Chapter
09

The UK's enforcement of dual-use export controls

Dominic Williams
Researcher - Alpha Project, King's College London

Ian J Stewart
Head - Alpha Project, King's College London»

1. INTRODUCTION

The United Kingdom has one of the longest standing export control systems in the world, with its origins dating back to at least the Second World War. This system has evolved over time – particularly after the end of the Cold War, the adoption of EU regulations, and the adoption of UNSC Resolution 1540.[222] The UK's long history with export controls and its advanced manufacturing base likely means that the country has among the greatest experience in enforcing export controls on dual-use items.

The purpose of this chapter is to examine the UK's enforcement of dual-use export controls. The chapter begins by providing a brief history of the UK's development of dual-use export controls. This includes examining the origins and history of UK export controls, how these measures transitioned to become an instrument of the Cold War, and the important events that shaped the modern enforcement environment, such as the Scott Inquiry into the sale of dual-use and military goods to Iraq. The infrastructure that was created to ensure that this Supergun scenario not be repeated is also examined. More recent enforcement practices are also examined. Finally, some current challenges in the enforcement landscape are set out.

---

222 UNSCR 1540 creates legally binding obligations for Member States to enforce measures against the proliferation of WMD using controls. UN Security Council "UNSCR 1540", Available at http://www.ipu.org/splz-e/civ1540/1540.pdf accessed 21 March 2016.

2. BRIEF CHRONOLOGICAL HISTORY OF ENFORCEMENT OF EXPORT CONTROLS IN THE UK

The UK has continuously applied strategic trade controls in some form since 1939 when, at the outset of the Second World War, the "Trading with the Enemy Act" and "Import, Export and Customs Powers (Defence) Act" were quickly passed through Parliament and into law. [223, 224,225] This legislation served to prohibit "any commercial, financial or other intercourse with, or for the benefit of, an enemy or a person acting on behalf of an enemy".[226] The laws amounted to a blanket ban on economic interaction between the UK and those states with which it was at war. It should be noted that this was not the first attempt to control the movement of goods between the UK and its adversaries; for example a trading with the enemy act was passed at the beginning of the First World War, but was allowed to expire in the mid-1930s. Rather, the acts passed in 1939, mark the start of an unbroken period of controls over the trade in strategic goods that has lasted until the present day.

Indeed, the end of WWII did not bring an end to the perceived need for restrictions on trade. The rivalry between East and West brought with it a fresh imperative to control trade, and the controls that emerged during the Cold War were more focused than previous efforts. They were political instruments in and of themselves, designed to deprive the Eastern Bloc of specific capabilities and technologies. A key feature of the Cold War export

223 "Trading with the Enemy Act 1939" available at http://www.legislation.gov.uk/ukpga/Geo6/2-3/89/enacted accessed 21 March 2016.

224 Measures to restrict trade between Britain and other nations had been put in place previously. For example during WW1. The underpinning legislation was eventually repealed.

225 "Import, Export and Customs Powers (Defence) Act", Chapter 69. Available at: http://www.legislation.gov.uk/ukpga/1939/69/pdfs/ukpga_19390069_en.pdf accessed 21 March 2016.

226 "Trading with the Enemy Act 1939", Chapter 89. Available at: http://www.legislation.gov.uk/ukpga/Geo6/2-3/89/enacted accessed 21 March 2016.

control landscape was The Coordinating Committee for Multilateral Export Controls (COCOM). COCOM was an informal multilateral organisation set up in 1947 which aimed to coordinate the national controls applied over the export of strategic technology and materials to communist states.[227] Unlike WWII era blanket trade bans, COCOM maintained several lists containing specific technologies. The aim of these lists was to allow trade to continue between East and West, whilst maintaining control over technologies that could be used to develop nuclear and conventional forces. This more targeted approach was in recognition that prohibiting all trade would harm economic growth in the west at the same time as harming the Soviet Bloc.

The next major development in the strategic export control landscape came in May 1974 when India conducted its first nuclear bomb test. Codenamed "Smiling Buddha," the Indian government claimed the test was a 'peaceful nuclear explosion'.[228] Despite its placid moniker, the test caused a great deal of concern internationally and highlighted how certain non-weapons specific nuclear technology could easily be used for the purposes of weapons development. It became apparent that further limits on the exports of nuclear equipment and technology were required. In response to the implications of the Indian nuclear test, the Nuclear Suppliers Group (NSG) was set up in 1975. Through meetings hosted by the UK, a "Trigger List" was created that placed controls on certain nuclear related technologies, essentially restricting such exports to those states that had specific safeguards in place with the International Atomic Energy Agency. In 1991, after the revelations of Iraqi weapons programmes, a "dual-use list" was drawn up in order to further

---

227 Office of Technology Assessment. Chapter 8, Multilateral Export Control Policy: The Coordinating Committee (CoCom) in "Technology and East-West Trade". (November 1979). Available at https://www.princeton.edu/~ota/disk3/1979/7918/791810.PDF accessed 21 March 2016.

228 Nuclear Weapon Archive. "India's Nuclear Weapons Program" available from http://nuclearweaponarchive.org/India/IndiaSmiling.html accessed 21 March 2016.

tighten access to equipment that had scope to be used in a nuclear weapons programme but which also had established non-nuclear industrial uses.

In the 1980s the UK continued to play a leading role in further developing the global trade control landscape. The extensive use of chemical weapons by Iraq during the Iran-Iraq war in the 1980s – with certain precursor chemicals and chemical manufacturing equipment having been sold legally from the UK - served to highlight the necessity for states to better identify, and subsequently control, exports which would facilitate the development of chemical and biological weapons. The Australia Group, with its lists of controlled chemical and biological related goods, was subsequently established in 1985 in order to aid governments in the effective control of such technologies. The 1980s also saw the establishment of The Missile Technology Control Regime (MTCR). Set up in 1987, the MTCR sought to further respond to increased WMD proliferation through the enactment of controls on un-manned delivery systems and their means of production.

