Civitas: Institute for the Study of Civil Society, First Floor, 55 Tufton Street, Westminster, London, SW1P 3QL. For enquiries, please contact Radomir Tylecote.
Tel: +44 (0)20 7799 6677. Email: radomir.tylecote@civitas.org.uk

Towards Strategic Coherence:

A discussion of reform proposals following 'Inadvertently Arming China?'

Dr Radomir Tylecote and Roberto White

July 2021

First published

July 2021

55 Tufton Street

London SW1P 3QL

email: **books@civitas.org.uk**

Independence: Civitas: Institute for the Study of Civil Society is a registered educational charity (No. 1085494) and a company limited by guarantee (No. 04023541). Civitas is financed from a variety of private sources to avoid over-reliance on any single or small group of donors.

All the Institute's publications seek to further its objective of promoting the advancement of learning. The views expressed are those of the authors, not of the Institute.

Summary

Our previous Civitas paper *Inadvertently Arming China?* revealed the widespread sponsorship of scientific research centres in UK universities by Chinese military-linked conglomerates and universities. Research at some of these centres is being sponsored by the British taxpayer.

Some of these conglomerates produce Weapons of Mass Destruction (WMDs) including intercontinental ballistic missiles (ICBMs) and nuclear warheads. Others manufacture strike fighter engines, stealth aircraft, military drones and navy ships.

The risk of the Chinese military sponsorship of UK academia is not just that outputs may be put to use by the Chinese military, but that they create other strategic risks. The Government's Integrated Review of March 2021 ('Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy') discussed how rival states might use economic tools to 'target and undermine the economic and security interests of rivals', highlighting how we should expect 'increased competition for scarce natural resources such as critical minerals, including rare earth elements [which] may be used as leverage on other issues'. This paper proposes detailed solutions to what we have called 'strategic incoherence'.

Sanctions

The UK Government has not yet prevented Chinese military companies from investing in the UK and benefitting from UK-based research, despite their products being put to use by the Chinese state in what is credibly called a genocide in Xinjiang, and supplying regimes including Burma and Syria. A sanctions regime would prevent investment in the UK, including its research facilities.

Academic Technology Approval Scheme (ATAS)

The Academic Technology Approval Scheme (ATAS) has been strengthened. But it should be further reviewed. The central ATAS requirement is to 'ensure that people who are applying to study certain subjects in the UK do not have existing links to WMD programmes'. ATAS should be amended to prevent the entry into the UK of the staff and students of certain military-linked universities, laboratories and conglomerates in China (and equivalents in some other autocracies).

UK equivalent of the Committee on Foreign Investment in the United States (CFIUS)

CFIUS is an inter-agency body, whereas the UK's new Investment Security Unit (ISU) is to be based under the Department for Business, Energy and Industrial Strategy (BEIS), whose priority is liable to be inward investment.

Defence research funding for universities

In the US, Defense Department funding comprises 40 per cent of all engineering research and development (R&D) in universities: the UK may need an equivalent of its Defense University Research Instrumentation Program (DURIP).

The UK should better distinguish between Basic and Applied Research in universities; university departments should also need to outline all the uses research *could* be put to, instead of what they *think* it will be used for.

Five Eyes cooperation

The UK should push to expand university collaboration under the Five Eyes' Technical Cooperation Program. A formal research collaboration programme funded by Five Eyes governments could closely involve leading universities.

Export rules

Some of the Export Control Order (ECO) is unclear. For example, the requirement to '[have] grounds for suspecting' allows considerable leeway. Article 34(3)(a) states that an offence will be committed if the person 'has been informed' that goods (and so forth) 'may be intended for [military] use', but this allows activities to be treated differently depending on the claims of researchers. The system's complexity is a concern in itself: leading lawyers say they do not fully grasp its implications.

University guidance

A number of requirements, such as to 'check whether your potential collaboration partner [has] been involved in activities of potential concern using [e.g.] internet searches' are unreliable.

The 'public domain' exclusion for published research also creates risks: other spin-offs from research that has also produced published papers may help military advancement. This needs clarification that restrictions on other transfers may still apply.

Authors

Dr Radomir Tylecote is Director of the Defence and Security for Democracy (DSD) Unit at Civitas. He is also a Fellow of the Institute of Economic Affairs. He has a PhD from Imperial College London and an MPhil in Chinese Studies from the University of Cambridge.

Roberto White recently finished studying for his BA in Politics and International Studies at the University of Warwick and will be pursuing a Masters in International Relations later this year. His research interests include Chinese policy in Asia and East Asian security studies. He has previously completed internships at the Institute of Economic Affairs and Bright Blue.

NB: None of the academics, researchers, or other staff whose research at UK universities or centres is discussed in this report or previous reports are accused of knowingly assisting the development of the Chinese military, of knowingly transferring information to that end, or of committing any breach of their university regulations. Nor are they accused of any other wrongdoing, or breach of national security, or any criminal offence. In some cases, research may be used solely for non-military ends; the purpose of the examples mentioned in this report is not necessarily to demonstrate that they risk being used for military purposes, but in some cases that the research may simply help improve the business or academic position of a PRC military-linked conglomerate or institution; where research may be put to use by the military of the PRC or organisations which are linked to it, we assume that researchers in the UK will have carried out this research without intending this to happen. Furthermore, none of the UK universities, institutes or funding bodies mentioned in this report are accused of knowingly contributing to the development of China's military or its military industries, as we believe that these universities have developed the sponsorship and research relationships we describe in good faith and in the belief that their scientific outputs will have purely civil ends. Where we discuss possible reforms to laws, regulations, guidelines or university practice, this should not be taken as referring to any of the researchers or research discussed in previous papers.

The purpose of this report is simply to draw attention to the risk that UK research may be exploited by the Chinese military in a way the researchers could never have envisaged. It is our belief that shedding light on this risk is unquestionably a matter of pressing and vital public interest.

Contents

Glossary

AA: Aluminium alloy
ACMT: Advanced Conventional Military Technology
AECC: Aero Engine Corporation of China
AI: Artificial Intelligence
AHV: Air-breathing hypersonic vehicles
ASRI: Aircraft Strength Research Institute (subsidiary of AVIC)
ARIA: Advanced Research and Invention Agency (UK)
ATAS: Academic Technology Approval Scheme
ATD: Advanced Technology Development
AVIC: Aviation Industry Corporation of China
BAMTRI: Beijing Aeronautical Manufacturing Technology Research Institute (former name of MTI, below)
BATRI: Beijing Aircraft Technology Research Institute (subsidiary of COMAC)
BIAM: Beijing Institute for Aeronautical Materials (subsidiary of AECC)
BIS: Bureau of Industry and Security, Department of Commerce (US)
BIT: Beijing Institute of Technology
BUAA/Beihang: Beijing University of Aeronautics and Astronautics
BWC: Biological and Toxin Weapons Convention
CALT: China Academy of Launch Vehicle Technology (subsidiary of CASC)
CASC: China Aerospace Science and Technology Corporation
CCP: Chinese Communist Party
CETC: China Electronics Technology Group Corporation
CGM: Control Momentum Gyroscopes
CGWIC: China Great Wall Industry Corporation
CNT: Carbon nanotube
COMAC: Commercial Aircraft Corporation of China
CQU: Chongqing University
CQUT: Chongqing University of Technology
CSSC: China State Shipbuilding Corporation
CSU: Central South University
DARPA: Defense Advanced Research Projects Agency (US)
DIT: Department for International Trade (UK)
DMU: Dalian Maritime University
DNN: Deep neural networks
DOD: Department of Defense (US)
ECJU: Export Control Joint Unit
ECO: Export Control Order (2008)
EPSRC: Engineering and Physical Sciences Research Council (UK)
FAI: First Aircraft Institute (subsidiary of AVIC)
FAST: Fast light alloys stamping technology
FDI: Foreign direct investment
FML: Fibre-metal laminate

FSS: Frequency selective surface
GNSS: Global Navigation Satellite System/s
GPS: Global Positioning System
HDPE: High-density polyethylene
HEFCE: Higher Education Funding Council for England
HEU: Harbin Engineering University
HfC: Hafnium Carbide
HIT: Harbin Institute of Technology
HUST: Huazhong University of Science and Technology
ICBM: Intercontinental Ballistic Missile
LPD: Low probability of detection
MIMO: Multiple Input Multiple Output
MSS: Ministry of State Security
MTCR: Missile Technology Control Regime
MTI: Manufacturing Technology Institute (subsidiary of AVIC)
NELA: Northeast Light Alloy Company
NCHU: Nanchang HangKong University
NJU: Nanjing University
Norinco: China North Industries Corporation
NPU/NWPU: Northwestern Polytechnic University
NUAA: Nanjing University of Aeronautics and Astronautics
NUDT: National University of Defence Technology (China)
PLA: People's Liberation Army
PRC: People's Republic of China
PZT: Lead zirconate titanate
QMUL/QMES: Queen Mary University of London/Queen Mary Engineering School
SASAC: State-owned Assets Supervision and Administration Commission
SASTIND: State Administration for Science, Technology and Industry for National Defence
SIPRA: China-Scotland Signal Image Processing Research Academy
SOE: State-owned enterprise
TPUN: Thermoplastic polyurethane elastomer nanocomposites
UAV: Unmanned aerial vehicle
UESTC: University of Electronic Science and Technology of China
UHF: Ultra-high frequency
UHSS: Ultra-high strength steel
UHTC: Ultra-high temperature ceramics
UWB: Ultra-wide band
USV: Unmanned submersible vehicle
UUV: Unmanned underwater vehicle
VLFS: Very large floating structures
WA: Wassenaar Arrangement
WMD: Weapons of Mass Destruction
WHUT/WUT: Wuhan University of Technology
WMG: Warwick Manufacturing Group

Introduction

Strategic incoherence

This paper draws on the analysis and conclusions of the lead author's previous Civitas publication, *Inadvertently Arming China? The Chinese military complex and its potential exploitation of scientific research at UK universities*[1] (Radomir Tylecote and Robert Clark, February 2021), and develops the broad recommendations in that paper for the national security reforms the authors believe are necessary (some of these are already underway, albeit in relatively early forms).

The paper *Inadvertently Arming China?* revealed the widespread sponsorship of high-technology research centres in many leading UK universities by Chinese military-linked conglomerates and universities, as well as research collaboration between these centres and their sponsors.

Many of these centres' staff in the UK are former employees or researchers, or graduates, of these Chinese companies and universities; some of their research has been carried out in collaboration with these Chinese military-linked universities and military-sponsored laboratories. Some research is carried out at UK universities; in other cases, research has been carried out at the Chinese universities or companies sponsoring the UK research centre. Most of the cases we analysed were extant; in some cases, the relationships were historic, but these relationships ended only recently.

The report demonstrated that over half of the 24 Russell Group universities' and other UK institutions, have or have had scientific research relationships with Chinese military-linked manufacturers and universities.[2] Research at these UK centres is being sponsored by the UK taxpayer through research councils and Innovate UK.

The UK universities studied (a non-exhaustive list) have established relationships with 22 Chinese military-linked universities, as well as companies. Many of these universities have been deemed 'Very High Risk' in analysis by the Australian Strategic Policy Institute (ASPI).[3] [4]

---

[1] Tylecote, R. and Clark, R. (2021). Inadvertently Arming China? The Chinese military complex and its potential exploitation of scientific research at UK universities. Civitas. February 2021. https://www.civitas.org.uk/publications/inadvertently-arming-china/

[2] This includes, in very limited cases, researcher/s and/or teaching fellow/s at one or more of the constituent colleges of these universities, who are not employed by the university, but merely by a constituent college of that university, and where their research is carried out independently of either the college or university.

[3] Joske, A. (2019). The Chinese Defence Universities Tracker. Australian Strategic Policy Institute, 2019. https://unitracker.aspi.org.au/; Joske, A. (2018). Picking Flowers, Making Honey: The Chinese Military's Collaboration with Foreign Universities. Australian Strategic Policy Institute, 2018. https://www.aspi.org.au/report/picking-flowers-making-honey

[4] This report included statements from the UK institutions analysed: provided they responded to our enquiries, the position of each was represented to the fullest extent possible. We have also told those institutions we did not hear from that we will update the online version of this report to the fullest extent possible, if and when

The companies sponsoring UK-based research centres include China's largest weapons manufacturers, including producers of strike fighter engines, ICBMs, nuclear warheads, stealth aircraft, military drones, tanks, military-use metals and materials, and navy ships. Many of the research projects will naturally have a civilian use, and UK-based researchers will be unaware of a possible dual use that might lead to a contribution to China's military industries.

Examples of research collaborations

Some examples of research cooperation are as follows.

At Heriot-Watt University, one researcher from the PRC cooperated with a researcher affiliated with Harbin Engineering University on research entitled 'Snoopy: Sniffing your smartwatch passwords via deep sequence learning',[5] where UK taxpayers funded research into a password-breaking tool with a leading Chinese military-linked university which is under US sanctions, known to specialise in information security, and whose staff have been charged with espionage. The research speculates: 'in the wrong hands, Snoopy can potentially cause serious leaks of sensitive information'. Another researcher was funded by UK defence groups to work on MIMO Radar.[6] She has researched radar-jamming with China's military-linked Key Laboratory of Radar Imaging and Microwave Photonics, including 'Target Tracking While Jamming by Airborne Radar for Low Probability of Detection',[7] which discussed stealth aircraft avoiding detection.

Warwick Manufacturing Group (WMG) trained one of the pioneers of China's ICBM programme in the 1980s. WMG says that its priorities 'align closely with the main priorities of the State Council's plan', and has boasted that its '[taught] courses have been of benefit to a wide range of organisations [including weapons giant] China North Industries Corporation' (also known as Norinco)[8]. WMG staff have researched with an alloys supplier to the Chinese military, and a military-linked university in high energy-density polymer

---

they contact us. We included any disagreements from the relevant universities; we reiterate that even so, in our view there remains the danger that research, which is carried out in good faith, may be co-opted and exploited by the Chinese military. We also made clear that none of the academics, researchers, or other staff whose research at UK universities or centres is discussed in this report were accused of knowingly assisting the development of the Chinese military, of knowingly transferring information to that end, or of committing any breach of their university regulations. Nor were they accused of any other wrongdoing, or breach of national security, or any criminal offence.

[5] https://dl.acm.org/doi/10.1145/3161196 in Tylecote, R. and Clark, R. (2021).

[6] https://www.udrc.eng.ed.ac.uk/archive/phase-2/people/edinburgh-consortium/mathini-sellathurai in Ibid.

[7] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6165476/ in Ibid.

[8] https://warwick.ac.uk/fac/sci/wmg/education/custom/china/p2477_wmg_in_china_8pp_final_web.pdf in Ibid.

nanocomposites: this research stated that 'functional polymer composites are attracting interest [for] high power weapons.'[9]

Strathclyde hosts a laboratory sponsored by China's leading ICBM manufacturer. A separate Strathclyde centre, for image processing, is backed by Chinese military-linked universities as well as the Royal Society.[10] Strathclyde researchers have cooperated with PRC institutions on research including 'person re-identification' in camera networks (for 'learning deep features'[11]).

A Southampton University researcher has investigated very large floating structures (VLFS) with at least two Chinese military-affiliated institutions.[12] VLFS bases have many civilian uses; they may allow improved sea and air power projection into disputed waters.

Glasgow University has established a joint college with a major military-backed PRC university whose collaborations include with nuclear warhead manufacturer the Chinese Academy of Engineering Physics.[13]

The aims of this paper: developing solutions

The UK Government promised in the Integrated Review that it would 'stop states using … UK academia to develop CBRN [chemical, biological, radiological and nuclear] weapons [and] advanced military technology',[14] but unlike the United States, the UK has not sanctioned Chinese military conglomerates or universities. Without these reforms, dangerous strategic incoherence will continue. China has a long history of weapons sales to regimes that carry out grievous human rights abuses. China's development of a surveillance state is also leading to systematic human rights abuses, with its treatment of the Uighur minority credibly described as genocide.[15]

The methods by which the UK monitors and controls Chinese involvement in UK university research are inadequate. That the UK government and taxpayer may be funding the technological development and therefore force-projection capabilities of the PRC military is not in the UK national interest. The aims of the paper are therefore:

---

[9] https://pubs.rsc.org/en/content/articlelanding/2019/cs/c9cs00043g#!divAbstract in Ibid.
[10] https://www.china-scotland-sipra.org/ in Ibid.
[11] https://ieeexplore.ieee.org/document/9043556 in Ibid.
[12] https://eprints.soton.ac.uk/434022/ in Ibid.
[13] https://www.govinfo.gov/content/pkg/FR-2012-09-19/pdf/2012-22952.pdf in https://unitracker.aspi.org.au/universities/chinese-academy-of-engineering-physics/ in Ibid.
[14] Cabinet Office (2021). The Integrated Review, 16 March 2021. https://www.gov.uk/government/collections/the-integrated-review-2021
[15] International Criminal Responsibility for Crimes Against Humanity and Genocide Against the Uyghurs Population in the Xinjiang Uyghur Autonomous Region. https://14ee1ae3-14ee-4012-91cf-a6a3b7dc3d8b.usrfiles.com/ugd/14ee1a_3f31c56ca64a461592ffc2690c9bb737.pdf

- To **limit the capacities** of the military-linked conglomerates and universities of China (and other expansionist autocratic states) to exploit the research capacities of UK universities to the UK's potential strategic detriment;
- To **prevent UK taxpayer-funding** helping the development of the Chinese armed forces (and theoretically others);
- Because this challenge to UK security has emerged in an environment in which funding to defence research has fallen – leaving many researchers with relevant skills seeking funding from elsewhere – to help **correct the lack of funding** to UK defence research, as well as **to create a more secure environment for research** (noting that in some cases Chinese military-linked institutions appear to have benefitted from UK research funding explicitly intended for defence purposes); and
- To **help universities make up for any shortfall** that may arise from the necessary loss of (some) Chinese funding.

