Shared statement on the update of the EU dual-use regulation

May 2017

Introduction

The NGOs below welcome the proposal of the European Commission to update controls on the export of dual-use items, which represents an important effort to make human rights central to European Union trade policy.

By expanding the definition of dual-use goods, and specifically including cyber-surveillance technologies, the Commission proposal recognizes that digital surveillance gravely threatens human rights; especially the right to privacy and freedom of expression. It poses a threat to the ability of human rights groups, journalists and activists to fulfill their watchdog role.

The proposal – by the explicit inclusion of human rights considerations – is also an important recognition of the pre-existing responsibilities of both states and businesses. Under international human rights law, states have a responsibility to protect people against human rights abuses by non-state actors, including by regulating such non-state actors under their controls to prevent them from causing or contributing to human rights abuses in other countries. Companies also have a pre-existing responsibility to respect human rights in their operations, including by carrying out human rights due diligence to "identify, prevent, mitigate and account for how they address their human rights impacts."

We applaud these positive steps and express the hope that the proposal will lead to regulations that will provide a mechanism for the realization of these human rights responsibilities. During the implementation phase, member states should aim to ensure that all EU level unilateral changes are adopted within international export control control lists.

In this spirit, we call attention to the following key areas which we hope can be further improved;

Human Rights Protections Must be Strengthened

Content of human rights considerations should be strengthened. Article 8, Article 4(1)(d) and Article 14 contain language regarding the consideration of human rights either in decisions on whether to subject non-listed dual-items to licensing, or whether to grant export licenses. However, these clauses either lack specificity (in the case of the latter) or contain limitations (in the case of the former).

These clauses should be strengthened to guard against all risks to human rights and to recognize that serious human rights violations may occur outside situations of armed conflict or recognized situations of internal repression. In doing so, the proposal should require the consideration of relevant European human rights protections, such as the EU Charter of Fundamental Rights as well as those developed by the Court of Justice of the European Union, and the European Court of Human Rights, such as the opinion in *Zakharov v. Russia*, which offers guidance on the specific safeguards needed to ensure that secret surveillance complies with human rights law. The EU should ensure that the same human rights standards apply abroad as do inside the EU.

Exports that pose a substantial risk to human rights must be denied. Article 14(1)(b) requires only that the competent authorities in Member States – when considering export authorizations –"take into account… respect for human rights in the country of final destination as well as respect by that country of international humanitarian law," while Article 14(1)(c) mandates consideration of the internal situation in that country, such as the existence of armed conflict. However, Article 14 does not mandate a denial of export licenses in cases where the consideration of the above criteria reveal human rights concerns.

The proposal should make clear that states are required to deny export licenses where there is a substantial risk that those exports could be used to violate human rights.

The proposal should also make clear that where there is no legal framework in place in a destination governing the use of a surveillance item, or where the legal framework for its use falls short of international human rights law or standards, the export must be denied.

All Relevant Surveillance Technology Must be Covered

A mechanism to update the EU control list should be agreed, which will decide on updates to the EU control list in a transparent and consultative manner, taking into account the expertise of all stakeholders, including civil society, and international human rights law.

The extension of the catch-all clause in the proposal is a welcome step which holds the potential to help future-proof export controls by allowing for the inclusion of new and emerging dual-use technology on the basis of the potential for human rights harms.

However, as drafted, the catch-all clauses do not adequately clarify the responsibilities of either states or businesses to assess the human rights risks posed by non-listed dual-use items. As such, this clause risks failing to achieve its human rights potential.

These requirements must be strengthened if they are to have a meaningful application. The human rights responsibilities of companies to investigate, prevent and mitigate human rights risks, as well as the obligations of states to oversee and regulate this process, must be clarified in order to ensure that all relevant dual-use technology is subject to licensing.

Greater Transparency is Needed

Transparency regarding export licenses granted, and denied, including information regarding the type of equipment concerned, the product category, description, value, destination country and end use/end user is crucial in enabling parliaments, civil society, industry, and the broader public – both in the EU and in recipient countries – to meaningfully scrutinize the human rights impact of the trade in dual-use items.

The Commission proposal contains provisions for the publication of an annual report by the Commission to the Parliament and Council, as well as requirements for publication when a non-listed dual-use item is subjected to authorization procedures by a member state. However, as it stands, neither of these provisions require a sufficient amount of detail.

The proposal should be amended to require that member states publicly disclose – at a minimum – information regarding individual license approvals and denials, the type of equipment concerned, the product category, description, value, destination country and end use/end user as well as the reasons for the approval or denial of licenses.

Protect Security Research and Security Tools

The proposal states, in the preamble, that export controls should “not prevent the export of information and communication technology used for legitimate purposes, including law enforcement and internet security research.” To reinforce the above principle currently stated in the preamble, the new regulation should include clear and enforceable safeguards for the export of information and communication technology used for legitimate purposes and internet security research.

First, the proposal should go still further to clarify that definitions of terms such as “intrusion software,” “technical assistance” and “intangible technology transfers” shall not be construed to cover uses such as private exploitation research, and legitimate security items such as anti-virus products, fuzzers, defensive pentesting, zero day exploits/vulnerabilities/proof of concepts, exploit generation software and jailbreak software. More and better defined exceptions for security research are required.

Second, the control language should be amended to prevent these sorts of over-breadth, taking into account the chilling effect of any language and also focusing on the intent of the exporter, in order to ensure that no offensive tools are controlled if they are used for defensive purposes. This should be accomplished via an inclusive consultation that takes account of specialized expertise in this area. If an item does not meet these requirements, it should be removed from the control list.

Third, cryptography items should be removed from the list, and no new items added where their inclusion undermines security research, such as forensics tools. Encryption is essential in supporting the safety and security of users, companies, and governments everywhere by strengthening the integrity of communications and systems.

We look forward to continuing to contribute to this process. Further information can be found at the individual websites of member organizations.