By the 1990s the Cold War had ended and so too had the need to enforce embargos on the Soviet states.[229] Indeed, COCOM had little relevance in the post-Cold War world. An arrangement that did not have an East vs West focus and allowed for the inclusion of former COMECON states was required. The Wassenaar Arrangement was established in July 1996 to fill this role, and deal with regional and international risks relating to the spread of conventional weapons and dual-use technology. Several former Soviet states were among its founding members.[230]

The 1990s also saw important domestic developments within the UK's export control framework. Following the end of the

---

229 COMECON, the Council for Mutual Economic Assistance (CMEA), was established in 1949 to facilitate economic development in the Eastern European countries that comprised the Soviet bloc. Oxford Public International Law "Council for Mutual Economic Assistance" available at http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e606 accessed 21 March 2016.

230 Wassenaar Arrangement. "About Us", available from http://www.wassenaar.org/about-us/ accessed 21 March 2016.

Gulf War, questions were asked about the involvement of British companies in the supply of weapons and dual-use equipment to Saddam Hussein's regime. In 1992 the directors of the Coventry-based machine tool manufacturer Matrix Churchill, were put on trial for supplying the Iraqi regime with equipment and knowledge. However the trial collapsed when it was revealed that the company had been advised by government officials on how best to sell arms to Iraq. Government officials had also failed to identify the true end use of massive highly machined tubes being sought by Iraq from the UK: in the construction of the barrel for Saddam's so-called Supergun that could fire satellites into orbit (or nuclear weapons a very long way indeed). This scandal, referred to as the "Arms to Iraq Affair," culminated in the 1996 publication of The "Report of the enquiry into the Export of Defence Equipment and Dual-Use Goods to Iraq and Related Prosecutions", commonly referred to as the Scott Report.[231] One of the primary findings was the inadequacy of the existing legislation covering export controls, and lack of transparency. For example, the Import, Export and Customs Powers (Defence) Act 1939, allowed the government to issue regulations relating to the control of the export of particular goods to particular countries without first presenting them before Parliament. This Act was emergency legislation and should have lapsed in 1945, yet it remained, even being included as part of the Import and Export Control Act (1990).

Another important outcome of the Scott Report was to formalise the use of intelligence in support of export licencing and enforcement in the UK. This reinforced the importance of the 'Restricted Enforcement Unit' as a forum to coordinate UK enforcement actions in the UK and elsewhere.[232] This forum involves several relevant government departments, including the Foreign and

---

231 "The Report of the Inquiry into the Export of Defence Equipment and Dual-Use Goods to Iraq and Related Prosecutions" Chapter 2.67. Available from http://www.iraqwatch.org/government/UK/Scott%20Report/Scott-TOC.htm accessed 21 March 2015.

232 *Ibid*.

Commonwealth Office, the Ministry of Defence, HM Revenue and Customs and the intelligence agencies.[233] This forum is a key focal point for interagency cooperation on enforcement action in the UK and continued to operate at least until one of the authors left government in 2010.

The UK's implementation of export controls began to shift for broader political reasons after this point. The UK, as a member of the EU, became bound by the European Council regulation 1334/2000 export controls were made a competence of the European Union under Article 30 of the Treaty establishing the European Community in June 2000.[234] As with other EU member states, the UK continued to be responsible for implementation of the regulation, however, meaning that the country would leverage its long experience in implementing non-proliferation measures to put the new EU regulation into effect.

A final important evolution of the implementation of export controls in the UK resulted from the adoption of Security Council resolutions. Of particular note was Security Council Resolution 1540 in 2004 which resulted in an expansion of controls to transit, transhipment and brokering activities. However, Security Council sanctions resolutions would also have an important effect on the UK's enforcement landscape as the trade-related provisions in these resolutions are generally implemented using the same apparatus that is used to implement export controls in the UK.

---

233 Commons Debates - Previous sessions, "Trade and Industry" available from http://www.publications.parliament.uk/pa/cm199798/cmhansrd/vo980604/text/80604w07.htm accessed 21 March 2016.

234 Council of the European Union. "COUNCIL REGULATION (EC) no. 1334/2000" Available from http://www.sussex.ac.uk/Units/spru/hsp/documents/2000-0622%201334-2000.pdf accessed 21 March 2016.

3. THE CURRENT EXPORT CONTROL LANDSCAPE

There are several main components of the present UK export control system. The main legal basis for controls on the export of dual-use goods in the UK is the EU Dual-Use Regulation (also known as Council regulation No 428/2009), which is applicable to all EU countries. The EU issued legislation to control exports of dual-use items and technology in 2000 (through EC Regulation 1334/2000) with the regulation being re-issued in 2009. The regulation "sets out the scope, authorisations (including brokering), control measures, customs procedures and other measures concerning the control of dual-use goods across the EU."[235] Subsequently, UK enforcement of dual-use export controls finds its legislative foundation in The Export Control Act (2002). The Act provides a consolidated framework of controls, which largely served to replace the existing system of secondary legislation and executive discretion.[236] It provides guidance on how export controls can be imposed, when they can be imposed and who may impose them, within the UK. The Act enshrines the authority of the Secretary of State to impose export or trade controls in relation to any goods whose export, acquisition, disposal, movement or use could lead directly or indirectly to any provisions on a list of "relevant consequences."[237] Importantly, it also includes clauses for activities that could be associated with the illegal export of controlled goods, placing controls on trafficking and brokering, as well as on the provision of 'technical assistance'.[238] Another significant aspect of

---

235 Department for Business, Innovation & Skills, "Controls on dual-use goods" Available from https://www.gov.uk/guidance/controls-on-dual-use-goods accessed 21 March 2016.

236 Joyner, D., "Non-proliferation Export Controls: Origins, Challenges, and Proposals for Strengthening" (Ashgate: Farnham, 2006), p. 142.