To achieve this, this paper outlines in detail how the UK Government can:

- List those Chinese military-linked companies and institutions to bar from sponsoring science research in UK universities, and entities it wishes to prevent making inward investments generally into the UK (this has been the practice of the US government and continues under the new administration);
- Establish an inter-agency UK equivalent of the Committee on Foreign Investment in the United States (CFIUS);
- Continue to review the Academic Technology Approval Scheme (ATAS) to better control entry to the UK of international students; and
- While it is important to preserve academic freedom, to assess whether some of what is currently deemed 'basic scientific research', or research with findings in the public domain may have possible dual-uses in sanctioned countries including China, and where approval for research centres may have allowed projects which are exposed to this risk to take place.

NB: None of the academics, researchers, or other staff whose research at UK universities or centres is discussed in this report or previous reports are accused of knowingly assisting the development of the Chinese military, of knowingly transferring information to that end, or of committing any breach of their university regulations. Nor are they accused of any other wrongdoing, or breach of national security, or any criminal offence. In some cases, research may be used solely for non-military ends; the purpose of the examples mentioned in this report is not necessarily to demonstrate that they risk being used for military purposes, but in some cases that the research may simply help improve the business or academic position of a PRC military-linked conglomerate or institution; where research may be put to use by the military of the PRC or organisations which are

linked to it, we assume that researchers in the UK will have carried out this research without intending this to happen. Furthermore, none of the UK universities, institutes or funding bodies mentioned in this report are accused of knowingly contributing to the development of China's military or its military industries, as we believe that these universities have developed the sponsorship and research relationships we describe in good faith and in the belief that their scientific outputs will have purely civil ends. Where we discuss possible reforms to laws, regulations, guidelines or university practice, this should not be taken as referring to any of the researchers or research discussed in previous papers.

The purpose of this report is simply to draw attention to the risk that UK research may be exploited by the Chinese military in a way the researchers could never have envisaged. It is our belief that shedding light on this risk is unquestionably a matter of pressing and vital public interest.

Chapter 1: The context of Chinese military expansion

China's military expansion and civil-military fusion

These relationships need to be understood in the context of China's stated aim to equal the US military by 2027. This would have far-reaching consequences for the UK, its allies, and other democracies.

The technological development of the People's Liberation Army (PLA) should also be set against the wider background of the increasingly hawkish strategy of, and strategic thinkers around, President Xi Jinping, as well as the authoritarian entrenchment of the state in China. China's research and development for next-generation military technology should be understood in this strategic context.

One element driving the growth in military technology in China is the mandated integration and joint development of military and civilian technology sectors, or 'civil-military fusion', which Beijing hopes will provide the PLA with a critical advantage in adapting emerging technologies, to be used by the military across technological fields. This integration means it is significantly more difficult to ascertain that research done for the civilian division of a military-linked Chinese conglomerate, or even a civilian-based department of a military-backed university, will not ultimately be used by the military.

China has an extensive record providing weapons to unstable, authoritarian regimes that routinely abuse human rights. For example, China has supplied military materiel to the Syrian regime; it has provided Burma with weapons including FN-6 surface-to-air missiles,[16] 107mm surface-to-surface rockets,[17] JF-17 aircraft,[18] armoured vehicles,[19] and possibly drones.[20] In Afghanistan, Chinese weapons are routinely used by the Taliban, including surface-to-air missiles and anti-aircraft guns.[21] Lastly, Chinese companies and organisations are suspected of having aided countries like Iran and North Korea in their pursuit of nuclear weapons.[22]

The Chinese military's force-projection capacity is growing, and it is committing more resources to researching destabilising materiel such as directed-energy weapons and hypersonic missiles. China's evolution into a surveillance state is already resulting in systematic human rights abuses.

---

[16] https://asiatimes.com/2019/11/chinas-mobile-missiles-on-the-loose-in-myanmar/ in Tylecote, R. and Clark, R. (2021).
[17] *Ibid*.
[18] https://thediplomat.com/2014/06/burma-to-purchase-chinese-pakistani-jf-17-fighter-jets/ in Ibid.
[19] https://www.burmalibrary.org/en/armed-and-dangerous-myanmars-military-goes-shopping in Ibid.
[20] https://thediplomat.com/2016/06/is-myanmar-using-armed-chinese-drones-for-counterinsurgency/ in Ibid.
[21] https://www.telegraph.co.uk/news/worldnews/1562148/Chinese-weapons-reaching-the-Taliban.html in Ibid.
[22] Tylecote, R. and Clark, R. (2021).

During the last generation, and especially during the leadership of Xi Jinping, China has reportedly carried out a doctrinal 'revolution in military affairs' (RMA), adopting an approach called 'asymmetric innovation'.[23] Instead of pursuing an expensive 'catch-up' with major 'big-kit' western defence systems, China is now adopting a different strategy. This comprises assembling major systems by using its heavy manufacturing capability (such as submarines, warships, and strike aircraft, where China will have $1 trillion to use on navy and air force procurement until 2030[24]), but focusing most of its innovation efforts on 'asymmetric defence technologies'. These include but are not limited to: cyber-warfare capability including paralysing attacks on core infrastructure; satellite and anti-satellite weapons; directed energy and electromagnetic pulse (EMP) systems; and global logistics disruption systems.[25]

Hypersonic missiles research: an example of strategic incoherence and advanced military technology

The Government's recent announcement in the Defence Command Paper of 23 March 2021 (which followed the Integrated Review of UK defence and security of 16 March) that it plans to spend billions on 'novel weapons' including hypersonic missiles, with defence chiefs worried by China and Russia's development of these new arms, demonstrates the strategic questions hanging over the research relationships we described. Hypersonic missiles are a core part of what the Government calls 'the threat': the Government notes how they allow 'conventional or nuclear warheads' to be delivered 'with very little warning'.[26]

Hypersonics are also at the centre of a new arms race, in which the US, and now the UK, are trying to match the capacities of China and Russia. Winning it has been called 'the first priority' in western defence security.

The term 'hypersonic missiles' refers to weapons that can navigate and travel five times faster than the speed of sound. These missiles have been labelled potentially 'massively destabilising': a study by *The New York Times* and Center for Public Integrity described them as a 'revolutionary new type of weapon [that would] strike almost any target in the world within a matter of minutes'.[27]

---

[23] *Ibid*.
[24] Crane, K. et al (2005) in Pillsbury, 2015 (in *Ibid*.)
[25] Discussed in Chang Mengxiong, 'Weapons of the 21st Century', *China Military Science*, 30:1, 1995, pp.19-24. in Pillsbury, 2015 (in *Ibid*.)
[26] The material in this section was first discussed in Tylecote, R. (2021), 'Novel weapons', *The Critic*, 21 March 2021 https://thecritic.co.uk/the-problem-with-chinas-hypersonic-missiles/, based on Tylecote and Clark (2021).
[27] Smith, R.J. 'Hypersonic Missiles Are Unstoppable. And They're Starting a New Global Arms Race.' *New York Times*, 29 June 2019. https://www.nytimes.com/2019/06/19/magazine/hypersonic-missiles.html in *Ibid*.

In March 2018, General John E. Hyten, Commander of US Strategic Command, told the Senate Armed Services Committee that 'We don't have any defence that could deny the employment of such a weapon against us'.[28] Gen. Hyten added that China 'has flight-tested its own hypersonic missiles at speeds fast enough to reach Guam from the Chinese coastline within minutes'.

Even so, our analysis demonstrated that some UK universities may have already spent years unknowingly helping China develop hypersonics;[29] the Government's statement in the Defence Command Paper that followed stated that hypersonic missiles show how 'our historic technological advantage is being increasingly challenged by targeted investments in capabilities designed to counter our strengths'.

Manchester University provided the China Aerospace Science and Technology Corporation (CASC), China's primary inter-continental ballistic missile (ICBM) conglomerate, with a research centre that was subsidised, like many others, by the UK taxpayer.[30] (Manchester states that the centre recently closed.) The former centre's hypersonic-based research included a paper depicting missiles converging on the same target.[31] (As Juliet Samuel, covering our paper for *The Daily Telegraph* put it: '[T]he paper, published in 2018, offers one way to solve the "cooperative simultaneous arrival problem". In plain English, that's when you want to point lots of missiles or rockets at a target and have them go boom at the same time.'[32])

Furthermore, the centre has collaborated with defence-funded Tianjin University on variable geometry inlets, whose purpose is to generate more powerful thrust ('favourable, it says, 'to the acceleration and manoeuvring flight'[33] [sic]). In the United States, variable geometry inlets appear in patents, developed by defence firms, that relate to hypersonic missiles.[34] The US is already hastening to develop this type of missile, with the Defense Research Advanced Projects Agency (DARPA) expected to conduct tests this year.[35]

One of the greatest obstacles in hypersonic missiles research is managing the extreme heat from the friction caused by flying at such speeds. Consequentially, researchers are searching for solutions in coatings.

---

[28] https://www.nytimes.com/2019/06/19/magazine/hypersonic-missiles.html

[29] We also emphasised here our belief that all the UK-based research we analysed had been intended for civilian use.

[30] https://web.archive.org/web/20191203090318/http://www.aerospace.manchester.ac.uk/our-research/sino-british-control-lab/ In https://www.aspi.org.au/report/china-defence-universities-tracker

[31] https://www.research.manchester.ac.uk/portal/files/65368508/2018TCST_Preprint.pdf

[32] Samuel, J. 'Finally we are waking up to how our universities may be arming China'. *The Telegraph*, 13 February 2021. https://www.telegraph.co.uk/politics/2021/02/13/finally-waking-universities-may-arming-china/

[33] https://www.research.manchester.ac.uk/portal/files/57550117/2017AESCTE_Preprint.pdf

[34] https://patents.google.com/patent/US4620679A/en

[35] https://www.thedrive.com/the-war-zone/37465/new-images-of-chinese-bomber-carrying-huge-mystery-missile-point-to-hypersonic-capability

The Manchester Graphene Aerospace Materials Centre has conducted research on potential uses for graphene and other materials in aerospace. The Centre receives funding from the Beijing Institute of Aerospace Materials (BIAM), a military and civilian manufacturer and subsidiary of the Aero Engine Corporation of China (AECC), China's largest military aircraft engine manufacturer. Recent reports indicate BIAM's researchers have developed graphene armour for China's newest military attack helicopter,[36] although there is no suggestion this was done in collaboration with Manchester University.

Nonetheless, some research from these Chinese-sponsored UK centres is unambiguous about its military potential. After a Chinese researcher from Manchester University joined a counterpart at Central South University (CSU), an institution with links to the Chinese military, to create a new ceramic coating, Manchester itself highlighted its 'new kind of ceramic coating that could revolutionise hypersonic travel for air, space and defence purposes', and commented how 'ultra-high temperature ceramics (UHTCs) are needed in aero-engines and hypersonic vehicles such as rockets, re-entry spacecraft and defence projectiles.'

Manchester remarked that the new material was partly manufactured at CSU's 'Powder Metallurgy Institute': the 'State Key Laboratory for Powder Metallurgy' is known to be a major defence laboratory.[37] The breakthrough was published in a paper that said: 'Ultra-high temperature ceramics are desirable for applications in the hypersonic vehicle, rockets, re-entry spacecraft and defence sectors…potential uses may include… defence army…'.[38]

Meanwhile, in November 2020, images appeared in the media depicting a Chinese H-6N aircraft carrying a missile whose features may 'be air-breathing and nuclear capable'.[39] Its shape resembled the DF-17 experimental hypersonic missile, which is also manufactured by a subsidiary of another Manchester sponsor, CASC.[40] The H-6N is assembled by a subsidiary of the Aviation Industry Corporation of China (AVIC), China's primary military aircraft supplier, which provides the PLA Air Force with its next-generation stealth fighter and strategic bomber.[41] AVIC is a major shareholder in the Aero Engine Corporation of China (AECC), whose subsidiary BIAM sponsors the hypersonic research conducted at Manchester.[42]

---

[36] https://www.defenseworld.net/news/23505/China_Flies_Graphene_armored_Z_10_Attack_Helicopter
[37] https://unitracker.aspi.org.au/universities/central-south-university/
[38] https://www.nature.com/articles/ncomms15836
[39] https://www.thedrive.com/the-war-zone/37465/new-images-of-chinese-bomber-carrying-huge-mystery-missile-point-to-hypersonic-capability
[40] https://www.thedrive.com/the-war-zone/30119/four-of-the-biggest-revelations-from-chinas-massive-70th-anniversary-military-parade
[41] https://www.globaltimes.cn/content/1204238.shtml
[42] https://web.archive.org/web/20171127182732/http://www.guancha.cn/Industry/2016_06_13_363868.shtml in https://unitracker.aspi.org.au/universities/aero-engine-corporation-of-china/

AVIC also sponsors the AVIC Centre for Structural Design and Manufacturing at Imperial College London. At Imperial, BIAM funds the Imperial Centre for Materials Characterisation, Processing and Modelling.[43] These centres exhibit the scope of the Chinese-sponsored research that includes – and extends well beyond – hypersonics projects. In the United States, all these Chinese military-linked companies are under sanctions.

[43] https://www.imperial.ac.uk/avic-design/people/zhusheng-shi/

Chapter 2: Solutions for UK university research security

This chapter analyses the security-related reforms which we believe recent revelations about UK universities and the Chinese military have demonstrated are needed. Next, we discuss possible specific reforms derived from our findings in the previous paper.

Sanctions

The United States has the most developed system of restrictions on investments, in particular those the US government believes pose a threat to national security. The US maintains four main lists (the Entity List and more specific lists) which have recently been extended to cover some of China's most widely known multinational corporates, including Huawei Technologies.[44] The lists function as follows.

The Entity List (Department of Commerce)

Companies on this list are prohibited from doing business with American firms without a US government license, which effectively, if not totally, bars them from economic cooperation. The list was started in 1997 to help prevent US companies aiding the creation of weapons of mass destruction (WMDs). The list's expansion since then has been designed to include commercial activities 'contrary to the national security or foreign policy interests of the United States.'[45] The list targets 'businesses, research institutions, government and private organizations, individuals, and other types of legal persons'[46] and is administered as part of the US Export Administration Regulations by the Bureau of Industry and Security of the Commerce Department.

The Military Companies List (Department of Defense)

Companies placed on the list have direct ties to the Chinese military and are 'off-limits for investment by Americans.'[47] The Pentagon was granted permission to publish a list of 'Communist Chinese military companies operating in the United States' by the National Defense Authorization Act 1999, and finally did so under the previous Trump Administration.

Using authority granted by the International Emergency Economic Powers Act of 1977, President Trump banned US investment in a number of companies (giving time for

[44] Lam, E. and Ossinger, J. (2021). 'What Do the Two U.S. Blacklists of Chinese Companies Do?' *Bloomberg Quint*, 15 January 2021. https://www.bloombergquint.com/onweb/what-do-the-two-u-s-blacklists-of-chinese-companies-do-q-a#:~:text=Inclusion%20on%20the%20Entity%20List,build%20weapons%20of%20mass%20destruction

[45] Ibid.

[46] The Commerce Department's Bureau of Industry and Security, in Ibid.

