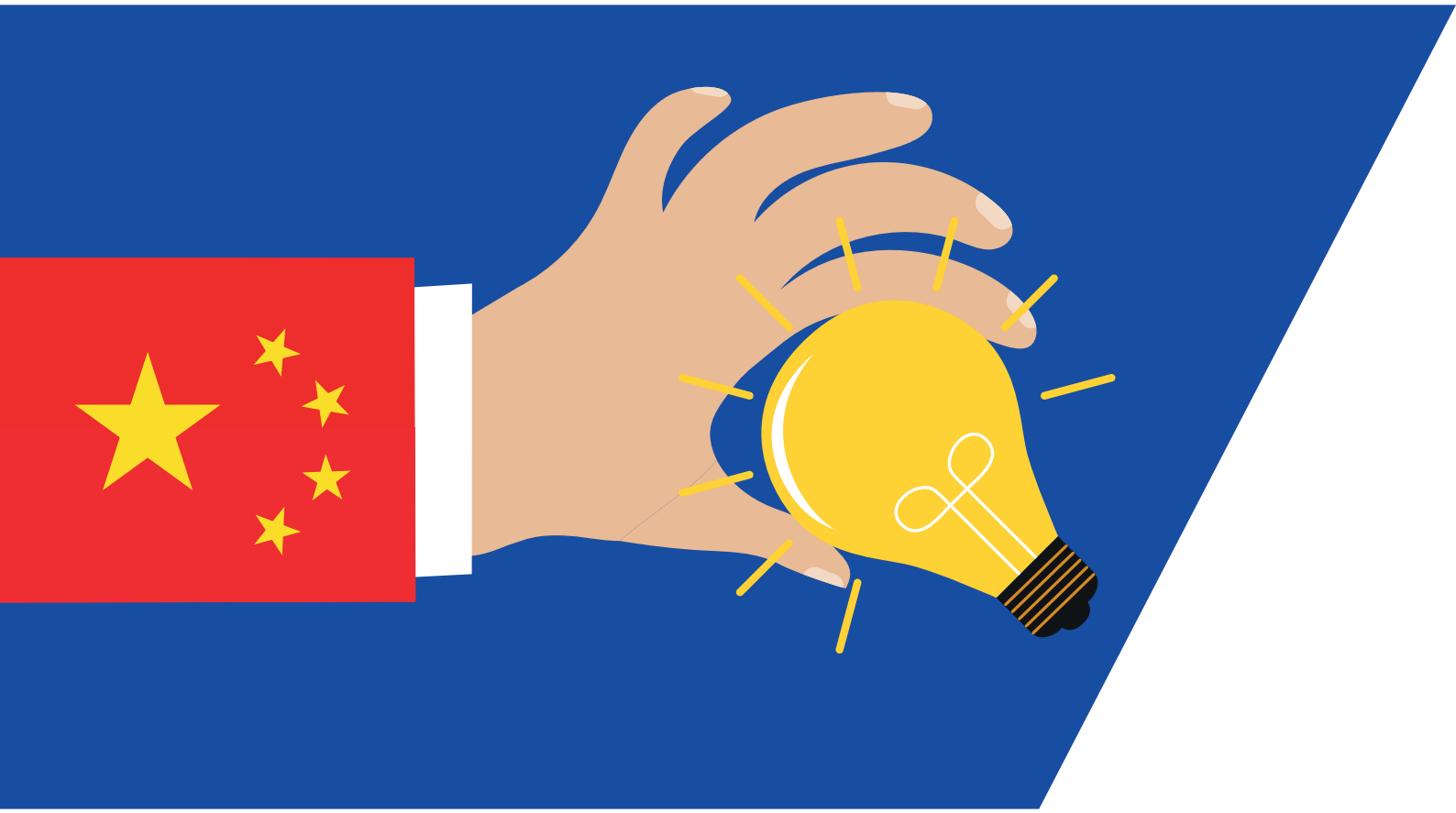
BRAIN DRAIN: THE UK, CHINA AND THE QUESTION OF INTELLECTUAL PROPERTY THEFT

BY SAM ARMSTRONG



HJS Henry Jackson Society

ASIA STUDIES CENTRE

DEMOCRACY | FREEDOM | HUMAN RIGHTS

September 2020

Published in 2020 by The Henry Jackson Society

The Henry Jackson Society
Millbank Tower
21-24 Millbank
London SW1P 4QP

Registered charity no. 1140489
Tel: +44 (0)20 7340 4520

www.henryjacksonsociety.org

Title: “BRAIN DRAIN: THE UK, CHINA AND THE QUESTION OF INTELLECTUAL PROPERTY THEFT”
Author: Sam Armstrong

ISBN: 978-1-909035-59-1

£20.00 where sold

BRAIN DRAIN: THE UK, CHINA AND THE QUESTION OF INTELLECTUAL PROPERTY THEFT

BY SAM ARMSTRONG

HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

ASIA
STUDIES
CENTRE

September 2020

About the Author

Sam Armstrong is the Director of Communications for the Henry Jackson Society, having joined HJS in August 2018.

Prior to joining the Society, Sam worked as Chief of Staff to a Conservative Member of Parliament. Before this, he worked in the Conservative Party's anti-UKIP division. Sam holds a degree in History and Politics from the University of Nottingham. He has repeatedly written on the challenges posed by the Chinese Communist Party, having previously co-authored two HJS reports on the topic (*Coronavirus Compensation?* and *Breaking the China Supply Chain*)

Sam also coordinates the strategy and communications of the Inter-Parliamentary Alliance on China, the global alliance of bipartisan parliamentarians concerned about the Peoples' Republic of China's conduct. He's often asked to advise legislators around the world on policy responses to the CCP.

Acknowledgments

The author is grateful to a very large number of people without whom this report would not have been possible.

Firstly, to a number of research assistants whose work was invaluable to the entire project but particularly to Chapter 4. They are Alexander Brookes, Carmen Ghazi, Daniel Klein, Max Klinger, Andrew Mahon, William McGee, and Sophie Poll. They each approached the task with an austere rigour as well as an admirable sense of patience and good humour. The work of Matthew Henderson and his team of research assistants, in Daniel Rossall-Evans and Alex Johnson, were essential to Chapter 2.

Secondly, to the large number of academics and experts who peer-reviewed the script and suggested essential and major edits. Particular thanks go to Craig Tiedman, Dan Cadman, and three other individuals who requested anonymity due to their role.

Thanks are also due to Kajol Kochar who arranged the production of this paper in impressively short order as well as to HJS's suppliers for facilitating this tight turnaround. A particular thanks is due to this paper's legal reviewer, Roger Field, whose studious pre-publication advice was gratefully received.

This project would not have been possible without the cutting-edge scholarship of the Australian Strategic Policy Institute. In particular, this project is very reliant on the work of Alex Joske in the China Defence Universities Tracker, whose work is more than worthy of the large amount of global attention that it has received.

Lastly, grateful thanks go to Dr Alan Mendoza who has shown great faith in this, ostensibly niche, interest of the author from the outset.

Contents

About Us

HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

About The Henry Jackson Society

The Henry Jackson Society is a think-tank and policy-shaping force that fights for the principles and alliances which keep societies free, working across borders and party lines to combat extremism, advance democracy and real human rights, and make a stand in an increasingly uncertain world.

ASIA
STUDIES
CENTRE

About The Asia Studies Centre

The Asia Studies Centre is a research centre within the Henry Jackson Society that aims to educate the public about the structural shifts, regional complexities and historic tensions that exist alongside the economic and social growth that constitutes the "rise of Asia". It also advocates a British role in the broader Indo-Pacific region, commensurate with Britain's role as a custodian of the rules-based international system.

1. Introduction

The United Kingdom (UK) is belatedly waking up to the broad gambit of threats posed by the People's Republic of China (PRC). The Chinese Communist Party (CCP) uses influence and infiltration operations against its adversaries, including the UK. These operations include the deployment of tactics that fall short of traditional armed conflict in an effort to overtake the West and become the world's foremost power. Central to its efforts is the theft and drainage of intellectual property (IP).

In its 2017 updated report, the United States-based independent and bipartisan Commission on the Theft of American Intellectual Property (IP Commission) estimated that IP theft cost the United States (US) economy anywhere between $225 and $600 billion annually. [1] This figure is equivalent to 1.3% to 3% of the Gross Domestic Product (GDP) of the US. In contextual terms, were the economic cost of IP theft to be commensurate with a nation's GDP, it would mean the cost to the UK of IP theft is in the region of $34 billion (£23 billion) to $82 billion (£61 billion). Comparably, in 2016–17, the UK spent just £46 billion on its entire defence budget, £29 billion on transport, and £24 billion on industry, agriculture and employment. [2]

In its report, the IP Commission was clear as to where the blame lay, stating unequivocally that China is "the world's principal IP infringer." [3] The rapid acquisition of intellectual property is central to both the CCP's 'Military-Civil Fusion' (MCF) doctrine and its "Made in China 2025" strategy. [4] Like the US, the UK is a target for this activity. In December 2018, the National Cyber Security Centre (NCSC) announced that a group of Chinese hackers "known as APT10 acted on behalf of the Chinese Ministry of State Security [MSS] to carry out a malicious cyber campaign targeting intellectual property" in the UK. [5] In its advisory note, the NCSC revealed that the UK was a "significant" target of APT10. [6]

The APT10 campaign targeted a diverse range of entities, including companies, government bodies, non-governmental organisations, and educational institutions. Far from being the exception, such diversity is the norm. In the US, where a series of indictments for IP-related crime have been brought over recent years, targets have varied in sector, structure, and nature. Of these targets, however, universities stand out as a particularly frequent focus. In the first nine months of 2020, 14 individuals at US universities have been indicted over charges connected to foreign interference.

British universities themselves acknowledge the existence of this risk. In a 2018 submission to the House of Commons' Foreign Affairs Select Committee (FASC), Universities UK (the representative body for British universities) said its "working assumption is that the most

1 'Update to the IP Commission Report; The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy', The Commission on the Theft of American Intellectual Property (2017), available at: ipcommission.org/report/IP_Commission_Report_Update_2017.pdf , last visited: 2 September 2020, p.1.

2 'Budget 2016', HM Treasury and The Rt Hon George Osborne (2016), available at: assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/508193/HMT_Budget_2016_Web_Accessible.pdf, last visited: 2 September 2020, p.5.

3 'Update to the IP Commission Report; The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy', The Commission on the Theft of American Intellectual Property (2017), p.2.

4 '"Made in China 2025" Industrial Policies: Issues for Congress', Congressional Research Service (2020), available at: fas.org/sgp/crs/row/IF10964.pdf, last visited 2 September 2020; 'Military-Civil Fusion and the People's Republic of China', *US Department of State* (2020), available at: www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf, last visited: 2 September 2020.