237 Export Controls Act 2002. Available from http://www.legislation.gov.uk/ukpga/2002/28/contents accessed 21 March 2016.

238 Export Control Act 2002, Section 3. Available from: http://www.legislation.gov.uk/ukpga/2002/28/section/3 accessed 21 March 2016.

this legislation allows controls to be imposed on acts undertaken outside the UK if they are carried out by a person who is or is acting under the control of a UK national.[239] The Customs and Excise Management Act (1979) serves to consolidate and codify the main customs powers of HMRC, the government department with the main responsibility for the enforcement of UK export control laws. Other legislation relevant to the UK enforcement of dual-use export controls include: The Terrorism Act (2000), Anti-Terrorism, Crime and Security Act (2001), Export of Goods, Transfer of Technology and Provision of Technical Assistance Order (2003), and the Trade in Goods Control Order (2003).

The list of dual-use items controlled by the UK is mostly drawn from EU legislation and their associated control lists. EU control lists in turn incorporate the guidance and control lists from the four multilateral export control regimes: the Australia Group (AG), The Missile Technology Control Regime (MTCR), The Nuclear Suppliers Group (NSG), and the Wassenaar Arrangement (WA). The UK has opted to add controls on certain "paramilitary" items as a result of its experience of Northern Ireland-related terrorism in the past.[240] All of the UK's control lists are published collectively as part of the UK Strategic Export Control Lists: Consolidated List of Military and Dual-Use Items.[241] Importantly, if a specific good is not listed on the control lists, it may still be subject to 'end-use' controls, and therefore require a licence in order to export. In keeping with the requirements of Resolution 1540, and building on the catchall concept developed by the UK, the British Government also has the

---

239 Export Control Act 2002, Section 11. Available from: http://www.legislation.gov.uk/ukpga/2002/28/section/11 accessed 21 March 2016.

240 Export control Organisation. "Guidance on export of technology" Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/15203/Export_of_technology_Guidance_-_URN_10-660_-_new_logo_-_2012.pdf accessed 21 March 2016.

241 Department for Business, Innovation & Skills. "Consolidated list of strategic military and dual-use items that require export authorisation" Available at: 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 accessed 21 March 2016.

power to make non-listed goods subject to control. These so-called 'end use controls' apply to goods where there is a concern that the end-use may be in a WMD programme.[242]

The Export Control Organisation (ECO) is responsible for the issuing of licences for the export of goods included in the UK Strategic Export Control Lists. It monitors and enforces exporters' compliance with export controls through visits to exporters and audits of their business.[243] The primary organisation involved in the enforcement of UK strategic export controls is HM Revenue and Customs (HMRC). The police – and indeed the National Crime Agency - could become involved in export control issues, although, at least at the time of writing, this was not generally the case. The agency that first detects a suspected offence is the one responsible for its investigation. Although, most offences are detected by customs officers at the border, or during trade audits, both of which are carried out by HMRC.[244] HMRC fields a staff of customs officers posted at sea and air ports that see high freight traffic volumes. Export violations investigated by HMRC are then prosecuted by an independent entity, the Revenue and Customs Prosecution Office (RCPO). The RCPO was set up in 2005 in order to separate the investigation and prosecution functions for customs offences, which had previously been handled by customs service prosecutors. This relationship mirrors that of the Crown Prosecution Service (CPS) and the Police.

Under the Customs and Excise Management Act, breaches of export controls fall into two categories. Strict Liability Offences are

---

242 Department for Business, Innovation & Skills and Export Control Organization. "Weapons of mass destruction: end-use control" Available from: https://www.gov.uk/guidance/weapons-of-mass-destruction-wmd-end-use-control accessed 21 March 2016.

243 Department for Business, Innovation & Skills. "Compliance and enforcement of export controls" (2012, September 6). Available at: https://www.gov.uk/guidance/compliance-checks-and-enforcement-of-export-controls-on-strategic-goods-and-technology accessed 6 April 2016.

244 Wetter, Anna. "Enforcing European Union Law on Exports of Dual-use Goods", SIPRI Research Report, no. 24 (2009). Available from: http://books.sipri.org/files/RR/SIPRIRR24.pdf accessed 21 March 2016.

offences that, regardless of the knowledge or intent of the exporter, lead to punishment. These types of offences therefore include acts of negligence, where an exporter may have been unaware that the goods being exported required a licence.[245] Punishment for this type of offence include: the seizure of goods, financial penalties up to three times the value of the goods exported (or attempted export), and if knowledge of a WMD end-use is proven, up to two years in prison.[246] Less serious cases could result in traders having to pay a compound penalty, which is a means by which HMRC can offer the exporter the chance to settle a case that would have justified being referred to the RCPO or CPS. This is offered in order to save the taxpayer and company time and legal fees.[247] The British government has been careful to establish that compounding should not be viewed as a light option. There is no maximum compound penalty limit. The largest compound penalty imposed for an export control related offence was for 575,000 British pounds in 2009.[248] Cases in which it has been proven that the exporter has deliberately attempted to circumvent export controls can result in more stringent penalties. Sanctions for this type of offence can involve prison sentences up to 10 years and unlimited fines.[249] Similar penalties can be imposed for acts relating to export control breaches, such as brokering and trafficking.

Perhaps the main practical tool for enforcement of export controls in the UK is the Customs system, Customs Handling of

---

245 *Ibid*.

246 Croner-I, "Export licencing controls: not just military equipment". Available from https://app.croner.co.uk/feature-articles/export-licencing-controls-not-just-military-equipment?product=32 accessed 21 March 2016.

247 Department for Business, Innovation & Skills. "Compounding penalty cases." (2012, June 6).. Available from http://blogs.bis.gov.uk/exportcontrol/prosecution/compound-penalty-cases/ accessed 21 March 2016.

