CENTRE FOR INTERNET
AND HUMAN RIGHTS

https://cihr.eu

EXPORT CONTROLS OF SURVEILLANCE TECHNOLOGIES

Background Paper[1]

TABLE OF CONTENTS

[1] This paper was prepared by the Centre for Internet & Human Rights at European University Viadrina. For further questions about the paper please contact bwagner@europa-uni.de or office@cihr.eu.

INTRODUCTION

In recent years, there has been a growing concern about oppressive regimes using surveillance technologies in ways that lead to human rights violations. As a result of these concerns, export controls of surveillance technologies are developing into an important mechanism of promoting human rights on the Internet. This background paper is part of a research project "Export controls of surveillance technologies" conducted by the Centre for Human Rights at the European University Viadrina (CIHR). This research is supported by the Ministry of Foreign Affairs of the Netherland as part of a wider effort of the government of the Netherlands to promote human rights online and to "put principles into practice" in the run up to the Global Conference on Cyberspace in the Hague on 16 and 17 April 2015.

The first phase of the project included a review of existing initiatives, extensive document analysis and input gathering from leading experts from civil society, private sector, European Union (EU) institutions and national governments. On February 5, 2015, over two dozen experts from different countries participated in an all-day workshop and an evening debate hosted by the CIHR and the Dutch Embassy in Berlin.[2]

This background paper is a result of the first phase of the research and the expert discussion. The first chapter provides a brief overview of the growing body of evidence that oppressive regimes purchased surveillance technologies to monitor and censor citizens online, leading to violations to right to privacy and freedom of expression. In the second chapter, the paper summarizes existing initiatives from international organisations, EU institutions and member states, private sector and civil society which seek to restrict exports of such technologies to countries where they can be used to harm human rights.

Input from participants of the workshop on February 5 is included in third and fourth chapter, but as those discussions took place under Chatham House rule, none of the views or opinions have been attributed to a specific individual or organisation. The third chapter attempts to evaluate whether existing export control measures are adequate and effective in promoting human rights worldwide. The final chapter discusses potential avenues for international policy initiatives to improve the use of export controls in their protection of human rights abroad.

Conclusions of the paper will be subject of a discussion at the Global Conference on CyberSpace in the Hague. The parallel session "Updating of export controls of dual use surveillance technologies" will take place on April 17. Following the conference, research will continue in close collaboration with experts representing different stakeholders. The results of this research will be consulted at a second expert meeting scheduled for fall of 2015.

[2] For more information about the event see: https://cihr.eu/panel-discussion-export-controls-of-surveillance-technology/

1. IMPACT OF SURVEILLANCE TECHNOLOGIES ON HUMAN RIGHTS

The Arab Spring of 2011 demonstrated that the impact of technology on human rights is twofold. On one hand, citizens of several countries in Middle East and North Africa used and profited of latest technologies on an unprecedented scale to fight for their rights and freedoms. On the other hand, the repression that followed the protests revealed that governments had built technological capacity to monitor their citizens online and offline. In many cases, these newly employed technologies enabled government to implement measures harming human rights.

The use of surveillance technologies is most frequently associated with infringements of the freedom of speech and the right to privacy. However, those are not the only rights affected – governments can use surveillance to limit freedom of assembly or increase discrimination based on ethnicity, religion, gender or sexual orientation. In the context of the most repressive regimes, individuals targeted by surveillance are at risk of discrimination, physical violence, imprisonment, torture and death.

1.1. EVIDENCE OF USE OF SURVEILLANCE TECHNOLOGIES MADE IN EUROPE

Four years after the start of the Arab Spring, there has been a growing body of evidence that various governments from different parts of the world, purchased surveillance technologies produced by companies located in the European Union. Civil society, researchers and investigative journalists have been incessantly uncovering evidence of surveillance technologies exported from Europe to countries where human rights might be harmed. Some of the key findings are summarized here:

- Companies in **Finland, Sweden, Denmark, Ireland, United Kingdom, France, Germany and Italy** developed surveillance technologies used in Iran, Syria, Bahrain and Tunisia.[3]
- Products developed by European companies **Gamma, Trovicor, Hacking Team and Amesys** were or are being used to commit violations of human rights.[4]
- Command and control servers for FinSpy backdoors, part of Gamma International's FinFisher "remote monitoring solution" were discovered in a total of **25 countries, many of which have long histories of human rights abuse.**[5]

[3] Wagner, Ben. 2012. *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy*. Brussels, Belgium.

[4] See Benedek, Prof. Wolfgang, and Dr Matthias C. Kettemann. 2014. Freedom of Expression and the Internet. Council of Europe, Section 6.6.2.