5 'UK and allies reveal global scale of Chinese cyber campaign', Foreign and Commonwealth Office, National Cyber Security Centre and the RT Hon Jeremy Hunt MP, 20 December 2018, available at: www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign, last visited: 2 September 2020.

6 'APT10 continuing to target UK organisations', *National Cyber Security Centre*, 20 December 2018, available at: www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations, last visited: 2 September 2020.

significant threat from hostile state actors is misappropriation of research output, including the seizing of research data and intellectual property." [7] Speaking in January 2019 in response to news that Oxford University was suspending new investments from Chinese technology companies given concerns that they might constitute a spying threat, the Chairman of the FASC, Tom Tugendhat MP, said that Oxford was "right to be concerned about the issue" of IP theft. [8]

Universities are, by their very nature, engaged in large quantities of original research, including within many of the areas most attractive to the Chinese State. Her Majesty's Government (HMG) has published detailed advice for the university sector on how to abate the risk of IP theft. The guidance, called 'Trusted Research' (TR), covers, in broad terms, four key themes of risk: cyber-hacking, human-conducted theft, research partnerships, and the admission of overseas individuals. Of these, cyber-hacking and more conventional theft are – as a matter of law – already criminal offences in almost all circumstances.

However, research partnerships and the enrolment of overseas-nationals are – in the majority of cases – not merely lawful but, as the TR guidelines make clear, positively encouraged. [9] These forms of international academic engagement – as well as countless others, such as the recruitment of overseas academic staff – offer considerable benefit to British universities in both financial and academic terms. However, these benefits give rise to an obvious tension between the not-insubstantial advantages of international engagement and the very real security concerns that accompany it.

The bulk of advice provided by the TR guidance concerns research collaborations between British and overseas institutions at a corporate level. This matches much of the public debate in which detailed coverage has been afforded to relationships between Chinese-linked entities (particularly Huawei) and British universities or Confucius Institutes based within them. Far less attention has been afforded to security risks associated with foreign-national students and staff. In many ways, this is unsurprising. Until recently, no Western nation had a bespoke policy arrangement to preclude IP drainage by foreign-nationals at their respective universities. That changed in May 2020 when Donald Trump issued a Presidential Proclamation banning graduates of Chinese universities linked to the People's Liberation Army (PLA) from studying in the US. While, in February 2020, Christopher Wray, the Director of the Federal Bureau of Investigation (FBI), said that the CCP "use some Chinese students in the US as non-traditional collectors of our intellectual property." [10]

These events have thrown a sudden light on the security arrangements adopted by the allies of the US, including the UK. And on this issue, the UK is well behind the curve. The Academic Technology Approval Scheme (ATAS), the regulatory framework that is used to face the threat of IP theft, emerged from the Voluntary Vetting Scheme (VVS) which was created in the 1990s as a mechanism to prevent Saddam Hussein, the then dictator of Iraq, from acquiring expertise in the development and delivery of weapons of mass destruction (WMD). [11] Administered

[7] 'Written Evidence from Universities UK', *Parliament UK*, October 2019, available at: data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/foreign-affairs-committee/autocracies-and-uk-foreign-policy/written/106141.html, last visited: 2 September 2020.

[8] 'Oxford University 'right to be concerned' over China trade secrets theft, MP warns', *The Telegraph*, 18 January 2019, available at: https://www.telegraph.co.uk/technology/2019/01/18/oxford-university-right-concerned-china-trade-secrets-theft/, last visited: 2 September 2020.

[9] 'Trusted Research Guidance for Academics', *National Cyber Security Centre* (2020), available at: www.cpni.gov.uk/system/files/Trusted%20Research%20Guidance%20for%20Academia.pdf, last visited: 2 September 2020.

[10] Wray, C. 'Responding Effectively to the Chinese Economic Espionage Threat', Department of Justice China Initiative Conference, Center for Strategic and International Studies, 6 February 2020, available at: www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat, last visited: 2 September 2020.

[11] 'What is ATAS?', *Foreign and Commonwealth Office*, July 2009, available at: webarchive.nationalarchives.gov.uk/20090704101923/http://www.fco.gov.uk/en/fco-in-action/counter-terrorism/weapons/atas/atas-what/, last visited: 2 September 2020.

by the then Foreign and Commonwealth Office as a counter-proliferation policy, ATAS was designed to preclude the capture of a relatively narrow range of technologies by nationals from a relatively small number of countries. To this day, its formal mission is limited to preventing only the proliferation of WMDs and their means of delivery.

The challenge of IP theft, however, is much broader and more complex in nature. Driven by economic as well as military interests, the range of targeted technologies are far more diverse than those sought by previous strategic adversaries. Moreover, the MCF doctrine means potential acquirers of IP are drawn from a much wider range of backgrounds. The emergence of the Thousand Talents Program (TTP) in 2008 transformed IP theft into an industrial-scale problem. This begs the question of whether the UK's current frameworks are capable of managing the conflicting interests of the proper desire to encourage overseas students to study here and the need to mitigate the risk of IP drainage.

This paper argues that serious questions need to be asked about our existing mechanisms and frameworks of reference. Hundreds of Chinese students are presently studying in the UK whose risk profile is such that they would be barred from admission to the US under the May 2020 ban. A significant proportion of these students study the most sensitive subjects possible.Despite concerns having been raised repeatedly about the threat of IP theft, it is striking that no prosecutions have ever been brought for offences connected to the Intangible Transfer of Technology (ITT). While this paper does not for a moment seek to suggest that all, or even some, Chinese students in the UK are engaged in such activity – or that UK institutions are even unintentionally aiding such an eventuality – it does conclude that there are national security concerns inherent in current UK systems that need to be tightened up to mitigate risks that have already been pointed out.

In addressing this situation, the UK need not reinvent the wheel, however. One advantage of facing a common threat with its allies is that the UK can take elements of best practice from them. Doing so will not eliminate the threat of IP drainage. It will, however, give the security services a fighting chance in limiting its impact.

2. Why and How is China Acquiring Foreign Intellectual Property?

From a very low baseline only 30 years ago, China has swiftly emerged as a significant economic power with increasingly sophisticated instruments for regional – even global – power projection. [12] Despite the role of globalisation in China's spectacular rise, the country's emergence on the global scene owes less than meets the eye to following the norms of free trade and fair acquisition of new technology. From the outset of its engagement in world markets, the CCP has practised protectionism, undercut Western prices by subsidising Chinese exports, denied competitive reciprocity, and used every available means to acquire foreign technological innovation and knowhow as fast as possible and at minimum cost, including through stealing IP. [13]

2.1 Why is China Trying to Acquire IP?

Under Xi Jinping's authoritarian leadership, the CCP is gripped by the assumption that all components and instruments of national power are intrinsically entwined. Xi's ambition for China, set out in his 2017 address to the CCP's National Congress, is to reach parity with – or even surpass – the world's most advanced economies, and to use China's burgeoning industrial and technological base to challenge Western military supremacy. [14] It should not, therefore, come as a surprise that China has focused on developing current and emerging dual-use technologies. [15]

In 2015, three years after Xi's ascent to power, the CCP issued a strategic plan to upgrade China's capacity to manufacture high-value, technologically advanced goods. Entitled "Made in China 2025", this plan aims to transform China into a high-tech manufacturer, able not only to compete with the world's most advanced economies but even to surpass them. [16] As outlined by Li Keqiang, Premier of the PRC, this is a ten-year campaign that foresees China reorienting its economy away from low- and mid-level manufacturing and enabling it to become a "global high-tech manufacturing powerhouse". [17] To achieve this, the plan seeks domestic mastery of emerging technologies that would enable China to grow beyond middle-income status and enter some of the most lucrative global markets as a serious full-spectrum competitor.

To provide this advanced industrial and technological base, "Made in China 2025" identified nine key tasks. These are: improving manufacturing innovation; integrating technology and industry; strengthening the industrial base; fostering Chinese brands; enforcing green manufacturing; advancing restructuring of the manufacturing sector; promoting service-oriented manufacturing and manufacturing-related service industries; internationalising manufacturing; and, promoting breakthroughs in ten key industrial sectors. [18]

---

[12] Hynes, H. A., 'China: the Emerging Superpower', Federation of American Scientists, 1998, available at: fas.org/nuke/guide/china/doctrine/0046.htm, last visited: 21 August 2020.

[13] 'How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World', *White House Office of Trade and Manufacturing Policy* (2018), available at: www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf, last visited: 21 August 2020.

[14] 'Full text of Xi Jinping's report at 19th CPC National Congress', *Xinhua*, 3 November 2017, available at: www.xinhuanet.com/english/special/2017-11/03/c_136725942.htm, last visited: 21 August 2020.

[15] 'China stealing foreign military technology in race to become world power: Report', *ABC News*, available at: abcnews.go.com/Politics/china-stealing-foreign-military-technology-race-world-power/story?id=62785573, last visited: 21 August 2020.

[16] 'Made in China 2025: The making of a high-tech superpower and consequences for industrial countries', *MERICS*, 12 August 2016, available at: merics.org/en/report/made-china-2025, last visited: 21 August 2020.

[17] 'Made in China 2025: Manufacturers absorb foreign tech', *The State Council The People's Republic of China*, 22 May 2017, available at: http://english.www.gov.cn/news/video/2017/05/22/content_281475663872644.htm, last visited: 21 August 2020.

[18] '"Made in China 2025" plan issued', *The State Council of the People's Republic of China*, 19 May 2015, available at: english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm, last visited: 21 August 2020.

The ten key industrial sectors were identified as:

1. New information technology;
2. High-end numerically controlled machine tools and robots;
3. Aerospace equipment;
4. Ocean engineering equipment and high-end vessels;
5. High-end rail transportation equipment;
6. Energy-saving cars and new energy cars;
7. Electrical equipment;
8. Farming machines;
9. New materials, such as polymers;
10. Bio-medicine and high-end medical equipment. [19]

All of these sectors fit into what would be known as 'science, technology, engineering, and mathematics (STEM) subjects' in the UK and elsewhere. The majority of technologies related to these key sectors – in particular, new information technology, robots, aerospace equipment, and new materials – have dual-use or security-related applications, some of which have strategic importance. [20]

It should come as no surprise, then, that the CCP's strategy for economic modernisation dovetails with its ambition to modernise China's armed forces. With the strategy of Military-Civil Fusion (MCF), the CCP aims to integrate military-driven activity with civilian sectors such as industry, academia, and commerce. Defined around the time of Xi's emergence as paramount leader of the CCP, MCF is the most recent and dynamic iteration of a concept that has existed under varying names since the early days of the PRC. [21] The primacy of "military" in all versions of the strategy reflects the symbiotic relationship between the CCP and its armed forces, whose core function is to defend the party.

