AmCham EU's position on the revision of EU dual-use export controls

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 2015, directly supports more than 4.3 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

* * *

POSITION PAPER

American Chamber of Commerce to the European Union (AmCham EU)
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium
Register ID: 5265780509-97
Tel: +32 (0)2 513 68 92 | www.amchameu.eu

Secretariat Point of Contact: [Brendan Moran]; [bmo@amchameu.eu] +32 (0)2 289 10 32

18 January 2016

AmCham EU supports the aim of the Commission's proposal for a revision of the EU's Regulation on the export control of dual-use items. This is to ensure that certain goods and technologies are not used by rogue actors, and to prevent human right violations associated with the use of certain technologies. However, while most export control tools and regimes have been developed to suit the trade in static tangible goods such as traditional ammunitions, it is debatable whether they are suited to cyber technology which is constantly evolving to keep pace with evolving threats and which in many cases must be deployed rapidly to protect information and privacy in the event of a cyber breach.

It is also debatable to what extent some of the additional human rights controls proposed will effectively address the underlying issue of rogue actors' access to dual use items. The existing Regulation already provides a legal basis for export control authorities to request licences for non-listed items on grounds of human rights concerns; a legal basis which in our member companies' experience is extensively applied. Industry remains fully committed to human rights but further extending controls under vague and ill-defined conditions on those companies that already dedicate significant resources to human rights and to internal compliance programmes for export control is unlikely to achieve the stated objective.

AmCham EU's main focus at this stage will be on explaining why it is not appropriate to subject cyber technology used for legitimate purposes to export controls, and why extending the catch-all clause should be approached with caution.

The legislator must ensure that the Regulation does not impede cyber activities conducted for legitimate purposes, such as the sale of products, provision of services or research and development undertakings. To a much larger extent than for many goods listed as dual-use in prior legislation, in the case of cyber technology, the underlying technology used by criminals or rogue actors is very often the same underlying technology used for legitimate purposes by governments and businesses across the globe to protect information networks, systems and infrastructure. Therefore any measures to restrict the export of such technologies must not hamper or hinder their normal use in commercially available defensive cybersecurity products and services, which could prevent legitimate access to protective technology.

Moreover, such restrictions could harm the further development of cyber technology, which is iterative by nature. Cyber technology needs to perpetually evolve to respond to the constant shifts in the cyberthreat landscape, including throughout the lifecycle of products and services in productive use.

For example, penetration testing tools are used to evaluate and improve the security and resilience of IT systems. As no two IT systems are identical, penetration testing tools need to be updated and tailored to the specificities of each user, often requiring the modification of code in very short cycles and even close to real-time as IT configurations get updated, system perimeters move and/or new cyberthreats arise. Having to apply for a new or additional export licence for every new user or after each iterative modification would be neither desirable, nor feasible for the exporters or the export control authorities. Additionally, it could highly hinder legitimate users' cyber preparedness or even set back or damage their resilience to cyberattacks. It would put those providers who export such technologies from the EU at a clear competitive disadvantage to those from other jurisdictions which apply no such restrictions.

We therefore very much welcome the recognition in recital 5 of the proposal that the aim is not to prevent the export of technology used for legitimate purposes, however we believe that some of the draft provisions could have a number of unintended consequences on the legitimate use of cyber technologies.

1. Cyber surveillance technology controls

Cybersecurity technologies are versatile and need to be able to be constantly modified to address evolving threats and the specific environment in which they are used. They are increasingly being delivered as a service rather than standalone.