[5] Citizen Lab. 2013. *You Only Click Twice: FinFisher's Global Proliferation - Citizen Lab.* https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

- Global market for surveillance technologies has been **growing by 20% annually** and is estimated to be **worth 3 to 5 billion dollars** by industry representatives.[6]
- The amount of EU surveillance technologies sold abroad without a license is increasing. Unlicensed surveillance technology sales by Gamma are estimated at **20 million euros in 2013 alone**, many times more than all German licensed surveillance technology exports combined.[7]

1.2. DEFINITION AND TYPES OF SURVEILLANCE TECHNOLOGIES

As the research develops, the understanding of the type of surveillance technologies that can be used to harm human rights becomes more focused.

- **Tools for interception & monitoring of mobile telephony** such as 'IMSI-Catchers', which "make it possible for the government directly to monitor mobile communications without having to involve the carriers."[8]
- **Mass communications surveillance technologies** that allow for the mass and indiscriminate surveillance of large data streams at a network level where the collection of information " is, by definition, arbitrary."[9]
- **Targeted surveillance technologies** that allow for the surveillance of one specific individual device or set of devices, typically through means of the use of intrusion technologies.[10]

[6] Silver, Vernon. 2011. "Spies Fail to Escape Spyware in $5 Billion Bazaar for Cyber Arms." *Bloomberg Business*, December. http://webcache.googleusercontent.com/search?q=cache:cxl_yairpgcJ:www.businessweek.com/news/2011-12-22/spies-fail-to-escape-spyware-in-5-billion-bazaar-for-cyber-arms.html+&cd=1&hl=en&ct=clnk&gl=de

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

[8] Hosein, G, and CW Palow. 2013. "Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques." *Ohio St. LJ*. Available via http://moritzlaw.osu.edu/students/groups/oslj/files/2013/12/13-Hosein-Palow.pdf

[9] Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8(2): 121–44.

[10] See Maras, Marie-Helen. 2013. "From Target to Mass Surveillance: Is the EU Data Retention Directive a Necessary Measure or an Unjustified Threat to Internet Privacy." In *New Directions in Surveillance Privacy*, eds. Benjamin J. Goold and Daniel Neylan. Routledge.

2. REACTIONS FROM STAKEHOLDERS: INTEGRATING HUMAN RIGHTS INTO EXPORT CONTROL

Findings about export of technologies from EU to countries where human rights might be harmed have motivated civil society organizations, governments and industry to take action. There has been a growing consensus that the EU should review its export control measures to bring them in line with its commitment to protect human rights in third countries.

2.1. INTERNATIONAL INITIATIVES

Wassenaar Arrangement

Of the existing international export control regimes that exist, the Wassenaar Arrangement is perhaps best equipped to govern dual-use ICT technologies at a global level. Currently the Wassenaar Arrangement remains the key coordinating point for harmonizing export controls among the 41 participating states.[11] The Wassenaar Arrangement controls exports by cooperating to establish a common List of Dual-Use Goods and Technologies that is then voluntarily implemented to national laws by participating states. Participating countries also exchange information about specific denials and licenses.

EU member states were among the main proponents of stronger regulation of surveillance technologies on the level of the Wassenaar Arrangement. During the annual plenary meeting in December 2013 in Austria, 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.”[12] These measures adopted by the Wassenaar Arrangement entered into force in the EU on 31 December 2014.

Freedom Online Coalition

The Freedom Online Coalition (FOC) is composed of governments, civil society and private sector around the world from a mix of developed and developing countries. The Coalition’s goal is to coordinate diplomatic efforts to support free expression, association, assembly, and privacy online. In October 2014, the Coalition has called on governments and businesses to curb use of surveillance technology in an international, multistakeholder effort, which “should include the development of appropriate and consistent national laws and policies governing the use and export of such technologies”.[13]

[11] See http://www.wassenaar.org/participants/index.html for further details.

[12] http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_152996.pdf

[13] See https://www.freedomonlinecoalition.com/wp-content/uploads/2014/10/2-FOC-Joint-Statement-on-the-USe-and-Export-of-Surveillance-Technology-October-2014.pdf for further details.

2.2. EUROPEAN UNION INITIATIVES

Since the onset of the Arab Spring, EU governments have increased their efforts to prevent surveillance technologies from getting to countries where human rights might be abused. To this end, the EU has already updated sanctions to Syria and Iran and implemented changes agreed within the Wassenaar Arrangement which came into force on 31 December 2014. It is also currently pursuing a broad review of its existing export control policies with a focus on ICTs and human rights which will be discussed in greater detail below.