Under MCF, neither China's research infrastructure nor its military-industrial complex makes a clear demarcation between "military" and "civilian" expertise and enterprise – insofar as such a distinction can be made in a Marxist-Leninist state. Instead, MCF blurs this demarcation by leveraging all instruments of state and commercial power to strengthen and support the armed wing of the CCP, the People's Liberation Army (PLA). As such, MCF recognises and consolidates the importance of aggressive and defensive military objectives to every aspect of developing China's national interests. Crucially, this reflects the reality that in the PRC, all state-led activity at home and abroad is framed in terms of struggle and competition, conducted using all and any means that are expedient, and constrained by no universally accepted norms.

2.2 How is China acquiring intellectual property?

While the "Made in China 2025" strategy was clear in its ambition that China would become a "global high-tech manufacturing powerhouse" [22], it was less clear about how China would achieve this. Chinese state-media outlets often describe the benefits of absorbing foreign technology as "win-win exchanges", a term familiar from Xi's descriptions of the spirit behind his

[19] '"Made in China 2025" plan issued', *The State Council of the People's Republic of China*, 19 May 2015, available at: english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm, last visited: 21 August 2020.

[20] 'Made In China 2025: China Manufacturing in the 21st Century – Opportunities for UK-China Partnership', *China-Britain Business Council* (undated), available at: https://www.mta.org.uk/system/files/resource/downloads/Made%20in%20China%202025%20Booklet%20One.pdf, last visited: 21 August 2020.

[21] Hannas, W. C. and Tatlow, D.K., *China's Quest for Foreign Technology* (Oxford: Routledge, 2020), p.5.

[22] 'Made in China 2025: Manufacturers absorb foreign tech', *The State Council The People's Republic of China*, 22 May 2017, available at: http://english.www.gov.cn/news/video/2017/05/22/content_281475663872644.htm, last visited: 21 August 2020.

Belt and Road Initiative.[23] However, this drive to achieve superiority has intensified PRC efforts to force technology transfer and steal IP.[24] China now aggressively drains foreign Research and Development at source, before replicating and adapting it so that Chinese manufacturers can produce, use and market indigenous applications capable of out-performing foreign competition.[25]

Despite recent advances, particularly in the telecommunications sector, China's scientific, research and technological base still trails behind that of the world's most advanced economies, such as the US, UK, Japan and Germany. For this reason, the CCP has set about appropriating, by hook or by crook, foreign IP in an attempt to catch up. Indeed, the US Department of State has accused the PLA of using MCF to justify IP theft, unfair business practices, and unethical research in pursuit of China's efforts to become the first state to master "intelligent warfare".[26]

Some of China's efforts to gain command of Western dual-use IP and knowhow are directed at sensitive strategic targets. Methods used include elaborate human and technical espionage operations. In the US, a human espionage operation exposed in 2017 sought to steal sensitive nuclear technology,[27] while a succession of computer-based operations have enabled the PRC to obtain details of US military aircraft and missile designs.[28] Though covert activity may make up only a small component of overall effort (most of which is overt), the number of such operations that have been exposed in the US indicate that the anticipated gains must be highly valued by Beijing.

In addition to more traditional forms of espionage, Beijing makes use of a large number of incentive programmes that co-opt individuals and institutions. The programmes target both Westerners and Chinese-nationals working or studying within STEM fields, and they are a key component in the CCP's drive for technological superiority over the West. The most well-known of these is the Thousand Talents Program (TTP).

First launched in 2008, the TTP was initially intended to address the brain-drain of PRC scientists. Later, however, it developed another objective: to encourage and reward overseas study by PRC experts and to lure foreign experts to work in China. According to a letter sent by Texas Tech University to its faculty, the TTP is now seen by Congress to be "part of a broader strategy to build technological superiority" by China.[29] The MCF policy combined with a selected choice of TTP beneficiaries plays an obvious role. A report produced by the US Senate Committee on Homeland Security and Governmental Affairs notes that TTP beneficiaries are, under the terms of their contracts, obliged to fill in US grant applications deceptively, including by failing to disclose their TTP status, and to take other steps that bring benefits to China at cost to the US.[30]

---

23 Yu, J. and Zhu, D., 'Commentary: Time to let win-win cooperation define China-U.S. economic, trade exchanges', *Xinhua*, 20 May 2018, available at: www.xinhuanet.com/english/2018-05/20/c_137192692.htm, last visited: 21 August 2020.

24 Crawford, E., 'Made in China 2025: The Industrial Plan that China Doesn't Want Anyone Talking About', *Frontline*, 7 May 2019, available at: www.pbs.org/wgbh/frontline/article/made-in-china-2025-the-industrial-plan-that-china-doesnt-want-anyone-talking-about/, last visited: 21 August 2020.

25 Gewirtz, J.B., 'China's Long March to Technological Supremacy', *Foreign Affairs*, 27 August 2019, available at: www.foreignaffairs.com/articles/china/2019-08-27/chinas-long-march-technological-supremacy, last visited: 21 August 2020.

26 'Military – Civil Fusion and the People's Republic of China', *US Department of State* (2020), op. cit.

27 'U.S. Nuclear Engineer Sentenced to 24 Months in Prison for Violating the Atomic Energy Act', *Department of Justice*, 31 August 2017, available at: www.justice.gov/opa/pr/us-nuclear-engineer-sentenced-24-months-prison-violating-atomic-energy-act, last visited: 21 August 2020.

28 'Chinese man charged with hacking into US fighter jet plans', *The Guardian*, 12 July 2014, available at: https://www.theguardian.com/technology/2014/jul/12/chinese-man-charged-with-hacking-into-us-fighter-jet-plans, last visited: 21 August 2020.

29 'China hushes up scheme to recruit overseas scientists', *Financial Times*, 10 January 2019, available at: www.ft.com/content/a06f414c-0e6e-11e9-a3aa-118c761d2745, last visited 21 August 2020.

30 'Threats to the US Research Enterprise: China's Talent Recruitment Plans', *US Senate Permanent Subcommittee on Investigations* (2019), available at: www.hsdl.org/?view&did=831878, last visited: 22 September 2020.

Those co-opted – wittingly or unwittingly – into the service of the CCP's IP ambitions have been drawn from a broad background. They have been domestic-nationals with no family ties to China (as in the case of two individuals indicted this year), [31] Chinese-nationals, or domiciled members of the Chinese diaspora. [32] Concerns have been raised that members of the Chinese diaspora may be vulnerable to pressure involving threats directed at relatives who remain in China. [33]

While many beneficiaries of TTP and other Chinese incentive schemes have no need to break any law to further CCP agendas, some have been linked to illicit IP transfers and other malpractices. [34] One indictment brought earlier this year by the Department of Justice concerns a senior researcher at Harvard University, who was charged on the basis of an alleged concealment of a highly lucrative association with the TTP, including opening a research laboratory in Wuhan. [35] Proceedings are ongoing and the defendant remains innocent until proven guilty in a court of law.

2.3 China's Universities and Their Relationships to the PLA

One manifestation of MCF is the close ties between the Chinese state security apparatus and Chinese universities. Unlike with British universities, ties between Chinese universities and the state security apparatus extend far beyond agreements over recruitment or research coordination. [36] Instead, the PRC's system sees universities directly supervised by Government agencies who have the authority to direct research and strategic priorities. [37]

In an attempt to analyse the long-standing relationship between China's state security apparatus and China's leading academic centres of STEM research and development, the Australian Strategic Policy Institute (ASPI) released the "China Defence Universities Tracker" (CDUT) in November 2015. The CDUT classifies Chinese research institutions on a risk scale, where risk is defined as "the risk that relationships with these entities could be leveraged for military or security purposes, including in ways that contribute to human rights abuses". [38] The risk scale encompasses four categories: "very high", "high", "medium" and "low" risk [39], based on each institution's record of defence and security connections, involvement in espionage or cyberattacks, inclusion on end-user lists that restrict exports, and other indications of conducting defence research.

The CDUT covers approximately 160 institutions. The "very high risk" category includes 52 PLA institutions, eight security or intelligence-agency institutions, 20 civilian universities and

31 'Former West Virginia University Professor Pleads Guilty to Fraud That Enabled Him to Participate in the People's Republic of China's "Thousand Talents Plan"', *Department of Justice*, 10 March 2020, available at: www.justice.gov/opa/pr/former-west-virginia-university-professor-pleads-guilty-fraud-enabled-him-participate-people, last visited: 22 September 2020; 'Harvard University Professor Indicted on False Statement Charges', *Department of Justice*, 9 June 2020, available at: www.justice.gov/opa/pr/harvard-university-professor-indicted-false-statement-charges, last accessed: 22 September 2020.

32 'Exclusive: Major U.S. cancer center ousts "Asian" researchers after NIH flags their foreign ties', *Science Mag*, 19 April 2019, available at: www.sciencemag.org/news/2019/04/exclusive-major-us-cancer-center-ousts-asian-researchers-after-nih-flags-their-foreign, last visited: 22 September 2020.

33 'Beijing's influence operations target Chinese diaspora', *War on the Rocks*, 1 March 2018, available at: warontherocks.com/2018/03/beijings-influence-operations-target-chinese-diaspora, last visited: 22 September 2020.

34 'Harvard University Professor Indicted on False Statement Charges', *Department of Justice*, 9 June 2020, op cit.; 'Zheng et al Indictment', *Department of Justice*, 18 April 2019, available at: www.justice.gov/opa/press-release/file/1156521/download, last visited: 28 September 2020.

35 Ibid.; 'Affidavit in Support of Application for Criminal Complaint', *Department of Justice*, 21 January 2020, available at: www.justice.gov/opa/press-release/file/1239796/download, last visited: 28 September 2020.

36 S, Han. and X. Xu, 'How far has the state "stepped back": an exploratory study of the changing governance of higher education in China (1978-2018), *Higher Education* 78 (2019): pp. 931-946. https://link.springer.com/article/10.1007/s10734-019-00378-4.

37 Ibid.

38 Joske, A., 'The China Defence Universities Tracker', *ASPI*, 25 November 2019, available at: www.aspi.org.au/report/china-defence-universities-tracker, last visited: 22 September 2020.

39 Ibid.

China's 12 leading defence conglomerates. The "high risk" category is made up of 23 civilian universities. A further 44 civilian universities are ranked as "medium" or "low" risk. Each institution has an entry with an overview of information such as research areas, suspected misconduct and/or criminal activities, and suspected or known links to the military.

In a report accompanying the publication of the CDUT, its author Alex Joske, an analyst at ASPI, highlighted the need for a shift in focus from identifying dual-risk technologies towards a better and more in-depth assessment of potential research partners. Joske points out that whilst "university researchers are generally well placed to understand the nature of a technology and… whether they're 'dual-use' technologies", universities are apparently less able to understand and scrutinise international partners, a result of "insufficient expertise, resources and processes". [40] Hence, Joske set about creating a system by which universities – should they use it – are able to identify potential risks when considering collaborations with Chinese universities.