248 *Ibid*.

249 Croner-i. "Export licencing controls: not just military equipment", https://app.croner.co.uk/feature-articles/export-licencing-controls-not-just-military-equipment?product=32 accessed 21 March 2016.

Import and Export Freight (CHIEF). It is through this system that exporters declare their exports to customs. Exporters are required to link any associated licences with the export declaration.

Customs authorities are able to utilise information from the CHIEF system for purposes of risk profiling.[250] Risk profiling in the customs context is "a practical means of replacing random examination of documents and consignments with a planned and targeted working method, making maximum use of customs resources".[251] Factors that could be taken into account when conducting risk profiling could include whether a licence has been declared in relation to an export (or otherwise), whether the recipient or any other party is known to be of concern, and whether the destination is subject to sanctions or other restrictions. Customs can also create 'risk profiles' in response to either specific intelligence or targeted campaigns intended to identify specific types of shipment of possible concern.[252]

Another important enforcement tool relates to audits. In the UK, both HMRC and the Export Control Organisation can undertake audits of companies to ensure compliance with export control requirements.[253] Such audits routinely identify cases of non-compliance where, for example, the paperwork associated with an export is incomplete or incorrectly completed. However, audits might also be undertaken in more serious cases, including where it is believed that a company is involved in problematic transactions. Audits also provide an opportunity to ensure that companies are compliant

---

250 HM revenue and Customs. "Customs Handling of Import and Export Freight: the processing system of trader declarations", Available from https://www.gov.uk/guidance/chief-trader-import-and-export-processing-system accessed 21 March 2016.

251 HM Revenue and Customs "INCHP08050 - Risk analysis: Part 1: risk analysis in Customs control", available from http://www.hmrc.gov.uk/manuals/inchpmanual/inchp08050.htm accessed 21 March 2016.

252 *Ibid*.

253 Department for Business Innovation and Skills "Compliance and Enforcement of Export Controls" available from https://www.gov.uk/guidance/compliance-checks-and-enforcement-of-export-controls-on-strategic-goods-and-technology accessed 21 March 2016.

with requirements to control intangibles, including with regards to technology. Customs officials typically would have no other way of ensuring compliance in this area as the "intangibles" are typically not detectable when they cross the border.

4. RECENT ENFORCEMENT ACTIONS

Typically, the UK undertakes a few hundred enforcement actions each year.[254] The majority of these are for violations that were non-deliberate in nature and the majority of cases are dealt with through an administrative penalty such as a warning letter. The most common issue, present in around 45% of instances of non-compliance, is incomplete or missing documentation. Other particularly common errors involve sanctioned or embargoed destination countries or goods which require a licence (found in 20 percent and 10% of instances respectively).[255] Cases deemed more serious – either because the exporter was aware of controls or because the export was seen to do harm by, for example, being destined for Iran – have been dealt with either through 'compound penalty' or prosecution. Prosecution is taken only in the most egregious of cases as there is a requirement for the prosecution authority to demonstrate that the prosecution is 'in the public interest'. A part of this determination relates to the harm done and the cost involved in pursuing the case. Cases that end in prosecution usually therefore involve either wilful and deliberate effort to evade controls or a repeat offence. Often it also involves destinations such as Iran. Several recent cases are examined below.

4.1. Delta Pacific Manufacturing

---

254 Information relating to penalties and prosecutions from 2009-2013 provided to the Authors by HMRC.

255 "United Kingdom Strategic Export Controls Annual Report 2014", Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/446050/Strategic_Exports_AR14_tagged.pdf accessed 16th February 2016.

During an investigation conducted by HMRC into a Cambridgeshire-based Company called 'Delta Pacific Manufacturing' it was found that the company director, Gary Summerskill, had attempted to conceal the illegal export of alloy valves to Iran, making three illegal shipments, valued at 3.4 million British pounds, without an export licence. Six types of valves were exported by DPM Ltd, four of which were controlled. Summerskill attempted to circumvent the export ban by diverting the components through Hong Kong. Hong Kong customs authorities discovered the shipment who then alerted HMRC. A second shipment was routed through Azerbaijan, and used a different company name. Both shipments were to go on to an offshore oil company in Iran.[256] HMRC investigators found evidence that Summerskill was fully aware that the final destination of the goods was Iran and that they were subject to an export ban. It is clear too, that Summerskill had knowledge of the export licencing system as well as the sensitivity of the valves which his company dealt in, and therefore knew that he was acting illegally.[257] Summerskill pleaded guilty to 3 counts of exporting controlled goods contrary to section 68 (2) of the Customs and Excise Management Act 1979. He was sentenced on 14 March 2014 at the Central Criminal Court to 30 months in prison.[258] He was also ordered to pay 68,000 British pounds personally within 6 months of his conviction or serve a further 15 months in jail. Delta Pacific Manufacturing Ltd was charged with three counts of exporting or shipping as stores alloy valves from the United Kingdom, with intent to evade the prohibition or restriction in

---

256 Department of Business, Innovation & Skills "Notice to exporters 2014/29: Illegal exporter to pay criminal profit." (2014, November 26). Available from http://blogs.bis.gov.uk/exportcontrol/uncategorized/notice-to-exporters-201429-illegal-exporter-ordered-to-repay-criminal-profit/ accessed 21 March 2016.

257 Iran Watch. "Illegal Exporter Ordered to Repay Criminal Profit", available from http://www.iranwatch.org/library/governments/united-kingdom/hm-revenue-customs/illegal-exporter-ordered-repay-criminal-profit accessed 21 March 2016.