There are a number of very ordinary and commonly used cyber technology products and services that could be caught – perhaps unintentionally – under some elements of the definition proposed in Article 2(21). In particular the notions of 'intrusion software', 'monitoring centres' and 'digital forensics' could easily be interpreted as applying, among others, to legitimate and much needed cybersecurity and incident response capabilities such as:

Vulnerability testing tools

Vulnerability testing is used by organisations to identify potential risks to their systems, software and infrastructure. When testing for potential vulnerabilities, the most valuable information is how this vulnerability can be exploited and how it works, not that it just exists. Intrusion software is a key tool to better understand the extent and nature of vulnerabilities and to demonstrate their actual impact. Given the very broad use of such tools, and the significant economic and societal benefits of organisations having unhindered access to these kinds of capabilities, extending export controls to them simply because they might also be used by malicious actors to identify and exploit vulnerabilities seems like an unnecessary, disproportionate, and even counterproductive measure. At any rate, malicious players have ample alternate means of pursuing their objectives.

Security-relevant and time sensitive information sharing on zero-day vulnerabilities

A zero-day vulnerability is a vulnerability that is exploited without having been previously known. As they pose imminent threats, they need to be fixed immediately and are the highest priority for companies to patch. The rapid identification and development of the remedy to the vulnerability will generally depend on the cybersecurity community's ability to quickly share data with partners, customers, competitors and even public authorities such as public CERTs and law enforcement agencies. Players routinely share threat information to enhance collective understanding or to support specific operations, often internationally. Export restrictions could hinder close-to-real-time information sharing and collaboration. Exemptions for intra-company transfer, though useful and welcome, will not suffice to remedy this concern.

Malicious players in possession of information on such vulnerabilities would gain strategic advantage for the rapid development of exploits (attack tools leveraging the particular vulnerability). Because of cyberattackers' agility in developing tools, it would be detrimental if the defending organisations' efforts to share information within and outside their perimeter were hindered by export licensing requirements.

Software intended for data protection and integrity

Our understanding is that products that enhance security and data protection, privacy, and integrity are not intended to be captured by the controls. Nonetheless, many of these products may fall within the current definition of 'intrusion software,' and could be captured by other real cyber-surveillance technology categories. Individuals, corporate entities, and governments in the EU and around the world rely on these tools to protect them and their data, and in some cases to comply with relevant laws and regulations for their industries. These types of products should not be controlled, and it is critical that the control language include explicit notes and/or exclusions.

Malware toolkits and malware samples

The sharing of malware samples could also be impacted by the proposed Regulation. While cyberattackers do often utilise malware toolkits (packaged products that contain and spread malware), samples of such malware (and even actual toolkits themselves) must also be used routinely by legitimate cybersecurity practitioners, researchers, service providers and incident investigation teams. It is essential that the cybersecurity community is not prevented from using these defensive cybersecurity tools by obstacles such as export licencing requirements.

Cybersecurity operations centres

The demand for cybersecurity expertise and operational capabilities is constantly growing. At the same time the scarcity of available resources is a common challenge across the globe. As a result, cybersecurity monitoring and incident response may be outsourced to specialised operators who will often provide the monitoring and response capabilities over the internet, and from multiple locations worldwide. When 24/7/365 monitoring and response is required, the service is provisioned on the basis of the 'follow the sun' model. This means migrating the delivery of the service from one operations centre to the next as the dayshifts alternate across time zones. Such a service will, in the course of a day, provide monitoring and response services from at least three different continents to individual clients. Subjecting such services (or certain parts thereof) to export licensing requirements on grounds that security operations centres could fall under the definition of 'monitoring centres' in the meaning of article 2(21) would deprive legitimate recipients of such services from protection and response capabilities. Moreover it could also discourage service providers from establishing their security operations centres on the territory of the European Union.

EU co-legislators should cross off 'intrusion software', 'monitoring centres' and 'digital forensics' from the definition of cyber surveillance technologies. Additionally, we advise specifying in more detail the specific set of tools meant for inclusion in scope by creating a clear definition of 'specially designed' around the main function and to explicitly exclude any other technology that may fall within the same definitions without actually serving the purposes. Finally, a clear definition of the concept of 'public networks' under proposed control entry 10A001 is required to ensure that controls are only applied for the intended purpose.