The ASPI tracking system is not a comprehensive list of all Chinese research institutions, a fact which Joske has acknowledged, saying that ASPI "intend[s] to update and expand the Tracker when possible". [41] Nevertheless, it does enable universities – if they were to use it – to identify potential risks when collaborating with Chinese institutional research partners. This is particularly the case with research partners who have "military links, security links or known connection to human rights abuses or espionage". [42] According to Joske, further bodies warrant further scrutiny:

> [T]here's room for further research on the Chinese Academy of Sciences and its dozens of subordinate research institutes. Twelve of China's defence conglomerates are included in the database, but their hundreds if not thousands of subsidiaries haven't been publicly catalogued.
>
> Nor have private companies and other major suppliers of equipment to the military and security apparatus been included in this project. Further research on the role of universities in supporting state surveillance and on companies that develop surveillance technology used in human rights abuses would be valuable. [43]

It should be noted that the guide considers universities not students. The fact that a university is high or low risk in no way means that every researcher or student from a risk-rated institution is of exactly equivalent risk. Whilst the ASPI tracker has its limitations, it remains the leading publicly available guide to Chinese-based institutions.

Within the tracker, Joske identifies and describes a group of leading Chinese universities with very close links to the Chinese military and defence industry. Joske coined the term the "Seven Sons of National Defence" for these bodies.

The Seven Sons universities are:

- Beijing Institute of Technology;
- Beihang University;
- Harbin Engineering University;
- Harbin Institute of Technology;

[40] Joske, A., 'The China Defence Universities Tracker', *ASPI*, 25 November 2019, available at: www.aspi.org.au/report/china-defence-universities-tracker, last visited: 22 September 2020.

[41] Ibid.

[42] Ibid.

[43] Ibid.

- Nanjing University of Aeronautics and Astronautics;
- Nanjing University of Science and Technology;
- Northwestern Polytechnical University.

Each of these institutes is supervised by the Chinese government's Ministry of Industry and Information Technology, one of whose subordinate agencies is the State Administration for Science, Technology and Industry for National Defense.

The Seven Sons are amongst China's best-funded universities; their research spending totalled some £1.6 billion in 2016 and is only likely to have increased over recent years. [44] In 2018, four of the Seven Sons institutions were amongst China's five best-funded universities "per research staff member". [45] Roughly half of their research spending went towards defence research, which includes developing weapons.

According to ASPI's CDUT, over 10,000 graduates from the Seven Sons join the defence research sector every year. Chinese state corporations specialising in aircraft, missiles, warships, armaments and military electronics are amongst their top employers, as are telecommunications companies with suspected links to Chinese state intelligence. The report claims that four of the Seven Sons universities have been publicly tied to "espionage or export controls violations". [46]

[44] Joske, A., 'The China Defence Universities Tracker', *ASPI*, 25 November 2019, available at: www.aspi.org.au/report/china-defence-universities-tracker, last visited: 22 September 2020.

[45] Ibid.

[46] Ibid.

3. What Has Been Done to Counter China's Acquisition of IP

While many graduates of PLA-linked universities enter the defence sector immediately upon graduation, others go on to continue their studies. Some of these students seek to do so in the West. Over many years, they have done so in an almost unabated manner.

The fear as to their activities and intentions, however, is such that policymakers in Western capitals are having to rapidly reassess what if any limitations and monitoring should be devoted to them.

3.1 The United Kingdom

The UK does not have a programme to counter China's acquisition of IP per se. Instead it has a policy called the Academic Technology Approval Scheme (ATAS) which seeks to mitigate risk from the "misappropriation or theft" of "sensitive intellectual property" in areas related to WMDs and their delivery systems. [47] The then Foreign and Commonwealth Office (FCO) introduced the scheme in 2007.

ATAS is a mandatory process for international students applying for postgraduate study in the UK in a specified list of 44 subjects. It aims to establish whether the student could be deemed to pose national security risks to the UK. [48] The scheme primarily focuses on postgraduate 'research' students but it also applies to 'taught' masters courses in seven especially sensitive subject areas [49]; the list of courses which require clearance are specified by subject category by ATAS (using the Common Aggregation Hierarchy (CAH)) whilst respective universities determine which of their particular courses and programmes fall into such categories. [50] It applies to all students subject to UK immigration control with exemptions for the nationals of 38 allied countries, a list expanded in September 2020 from members of the European Economic Area (EEA). [51] To apply for an ATAS certificate, students are required to submit an online application to the now Foreign, Commonwealth and Development Office (FCDO) containing extensive background information as well as details on their proposed research area. The certificate enables an applicant to secure a Tier-4 visa for a period of six months from the date of issue. [52]

ATAS replaced the Voluntary Vetting Scheme (VVS), under which universities were asked to refer students for vetting by the then FCO on a discretionary basis. This provided inconsistent coverage, with the majority of universities declining to participate. [53] In a 2003 report, the House

47 'Academic Technology Approval Scheme', *Foreign & Commonwealth Office* (2020), available at: www.gov.uk/guidance/academic-technology-approval-scheme, last visited: 29 September 2020.

48 'Immigration Rules Appendix 6: academic subjects that need a certificate', *UK Government Immigration Rules*, available at: www.gov.uk/guidance/immigration-rules/immigration-rules-appendix-6-academic-subjects-that-need-a-certificate, last visited: 15 September 2020.

49 Ibid.

50 'Note of HECOS/ATAS Meeting – Friday 26 January 2018', *Higher Education Statistics Authority* (2018), available at: www.hesa.ac.uk/files/HECoS_ATAS_meeting_2018-01-26_note.pdf, last visited: 3 September 2020.

51 'Statement of Changes in Immigration Rules', *HM Government* (2020), available at: https://assets.publishing.service.gov.uk/ government/uploads/system/uploads/attachment_data/file/916565/CCS001_CCS0920158512-001_Stat_of_change_Immigration_Rules_HC_707_Print.pdf, last visited: 29 September 2020.

52 'Academic Technology Approval Scheme', *Foreign, Commonwealth and Development Office*, 25 March 2013, available at: www.gov.uk/guidance/academic-technology-approval-scheme, last visited: 3 September 2020.

53 Shepherd, J., 'Vetting gets a mixed reception', *The Guardian*, 29 January 2008, available at https://www.theguardian.com/education/2008/jan/29/administration.postgraduate#:~:text=Atas%20is%20designed%20to%20ensure,have%20links%20to%20WMD%20programmes.%22&text=A%20voluntary%20vetting%20scheme%20in,the%20Foreign%20Office%20preceded%20Atas.&text=The%20Foreign%20Office%20says%20it%20will%20do%20this%20in%20May, last visited: 2 September 2020.

of Commons Science and Technology Committee concluded that the "poor participation of some universities in the Voluntary Vetting Scheme mean[t] that it need[ed] to be replaced". [54]

The origins of the VVS are instructive in understanding the operation of the current regulatory framework. The VVS system was established in 1994 after it emerged that the head of Iraq's biological warfare programme had pursued postgraduate studies in microbiology at a British university in the 1980s. [55] A subsequent review of VVS was conducted in 2003, when a number of Iraqi scientists were arrested and deported having attempted to study antibiotic resistant pathogens at another British university. [56] In short, since its initiation, the framing of the UK's vetting system has been one of counter-proliferation – designed to preclude access to WMD by prospective adversaries.

Ostensibly, this remains the focus of the programme today. The FCDO administers the scheme as part of its counter-proliferation purview. Subjects deemed sensitive are those involving knowledge "which could be used in programmes to develop weapons of mass destruction (WMDs) or their means of delivery". [57] However, while the FCDO has never announced a change in objective, recent departmental communications point to a broader objective.

In its response to a 2019 report from the Foreign Affairs Select Committee in which the Committee praised the scheme, the Government said that it "regularly reviews the Scheme to ensure it remains a valid and effective means to protect sensitive intellectual property from misappropriation or theft." [58] Recent reviews have seen the subject areas for which applicants require clearance orientate away from a primary concern with WMD. Today, mechanical, material, and mineral engineering are subject to additional scrutiny, while microbiology is not.

Such a shifting focus reflects the nature of concerns within the higher education sector. During the 2019 Foreign Affairs Committee inquiry which explored the implications of autocratic states on UK universities, Universities UK stated that "the most significant threat from hostile state actors is misappropriation of research output, including the seizing of research data and intellectual property". [59] The seven especially sensitive subject areas which are subject to additional scrutiny lend themselves far more easily to military technology generally than they do to WMD or their means of delivery. Other subjects included on the wider ATAS list – which includes information technology, software engineering, civil engineering, and artificial intelligence – could not reasonably be seen to primarily concern the development of WMDs or their or their means of delivery.

However, the lack of shift in framing has left the FCDO conducting a form of linguistic gymnastics as it seeks to explain a "counter-proliferation" programme that appears, on closer inspection, to have other objectives. It also raises questions of expertise, with a counter-proliferation

54 'The Scientific Response to Terrorism', House of Commons Science and Technology Committee, 20 October 2003, available at: publications.parliament.uk/pa/cm200203/cmselect/cmsctech/415/415.pdf, last visited: 7 September 2020, p.63.

55 'BBC investigation exposes flaws in biological research vetting scheme', *BBC Press Office*, 19 November 2002, available at: www.bbc.co.uk/pressoffice/pressreleases/stories/2002/11_november/19/scientists_vetting.shtml, last visited: 7 September 2020.

56 'Postgrad checks worry scientists', *BBC News*, 12 March 2007, available at: news.bbc.co.uk/1/hi/education/6441263.stm, last visited: 7 September 2020.

57 'Academic Technology Approval Scheme (ATAS)', *Foreign and Commonwealth Office*, *Foreign, Commonwealth and Development Office*, available at: https://www.gov.uk/guidance/academic-technology-approval-scheme, last visited: 7 September 2020.

58 'A cautious embrace: defending democracy in an age of autocracies: Government Response to the Committee's Second Report of Session 2019', *Parliament UK*, 6 March 2020, available at: publications.parliament.uk/pa/cm5801/cmselect/cmfaff/116/11602.htm, last visited 7 September 2020.

59 'Written evidence from Universities UK (AFP0032)', *Parliament UK*, October 2019, available at: data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/foreign-affairs-committee/autocracies-and-uk-foreign-policy/written/106141.html, last visited: 7 September 2020.

unit leading what is a much broader undertaking. Unless and until the ATAS programme is to formally recognise the role that it has come to play in preventing the intangible transfer of a broader range of advanced military technology, it will be limited in its effect.

If the scope of the ATAS programme gives rise for concern, so too does its operationality. Today, the ATAS certification programme is a broadly self-standing element of the immigration process for international applicants for postgraduate study in the UK. While its criteria require comparatively similar responses to that of a standard student visa application, it exists as a standalone process. Segmenting it from the visa application process means — unlike with other information — applicants cannot be questioned face-to-face by Entry Clearance Officers (ECOs) on the responses they provide.