[47] Ibid.

shareholders to divest). In its final days, the Trump Administration added nine Chinese companies, including aerospace manufacturer Commercial Aircraft Corporation of China (Comac).[48]

The Military End-User List (Department of Commerce)

In December 2020, the Commerce Department established the new 'MEU' List under the Export Administration Regulations (EAR) with an initial 57 Chinese and 45 Russian entities, building on the June 2020 amendment to the EAR that widened restrictions on the 'export, reexport, and in-country transfer of items to military end users and for military end uses in China, Russia, and Venezuela'. The new MEU list is intended to 'ease the compliance burden on the public'.[49]

The list identifies 'foreign parties that are prohibited from receiving [certain items][50] unless the exporter secures a license.' These companies are identified by the US Government as 'military end users',[51] representing what the Department calls 'an unacceptable risk of use in or diversion to a "military end use" or "military end user" in China, Russia, or Venezuela'. The list is not exhaustive: exporters, re-exporters, or transferors must conduct their own due diligence for entities not identified.[52] [53]

Non-SDN Chinese Military-Industrial Complex Companies List (NS-CMIC list) (US Treasury)

The Non-SDN[54] Chinese Military-Industrial Complex Companies List (NS-CMIC list) is described in a 3 June 2021 Executive Order from President Biden aimed at 'further address[ing] the ongoing national emergency declared in Executive Order (EO) 13959 of November 12, 2020 with respect to the threat posed by the military-industrial complex of the People's Republic of China (PRC).'

To prevent 'indirect' investment, in January 2021, Executive Order 13959 restricted Americans from investing in US or foreign securities, including Exchange Traded Funds or mutual funds that hold any publicly traded securities of an 'Office of Foreign Assets Control

[48] Shepardson, D. et al (2021). 'Trump administration takes final swipes at China and its companies'. Reuters, 14 January 2021. https://www.reuters.com/business/energy/trump-administration-takes-final-swipes-china-its-companies-2021-01-15/

[49] U.S. Department of Commerce Establishes Military End User List. Jones Day, February 2021. https://www.jonesday.com/en/insights/2021/02/us-department-of-commerce-establishes-military-end-user-list

[50] Described in Supplement No. 2 of Part 744 of the EAR.

[51] Defined in Section 744.21(g) of the EAR.

[52] Bureau of Industry and Security, Department of Commerce, 2020. *Military End User (MEU) List*. https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/1770

[53] Burke, R. et al (2021). *US Commerce Department issues 'Military End User' List*. White and Case, 7 January 2021. https://www.whitecase.com/publications/alert/us-commerce-department-issues-military-end-user-list Hong Kong has also been removed as a separate destination and is largely subjected to the same requirements and restrictions as China.

[54] Specially Designated National

(OFAC)-listed CCMC (regardless of the CCMC securities' share of the underlying fund or derivative thereof).' [55] [56] [57]

President Biden's Executive Order (EO) is intended to restrict 'the use of Chinese surveillance technology outside the PRC, as well as the development or use of Chinese surveillance technology to facilitate repression or serious human rights abuses', which 'constitute unusual and extraordinary threats.' It allows the US to prohibit American investments in Chinese firms that may 'undermine the security or democratic values of the United States and our allies.'

The Executive Order will:

> 'strengthen [the] previous EO [which] prohibit[s] US investments in the military-industrial complex of the People's Republic of China [EO 13959] by creating a sustainable and strengthened framework for imposing prohibitions on investments in Chinese defense and surveillance technology firms.'

It prohibits US persons from:

> 'engaging in the purchase or sale of any publicly traded securities of any person listed in the Annex to the E.O. or determined by the Secretary of the Treasury, in consultation with the Secretary of State, and, as the Secretary of the Treasury deems appropriate, the Secretary of Defense: to operate or have operated in the defense and related materiel sector or the surveillance technology sector of the economy of the PRC; or to own or control, or to be owned or controlled by, directly or indirectly, a person who operates or has operated in any sector described above, or a person who is listed in the Annex to this E.O. or who has otherwise been determined to be subject to the prohibitions in this E.O.'

The EO is designed to make sure that American investment does not support Chinese companies that may undermine US security (or, notably, values) and is also explicitly intended to prevent investment supporting China's military sector, including the 'Chinese surveillance technology firms that contribute — both inside and outside China — to the

[55] Bombach, K.M. et al (2021). 'U.S. Prohibits Trading in Securities of Communist Chinese Military Companies, but NYSE Reverses Plan to Delist'. *Greenberg Traurig*, 4 January 2021. https://www.gtlaw.com/en/insights/2021/1/us-prohibits-trading-in-securities-of-communist-chinese-military-companies

[56] Other relevant executive orders are Executive Order 13959 (Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies (November 12, 2020)), amended by 13974 (Amending Executive Order 13959–Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies (January 13, 2021)).

[57] The United States also operates the Specially Designated Nationals and Blocked Persons List, which we do not cover here.

surveillance of religious or ethnic minorities or otherwise facilitate repression and serious human rights abuses.'[58]

President Biden listed the prohibited 59 entities, including firms he called 'defence-related', such as the Aero Engine Corporation of China, Aviation Industry Corporation of China, Ltd. (and its subsidiaries), China Academy of Launch Vehicle Technology, China Aerospace Science and Technology, China Electronics Technology Group Corporation, China North Industries Group Corporation Limited and Huawei (all of whose sponsorship of UK universities is described in our previous paper); as well as Hikvision and others.[59] As with the other US sanctions, appearing on one list does not preclude a company appearing on others.

The overall framework of sanctions on Chinese military companies draws on various legal authorities, in executive orders and legislation passed by Congress, some codified as regulation under the Office of Foreign Assets Control (OFAC) at the US Treasury. [60] [61]

Eight out of the 10 Chinese military companies we previously documented are under some form of US sanctions, all as Chinese military companies or military end-users; the two that are not under sanction are Shougang Steel and the Northeast Alloy Company. In Shougang's case the vast majority of its steel products are for civilian use. Northeast Alloy Company is a minor company compared to those sanctioned, and combined, these two constitute a tiny fraction of the sponsorship and/or broader relationships that we studied. This means the vast majority of Chinese military-linked sponsorship of UK universities comes from companies that are under sanctions in the United States.

Summary of possible reforms

The Government has declined to prevent Chinese military companies from investing in the UK and from benefitting from UK-based research, despite some of their equipment apparently being put to use by the Chinese state in what is credibly called a genocide in Xinjiang, and their supplying of other regimes with grievous human rights records, including Burma and Syria. In the United Kingdom, the Sanctions and Anti-Money Laundering Act 2018[62] now includes 'human rights violations' as a reason for imposing sanctions on a

[58] White House Briefing Room. Fact Sheet: Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China. 3 June, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/03/fact-sheet-executive-order-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/

[59] Office of Foreign Assets Control. Non-SDN Chinese Military-Industrial Complex Companies List. 16 June 2021. https://www.treasury.gov/ofac/downloads/ccmc/nscmiclist.pdf

[60] Non-SDN Chinese Military-Industrial Complex Companies List (NS-CMIC List). US Department of the Treasury, 16 June 2021 https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/ns-ccmc-list; Chinese military companies sanctions, US Department of the Treasury, 2021. https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/chinese-military-companies-sanctions

[61] US Sanctions lists: https://sanctionssearch.ofac.treas.gov/

[62] Sanctions and Anti-Money Laundering Act 2018. UK Parliament. https://www.legislation.gov.uk/ukpga/2018/13/contents/enacted/data.htm

person or an entity,[63] a clear basis to begin sanctioning companies linked to the Chinese military, even beyond the national security hazards we have raised.

Besides the long-term challenge of Chinese military expansion, the Government may also investigate equivalent risks posed by companies from other 'systemic challengers' such as Russia.

The most sensible approach may be to create a combined list that prevents investment in the United Kingdom and its research facilities, military end-use transfers, and investment by Britons in these companies. This list should include companies involved in surveillance technologies and research.

Entry of scientific researchers to the United Kingdom

The Academic Technology Approval Scheme (ATAS) is a UK entry-control certification scheme for international students who intend to study sensitive subjects at postgraduate level (and some undergraduate courses with an integrated master's year). Some occupations also fall under ATAS, including chemical and mechanical engineers, laboratory technicians and aircraft maintenance workers.[64] [65] The nationals of European Union (EU) or European Economic Area (EEA) countries and Australia, Canada, Japan, New Zealand, Singapore, South Korea, Switzerland, or the United States and those applying for Global Talent Visas are exempt.

ATAS-regulated fields have included those where a student's knowledge could be used to develop Advanced Conventional Military Technology (ACMT) or Weapons of Mass Destruction (WMDs) or their means of delivery, and the scheme is designed to help prevent the spread of '*knowledge and skills* that could be used in the proliferation of WMD and their means of delivery through advanced education' [our italics].[66] The UK Government regards WMDs as including:

---

[63] Smith, B. and Dawson, J. *Research Briefing: Magnitsky legislation.* House of Commons Library, 20 July, 2020. https://commonslibrary.parliament.uk/research-briefings/cbp-8374/

[64] Home Office. *Immigration Rules Appendix ATAS: Academic Technology Approval Scheme (ATAS)*. Updated 21 May 2021. https://www.gov.uk/guidance/immigration-rules/immigration-rules-appendix-atas-academic-technology-approval-scheme-atas

[65] Home Office. *Statement of changes to the Immigration Rules*, 4 March 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/966644/CCS001_CCS0221107260-001_Statement_of_changes_in_Immigration_Rules__Web_Accessible_.pdf

[66] Association of University Legal Practitioners and Project Alpha of King's College London (2015). *Higher Education Guide And Toolkit On Export Controls And The ATAS Student Vetting Scheme*. (In partnership with the Export Control Organisation and the Foreign and Commonwealth Office). Version 1, 2 April 2015. https://www.research-operations.admin.cam.ac.uk/files/policies_and_procedures/export_control_guide_july_2015.pdf

- Nuclear weapons programmes and nominally civil nuclear programmes suspected of being intended to support nuclear weapons ambitions;
- Biological weapons;
- Chemical weapons; and
- Ballistic and cruise missiles (and so forth; due to their potential use in delivering the above weapons), including unmanned large aerial vehicles, space launch vehicles and sounding rockets.[67]

Following amendments in 2021, a broader range of subjects have come under the scheme, including certain materials sciences, biological sciences, subjects allied to medicine, and fields of engineering, mathematics and computing.[68]

Following the recommendations in the previous Civitas paper, the Integrated Review stated that: 'Improvements to the Academic Technology Approval Scheme will help to stop states from using research relationships with UK academia to steal intellectual property and obtain knowledge that could be used to develop CBRN weapons and their means of delivery, or advanced military technology'.[69] However, that ATAS is designed 'to ensure that people who are applying to study certain subjects in the UK do not have existing links to WMD programmes',[70] implies more reforms are needed to prevent their entry to the United Kingdom.

Summary of possible reforms

We recommend that the Academic Technology Approval Scheme (ATAS) is further reviewed to better control entry to the UK for international students whose research may create risks in sensitive fields. The central requirement that ATAS 'ensure that people who are applying to study certain subjects in the UK do not have existing links to WMD programmes' does not fully take into account that it is typically impossible to know how knowledge acquired in the UK may be used in the military-linked universities where staff may officially have worked in civilian programmes but may participate in WMD-linked (and other arms-linked) programmes. ATAS should be amended to prevent the entry into the UK of the staff and students of closely military-linked universities, laboratories and conglomerates in China (as well as the equivalents in other strategic-challenger autocracies).

---

[67] *Ibid*.
[68] Imperial College London (2021). Academic Technology Approval Scheme (ATAS) – for international researchers. https://www.imperial.ac.uk/human-resources/compliance-and-immigration/immigration/academic-technology-approval-scheme-atas/; Home Office. *Immigration Rules Appendix ATAS: Academic Technology Approval Scheme (ATAS)*. Updated 21 May 2021. https://www.gov.uk/guidance/immigration-rules/immigration-rules-appendix-atas-academic-technology-approval-scheme-atas
[69] Cabinet Office (2021). *The Integrated Review*, 16 March 2021. https://www.gov.uk/government/collections/the-integrated-review-2021
[70] Association of University Legal Practitioners and Project Alpha of King's College London (2015).

A UK version of the Committee on Foreign Investment in the United States (CFIUS)

The UK Government is planning an equivalent of the Committee on Foreign Investment in the United States (CFIUS). We analyse how CFIUS and its Australian counterpart function, before making recommendations for how the UK version might operate, while highlighting concerns about the current plans.

CFIUS was established in 1975 by President Gerald Ford[71] and is an interagency committee authorised to review foreign investments in the United States for possible national security risks, including some real estate transactions.

CFIUS is designed to be an interagency organisation. Its chair is the Secretary of the Treasury and is members include the Secretaries of the Departments of Justice, Homeland Security, Commerce, Defense, State, Energy, Education, and the Office of the U.S. Trade Representative and Office of Science and Technology Policy. A cluster of White House offices also observe and sometimes participate in CFIUS activities: the Office of Management and Budget; Council of Economic Advisors; National Security Council; National Economic Council; and Homeland Security Council.

To decide whether transactions are national security concerns, CFIUS generally considers whether:

- The US business has contracts with US government agencies involved in national security;
- The US business has (or has had) classified contracts;
- The US business possess or deals with critical technologies or products, including but not limited to commodities, software, or technology under export control laws;
- The transaction would result in foreign control over physical or virtual 'critical infrastructure'; and
- The US business has any offices or facilities in locations near sensitive government facilities such as military bases and national laboratories.[72]

CFIUS may review 'covered transactions', meaning proposed or pending transactions with any foreign person which could result in control of US business by a foreign person.[73] CFIUS

[71] Through Executive Order 11858, pursuant to section 721 of the Defense Production Act 1950.
[72] *Committee on Foreign Investment in the United States: CFIUS Overview.* Cooley LLP, 2021. https://www.cooley.com/services/practice/export-controls-economic-sanctions/cfius-overview
[73] *Ibid*. Transactions include mergers, acquisitions, joint ventures, leases, and other investments. Foreign persons are defined as a foreign national, foreign government or foreign entity, including a partnership,

was also augmented by the Foreign Investment Risk Review Modernization Act 2018 (FIRRMA) to widen the abilities of the President and CFIUS itself to review *non-controlling investments* and real estate transactions and respond, including the capacity to suspend or prohibit transactions.[74] The Office of Investment Security Monitoring & Enforcement administers penalties and orders from CFIUS (and researches notified and non-declared transactions).

CFIUS, universities and research security

Strategic Competition Act 2021

The Strategic Competition Act 2021 made the Secretary of Education a member of CFIUS and will require CFIUS to review the national security implications of US universities' foreign contracts and gifts, including single or combined gifts of $1 million or more, when related to 'research, development, or production of critical technologies and [which] provid[e] the foreign person potential access to any material non-public technical information' held by those institutions.' This includes gifts with conditions attached, including 'the creation of a research programme or the assignment of certain employees.'

- **Protecting Critical Technology Task Force (PCTTF)**

Following a changed 'top-level view of the threat to U.S. academic research' at the Department of Defense (DOD)[75] in October 2018, General Mattis also established the DOD Protecting Critical Technology Task Force (PCTTF). Mattis outlined[76] his commitment to protecting the Department's critical technology:

> 'Each year, it is estimated that American industry loses more than $600 billion dollars to theft and expropriation. Far worse, the loss of classified and controlled unclassified information is putting the Department's investments at risk and eroding the lethality and survivability of our forces.'

The cross-functional task force will report to the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff (VCJCS) and brings in staff from across the military. Senators also outlined the need for Congressional assistance to PTCCF to 'screen researchers involved in DOD-funded grants' to protect academic research from 'foreign

---

corporation, trust, or other entity organised abroad. Control is taken to mean the power, exercised or not, to 'directly or indirectly determine, direct, or decide important matters affecting the US business'.

[74] Jalinous, F. et al (2018). *CFIUS Reform Becomes Law: What FIRRMA Means for Industry*. White and Case. https://www.whitecase.com/publications/alert/cfius-reform-becomes-law-what-firrma-means-industry

[75] Kenlon, F. (2019). Protecting DoD-Funded Research in Universities and Research Centers (Blog post, October 18, 2019). Defence Acquisition University. https://www.dau.edu/training/career-development/intl-acq-mgmt/blog/Protecting-DoD-Funded-Research-in-Universities-and-Research-Centers

[76] Secretary of Defense, 24 October 2018. Memorandum. https://www.dau.edu/cop/iam/_layouts/15/WopiFrame.aspx?sourcedoc=/cop/iam/DAU%20Sponsored%20Documents/DoD%20Protecting%20Critical%20Technology%20Task%20Force%20Memo%2010-24-18.pdf&action=default

threats'[77] and 'to improve research protection to guard against foreign government exploitation that intentionally targets US and allied partner research and intellectual capital'.[78]

- **Joint Committee on the Research Environment (JCORE)**

In 2019 the White House Office of Science and Technology Policy also announced its leadership of a new interagency **Joint Committee on the Research Environment (JCORE)**, where DOD is a participant. JCORE will monitor and advise on disclosure requirements for federally funded research, best practice for research institutions and risk identification and assessment[79] (since March 2019, all DOD grant-funded research staff must disclose all funding sources, current and pending projects, and time commitments).[80]

The United States has also recently enacted a cluster of other laws and regulations to grant further protection for scientific research.

- **Proclamation 10043-May 29, 2020**. This suspended entry of any (non-immigrant) national of the PRC seeking to enter the US[81] to study or conduct research in the United States who currently 'receives funding from or who currently is employed by, studies at, or conducts research at or on behalf of… an entity in the PRC that implements or supports the PRC's 'military-civil fusion strategy',' or in the past 'has been employed by, studied at, or conducted research at or on behalf of... an entity in the PRC that implements or supports the PRC's "military-civil fusion strategy"'. The proclamation 'focuses on the specified connections with PRC entities that implement or support the PRC's effort "to acquire and divert foreign technologies, specifically critical and emerging technologies, to incorporate into and advance the PRC's military capabilities"'[82] (broadly similar to ATAS).

The **Safeguarding American Innovation Act (SAIA) 2021**. This Act was introduced by the Senate in a bipartisan effort to protect US national and economic security by targeting efforts made by foreign states to attack research activities. The Bill is yet to become law but is designed to authorise new limits on visiting foreign scientists, make certain grant

[77] Undersecretary of Defense, 1 July 2019 Memorandum. https://www.dau.edu/cop/iam/_layouts/15/WopiFrame.aspx?sourcedoc=/cop/iam/DAU%20Sponsored%20Documents/USD%20R-E%20Ltr%20to%20Sen%20Grassley%20on%20Foreign%20Threats%20to%20Taxpayer%20Funded%20Research%207-1-2019.pdf&action=default

[78] Another Memorandum from the Undersecretary of Defense, 10 October 2019; also outlined in a 16 September 2019 letter (Dr Kevin Droegemeier, Director of the White House Office of Science and Technology Policy (OSTP)).

[79] *Ibid*.

[80] Secretary of Defense, 24 October 2018. Memorandum.

[81] Pursuant to an F or J visa

[82] NAFSA: Association of International Educators (2021). *Proclamation Suspending Entry of Chinese Students and Researchers Connected to PRC 'Military-Civil Fusion Strategy'*. 11 June 2021. https://www.nafsa.org/regulatory-information/proclamation-suspending-entry-chinese-students-and-researchers-connected-prc

compliance failures a crime, and lower the reporting threshold for foreign gifts to higher education institutions. The Act also recommends creating a **Federal Research Security Council** to develop uniform standards across federal research agencies, protect sensitive technologies and help deny visas to certain foreign nationals.[83]

- The **National Defense Authorization Act (NDAA) 2020**. This addresses specific scientific areas where there is perceived particular security risk (the NDAA constitutes the annual legal approval of the US defence budget). Its provisions include:
    - Agreement between the Secretary of Defense and the National Academies of Sciences, Engineering and Medicine for the National Academies to study 'the status of defense research at covered institutions [and] methods and means necessary to advance research capacity at covered institutions to comprehensively address the national security and defense needs'.
    - An assessment of high energy density physics, whereby: 'the Administrator for Nuclear Security shall enter into an agreement with the National Academies of Sciences, Engineering and Medicine to conduct an assessment of recent advances and the current status of research in the field of high energy density physics.'
    - The Principal Cyber Advisor to the Secretary of Defense and Chief Information Officer to the DOD will report on cyber-attacks and intrusions by agents of China, Russia, Iran and North Korea, against or into information systems of any contractor of the DOD that works on sensitive military technology.
    - In Section 1746 (Securing American Science and Technology), an interagency working group will coordinate activities to protect federally funded research and development from foreign interference, cyber-attacks, theft, or espionage and develop common definitions and best practices for federal science agencies and grantees (agencies will include the National Science Foundation, NASA, the Departments of Defense, Energy, Commerce, Health and Human Services, Agriculture, State, Treasury, Education, Justice, and Homeland Security, the CIA, the office of the Director of National Intelligence (DNI), and the Office of Management and Budget (OMB)).
    - Section 1286 directs DOD to establish a programme to reduce the impact of foreign talent recruitment programmes and gather more information on threat of exfiltration of IP, personnel and information.

[83] Senate Introduces the 'Safeguarding American Innovation Act,' Targeting Foreign Influence and Unreported Foreign Ties in Research. Ropes and Gray LLP, 24 June 2020. https://www.lexology.com/library/detail.aspx?g=2921e4ce-4613-45ee-94cd-9543f3d6a8ff

Australia and the Foreign Investment Review Board (FIRB)

Australia's Foreign Investment Review Board (FIRB) is a non-statutory body established in 1976 to advise the Government and Treasurer (the head of the Ministry of the Treasury). FIRB is an advisory body: ultimate decisions rest with the Treasurer and Government.[84] [85]

FIRB's responsibilities include examining proposed investments that are subject to the Foreign Acquisitions and Takeovers Act 1975 and supporting legislation; making recommendations to ministers; and providing guidance to foreign individuals.

Membership is more *ad hoc* than CFIUS, including the following members (as of January 2021): David Irvine (Chair), former Director-General of the Australian Security Intelligence Organisation and the Australian Secret Intelligence Service; David Peever, former Managing Director of Rio Tinto Australia; Ms Teresa Dyson, former chair of the Board of Taxation; Nick Minchin, former Australian Consul-General in New York; and Tom Hamilton, Head of the Treasury's Foreign Investment Division.[86]

FIRB's 'National Security Test', which grants the Treasurer the ability to address new national security risks from foreign investment:

- Requires mandatory notification of proposed investments in 'national security land';
- Requires the same for proposed direct investments in a national security business or starting a new national security business;
- Allows investments that are not notified to be called in for review on national security grounds; and
- Provides a last resort power for exceptional circumstances which permits the Treasurer to impose conditions, vary existing conditions, or require the divestment of any approved investment where national security risks emerge.[87] [88]

Current UK plans

The UK Government is planning to create a UK agency broadly similar to CFIUS or FIRB**.** A number of other CFIUS-related activities are underway.

---

[84] Foreign Investment Review Board (2020). *About FIRB*. https://firb.gov.au/about-firb

[85] A number of researchers at the Australian Strategic Policy Institute (ASPI) have discussed Australian examples of relevant agencies and reforms. These include M. Shoebridge, R. Clarke, M. Hellyer and P. Jennings. We discuss their proposals and findings here.

[86] *Ibid*.

[87] *Ibid*.

[88] FIRB is backed by the following pieces of legislation: The Foreign Acquisitions and Takeovers Act 1975, most recently amended by the Foreign Investment Reform (Protecting Australia's National Security) Act 2020; the Foreign Acquisitions and Takeovers Fees Imposition Act 2015, most recently amended by the Foreign Acquisitions and Takeovers Fees Imposition Amendment Act 2020; and the Register of Foreign Ownership of Water or Agricultural Land Act 2015.

In November 2020 the Government introduced the National Security and Investment Bill to modernise powers to investigate and intervene in FDI that may threaten national security. The Bill will require investors and business to notify a dedicated government unit (the Investment Security Unit, ISU) about certain types of transactions in sensitive sectors (defence, energy and transport) to ensure the Government can take action against national security risks. It targets investors from any country, not just China, Russia or Iran, for instance.

The ISU will sit within the Department for Business, Energy and Industrial Strategy (BEIS). The Secretary of State's ability to 'call in' or intervene in an investment will not be limited by turnover/asset value thresholds and there is no requirement for a target to have a UK subsidiary or UK-based assets (the target must simply have relevant activities in the UK).

The ISU will be responsible for 'identifying, addressing and mitigating' national security risks to the UK arising when a person gains control of a qualifying asset or qualifying entity. Companies and entities making certain acquisitions will need to notify the Secretary of State for approval. A voluntary notification system will apply to parties who consider that their transaction or acquisition may create national security risks (outside sectors where notification is mandatory).[89]

In November 2020, the Prime Minister also announced the creation of the Office for Investment to support high-value investment in the UK (while advancing government priorities such as infrastructure investment, increasing R&D spending, and reaching 'net zero'). It will sit within the Department for International Trade and the Minister for Investment will lead its work in partnership with Downing Street.[90]

Summary of possible reforms

The establishment of the ISU as a UK equivalent to CFIUS is welcome. However, CFIUS is an inter-agency body, whereas ISU is to be based under BEIS. Like any single department, BEIS must specialise, and its priority is liable to be inward investment ahead of national security.

An inter-departmental ISU would be preferable; it could also incorporate consulting sessions with representatives from departments including the Ministry of Defence (MoD), Department for International Trade (DIT), HM Treasury and the Foreign, Commonwealth and Development Office (FCDO), as CFIUS does with US equivalents.

---

[89] Davies, C and Ormond, J. *Briefing Note: National Security and Investment Act 2021*. Ashfords, 11 June 2021. https://www.ashfords.co.uk/news-and-media/general/national-security-and-investment-act-2021-briefing-note

[90] *Press release: New Office for Investment to drive foreign investment into the UK*. Department for International Trade, 29 November 2020. https://www.gov.uk/government/news/new-office-for-investment-to-drive-foreign-investment-into-the-uk

The National Security and Investment Bill aims to assess investments made by investors from all nationalities, but a more in-depth review process might be established for investments from China, Russia, and Iran, for example.

US-style Ministry of Defence-led defence research funding

The US has a major DOD-led government university-funding programme at the centre of its defence R&D efforts, a format that has recently been reformed. This structure may inform UK initiatives. The DOD funds defence R&D activities in-house, in universities, and in the private sector, through three budget categories:[91]

- 6.1 – Basic Research.
- 6.2 – Applied Research.
- 6.3 – Advanced Technology Development (ATD).

Universities and university-linked centres receive a significant share of DOD Basic Research funding; those which 'possess relevant research capabilities in specific areas of DoD interest' may compete for Applied Research and ATD funding.[92]

- The category of Basic Research outputs (including research results) is regarded as public domain information ('typically very important to the academics involved') so are not subject to US export controls.
- Applied Research and ATD is typically conducted at the level of Controlled Unclassified Information (CUI) or Classified Military Information (CMI); research outputs are therefore subject to export control requirements. One study has found 'it can be quite difficult to categorize the actual nature of real-world S&T efforts, so an activity that starts out [as] Basic Research can rapidly morph [into] Applied Research'.[93]

DOD is the third largest federal sponsor of R&D at colleges and universities (behind the NIH and National Science Foundation). DOD funds around 40 per cent of all engineering R&D in US universities. DOD-sponsored Basic Research makes up over 70 per cent of annual federal investment at US universities in electrical engineering, over 65 per cent in mechanical engineering, over 20 per cent in computer sciences, oceanography, and metallurgy and materials, and over 15 per cent in aeronautical and astronomical engineering, chemistry and

[91] Kenlon, F. (2019). Protecting DoD-Funded Research in Universities and Research Centers (Blog post, October 18, 2019). Defence Acquisition University. https://www.dau.edu/training/career-development/intl-acq-mgmt/blog/Protecting-DoD-Funded-Research-in-Universities-and-Research-Centers

[92] *Ibid*.
[93] *Ibid*.

mathematics.[94] This may help maintain interest within government in long-term R&D against immediate procurement needs.[95]

The **Defense University Research Instrumentation Program (DURIP)** is the main university defence research programme. Established by DOD in 1997, DURIP is competitive, run through a joint competition by the Air Force Office of Scientific Research, Army Research Office, and the Office of Naval Research (it received 742 proposals in the 2021 competition from 'investigators in academia conducting [science] research that is relevant to national defense').[96] Its awards are designed for universities to create 'advances that will drive unparalleled military capabilities… and help train our future STEM workforce.'[97]

Under DURIP's auspices, in 2021, DOD has released $50 million of funding to 150 university researchers in 85 institutions for equipment purchases for basic research in 'quantum sciences, materials design, development… characterization, machine learning [and] hypersonics'.[98] (However receipt of this type of funding in the UK may need to be dependent on other university reforms, including Five Eyes-type reforms, described below.)

Summary of possible reforms

That DOD basic research comprises the majority of annual federal investment at US universities in electrical and mechanical engineering, and a significant proportion in computer sciences, materials, and other fields, demonstrates how an overt 'defence umbrella' can help university science research funding.

With an eye to an expansive UK equivalent of the Defense University Research Instrumentation Program (DURIP), the UK should also review, then properly distinguish between, Basic and Applied Research in universities, as some of the universities we analysed provided examples of types of research whose classification should change. (UK university departments should also be required to outline all the uses that a research project *could* be put to, instead of being able to submit what they *think* it will be used for: see also the discussion of export controls, below.)

The 'apex': coordinating long-term defence procurement and defence research

Defence research in UK universities is a major strategic question. At the strategic level, there

[94] Peled, D. (2001). Defense R&D and Economic Growth in Israel: A Research Agenda. Paper prepared for 'Science, Technology and the Economy' (STE) Program/Workshop, University of Haifa, March 2001. https://econ.hevra.haifa.ac.il/~dpeled/papers/ste-wp4.pdf
[95] Smith, J. (2020). 'DOD to award $50m to universities to accelerate basic research.' MeriTalk. https://www.meritalk.com/articles/dod-to-award-50m-to-universities-to-accelerate-basic-research/
[96] *Ibid*.
[97] According to Director for the Basic Research Office within the Office of the Undersecretary of Defense for Research and Engineering Dr Bindu Nair, in press release. In *Ibid*.
[98] *Ibid*.

is a need to define procurement needs over 20-year timeframes, then plan defence research needs below this, allowing sustained and productive investment in UK universities (and other research institutions). This will also give investors in defence-related venture capital greater certainty of future procurement uptake for their portfolio firms.

As an 'apex' component, Government can link universities to Five Eyes Funds and other mechanisms in the collaborative process of planning for defence research investment strategy using a 20-year timeframe of procurement needs. (Below this, this would allow initiatives like the Advanced Research & Invention Agency (ARIA, the UK equivalent of DARPA) to better plan defence spin-outs with universities.[99] [100] The Defence Growth Partnership, an inter-departmental industry partnership chaired by the BEIS Business and Industry Minister, interfaces with academia and may be a suitable forum for related procurement coordination.)

Government should also mandate that funding from the seven core research councils,[101] UKRI (which in 2018 became an umbrella body for these), the Royal Society, or UK or Five Eyes defence firms becomes conditional on their being no co-funding with listed Chinese military organisations (the same would apply to funding from the Higher Education Funding Councils which form the 'dual support mechanism' with the research councils).[102]

Because the UKRI budget is a major funding source for universities, UKRI resources might be deployed in conjunction with ARIA to fund defence development from the early research stages through the life-cycle.[103]

Large incumbent defence corporates also have a role to play in filling any shortfall from a loss of research funding from China and other states. Government might make their future defence procurement contracts dependent on their funding more UK R&D, including in universities (discussed below). A fuller review of universities and national security would also encourage universities to pursue more private funding generally. Universities have been encouraged to seek corporate sponsorship abroad but have often remained dependent on government-funded research councils for domestic science funding.

---

[99] Taylor T. and Lucas, R. (2021). New UK Government Initiative to Support High-Risk, High-Reward Military Science Needs Refinement. Royal United Services Institute (RUSI). https://rusi.org/commentary/new-uk-government-initiative-support-high-risk-high-reward-military-science-needs

[100] Salisbury, E. (2021). ARIA and Defence: A Missed opportunity? LSE Blogs 8 March 2021. https://blogs.lse.ac.uk/impactofsocialsciences/2021/03/08/aria-and-defence-a-missed-opportunity/

[101] The Arts and Humanities Research Council (AHRC), the Engineering and Physical Sciences Research Council (EPSRC), the Biotechnology and Biological Sciences Research Council (BBSRC), the Economic and Social Research Council, the Medical Research Council, the Natural Environment Research Council, and the Science and Technology Facilities Research Council.

[102] University of Sheffield (2020). *Information for staff: Funding of Research in UK Higher Education*. https://www.sheffield.ac.uk/finance/staff-information/howfinanceworks/higher_education/funding_of_research

[103] House of Lords Science and Technology Select Committee. Science research funding in universities (4th Report of Session 2017-19 – published 8 August 2019 – HL Paper 409). https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/409/40902.htm

Universities and Five Eyes collaboration: focus on Australian reform discussions

At a high strategic level, developments within the other Five Eyes countries – especially Australia and the United States – demonstrate new ways for universities and research institutions to improve research security, including by encouraging inter-university collaboration and securing investments from Five Eyes defence corporates.

