Council of the European Union
General Secretariat

Brussels, 15 May 2018

WK 5755/2018 INIT

LIMITE

CONOP
COMER
CFSP/PESC
ECO
UD
ATO

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

CONTRIBUTION

From:	CZ, CY, EE, FI, IE, IT, PL, SE, UK Delegation
To:	Working Party on Dual-Use Goods
Subject:	Paper For Discussion - For Adoption Of An Improved EU Export Control Regulation 428/2009 and For Cyber-Surveillance Controls Promoting Human Rights and International Humanitarian Law Globally

On behalf of the Czech, Cypriot, Estonian, Finnish, Irish, Italian, Polish, Swedish and the United Kingdom's delegation, delegations will find attached a discussion paper on the recast of the dual-use regulation.

14 May 2018

PAPER FOR DISCUSSION

FOR ADOPTION OF AN IMPROVED EU EXPORT CONTROL REGULATION 428/2009 AND FOR CYBER-SURVEILLANCE CONTROLS PROMOTING HUMAN RIGHTS AND INTERNATIONAL HUMANITARIAN LAW GLOBALLY

1. Introduction

The Czech Republic, Cyprus, Estonia, Finland, Ireland, Italy, Poland, Sweden and United Kingdom express their sincere gratitude to all experts having submitted the working paper WK 1019/2018 INIT (hereinafter the "working paper") on the recast of Regulation 428/2009, which, by clearly defining options and clusters, is helpful for the Presidency and the Dual-Use Working Party (DUWP) to focus their deliberations. We also welcome the working paper's calibrations and restraints on issues that several Member States considered as problematic with the recast proposal.

We believe all Member States recognize that cyber-surveillance technologies could be misused in connection with serious violations of human rights and international humanitarian law in repressive states. It is also true that cyber-surveillance technologies have entirely legitimate uses for law enforcement, countering radicalization and fighting terrorism. Withholding such products could also be detrimental to human rights in many instances. Therefore, measures to prevent misuse must be proportionate, balanced and predictable.

Dual-use products make up 5-24 % of EU's total exports depending on calculation model and supports at least 1 million jobs.[1] As is the case for exports generally, well-functioning legislation is vital for jobs, growth and future innovation in the EU production and export of dual-use goods and services, including high-tech goods such as cyber-surveillance technologies. Amendments to the Regulation that will create legal uncertainties and introducing unilateral measures deviating from the international control regimes,

[1] EC Impact assessment on the recast (12785/16, September 2016) p. 19-21 and Ecovry's and Sipri's study FINAL REPORT Data and information collection for EU dual-use export control policy review (November 2015) p. 48]

such as an autonomous EU control list, could seriously undermine the competitiveness of EU-based industry.

The working paper lists the following options for addressing cyber-surveillance controls: a) an EU autonomous list, b) the extended use of national measures under article 8 of the regulation, c) any other practical solution such as establishing a common EU position for proposing new listings in the Wassenaar Arrangement for certain cyber-surveillance items, and d) a specific definition (amending the wording of article 2 and taking into account practical needs on effective network security solutions).

This paper is aimed at developing the other options in b) and c,) thus complementing the working paper and giving Member States a better assessment of which option or options to choose from. The final part of the paper is addressing the important issue of cyber-surveillance controls in a manner that is effective, credible and global. The proposed way forward is also fully in line with other important interests for the EU such as security, promotion of the EU's foreign policy objectives and a level playing field for the industry.

Building on the working paper, this is a paper aiming to be helpful in the search for a possible compromise in the Council and in the trilogues. The right for further comments is reserved and this text does not change the national negotiation directives in the Member States supporting this paper, all subject to national government and parliament decision-making procedures.