Equally troubling are the limitations in the extent of questions that the ATAS scheme asks of applicants. By way of example, it currently requires no information as to whether applicants have previously received state support for their research. Similarly, it requires or requests no information from applicants as to political affiliation, membership of programmes such as the TTP, or detailed military connections. Accordingly, it is not clear how certificating officers are able to form a full impression about an applicant prior to making a decision.

Just as unclear is the role of the UK's enforcement measures. In contrast to the US, in which 13 individuals have been indicted this year, the UK has announced the charging of no individuals tied to hostile states for IP-related charges at any point over the past decade. While it is certainly possible that this has occurred because there are simply no such cases in the UK to prosecute, it is an unusual outcome in the sense that various UK authorities have decried the threat of IP drainage publicly, and the UK has Chinese-national student numbers that are not markedly dissimilar to that of the US yet a dramatically different prosecution rate. This disparity is even more marked when it is considered that the UK possesses statutes that criminalise dishonesty in ATAS applications and the unauthorised transfer of dual-use technology. At the very least, the different prosecution rates should be sparking questions as to why this might be so.

British intelligence insiders have long pointed out that the UK's approach to policing intelligence matters is markedly different from that of the US. [60] The UK prioritises the recruitment of hostile state agents for its own ends over the overt process of prosecution. That may be so here, though, it is not clear what action the UK takes when such attempts are unsuccessful. Nor is it clear why these two approaches – recruitment versus prosecution – would be considered to be mutually exclusive.

It is equally unclear if the UK possesses the expertise or has the structures in place to bring any offenders in this area to justice, if it so desired.

Unlike in the US, offences likely to apply in these scenarios fall under split jurisdictions. The "enforcement agency" for export control violations including illegal ITT would be Her Majesty's Revenue and Customs (HMRC), [61] a body principally charged with enforcing tax rules, while offences for dishonesty in ATAS applications would fall under the jurisdiction of the UK Border Force. Neither of these bodies have sections dedicated to offences as complex and specific as state-directed IP theft. Nor have either of these bodies ever successfully pursued a prosecution for any offence connected to state-linked IP theft. Neither body lists countering hostile-state

[60] O'Flaherty, K., 'How the UK can get a better grip on Russian espionage', *Wired*, 25 July 2020, available at: www.wired.co.uk/article/russia-report-official-secrets-act, last visited: 28 September 2020.

[61] 'The enforcement of export control breaches', *Lexis Nexis*, undated, available at: www.lexisnexis.co.uk/legal/guidance/the-enforcement-of-export-control-breaches, last visited: 3 August 2020.

interference as one of its priorities on their website. [62] [63] HMRC's organisational chart specifies no single individual with singular responsibility for this area of enforcement. [64]

Equally unclear is how closely either of these groups work with the Security Services. One symbolic shortcoming of the lack of coordination is that, at the time of writing, MI5's website describes responsibility for "maintaining the export licensing system" as being that of the "Department for Business, Innovation and Skills", linking to their now defunct website. [65] The "Department for Business, Innovation and Skills" ceased to exist in July 2016 after it was merged into the Department for Business, Energy and Industrial Strategy. [66] Meanwhile, the responsibility for maintaining the export licensing system has been with the separate Department for International Trade since 2016. [67]

With enforcement, as with risk-mitigation, the UK has the building blocks of a comprehensive system of regulation. However, it neither appears to fully enforce current law, having prosecuted no offenders despite an acknowledged threat in this area, nor to have adequately established structures readily capable of doing so.

3.2 The United States

In contrast to the UK, the US does have a policy, albeit a recent one, to counter China's acquisition of IP.

Signed by President Donald Trump on 29 May 2020, the Presidential Proclamation bars Chinese postgraduate students from entering the US should they have ties to entities which "implement or support the PRC's military-civil fusion strategy". [68] The proclamation stated that some Chinese postgraduate students are utilised by Beijing as "non-traditional collectors of intellectual property". [69] It goes on to say that such IP drainage "is a threat to our Nation's long-term economic vitality and the safety and security of the American people". [70]

The Presidential Proclamation was signed two days after Republican Senators Tom Cotton and Marsha Blackburn introduced the Secure Campus Bill in the US Senate. The Bill would have mandated that any Chinese-nationals' visa applications were declined when applying to study STEM subjects in the US. [71] The Bill was motivated, in part, by the IP Commission's 2019 report, which claimed that espionage within universities and research departments was a tool through which China was stealing IP. Those fears – often put in the terms of "non-traditional collectors"

62 'Border Force: About Us', *UK Government*, available at: www.gov.uk/government/organisations/border-force/about#corporate-information, last visited: 28 September 2020.

63 'HM Revenue and Customs: About us', *UK Government*, available at: www.gov.uk/government/organisations/hm-revenue-customs/about, last visited: 28 September 2020.

64 'HMRC Organisation Chart', *UK Government*, August 2020, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/911546/HMRC_Organisation_Chart_August_2020.pdf, last visited: 28 September 2020.

65 'Counter-Proliferation', *MI5 – The Security Service*, available at: https://www.mi5.gov.uk/counter-proliferation, last visited: 28 September 2020.

66 'Department for Business, Innovation and Skills was replaced by Department for Business, Energy & Industrial Strategy', *UK Government*, available at: www.gov.uk/government/organisations/department-for-business-innovation-skills, last visited: 28 September 2020.

67 'Export Control Joint Unit', *UK Government*, available at: www.gov.uk/government/organisations/export-control-organisation, last visited: 28 September 2020.

68 'Proclamation on the Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China', *White House*, 29 May 2020, available at: www.whitehouse.gov/presidential-actions/proclamation-suspension-entry-nonimmigrants-certain-students-researchers-peoples-republic-china/, last visited: 3 August 2020.

69 Ibid.

70 Ibid.

71 'Cotton, Blackburn, Kustoff Unveil Bill to Restrict Chinese STEM Graduate Student Visas & Thousand Talents Participants', Tom Cotton, US Senator for Arkansas, 27 May 2020, available at: www.cotton.senate.gov/?p=press_release&id=1371, last visited: 11 August 2020.

of IP – have been echoed by law enforcement including in remarks from Christopher Wray, the Director of the FBI. [72]

The language of the Presidential Proclamation specifies that the ban is intended to be limited to visa applicants who "implement or support the PRC's military-civil fusion strategy". [73] According to multiple media reports, published contemporaneously and citing anonymous US officials, "the ban targets seven military-affiliated universities in China" or "the Seven Sons of National Defence". [74] Additionally, the ban is said to affect the National University of Defense Technology (NUDT), which is directly subordinate to the Central Military Commission and the only military institution to be sponsored by Chinese government university development programmes. [75]

The Proclamation does include an exemption for prospective entrants who are "studying or conducting research in a field involving information that would not contribute to the PRC's military-civil fusion strategy, as determined by the Secretary of State and the Secretary of Homeland Security, in consultation with the appropriate executive departments and agencies". [76] The terms of that exemption are specified in the State Department's "Foreign Affairs Manual" (FAM). [77] However, the list of non-screened subject areas is listed as "unavailable" in the public version of the FAM, a status commonly used for classified information.

While the ban – extending to a wide range of study in the US – is broad in remit, its scope is comparatively limited, targeting a comparatively small number of foreign students. According to Robert Daly, Director of the Wilson Center's Kissinger Institute on China and the US, the ban would affect roughly 3,000–4,000 students. [78] Targeting as few as 2% of Chinese postgraduate students, based on historic estimates, it targets a relatively limited number of Chinese-national students who might be considered to pose a potential security risk. It covers graduates from only a relatively small number of Chinese institutions deemed "very high risk" by ASPI.

In that vein, Dan Cadman, a fellow at the Washington D.C.-based think tank Center for Immigration Studies, raised concerns that the US authorities may not be aware of the full spectrum of CCP entities facilitating the MCF strategy. [79] His concerns have not been shared by the university sector, however. Representative bodies for American universities have raised fears as to the ban's "sweeping" effect. [80] Susan Shirk, chairwoman of the 21st Century China

72 Wray, C. 'Responding effectively to the Chinese economic espionage threat', Department of Justice China Initiative Conference, Center for Strategic and International Studies, 6 February 2020.

73 'Proclamation on the Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China', *White House*, 29 May 2020, available at: www.whitehouse.gov/presidential-actions/proclamation-suspension-entry-nonimmigrants-certain-students-researchers-peoples-republic-china/, last visited: 3 August 2020.

74 Cong, F., 'US Ban on Chinese Students With Military Links Divides Experts on Impact', *Voice of America*, 4 June 2020, available at: https://www.voanews.c.om/usa/us-ban-chinese-students-military-links-divides-experts-impact, last visited: 10 August 2020; Wong, E and Barnes, J.E., 'U.S. to Expel Chinese Graduate Students With Ties to China's Military Schools', *The New York Times*, 28 May 2020, available at: www.nytimes.com/2020/05/28/us/politics/china-hong-kong-trump-student-visas.html, last visited: 17 August 2020; Palmer, J., 'How Is China Responding to the U.S. Protests?' *Foreign Policy*, 3 June 2020, available at: https://foreignpolicy.com/2020/06/03/how-is-china-responding-to-the-u-s-protests/, last visited: 17 August 2020.

75 'U.S. to Expel Chinese Graduate Students With Ties to China's Military Schools', *The New York Times*, 28 May 2020; 'National University of Defense Technology', China Defence Universities Tracker, *Australian Strategic Policy Institute*, available at: unitracker.aspi.org.au/universities/national-university-of-defense-technology/, last visited: 7 September 2020.

76 'Proclamation on the Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China', *White House*, 29 May 2020.

77 '9 FAM 302.14 (U) Ineligibility based on sanctioned activities' *Foreign Affairs Manual: US Department of State*, 14 September 2020, available at: fam.state.gov/fam/09FAM/09FAM030214.html#M302_14_12_C 9 FAM 302.14-12 (U), last visited: 22 September 2020.

78 *Voice of America*, op. cit.

79 Cadman, D., 'Stopping Chinese Infiltration of U.S. Educational and Research Institutions', *Center for Immigration Studies*, 25 June 2020, available at: https://cis.org/Report/Stopping-Chinese-Infiltration-US-Educational-and-Research-Institutions, last visited: 26 August 2020.

80 'International Education Grows Concerned about Latest Executive Action to Restrict Chinese Students & Scholars', *NAFSA*, 29 May 2020, available at: www.nafsa.org/about/about-nafsa/international-education-grows-concerned-about-latest-executive-action-restrict, last visited: 26 August 2020.