258 Illegal exporter ordered to pay criminal profit [Press Release], HM Revenue & Customs. Available from http://www.mynewsdesk.com/uk/hm-revenue-customs-hmrc/pressreleases/illegal-exporter-ordered-to-repay-criminal-profit-1087729 accessed 21 March 2016.

force with respect to these goods by virtue of EC Regulation No 428/2009 Article 4. Fines totaling 1,072,000 British pounds were imposed on the company.[259]

4.2. NDT Mart

Another enforcement action, this time involving the export of radiation testing equipment, centres around Philip Bisgrove who was the owner of NDT Mart, a company which deals in non-destructive testing equipment. Bisgrove was jailed for eight months and fined 30,000 British pounds in October 2010, after pleading guilty to exporting controlled radiation testing equipment to Iran without a licence. Between 2007 and 2008, Bisgrove made 10 shipments of dosimeters and doserate meters, and three shipments of MY-2 electromagnets to Iranian Company Sakht Afzar Farayand Eng Co (SAFCO), as well as routing a consignment of equipment through Taiwan.[260] Dosimeters measure an individual or object's exposure to ionizing radiation and can be used in both medical and industrial processes. HMRC officers conducted a search of Bisgrove's home, taking emails, invoices and other documents as evidence. These documents revealed that Bisgrove was eminently aware of the necessity for a licence to export. Indeed, emails between Bisgrove and his contact at SAFCO, Peyman Rostami, showed that he had even discussed shipping goods through Dubai, Malaysia and China in order to avoid export controls.[261] In an attempt to conceal his activities, he paid a third company to ship and receive

---

259 HM Revenue & Customs. "Illegal exporter ordered to pay criminal profit [Press Release]", Available from http://www.mynewsdesk.com/uk/hm-revenue-customs-hmrc/pressreleases/illegal-exporter-ordered-to-repay-criminal-profit-1087729 accessed 21 March 2016.

260 Iran Watch. "Philip Bisgrove." See http://www.iranwatch.org/suppliers/phillip-bisgrove accessed 21 March 2016.

261 HM Revenue & Customs "Businessman jailed for selling radiation detection equipment to Iran [Press Release]", (National) (2010). Available from http://www.mynewsdesk.com/uk/pressreleases/hm-revenue-customs-national-hm-revenue-customs-national-businessman-jailed-for-selling-radiation-detection-equipment-to-iran-498351 accessed 21 March 2016.

goods on behalf of NDT Mart.[262] Bisgrove initially tried to mislead the HMRC interviewers, and claimed he was not aware that the equipment required an export licence. However, when presented with evidence gathered by HMRC investigators, particularly his correspondence with SAFCO, he admitted knowing that a licence was required for the exports to be legal.[263]

4.3. Medrdad Salashoor

British businessman Mehrdad Salashoor was jailed for 18 months in March 2008 after admitting to exporting high-tech navigation equipment to Iran illegally. Salashoor exported gyro-compasses, which despite being designed as self-contained maritime navigation systems, contain accelerometers and gyros of adaptable for use in missile guidance systems, and are therefore classified as dual-use goods. The total value of the shipments was around 650,000 British pounds. In May 2006 Salashoor submitted an export licence enquiry relating to the export of eleven gyrocompass devices to Azerbaijan. He was informed that the export would indeed require a licence. Salashoor did not to apply for an export licence however, and instead diverted the goods to Malta, with instructions for onward-shipment to a company in Iran that was later found to be the Iranian Ministry of Defence. The export was blocked by the Maltese government, and the eleven devices were returned to the UK.[264] Salashoor subsequently attempted to find a new customer for the devices in Norway. Two of the devices were sent to Norway, supposedly to be fitted to two ships berthed in Oslo. Investigators discovered however that the ships did not exist and

---

262 "Businessman jailed over radiation meter deal with Iran." *The Visitor.* Available from http://www.thevisitor.co.uk/news/local/businessman-jailed-over-radiation-meter-deal-with-iran-1-2161037 accessed 21 March 2016.

263 "Jail for boss who broke the rules." *The Business Desk*. Available from http://www.thebusinessdesk.com/northwest/news/78209-jail-for-boss-who-broke-export-rules.html# accessed 21 March 2016.

264 Department for Business, Innovation & Skills. "UK Businessman jailed for Iran missile guidance exports." Available from http://blogs.bis.gov.uk/exportcontrol/prosecution/uk-businessman-jailed-for-iran-missile-guidance-exports/ accessed 21 March 2016.

the goods were covertly diverted to Iran from Norway.[265] When HMRC Investigators visited Salashoor he provided them with a disc containing copies of email correspondence and contracts with an "Azeri Shipping Company". The contents of the disk presented an account that made Salashoor appear to have been misled by a series of middle men and front companies. The email records also suggest that Salashoor, on discovering about the Iranian element of the deal, attempted to prevent the devices from leaving Malta. HMRC investigators uncovered evidence from the disc that showed the documents were a cover story fabricated by Salashoor as part of an attempt to conceal his activities. Following his arrest, Salashoor was interviewed, and his computers and business records further analysed. This investigation revealed further illegal exports and revealed orders from the Iranian Air Force and the Iranian Ministry of Defence. Salashoor pleaded guilty to four offences of "Being knowingly concerned in the exportation of goods contrary to the Customs and Excise Management Act 1979," He also pleaded guilty to one count of perverting the course of public justice and three further counts relating to other illegal exports discovered as a result of his investigation.[266] He was ordered to pay a 432,970 British pounds confiscation order under the Proceeds of Crime Act (2002). He was ordered to pay that sum within 6 months or face a 3 year prison sentence by default.

---

265 "British dealers supply arms to Iran." *The Guardian.* Available from http://www.theguardian.com/world/2008/apr/20/armstrade.iran accessed 21 March 2016.

266 Department for Business, Innovation & Skills. "UK Businessman jailed for Iran missile guidance exports." Available from http://blogs.bis.gov.uk/exportcontrol/prosecution/uk-businessman-jailed-for-iran-missile-guidance-exports/ accessed 21 March 2016.

