage*.

But certainly, the early act of copying, followed by secondary invention (the engineers adapted the technology to make it mobile in order to suit conditions in often crowded Chinese ports, something that has proved popular everywhere), demonstrates how CCP-run China has grown so fast, and come so far—to the point where it challenges the world for political and technological leadership in ways that could change our lives, if we let it.

Endotes

[1] The U.S. Department of Commerce's Entity List consists of "businesses, research institutions, government and private organizations, individuals, and other types of legal persons" seen as acting contrary to the national security or foreign policy interests of the United States. These are subject to specific license requirements for the export, reexport, or transfer of specified items. See "Entity List," Bureau of Industry and Security, U.S. Department of Commerce; U.S. Department of Commerce, Bureau of Industry and Security, "Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities From the Entity List," *Federal Register*, Vol. 85, Issue 246, 22 December 2020, 83416-31.
[2] "以多种途径和形式"or "以多种方式".
[3] William C. Hannas and Didi Kirsten Tatlow (eds), *China's Quest for Foreign Technology: Beyond Espionage* (London: Routledge, 2021).
[4] *Constitution of the People's Republic of China*, updated 20 November 2019 (Beijing: The State Council, The People's Republic of China).
[5] Ibid.
[6] Chuin-Wei Yap, "State Support Helped Fuel China's Rise", *The Wall Street Journal*, 25 December 2019.
[7] "中共中央办公厅印发,'关于加强新时代民营经济统战工作的意见'" (General Office of the CCP Central Committee issued an opinion, "Concerning the strengthening of united front work in the private economy in the New Era"), *Xinhua*, 15 September 2020.
[8] "Conversation on Technological Change and its Implications, with Audrey Tang, Digital Minister, Taiwan (videoconference)," IFRI online seminar, 2 December 2020.
[9] "China: Big Data Program Targets China's Muslims," Human Rights Watch, 9 December 2020; see also "How Mass Surveillance Works in Xinjiang, China," Human Rights Watch, 2 May 2019.
[10] Hannas and Tatlow, op. cit.
[11] Read more about Chinese surveillance technology's growing presence around the globe from: Kelsey Munro and Lin Li, "Should Australia be buying border security technology from Nuctech?," *The Strategist*, Australian Strategic Policy Institute, 17 December 2020.
[12] "About Us", Nuctech, accessed 17 December 2020.
[13] Following corruption allegations in Africa, Chinese-language references to Hu Haifeng's role in the company were taken down from the internet. For an English-language reference from that time see: Marius Bosch, "Namibia graft body wants to interview son of Hu Jintao," *Reuters*, 24 July 2009; More recently: Brian Platt, "Security scanners from a Chinese firm not the best plan for our embassies, government decides," *National Post*, 19 November 2020; Xu Wenyan ,Ye Ruisheng, "丽水市委书记和政协委员研讨协商民主文化" (Lishui Party Secretary and CPPCC members talk about consultative democratic culture), Zhejiang Provincial Committee of the Chinese People's Political Consultative Conference, 3 November 2020.
[14] Lithuanian commission launches review of Chinese bidder for airport equipment contract, *The Baltic Times*, 4 December 2020.
[15] Shi Yinglun (ed.), "First full-automatic railway scanner to enhance Estonian customs capacity," *Xinhua*, 1 June 2018.
[16] "Customs container inspection comprehensive solution (Nuctech Co Ltd)," Tsinghua Holdings.
[17] Kaia-Liisa Kallas, "Narva Railway Border Crossing Point got a new X-ray equipment," Republic of Estonia Tax and Customs Board, 31 May 2018.
[18] "Serbia, China sign MoU for customs scanners," Chinese Embassy in Serbia, 22 September 2009.
[19] "肖凤怀副主任率组赴同方威视技术股份有限公司开展"不忘初心、牢记使命"主题教育调研活动" (Deputy chairman Xiao Fenghuai leads a group to research Tongfang Weishi Technology Co., Ltd.'s educational activity on the theme of 'Don't forget your original heart and remember your mission'), Ministry of Commerce, People's Republic of China, 13 August 2019.
[20] "同方威视第一次党代会取得圆满成功" (The first meeting of the Tongfang Weishi party committee achieved full success), Tsinghua Tongfang News Center, 4 January 2018.
[21] Tai Ming Cheung, "The Chinese National Security State Emerges from the Shadows to Center Stage," *China Leadership Monitor*, Fall 2020, Issue 65, 1 September 2020.
[22] U.S. Department of Commerce, "Addition of Entities to the Entity List," 83417.

About the Author

Didi Kirsten Tatlow

Didi Kirsten Tatlow is Senior Fellow of the Asia Program at the German Council on Foreign relations in Berlin, Germany, and Senior Non-resident Fellow at Project Sinopsis in Prague, Czechia.

ICDS.Tallinn
@ICDS_Tallinn
ICDS-Tallinn
www.icds.ee
EVI.EESTI
@EFPI_EST

International Centre for Defence and Security
Estonian Foreign Policy Institute
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee

ISSN 2228-2076