Treaty level framework

Universities are increasingly seen as vital for the 'enabling technologies' needed for future defence capabilities.[104] In Australia, as in the United States, this means growing defence commitments to universities: $1.2 billion has been earmarked for the next decade for next-generation R&D (including $800 million for the prototype-focused Defence Innovation Hub).[105]

Accountability for university leadership

Australian researchers' view of the strategic challenge for their universities is instructive for the UK. The level of dependence on China – in student numbers and research funding[106] – has led to the 'vice-chancellors of Australia's leading universities get[ting] obscenely high salaries, like the CEOs of large private corporations', despite the impact this has on the genuine diversity of the student body, for instance. But unlike corporate CEOs, who are expected to manage risk and 'not just blindly pursue low-hanging opportunity', these vice chancellors (VCs) have sometimes not developed risk-mitigation strategies for this dependence.[107]

This risk hinders universities' capacity to be a useful 'force multiplier'[108] for the national defence, as the dominance of research student numbers by one nationality has led, on occasion, to direct security risks and, via funding leverage, a potential tool of research and policy coercion. In the UK, universities and their associations might experiment with creating CEO-like metrics for accountability for the appointment of new VCs. These metrics could be

[104] Ausmin followed the Australian 'Strategic Update': Australian Government Department of Defence. *2020 Defence Strategic Update & 2020 Force Structure Plan* https://www1.defence.gov.au/strategy-policy/strategic-update-2020

[105] Jennings, P. and Clark, R. (2020).

[106] Shoebridge, M. (2020). 'Partnership with government needed to rebuild universities' business model.' The Strategist (ASPI Blog). 17 June 2020. https://www.aspistrategist.org.au/government-partnership-needed-to-rebuild-universities-business-model/

[107] Hellyer, M. and Jennings, P. (2020). 'Australian universities must rethink their broken business model or risk failure.' The Strategist (ASPI Blog). 28 May 2020. https://www.aspistrategist.org.au/australian-universities-must-rethink-their-broken-business-model-or-risk-failure/

[108] Jennings, P. and Clark, R. (2020). University funding can be boosted through defence research. Australian Strategic Policy Institute, 11 August 2020. https://www.aspi.org.au/opinion/university-funding-can-be-boosted-through-defence-research

monitored by university 'security councils' to vet progress and could include balancing universities' financial dependency and working towards targeted funding caps.

Five Eyes' Technical Cooperation Program and ad hoc university group alliances

The Five Eyes' Technical Cooperation Program now covers 11 major fields, including electronic warfare, conventional weapons and materials processing. The UK should drive the expansion of the programme for deeper university collaborations. Such collaboration is growing, meaning joint R&D opportunities: in 2020 the US Congress added the UK and Australia to the 'National Technology and Industrial Base', the legal framework that had been the domain of the US and Canada.[109]

In Australia, supplementary proposals include a 'university research partnership with alliance nations' funded by the Defence Department and defence industry under a 'Five Eyes-friendly' treaty-level framework. The 'Quad' framework is also seen as a supplementary vessel for future defence R&D collaboration, especially with Japan.[110]

We note in passing that universities carrying out research that will be central to the defence of Anglosphere nations may also help reform university cultures that have become increasingly hostile to these nations' core values such as freedom of speech.

Summary of possible reforms

The UK should push for expansion of university collaboration in the Five Eyes' Technical Cooperation Program and potentially all its 11 research fields. A formal research collaboration programme funded by Five Eyes governments should involve UK universities and help engage them with universities in the other Five Eyes countries. Here, the UK Government would help set 'priority areas for bilateral research collaboration'.[111]

Five Eyes cooperation is made easier by the fact that member countries have long worked to standardise technical specifications. The UK might pursue MoD- and defence industry-funded 'university research partnerships with alliance nations', within a 'Five Eyes friendly' treaty-level framework.[112] University collaborations across Five Eyes countries will also help restore university finances affected by Covid-19.

---

[109] Kliman, D. and Thomas-Noone. B (2018). 'How the Five Eyes Can Harness Commercial Innovation'. Center for A New American Security (Blog). 27 July 2018. https://www.cnas.org/publications/commentary/how-the-five-eyes-can-harness-commercial-innovation

[110] Clark, R. and Jennings, P. (2020). *Defence and industry could fund cutting-edge university research with Five Eyes allies.* The Strategist (ASPI Blog). 12 August 2020. https://www.aspistrategist.org.au/defence-and-industry-could-fund-cutting-edge-university-research-with-five-eyes-allies/

[111] *Ibid*.

[112] *Ibid*.

Universities' security policies: the need for review

A recent US report by the Association of American Universities (AAU) and the Association of Public and Land-grant Universities (APLU), *Actions Taken by Universities to Address Growing Concerns about Security Threats and Undue Foreign Influence on Campus* (2019)[113], outlines approaches that universities can take to improve research security. The examples in our previous paper demonstrate the urgent need for many of these in the UK, yet a recent Universities UK report on how to manage the risks of 'internationalisation' does not mention national security or human rights concerns.[114]

The report finds that security measures that universities may explore include:

- Distributing letters to faculty to increase awareness of systematic programmes of foreign influence, how such programmes pose risks to core scientific and academic values and threaten research integrity;
- High-level working groups and task forces;
- International activities and compliance coordination offices (for example, relevant to Five Eyes);
- Comprehensive processes to review foreign gifts, grants and contracts;
- Using restricted or denied-party screening (institutions are expanding their techniques for screening foreign sponsors and collaborators);
- Clear point of contact (POC) with security officials. US institutions have developed stronger relationships and are regularly interacting with local and regional officials from relevant organisations;
- Foreign travel review or advice for staff. Even before government action, universities should proactively review staff participation in 1000 Talents and related programmes; and
- University staff with export control expertise. Most AAU and APLU institutions have at least one staff member responsible for export control compliance. Many belong to the Association of University Export Control Officers (AUECO) which shares information on best practice.

[113] Association of Public and Land-grant Universities (APLU) (2019). *Actions Taken by Universities to Address Growing Concerns about Security Threats and Undue Foreign Influence on Campus*. Updated April 22, 2019. https://www.aplu.org/members/councils/governmental-affairs/cga-miscellaneous-documents/Effective-Sci-Sec-Practices-What-Campuses-are-Doing.pdf

[114] Universities UK (2020). Managing risks in Internationalisation: Security related issues. https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/managing-risks-in-internationalisation.aspx (p.7)

Improved export controls for UK university research

The UK Government has now established a specialist unit to offer academics confidential advice 'before entering overseas research partnerships' due to the risks from ''hostile actors' such as China.' The Research Collaboration Advice Team (RCAT) will analyse areas which 'could have both civilian and military applications, including aerospace and robotics', which are seen as 'particularly sensitive'.[115]

This office of 10-15 advisers, based in Manchester, will be managed by BEIS and is expected to be operational by October 2021 (the *Financial Times* has described how the government's announcement followed the revelations in our previous paper). The RCAT will 'answer queries from academics' and 'proactively approach universities' to help them 'mitigate threats'. However, the concept has already met resistance from unnamed senior Russell Group university administrators: one feared 'getting tied in knots with the government'.[116] However we believe that there is also a need for reform of export controls for universities.

Main relevant treaties and regimes

The UK has its own (partial) arms embargo on the PRC (which now includes Hong Kong), implemented through the Export Control Order 2008, covering:[117]

> 'lethal weapons, such as machine guns, large-calibre weapons, bombs, torpedoes, rockets and missiles; specially designed components of the above and ammunition; military aircraft and helicopters, vessels of war, armoured fighting vehicles and other weapons platforms; any equipment which might be used for internal repression. This embargo covers the export of these items from the UK.'

There are also two central counter-proliferation regimes on which the UK's export controls (below) are based: the Wassenaar Arrangement (WA) and the Missile Technology Control Regime (MTCR). These help the UK's military and dual-use lists (also below) provide more coverage than the embargo alone would imply.

---

[115] Warrell, H. and Staton, B. 'UK universities to be offered advice on national security threats.' *Financial Times*, 25 May 2021. https://www.ft.com/content/a264793d-cfd6-4fb3-89e7-d65ffb5ec01f

[116] *Ibid*.

[117] Foreign, Commonwealth & Development Office and Export Control Joint Unit. (2020). Collection: UK arms embargo on mainland China and Hong Kong. Published 31 December 2020. https://www.gov.uk/government/collections/uk-arms-embargo-on-mainland-china-and-hong-kong#:~:text=Since%201989%2C%20following%20Chinese%20military,was%20extended%20to%20Hong%20Kong

The Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies

The WA is a non-legally binding regime ('non-treaty') asking its 42 member states to be accountable for exports of conventional arms and dual-use goods and technologies to countries outside the WA.[118] The UK is a signatory; the PRC is not.

Volume 2 of the WA details the dual-use goods and technologies that member states must consider when exporting or sharing such items. Dual-use goods and technologies whose export should be controlled are 'major or key elements for the indigenous development, production, use or enhancement of military capabilities'.[119] The evaluation of dual-use items includes for:

- Foreign availability outside member states;
- The ability to effectively control the export of the goods; and
- The ability to make a clear and objective specification of the item.

Three categories in the dual-use list could apply to most of the research centres we have studied:[120]

- Category 1 – Special Materials and Related Equipment;
- Category 2 – Materials Processing; and
- Category 9 – Aerospace and Propulsion.

Missile Technology Control Regime (MTCR)

The MTCR is an informal arrangement between 35 member states to limit missile and missile technology proliferation. One of its aims is vigilance over the transfer of equipment,

[118] Source: https://www.wassenaar.org/

[119] Wassenaar Arrangement (Wassenaar.org). (2019). Criteria for the selection of dual-use items. (Adopted in 1994 and amended by the Plenary in 2004 and 2005). https://www.wassenaar.org/app/uploads/2019/consolidated/Criteria_for_selection_du_sl_vsl.pdf

[120] Wassenaar Arrangement Secretariat. (2020). Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Public Documents. Volume II List of Dual-Use Goods and Technologies And Munitions List, December 2020. https://www.wassenaar.org/app/uploads/2020/12/Public-Docs-Vol-II-2020-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-20-3.pdf; The US Commerce Department's Bureau of Industrial Security announced in October 2020 that six technologies related to chip manufacturing would be included in its new export control under the WA (in: Gibson and Dunn. (2020). New Controls on Emerging Technologies Released, While U.S. Commerce Department Comes Under Fire for Delay. Blog: 27 October 2020. https://www.gibsondunn.com/new-controls-on-emerging-technologies-released-while-us-commerce-department-comes-under-fire-for-delay/)

material, and related technologies for systems capable of delivering weapons of mass destruction (WMD).[121]

The MTCR seeks to reduce the risk of WMD proliferation by controlling exports of goods and technologies that could contribute to delivery systems (other than manned aircraft).[122] The following passages are derived from MTCR text.

- The MTCR aims to use export controls on a list of controlled items[123] – including equipment, materials, software and technology needed for missile development, production and operation. MTCR members should impose license authorisation requirements before listed items are exported. The list contains Category I and Category II items.[124]
- Category I items include: Complete rocket and unmanned aerial vehicle systems (such as ballistic missiles, space launch vehicles, sounding rockets, cruise missiles, target drones, and reconnaissance drones), their major complete subsystems (such as rocket stages, engines, guidance sets, and re-entry vehicles), and related software and technology, and production facilities for these items. These exports are subject to 'unconditional strong presumption of denial', regardless of the purpose of export, and rarely licensed for export.
- Category II items include less-sensitive and dual-use missile-related components. Exports judged by the exporting country to be intended for use in WMD delivery are to be subject to 'strong presumption of denial'.[125]

Regarding UK commitment to the Missile Technology Control Regime (MTCR), MTCR member states exercise their own discretion in implementing the guidelines. UK compliance with MTCR (and the WA) is maintained through the **UK Strategic Exports Control List**, including a **military** and a **dual-use list**, as well as remaining EU compliance legislation.

What is an 'export'?

The UK Government's *Higher education guide and toolkit on export controls* states:[126]
'Through the Export Control legislation, the UK implements international treaty obligations, as well as the foreign policy of the UK which is often coordinated with likeminded states.'

---

[121] Missile Technology Control Regime. Frequently Asked Questions (FAQS) (Accessed: 15 April 2021). https://mtcr.info/frequently-asked-questions-faqs/
[122] *Ibid*.
[123] *Ibid*. and The MTCR Equipment, Software, and Technology Annex.
[124] *Ibid*.: including rockets capable of delivering a payload of at least 500kg over at least 300km and equipment, software, and technology for these.
[125] *Ibid*.
[126] Association of University Legal Practitioners and Project Alpha of King's College London (2015). Higher Education Guide And Toolkit On Export Controls And The ATAS Student Vetting Scheme. (In partnership with the Export Control Organisation and the Foreign and Commonwealth Office). Version 1, 2 April 2015.

It also sets out what Government means by 'export':

- **1.2 What does 'export' mean?**

  'Normally 'Export Controls' apply to the physical removal of goods or the transfer (by any means) of goods, technology or software **and/or knowledge (which may capture teaching)** from the UK to a destination outside the UK. However, controls can apply to transfers by facsimile, e-mail and also telephone and, under exceptional circumstances, to transfers within the UK when it is known that the ultimate end use is WMD-related outside the UK.

  Export can take place via physical or electronic means, [such as] by being shipped or freighted overseas (including carriage of a laptop on a trip for example); or electronic transfer (fax, email, telephone, text messaging or video-conferencing) from within the UK to a person or place abroad. Oral transmission by telephone could be within the scope where the detail about the technology is contained in a document and is read out or communicated so as to achieve substantially the same result as if the recipient had read the document.'[127]

- **Technology means:** Information necessary for the development, production or use of [controlled] goods. This may include:

  Blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, or manuals and instructions, either written or recorded on other media or devices such as disks, tapes or read-only memories.[128] [129]

What are the forms of control?

The UK Strategic Export Controls contain **four primary elements** and 'form the basis of determining whether any products, software or technology require an export licence':[130]

i. Control of exports of military and certain paramilitary and radioactive items outside the UK.
ii. Exports to non-EU destinations of controlled dual use technologies (as listed on the EU Dual Use List: generally civil items and technologies that could be used for WMD purposes or potentially have military application generally).

---

https://www.research-operations.admin.cam.ac.uk/files/policies_and_procedures/export_control_guide_july_2015.pdf

[127] *Ibid*.

[128] Definition in the Export Control Order 2008 Regulation 2.

[129] EU Dual-Use Regulation (EC) No 428 2009 also refers to information including skills, training, working knowledge or consulting services.

[130] Department for International Trade and Export Control Joint Unit. Guidance: UK Strategic Export Control Lists. Published 3 August 2012. (Last updated 23 February 2017). https://www.gov.uk/guidance/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items

iii. Export is also restricted for more sensitive controlled dual use items of technology on the Dual Use List (Annex IV EU Dual Use Regulation) to any destination, including within the EU.

iv. 'Catch-all' control, based on end-user concerns and intended to control unlisted goods and technologies which have possible utility in an area of WMD concern, namely for chemical, biological or nuclear weapons or other nuclear explosive devices or their delivery; or a military end-use in an embargoed destination.

In sum, the UK strategic export control lists are: the UK military list, the UK dual-use list, non-military firearms list, human rights list, UK security and human rights list, UK radioactive source list, and the dual-use list.

The lists are drawn in particular from the following legal sources:

- The Export Control Order 2008 Schedule 3[131];
- Annexes 2 and 3 of Council Regulation (EC) No. 1236/2005 (as amended) (the EU Human Rights List); and
- Annex 1 of Council Regulation (EC) No. 428/2009 (as amended) (the EU Dual-Use List).[132]

What does 'Dual-use' mean?

Controlled dual-use goods cover thousands of items controlled, *but not necessarily designed*, for dual-use, having benign civil applications but significant potential for military use, including for WMD, and potential for human rights abuses. According to DIT, items of concern will have some utility 'in a weapons manufacture programme'. Controls can cover 'key components, accessories, technology and software, in addition to actual goods.'[133]

Importantly, under the lists, 'technology' means '*information*' necessary for the 'development', 'production', or 'use' of goods or software (which are subject to controls).[134] There are some exceptions for information 'in the public domain'. Exports can take the form of physical or electronic transfers. The dual-use categories are as follows:[135]

0 Nuclear materials, facilities and equipment.
1 Special materials and related equipment.
2 Materials processing.
3 Electronics.

[131] Including the explosive-related list.
[132] The Trade Controls are set out in Articles 20 to 25 of the Export Control Order 2008 (following the Export Control Act 2002) and Schedule 1 Part 1 – Category A goods; Schedule 2 (the Military list (items 'specifically designed or modified for military use')) Part 2 – Category B goods; Schedule 3 – the UK dual use list.
[133] Sometimes technical parameters must be met, such as purity, accuracy, and so on.
[134] See also: Research Services, University of Sheffield (2021). *Guidance on Export Control Legislation*. https://www.sheffield.ac.uk/rs/export
[135] Dual-use lists are drawn from the Wassenaar Agreement and MTCR, as well as the Nuclear Suppliers Group, Australia Group, and Chemical Weapons Convention.