Center UC San Diego, has said that universities are concerned that the order could lead to overreach, which might "discourage talented Chinese students from doing graduate work or research at American universities, which would be very counterproductive from the standpoint of [US] scientific and technological innovation." [81]

This dispute follows a long line of political disagreements over the fundamental question of whether treating Chinese-national students as a higher-risk group irrespective of direct ties to the military is proportionate or fair. When, in 2018, Christopher Wray, Director of the FBI, was asked about the threat posed by Chinese students in "advanced programs in the sciences and mathematics", he responded:

> I think in this setting I would just say that the use of nontraditional collectors, especially in the academic setting, whether it's professors, scientists, students, we see in almost every field office that the FBI has around the country. It's not just in major cities. It's in small ones as well. It's across basically every discipline.
>
> I think the level of naivete on the part of the academic sector about this creates its own issues. They're exploiting the very open research and development environment that we have, which we all revere, but they're taking advantage of it. So one of the things we're trying to do is view the China threat as not just a whole of government threat, but a whole of society threat on their end. I think it's going to take a whole of society response by us. So it's not just the intelligence community, but it's raising awareness within our academic sector, within our private sector, as part of the defense. [82]

His remarks – pointing out that IP theft risks could not be isolated to the military but emanated from the whole of Chinese society – faced severe criticism. Representatives Judy Chu, Ted Lieu, and Grace Meng, each Democrat members of the Congressional Asian Pacific American Caucus, issued statements denouncing Wray's comments. [83] Chu argued that the "assumption" that "having ties to China makes you prone to espionage" was ill-founded and "sweepingly broad". [84]

Concerns over IP theft or drainage, however, do not merely emanate from individuals with direct ties to the PLA, as the string of indictments filed over the last year show.

Since January 2020, the US Department of Justice (DOJ) has brought 13 indictments against individuals at American universities with varying connections to Chinese universities. Six of these individuals were employed staff whilst the remaining seven were Chinese-nationals studying on student visas. Various offences have been cited amongst the indictments: five individuals were charged with counts of visa fraud, five were charged with counts of making false statements, two were charged with conspiracy, two with tax offences, two with wire fraud, one was charged with counts of acting as an agent of a foreign government, two with grant fraud, one individual was charged with smuggling, and one with destroying evidence.

The research fields of the individuals vary. While the US does not publish lists of regulated subjects, seven of the individuals are researchers in fields that would be included in subject fields subject to regulation by the UK's ATAS scheme. They include: chemistry, physics,

---

81 Watanabe, T., ''It's the new Chinese Exclusion Act': How a Trump order could hurt California universities', *Los Angeles Times*, 7 June 2020, available at: https://www.latimes.com/california/story/2020-06-07/trump-move-to-bar-entry-of-some-chinese-graduate-students-stirs-campus-anxiety-anger, last visited: 26 August 2020.

82 'Senate Hearing 115-278', *U.S. Government Publishing Office*, 13 February 2018, available at: www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-0#, last visited: 28 September 2020.

83 'CAPAC Members on Rubio and Wray's Remarks Singling Out Chinese Students as National Security Threats, *Congressional Asian Pacific American Caucus*, 15 February 2018, available at: https://capac-chu.house.gov/press-release/capac-members-rubio-and-wray's-remarks-singling-out-chinese-students-national-security, last visited: 28 September 2020.

84 Ibid.

biomedical engineering, mechanical engineering, chemical engineering, aerospace engineering, mathematics, and machine learning and artificial intelligence. [85]

The indicted individuals were linked to 12 Chinese universities, of which five are considered to be "high" or "very high" risk, as designated by ASPI. [86] The two universities labelled as "high risk" are the Wuhan University of Technology and Sun Yat-Sen University and the three "very high risk" are the NUDT, Air Force Medical University and Aviation University of Air Force. Two individuals were linked with the Chinese Academy of Sciences, which, along with four of the universities, is not included on the ASPI tracker, whilst the remaining two universities were unnamed by the DOJ, although one was referred to as a "military university". [87] In the majority of cases, proceedings remain ongoing and the defendants remain innocent until proven guilty in a court of law.

There were three individuals, all Chinese students, linked to NUDT, the only university of the 12 linked where the indicted individuals are thought to be covered by the US proclamation. Even if the ban – as it has come to be implemented – contains all Chinese military universities, it would fall far short from covering all risk groups.

Contrary to fears of disproportionality, a real concern is that the US's risk-mitigation approach might reduce threats by as little as a quarter. Such a reality is – in part – a consequence of China's MCF doctrine in which individuals and organisations of all backgrounds may be co-opted into activities on behalf of the state. This does not of course mean that such outcomes occur on a common or regular basis. But the fact they can exist at all because of Chinese state policy is surely cause for concern.

85 'Immigration Rules Appendix 6', *UK Government Immigration Rules*, op. cit.

86 'China Defence Universities Tracker – About', *ASPI* (2019), available at: https://unitracker.aspi.org.au/about/, last visited: 14 September 2020.

87 'Researchers charged with visa fraud after lying about their work for China's People's Liberation Army', *Department of Justice – Office of Public Affairs*, 23 July 2020, available at: www.justice.gov/opa/pr/researchers-charged-visa-fraud-after-lying-about-their-work-china-s-people-s-liberation-army, last visited: 14 September 2020.

4. What Would British Policy Look Like if it Applied US Methods?

The UK's thus-far piecemeal and evolving approach to university IP theft has seen a lack of serious analysis of the implications of the various regulatory approaches open to policymakers. The dramatic change in regulatory approach contained within the May Presidential Proclamation begs the question of what impact – if any – a similar policy would have were it to be replicated in the UK.

To answer this question, a freedom of information (FOI) request was submitted to the then FCO in June 2020 which asked for the total number of ATAS certificates granted to graduates of the Seven Sons in the 2019 calendar year, as well as a breakdown of which Seven Son university they previously attended. The reply stated that "the information you have requested is not held centrally and would require us to consider each application individually to establish whether information [sic] is held". [88] As such, it appears that no central registry is kept of postgraduate students studying sensitive subjects who have previously attended PLA-linked facilities. In this circumstance, it was necessary to turn to a more localised form of information and to contact universities directly.

4.1 Selection of Universities

A study-set of the most research-intensive universities was collected as the sample for this exercise. These universities are often divided into seven groups. These are:

1. The Russell Group;
2. The Ancient Universities of Scotland;
3. SETsquared;
4. The N8 Research Partnership;
5. The GW4 group;
6. The Midlands Innovation Group;
7. Science and Innovation South (SES).

Any university that was a member of one of these groups was included in the sample. A large degree of overlap exists between the universities in each group, but in total there are 34 individual universities. [89] Due to the report's focus on STEM subjects, a decision was taken to exclude the London School of Economics from the study-set as it is not involved in STEM research. This resulted in a final study-set of 33 universities.

4.2 Number of Seven Sons Students

FOI requests were sent to each of the 33 universities in June 2020. These requests asked for both the total number Seven Sons graduates currently enrolled at the university (i.e., in the 2019–20 academic year) and a breakdown of which Seven Sons university these graduates attended. As can be seen in Figure 1, 25 universities replied, five declined on the basis that data was not stored, and three did not respond. In total, the responses reveal a minimum of 899

[88] Foreign and Commonwealth Office, "FREEDOM OF INFORMATION ACT 2000 – REQUEST REF: 2020/14720", received 17 August 2020.

[89] These universities were: the University of Aberdeen, Aston University, the University of Bath, the University of Birmingham, the University of Bristol, the University of Cambridge, Cardiff University, Cranfield University, Durham University, the University of Edinburgh, the University of Exeter, the University of Glasgow, Imperial College London, Keele University, King's College London, Lancaster University, the University of Leeds, the University of Leicester, the University of Liverpool, London School of Economics, Loughborough University, the University of Manchester, the University of Newcastle, the University of Nottingham, the University of Oxford, Queen Mary University, Queen's University Belfast, the University of Sheffield, the University of Southampton, the University of St Andrews, the University of Surrey, University College London, the University of Warwick, and the University of York.

Figure 1: Graduates of the Seven Sons enrolled at British Universities (2019–20)

University	Seven Son Graduates enrolled
University of Sheffield	140
University of Glasgow	79
University College London	70
University of Edinburgh	69
University of Warwick	62
University of Manchester	58
Cranfield University	54
Imperial College London	49
University of Leeds	41
University of Bristol	39
University of Southampton	35
University of Exeter	34
Durham University	30
King's College London	25
University of Bath	25
University of Oxford	15
Aston University	13
University of Leicester	13
Loughborough University	13
University of Cambridge	11
Lancaster University	10
University of St Andrews	7
Cardiff University	6
Queen Mary University of London	<5
Keele University	0
University of Birmingham	No response
Newcastle University	No response
Queen's University Belfast	No response
University of Liverpool	Refused
University of Nottingham	Refused
University of York	Refused
University of Surrey	Refused
University of Aberdeen	Refused
TOTAL	**899**

Seven Sons graduates currently enrolled at the 33 most research-intensive universities. Given the limitations of this search, it seems likely that well over a thousand Seven Sons graduates are currently enrolled at British universities.

Of the universities that were surveyed, the University of Sheffield accounts for the highest number of these graduates, at 140. Next is the University of Glasgow with 79, followed by the University College London with 70. The universities of Edinburgh, Warwick and Manchester register 69, 62, and 58 Seven Sons graduates respectively. All but one university (Keele) had Seven Sons graduates currently enrolled.

4.3 Most Sensitive Subjects

The ATAS system applies only to prospective students seeking admission to study a variety of postgraduate subjects predominantly in the STEM field. The FCDO has set out a list of 44 Common Aggregation Hierarchy (CAH) course codes which would necessitate an ATAS certificate. It is for each university to specify which of their programmes fit under the CAH codes that are listed and, therefore, which courses require approval to be studied.

Of the 44 course types that are subject to the ATAS system, 37 require certification prior to study only when the nature of the course is "research" orientated. [90] Seven subject areas are subject to the ATAS system whether the course is "research" or "taught". These subjects are Materials Science, Physics (including Nuclear Physics), Mechanical Engineering, Aeronautical and Aerospace Engineering, Chemical, Process and Energy Engineering, Minerals Technology, and Materials Technology. The FCDO does not detail its methodology for the selection of these subject matters.

4.4 High-Risk Students Studying High-Risk Subjects

Using these seven subjects – identified as the most sensitive subjects by the ATAS scheme – this report undertook a quantitative analysis of the individuals currently enrolled in "research" programmes about them. "Taught" programmes were excluded from this exercise because the ATAS system recognises that "research" programmes are more sensitive. [91]

Against this criteria, lists of open-source postgraduate researchers in the relevant research groups were examined at each of the 33 British universities. Having identified potential individuals at the universities, personal university profiles were cross-examined against other open-source data, including Facebook, ResearchGate, and LinkedIn profiles to identify previously attended Chinese institutions. The records of all individuals who had previously attended Chinese universities were then collated.