2. Extension of powers to create new product lists

The Commission includes a new product list under Section B of Annex I: Category 10, 'Other Items Of Cyber-Surveillance Technology'. This list can be updated by means of a delegated act, as for Section A of Annex I, in accordance with art. 16. Importantly, the update of Section B may be incompatible with international commitments of EU Member States who are also members of the Wassenaar Arrangement, but would be amended as necessary on human rights concerns (art. 16(2)b, in line with the new definition of a dual use item). This is in breach of the fundamental principle underpinning the EU export control regime. So far, that the product list (Annex I) is firmly based on and in conformity with the obligations and commitments Member States have undertaken in relevant international fora. Deviating from this principle severely threatens European competitiveness as it puts products under control that the EU's international partners do not control. As such it does not address the availability of such products but increases compliance costs and lead times for European exporters. Concerns over specific products and the need to adapt controls accordingly should be addressed at the international level in order that the EU does not unilaterally increase controls.

AmCham EU recommends that the co-legislators maintain the current system based on international commitments, or establish clear criteria in the Regulation that the Commission would have to follow in the event of seeking to update the section. This should include mandatory involvement of industry and the following selection criteria: 1/ foreign availability outside EU, 2/ ability to control effectively the export of the items, 3/ ability to make a clear and objective specification of the item, and 4/ need to seek harmonisation and to remove disparities with the regimes of key trading partners that can adversely impact international trade.

3. Catch-All Controls

The possibility for Member States to require an export licence for non-listed items under the catch-all clause in Article 4 is being significantly expanded with the extension of the catch-all clause to cover human rights concerns. A licence will be required if the competent authority has informed the exporter or if the exporter is 'aware' 'under its obligation to exercise due diligence' that the items are or may be intended for human rights violations (art. 4(2)).

As opposed to the existing provision where controls for non-listed items are based on a minimum of legal certainty, (e.g. if the country of destination is subject to an arms embargo), the extension to cover potential human rights abuse is much more open-ended; there may not always be any equivalent objective evidence to 'be aware of', even for companies that do exercise due diligence and invest significant financial and human resources in internal compliance programs. Companies need certainty and consistency. An ability for Member States to expand licences to any technology in which they perceive a dual-use risk wouldn't offer much certainty. Industry needs stable and predictable legislative regimes to plan investment efficiently and to sustain financial growth. This is true for all business activities and decisions, including cybersecurity vendors' choice of where to conduct their research and development activities, where to locate their monitoring and response facilities, where to launch their innovations and where to trade their technologies from. The potential of any of the results of these

activities randomly coming under a catch-all control in the EU could create sufficient uncertainty to undermine the European market's competitive position and attractiveness.

AmCham EU recommends that guidance be issued on the sources and tools that can be utilised by companies to self-determine when catch-all controls should be applied. As a general rule, Member States' governments are best placed, to obtain end user information that can then be shared with exporters on an individual basis to reduce the need for self-determinations. In that regard, the awareness requirement laid out under the proposed new article 1(d) appears vague, and will not serve the pursued objectives, for the following reasons:

- from the exporter's perspective, simple awareness is too low a threshold because it could be based on little evidence;
- and from the government's perspective, it may prove ineffective as desirable controls may be evaded on mere claims of the exporter's unawareness.

Our recommendation is to build on regulatory terminology customarily used by trading partners of the EU, such as the U.S., and to refer to 'a reason to know' criterion. Such a requirement would make both compliance and enforcement easier.

AmCham EU has doubts as to whether the blanket provision for catch-all controls as proposed in Article 4 is at all desirable. This should be communicated through a common harmonised EU list. Companies' due diligence obligation should also be clearly defined to a knowledge criterion relieving companies from any affirmative duty to inquire, verify or otherwise challenge the declared intended use of the dual-use item. At the very least, the Commission should provide a knowledge standard by which decisions must be made, or at a minimum provide guidance on an appropriate 'awareness' standard.

