DIGITALEUROPE

DIGITALEUROPE Comments on Recent Developments in Council Export Control Working Group

Brussels, 22 November 2018

DIGITALEUROPE, the industry association representing the digital technology industry in Europe, welcomes the continued efforts in the Council to find a practical and workable outcome for a reformed EU Export Control Regulation. As stated from the beginning, DIGITALEUROPE supports the objectives of the European Commission to prevent serious human rights violations by repressive regimes related to the export of offensive cyber surveillance technologies. However, we believe that the means to achieve it should be well considered to facilitate a legally sound and operational export control regime aligned with international best practices. Only when new rules are added internationally, real impact and improvement of the human rights situation globally can be achieved.

Any changes made to the existing Regulation should follow a careful analysis and discussion to prevent any unintended consequences. Existing gaps, such as the continued lack of harmonisation between EU Member States, must be addressed in the review process. It should also be considered to what extent this issue could be better addressed by using other instruments.

We recognise the effort by EU Member States to find a compromise on the human rights aspects. Recent proposals illustrate constructive contributions to the debate that seem to be built on the right principles, in particular that:

- The dual use definition must not be infringed by specific issues such as cyber surveillance.
- International control regimes must remain the baseline for the European dual-use list of items subject to control. New rules should only be added internationally where they can truly have an impact and improve the human rights situations globally.
- Burdensome obligations, responsibilities and uncertainty for exporters must not be increased; any human rights-based controls should only occur upon notification from the competent national authority to the exporter.

We understand Council members have made substantial progress in their discussions, and compromise proposals have started to emerge. Should the consensus be to move forward on the basis of the latest proposed text regarding the issue of human rights, DIGITALEUROPE wishes to highlight the need for further fine-tuning. We are offering below some comments to that end. Moreover, DIGITALEUROPE would like to underline how industry has a keen interest in ambitious proposals on other parts of the Regulation, the new EUGEAs in particular.

The proposals to simplify licensing processes deserve the necessary time for discussion before considering the adoption of a Council General Approach; the Commission's proposed EUGEAs are

critical to create a level playing field for EU exporters both in comparison to similar obligations in third countries and internally within the EU. As such, concerns to reach a final agreement with the European Parliament before the upcoming elections should not override concerns to reach a balanced and well-worked recast across all issues.

It is critical that GEAs for intra-company transmissions of software and technology and export of cryptography are practical. They should simplify and reduce the amount of administrative work required to manage licensing by industry and authorities through a clear and unambiguous legal framework. Adopting licensing simplifications in a fast manner in order to adopt new controls related to human rights violations and acts of terrorism can significantly undermine the very meaning of the EU export control reform. DIGITALEUROPE would like to reiterate its strong support for the new EUGEAs proposed by the European Commission. We believe that they deserve the same attention as the human rights dimension of the recast in the ongoing discussion in the Council export control working group. In this respect, we are providing below our perspective on how they can be the most effective and practical for industry.

KEY MESSAGES

1. EUGEA (009) for Encryption

DIGITALEUROPE strongly supports the steps taken by the European Commission to reduce the barriers surrounding the handling of this crucial technology and to create a common baseline for export control on cryptography in order to facilitate a level playing field. Currently, there are several national general export authorizations (NGEAs) for encryption products at EU Member State level, some of which have a very wide coverage. For instance, Germany, the Netherland and the UK implemented such simplified licensing arrangements in their countries already. Additionally, the US Government implemented licensing simplifications for cryptographic products (ENC license exception).

DIGITALEUROPE strongly recommends that the new EUGEA 009 for encryption should at least match or exceed all benefits already available under NGEAs in the EU as well as ENC license exceptions in the US. This is the only way to create a level playing field within the EU and with countries from outside of the EU and to ensure an added value for most of the industry using them; the EUGEA should mirror the same export privileges awarded by the US ENC license exception and set a more level playing field. Otherwise, EU exporters will continue to face competitive disadvantages. Moreover, if too narrow, an EUGEA could be redundant in comparison to existing NGEAs and thus be inexpedient for harmonization by creating further segmentation and different benefits across the EU.

Moreover, the categorization of items eligible for the proposed EUGEA 009 (other than parameters from Annex I to EU Reg 428/2009) is likely to result in additional administrative burden which can dilute the benefits of adopting licensing simplifications. This is because such categorization will require time-consuming assessment of item eligibility for EUGEAs. With shorter lifecycles of

technology products today, frequent re-assessment of categorization for comparable but distinct products will be required. Similarly, encryption standards will continue to change. DIGITALEUROPE would also like to highlight that notifications or reporting require a significant amount of technical details. They have the potential of diluting the benefits of using EUGEA 009 for cryptography. This should be avoided by all means.

In light of the above, exporters should continue to have the option to use current licensing arrangements instead of EUGEA 009 for cryptography in case the existing authorizations are more beneficial e.g. very comprehensive global export authorizations.