This search produced a total of 151 students studying high-risk subjects at British universities who had previous links to a Seven Sons institution. As can be seen in Figure 2, the research revealed that the universities of Sheffield and Oxford both had 16 Seven Sons graduates enrolled in the highest risk fields. While the universities of Bristol, Cranfield, Loughborough and Warwick all reported nine students each.

While the Seven Sons list of Chinese institutions is the basis of the US regulatory actions, it is drawn from the wider CDUT list of some 159 Chinese universities. [92] Many of the facilities

[90] Taught subjects are those in which existing knowledge and scholarship is passed onto students. Research subjects ordinarily require original work which expands the corpus of work in a given field.

[91] In the case of one subject, Physics, a research decision was taken to include only nuclear physics programmes in order to further refine the focus on sensitive intellectual property.

[92] Joske, A., 'The China Defence Universities Tracker: Exploring the military and security links of China's universities', *ASPI* (2019), available at: https://www.aspi.org.au/report/china-defence-universities-tracker, last visited: 3 August 2020.

Figure 2: Number of Seven Sons graduates enrolled in high-risk subjects

University	High-risk subject Seven Sons
University of Oxford	16
University of Sheffield	16
University of Bristol	9
University of Warwick	9
Loughborough University	9
Cranfield University	9
University of Nottingham	8
University of Manchester	8
Cardiff University	6
Imperial College London	6
University of Edinburgh	5
University of Cambridge	4
University of Birmingham	4
Durham University	4
University of Southampton	4
University of Bath	4
University of Glasgow	3
Queen's University Belfast	3
University of Surrey	3
Queen Mary University of London	3
University College London	3
Aston University	3
Newcastle University	2
University of Leeds	2
King's College London	2
University of Exeter	1
University of Liverpool	1
Lancaster University	1
University of York	1
University of Leicester	1
University of Aberdeen	1
Keele University	0
University of St Andrews	0
TOTAL	**151**

Figure 3: High-risk individuals enrolled in high-risk subjects at UK universities

University	High-risk subject Seven Sons	High-risk subject Very High Risk	High-risk subject High Risk	High-risk subject Medium Risk	High-risk subject Low Risk	High-risk subject ASPI Total
University of Oxford	16	38	44	16	2	100
University of Cambridge	4	22	20	7	1	50
University of Sheffield	16	24	16	8	1	49
Imperial College London	6	17	17	11	0	45
University of Manchester	8	32	11	11	2	56
Loughborough University	9	19	17	6	0	42
Cranfield University	9	17	12	3	1	33
University of Bath	4	8	5	2	0	15
University of Warwick	9	13	9	6	2	30
University of Edinburgh	5	15	9	6	0	30
University of Birmingham	4	11	14	6	1	32
University College London	3	8	13	8	0	29
University of Liverpool	1	15	7	9	0	31
Aston University	3	11	8	8	0	27
Durham University	4	11	7	8	0	26
University of Southampton	4	15	7	3	0	25
Cardiff University	6	15	4	4	1	24
Queen Mary University of London	3	10	6	9	1	26
University of Surrey	3	13	7	0	0	20
University of Bristol	9	10	6	3	0	19
University of Nottingham	8	10	4	5	0	19
University of Glasgow	3	9	5	2	0	16
University of St Andrews	0	1	6	8	0	15
University of Leeds	2	8	6	3	0	17
Newcastle University	2	2	7	3	0	12
University of Exeter	1	2	6	1	1	10
King's College London	2	3	4	3	0	10
Queen's University Belfast	3	4	4	2	0	10
Lancaster University	1	4	3	2	1	10
University of York	1	3	2	2	0	7
University of Leicester	1	2	4	1	0	7
University of Aberdeen	1	3	1	3	0	7
Keele University	0	2	1	0	0	3
TOTAL	**151**	**377**	**292**	**169**	**14**	**852**

included within this wider list have such close ties to China's broader state-security apparatus that they can be considered to be of equivalent risk to the Seven Sons. As such, any identified individuals who had previously attended any university listed on the ASPI website as being of any level of risk were included in an additional search. [93]

This search identified a total of 852 individuals in British higher education institutions, at the postgraduate level, with links to universities in the PRC that have been flagged by ASPI as being of a level of risk due to their connections with the military and defence industry.

These individuals may not, under the present US policy, be barred from acquiring a student visa. However, it is legitimate to consider if they pose some security risk and, as such, they are worth considering in the overall analysis of the picture in the UK.

Again, some of the UK's most prestigious universities ranked highly in this search. The University of Oxford reported 38 students who had attended very "high-risk" universities, Sheffield 24 and Cambridge 22.

Overall, the University of Oxford reported by far the highest number of Chinese students involved in sensitive subjects from universities of all risk levels, with 100 students identified. Following Oxford are the universities of Cambridge and Sheffield, showing a similar pattern to Figure 2. Respectively, they had 50 and 49 Chinese students from universities categorised under all levels of risk. Those that reported the fewest total Chinese students from institutions of all risk levels were the universities of Aberdeen, Leicester, York and Keele. The former three universities had seven students each, whilst three were found at Keele.

It is important to note that this report does not suggest that any Seven Sons students/graduates, or for that matter any "risk" students on "risk" courses as highlighted by Figures 1–3, are actually involved in stealing IP and/or passing it back to the CCP. However, it is our opinion that common sense and US experience should surely dictate that the identified categories of graduates/students on these types of courses should be vetted far more carefully before being given access to our valuable, strategic, IP as a 'belt and braces' exercise at the very least.

[93] This search includes the same graduates of the Seven Sons listed in Figure 2. They are each included in the "very high risk" category of students in Figure 3.

5. What is to be Done?

Her Majesty's Government (HMG) says that it recognises the seriousness of "the industrial-scale theft of intellectual property" from British universities.[94] Yet every year, thousands of Chinese students enrol at British universities who would be barred from entering the US on security grounds. While prosecutions for IP theft from university campuses are increasingly common in the US, not a single one has ever taken place in the UK. While one possible explanation is that IP is simply not being stolen here, there are other more troubling conclusions that also must be considered.

It is clear that the UK's ATAS is no longer fit for purpose and requires comprehensive rethinking in the face of the scale of the challenge. Such a system must recognise both the benefits and the risks of international students.

Chinese-national students at British educational institutions are doubtless conscientious and diligent students who – as well as making financial contributions to the sector – bring genuine scholarly benefits to the academy. Despite the threat posed by China, it is neither desirable nor proportionate for the UK to preclude Chinese-nationals from studying in British universities. As such, any system that attempts to address the challenge of IP drainage must recognise how different types of students fit into an analysis of a national security risk framework.

However, the CCP poses an altogether different threat to either Saddam Hussein's Iraq in the 1990s or the Soviet Union during the Cold War. Its adoption of the MCF doctrine, together with its willingness to co-opt its own citizens into the acquisition of IP, makes the identification of the source and nature of the threats it poses far harder to identify – and thus to mitigate. As such, it is necessary to consider these characteristics when creating a counter-IP-drainage strategy capable of rising to this new challenge. A regulatory system built on assumptions borne solely from experiences related to previous adversaries – be they Saddam Hussain or the USSR – is unlikely to rise to the challenge of this new threat which differs from earlier ones because of technological advances, levels of global integration, and societal openness.

In this situation, the UK ought to adopt policies to secure the safety of sensitive technology. Broadly speaking, such policies take two primary forms: 'risk mitigation' and 'enforcement'. Risk mitigation policies aim to reduce the number of potential threats within the sector. Enforcement approaches, meanwhile, aim to root out those that already exist. The optimal system relies on both of these approaches: reducing the potential number of threats to a level at which enforcement measures can be used to monitor and eliminate any residual threats.

5.1 Risk Mitigation

Risk-mitigation policies – insofar as they are applicable to countering this form of threat – exist to reduce the overall number of threats to a level in which robust security measures and proper policing can focus on removing small numbers of residual concerns. This is the first basic characteristic of an effective policy: it must reduce risk.

Such policies must, however, be properly balanced in order that they have a proportionate impact and prevent excessive numbers of innocent parties being caught up in their effect. This is particularly true when, as is likely in this circumstance, such measures may face severe criticism from the university sector and/or quarters of political opinion. Proportionality is the second basic characteristic of an effective policy.

[94] 'National Cyber Security Centre to unite UK cyber expertise', *NCSC*, 14 March 2016, available at: www.ncsc.gov.uk/news/national-cyber-security-centre-unite-uk-cyber-expertise, last visited: 28 September 2020.

The task is, therefore, to build a system that both reduces the risk and does so in proportion to the risk. The system should then be combined with a concept of 'openness where possible' to ensure support from the sector. To create this, a hybrid approach that utilises the best of the US and UK systems would appear to be best.

On the one hand, the UK's *de facto* focus on courses that have military or other sensitive uses is sensible. Despite its widespread mendacity, China has been transparent about the security-sensitive technologies it seeks to acquire. Consequently, HMG possesses sound information about the subject areas that it needs to protect. The course list already attached to ATAS covers each of the ten-point list of technologies targeted for acquisition in China's "Made in China 2025" strategy. That said, it is far from clear who, if anyone, the system precludes from studying in the UK.

On the other hand, the US system has clearly defined risk parameters and offers a more sensible method for excluding students. It is simply not practical for every applicant for postgraduate study to be vetted in great detail. In these circumstances, broad approaches, including making decisions on the basis of previous institutional affiliation, become necessary to determine levels of risk that are tolerable.

Despite legitimate security concerns, neither the UK nor the US, however, has provided as much detail about its systems as they could have. The UK refuses to detail which institutions of previous affiliation it bars prospective entrants from, information that the US, at least partially, released in May. The US, meanwhile, does not disclose the list of subject areas impacted by its ban. The UK details its list of regulated subjects on the FCDO website. Given that an adversary with the resources of China will be readily capable of identifying the nature of any ban, the justification for refusing to publish either seems slight.

In practice, an effective risk-management approach for the UK must:

1. Reduce numbers of students deemed to be high-risk on account of previous institutional affiliation to the level that residual threats can be addressed by enforcement activities. This requires an end to a situation in which high-risk Chinese-nationals enrolled at UK universities number in the high thousands or tens of thousands.

2. Constrain only those subject areas whose research faces the serious prospect of acquisition by hostile states and whose acquisition could prove seriously prejudicial to the interests of the UK. These areas should be guided by China's own stated ambitions and should consider economic as well as military damage. If it is palatable only to regulate subjects with military applications, the challenge requires a broader approach than counter-proliferation. At the very least, any regulation should extend to 'advanced military technology'.

