Final Draft

Overview of Recent Developments in the Export Controls of Surveillance Technologies in Europe

There have been many developments in recent years in regards to the control of the exports of surveillance technologies in Europe – so many in fact that it is hard even for experts to retain an overview of what is going on. The following document is designed to provide a brief precisely this overview of key developments in 2015 as well as a better idea of the current status of the main debates on export controls. As further changes in the existing export control regime are to be expected in Europe and beyond in 2016 & 2017, it is particularly important that all actors engaged in the debate are aware of the current state of play.

1. The European Union

a. The European Commission

Regulation No. 428/2009, regulating the European export of dual-use items, has been under review by the European Commission since 2011. As pointed out in Communication (2014)244, the European Commission has set out to review export control policy in Europe as a means to "ensuring security and competitiveness in a changing world."[1]

A new draft Regulation is expected **around the beginning of 2016**. The Commission is currently in the final stages and setting out to complete the impact assessment that started in 2015.[2] The goal of the impact assessment is to analyze the costs and benefits associated with different review options mentioned in the Communication. The European Commission held a public consultation via an online survey from July to October 2015.

Results of the Public Consultation

The results of the public consultation are now available.[3] 97 stakeholders participated in the survey and provided some feedback regarding export control of dual-use good and possible new regulations. Most of the participants hailed from the private sector: industry associations and dual-use exporters and manufactures represented 78% of the respondents, whereas civil society representatives corresponded to 8%. The large majority of the respondents agreed that the current export control regulations could be improved through a review. Key conclusions from the consultations are summarized here:

- Human Security Approach: Around 40% of the respondents found that adding the **human security approach would not increase EU security** and that it would also not decrease the risk that EU exports of cyber-surveillance technology that

[1] http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf

[2] The Commission launches a data collection project in support of the Impact Assessment of its export control policy Brussels, 23 April 2015 http://trade.ec.europa.eu/doclib/docs/2015/april/tradoc_153352.pdf

[3] EU Export Control Policy Review- Online Publication Report http://trade.ec.europa.eu/doclib/docs/2015/november/tradoc_154003.pdf

could be used to commit human rights violations. There were equally many participants who **did not believe that adding human rights criteria** be an adequate instrument in preventing the misuse of dual-use goods to perpetrate human rights violations. Most agreed that pursuing a human security approach would have the best impact in increasing security and competitiveness of the EU industry and more level-playing field across the EU if it were done through a **multilaterally-agreed list-based control** rather than EU autonomous list-based controls.

- "Smart security" mechanism and modernization of trade controls: There was broad consensus regarding the smart security approach via **voluntary consultations** on dual-use items and **yearly updates** of the EU control list, as well as **regular consultations** with industry and development of guidelines. It was generally agreed that these measures would be favorable for EU export control policy.

Export Control Forum-December 7,2015

At the most recent Export Control Forum held in December in Brussels, the most heated debate surrounded the topic of the “Human Security Approach”[4]. Several private sector actors **argued against the idea**, many fearing it would **hurt European exports** and place European exports at a **disadvantage with competitors** such as the USA and China, if stricter export regulations were to be adopted in relation to human rights issues. Another concern expressed by several representatives of businesses exporting dual-use goods, was that such approach is **not specific enough** and would make it hard for businesses to determine what constitutes a human rights violation. Some even asked, if this approach would require hiring political scientists to evaluate such risks.

Additional sources:

The Roadmap for the review, February 2015: http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2015_trade_027_duxc_en.pdf

Consultation strategy, July 2015:
http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153627.pdf

Comprehensive Change Note Summary for Council Regulation (EU) No. 428/2009 - October 2015: http://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153892.pdf

Update of the EU Control List of Dual-Use Items Brussels, 22 October 2015
http://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153907.pdf

Annual report on the implementation of Regulation (EC) No 428/2009, July 2015: setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items
http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153612.pdf

[4] For more information regarding the Export Control Forum held December 7, see:
http://trade.ec.europa.eu/doclib/docs/2015/december/tradoc_154041.pdf

Public results survey:
https://ec.europa.eu/eusurvey/publication/Exportcontrolpolicyreview