4 Computers.
5 Telecommunications and information security.
6 Sensors and lasers.
7 Navigation and avionics.
8 Marine.
9 Aerospace and propulsion.

What are the specific lists?

Any **goods, software or associated intangible technology** expressly for use in military, WMD, or missile systems is likely to be in the UK Consolidated Lists. These include **dual use technology**. If an item is included on the lists, it does not mean it cannot be exported, 'but that any individual wishing to transfer such an item by electronic means or physically to export it will require an export licence to be able to do so.' These lists 'cover a wide range of items from diverse industries and academic disciplines.'[136]

With the exception of nuclear technology, technology listed in the UK Consolidated Lists is controlled if it is '**required**' and '**necessary**' for the development, production or use of the controlled items. Even when knowledge is intended for civilian use, this does not mean there is no need to seek a licence (however it could be relevant to whether this licence is granted).

What are WMD end-use controls?

According to Project Alpha[137]:

- End Use Controls typically involve an export, but passing information (including through teaching) could be subject to control if, for example, the tutor knew that the student intended to transfer the information to a destination for 'WMD purposes'.
- Providing technical assistance to a WMD programme is subject to end use control; the general principle governing End Use Controls is that the exporter must not export without a licence if he or she has been informed or is aware of or suspects there is intended WMD end-use'.

In its briefings, DIT states: 'end-use control can be applied to ANYTHING (e.g. main equipment or components) or ANY activities (e.g. training or helplines), if potentially connected to a WMD programme.' (However, according to DIT, 'Most of the goods or technology required for WMD or missile delivery systems may not be on any control list',

[136] Research Services, University of Sheffield (2021). *Guidance on Export Control Legislation*. https://www.sheffield.ac.uk/rs/export
[137] King's College London News Centre, 19 July 2015. Project Alpha and association of university legal practitioners issue export control guidance for academia. https://www.kcl.ac.uk/news/project-alpha-and-association-of-university-legal-practitioners-issue-export-control-guidance-for-academia

meaning it is incumbent on the party supplying the technology to contact the authorities to check whether its activities may be proscribed.)[138]

The Export Control Order 2008 (Article 6) contains 'additional controls on transfer of technology by any means and provision of technical assistance in relation to WMD.' DIT states:

> 'If you know or suspect an export will be used in connection with a WMD programme you have a legal obligation to contact [the authorities] and ask for a licence.' 'WMD purposes' mean 'use in connection with the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons or other nuclear explosive devices, or the development, production, maintenance or missiles capable of delivering such weapons.'

DIT also defines 'in connection with' as 'includ[ing] exports which may be used directly in a weapon or missile *or indirectly in WMD development*'. Indirect uses include 'infrastructure projects; *research programmes at universities or government laboratories*; un-safeguarded nuclear activities; civil space programmes' [our italics]. A licence is therefore required if the exporter 'knows', has been 'informed', or even 'suspects' that the goods software or technology are intended for 'any relevant use'. Parties are advised to consult the Consolidated list of strategic military and dual-use items that require export authorisation[139] (a few of whose categories are listed below).

While controls exclude some basic scientific research or findings that will be or are in the public domain, this will not exclude all such research.[140] According to Export Control Joint Unit (ECJU) guidance for academics,[141] 'Even if the item, technology or software is not listed in the UK Consolidated Lists, a licence could also be required if the exporter knows, has been informed, or suspects there is a WMD end use.' Under government guidance on the UK Strategic Export Control Lists,[142] 'if your goods are not listed on the UK Strategic Export Control Lists, [the ECJU] has the power to invoke "end-use controls" if there are any specific

[138] This does not mean that any researchers have personally broken UK rules, because we assume that university centres and their research focuses have been approved. However it may suggest that individual research projects which risk falling under dual use areas which in future may need prior approval on a case by case basis.

[139] Department for International Trade Export Control Joint Unit. Consolidated list of strategic military and dual-use items that require export authorisation. 10 April 2013. https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation

[140] Research Services, University of Sheffield (2021). *Guidance on Export Control Legislation*. https://www.sheffield.ac.uk/rs/export

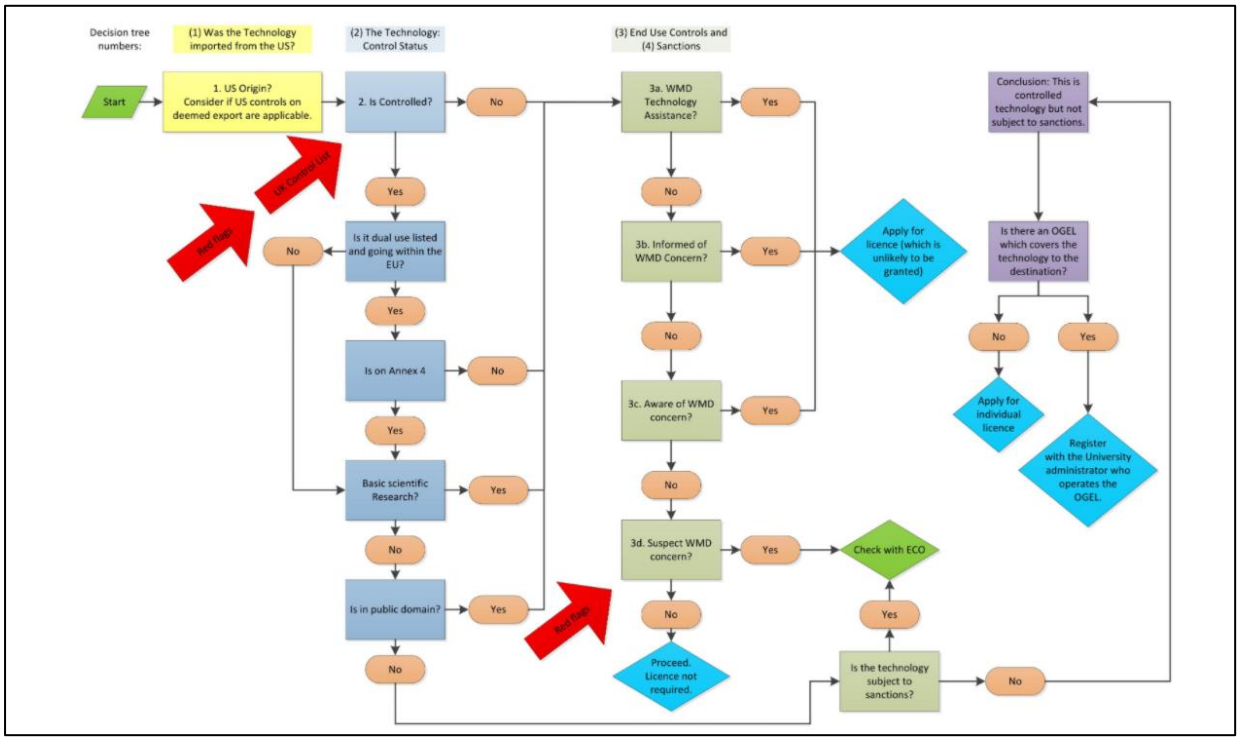
[141] King's College London News Centre, 19 July 2015. *Project Alpha and association of university legal practitioners issue export control guidance for academia*. https://www.kcl.ac.uk/news/project-alpha-and-association-of-university-legal-practitioners-issue-export-control-guidance-for-academia

[142] Department for International Trade Export Control Joint Unit, 2013.

concerns about military or weapons of mass destruction (WMD) end-use'[143] (it adds: 'Additional restrictions can apply when dealing with countries that are subject to sanction… which often have the effect of broadening the UK Consolidated Lists to include items which would not normally be included in the UK Consolidated List').

Project Alpha's flowchart shows why specific research projects may still be proscribed even if the funding (for a research centre) has been approved. If we begin from Question 2 ('Is it controlled?') at the top, the possible responses for cooperation with China all lead to 3a ('WMD technology assistance?'). Where this is deemed possible, the advice is 'Apply for licence (which is unlikely to be granted)'.

Figure 2.1: Export Control Flowchart



Source: Project Alpha, King's College London (2015). [144]

Offences

The Export Control Order 2008 (ECO) is the regulation under Section 1 of the Export Control Act 2002 that sets out possible offences that arise from prohibitions on the export without a licence of military goods, software and technology.[145] Article 2(1) of the ECO states that

[143] 'The UK Strategic Export Control Lists specify goods that need an export licence for 'strategic' purposes.' (Department for International Trade Export Control Joint Unit, 2013).
[144] *Ibid*.
[145] Henley, C. *Blog: Will 200 academics really be jailed? The Export Control Order 2008, the People's Republic of China, and the Daily Mail*. Carmelite Chambers, 10 February 2021. https://www.carmelitechambers.co.uk/blog/blog-will-200-academics-really-be-jailed-export-control-order-

'dual-use' means 'usable for both civil and military purposes'. According to barrister Chris Henley QC, this means it is 'therefore drawn very widely, and deliberately so. Research departments, or indeed any technology and software developers, must consider the possibility that an item exported ostensibly for one purpose may be put to another use.'[146]

Part 6 of the ECO outlines how offences are 'layered in levels of seriousness, depending on the relevant state of mind.'[147] The levels below the most severe ('with intent to evade any such prohibition or restriction', carrying a jail sentence of up to 10 years) have 'not been drafted with particular clarity'.[148] Offences under Part 6, with a maximum two-year sentence, include a two-year prison sentence if 'the person **has grounds** for suspecting that goods, software or technology are or **may be intended**, in their entirety **or in part**, for WMD purposes' (Art. 34(3)(c)); however, the words 'suspecting' and 'may be' are 'rich with uncertainty').[149] Article 34(3)(a) states that an offence is committed if an individual 'has been informed' that a transfer 'may be intended for such use'. As such:

> 'at the lower end of the scale [t]he traditional criminal burden of proof appears to be reversed, as the onus is placed on the person to show that they 'did not know, and had no reason to suppose that the goods were destined for an embargoed destination' (s34(2)). The requirement on a suspect to show that they had 'no reason to suppose' may be challenging, particularly with all the news stories now in circulation suggesting that most if not all Chinese companies are ultimately controlled by the Chinese State.'[150]

Summary of possible reforms

A number of reforms may be needed. For example, Part 6 of the ECO, whereby an exporter is at risk of a two-year prison sentence if 'the person [has been informed or] has grounds for suspecting that goods, software or technology are or may be intended, in their entirety or in part, for WMD purposes', may allow leeway and may allow the same activities to be treated

---

2008-peoples-republic-china-and (this states: 'The products (particularly, so far as academic institutions are concerned, including electronic equipment and software) which have or may have export restrictions are set out in the UK Military List or national control list; one of the international export control regimes including those set out by the Nuclear Suppliers Group, the Missile Technology Control Regime, the Australia Group and the Wassenaar Arrangement, the EU's Torture Regulation and the UK's Export of Radioactive Sources (Control) Order 2006. Failing appearance on one of those lists, some dual-use items are covered by Art. 4 of Council Regulation No 428/2009. It is not at present clear how the government has transposed the EU legislation into domestic law.')

[146] *Ibid*.
[147] *Ibid*.
[148] *Ibid*.
[149] *Ibid*.
[150] *Ibid*.

differently depending on people's claims. (Overall, the complexity of the controls is a concern in itself: leading lawyers say they do not fully grasp its implications.)

While universities' responses to our enquiries suggested that they had received Government approval for entire research centres, dual-use concerns suggest that research approval may be needed on something more like a project-by-project basis.

On the Consolidated Lists, the concept of what is 'required' or 'necessary' (that is, 'technology listed in the UK Consolidated Lists is only controlled if it is 'required' and 'necessary' for the development, production or use of the controlled items') may need clarification: sometimes scientific collaboration will simply increase the skills of visiting scientists, but this may also be 'necessary' to military programmes in the long-run.

Finally, according to the toolkit drawn up by the Export Control Organisation (now the ECJU) and the Foreign and Commonwealth Office:

> 'An indirect effect of sanctions may be that it might become unlawful to teach certain subjects to students from certain countries [e.g.] Iranian national[s] (i.e. it is likely that an Iranian citizen who wished to study nuclear engineering outside Iran might be unable to do so because of UN sanctions on Iran, which have been in place since 2006/2007).'

If UN sanctions on Iran justify better assessment of the entry of Iranian students, then UK sanctions on China should also lead to reassessment of research collaboration with students and employees of Chinese military-linked universities, and especially the staff and former staff of Chinese military-linked conglomerates.

UK Government guidance on how dual-use lists impact academic research

As of March 2021, UK Government guidance states [our bold type]:[151]

'UK strategic export controls focus on high risk activities, such as applied research, and could affect your activities if you:

- Work with colleagues overseas on research projects;
- Take your research overseas; or
- Export your technology.

Unless your work qualifies for an exemption, you might need an export licence if one of the following apply:

- Your software or technology is linked to items in the consolidated list of strategic military and dual-use items that require export authorisation;

[151] Export Control Joint Unit and Department for International Trade (2021). Guidance: Export controls applying to academic research. 31 March 2021. https://www.gov.uk/guidance/export-controls-applying-to-academic-research

- You have been informed, are aware, or suspect that the recipient of the software or technology intends to use it for WMD purposes; and
- You answer yes to any of the following:
    - The software or technology is not in the public domain;
    - The technology does not meet the definition of basic scientific research;
    - Your research is in one of the disciplines that could be targeted by would-be proliferators;
    - The recipient intends to use or send the information outside the EU; and
    - Preliminary online searches or other open-source checks show the recipient is potentially involved in suspicious activity.

The following paragraphs on 'High risk research' and 'Collaborating internationally' were added in 2021 following our previous paper.

High risk research:

- Applied research in certain fields is high risk and could potentially be misused for military purposes.
- These areas are usually in the science, technology, engineering and mathematics (STEM) subjects. They include:
    - Aeronautical and space technology; applied chemistry, biochemistry and chemical engineering; applied physics; biotechnology; electrical and mechanical engineering; instrumentation and sensors; materials technology; nuclear technologies; production and process technology; telecommunications and information technology.

Collaborating internationally:

- Before agreeing to any international research collaboration, researchers and institutions must first undertake a due diligence process. A particular collaboration may not on first appearance be directly relevant to such activities. However, a transfer of technical information or data for one purpose could unwittingly be used for another purpose, including assisting in the development or production of WMD.
- This is particularly important with organisations in countries subject to sanctions relating to WMD, or countries that have WMD or ballistic missile programmes.
- **You should note certain countries have an active state policy concerning the diversion of advanced and emerging technologies. This is to support the development of their military including in WMD.**

You should:

- Check if there will be any transfer of **controlled items, including 'technology'**;
- Check if there is a risk that the activities of a party to the collaboration could divert items, including non-controlled items, to a WMD programme; and

- Get an export licence for **any transfers.**

Assessing risk of collaboration:

- You must check whether your potential collaboration partner individuals and their organisation have been involved in activities of potential concern using:
- Internet searches to see what is in the public domain; the list of entities subject to government-imposed sanctions or restrictions; news articles and press releases about involvement in military or defence projects; online resources run by non-government organisations, such as King's College's Centre for Science and Security Studies and academic think tanks; Export Control Joint Unit (ECJU) for help with specific enquires if more information and advice is required.

When UK strategic export controls apply:

- Export controls apply: to **goods, software and technology** appearing on control lists [discussed in dual-use above]; when there are concerns about end-use or end-user; **when destinations are subject to sanction** or other restrictions. Exemptions for the academic community include:

In the public domain:

This is technology or software available without restrictions on its further dissemination. It excludes the normal copyright restrictions that may apply.

It is unlikely that undergraduate level courses need to consider export controls. Most of the information and technical data used in teaching such degrees is in the public domain. Therefore, the exemption would generally apply.

In the case of individual projects, it is unlikely that export controls apply. This is because the work generated would generally not meet the full definition of sensitive technology. The same is generally true of most types of taught master's degrees.

Basic scientific research:

This exemption only applies to controlled dual-use technologies. This is experimental or theoretical work undertaken to solely obtain new knowledge of the fundamental principles of phenomena or observable facts. It is not directed towards a specific practical aim or goal.

This exemption only applies to controlled dual-use technologies. *It does not apply where there are end-use, end-user or destination concerns.* By definition, military listed technology is for a specific application, and therefore is not basic scientific research.

- Limits of academic exemption:

Any academic exemption is unlikely to apply to all aspects of research focused advanced postgraduate degrees such as MPhil or PhD looking at areas of controlled technology.

Especially as such research programmes will typically be applied research. By their very nature, they will include technology not covered by the 'public domain'.

Research may be able to use the 'basic scientific research' exemption. The use of this exemption is limited by the definition of what is intended by 'basic scientific research'.

To qualify for this exemption, any technology generated by the research for basic scientific research purposes must: be solely to add to the sum of human knowledge; not be aimed at a specific (short-term) practical aim; and not address a specific technical problem.