3. Publish as much justification and detailed information on the extent of the policy as is possible. This must involve an open and transparent admission about the national security purpose of the policy. Universities will rightly be wary of powers or restrictions that they view as 'sweeping' or 'going too far'. Demonstrating that powers are necessary to tackle clearly defined problems is possible but HMG should not fear transparency in demonstrating this. A list of overseas educational institutions whose graduates will not be granted ATAS certificates would allow for an open discussion of HMG's risk balance. HMG must also continue to do more to continue to educate the university sector on the scale of the threats posed by the CCP.

4. Make clear that Chinese students are still very welcome in the UK, but that it is the policies of the Chinese Communist Party and concerns over the aims of the Chinese state that have led to a tightening of the UK system of admission as a risk mitigator.

For it to be effective, ATAS will have to significantly reduce the overall number of risk factors in the UK higher education ecosystem. The scale of these changes will require a significant change in the philosophy that HMG applies to decision-making in this space. National security must be prioritised over and above the short-term economic interest of the university sector. It will also require significant additional investment in the ATAS apparatus. One funding model could see the costs for this enforcement paid by the applicants or the UK university they seek to enrol at. Such a cost could perhaps be offset by greater UK research investment in those fields of science targeted by Beijing, in order to reduce the need for lucrative but high-risk fees from overseas students.

In addition, there is a series of more practical steps that HMG may consider adopting:

- **Cease considering the threat of IP drainage as primarily a counter-proliferation problem.** Counter-proliferation is a serious and present danger. However, it is concerned chiefly with the protection of a narrow and clearly defined set of highly dangerous technologies. IP drainage, on the other hand, is concerned with a far broader range of technologies. HMG should seek to handle these threats as separate – if closely related – concerns. It may be necessary to maintain different structures in order to tackle both.
- **Transfer the responsibility for ATAS to the Home Office.** Immigration controls are the statutory responsibility of the Home Office, a department whose arms-length agencies are responsible for screening applicants and issuing visas. The FCDO's expertise has historically been chiefly that of diplomacy. The Home Office (through its supervision of the Centre for the Protection of National Infrastructure) also supervises the "Trusted Research" scheme which sits alongside ATAS in HMG's ITT strategy. The current split in departmental supervision is presumably also a factor in the fact that the ATAS and visa application processes happen independently of one another.
- **Fuse the ATAS application into the tier-4 visa application process as a single procedure.** The two-stage ATAS certification and visa application process is an unnecessarily bureaucratic and segmented mechanism for approaching this task. It also precludes Entry Clearance Officers from interrogating applicants about information on their ATAS form before making a decision. Merging the two processes into one joint digital application process, in which relevant information from the form could be distributed as necessary, would be a beneficial step.
- **Expand the ATAS questionnaire to require the disclosure of more information.** Currently, the application requires no information on whether the applicant is a member of the CCP, a participant in the TTP (or similar), or has made undertakings related to IP drainage (e.g. "have you agreed to share intellectual property gathered as part of your course or other academic activities with your Government or other entities in your country of residence?"). These missed opportunities preclude the certificating officer from making judgements based on full information. HMG should undertake to require far more information from applicants.
- **Maintain centralised, easily searchable databases of ATAS recipients so that risk factors can be monitored.** Given the need to monitor risk across a pool of thousands of potential threats, HMG must be able to consider commonalities between transfers or suspected transfers of intellectual property. In order to do so, the coordinating department must keep detailed and readily accessible records of applicants for ATAS certificates.

5.2 Enforcement

The other tool the UK possesses to prevent undesired ITT of sensitive IP is enforcement measures.

There is a broader disagreement over the utility or otherwise of openly identifying and prosecuting agents of foreign states. In the past, European powers, including the UK, have sought to target agents of foreign states surreptitiously. Over a number of publications, the Henry Jackson Society has argued that a more open approach ought to be adopted by the UK. [95]

The benefits of extending an open and robust enforcement system to the challenge of unauthorised ITT are straightforward. Firstly, transfers that occur are frequently criminal and it is in the interests of justice that criminality is prosecuted. Secondly – and just as importantly – the spectre of prosecutions would send an important signal both to British universities and to potential agents of hostile states that the Government is serious about responding to the problem.

In building – seemingly from a small base – a system to handle enforcement, the UK could learn from the US system, particularly as it has developed over the past year. The US has brought more than a dozen indictments since the beginning of 2020. The offences charged by the DOJ are also instructive. Frequent use of charges related to dishonesty in application forms (whether for grants or visa applications) is a clearly identifiable strategy. The logic is sensible – evidence of the level needed to secure a criminal conviction can be both difficult and resource-intensive when the 'stolen good' is intangible. However, dishonesty, especially in order to obtain entry to the UK's universities or those of its allies, is a reliable indicator of malice.

Given the possibility of criminality occurring, the UK ought to look to replicate this US model of regular, well-publicised prosecutions for IP theft-related offences.

In addition, as with risk mitigation, there are some more operational changes that HMG may consider adopting:

- **Transfer enforcement responsibility for the policing of offences related to state-orchestrated IP theft to a single body, preferably the National Crime Agency (NCA).** Individuals engaged in unauthorised ITT may commit a number of offences under English law. However, the specialist nature of these offences means that the responsibility for enforcing and investigating them is split across multiple agencies, none of whom have particular counter-intelligence expertise. In the US, the National Security Division of the FBI has a leadership role in enforcing and investigating the full gambit of crimes connected to IP drainage lies. [96] The UK would do well to afford one agency with overall responsibility for countering this form of economic crime, most obviously the NCA. Expertise and intelligence could then be pooled in one central body, which would need to be properly resourced. Transferring responsibility to more conventional law enforcement would also send a signal about the seriousness with which HMG treats this issue.

- **Conduct an urgent audit of ATAS applications made in the past three years to identify dishonest declarations made as part of individual applications.** Submitting dishonest information when applying for an ATAS certificate is a criminal offence under UK law as well as a potential marker of malice. In the US, a string of indictments carrying charges related to visa dishonesty have been brought, and it would be naive to think that similar offences have not taken place in the UK. Reviewing recent applications for dishonesty could help to promptly identify a number of prosecutable individuals

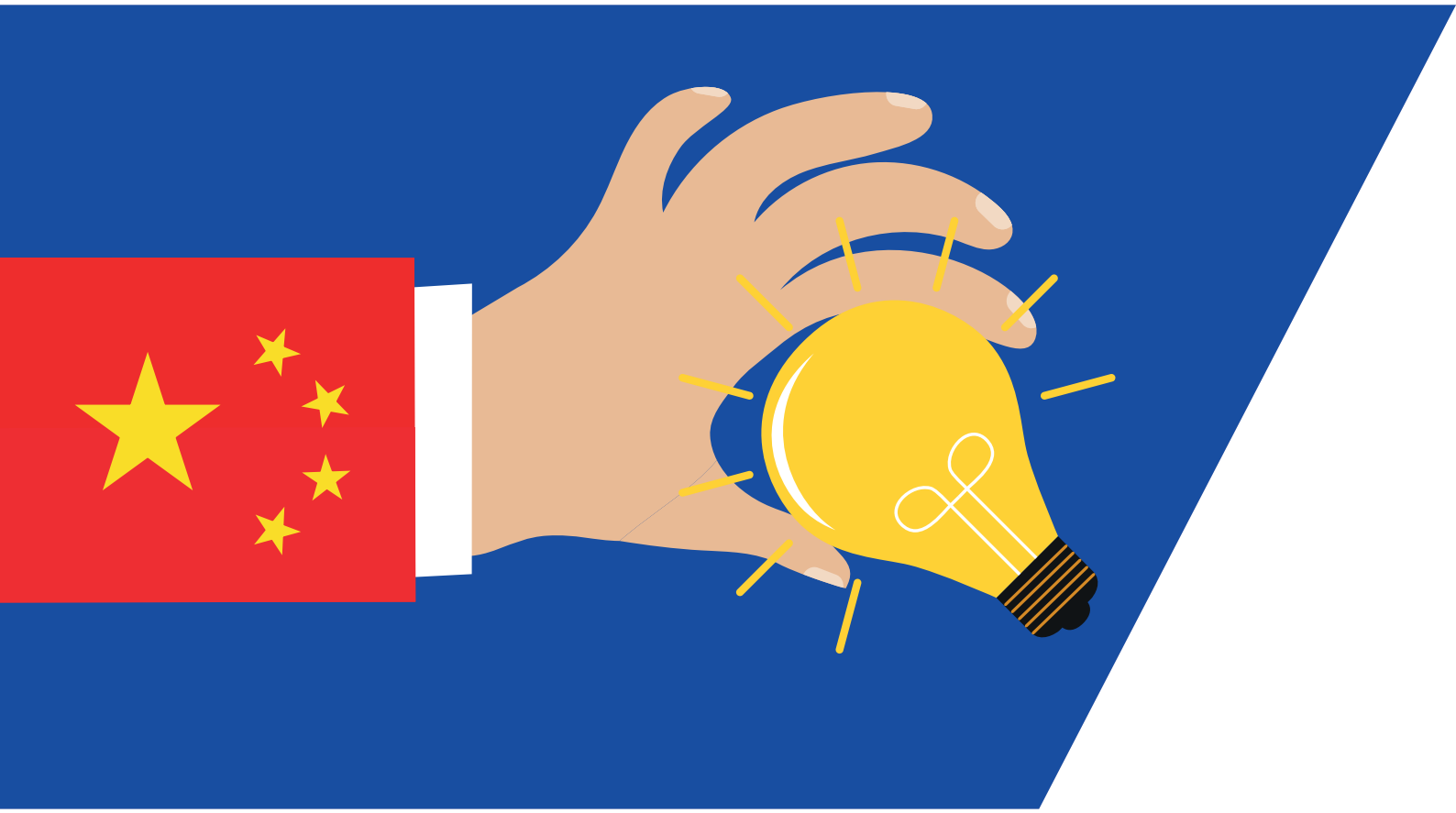
[95] Foxall, A., 'Putin Sees and Hears It All: How Russia's Intelligence Agencies Menace The UK', *The Henry Jackson Society* (2018), available at: https://henryjacksonsociety.org/wp-content/uploads/2018/11/HJS-Putin-Sees-and-Hears-It-All-Report-web.pdf, last visited: 28 September 2020.

[96] Such investigations are, in practice, often conducted in a task-force environment involving representatives of multiple agencies, including those of the Diplomatic Security Service and the Department for Homeland Security.

Title: “BRAIN DRAIN: THE UK, CHINA AND THE QUESTION OF INTELLECTUAL PROPERTY THEFT”
By Sam Armstrong

The Henry Jackson Society
Millbank Tower, 21-24 Millbank
London SW1P 4QP, UK

www.henryjacksonsociety.org



HJS
Henry
Jackson
Society

ASIA
STUDIES
CENTRE

DEMOCRACY | FREEDOM | HUMAN RIGHTS

September 2020