5. RECENT CHALLENGES IN ENFORCEMENT OF EXPORT CONTROLS IN THE UK

There are of course numerous challenges to the effective enforcement of export controls in the UK and internationally. Some of these are technical, and some more abstract. All are compounded by a general reduction in government expenditure, which has resulted in a cutback in the number of staff working on export control-related issues in government.[267] The following section details several broadly applicable challenges to export control enforcement, including those posed by emerging technologies such as cloud computing, as well as issues relating to the engagement of stakeholders in academia.

5.1. Outreach and Awareness Raising

A key challenge to enforcement of export controls in the UK – as in many countries – relates to outreach and awareness raising. The UK Export Control Organisation has maintained an active outreach programme for many years.[268] This is complemented by activities of other government departments, including HMRC and the FCO.[269] However, there is a concern that this outreach is not resulting in a sufficiently broad awareness of export control issues – particularly among small and medium sized enterprises. The British government has taken measures in recent years to expand outreach – including by launching an annual "export control symposium".[270] The UK also undertakes targeted outreach, often in

---

267 Wheeler, Brian. "Spending Review: Department-by-department cuts guide" available from http://www.bbc.co.uk/news/uk-politics-34790102 accessed 21 March 2016.

268 UK Government. "Quadripartite Select Committee First Report" available from http://www.publications.parliament.uk/pa/cm200506/cmselect/cmquad/873/87307.htm accessed 21 March 2016.

269 "UK Strategic Export Controls Annual Report 2014" available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/446050/Strategic_Exports_AR14_tagged.pdf accessed 21 March 2016.

270 UK Government. "invitation: Export Control Symposium 2015" available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/441852/ECS-2015-Invitation-030715.pdf accessed 21 March 2016.

response to specific intelligence information concerning approaches to specific British companies. However, the concern about broader awareness remains.

It was partly for this reason that Project Alpha was launched at King's College London in 2010 with UK government funding. The project has worked on a sectoral basis to raise awareness in key sectors, such as the alloys industry, composites sector, and in academia (as set out below). The project has also made available free-to-access e-learning materials on export controls and other materials via its website intended to raise awareness about export control issues.

5.2. Cloud Computing

Strategic trade controls are designed not just to control the movement of physical goods, but also so called, intangible technology. That is, technology associated with controlled items and their use that may not have to take a physical form. This type of technology can include blueprints, operational manuals, and working knowledge and skills training.[271] How to control the spread and dissemination of intangible information has been a consistent challenge to the effectiveness of export controls both in the UK and around the world for some time. There was, for example, concern during World War I that the use of the telegraph to transmit data would lead to the loss of military secrets.[272]

Cloud computing, the practice of using a network of remote servers hosted on the internet to store, manage and process data, rather using than a local server or personal computer, may represent a new challenge in the enforcement of export controls in the UK and internationally, by challenging our current understanding

---

271 The Wassenaar Arrangement "The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies."(2013). Definitions and terms used in these lists, http://www.wassenaar.org/controllists/index.html. accessed 21 March 2016.

272 Project Alpha. "Export controls and 3d printing". available from http://www.projectalpha.eu/news/item/236-export-controls-and-3d-printing accessed 21 March 2016.

of export control related concepts, and further obscuring intangible technology transfers from those government departments responsible for enforcement of export controls.[273] The question of how cloud-based services will impact the enforcement of export controls is becoming increasingly important too. Such services have enjoyed considerable growth in recent years and companies are increasingly migrating to cloud computing solutions in areas such as workforce automation, email and productivity suites.[274] The European Commission estimates that revenues in the EU cloud sector could reach 80 billion euros by 2020.[275]

The "location independence" of cloud computing services, that is to say, the lack of user control over the exact location of cloud infrastructure means that, for the first time, a transfer of data that would require an export licence between two companies based in the same country could result in an export taking place.[276] For example if a company based in the United Kingdom stores data on a remote server owned by another UK-based company which provides such cloud storage and commuting services, but the server in which that data is stored by the second company server is based in another country, an export takes place as soon the data is sent from the UK to the server.[277] In spite of the increased ambiguity that now exists within the definition of "export", the treatment of cloud computing under EU and by extension UK export control

---

273 PCMagUK. "What is cloud computing?" Available from http://www.pcmag.com/article2/0,2817,2372163,00.asp accessed 21 March 2016.

274 Nagel, Trevor W. "Cloud services and export control: what you don't know can hurt you." White & Case Technology Newsflash available from http://www.whitecase.com/publications/alert/cloud-services-and-export-control-what-you-dont-know-can-hurt-you accessed 21 March 2016.

275 Mason Hayes & Curran Technology Law Blog. "Export control: how does it impact on cloud computing?" http://www.mhc.ie/latest/blog/export-control-how-does-it-impact-on-cloud-computing accessed 21 March 2016.

276 Liptrap, Hunter. "16 tips: cloud computing advantages and disadvantages" Simplify Workflow. Available from http://www.modgility.com/cloud-computing-advantages-and-disadvantages/ accessed 21 March 2016.

277 Ahmed, Sajid & Haellmigk, Philip "Cloud Computing and EU Export Compliance." Available from: http://www.worldecr.com/wp-content/uploads/Cloud-computing-issue-181.pdf accessed 21 March 2016.

law is not immediately clear. The EU Regulation includes within its definition of an "export"; "transmission of software or technology by electronic media… to a destination outside the EU; it includes making available in an electronic form such software and technology to natural and legal persons and partnerships outside the EU."[278] This suggests that there are two acts, either of which constitutes an export; transmitting software or data outside the EU and/or making software or data available to any person physically located outside the EU. The advent of cloud computing makes these two scenarios more distinct than has been the case before. Specifically, data could be transmitted outside the EU, but this does not mean that the data has necessarily been made available to anyone outside the EU, it is merely being stored there.