2. Reasons for not accepting the proposal for an EU-autonomous list

One of the most difficult issues, where several Member States have concerns, is the Commission's proposal for an EU-autonomous list. Currently, EU export controls under Regulation 428/2009 derive from international obligations, implementing the commitments previously agreed upon in the international export control regimes. The EU's control list is a compilation of the controls agreed upon in the international export control regimes (the Wassenaar Arrangement, the Nuclear Suppliers Group, the Australia Group and the Missile Technology Control Regime).

The success of a trade control regime is predicated on a multilateral, coordinated approach. Traditionally, the EU has adhered strictly to the international regimes. The current proposal would result in a fundamental deviation from this practice and could have a detrimental impact on the multilateralism that has underpinned the success of the regimes to date.

The export control regimes have the highest available technological competence and broad participation, encompassing between 35-50 states which are the main dual-use suppliers ranging from EU Member States, Australia, Canada, Japan, Republic of Korea and the United States, but in some regimes also Brazil, Russia, India, China and South Africa.[2]

The EU and its Member States should make every effort at this timely moment to encourage newly admitted and potential members with significant growth prospects, such as India, to commit to the regimes and to effective implementation of the controls in practice, as well as to encourage the United States to remain unwavering in its commitments to strengthen the regimes and to nationally implement all controls agreed in the regimes.

The impacts of introducing an EU-autonomous list within the existing dual-use export control system would be far-reaching, and difficult to assess. They relate to foreign, security and trade policies.

If the EU were to change the Regulation to address new areas that go beyond what the Regulation was originally created for, and take an approach which is not supported by the international export control regimes, there would be a risk of retaliatory actions or counter-measures by important non-EU trading partners. This risk would be much greater in the case of EU controls than that of MS national measures, due to the EU's size.

There is a significant risk that the EU listing cyber-surveillance items separately from dual-use items, would set a precedent that undermines attempts to incorporate them into international dual-use regimes. Similarly, if international partners perceive the EU to be expanding its interpretation of 'dual-use' beyond the agreed definition, those countries will be very wary of any subsequent proposals by Member States' to include new types of items in the regimes.

For EU companies, the EU-autonomous list would mean they were no longer operating on a level playing field in the global market, where sustained competitiveness is key for survival.

Related to the issue of level playing field, it is important to point out that the effect of EU-only controls would be symbolic rather than preventative: those seeking cyber-surveillance technology have no shortage of non-EU vendors from which to choose. While EU industry has strengths in this area, it is far from having a global majority market share on high-end technology in the rapidly-developing cyber-

---

[2] Brazil, Russia, India, China and South Africa form the group "BRICS", an association of five major emerging national economies.

security sector. Controls on EU exports without parallel measures in the other major economies would serve only to push the development and production of relevant technologies outside of the EU.

EU dual-use legislation that deviates from international dual-use legislation would also be less attractive for third countries to emulate as a model. This would be unfortunate as this model legislation serves as the basis for many third countries' efforts in preventing the proliferation of Weapons of Mass Destruction. Adoption of the EU legislation as a model does also stimulate mutually beneficial trade between the EU and third countries.

The quality of the EU-autonomous list would be inferior to the quality of the current control lists as it would not be processed through the regimes' thorough working methods involving the most competent experts in the world. Poorly defined EU-controls would not make much of an impact for the promotion of Human Rights and International Humanitarian Law.

In addition, it remains unclear to Member States if the proposed EU-autonomous list, albeit limited when first introduced, could, in the worst case, over years develop into a broad-ranging list of any new technologies such as artificial intelligence, robotics etc., thus portraying Europe as a technology-averse continent and an unlikely home for any global frontrunners on ICT or other technologies of the future generations.

Safeguards against this are needed. Controls should be avoided where they would be excessive or where their impact has not been assessed sufficiently.

3. Promoting Human Rights and International Humanitarian Law more effectively in the Exports of Cyber-Surveillance Technology in the EU and Globally

We would like to seek common ground in the Council on highlighting the need to respect human rights and to do more to ensure this with regard to export of cyber-surveillance technology to third countries.