1.2. The European Parliament

Workshop on Dual Use Export Controls

In June 2015, the European Parliament's Committee on International Trade and Sub-Committee on Security and Defense held a workshop to provide information to the members about the review process.[5] Due to the co-decision powers granted in the Lisbon Treaty, the European Parliament will play an important role in the review. The report produced by Sybille Bauer and Ian Stewart provides an analysis of the review options. On the topic of cyber-surveillance technologies the paper mentions that in recent years several "off-the-shelf" surveillance technologies that allow governments to intercept private information even when encrypted are more readily available and often fall through the cracks due to lacking regulation of such technologies. The report also discusses the **additions of intrusion software** to the Wassenaar Arrangement and the ensuing criticism that followed from security researchers. The European Union adopted these changes in 2014 and the U.S. Bureau of Industry (BIS) proposed to also adopt the provisions. The authors also mention the position of certain that the EU should create its own list, their position is that the best solution is "to first put proposals to the Wassenaar Arrangement in the first instance and consider EU-only controls if these proposals are not accepted".

Resolution on human rights and technology

On September 8th, the European Parliament adopted by 371 votes to 293, a resolution drafted by Marietje Schaake concerning "Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries"[6]. The Parliament highlighted the importance of technological developments and access to an open internet in allowing the fulfillment and respect of human rights. Parliament recognized that surveillance of communications violates the rights to privacy and freedom of expression if it is not conducted within an adequate legal framework. The members called for further coherence between the EU's external actions and its policies connected to ICTs.

On the topic of the dual-use regime, Parliament prompted the Commission to bring a proposal for smart and effective policies to limit and regulate the export of dual-use technologies, address exports of harmful exports of ICT products and services to third countries. It also called on the Commission to include safeguards that would protect security research. Members also reiterated the importance of the EU Charter of Fundamental Rights in the consideration of incidents concerning dual-use technologies'

[5] Ian J. Stewart & Sybille Bauer, Workshop on Dual Use Export Controls (Section 6.4 Cyber Tools and Surveillance Technologies, p.30)
http://www.europarl.europa.eu/RegData/etudes/STUD/2015/535000/EXPO_STU(2015)535000_EN.pdf

[6] European Parliament resolution of 8 September 2015 on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries' (2014/2232(INI))
http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2015-0288
More information on Marietje Schaake's work on stopping EU aided surveillance
http://www.marietjeschaake.eu/2015/12/five-years-of-stopping-eu-aided-surveillance-interactive-timeline/

misuse that result in human rights violations. Parliament lamented the active cooperation of some European companies and international companies who traded in dual-use technologies involving potential restriction of human rights. Parliament also urged the Commission to exclude such companies from EU procurement procedures, from research and development funding as well as other financial support.

Marietje Schaake's Recommendations

On October 15, 2015 Marietje Schaake submitted recommendations in the scope of the online public consultation conducted by the European Commission on the review of the export control of dual-use items.[7] The submission gives a brief outline of the current export control procedures relating to human rights concerns and the EU's policy objectives and how the current mechanisms fail to address those concerns. It recommends a series of amendments that would improve the current Regulation that and its shortcomings. Schaake approves of the human security approach because it recognizes that security and human rights are inextricably interlinked. The approach represents a better way to address risks that EU exports of cyber-surveillance technology would result in human rights violations and security threats to European digital infrastructure.

In the submission, Marietje Schaake proposes 12 actions that would remedy the EU's shortcomings in dual-use regulation. Some of these actions include the creation of a "EU-wide catch-all clause, establishing country-specific lists by imposing ad hoc export license requirements on certain products, to certain countries, to prevent the ongoing export, setting up EU 'know your customers' guidelines on exports, allowing third country citizens to report instances where export control legislation has been circumvented and address unintended consequences of the intrusion software control"[8].

1.3 National parliaments

Public expert hearing at the German Bundestag

On December 16th, 2015 a public expert hearing was held at the German Bundestag. The topic of this hearing was "Improving effectiveness of export controls of surveillance and espionage software on the German national and European level and public calls for tenders". The hearing was proposed by the parliamentary committee "Digital Agenda".[9] Several experts were called on to provide their point of view on the issue.

Götz Neuneck declared that the recent additions to the WA of IP network surveillance, of intrusion software to the dual-use regulation Nr.428/2009 in category 4 and the resolution of the European Parliament on September 8, 2015 were all steps in the right direction when it comes to the export control of cyber-surveillance technologies.

[7] Final written submission to the public online consultation on the export control policy review (Regulation (EC) No 428/2009): http://www.marietjeschaake.eu/wp-content/uploads/2015/10/MarietjeSchaakeMEP-SubmissionCommission-consultation15102015.pdf

[8] For an overview of the 12 actions, see : http://www.marietjeschaake.eu/2015/10/marietje-schaake-proposes-12-actions-to-remedy-human-rights-shortcomings-in-the-eus-dual-use-regulation/

[9] https://cihr.eu/export-controls-bundestag-hearing/
https://www.bundestag.de/bundestag/ausschuesse18/a23/anhoerungen/fachgespraech/399038

Sandro Gaycken also believed that the expansion of the control list in the Wassenaar Arrangement is a very important step. However he did no believe that a liberalization of cryptography would be helpful and like Neuneck argued for greater regulation of computer software exploits.

Ben Wagner stated that export controls regulations remain one of least transparent areas of government regulation, and that human rights should be at the core of current export control regulations in Europe. He also recommends the liberalization of current encryption controls, as demanded both by European civil society and industry.

Christian Mihr mentions that transparency regarding the export of dual-use goods must be ameliorated. He provided numerous examples of how the use of surveillance technology enables human rights violations around the world.

Michael Waidner argued that computer software exploits should be 'radically banned.'[10] He welcomes existing export controls and argues that they should be much more restrictive in order to ensure better network security.

2. Civil society reports

a. Report "Data and information collection for EU dual-use export control policy review" by Ecorys and SIPRI

Ecorys, a European research and consultancy company, and the Stockholm International Peace Research Institute (SIPRI), carried out a data collection project, that included a section on surveillance technologies, on behalf of the European Commission and which was aimed at informing the review of the EU's Dual-use Regulation. The final report from this study was published in November 2015. The study looked at surveillance methods, which can cause human rights violations, including mobile telecommunications interception equipment, intrusion software, monitoring centres, lawful interception systems and data retention systems, and biometrics. .[11] Here are some key findings from the study:

- Monitoring centres and lawful interception systems are **only partially** covered by Annex 1 whereas **biometrics is not covered**.
- There were **no agreed standards** on use at EU level for mobile telecommunications interception equipment, intrusion software and monitoring centres.
- The expansion of the control list to monitoring centres has led **some companies to move outside of the EU**. The companies that did not move found that there were some advantages to the controls. However, there is a need for clearer

[10] Experten zu Überwachungstechnik: "Exploits radikal verbieten" www.heise.de/newsticker/meldung/Experten-zu-Ueberwachungstechnik-Exploits-radikal-verbieten-3045606.html

[11] Ecorys & SIPRI, Final report: Data and information collection for EU dual-use export control policy review, November 6, 2015 (Section 7 The cyber-surveillance sector, p.142-221). The final report is available from the European Commission's DG Trade or from SIPRI upon request.

information from EU bodies and national licensing authorities on what destinations and end-users should be considered suitable customers.

- Germany has already expanded its control to monitoring centres but it estimates that these **changes will have a limited effect on the German economy**, even though Germany has the most companies active in this field. Germany maintains that the controls affect only a small number of companies, many of which are already subject to export controls.
- **Human security approach**: The respondents to the case study on the human security approach did not see this approach in a positive way. Several industry representatives found that adopting a EU-based human security standards for the export of cyber-surveillance technologies could disadvantage European companies versus companies outside the EU, thus having a negative impact on exports, compliance costs and EU-wide level playing field. Several stakeholders reiterated the need for the EU to develop clearer guidance on assessing such license requests.
- **Obligatory EU-wide self-regulation** for producers of cyber-surveillance technologies: Most respondents identifying themselves as suppliers of cyber-surveillance technologies found the obligatory EU-wide self-regulation viewed this as the less negative of the review options. In support of this there was mention of good practice guidelines that can be used to develop standards for self-regulation.
- **Autonomous control list in the EU**: Government officials and industry representatives agreed that control list additions via the Wassenaar Arrangement were preferable adding only at the EU level.
- EU **catch-all mechanism** on cyber-surveillance technology: Ten EU Member States responded that the adoption of an EU catch-all clause for cyber-surveillance technologies **would have a negative impact on administrative costs** and **the EU-wide level playing field**. It would however, have a positive impact on avoiding the transfer of exports that could result in human rights violations.
- Suppliers found that a **catch-all would have a negative impact** on their exports, compliance costs, investment and production, and the EU-wide level playing field. Stakeholders pointed out that if the technology and end-users covered by the catch-all were not well defined it would be **difficult to effectively implement**, a possible solution would be to have a specific list of destinations.
- Those in favor of the catch-all argued that it could potentially capture exports that are not covered by a list but still cause a threat to human rights, it can keep up with the rapid developments in cyber-surveillance technology.

b. Report “A critical opportunity: bringing surveillance technologies within the EU Dual-Use Regulation” by CAUSE

Released in June 2015, the report calls for regulation that is “sufficiently comprehensive, detailed and precise to ensure that all relevant technologies are regulated, while preserving a space for legitimate security research and the development of ICTs essential to the realisation of human rights.”[12]

[12] The Coalition Against Unlawful Surveillance Exports (CAUSE) was formed in April 2014 and is made up of the following NGOs: Amnesty International, Digitale Gesellschaft, FIDH, Human Rights Watch, Open

CAUSE advances that an effective export control policy that prevents violations of human rights needs regulation that requires export control authorities to take into account human rights implications when taking decisions. The report also stresses the importance of the disparities between the member states to be addressed via the new regulation, these disparities allow for certain countries avoiding licensing and finding loopholes.

The report addresses five issues that need to be addressed for the EU dual-use regulation to effectively prevent human rights violations through the export of its surveillance technology:

- all relevant surveillance technology must be subjected to licensing,
- human rights must be considered within the assessment criteria,
- disparities between national policies must be addressed,
- security research and security tools should be exempt from control
- encryption control should be eliminated.

To ensure that all relevant surveillance technologies be subject to export control the report recommends the following measures:

- Establishment of autonomous list of equipment and technology used for surveillance that should be reviewed regularly and later added to the Wassenaar Arrangement (WA)
- Use of dedicated catch-all mechanisms with specifications on end-use and end-users, this mechanism would prevent new technologies of avoiding licensing requirements
- Items used by intelligence gathering and law enforcement should be subject to licensing
- Protection for security research and open source software
- Security researchers, industry and civil society should be involved in policy process
- Surveillance technologies should be included in EU embargoes

The report calls for a human rights approach in line with the obligations held in the Charter of Fundamental Rights of the European Union rather than the human security approach. CAUSE argues that the concept of “human security” is not widely known and is mostly found the in academia as a result it is not well-defined or legally binding, this has the risk of reducing human right protection rather than broadening it. It is the coalition’s view that a human rights-based approach would be the most effective approach, as human rights law is already well defined within international law. Furthermore there are opinions by UN special rapporteurs and international courts’ rulings on the topic of a human rights approach in cyberspace. Additionally, the Charter of Fundamental Rights of the European Union protects among others the rights to privacy, freedom of expression and the protection of personal data.

Technology Institute, Privacy International, Reporters Without Borders and Access. https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf

The report also recommends that if the new regulation adds human rights implications in export assessment criteria, there will be need for guidance provided by respective member states.

2.c. Report "Surveillance, Software, Security, and Export Controls" by Thomas Dullien, Vincenzo Iozzo and Mara Tam

A draft report was submitted **to the Bureau of Industry and Security, U.S. Department of Commerce** (BIS) with comments and recommendations regarding surveillance, software, security and export controls.[13]

The report comments that the recent additions of intrusion software to the Wassenaar Arrangement, more specifically entries 4.A.5., 4.D.4. and 4.E.1.c., **do not represent an effective control of harmful intrusion software**. They argue that the current definition of "intrusion software" is formulated in such a way that many security practices and tools are encompassed, whereas **several types of malicious software are not adequately covered**.

As a result, states are having difficulty implementing the new Category 4 entries and it seems the current mechanism of capture does not produce efficient controls as was originally intended and causes a significant burden to those involved in security research. For these reasons, the authors recommend amendments that would improve the current regulation by providing "clear, viable points of control relevant to commercial surveillance and monitoring tools, but not relevant to the tools and practices of information security".

