# Dual-use Research and non-proliferation of military technology

*This note is designed to improve awareness of controls enforced by the UK and US governments on the export of military and dual-use items, software and technology. It was approved by the University of Cambridge Research Policy Committee in January 2020.*

*It is being issued alongside a revised University Export Control Policy. Heads of Department and Faculty are encouraged to use this note, the policy and the accompanying guidance on the University's export control pages to raise awareness of these controls and researcher responsibilities at a local level. The note is also accompanied by a short information sheet designed to help researchers understand what steps they should take to ensure compliance with export controls (see appendix 1).*

*Overview*

1. The United Kingdom, alongside most other countries including the United States, enforces controls on the export of military and dual use (i.e. civil technologies which have the potential to be used for military purposes) items, software and technology ('technology' is defined as information necessary for the development, production or use of goods).

2. As such, researchers at the University of Cambridge may be subject to UK Export Control legislation, and also US export licence conditions for technology imported from the United States. These regulations have the potential to apply to a range of activities, including research, teaching, visiting scientists and technology transfer.

3. Failure to observe these rules is a criminal offence for the researcher (responsible for primary awareness as the application of the rules to their research) and/or the University (failure to provide adequate guidance/internal processes/regulation at the appropriate level). Extradition to the USA could be applied for a breach of US rules. It is therefore extremely important that researchers in relevant disciplines are aware of their responsibilities.

*UK legislation*

4. UK export control law requires an export licence for the export of items, software or technology considered to be military-use or dual-use. All such controlled goods or technologies are compiled on the UK Strategic Export Control Lists (or 'Consolidated Lists'). The Consolidated lists are formed of three parts:

a) The military list: covering items of direct military use.
b) The dual-use list: covering civil items with the potential for military use.
c) The Annex IV list: a list of sensitive dual-use items for which there are additional controls.

5. Primary responsibility for deciding whether research will require a licence falls to the individual researcher. Although assistance is available from the University Research Office (see attached University Export Control policy) only the researcher concerned is likely to be able to make the technical assessment to decide whether an item or technology meets the technical descriptions and requirements set out in the Consolidated Lists. The lists are available online, see 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.

6. The controls have the potential to impact the export of physical items, software and intangible technology.

7. On occasions University research will require the export of controlled physical items. Researchers should be aware that the control lists do not only control military and dual-use machines (such as spacecraft or drones) but also materials, components, tools and chemicals that have the potential to be dual-use (e.g. hardened materials that could be repurposed for military use, valves and components suitable for the manufacture of controlled chemicals, and viruses with the potential for use in biological warfare).

8. Software and algorithms may also be controlled where they have potential military applications (such as supporting advanced flight control systems).

9. Most controlled exports undertaken by universities are of intangible 'technology'. Technology is information needed for the development, production or use of controlled items. This might take the form of research data, blueprints, methodologies, plans, diagrams, models, formulae, source code, tables, technical reports, engineering designs and specifications, or manuals and instructions, either written or recorded on other media or devices. It is only controlled, however, if it is "required" for the development, production or use of controlled items.

***'Required' technology:*** *Most items on the control lists will have a particular performance level, characteristic or function that needs to be exceeded or be present in order for the item to be controlled. "Required" technology is technology that is responsible for achieving or exceeding the controlled level or function.*

*For example, technology for the development or production of composite propeller blades or propfans is controlled, but only where it is 'required' for achieving or exceeding a capability of absorbing more than 2,000 kW at flight speeds exceeding Mach 0.55.*

*If Company X exports technology allowing an overseas manufacturer to produce propeller blades that can only achieve a capability of absorbing 1,500kW at flight speeds exceeding Mach 0.55, they do not need a licence to do so. However, if researcher Y subsequently provides that same company with information (technology) allowing them to upgrade their manufacturing process to allow 2,000kW, the researcher would require a licence.*

9. In addition to standard technology exports (i.e. the export of information that is written down in some form), technical assistance can also be controlled. Technical assistance may take forms such as instructions, skills, training, working knowledge and consulting services. Such activities may involve the transfer of controlled intangible technology.

10. Another possible trigger for control is that technology, which is not normally subject to control, is controlled because the end-user is involved in an area or activity of concern (i.e. a weapons of mass destruction - WMD). No assistance of any kind at all can be given to a WMD programme.

11. There are exemptions to the controls for software and technology (but not goods). These exemptions will apply to a large amount of the work done at the University. They apply to:

a) information that is already in the public domain: i.e. information that is available without restriction upon further dissemination (with the exception of copyright restrictions). Information that has to be purchased from a supplier who controls the supply, requires registration, has restrictions on access, or is subject to Government or MoD security classifications is not considered to be in the public domain.
b) the dissemination of basic scientific research: i.e. experimental or theoretical work 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.
c) the minimum information necessary for a patent application.

It is important to note that these exemptions do not apply to WMD end use or sanctions controls.

12. The UK Export Control Joint Unit issues licences for the export of controlled goods and technologies. Licences are required for:

a) the physical removal of goods or the transfer (by any means) of controlled goods, technology or software and/or knowledge from the UK (teaching is unlikely to affected unless written teaching materials containing controlled information are exported out of the country):
    a. To a destination outside the UK for goods on the military list and/or the Annex IV list of sensitive dual-use items.
    b. Outside the EEA for other dual-use technologies (please note that this may change post-Brexit).
b) Any assistance within the UK for use in a WMD programme outside the UK, including teaching or other engagement taking place in the UK.

13. If any researcher suspects that their work may involve the export of controlled technology, software or items, they must seek advice according to the University's Export Control policy. If the technology, software or item is on the control lists or is for use in a WMD programme outside the UK, a licence must be sought. Failure to apply for a licence may lead to prosecution. The purpose of applying for a licence is so that ECJU can assess whether the kind of work being done with that collaborator should be permitted. The ECJU maintain that only a small percentage of licence applications are refused.

14. Further controls require visas for entry of students to specified engineering and science courses (the ATAS scheme administered by the FCO). These rules do not dovetail with or replace the obligation to comply with US or other UK export controls. They do not apply to post docs or visiting researchers.

*US legislation*

15. While there are similarities, US export control rules differ to the UK approach. US export controls distinguish between military (ITAR) and dual use (EAR) controls. The EAR controls are usually the ones applicable to the University.

16. US export controls operate via restrictions on disclosure to certain 'parties of concern' (see paragraph 18 below) that apply to controlled products or technology. This can mean disclosure within the UK and potentially even within a University group. Restrictions apply even if only a percentage of the technology to be disclosed has come from the US (normally 25%).

17. The controls operate via specific licence conditions, which exporters are meant to notify importers (i.e. the University recipient). Researchers must be aware if technology has been received under US export licence conditions which restrict giving access to parties of concern. Researchers should seek advice from the University Research Office to ensure that the exporter provides the specific conditions that must be complied with, which is a duty on the exporter – a general requirement to comply with US export control law should not be accepted.

18. Parties of concern are:

- entities on the US entity list or
- nationals of prohibited countries

The US lists *parties of concern* at https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern. If a person to whom the technology is to be disclosed appears to be on one of the lists, additional due diligence is required before proceeding, in particular consulting the exporter. Researchers are encouraged to consult with the Research Office for assistance. Depending on which list applies there may be a strict export prohibition or lesser limitations and requirements.

19. University personnel receiving US technology must be mindful at all times of the rules that apply and seek advice where necessary.

***UK links with overseas defence companies:*** *A report by the Australian Strategic Policy Institute on the links between the Chinese military and universities identified 16 labs around the world in which Chinese state-owned defence conglomerates had a substantial presence. Of these 10 are based in UK universities, undertaking research including aeronautics, robotics, graphene, satellites, and turbine technology.*

*Recent developments*

20. Until recently the Export Control Joint Unit was primarily interested in the export of physical items by business and industry. Recently, however, concerns have been raised regarding the risks posed by close collaboration by universities with foreign (particularly defence) companies, particularly those with close ties to their national governments. This focus is particularly on:

a) Technical assistance – including research collaborations, conferences, visiting scientist schemes and any other interaction through which scientists from countries of concern can get access to UK scientists; and
b) Flow of controlled technology to programmes of concern in destinations of concerns (such as WMD programmes or state defence companies.

21. The UK government is encouraging researchers to take greater care in their choice of collaborators and to consider what technical knowledge those collaborators might pick up during the collaboration. The concern is not about the final public dissemination but what might be picked up on the way and indigenised in the collaborator's country, especially its military complex. The Trusted Research guidance issued by the Centre for the Protection of National Infrastructure and National Cyber Security Centre addresses these issues in more detail. The key theme of the guidance is the importance of knowing whether research is has the potential to be used for military purposes and undertaking due diligence on collaborators.

22. In addition, the US have recently updated their entity list, increasing the number of entities that are impacted by US export legislation. See: https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.

23. The attached export control policy has been updated in light of these developments. In addition, a short set of actions that researchers should take to ensure compliance with export controls is attached to this note – this has been developed to encourage researchers to focus on the key steps that should be taken in light of recent developments.

## *Appendix 1: Actions to ensure compliance with export control*

The following steps should be followed by all researchers to help ensure compliance with export control legislation.

1. **Know your research**: Be aware of the export control lists and whether your research has the potential to be covered by them.

2. **Know your exports:** If you undertake an activity that could lead to the export of goods, software or technology outside the UK or the transfer of knowledge within the UK for use in a WMD programme outside the UK consult the University Export Control website and the export control lists. If you believe that export controls may apply, seek advice according to the University's export control policy.

3. **Know your collaborator:** Consider new collaborators carefully. Is your collaborator :
   a. from a sanctioned country on the ECJU published list https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions
   b. Any collaborator from another country having or developing a nuclear programme
   c. on the US entity list (the UK list is not publically available)

   AND IF YES
   d. Is the collaborator linked to their national military complex or genuinely only civil?
   e. Is the only use of the technology is for military purposes (e.g. stealth technology).

   If this process raises concerns about the collaborator contact the Research Office (RO) for advice. The RO will likely support you to make an enquiry to the ECJU to establish whether the collaborator is of concern. If they are, any collaboration is likely to require a licence.

4. **Know your technology inputs:** All researchers need to be aware of whether they are using US controlled technology and if so check:
   a. whether the technology is subject to restrictions on providing access to nationals of a prohibited country (this will apply even if that individual is based in the UK, a University employee, member of the research team, or visiting scientist); and
   b. whether the exporter is on the US list of parties of concern.

   AND IF a or b apply

   c. work with the RO to contact the exporter and the relevant US licensing authority for advice (BIS for ITAR and Commerce for EAR controls).

***Example:*** *You are planning a collaboration with an automotive company based outside the EEA. You should:*

*a) Consider whether the research you will be doing has the potential to be on the control lists. If so, will you be exporting controlled technology or goods? If so, seek advice.*
*b) Consider the collaborator. Are they from a country that has been sanctioned? Are they on the US entity list? Are they linked to their national military? Could they potentially be linked to a nuclear research programme? If so, seek advice.*
*c) Consider the technology you will be using: Are you using any technology that has been imported from the US? If so, are there export control restrictions on that technology? If so, seek advice.*

*If controls apply you will likely need a licence to share controlled goods or information with your collaborator. In rare cases this may not be granted and the work may not be able to go ahead. If US controls apply you may be restricted in how you can use the technology and with whom you can share it.*

*Care should also be taken not to take controlled technology overseas unless there is a licence in place (e.g. taking controlled research data on a laptop).*