EU Restrictive Measures

In reaction to media reports about European companies delivering surveillance technologies to Syria and Iran, the European Union reacted by updating existing sanctions to include embargo on telecommunications monitoring and interception equipment in 2011 and 2012 respectively.[14] Moreover, the EU also prohibits export of equipment that might be used for internal repression as part of measures targeting Belarus, Cote d'Ivoire, Republic of Guinea, Libya, Myanmar (Burma), and Zimbabwe.[15]

EU Dual-Use Regulation

The EU Dual-Use Regulation (EC) N°428/2009, is the primary document regulating the export of dual use goods and technologies, including surveillance technologies.[16] It is through regular updates of this regulation that Wassenaar Arrangement lists are implemented by EU Member States. The regulation is directly binding for all member states, but the implementation and enforcement of the specific procedures takes place on the national level.

On 12 June 2014, the EU institutions adopted a joint statement acknowledging "the issues regarding the 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."[17] In the same document, the EU institutions committed to further developing "catch-all" mechanisms to control goods and technologies that fall outside of Annex I of the Regulation.

The European Commission

The European Commission has also demonstrated willingness to review existing policies in its Communication "The Review of export control policy: ensuring security and competitiveness in a changing world" (COM(2014) 244).[18] The Communication

[14] Syria http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:147:0014:0045:EN:PDF; Iran: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:087:0085:0089:EN:PDF

[15] http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf

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

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0599&from=EN

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

published on 24 April 2014, explicitly discusses a regulation of "cybertools for mass surveillance, monitoring, tracking and interception."

As part of the process of reviewing export control policies, the European Commission is conducting an Impact Assessment and will explicitly include an impact assessment on the export of surveillance technologies. The will be completed by the end of 2015 and pave the way for an update to the dual use regulation in 2016.

On 22 October 2014, the Commission updated the EU list of dual-use items to include, IT intrusion software ('spyware') and IP surveillance equipment in line with the changes adopted at the Wassenaar plenary meeting in December 2013. It reiterated "growing security concerns regarding the use of surveillance technology and cybertools that could be misused in violation of human rights or against the EU's security".[19] The updates to the EU list entered into force on 31 December 2014.[20]

The European Parliament

The European Parliament has been a strong voice pushing for change in the area of export controls for surveillance technologies. Of particular importance was the European Parliament resolution adopted on 5 April 2011[21] calling for a limitation of the export of surveillance technologies: "in connection with a violation of human rights, democratic principles or freedom of speech as defined by the Charter of Fundamental Rights of the European Union, to which Article 6 of the Treaty on the European Union refers, by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use (for example through Monitoring Centres and Lawful Interception Gateways)."[22]

Restriction of the export of surveillance technologies in Europe was also a key part of the Report on a *Digital Freedom Strategy in EU Foreign Policy* of the European Parliament Foreign Affairs Committee (2012/2094(INI)). The strategy explicitly explores the fact that EU-made technologies and services are sometimes used in third countries to violate human rights through censorship of information, mass surveillance, monitoring, and the tracing and tracking of citizens and their activities on (mobile) telephone networks and the internet" (2012/2094(INI)).

Finally, in a resolution adopted on 17 July 2014, the European Parliament calls for an "EU-wide ban on the export to Egypt of intrusion and surveillance technologies which could be used to spy on and repress citizens, and for a ban, in line with the Wassenaar Arrangement, on the export of security equipment or military aid that could be used to suppress peaceful protest".[23] Export controls were also discussed

[19] http://trade.ec.europa.eu/doclib/press/index.cfm?id=1166&title=Commission-updates-EU-control-list-ondual-use-items

[20] http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_152996.pdf

[21] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2011-0125

[22] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2011-0125

[23] http://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/provisoire/2014/07-17/P8_TA-PROV%282014%2907-17_EN.doc

at a public hearing organized jointly by the Subcommittee on Human Rights and the Committee on International Trade.[24]

The Council of the European Union

On 21 November 2014 the Council of the European Union adopted conclusions reviewing the priorities of the EU's trade agenda for the next five years, which express support for further development of the EU export controls.[25] In this document, the Council recognizes 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." In this document, the Council also calls upon Member States to assess the level of harmonization in licensing and in issuing denials, as well as to consider whether the application of "catch all" controls in the area of ICT & Human Rights for non-listed dual-use items could be further developed.