A possible way of determining whether a piece of research is 'basic scientific research' is to consider the Technology Readiness Level (TRL) of the research being undertaken. A low TRL, around 1 to 3, is more likely to fall within the area of 'basic scientific research'.[152]

If the sole intended output of a piece of work is a published article in a peer reviewed scientific journal, then this is a further useful indicator to this being 'basic scientific research', especially as the intended output is to be in the 'public domain'.[153]

- How nationality affects export controls:

The nationality of any intended recipient is not a factor as to whether or not export controls apply. Therefore, the UK does not have what is termed 'deemed exports'. The transfer of controlled 'technology' to a non-UK national, that takes place solely in the UK, and does not involve any transfer from the UK, is not deemed to be an export.'[154]

Summary of possible reforms

The guidance states that export controls focus on high-risk activities like 'applied research [which] could affect your activities if you: work with colleagues overseas on research projects; take your research overseas [or] export your technology'[155], but these do not necessarily cover domestic research sponsored by foreign military-linked organisations, the outputs from which may largely go into public domain (and many academics presumably will not check this guidance if they do not perceive that they are involved in exporting, or do not mean to be). The apparent need to 'suspect' provides another justification for high-risk behaviour; the need to 'get an export licence for any transfers' also needs to be addressed because what constitutes a transfer is still unclear.

The requirement to 'check whether your potential collaboration partner individuals and their organisation have been involved in activities of potential concern using: Internet searches… list of entities subject to government-imposed sanctions or restrictions; news

[152] *Ibid*.
[153] *Ibid*.
[154] *Ibid.*
[155] *Ibid*.

articles and press releases [etc]' also appears to be unreliable (especially until the relevant 'entities' are 'subject to government-imposed sanctions or restrictions').

Furthermore, the following statement may assume too much: 'In the case of individual projects it is unlikely that export controls apply. This is because the work generated would generally not meet the full definition of sensitive technology. The same is generally true of most types of taught master's degrees'; research in the public domain can also still generate skills for military-linked companies abroad.

That '[t]he in the "public domain" exclusion does not apply if the commercial research is not published'[156] asks: what if it is published? That is, if commercial research is published then why should the public domain exclusion necessarily apply in totality? After all, there may be other spin-offs that do not become public that are useful to foreign military forces from research that has produced published papers, pointing to the need for more rigorous assessment of research centres and their projects.

Finally, another point in this guidance is a cause for concern. That academic exemptions '[do] not apply where there are end-use, end-user or destination concerns' (and it is understood that the new Research Collaboration Advice Team (RCAT) has been established in part because the Chinese military-linked organisations we have discussed are considered 'end-user or destination concerns') also implies that these entities should be sanctioned from investing and research collaboration in the UK.

[156] Following this guidance, ECJU/DIT provides some case studies, in: Export Control Joint Unit and Department for International Trade (2021). Case study: Export controls on academic research. (31 March 2021). https://www.gov.uk/government/case-studies/export-controls-on-academic-research

Conclusions and recommendations

Our previous paper *Inadvertently Arming China?* revealed widespread sponsorship of high-technology research centres in UK universities by Chinese military-linked conglomerates and universities, and scientific collaboration between these centres and their sponsors. For this picture of 'strategic incoherence' to be addressed, greater strategic coordination is required.

The risk of the Chinese military sponsorship of UK academia is not simply that it will lead to outputs which might be put to use by the Chinese military, but that its scientific outputs create other strategic risks. The Government's Integrated Review discussed how rival states might use economic tools to 'target and undermine the economic and security interests of rivals', highlighting how we should expect 'increased competition for scarce natural resources such as critical minerals, including rare earth elements, and control of supply may be used as leverage on other issues'. These companies may continue to sponsor research that is against the broader strategic interests of the United Kingdom.

Sanctions

- A UK sanctions regime should cover companies linked to the militaries of China and other systemic competitors. The Government has not yet prevented Chinese military companies from investing in the UK and benefitting from UK-based research, despite their equipment apparently being put to use by the Chinese state in what is credibly called a genocide in Xinjiang, and supplying regimes including Burma and Syria.
- A combined sanctions regime would prevent investment in the UK (including its research facilities) and investment by Britons in these companies. This should extend to companies involved in surveillance technologies and associated research.

Academic Technology Approval Scheme (ATAS)

- The Academic Technology Approval Scheme (ATAS) should be further reviewed to better control entry to the United Kingdom. The central requirement that ATAS 'ensure that people who are applying to study certain subjects in the UK do not have existing links to WMD [or other known military] programmes' does not fully account for the fact that it is typically not possible to know how knowledge acquired in the UK might be used in China's military-linked universities and conglomerates (where staff may officially have worked in civilian programmes). ATAS should be amended to prevent entry of the staff and students of a list of closely military-linked universities, laboratories and conglomerates in China (as well as the equivalents in a number of other autocracies).

UK equivalent of CFIUS

- The establishment of the Investment Security Unit (ISU) as the UK equivalent of the Committee on Foreign Investment in the United States (CFIUS) is a positive development. However, CFIUS is an inter-agency body, whereas ISU will be based under BEIS, whose priority, understandably, is liable to be inward investment.

Defence research funding for universities

- In the United States, DOD basic research comprises 40 per cent of all engineering R&D funding in US universities, funds which show how a 'defence umbrella' can help research funding, pointing to a UK equivalent of the US Defense University Research Instrumentation Program (DURIP).
- The UK should also review, then better distinguish between, Basic and Applied Research in universities. In some of the universities we analysed, research classifications should change. (For instance, before receiving funding, UK university departments should be required to outline all the uses that a research project *could* theoretically be put to, instead of how they think it will be used.)
- Government should mandate that funding from the seven core research councils, UKRI (which in 2018 became an umbrella body for these), the Royal Society, or UK or Five Eyes defence firms becomes conditional on their being no co-funding with listed Chinese military organisations (the same would apply to funding from the Higher Education Funding Councils).
- Large incumbent defence corporates have a role to play in filling any shortfall from a loss of research funding from other sources. Government might make their future defence procurement contracts dependent on their funding more UK R&D, including in universities.

Five Eyes cooperation

- The UK should aim to expand university collaboration under the Five Eyes' Technical Cooperation Program, potentially in all its 11 research fields.
- A formal research collaboration programme funded by Five Eyes governments could engage UK universities with university groups in other Five Eyes countries. The UK might pursue MoD- and defence industry-funded 'university research partnerships with alliance nations' within a '5 eyes friendly' treaty-level framework.

Export Controls

- Part 6 of the ECO, whereby an exporter is at risk of a two-year prison sentence if 'the person… *has been informed* [or] *has grounds for suspecting* that goods, software or

technology are or may be intended, in their entirety or in part, for WMD purposes' may allow leeway and may allow activities to be treated differently depending on researchers' claims.

- Overall, the complexity of the export system is a concern in itself: leading lawyers say they do not fully grasp its implications.
- Some universities' responses to our enquiries suggest that they have received government approval for an entire research centre (and that specific projects may not have been checked). If sponsorship arrangements are allowed to continue without sanctions – and we recommend they should not be – research approval may be needed on something like a project-by-project basis.
- On the Consolidated List, the concept of what is 'required' or 'necessary' (that is, 'technology listed in the UK Consolidated Lists is only controlled if it is 'required' and 'necessary' for the development, production or use of the controlled items') needs to be clarified: in some cases the immediate result of a collaboration will simply increase the skills of the scientists associated with these programmes, which may appear innocuous but could theoretically be 'necessary' to weapons programmes in the long-run.

Guidance to universities

- Guidance states that export controls focus on high-risk activities like 'applied research [which] could affect your activities if you: work with colleagues overseas on research projects; take your research overseas [or] export your technology', but these do not necessarily cover domestic research sponsored by foreign military-linked organisations, the outputs from which may largely go into the public domain (and many academics presumably will not check this guidance if they do not perceive that they are involved in exporting, or do not mean to be). The apparent need to 'suspect' provides another possible justification for high-risk behaviour; the need to 'get an export licence for any transfers' should also be amended, because what constitutes a transfer is still unclear.
- Some master's degree research may also be a concern; research in the public domain may still generate skills for military-linked companies abroad.
- If commercial researched is published beyond the 'public domain' exclusion, other spin-offs may be possible.

Bibliography

American Geosciences Institute (2021). *What are rare earth elements, and why are they important?* https://www.americangeosciences.org/critical-issues/faq/what-are-rare-earth-elements-and-why-are-they-important

Association of Public and Land-grant Universities (APLU) (2019). *Actions Taken by Universities to Address Growing Concerns about Security Threats and Undue Foreign Influence on Campus*. Updated April 22 2019. https://www.aplu.org/members/councils/governmental-affairs/cga-miscellaneous-documents/Effective-Sci-Sec-Practices-What-Campuses-are-Doing.pdf

Association of University Legal Practitioners and Project Alpha of King's College London (2015). *Higher Education Guide And Toolkit On Export Controls And The ATAS Student Vetting Scheme*. (In partnership with the Export Control Organisation and the Foreign and Commonwealth Office). Version 1, 2 April 2015. https://www.research-operations.admin.cam.ac.uk/files/policies_and_procedures/export_control_guide_july_2015.pdf

Australian Government Department of Defence. *2020 Defence Strategic Update & 2020 Force Structure Plan* https://www1.defence.gov.au/strategy-policy/strategic-update-2020

Bailey Grasso, V. (2013). *Rare Earth Elements in National Defense: Background, Oversight Issues, and Options for Congress.* Congressional Research Service. https://fas.org/sgp/crs/natsec/R41744.pdf

Bombach, K.M. et al (2021). 'U.S. Prohibits Trading in Securities of Communist Chinese Military Companies, but NYSE Reverses Plan to Delist'. Greenberg Traurig, 4 January 2021. https://www.gtlaw.com/en/insights/2021/1/us-prohibits-trading-in-securities-of-communist-chinese-military-companies

Bureau of Industry and Security, US Department of Commerce. *Military End User (MEU) List* and *Supplement No. 4 to Part 744 – Entity List* (2020). https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/1770; https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file

Bureau of Industry and Security, US Commerce Department, 19 April 2014. 'US Commerce Department Adds Nine Persons Associated with Missile Proliferator to Entity List'. https://www.bis.doc.gov/index.php/about-bis/newsroom/107-about-bis/newsroom/press-releases/press-release-2014/667-u-s-commerce-department-adds-nine-persons-associated-with-missile-proliferator-to-entity-list

Burke, R. et al (2021). US Commerce Department issues 'Military End User' List. White and Case, 7 January 2021. https://www.whitecase.com/publications/alert/us-commerce-department-issues-military-end-user-list

Cabinet Office (2021). *The Integrated Review*, 16 March 2021. https://www.gov.uk/government/collections/the-integrated-review-2021

Cabinet Office, UK Statistics Authority, Government Digital Service HM Passport Office. *Research Code of Practice and Accreditation Criteria*. Updated 1 March 2018. https://www.gov.uk/government/consultations/digital-economy-act-part-5-data-sharing-codes-and-regulations/research-code-of-practice-and-accreditation-criteria

Chang, M. (2015). 'Weapons of the 21st Century', *China Military Science*, 30:1, 1995, pp.19-24. In: Pillsbury, 2015.

Cooley LLP (2021). *Committee on Foreign Investment in the United States: CFIUS Overview*. https://www.cooley.com/services/practice/export-controls-economic-sanctions/cfius-overview

Clark, R. and Jennings, P. (2020). Defence and industry could fund cutting-edge university research with Five Eyes allies. *The Strategist (ASPI Blog)*. 12 August 2020. https://www.aspistrategist.org.au/defence-and-industry-could-fund-cutting-edge-university-research-with-five-eyes-allies/

Crane, K. et al.: *Modernizing China's Military: Opportunities and Constraints*. Santa Monica, CA: RAND Corporation, 2005.

Davies, C and Ormond, J. *Briefing Note: National Security and Investment Act 2021*. Ashfords, 11 June 2021. https://www.ashfords.co.uk/news-and-media/general/national-security-and-investment-act-2021-briefing-note

Defense Advanced Research Projects Agency. 'DARPA mission'(https://www.darpa.mil/about-us/mission). Retrieved 3 July 2020.

Press release: New Office for Investment to drive foreign investment into the UK. Department for International Trade, 29 November 2020. https://www.gov.uk/government/news/new-office-for-investment-to-drive-foreign-investment-into-the-uk

Department for International Trade Export Control Joint Unit. *Consolidated list of strategic military and dual-use items that require export authorisation.* 10 April 2013. https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation

Department for International Trade and Export Control Joint Unit. *Guidance: UK Strategic Export Control Lists*. Published 3 August 2012. (Last updated 23 February 2017).

https://www.gov.uk/guidance/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items

Department of Defence (Australian Government). *2020 Defence Strategic Update & 2020 Force Structure Plan*. https://www1.defence.gov.au/strategy-policy/strategic-update-2020

Export Control Joint Unit and Department for International Trade (2021). *Case study: Export controls on academic research*. (31 March 2021). https://www.gov.uk/government/case-studies/export-controls-on-academic-research

Export Control Joint Unit and Department for International Trade (2021). *Exporting military or dual-use technology: definitions*. (18 March 2021). https://www.gov.uk/government/publications/exporting-military-or-dual-use-technology-definitions

Export Control Joint Unit and Department for International Trade (2021). *Guidance: Export controls applying to academic research*. (31 March 2021). https://www.gov.uk/guidance/export-controls-applying-to-academic-research

Export Control Joint Unit and Department for International Trade (2020). *Guidance: Consolidated list of strategic military and dual-use items that require export authorisation*. 10 April 2013 (Last updated 14 December 2020). https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation

Foreign & Commonwealth Office; Foreign, Commonwealth & Development Office. *Academic Technology Approval Scheme (ATAS)*. Published 25 March 2013. Last updated 6 October 2020. https://www.gov.uk/guidance/academic-technology-approval-scheme

Foreign, Commonwealth & Development Office and Export Control Joint Unit. (2020). *Collection: UK arms embargo on mainland China and Hong Kong*. Published 31 December 2020. https://www.gov.uk/government/collections/uk-arms-embargo-on-mainland-china-and-hong-kong#:~:text=Since%201989%2C%20following%20Chinese%20military,was%20extended%20to%20Hong%20Kong

Foreign Investment Review Board (2020). *About FIRB*. https://firb.gov.au/about-firb

Gibson and Dunn. (2020). *New Controls on Emerging Technologies Released, While U.S. Commerce Department Comes Under Fire for Delay.* Blog: 27 October 2020. https://www.gibsondunn.com/new-controls-on-emerging-technologies-released-while-us-commerce-department-comes-under-fire-for-delay/

Greenberg Traurig (2021). *GT Alert: U.S. Prohibits Trading in Securities of Communist Chinese Military Companies, but NYSE Reverses Plan to Delist* (4 January 2021).

https://www.gtlaw.com/en/insights/2021/1/us-prohibits-trading-in-securities-of-communist-chinese-military-companies

Hellyer, M. and Jennings, P. (2020). 'Australian universities must rethink their broken business model or risk failure.' *The Strategist (ASPI Blog)*. 28 May 2020. https://www.aspistrategist.org.au/australian-universities-must-rethink-their-broken-business-model-or-risk-failure/

Henley, C. (2021). *Carmelite Chambers Blog: Will 200 academics really be jailed? The Export Control Order 2008, the People's Republic of China, and the Daily Mail*. https://www.carmelitechambers.co.uk/blog/blog-will-200-academics-really-be-jailed-export-control-order-2008-peoples-republic-china-and

Home Office. (2021). *Immigration Rules Appendix ATAS: Academic Technology Approval Scheme (ATAS)*. 21 May 2021. https://www.gov.uk/guidance/immigration-rules/immigration-rules-appendix-atas-academic-technology-approval-scheme-atas

Home Office (2021). *Statement of changes to the Immigration Rules*. 4 March 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/966644/CCS001_CCS0221107260-001_Statement_of_changes_in_Immigration_Rules__Web_Accessible_.pdf

House of Commons Foreign Affairs Committee. Striking the balance: Protecting national security through foreign investment legislation. Sixth Report of Session 2019-2021. January 2021. https://committees.parliament.uk/publications/4319/documents/43959/default/

House of Lords Science and Technology Select Committee. Science research funding in universities (4th Report of Session 2017-19 – published 8 August 2019 – HL Paper 409). https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/409/40902.htm

HM Government. *Sanctions and Anti-Money Laundering Act 2018*. https://www.legislation.gov.uk/ukpga/2018/13/contents/enacted/data.htm

Imperial College London (2021). *Academic Technology Approval Scheme (ATAS) – for international researchers*. https://www.imperial.ac.uk/human-resources/compliance-and-immigration/immigration/academic-technology-approval-scheme-atas/

Jalinous, F. et al (2018). *CFIUS Reform Becomes Law: What FIRRMA Means for Industry*. White and Case. https://www.whitecase.com/publications/alert/cfius-reform-becomes-law-what-firrma-means-industry

Jennings, P. and Clark, R. (2020). University funding can be boosted through defence research. Australian Strategic Policy Institute, 11 August 2020. https://www.aspi.org.au/opinion/university-funding-can-be-boosted-through-defence-research

Joske, A. (2018). *Picking Flowers, Making Honey: The Chinese Military's Collaboration with Foreign Universities*. Australian Strategic Policy Institute.