2. EUGEA (008) for Intra-Company Transfers of Software and Technology

DIGITALEUROPE would like to stress the importance of the proposal of the European Commission and amendments by the European Parliament to establish a new EUGEA on intra-company transmissions of software and technology transfers. For the member companies of DIGITALEUROPE, the ability to innovate and offer market-leading solutions and products is closely linked to the free flow of information and technology within a company. To date, these transactions may need multiple export licenses from different export authorities for company internal operations. With an effective general licence in place, resources of the private sector and licensing authorities would be saved, and more focus can be given to critical transactions. Hence, an effective and comprehensive EUGEA on intra-company technology transfers would add substantive value to the industry and contribute to reducing administrative burden and speeding up internal processes for instance in the area of product development. As a general rule, global licenses do not fulfil these objectives to the same extent as they are too static for an international (project) environment that constantly evolves.

In order to make the EUGEA effective and ensure an added value for the industry in using it, it is important that the EUGEA does not only cover transfers from a parent company to its wholly-owned or controlled entities (downstream), but also from a subsidiary / controlled entity back to its parent company (upstream) as well as among its subsidiaries (horizontal transfers). Moreover, the scope of the EUGEA should not be limited to commercial product development but company internal cooperation projects in general.

In addition to the intra-company sharing of technology and software, it should also be considered how the transfer of hardware within one corporate structure for research purposes could be facilitated.

DIGITALEUROPE is aware of existing concerns related to this proposal, linked e.g. to high risk of diversion or uncontrolled transfer of intellectual property, including via acquisitions. However, transfers between corporate entities represent low risk transactions as they will remain within one corporate structure and no external transfer will take place outside the company. There is indeed a very strong rationale for companies to prevent any outside transfer of their technology as they are careful to protect their intellectual property. The EUGEA for intra-company transfers of technology and software should therefore apply to all internal transfers as long as the technology/software

remains under the ultimate ownership of the company (excluding countries of concern). Importantly, given that also company internal research is generally undertaken with a view to commercial product development, there should be no limitation to "pure" research purposes.

To ensure that transfers do not occur to any unauthorized external party, companies must establish an Export Management and Compliance Program (ICP) to ensure consistent instruction and operational application of a company's export policies, procedures, decisions, and transactions. This provision was outlined in the EUGEA 008 proposal as one of the conditions of this new EU-wide general authorization.

3. New Catch-All Provisions

As expressed in previous contributions, DIGITALEUROPE considers that a very broad catch-all clause will not be an effective instrument to prevent the misuse of cyber-surveillance goods and technologies. We continue to have serious concerns around extending the catch-all to cyber surveillance technologies. However, should such controls be included, we welcome proposals to make such a catch-all more targeted and managed only by relevant state authorities; any specific instrument should apply at national level only, and controls should be targeted and practical with respect to the information businesses have at their disposal and without adding unclear demands of due diligence.

The proposal that the Commission should be given powers to adopt delegated powers to amend the definition of cyber surveillance technologies, based on which Member States could adopt catch-all provisions under article 8, should be rejected. Delegated powers can only be given to amend non-essential elements of the Regulation. Definitions are an essential element and should only be amendable via the normal legislative procedure.

4. New Autonomous List and Definition of Cyber Surveillance

DIGITALEUROPE is of the opinion that the proposal by the European Commission for an autonomous list would expand the category of items considered "dual use" in a conceptually concerning manner. Dual-use items should continue to be identified by their technical characteristics rather than their potential misuse.

Moreover, we are concerned that an EU autonomous list would give a competitive disadvantage to industry established in the EU as industry established elsewhere would not be required to apply for export licenses for the same items. While critical items would continue to be exported to the same destinations and non-compliant actors would go unpunished, compliant companies taking human rights obligations seriously would suffer essential economic loss.

We have taken note of the proposal to introduce the products listed in the Commission's proposed Annex I.B into the definition of cyber surveillance technologies for products that could be captured by the human rights catch-all licence. Whilst we strongly continue to prefer not to have the items mentioned at all in line with above argumentation, we believe there is some merit in including them

in the definition rather than in an annex as an autonomous list. Pursuing this model would have the benefit that a license would only be needed for these items when requested by the authorities and not for all export of such items which is the consequence of creating the autonomous list. However, this should be made fully clear to be the case and that no license requirement for this type of items can arise from article 4.

We also appreciate the reworked definition of cyber surveillance technologies which seems to at least partially follow a similar approach to the European Parliament's amendment. As DIGITALEUROPE commented on the European Parliament's amendment, it is however crucial that the wording "or of the owner or administrator of the system" be added to the sentence "without the specific, informed and unambiguous authorisation of the owner of the data" to ensure defensive cyber security technology does not get captured. Furthermore, the examples mentioned in the definition should be deleted. If you have a clear definition you should not need examples and the risk is they leave room for interpretation. If your item is not covered by the example it can either be controlled or not.

Overall, the definition should thus read: "'Cyber surveillance items' shall mean items (hardware, software, technology) specially designed to enable the covert intrusion into information and telecommunication systems with a view to monitoring, extracting, collecting and analysing data and/or incapacitating or damaging the targeted system without the specific, informed and unambiguous authorisation of the owner of the data ***or the owner or administrator of the system***. ~~This includes items related to the following technology and equipment such as, for example, mobile telecommunication interception and data analysis equipment; intrusion software; monitoring and data analysis centers; lawful interception systems and data retention systems; and digital forensics.~~"

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total over 35,000 ICT Companies in Europe represented by 66 Corporate Members and 39 National Trade Associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK