Marietje Schaake – Member of European Parliament (ALDE / D66)

DATE of SUBMISSION: 15.10.2015

Final written submission to the public online consultation on the export control policy review (Regulation (EC) No 428/2009)

A. Introduction

1. In this submission to the European Commission's public consultation on the review of Regulation (EC) No 428/2009 [1], I will give a basic outline of the current export control mechanism in relation to human rights concerns and the EU's strategic foreign policy objectives, and where it fails to address these concerns. Consequently I will list a series of amendments to the Regulation that can fix the current shortcomings in section C of this document.

2. I welcome that the Commission before the summer also provided stakeholders an opportunity to contribute to the "data collection process", which would support the impact assessment that accompanies this review process.[2]

3. Given that article 25 of the Council Regulation (EC) 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use (the **"Regulation**") requires the Commission to review the Regulation after three years, I cannot help but note that this review process is long overdue. This is especially the case given the rapid developments of and changes in technologies, changes in the political situation in third countries and the fact that legislation was not up to date with technological developments to begin with. Nevertheless I am happy to once again contribute to the review process, which I did on several occasions from 2011 onwards.[3]

4. Throughout my contributions to this process, I have consistently noted the need to take into account newly developed technologies that facilitate or have an impact on access to information, the right to privacy, surveillance, censorship and freedom of speech. Particularly in light of these new technologies, a human rights approach to the review process should be strengthened, and explicitly include human rights concerns in the framework of the dual-use export control mechanism. I therefore stress that the Commission should indeed evolve towards a "human security" approach[4], which recognizes that security and human rights are inextricably interlinked. This approach would better address the risks that EU

[1] http://trade.ec.europa.eu/consultations/index.cfm?consul_id=190
[2] http://trade.ec.europa.eu/doclib/docs/2015/april/tradoc_153352.pdf
[3] See most recently my own initiative report on Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries' (2014/2232(INI)) which was adopted by the European Parliament on 8 September 2015.
[4] COM(2014) 244 final, para.

exports of 'cyber-surveillance technology' could violate human rights and threaten the digital infrastructure of the EU and its Member States.

5. It should be noted that the regulation in fact addresses more than just the exports of technologies. It is a broad regulation that was created to control the exports of all goods, software and technology which have a legitimate civilian use, but which can also be used for military applications or can contribute to the proliferation of Weapons of Mass Destruction. Given that many technologies that are used for surveillance, hacking and intrusion purposes could also have legitimate law-enforcement purposes, the dual use regulation has been the legislation under which it has been proposed to address their proliferation.

B. Human rights concerns

Current practices

6. The export, transit and brokering of dual-use goods from the EU is governed by Regulation (EC) No 428/2009.[5] This export control policy is based on lists compiled in the following international fora: the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, the Australia Group, the Missile Technology Control Regime and the Nuclear Suppliers' Group.

7. Exporters have a licensing obligation if they want to export an item or product that (1) is not covered by a General Export Authorization (**GEA**) and (2) is listed in the annexes to the Regulation or (3) if Member States (**MS**) invoke a so-called 'catch-all control' (the "**catch-all**") as per article 4 of the Regulation.

8. In case a MS invokes an abovementioned catch all control concerning a non-listed item (e.g. because technical specifications have been changed in order to evade the threshold) this only constitutes an (ad hoc) licensing obligation for this specific item to be exported from that specific MS. A serious shortcoming of this measure is that it allows multi-national companies to choose the most favourable MS as their 'safe haven' for exports. The strictly national nature of the catch-all mechanism does not create a level-playing field for companies and creates unwanted competition between MS.

9. An exporter who is not sure whether an item requires an export licence (proactively) asks the licensing authority in the MS where he is registered whether an export license is required. This requires a voluntary decision by the exporter – which also seriously undermines the effectiveness of a catch-all control. Also note that the MS bear responsibility for the assessment and not the Commission, meaning MS will be forced to make a decision where they balance economic gains against potential human rights violations.

10. This is where the asymmetrical implementation of the Regulation comes into play. As the Commission has very little or no access or knowledge of the benchmarks and assessments,the MS apply in considering whether a license will be issued, it cannot smoothen the dissimilar practices and ensure a level playing field.

11. The result of the diverging national export mechanisms are that companies in certain MS experience huge competitive disadvantages (or advantages) but also

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF

that there is no universal EU export policy or analysis of the situation on the ground in third countries – which can potentially constitute threats to both human rights in third countries as well as to the EU's own security policy. This in turn systemically undermines the EU's Common Foreign and Security Policy and credibility in third countries.

12. While the export of dangerous technology has mostly been addressed within the context of the dual-use regulation, it is a question whether some technologies should not fall under the weapons export control regime, since their only legitimate use would either be military or by law enforcement agencies. This is a question the Commission should address when looking at how to define specific technologies, its parts and/or functions.

Examples

13. In the summer of 2015 the client list of Italian company Hacking Team was leaked online. Evidence emerged that Hacking Teams´ products were marketed and sold to various countries, including Azerbaijan, Bahrain, Egypt, Ethiopia, Kazakhstan, Morocco, Nigeria, Russia, Saudi Arabia, the UAE and Uzbekistan, many of whom have been criticised by international human rights organisations for their aggressive surveillance of citizens, activists and journalists both domestically and overseas.[6]

14. Below I have listed a number of reports on the direct involvement of EU technologies in human rights violations. I believe that only a dialogue between policy makers, companies, security researchers and NGO's will result in a comprehensive and efficient solution.

Iran:

1. Iran's web spying aided by western technology (2009).

http://online.wsj.com/article/SB124562668777335653.html#mod=rss_whats_news_us

2. Iranian policy seizing dissidents get aid of western companies (2011).

http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html

Bahrain:

3. Torture in Bahrain becomes routine with help from Nokia Siemens (2011).

http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

Libya:

4. Firms aided Libyan Spies (2011).

[6] http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html

Syria:

5. U.S. firm acknowledges Syria uses its gear to block web.

http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html?mod=googlenews_wsj

Egypt:

6. Vodafone under fire for bowing to Egyptian pressure (2011)

http://www.guardian.co.uk/business/2011/jul/26/vodafone-access-egypt-shutdown

Ethiopia

7. "They Know Everything We Do" Telecom and Internet Surveillance in Ethiopia

http://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_0.pdf

Morocco

8. How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists

http://www.slate.com/blogs/future_tense/2012/08/20/moroccan_website_mamfakinch_targeted_by_government_grade_spyware_from_hacking_team_.htm l

Relevant developments in export control policy since 2011

15. In specific cases, the export of dual-use items may be subject to additional EU restrictive measures (sanctions). Such restrictive measures currently apply with respect to trade of dual use items with Iran and Syria. In view of the "continued brutal repression and violation of human rights by the Government of Syria", Council Decision 2011/782/CFSP included a prohibition on the export of telecommunications monitoring equipment for use by the Syrian regime. Similarly, one year later the Council Decision 2012/168/CFSP of 23 March 2012 included a "prohibition on the export of telecommunications monitoring equipment for use by the Iranian regime (...) in view of the gravity of the human rights situation in Iran".

16. In June 2012 the Council adopted the European Union's Strategic Framework on Human Rights and Democracy, which urged the Council, Member States and the Commission to "include human rights violations as one of the reasons following which non-listed items may be subject to export restrictions by Member States" in order to preserve freedom of expression online and offline.[7]

[7] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/131181.pdf

17. In December 2012, the European Parliament adopted my report ´Digital freedom Strategy´ in EU Foreign Policy[8], which called for (1) a ban on exports of repressive technologies and services to authoritarian regimes, (2) the establishment of a list, to be regularly updated, of countries which are violating freedom of expression in the context of human rights and to which the export of ´single use´ items should be banned; single use items could include certain targeted jamming, surveillance, monitoring and interception technology products and services and (3) called on the Commission to provide EU businesses with a wide range of information and guidance, based on the UN's 'Ruggie principles', so as to ensure compliance with both business interests and corporate social responsibility.

18. This 2012 Strategy also stressed that the Commission should be able to provide companies that are in doubt as to whether to apply for an export licence "with real-time information on the legality or potentially harmful effects of trade deals; this should also apply to EU or EU-based companies entering into contractual relations with third-country governments, whether in order to win operating licenses or negotiate standstill clauses or by accepting public involvement in business operations or public use of networks and services".

19. The Strategy further urged the commission to submit proposals "requiring increased transparency and accountability on the part of EU-based companies, as well as the disclosure of human rights impact assessment policies, with a view to improving the monitoring of exports of ICTs, products and services aimed at blocking websites, mass surveillance, tracking and monitoring of individuals, breaking into private (email) conversations or the filtering of search results".

20. Finally, the Strategy urged the Commission to exclude companies which are selling these technologies to countries deploying repressive government policies against human rights activists and political dissidents with regard to digital rights, internet access and ICTs from EU procurement procedures and calls for tender;

21. During the 19th Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, held in Vienna on 3-4 December 2013, two EU members on behalf of the expert group proposed that the list be expanded to include two types of surveillance technologies: "Systems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery of, or communication with 'intrusion software'" and mass "IP network surveillance systems." These measures adopted by the Wassenaar Arrangement entered into force in the EU on 31 December 2014.

22. Regulation (EC) No 428/2009 was amended in April 2014. However, this update did not contain many of the points that the European Parliament had been pushing for. The most important part of the update was that it allowed the Commission to more speedily update the export control lists that the MS authorities should use.

23. As part of the update to Regulation (EC) No 428/2009, the European Parliament, the Council and the Commission (on initiative of the European Parliament negotiators) issued a joint statement on a further review of the dual-use export control system. The three institutions acknowledged "the issues regarding the

[8] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0470&language=EN&ring=A7-2012-0374

export of certain information and communication technologies (ICT) that can be used in connection with human rights violations as well as to undermine the EU's security, particularly for technologies used for mass-surveillance, monitoring, tracking, tracing and censoring, as well as for software vulnerabilities".[9]

24. The statement continued: "Efforts will also be intensified to promote multilateral agreements in the context of export control regimes, and options will be explored to address this issue in the context of the on-going review of EU dual-use export control policy, and the preparation of a Commission Communication. In this context the three institutions took note of the agreement on 4 December 2013 by the Participating States of the Wassenaar Arrangement to adopt controls on complex surveillance tools that enable unauthorised access to computer systems, and on IP-network surveillance systems". Most importantly, the statement stated that the three institutions "commit to further development of the existing 'catch-all' mechanism for dual-use items falling outside the Annex I of the Regulation, in order to further enhance the export control system and its application within the European single market".

25. In its 2014 communication on the review of the export control policy the Commission indicated that it might consider a "human security approach", which "may also imply a clarification of control criteria to take into consideration broader security implications, including the potential effect on the security of persons e.g. through terrorism or human rights violations". The Commission also indicated that it might consider developing a "smart security" approach, which "may imply EU actions to promote multilateral decisions on cyber-tools, or alternative options such as the introduction of EU autonomous lists or a dedicated catch-all mechanism".[10]

26. The Council´s adopted in May 2014 its "EU Human Rights Guidelines on Freedom of Expression Online and Offline", which stated that the EU "will promote action at the international level to develop best practices and respect for human rights with regard to the export of technologies that could be used for surveillance or censorship by authoritarian regimes". [11] These guidelines mirrored many ideas that the European Parliament had previously set out in its resolution on a Digital freedom Strategy in EU foreign policy.

27. In November 2014 the Council recalled the joint statement of the three institutions of 16 April 2014, and stated in its conclusions on the review of the export control policy that "Member States will assess whether further export controls are necessary to prevent internal repression or terrorism. Therefore, the Council welcomes further discussion and an intensified exchange by the relevant technical experts".[12] The Council also agrees that a tighter cooperation with academia and research centres would improve the control of "dual-use research", while avoiding undue obstacles to the free flow of knowledge and the global competitiveness of EU science and technology. Finally, the Council notes "that

[9] Joint statement attached to Regulation (EU) No 599/2014 of the European Parliament and of the Council of 16 April 2014 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items
[10] http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf
[11] http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf
[12] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/145903.pdf

controls on non-listed dual-use items are an essential part of controls. Member States should consider whether the application of “catch all” controls could be further developed, while acknowledging at the same time that the instrument is aimed at specific cases. The Council calls for Member States and the Commission to explore options for enhanced information sharing".[13]

28. In September 2015, in adopting my report on Human Rights and Technologies, the European Parliament recalled the "incomplete nature" of the EU dual use regulation "when it comes to the effective and systematic export control of harmful ICT technologies to non-democratic countries". The Parliament urged the Commission to swiftly put forward "a proposal for smart and effective policies to limit and regulate the commercial export of services regarding the implementation and use of so-called dual-use technologies, addressing potentially harmful exports of ICT products and services to third countries, as agreed in the Joint Statement of the European Parliament, Council and Commission of April 2014; calls on the Commission to include effective safeguards to prevent any harm of these export controls to research, including scientific and IT security research".

29. The Parliament stressed again (cf. para 37) that the Commission should swiftly be able to provide companies that are in doubt as to whether to apply for an export licence with accurate and up-to-date information on the legality or potentially harmful effects of potential transactions.

30. The Parliament also called on the Commission "to submit proposals for a review of how EU standards on ICTs could be used to prevent the potentially harmful impacts of the export of such technologies or other services to third countries where concepts such as ‘lawful interception’ cannot be considered equivalent to those of the European Union, or, for example, that have a poor record on human rights or where the rule of law does not exist".

31. The Parliament reaffirmed “that EU standards, particularly the EU Charter of Fundamental Rights, should prevail in assessments of incidents involving dual-use technologies used in ways that may restrict human rights;

32. The Parliament deplored the "active co-operation of certain European companies, as well as of international companies trading in dual-use technologies with potential detrimental effects on human rights while operating in the EU, with regimes whose actions violate human rights" and urged the Commission publicly to exclude companies engaging in such activities from EU procurement procedures, from research and development funding and from any other financial support.

33. The Parliament called on the Member States to ensure that existing and future export control policies do not restrict the activities of legitimate security researchers, and that export controls are applied in good faith, and only to clearly defined technologies intended to be used for mass surveillance, censorship, jamming, interception or monitoring purposes, or for tracing and tracking citizens and their activities on (mobile) telephone networks.

34. The Parliament further called on the Commission to appoint an independent group of experts that can perform a human rights impact assessment on existing EU standards for ICTs, with the goal of making recommendations for adjustments that will increase the protection of human rights, particularly when systems are

[13] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/145903.pdf

exported. The Parliament further noted that a voluntary approach is not enough, and that binding measures are required to encourage companies to take into account a country's human rights record before selling their products there, and to carry out an assessment of the effect their technologies will have on human rights defenders and government critics;

C. Remedies to current shortcomings in the Regulation

Action 1: EU wide catch-all

35. The current catch all controls do not require an EU wide application if a MS decides to invoke such a control triggered by grave human rights concerns. If exported technologies are to become instrumental in human rights violations, then all MS should work together and establish an EU wide ad hoc licensing requirement. This will also prevent the 'race to the bottom' by multinational companies active on the EU's internal market.

Action 2: Ensure transparency and accountability

36. A key component of the upcoming review of the dual-use regulation must be to ensure more transparency and accountability in the export control regime. MS and the European Commission should have a pro-active notification obligation towards the Parliament and submit an annual report of the number and nature of license applications, in order to ensure proper oversight and eventually set up one objective standard for the issuing of export licenses. Where possible, documents relating to the number of licenses, customers and products must be made public.

Action 3: Penalties

37. The EU needs a coherent system of penalties for companies who transgress the export control legislation. It should be clear that a failure to adhere to the rules is unacceptable and will carry a large penalty. A uniform system across the EU should be introduced consisting of fines and personal liability of the board and CEO of companies that illegally export products to third countries.

Action 4: Introduction of a simplified GEA for intra-company transfers

38. Companies with employees in different jurisdictions face challenges in complying with export control regulations, especially in the context of intangible transfers of technology. In order to avoid infringing on scientific freedoms and risk constraining innovation in order to promote legal clarity, the EU should establish a precise GEA relating to intra company transfers, which enables the EU to draw up a list of items that are not allowed to be transferred (without prior consent) to non-EU entities outside the company.

Action 5: Country specific lists

39. The changes in North Africa and the Middle East, but also in Ukraine and Russia, have over the past years required urgent EU action, e.g. in relation to the adoption of (targeted) restrictive measures like oil embargoes, asset freezes and investment bans. In a similar way the EU should be able to address what some have called the 'buy-side' of dual use technologies in a flexible way, by imposing ad hoc export license requirements on certain products, to certain countries, to prevent the ongoing export. Reportedly the U.S. pressed for additional export

controls in the Australia Group on the export of biochemical technology to Syria. This is an example of how the goal of more targeted action and flexibility can be accomplished when applied to monitoring / surveillance items. There should be more effective coherence between human rights and political assessments that are made by the EEAS and MS on an ongoing basis and licensing applications.

40. It should be noted that these additional export controls do not address the problems of so-called technical assistance by EU companies (e.g. software updates, operational teams on the ground) to governments of countries that are subject to (ad hoc) restrictive measures, as technical assistance is not qualified as the export of items, but are services.

41. Technical assistance is covered in the current dual regulation. It is important to make sure that the provision of technical assistance is also controlled when it is part of a contract to buy a certain product, i.e. when there is no direct payment for the technical assistance. This could for example concern software updates.

Action 6: EU 'know your customers' guidelines on exports

42. The Commission should set-up and provide 'know your customer guidelines' on the basis of the UN "Guiding Principles on Business and Human Rights"[14] that give guidelines to companies to assess whether their goods may be used for internal repression or human rights abuses. These guidelines can consist of a checklist of 'flagging criteria' that could indicate potentially suspicious transactions. On this basis, companies can assess the plausibility that their products may be used to violate human rights before the sale is completed. The Commission in turn should monitor enforcement of these know your customer rules. Whistleblower protection should be offered to employees of exporters that report non-compliance.

Action 7: Helpdesk for companies

43. The Commission should swiftly be able to provide companies that are in doubt as to whether to apply for an export licence with accurate and up-to-date information on the legality or potentially harmful effects of potential transactions. To this end, a company helpdesk should be set, which should closely liaise with MS export control authorities to provide companies with the necessary information. In order to consider companies' needs, guidance should be provided by sufficiently qualified personnel through a helpdesk on a confidential, or – where necessary – on an anonymous basis.

Action 8: Dialogue with exporters

44. Given the often intangible transfer (or export) of technologies, it is key that the exporters are also pro-actively engaged in preventing their tools from becoming instrumental in human rights violations. Obviously exporters that are well known by the public, and whose sales are dependent on a good reputation will most likely comply with the EU's and MS export mechanisms. However, subsidiaries and spin offs of these companies, or companies that do not fear reputation loss often operate under the radar out of tax havens and are less vulnerable to a public outcry. Exporters should take responsibility and increase transparency regarding exports by smaller companies that belong to their holdings. The Commission should have a clear mandate to demand transparency.

14 http://www.business-humanrights.org/SpecialRepPortal/Home/Protect-Respect-Remedy-Framework

Action 9: Investigate possibility to start infringement procedure

45. The Commission should investigate the possibilities for launching infringement proceedings against a country whose export control authority has exported dual use goods in violation of the updated dual use regulation. It must be clear that the dual use regulation requires a uniform and consistent application in order to be effective. The European Commission needs to make sure that this happens and, when necessary, be ready take steps against national authorities

Action 10: Dialogue with security researchers in STEG

46. The Commission and MS authorities must engage in dialogue with security researchers. An appropriate framework for this is the Surveillance Technology Working Group (STEG) within the DG Trade Dual Use Working Group. While controlling the export of technology to prevent human rights abuses is essential, export controls should not hinder the legitimate transfer of technology which can be used to protect human rights and for research. With this in mind, consulting security researchers and experts is essential.[15]

Action 11: Allowing third country citizens to report

47. Those in third countries often suffer the most damage from violations of or loopholes in EU export control legislation. Therefore the EU needs to create a mechanism for citizens, human rights organisations and human rights defenders in third countries to report instances where they believe export control legislation has been circumvented or should be updated. This could be done in the form of a reporting hotline, or by creating a separate contact point within the dual-use coordination group. The European Commission should collect reports and disseminate them to the relevant MS export control authorities.

Action 12: Address unintended consequences of the intrusion software control

48. The 2013 inclusion of 'intrusion software' in the List of Dual-Use Goods and Technologies and Munitions List of the Wassenaar Agreement has led to an unintended chilling effect on the work of (independent) security researchers, despite numerous statements of members of the Wassenaar Agreement, export control authorities, NGO's, the European Parliament and the European Commission, and despite the existence of numerous safeguards in the Wassenaar Agreement and the Dual Use Regulation. In order to remove this unintended chilling effect, the Commission could find inspiration in statements that clarify that the scope of control on the "development" of intrusion software applies only to end use cases and end users facilitating or conducting surveillance activities.[16]

[15] See also the discussion in the first session of the 'Real Digital Security' hearing at the European Parliament http://www.marietjeschaake.eu/2015/10/video-real-digital-security-how-to-modernize-the-eus-export-control-regime-and-the-trade-in-zero-day-vulnerabilities/

[16] See also https://cdt.org/files/2015/07/JointWassenaarComments-FINAL.pdf, pp.21-25.