Member States initiatives

The EU Regulation allows Member States to expand export controls to non-listed items priorities, if they make use of this provision included in Article 8 of the Dual-Use Regulation. For example, Italy imposed such a unilateral requirement on the export of a "Public LAN database centralised monitoring system" to the Syrian Telecommunications Establishment in 2012.[26] It was also under this article that the UK restricted exports of tropospheric scatter communication equipment using analogue or digital modulation techniques to Iran in 2008.[27]

Member states can also play an important role by establishing soft law measures such as codes of conduct or guidelines for private sector. This approach was adopted in the UK, where trade association TechUK issued a guide to "Assessing Cyber Security Export Risks" for industry, which helps companies to understand the negative impacts that may arise from uses not intended by the seller.[28]

2.3. PRIVATE SECTOR INITIATIVES

The response of the representatives of the private sector is important in implementing human rights standards in the EU and its export practices with trade partners from outside of the EU. In a position paper on the review of export control policy in the EU, DIGITALEUROPE, an organization representing 59 international companies, recognises a 'special responsibility' in controlling impact of their products on human rights.[29] The paper states that members "have introduced due diligence programs, applied range of policies and processes, and integrated human rights into

[24] http://www.europarl.europa.eu/meetdocs/2014_2019/documents/inta/dv/hearingdigitalsurv_prog_/hearingdigitalsurv_prog_en.pdf

[25] http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/145922.pdf

[26] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2012.283.01.0004.01.ENG

[27] http://www.legislation.gov.uk/uksi/2008/3231/schedule/3/made

[28] http://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf

[29] See http://www.europarl.europa.eu/meetdocs/2014_2019/documents/droi/dv/412_digitaleurope_position_paper_/412_digitaleurope_position_paper_en.pdf for further details.

their corporate culture, while respecting the Universal Declaration of Human Rights and the UN Guiding Principles on Business and Human Rights. DIGITALEUROPE members are committed to respect Human Rights throughout the lifecycle of their products and services, when it comes to design, development and use."

Although big industry players have expressed their willingness to comply with human rights standards, corporate and government transparency measures would help to assess whether they follow through with their commitments. At the same time, it is important to remember that many of the most problematic surveillance technologies are produced and exported by small companies, which often manage to stay under the radar of public authorities and civil society monitoring.

2.4. CIVIL SOCIETY INITIATIVES

Civil society organizations from the EU have intensified their advocacy in favour of greater restrictions in trade of surveillance technologies. In particular, the global Coalition Against Unlawful! Surveillance Exports (CAUSE)[30] has played an important role by compiling and analysing available evidence and urging governments to take action.[31]

Civil society organizations have also assisted victims of unlawful surveillance by filing complaints against EU companies to national courts – in France cases against Amesys and Qosmos were filed by FIDH and LDH, and in the UK, Privacy International filed a complaint against Gamma.[32] Yet, the impact of civil society actors is limited by lack of access to information about licenses requested and approved and the list of companies supplying surveillance technologies.

[30] Cause includes includes Privacy International, Human Rights Watch, Amnesty International, Digitale Gesellschaft e.V., Open Technology Institute, FIDH and Reporters Without Borders.

[31] See www.globalcause.net for further details.

[32] See FIDH. 2014. *Surveillance Technologies "Made in Europe". Regulation Needed to Prevent Human Rights Abuses.* https://www.fidh.org/International-Federation-for-Human-Rights/globalisation-human-rights/business-and-human-rights/16563-surveillance-technologies-made-in-europe-regulation-needed-to-prevent

3. EVALUATION OF EXISTING MEASURES

Workshop participants provided extensive input on the following topics:

3.1 TRANSPARENCY AND ASSESSING IMPACT

There was a broad consensus between participants that more information is needed to ensure that existing and future measures are effective. Information gathering cannot be limited to anecdotal data collected by investigative journalists, whistle-blowers and NGOs, although their work in this area remains crucial and should be supported. Much of the publicly available information about the surveillance technology trade needed to be attained through FOIA requests and parliamentary questions.

Public institutions can be more supportive of systematic research into the subject by voluntarily sharing data about licences they grant and reject. Corporate actors can also be more forthcoming about data available to them. Lack of transparency impedes independent research on the subject, accurate impact assessment of existing regulations and better public understanding of the issue.

3.1.1 Transparency of governments is lacking:

- While some countries have taken steps to improve transparency, access to data about what licences were granted or rejected is limited.
- Some governments in the EU publish some information about individual export control licenses or make it available at request, either through parliamentary questions, freedom of information requests or simply contacting the export control authorities.[33] Many are considering how to improve transparency and provide more information about licensing decisions to the public.
- The European Commission obtains considerable data about export licenses from the Member States, but cannot share it under current regulations.
- Governments are reluctant to share data about licences, because it includes information about companies, which are potentially confidential commercial information. However, governments could evidently share granular data, even if it doesn't disclose specific companies.