As the authors point out, the WA currently presents "intrusion software" to be designated by qualities of design or modification for the purposes of avoiding detection by monitoring tools or for the defeat of protective countermeasures. Nonetheless, such criteria can be found in several analytic, systems administrative, and security tools. Therefore, those criteria are not efficient in differentiating between malicious and harmless software, as those attributes are shared by both.

The document offers new formulations to the WA Control List with the goal of providing a more efficient control and avoiding negative impact on information security practices. The amendments change the formulation of entry 4.E.1.c., and the definition of "intrusion software". The authors emphasize the importance of adding the criteria of authorization and ownership in order to identify malicious software.

The proposed definition is as follows (changes are highlighted):

[13] "**Surveillance, Software, Security, and Export Controls:** Reflections and recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting," Draft report by Thomas Dullien Vincenzo Iozzo Mara Tam https://tac.bis.doc.gov/index.php/component/docman/doc_view/299-surveillance-software-security-and-export-controls-mara-tam?Itemid=

Cat 4 "Intrusion software" 1. "Software" specially designed or modified to *be run or installed without obtaining the authorization of the owner or 'administrator' of a computer or networkcapable device*, and performing any of the following:
a. The unauthorized extraction of data or information from a computer or networkcapable device;
b. The modification of *system or user data to facilitate access to data stored on a computer or networkcapable device by parties other than parties authorized by the owner or 'administrator' of the computer or networkcapable device*

If the amendments proposed by the authors were adopted, it would prevent the control of legitimate software such as "commercial penetration testing tools, exploits for vulnerabilities, threat information sharing activities, and malware samples distributed among academic or independent researchers". The proposed amendments would in return allow for a control of software that is currently not captured under the current WA: "malicious or modified smartphone apps, attacks that disable encryption functionality on devices for later acquisition and rootkits that are hypervisors".

The report can be seen in the context of similar proposals by Sergey Bratus, Eleanor Saitta and the EFF to improve the existing definition of targeted surveillance technologies in the Wassenaar arrangement. While there has been considerable disagreement among exports on which technologies the Wassenaar arrangement lists should control, many of the actual implementations in countries such as the United States or Japan have been heavily criticised as posing problems for security research.

Thus the report by Thomas Dullien, Vincenzo Iozzo and Mara Tam is important as it represents the best-developed proposal to update export controls of targeted surveillance technologies currently available. It also has the advantage of being particularly surgical in how it updates existing definitions to ensure that the definition of surveillance technologies caught is improved while avoiding overly broad definitions which can more easily be misused.

Additional sources:

EFF to Commerce Department: We Must Revise Overbroad Export Control Proposal
https://www.eff.org/deeplinks/2015/07/eff-commerce-department-we-must-revise-overbroad-export-control-proposal

Bratus, S., I. Arce, ME Locasto, and S. Zanero. 2013. "Why Offensive Security Needs Engineering Textbooks." *Yale Law & Policy Review*.
http://www.cs.dartmouth.edu/~sergey/drafts/why-offensive-security-needs-textbooks.pdf.

Saitta, Eleanor. 2014. "Newly Controlled Items Under the Wassenaar Arrangement." *Dymaxion.org*. https://dymaxion.org/essays/wa-items.html.

Conclusion

The following overview is an attempt to provide a better understanding of the key debates and current state of play in export controls in Europe. It is necessarily selective but also attempts to provide the reader with a better understanding of the most important ideas and proposals currently being discussed on export controls. It also preempts the upcoming proposal in 2016 by the European Commission for a new dual-use regulation of export controls in Europe. Due to the current state of the debate it seems likely that this revision will incorporate a stronger human-rights based approach and more effective control mechanisms.

It can also be expected that in coming years both the EU, it's member states and the Wassenaar arrangement update their export control policies to reflect changes in the surveillance technologies on the market and some of the deficiencies of existing definitions. Export controls on surveillance technologies have had considerable influence on the surveillance technology trade[14] and in order to ensure that they do so effectively changes in existing definitions of surveillance technology will be necessary.

[14] Wagner, Ben, and Claudio Guarnieri. 2014. "German Companies Are Selling Unlicensed Surveillance Technologies to Human Rights Violators – and Making Millions ·." *Global Voices*, September. https://globalvoices.org/2014/09/05/exclusive-german-companies-are-selling-unlicensed-surveillance-technologies-to-human-rights-violators-and-making-millions/comment-page-2/