Cloud computing capabilities raise important questions within the context of intangible technology controls in the UK and globally. Chief among them; what acts now constitute an export of intangible technology? Guidance from the UK government on what constitutes a controlled transfer of data or software overseas hinges upon who has access to that data and from where. So while software or data may have been transmitted across a border and be physically stored in electronic form outside the EU, if no one has access to its content then the opportunity to make use of them has not in fact been transferred. This is an important and useful clarification, but does not put the issue to bed completely. This definitional distinction, whilst making sense, may prove hard to police reliably. What for example are the responsibilities and obligations of the cloud service provider in this scenario? Once the transfer has taken place, what duty of care do they have over the data that they are now, physically at least, in custody of? Further clarification may be required in order to make the responsibilities of all parties involved in cloud based activities clear and reduce the chances of inadvertent non-compliance. Further complications still, could come from states that play

278 European Union "Council regulation (EU) 428/2009" available from: http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc_143390.pdf accessed 21 March 2016.

host to cloud infrastructure. The debate over the degree to which a state is able to exercise sovereignty over that which is contained within its borders, specifically as that sovereignty relates to cloud infrastructure is one that has yet to finish playing out.

5.3. Academic Engagement

UK universities operate in an increasingly international arena with respect to their research and teaching collaborations. The research engagement between British universities and foreign partners is a necessary and valuable activity, and while the increasingly global outlook of UK educational institutions is generally welcomed by UK government, these kinds of activities are not without risk within the context of UK export controls. UK export controls relating to transfers of technology and technical assistance, are not limited in their applicability to just commercial entities. This means that UK universities and academics are also obliged to ensure that they do not become involved in the transfer of sensitive technology. The broad implication of this is that academics at universities may require export licences to carry out certain activities.

A particular challenge at the interface between academia and export controls relates to a lack of awareness. Most universities in the UK have in place their own export controls policies and in-house legal and research support services to advise academic staff on how to ensure compliance. However, ensuring that UK academics are aware, not simply of the idea that the work that they do may be subject to export controls, but also the kinds of actions that could constitute non-compliance is a challenging task. There are numerous circumstances under which an inadvertent violation of export controls could take place within the academic context, and legal practitioners working in the academic field face the challenge of communicating the conceptual nuances that exist within UK export control vernacular, that may result in accidental non-compliance. Specifically, this includes the numerous different kinds of acts that would constitute an "export". Activities such as the delivery of presentations at international conferences, or the

employment of a research assistant from another country, which are commonplace within academia, may be considered exports that would require a licence if sensitive technical information is involved. An added layer of complexity in the relationship between the academic world and export controls are the concepts of "basic scientific research," where "experimental or theoretical work [is being] undertaken principally to acquire knowledge of the fundamental principles or phenomena or observable facts and not primarily directed towards a specific practical aim or objective" and "in the public domain" whereby the information is "available without restriction upon further dissemination".[279] Decontrols apply to these kinds of information, and therefore no licence is required in order to disseminate this type of technology. However, the status of a given piece of research may be unclear or subject to dispute, the risk of inadvertent non-compliance.

The following case, while it relates to a US prosecution, serves as a useful illustration of the challenges posed by academic activities within the context of export controls. In 2009, John Reece Roth, a former emeritus professor of electrical engineering at the University of Tennessee (UT) in Knoxville was sentenced to four years in prison for non-compliance with export control requirements relating to a United States Air Force (USAF) funded-project subcontracted through the private company Atmospheric Glow Technologies (AGT) between 2005 and 2006. In April 2005 the USAF awarded a 749,751 US dollars contract to AGT. The Air Force was especially interested in research being conducted by Roth, UT professor and co-founder of AGT Daniel Sherman, and NASA scientist Stephen Wilkinson, into the application of plasma actuators to enhance flight performance of unmanned air vehicles (UAVs). AGT awarded Roth and UT a 73,000 US dollars – a-year subcontract to continue developing the actuators. During this time Roth insisted that a Chinese doctoral student assist him on the pro-

279 "19 Export Control Order 2008, Regulation 18". Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/68680/Guidance_on_ accessed 21 March 2016.

ject. The student had been employed by UT College of Engineering as a graduate research assistant and graduate teaching assistant under Roth's supervision since August 2002. Sherman, who was concerned about a potential leak of sensitive information to the PRC, compromised with Roth, agreeing to appoint the student to work on basic research whilst US graduate student Truman Bonds conducted the more sensitive applied research. This arrangement did not prove sustainable, and the two began to share research with the support of both Sherman and Roth. Sherman later admitted that he had known research should have been restricted to US citizens.[280]

Moreover, in May 2006 Roth returned from a lecture tour in China to be met at the Detroit Airport by federal customs agents who photocopied documents in his briefcase and luggage; these included a report on the USAF project and an agenda that showed Roth had lectured on the plasma actuator project whilst in the PRC. Roth then flew to Knoxville where the FBI seized his computer and thumb drive. Another report from the Chinese research student was discovered, as well as a draft paper on plasma aerodynamics that had been sent to Roth in China via a Chinese professor because Roth's email was not working in the PRC. This method of transmission meant that a highly sensitive document had been sent to a Chinese scientist.[281] Roth was accused of one count of conspiracy to export defence articles and services to foreign nationals, 15 counts of exporting defence articles and services without a licence, and one count of wire fraud for defrauding UT of his honest services. Sherman, in the hope of avoiding multiple charges, pleaded guilty to one count of conspiring to violate export controls and supplied emails and journal entries for the prosecution. Sherman was sentenced to 14 months in prison and prohibited from working on federal contracts in the future. AGT tried for bankruptcy protection in March 2008 and pleaded guilty to 10 counts of export control

280 Golden, Daniel. "Why the professor went to prison". Bloomberg Businessweek. Available at: http://www.bloomberg.com/bw/articles/2012-11-01/why-the-professor-went-to-prison#p3 accessed 4 February 2016.

