Cybersecurity and Export Control

5 November 2020

The digitalisation of global trade is constantly expanding. In the 21st century data will become the most important commodity, according to a report in the German newspaper "Handelsblatt". The continuing development of 3D printing technology makes it possible to send, instead of the actual goods, data that can then be used to print the goods directly at the receiving end. The more the digitisation of trade develops, the more important cybersecurity products are becoming.

What many companies do not realise is that actions such as uploading construction plans to the cloud or transferring (cybersecurity) software may already fall within the scope of state export controls. As a result of this, there are companies that are actually subject to export controls, but are unaware of it. This also means that "traditional" export companies now have to expand their export control systems to include the transfer of technology and software.

Background

A central aim of export controls is to avoid any threat to Germany or its allies from conventional weapons, weapons of mass destruction and goods that can be used for civil as well as potentially military purposes (*dual-use goods*). Increasingly, following recent reforms put forward by the EU, export rules are also intended to protect human rights.

In both cases, the prominence of cybersecurity is contributing to changes to the nature of risks and threats. Software now has the potential to cause as much damage as conventional weapons, or even more. Moreover, surveillance technology might be used by autocratic states to perpetrate human rights violations. For this reason, trade involving cybersecurity software is now becoming a focus of export controls.

The transforming nature of security threats is leading to changes to the legal framework of state export control. For example, there was an amendment to Annex 1 of the Council Regulation (EC) No 428/2009 (the *Dual-use Regulation*) which came into force on 31 December 2019. The European legislator adhered to its decision taken in 2018 to exclude both "vulnerability disclosures" and "cyber incident responses" from the legal definition of technology subject to export controls. The determination, notification or exchange of "vulnerability disclosure" to an individual or an organisation as well as the exchange of necessary information about a "cyber incident response" thus continue to be excluded from the scope of export control.

The General Framework of Export Control

In general, the export of goods is usually unrestricted. State export controls restrict this freedom and may either prohibit a transaction, require authorisation or impose reporting obligations for an export. An example of a prohibited transaction might be one involving a person or country subject to a trade ban. An exporter would need authorisation especially when the product is listed in Annex I of the Dual-use Regulation which sets out a list of dual-use items, or which is listed in the military export list. The characteristics of the product must match the requirements that are listed.

Article 4 paragraph 4 of the Dual-use Regulation states an important exception to this. Article 4 requires authorisation for exporting dual-use items based not on the characteristics of the good, but rather on its intended use. This is a catch-all clause that covers the export of any good, software or technology that is not explicitly listed, but which still requires authorisation. It applies when the exporter knows that the products they are exporting may be used in a way that would mean they are subject to export restrictions (e.g. in the development or production of weapons of mass destruction). In this case, the exporter is required to disclose all available information known to them, including information in the public domain, for assessment.

Exporting without authorisation can be either an administrative or a criminal offence. It carries a prison sentence of up to five years, and/or a fine (section 18, Foreign Trade and Payments Act, *FTPA*). If the breach was a result of negligent behaviour, the responsible person can be found to have committed an administrative offence and be subject to a fine of EUR 500,000 for each export (section 19 FTPA). The responsible people may be the management of the company, or the person arranging the export. The company itself can also be handed a fine of up to EUR 10 million (section 30, Act on Regulatory Offences).

The Reach of State Export Control Using the Example of Software

In basic terms, any export of software will require authorisation if the software is going to be used in the context of goods that would be subject to an authorisation, or the software itself could be considered to be potentially damaging on its own. The latter can, for example, be the case when the software that will be exported has modifiable encryption technology. Self-driving cars rely on such software for their operation. This type of encryption technology, the technical means to produce it, and even self-driving vehicles are all therefore subject to export controls in Canada. Due to the increasing prevalence of cyberwarfare and the resulting threats posed to Germany and its allies, any software could be subject to export control if that software could also be used for military means. For example, software that can force a power plant to shut down could also be used as part of a military attack.

In contrast to the export of conventional goods, the export of software is not just about physically moving goods abroad. It also includes any intangible transfer through electronic media. According to the authorities, for cloud-based software, this means that each upload of data into the cloud outside the EU or arranging a non-EU third-party access to a cloud-based platform – even when the server is in Germany – could be considered, in principle, as an export transaction that requires authorisation. This also applies to access rights granted within the same company. When considering software exports, the value of the transaction is irrelevant.

The Need for Corporate Export Control Systems

Because of the very intricate sanction regime set forth in foreign trade law, companies that trade with cybersecurity products should check internally if, and to what extent, they are subject to export controls. It may be that an effective export control system must be set up. How much information must be gathered and evaluated to accurately determine the use of the product abroad depends on each individual case. The reform of the Dual-use Regulation for the enhanced protection of human rights discussed above could lead to extensive investigations and expansive liability for the responsible people. In its current amendment proposal, the Council emphasizes the importance of export control with regard to non-listed dual-use surveillance technology and software (recital 5). In addition, the proposal envisages harmonising the control of the provision of technical assistance for sensitive goods (recital 11), which may go beyond existing licensing requirements. However, it is yet to be seen how the reform of the Dual-use Regulation will play out in practice.

Conclusion

The expansion of state export controls under the umbrella of cybersecurity is mainly a result of changes to the scope of possible threats now faced. The flipside of this development is that companies that were never previously affected by foreign trade legislation now fall under its scope. These companies are now subject to the legal challenges discussed above. To comply with these rules, they need to implement effective export control systems.

BLOMSTEIN will continue to monitor and report on the developments. If you have questions about the potential impact of cybersecurity in your company or sector, Roland M. Stein and Leonard von Rummel are more than happy to provide assistance.