AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Scenarios for a successful dual-use items export regime

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2017, directly supports more than 4.7 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

In May 2018 a group of Member States proposed a working paper setting out their vision for the dual-use items export regime recast. This working paper laid out four options for addressing cyber surveillance controls. While these solutions were proposed for issues surrounding the controls of cyber surveillance technologies, they can also be seen as addressing the wider dual-use framework.

For the sake of this paper, these options have been understood as establishing four scenarios of how the recast can be finalised. These scenarios would be:

A) An EU autonomous list;

B) The extended use of national measures under Article 8 of the regulation;

C) Establishing a common European (EU) position for proposing new listings in the Wassenaar Arrangement; and

D) A specific definition for cyber surveillance items that would take account of practical needs on effective network security solutions.

The above four scenarios have been a broken down into two sections, preferred scenarios (++/+) and challenging scenarios (--/-).

I. Industry preferred scenarios

Establishing a common EU position for proposing new listings in the Wassenaar Arrangement – strengthening the multilateral system *(Scenario C)* ++

By continuing to fully adhere to the current international framework on dual-use export controls, the EU would not only uphold its international credibility, but also strengthen the protection of human rights at an international level and help maintain the competiveness of its businesses.

Continuing to work through multilateral avenues, such as the Wassenaar Arrangement, will enable the EU to lead and encourage all other signatories to uphold the highest level of controls on dual-use items. By contrast, implementing its own regime would only weaken the multilateral system and limit the EU's ability to influence the debate and enhance the protection of human rights. Should the EU work through international frameworks, the process would result in a much more targeted and realistic set of controls that regulate the export of malicious surveillance products, while protecting legitimate manufacturers of security software and hardware. Moreover, controls defined under such frameworks would apply beyond the EU and therefore make newly controlled products more difficult to purchase from third countries.

Close alignment with the Wassenaar Arrangement would ensure that companies are not subjected to unnecessary administrative costs and burdens to adapt internal systems to EU specific rules. Moreover, it would ensure that there is no competitive disadvantage for EU producers compared to companies that are working under the Wassenaar Arrangement and therefore not subject to EU only requirements.

A common classification basis that is provided through international frameworks greatly reduces efforts around the classification of products for different international entities of a company, and helps avoid violations of export regulations due to the incorrect local determination of export classifications. Such mistakes can have major impacts on deliveries and after sales support.

Further alignment with the international order would provide more certainty and transparency, while limiting the regulatory burdens for industry. An EU dual-use legislation that is as closely aligned as possible to the multilateral system will ultimately ensure a level playing field for EU businesses and an attractive investment environment.

Practical implications of scenario C on businesses:

- Alignment with international frameworks will provide predictability and legal certainty;
- Enhanced harmonization of regulatory requirements across geographies for those involved in complex supply chains;
- Promotion of a level-playing field that ensures EU producers are not at a competitive disadvantage; and
- Reduced burden and number of violations around the classifications of products.

A specific definition of cyber surveillance technology – protecting human rights while fostering innovation and growth *(Scenario D)* +

Any definition for the control of cyber surveillance technologies must be specific and detailed so as to capture items that can be clearly identified by industry stakeholders. Such a definition would need to be interpreted under the general legal principle that any restriction of rights must be narrowly interpreted.

The definition should consider the intent of the product and allow for the fact that cyber surveillance can be positive. With such an approach, new controls would achieve their goal of controlling the export of malicious products. Controls would hence be focused on exporters of higher risk products, while exporters of legitimate dual-use products would not be impacted.

Further, the European Commission has identified the cyber security dual-use sector as an opportunity for the European market, however, without the right definition the EU will not be able to achieve its self-proclaimed goals. An inadequate definition would inhibit innovation in the EU, as it could disincentivise companies from developing new technologies in the digital sphere. These are critical to the proper development of the digital economy in the EU and its privacy and data security dimensions.

Accordingly, any definition must be developed in consultation with the cybersecurity community, to ensure that it does not inadvertently include items needed for legitimate purposes, such as defensive information security solutions, data leakage prevention, penetration testing or cyber incident response tools.