The EU is already acting within the EU Common Foreign Security Policy-framework to prevent EU exports of cyber-surveillance items to certain repressive regimes. The EU sanctions on Syria and Iran were expanded in 2011 to include cyber-surveillance technology and recently a similar set of controls was included on EU's sanctions on Venezuela. It is appropriate to evaluate these measures and their impact in order to make the EU sanctions on cyber-surveillance technology smarter and more effective when decided by the Council.

The Wassenaar Arrangement already covers some cyber-surveillance items (5A001f,j and 4A005, 4D004, 4E001 a, c) and it is important to keep the momentum for new proposals in this field. While cyber-surveillance items are one group of new emerging sensitive technologies that can affect individual security and freedoms, they are equally military relevant as they can affect regional and international

security and stability. Cyber-surveillance items therefore have their rightful place in the control list in the Wassenaar Arrangement and are likely to become an even more important in the future. The EU could advance a common approach on its general support for cyber-surveillance items listing in the Wassenaar Arrangement.

In addition, Article 8 allows Member States to continue or begin implementing national measures to control their exports of certain cyber-surveillance technology. These measures should be strengthened by developing new information exchange elements, so that all Member States would become aware of denials issued on the basis of national measures and also to learn from each other's experiences.

The Council should discuss possibilities to increase transparency between Member States and to the public on licenses and denials based on Human Rights and International Humanitarian Law grounds. This would have significant long-term positive effects as Member States would adapt their controls – and their practical implementation – while companies would increase their level of corporate social responsibility and all this would be done without weakening the international regimes.

One new commitment could be that Member States make public, at their own initiative or at request, information where denials to destinations are mentioned as well as approved licenses, destinations and category items.

4. The need for legal clarity

We fully endorse the position in the working paper that "the Regulation itself must provide for legal clarity, foreseeability of controls for stakeholders and enforceability by national authorities". There are several elements in the proposal that do not live up to these requirements, for instance additional catch-all controls (art 4.1 d) and new broad assessment criteria (art 14), which therefore should not be accepted. It is also important to find legal clarity and a balanced approach on proposed relaxations by EU-licenses for exports to third states.

5. Organising the work in the Council during the Recast Process

We trust that the Presidency will want to keep the Council as united as possible. Voting in the Council should be avoided, whenever possible, especially on issues relating to foreign and security policy and national security considerations.

The EU Council key test of leadership should not be on adopting a controversial reform of EU legislation by a vote, but on finding a united common position which can also be supported by those third countries which have key roles internationally, thus making the European views shape the export controls globally.

6. Proposed Way Forward

For the reasons outlined in this paper the following options are proposed for Member States to consider:

1) To recognize in Council that cyber-surveillance technologies could be misused in connection with serious violations of human rights and international humanitarian law in repressive states and that misused cyber-surveillance technology can also create risks to essential security interests of the EU and its Member States.

2) Based on an evaluation of EU restrictive measures already in place, to develop smarter and more effective EU sanctions controls on cyber-surveillance technologies, including those not controlled by the Wassenaar Agreement, which are likely to be used in connection with serious violations of human rights and international humanitarian law.

3) To make concerted efforts in the international export control regimes to address the issues relating to cyber-surveillance items. An EU common approach on general support for cyber-surveillance listing in the Wassenaar Arrangement could be considered.

4) To explore the extended use of national measures in the context of Article 8, which may be adapted to facilitate this option. Member States could engage in peer-to-peer exchange to learn from those Member States which have national implementation of cyber-surveillance controls under Art. 8 of the EU Regulation, including sharing all relevant denials in the DUeS, as appropriate.

5) To increase transparency in EU export control, for example by making public at Member States' own initiative or at request, information where denials to destinations are mentioned as well as approved licenses, destinations and category items, as appropriate.

The options above could be manifested in Council Conclusions (Foreign Affairs - Trade) upon adoption of the recast.