THE CONVERSATION

19 May 2015, 5.37am BST

Paranoid defence controls could criminalise teaching encryption

AUTHOR

Daniel Mathews

Lecturer in Mathematics at Monash University

Anyone teaching encryption without first getting clearance from the government could soon be wearing these.
banspy/Flickr, CC BY

You might not think that an academic computer science course could be classified as an export of military technology. But under the Defence Trade Controls Act – which passed into law in April, and will come into force next year – there is a real possibility that even seemingly innocuous educational and research activities could fall foul of Australian defence export control laws.

Under these laws, such “supplies of technology” come under a censorship regime involving criminal penalties of up to ten years imprisonment. How could this be?

The story begins with the Australian government’s Defence and Strategic Goods List (DSGL). This list specifies goods considered important to national defence and security, and which are therefore tightly controlled.

Regulation of military weapons is not a particularly controversial idea. But the DSGL covers much more than munitions. It also includes many “dual-use” goods, which are goods with both military and civilian uses. This includes substantial sections on chemicals, electronics and telecommunications, among other things.

Disturbingly, the DSGL risks veering wildly in the direction of over-classification, covering activities that are completely unrelated to military or intelligence applications.

To illustrate, I will focus on the university sector and one area of interest to mathematicians like myself: encryption. But similar considerations apply to a wide range of subject material, and commerce, industry and government.

Encryption: an essential tool for privacy

Encryption is the process of encoding a message so that it can be sent privately. Decryption is the process of decoding it, so that it can be read. Encryption and decryption are two aspects of cryptography, the study of secure communication.

As with many technologies subject to dual-use regulation, the first question is whether encryption should be covered at all.

Once the preserve of spies and governments, encryption algorithms have now become an essential part of modern life. We use them almost every time we go online.

Encryption is used routinely by consumers to guard against identity theft, by businesses to ensure the security of transactions, by hospitals to ensure the privacy of medical records, and many other organisations. Given that email has about as much security as a postcard, encryption is the electronic equivalent of an envelope.

Encryption is perhaps dual-use in the narrow sense that it is useful to both military/intelligence agencies as well as civilians. But so are other relatively mundane technologies like *cars*.

Moreover, since the Edward Snowden revelations —- and even much earlier for those who were paying attention – essentially everyone knows they are subject to mass surveillance by the US National Security Agency, along with its Five Eyes partners, including Australia.

While states have no right to privacy, an individual's right to privacy is considered a fundamental human right. And in today's world, encryption is essential for individual citizens to safeguard this human right. Strict control of encryption as dual-use technology, then, would not only be a misuse of state power, but would represent the curtailment of a fundamental right.

How the DSGL covers encryption

Nonetheless, let's assume for the purposes of argument that there is a justification for regarding at least some aspects of cryptography as dual-use, and consider how the DSGL covers encryption.

The DSGL contains detailed technical specifications. Very roughly, it covers encryption above a certain "strength" level, as measured by technical parameters such as "key length" or "field size".

The practical question is how high the bar is set: how powerful must encryption be in order to be classified as dual-use?

The bar is currently set low. For instance, software engineers debate whether they should use 2,048 or 4,096 bits for the RSA algorithm. But the DSGL classifies anything over 512 bits as dual-use. In reality, the only cryptography not covered by the DSGL is cryptography so

weak that it would be imprudent to use.

Moreover, the DSGL doesn't just cover encryption software: it also covers systems, electronics and equipment used to implement, develop, produce or test it.

In short, the DSGL casts an extremely wide net, potentially catching open source privacy software, information security research and education, and the entire computer security industry in its snare.

Most ridiculous, though, are some badly flawed technicalities. As I have argued before, the specifications are so imprecise that they potentially include a little algorithm you learned at primary school called *division*. If so, then division has become a potential weapon, and your calculator (or smartphone, computer, or any electronic device) is a potential delivery system for it.

These issues are not unique to Australia; the DSGL encryption provisions are copied almost verbatim from an international arms control agreement. What is unique to Australia is the strict level of regulation.

Criminal offences for research and teaching?

The Australian Defence Trade Controls Act (DTCA) regulates the DSGL and enacts a censorship regime with severe criminal penalties.

The DTCA prohibits the "supply" of DSGL technology to anyone outside Australia without a permit. The "supply" need not involve money, and can consist of merely providing access to technology. It also prohibits "publishing" DSGL technology, but after recent amendments, this offence only applies to half the DSGL: munitions, not dual-use technologies.

What is "supply" then? The law does not define the word precisely, but the Department of Defence suggests that merely explaining an algorithm could constitute "intangible supply". If so, then surely teaching DSGL material, or collaborating on research about it, would be covered.

University education is a thoroughly international and online affair – not to mention research – so any such "supply", on any DSGL topic, is likely to end up overseas on a regular basis.

Outside of academia, what about programmers working on international projects such as Tor, providing free software so citizens can enjoy their privacy rights online? Or network security professionals working with overseas counterparts?

Examples of innocuous, or even admirable, activities potentially criminalised by this law are easily multiplied. Such activities must seek government approval or face criminal charges -— an outrageous attack on academic freedom, to say the least.

There are exemptions, which have been expanded under recent amendments. But they are patchy, uncertain and dangerously limited.

For instance, public domain material and "basic scientific research" are exempted. However, researchers, by definition, create new material not in the public domain. And according to the Australian Bureau of Statistics, "basic scientific research" is a narrow term, which excludes research with practical objectives. Lecturers, admirably, often include new research in teaching material. In such circumstances none of these exemptions will be of assistance.

Another exemption covers supplies of dual-use technology made “preparatory to publication”, apparently to protect researchers. But this exemption will provide little comfort to researchers aiming for applications or commercialisation, and none at all to educators or industry. A further exemption is made for oral supplies of DSGL technology, so if computer science lecturers can teach without writing (giving a whole new meaning to “off the books”) they might be safe.

There is no explicit exemption for education. None for public interest material. And indeed, the government clearly envisions universities seeking permits to teach students DSGL material – and, by implication, criminal charges if they do not.

On a rather different note, the DTCA specifically enables the Australian and US militaries to share technology.

Thus, an Australian professor emailing an American collaborator or postgraduate student about a new applied cryptography idea, or explaining a new variant on a cryptographic algorithm on a blackboard in a recorded lecture broadcast over the internet — despite having nothing explicitly to do with military or intelligence applications — may expose herself to criminal liability. At the same time, munitions flow freely across the Pacific. Such is Australia’s military export regime.

Brief reprieve

There is nothing wrong in principle with government regulation of military technology. But the net is cast too broadly in the DSGL, especially in the case of encryption. The regulatory approach of the DTCA’s permit regime is effectively one of censorship with criminal penalties for breaches.

The result is vast overreach. Even if the Department of Defence did not exercise its censorship powers, the mere possibility is enough for a chilling effect stifling the free flow of ideas and progress.

The DTCA was passed in 2012, with the criminal offences scheduled to come into effect in May 2015. Thankfully, emergency amendments that passed into law in April this year have provided one year’s reprieve.

Despite those amendments, the laws remain paranoid. The DSGL vastly over-classifies technologies as dual-use, including essentially all sensible uses of encryption. The DTCA potentially criminalises an enormous range of legitimate research and development activity as a supply of dual-use technology, dangerously attacking academic freedom —- and freedom in general —- in the process.