Jones Day (2021). *U.S. Department of Commerce Establishes Military End User List.* Jones Day, February 2021. https://www.jonesday.com/en/insights/2021/02/us-department-of-commerce-establishes-military-end-user-list

Joske, A. (2019). *The China Defence Universities Tracker*. Australian Strategic Policy Institute.

Kenlon, F. (2019). *Protecting DoD-Funded Research in Universities and Research Centers* (Blog post, October 18, 2019). Defence Acquisition University. https://www.dau.edu/training/career-development/intl-acq-mgmt/blog/Protecting-DoD-Funded-Research-in-Universities-and-Research-Centers

King's College London News Centre, 19 July 2015. *Project Alpha and association of university legal practitioners issue export control guidance for academia*. https://www.kcl.ac.uk/news/project-alpha-and-association-of-university-legal-practitioners-issue-export-control-guidance-for-academia

Kliman, D. and Thomas-Noone. B (2018). 'How the Five Eyes Can Harness Commercial Innovation'. *Center for A New American Security (Blog).* 27 July 2018. https://www.cnas.org/publications/commentary/how-the-five-eyes-can-harness-commercial-innovation

Lam, E and Ossinger, J. 'What Do the Two U.S. Blacklists of Chinese Companies Do?' *Bloomberg Quint*, 15 January 2021. https://www.bloombergquint.com/onweb/what-do-the-two-u-s-blacklists-of-chinese-companies-do-q-a#:~:text=Inclusion%20on%20the%20Entity%20List,build%20weapons%20of%20mass%20destruction

Missile Technology Control Regime. Frequently Asked Questions (FAQS) (Accessed: 15 April 2021). https://mtcr.info/frequently-asked-questions-faqs/

NAFSA: Association of International Educators (2021). *Proclamation Suspending Entry of Chinese Students and Researchers Connected to PRC 'Military-Civil Fusion Strategy'*. 11 June 2021. https://www.nafsa.org/regulatory-information/proclamation-suspending-entry-chinese-students-and-researchers-connected-prc

National Law Review. 'CFIUK Comes to Life: The National Security and Investment Act 2021'. *The National Law Review*, 20 May 2021. https://www.natlawreview.com/article/cfiuk-comes-to-life-national-security-and-investment-act-2021

Parman, R. (2019). *An elemental issue*. The United States Army, 26 September 2019. https://www.army.mil/article/227715/an_elemental_issue

Peled, D. (2001). *Defense R&D and Economic Growth in Israel: A Research Agenda*. Paper prepared for 'Science, Technology and the Economy' (STE) Program/Workshop, University of Haifa, March 2001. https://econ.hevra.haifa.ac.il/~dpeled/papers/ste-wp4.pdf

Pensana Plc (2021). *Establishing a World-Class Sustainable Supply of critical Rare Earths for the Green economy*, 21 April 2021. https://pensana.co.uk/wp-content/uploads/2021/04/21.04.21-FINAL-Pensana-Announcement-of-Business-Plan.pdf

Pillsbury, M. (2015). The Hundred-Year Marathon: China's Secret Strategy to Replace America As the Global Superpower. St Martin's Griffin.

Salisbury, E. (2021). *ARIA and Defence: A Missed opportunity?* LSE Blogs 8 March 2021. https://blogs.lse.ac.uk/impactofsocialsciences/2021/03/08/aria-and-defence-a-missed-opportunity/

Samuel, J. 'Finally we are waking up to how our universities may be arming China'. The Telegraph, 13 February 2021. https://www.telegraph.co.uk/politics/2021/02/13/finally-waking-universities-may-arming-china/

Secretary of Defense. *Memorandum*. 24 October 2018. https://www.dau.edu/cop/iam/_layouts/15/WopiFrame.aspx?sourcedoc=/cop/iam/DAU%20Sponsored%20Documents/DoD%20Protecting%20Critical%20Technology%20Task%20Force%20Memo%2010-24-18.pdf&action=default

Shepardson, D. et al. 'Trump administration takes final swipes at China and its companies'. Reuters, 14 January 2021. https://www.reuters.com/business/energy/trump-administration-takes-final-swipes-china-its-companies-2021-01-15/

Shoebridge, M. (2020). 'Partnership with government needed to rebuild universities' business model.' *The Strategist (ASPI Blog)*. 17 June 2020. https://www.aspistrategist.org.au/government-partnership-needed-to-rebuild-universities-business-model/

Smith B. and Dawson J. (2020). *House of Commons Library Research Briefing: Magnitsky Legislation*. (20 July, 2020). https://commonslibrary.parliament.uk/research-briefings/cbp-8374/

Smith, J. (2020). 'DOD to award $50m to universities to accelerate basic research.' *MeriTalk*. https://www.meritalk.com/articles/dod-to-award-50m-to-universities-to-accelerate-basic-research/

Smith, R.J. 'Hypersonic Missiles Are Unstoppable. And They're Starting a New Global Arms Race.' *New York Times*, 19 June, 2019. https://www.nytimes.com/2019/06/19/magazine/hypersonic-missiles.html

Stretton, A. and Harriss, L. (2019). *Research briefing: Access to critical materials*. UK Parliament, 13 September 2019. https://post.parliament.uk/research-briefings/post-pn-0609/

Sutton, P. *UK policy for defence research and technology*. (Ch. 7) and Kirkpatrick, D. *Research, technology and UK national security*. (Ch. 9). In: *Britain and security* (Paul Cornish, Ed.) Smith Institute. http://www.smith-institute.org.uk/wp-content/uploads/2015/10/BritainandSecurity.pdf

Research Services, University of Sheffield (2021). *Guidance on Export Control Legislation*. https://www.sheffield.ac.uk/rs/export

Ropes and Gray LLP (2020). Senate Introduces the 'Safeguarding American Innovation Act,' Targeting Foreign Influence and Unreported Foreign Ties in Research. Ropes and Gray LLP, 24 June 2020. https://www.lexology.com/library/detail.aspx?g=2921e4ce-4613-45ee-94cd-9543f3d6a8ff

Taylor T. and Lucas, R. (2021). *New UK Government Initiative to Support High-Risk, High-Reward Military Science Needs Refinement*. Royal United Services Institute (RUSI). https://rusi.org/commentary/new-uk-government-initiative-support-high-risk-high-reward-military-science-needs

Tylecote, R. (2021). 'Novel weapons: Could we be unwittingly researching both sides of a hypersonic arms race?' *The Critic*. 26 March 2021. https://thecritic.co.uk/the-problem-with-chinas-hypersonic-missiles/

Tylecote, R and Clark, R. (2020). *A Long March through the Institutions: Understanding and responding to China's Influence in international organisations* London: Civitas. https://www.civitas.org.uk/content/files/A-Long-March.pdf

Tylecote, R and Clark, R. (2021). *Inadvertently Arming China? The Chinese military complex and its potential exploitation of scientific research at UK universities.* London: Civitas. https://civitas.org.uk/publications/inadvertently-arming-china/

Undersecretary of Defense. *1 July 2019 Memorandum*. https://www.dau.edu/cop/iam/_layouts/15/WopiFrame.aspx?sourcedoc=/cop/iam/DAU%20Sponsored%20Documents/USD%20R-E%20Ltr%20to%20Sen%20Grassley%20on%20Foreign%20Threats%20to%20Taxpayer%20Funded%20Research%207-1-2019.pdf&action=default

Universities UK (2020). *Managing risks in Internationalisation: Security related issues*. https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/managing-risks-in-internationalisation.aspx

University of Sheffield (2020). *Information for staff: Funding of Research in UK Higher Education*. https://www.sheffield.ac.uk/finance/staff-information/howfinanceworks/higher_education/funding_of_research

US Department of the Treasury. *Chinese Military Companies Sanctions*. (Accessed 1 May 2021). https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/chinese-military-companies-sanctions

US Department of the Treasury. *Non-SDN Communist Chinese Military Companies List (NS-CCMC List)* (last updated: 30 April 2021). https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/ns-ccmc-list

Warrell, H. and Staton, B. 'UK universities to be offered advice on national security threats.' *Financial Times*, 25 May 2021. https://www.ft.com/content/a264793d-cfd6-4fb3-89e7-d65ffb5ec01f

Wassenaar Arrangement (Wassenaar.org). (2019). Criteria for the selection of dual-use items. (Adopted in 1994 and amended by the Plenary in 2004 and 2005). https://www.wassenaar.org/app/uploads/2019/consolidated/Criteria_for_selection_du_sl_vsl.pdf

Wassenaar Arrangement Secretariat. (2020). Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Public Documents. Volume II List of Dual-Use Goods and Technologies And Munitions List, December 2020. https://www.wassenaar.org/app/uploads/2020/12/Public-Docs-Vol-II-2020-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-20-3.pdf

White House Briefing Room. *Fact Sheet: Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China*. 3 June, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/03/fact-sheet-executive-order-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/

Appendices

Appendix 1

Exporting military or dual-use technology: definitions[157]

Advice on how military and dual-use technology is defined for export controls:

Export controls for technology aim to prevent transfers that can lead to developing or producing weapons or goods which: could be used against the UK and allied forces; cause national security concerns.

Technology: definition and scope:

…You can find complete list of defined terms in the UK strategic export control lists… information may take many forms, including: blueprints, plans, diagrams, models, formulae [etc.]

Certain technology may also be subject to end-use controls if it is in relation to: WMD, certain arms embargoes [and] unauthorised military exports.

In the case of technology related to WMD, here the definition of technology is very broad.'

'Information in the public domain and for basic scientific research

The controls on technology do not apply to: information that is in the public domain; basic scientific research.

For technology to be in the public domain it has to be freely available with no restriction other than copyright placed on its further dissemination, such as in a book, on a website, at an exhibition.

Information in the public domain may come in many forms including: general product information, brochures [etc.]

Technology is not in the public domain: if it needs to be obtained from a supplier who controls the supply; where access is restricted to certain persons, like membership of an institute or requiring passwords; where it is subject to the Official Secrets Act, or MoD or government security classifications such as commercially confidential information; [or]if it has been placed in the public domain in contravention of a statutory prohibition, for

[157] Export Control Joint Unit and Department for International Trade. *Exporting military or dual-use technology: definitions*. (18 March 2021). https://www.gov.uk/government/publications/exporting-military-or-dual-use-technology-definitions

example classified material, as it is unlikely to be available without further restriction upon its dissemination.

The same relaxations apply to published technical papers if the content is in the public domain. However, the intention to publish a paper containing controlled technology does not in itself place that information in the public domain. Any collaboration or sharing of controlled technology overseas, such as through a peer review before publication of a technical paper or the results of research and development, would require a licence.

‘Technology (UK)

Technology means specific ‘information’ necessary for the development, production or use of goods or software. where:

‘Information’ may take forms including, not limited to: blueprints, plans, diagrams, models, formulae, tables, ‘source code’, engineering designs and specifications, manuals and instructions written or recorded on other media or devices (for example disk, tape, read-only memories).

‘Source code’ (or source language) is a convenient expression of one or more processes which may be turned by a programming system into equipment executable form.’

Transfer (UK):

Transfer, in relation to software or technology, means transfer by electronic or non-electronic means (or any combination of electronic and non-electronic means) from a person or place within the United Kingdom to a person or place outside the United Kingdom, except in articles 10 and 11 where the limitations as to the origin and destination of the transfer do not apply, and cognate expressions shall be construed accordingly.’

Appendix 2

Items on current UK control lists

The following examples illustrate goods and technologies on UK control lists.[158] These are only indicative of the covered areas.

The UK Military List

This includes:

- Electronic guidance and navigation equipment;
- Vessels (surface or underwater);
- 'Aircraft', 'lighter-than-air vehicles', 'Unmanned Aerial Vehicles' ('UAVs'), aero-engines and 'aircraft' equipment, related goods, and components as follows, specially designed or modified for military use:
    - 'UAVs', Remotely Piloted Air Vehicles (RPVs), autonomous programmable vehicles and unmanned 'lighter-than-air vehicles';
- Launchers, recovery equipment and ground support equipment;
- Equipment designed for command or control; Propulsion aero-engines and specially designed components therefor; and
- Electronic equipment, 'spacecraft' and components, not specified elsewhere in [this] Schedule [including] Global Navigation Satellite Systems (GNSS) jamming equipment and specially designed components therefor.

The list also 'controls all electronic guidance and navigation equipment Goods and material, coated, treated or prepared to provide signature suppression, specially designed for military use'.

The UK Dual-Use List

This includes the products listed below and the 'technology' for many of these:

- Remotely operated vehicles;
- [Various] metal alloys, metal alloy powder and alloyed materials;
- Metals in particle sizes of less than 60 µm whether spherical, atomised, spheroidal, flaked or ground, manufactured from material consisting of 99 per cent or more of zirconium, magnesium and alloys thereof;
- Materials and devices for reduced observables, such as radar reflectivity, ultraviolet/infrared;
- [Various] signatures and acoustic signatures [usable] in 'missiles', 'missile' subsystems or unmanned aerial vehicles (specified; includes: a. Structural materials and coatings specially designed for reduced radar reflectivity; b. Coatings, including

[158] Department for International Trade Export Control Joint Unit, 2013.

paints, specially designed for reduced or tailored reflectivity or emissivity in the microwave, infrared or ultraviolet regions of the electromagnetic spectrum);

- A range of graphite, ceramic, and ultra-high temperature ceramic materials – including Hafnium carbide (HfC) (including usable for missile components (such as nose-tips, re-entry vehicles, leading edges, jet vanes, control surfaces or rocket motor throat inserts) in 'missiles', [some] space launch vehicles, [some] sounding rockets [or] 'missiles');
- Hafnium metal and alloys (with certain properties);
- Maraging steels useable in 'missiles' (with certain properties);
- Certain single or complex oxides of zirconium and complex oxides of silicon or aluminium; and
- Robots designed to comply with national safety standards applicable to potentially explosive munitions environments, to operate at high altitudes or withstand high radiation.

Under the category *Telecommunications and Information Security*:

- Mobile telecommunications interception or jamming equipment;
- Telemetry and telecontrol equipment (including ground equipment, designed or modified for 'missiles');
- 'Information security' systems and components for the control of 'satellite navigation system' receiving equipment containing or employing decryption;
- 'Cryptography for data confidentiality' having a 'described security algorithm' in some conditions; and
- Certain systems, equipment and components for defeating, weakening or bypassing 'information… security' (including 'functions designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data, including clear text, passwords or cryptographic keys').

The dual list includes:

- Hydrophones (including 'Flexible piezoelectric composites');
- Gyros usable in missiles; and
- Certain 'integrated navigation systems', designed or modified for 'missiles'.

Under the *Marine* category:

- Submersible vehicles and surface vessels;
- Unmanned submersible vehicles;
- 'Robots' specially designed for underwater use, controlled by using a dedicated computer; and
- Propellers, power transmission systems, power generation systems and certain noise reduction systems.

Under *Aerospace*:

- Aero gas turbine engines with various technologies;
- Ramjet, scramjet or 'combined cycle engines', and specially designed components therefor;
- 'Unmanned aerial vehicles' ('UAVs'), unmanned 'airships', related equipment [and] components [including] Air breathing reciprocating or rotary internal combustion type engines, specially designed or modified to propel 'UAVs' or unmanned 'airships', at altitudes above 15,240 metres (50,000 feet);
- Vehicles for transport, handling, control, activation or launching, designed or modified for space launch vehicles (specified elsewhere), sounding rockets (specified elsewhere) or 'missiles';
- Other 'technology' 'required' for the 'development' or 'production' of any of the following gas turbine blades, vanes or 'tip shrouds', made from directionally solidified (DS) or single crystal (SC) alloys; and
- Components [manufactured] from organic 'composite' materials designed to operate above 588K (315°C).

Under *Stealth technology*:

- Materials specially designed for absorbing electromagnetic radiations, or intrinsically conductive polymers (and some materials and devices for reduced observables, such as radar reflectivity, ultraviolet/infrared signatures and acoustic signatures, or usable in some 'missiles', 'missile' subsystems or unmanned aerial vehicles, unless formulated solely for civil applications);
- 'Software' for analysis of reduced observables, such as radar reflectivity, ultraviolet/infrared signatures and acoustic signatures; and
- Some pulse radar cross-section measurement systems and components.