Practical implications of scenario D on businesses:

- A detailed, narrow definition will enhance predictability and legal certainty;
- An imprecise definition will create uncertainty and unnecessary administrative burden for both regulators and industry without enabling the intended protections, especially if there are discrepancies of interpretation and procedure across EU countries.

II. Challenging scenarios

Creation of an EU autonomous list – diverging from the multilateral success story *(Scenario A)* --

The Commission's proposal for a unilateral or autonomous EU list would most certainly have far reaching implication for the EU dual-use business ecosystem. By introducing its own, separate control list, the EU would deviate from the internationally agreed control regimes framework. This framework is widely recognised as a successful tool, in that it applies to dual-use suppliers involved in global supply chains with minimal national deviations. An international framework on the exports of pre-defined dual-use products provides a level playing field for all producers.

An EU autonomous list threatens this success story by introducing new, unilateral controls, potentially creating a risk of retaliation from stakeholders against EU businesses, and placing significant strain on industry to comply with different and diverging export regimes.

An EU specific dual-use legislation would harm EU companies, as these would no longer operate on a level playing field with their global competitors, making the EU less attractive for third country investors without achieving their protective objectives. Indeed, it can be expected that the EU controlled technologies would remain accessible to malicious actors through other, non-regulated channels. Some products, when exported from outside the EU, currently benefit from being decontrolled through licence exceptions (ENC). Should the EU introduce a new list of strictly-controlled products that doesn't exist elsewhere, this will further deepen the competitive disadvantage to non-EU companies. Many non-EU and EU controlled companies are already facing increased pressure to ship more products from outside the EU to avoid export controls, should a new EU autonomous list be introduced, this pressure will increase.

The additional burden that an EU specific regulation would introduce could be especially impactful for European Small and Medium-sized Enterprises (SMEs), since larger companies are able to absorb the initial and long-term costs of compliance more easily. For SMEs these could present critical factors in their decisions not to export from the EU, or even change their business models altogether.

Practical implications of scenario A on businesses:

- Heightened administrative and regulatory burdens and risk for businesses;
- Isolation of the EU business community in impacted industries, fragmentation of related activities for multinational (groups of) companies and potential divestment in EU cyber development activities;
- Loss of competitiveness and innovation of EU industries involved in the cyber security business;
- Additional classification and administrative burdens for EU companies that would let non-EU competitors benefit from weaker controls in other countries; and
- No significant improvement of human rights intended to be protected by the measure.

Extended use of national measures – risking the coherence of EU dual-use legislation *(Scenario B)* -

This scenario would threaten the greatest economic attribute of the EU, which is the EU Single Market and the continued harmonisation of legislation across the EU. The single European regulatory framework, a common EU rulebook and a set of uniform compliance requirements, allows companies to function efficiently and limits the duplication of compliance efforts.

However, through the extended use of national measures, the EU would run the risk of fragmenting its dual-use legislation and therefore place additional burden on Member States and industry. A fragmented framework, made up of potentially 28 different approaches, would significantly increase costs, burdens and the complexity of internal compliance systems within companies.

It is also more likely that smaller Members States will not have the resources to implement a complex set of national measures. Instead, it is probable that out of necessity the controls will have to be quite broad and therefore more restrictive. These developments will lead to national variations that will fragment the level playing field between exporters based in different Member States, meaning that they will have to operate multiple separate sets of processes to allow for the different approaches in each country. This subsequently could lead to exporters, where possible, moving as many impacted products to Member States with more relaxed rules, which will ultimately limit the effectiveness of the controls.

A fragmented approach will create legal uncertainty and considerably slow down compliance processes, as companies would need more time to check and ensure compliance before exporting. This would be very much to the detriment of customers and consumers.

Practical implications of scenario B on businesses:

- Heightened administrative and regulatory burdens and risk for businesses;
- Multiplication of regulatory requirements, inducing loss of efficiency; and
- Risk of forum shopping across Member States as to where to invest in cyber security research and development (R&D) – to the extent the EU remains attractive in that respect.