281 *Ibid*.

violations in August 2008. The University of Tennessee was not prosecuted, as they claimed to be ignorant of Roth's actions and disclosed his violations to the government as soon as they became aware. While Roth was not responsible for the physical removal of sensitive physical goods from the USA, many of his actions were indeed exports, and thus violated the controls placed on the project.

The case is useful, in that it highlights several different examples of technological transfers that may not be immediately identified as exports. This is primarily due to the fact that the transfers involved intangible technology.[282] First, the employment of a Chinese national on the project and the subsequent sharing of sensitive research and knowledge while on US soil. Even though no goods had left US soil, this was still an export of technology.[283] His visit to China involved three methods of transfer that again, may not be hard to identify as exports. The act of bringing a laptop containing sensitive documents relating to the Air Force project, presenting on aspects of the project to audiences in China, and the emailing of documents to Chinese nationals, all represent technology transfers.

The ambiguity inherent in the interface between export controls and academia is added to further, not only by the upward trend in international research collaborations, but also by the types of research organisations with which it is possible to collaborate. There is a general trend towards university/industry research partnerships in the UK results in university research becoming increasingly "applied" in nature. Over the course of the past 10 years, UK universities have listed a number of research partners with proven links to the weapons programmes of several countries. It is important to stress however that these examples are not meant to be viewed as instances of non-compliance with UK export con-

---

282 This includes, but is not limited to, software, instructions, working knowledge, design drawings, models, operational manuals, skills training, and parts catalogues.

283 Golden, Daniel. "Why the professor went to prison". Bloomberg Businessweek. Available at: http://www.bloomberg.com/bw/articles/2012-11-01/why-the-professor-went-to-prison#p3 accessed 4 February 2016.

trol laws, nor are they necessarily instances of institutions doing wrong in a philosophical sense. They are intended to highlight the complexity inherent in international academic collaboration by showing that many mainstream research partners in the fastest growing and most dynamic countries in the world, such as China and India, including some of the world's most respected universities, are also involved in work on weapons of mass destruction and their delivery systems. Collaborations between UK universities and foreign research partners have included activities with;

- The Indian National Aerospace Laboratories, which has been closely involved with the development of components for Indian ballistic missiles.
- China's National University of Defence Technology (NUDT).[284] NUDT is controlled by the People's Liberation Army and is involved in missile-related research. In February 2015, the US Government stated that NUDT has used US-origin computer components to produce supercomputers 'believed to be used in nuclear explosive activities.'[285] For that reason, NUDT is on a US Department of Commerce export control watch-list.[286]
- Pakistan's Atomic Energy Commission (PAEC) The PAEC oversees all of Pakistan's nuclear-related activities, including nuclear weapons research and production; and
- The Beijing Aeronautical Manufacturing Training and Research Institute (BAMTRI), a research subsidiary of Chinese state aerospace maker AVIC. In April 2014, the US Department

---

284 University of Huddersfield. "National University of Defence Technology." https://www.hud.ac.uk/international/partnerships/china/nationaluniversityofdefencetechnology/ accessed 21 March 2016.

285 US Department of Commerce Bureau of Industry and Security. "Addition of certain persons to the entity list; and removal of person from the entity list based on a removal request." Federal Register, Vol. 80, no. 32 available from http://bis.doc.gov/index.php/forms-documents/doc_download/1196-80-fr-8524 accessed 21 March 2016.

286 US Department of Commerce Bureau of Industry and Security. "Addition of certain persons to the entity list; and removal of person from the entity list based on a removal request." Federal Register, Vol. 80, no. 32 available from http://bis.doc.gov/index.php/forms-documents/doc_download/1196-80-fr-8524 accessed 21 March 2016.

of Commerce stated that BAMTRI had supplied Iran's ballistic missile programme via a Chinese middleman named Li Fang Wei, who has been accused of repeatedly supplying dual-use goods to Iran's UN-prohibited ballistic missile programme.[287] BAMTRI remains on the US Department of Commerce's watch-list.

Again it is important to stress here that these collaborations are unlikely to have resulted in the transfer legally or otherwise of sensitive strategic technology. Rather they are meant to highlight just how complex the landscape of international academic collaboration is as it applies to the control of strategic exports. This is a situation that is only going to become more complex as more and more universities seek to expand their research footprint internationally. As a result, it will be essential for universities and individual academics alike to be cognizant of their legal obligations and ensure that proper oversight is exercised in order to avoid non-compliance with UK export control legislation.

6. CONCLUSIONS

The UK has been implementing export controls for a long time and is probably as a result among the most experienced of export control implementers. The UK has established a sophisticated enforcement architecture that is integrated into the cross-governmental apparatus. This apparatus is also well exercised in responding to specific cases, with a few hundred enforcement actions being taken each year. The general approach of the UK has been to take a tiered approach to enforcement, in which only the most serious cases progress to either compound fines or prosecution. Despite the UK's long experience in implementing export controls, there are substantial challenges to enforcement even in the UK. Several

287 Clover, Charles. (2013, June 23). "UK universities under scrutiny over China ties." *Financial Times*. Available from https://next.ft.com/af5ea60e-1578-11e5-be54-00144feabdc0 accessed 21 March 2016.

specific challenges were highlighted, including the difficulties associated with outreach and awareness raising, the difficulty in enforcing intangible technology controls, and the challenges of ensuring non-traditional sectors are compliant, such as the academic sector. These challenges have been compounded by resource constraints that resulted from the global recession in the late 2000s.These challenges likely apply in many countries other than the UK. One unique solution undertaken in the UK was to launch Project Alpha at King's College London. Project Alpha has helped to address at least some of the challenges facing export control enforcement in the UK and might thus serve as a model for other states to consider. Nonetheless, export controls are inherently challenging to implement, and it must be recognised that no country can have a perfect or full-proof system. As such, it is likely that there will be a constant effort to improve implementation of controls while, at the same time, proliferators continue to seek new ways to evade controls.