4. Concepts of 'export' and 'technical assistance'

The broad definition of the notion of 'export', especially in article 2(2)(d), and the additional inclusion of the concept of 'technical assistance' in article 2(8) have the potential to extend the export control requirements to any company providing cybersecurity software, services, advice or support from within the European Union, or by EU personnel, to recipients in third countries. This approach could unintendedly bring within the purview of the regulation a wide range of services that should not normally fall under export controlled regimes, and whose inclusion appears neither necessary nor proportionate. Conversely, it is difficult to perceive prima facie how most of these immaterial exports (whether through the 'transmission of software or technology by electronic media' or via technical assistance) could involve a dual-use risk as grave as the 'serious violation of human rights or international humanitarian law, or (…) a threat to international security or the essential security interests of the Union and its Member States' (article 2(1)(b), core definition of cyber surveillance technology).

The definitions in article 2(2)(d) and article 2(8) could be interpreted as applying to any form of cybersecurity consultancy and training, as well as to any form of remote software or IT service delivery, hosted and managed services such as security operations centres, and call-centres and customer support

facilities. Subjecting the bulk of these operations to export licensing requirements would be unjustified, the hindrances it could cause in the normal course of business are undesirable.

AmCham EU recommends refining the wordings of both article 2(2)(d) and article 2(8) as they could apply to EU-based cybersecurity operators' international trade in legitimate cyber technologies. A useful change in the EU regulation would be to distinguish, between 'source code' and 'object code' to the effect of releasing the latter from controls.

5. Intra-company transfer and encryption general authorisations

Two positive elements introduced are the new general EU authorisations for intra-company transfer and listed encrypted items. These authorisations could help reduce compliance burdens and costs.

AmCham EU urges co-legislators to maintain both these authorisations in full as essential counter-measures to the significantly increased burdens EU exporters are likely to face as a result of the proposed Regulation. AmCham EU would like to recommend the following change aimed at making Union General Authorization No EU008 a truly effective tool for the intended users:

Union General Authorization No EU008 ought to refer to the known and defined concept of 'group of undertakings' (ref. EU Regulation 2016/679), since as its scope is currently defined, it would be of extremely limited use to complex organisational structures. We recommend it to be retitled 'Intra-group transfers' and to refer to the definition of 'group of undertakings' used in EU Regulation 2016/679, i.e. where 'group of undertakings' means a controlling undertaking and its controlled undertakings.

Conclusion

The inclusion of cyber surveillance technology and human rights controls within the Regulation could have a serious effect on the cybersecurity industry. It could also impact all legitimate users of lawful cyber capabilities and the research and academic sectors, ultimately hindering also national, European and international cybersecurity efforts.

While industry would be bound by the export licencing regime, rogue players in cyberspace who operate across borders would not be significantly deterred by such provisions and would continue to expand and evolve their methods. Extending controls unilaterally, as the Commission proposes, does little to address global availability. For those items where there are true and genuine concerns they should be included in international commitments, e.g. the Wassenaar Arrangement, in a clearly defined manner.

Instead of simply limiting the use of dual-use cyber surveillance technology, too broadly applied controls, including the human rights catch-all, could harm legitimate usage and impact security professionals and their customers. Legitimate companies and cybersecurity providers may face onerous and time consuming processes to seek export licences before even undertaking operations which have traditionally been viewed as highly critical but quite harmless and straightforward such as sharing cybersecurity relevant information with their customers, partners and affiliates across different regions. Overly strict controls could also impact users of cybersecurity technology as they would have to wait for providers to gain export licences before they can benefit from the latest protective capabilities.

The European academic and research community could also suffer from the administrative overhead and procedural delay that could result from subjecting parts of their daily activities and international collaborations to the regime of dual-use export controls.

For all these reasons, AmCham EU is looking forward to discussing with EU co-legislators options to amend and improve the draft Regulation proposed by the Commission.