3.1.2. Transparency of the private sector should be promoted:

- Transparency reports have become increasingly common in the Internet industry. Companies like Twitter, Facebook, Google and Vodafone have all published transparency reports about request for information about customers or removal of content received from law enforcement agencies in various countries. These existing transparency reports have not however shed light on the increasing growth of the surveillance trade that remains highly opaque.

[33] See http://www.agnieszka-brugger.de/fileadmin/dateien/Dokumente/Abruestung/Ruestungsexporte/20140808_Antwort_KA_Spaehsoftware_Drs182067_1.pdf and https://www.privacyinternational.org/sites/default/files/Privacy%20International_v_HMRC%20Judgment.pdf

- If private sector organisations believe that they are engaged in legitimate transactions of goods that could be considered surveillance technologies either as buyers or sellers they should make these transactions public either in individualised or aggregate form.

3.2 ‘SMART’ REGULATIONS: DEFINITIONS AND SCOPE

There was broad agreement among participants that not all relevant technologies require an authorisation under current export control regimes. Several participants pointed to the fact that the challenge is that definitions are too broad and not ‘smart’ enough to catch the latest technologies. Others expressed concerns about loopholes in existing regulatory frameworks and called for more precise definitions as to technologies under control. In order to balance human rights, security interests and economic interests.

3.2.1 Definitions of surveillance technologies need to be further clarified:

- Technologies evolve quickly and it is a challenge for all actors involved to make definitions clear. The main concern of civil society is for those definitions to be future-proof, to ensure that new technologies will be covered as they emerge. At the same time, clear parameters would help all actors involved: civil society, the private sector and national agencies.
- It was suggested that the expert group in the EU consisting of technical experts from Member States governments (Surveillance Technologies Experts Group) could play a crucial role in bringing in technical knowledge and identifying surveillance technologies that pose a risk to human rights.
- Close cooperation with private industry would facilitate identification of new technologies, so it would be recommended that challenges with new technologies are identified as early as in the research and development phase.

3.2.2. Overregulation can hurt legitimate actors:

- **Research and development:** the potential regulation of Fuzzers[34] in the Wassenaar list, intended to control FinFisher trojans, has proved controversial among security researchers who are concerned it might hinder their work.[35] These concerns are taken seriously by governments and regulatory agencies, who emphasised their intention to implement existing and future controls in a manner that does not negatively affect security research.
- **Civil society actors using encryption:** under the current regime, export of certain cryptography products is restricted even though it can be used by legitimate actors, such as civil society members, journalists or researchers, to protect privacy of communications from surveillance. Most of the participants agreed that regulation of control of encryption needs to be further reduced to ensure that citizens and companies have broad access to cryptography.

[34] See http://dymaxion.org/essays/wa-items.html for further details.
[35] http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf

- **Companies involved in legitimate trade:** the measures aimed at controlling export should consider the interest of private sector by providing certainty and clarity concerning the regulations in place. In order for measures to be effective and consistent they need to be manageable for administration and companies that apply for licences. Some companies also expressed concern that current regulations on cryptography are hurting their legitimate business interests.

3.2.3. Clear definitions help licensing authorities with consistency in implementation:

- Regulations need to be smart for governments to be able to implement them effectively;
- Definitions and lists need to provide clear guidance for companies and for national licensing authorities;
- Clear definitions help to build consistency in implementation between Member States and Wassenaar members.

3.3. POLICY INSTRUMENTS IN THE EU

The role of the EU is to create a regulatory model that is effective and based on high human rights standard. EU regulation can also provide a template for similar regulatory measures in third countries.

3.3.1. EU Dual Use Regulation:

- The current review is an important process, albeit lengthy and slow. Data collection and impact assessment are crucial, so maybe worth the wait: we need to get it right, so it is 'future-proof'.
- One of the main challenges with the Regulation is ensuring uniform implementation across Member States. Subsidiaries take advantage of lack of uniformity.
- Reviewed regulation will have a direct reference to human rights. Also, so it can be used as a model for non-EU countries. Principles are more important than products and lists.
- Different regulatory approaches might be combined:
  - **list-based approach:**
    - **for:** easy to understand for companies and public administration
    - **against:** takes a while to update lists, difficult to be both effective and proportionate.
  - **end-user approach or catch-alls:**
    - **for**: it would give flexibility to act on specific developments but need to make sure that applied uniformly
    - **against**: additional work for regulators, shifting responsibility to companies, runs risk of diverse application across Member States

3.3.2. Access to justice in the EU should be more effective:

Access to justice for victims of surveillance depends on national legislation, which is often not consistent between different EU countries. Prosecutions in the cases that were put forward are lengthy and, in many cases, yet to be concluded. The EU could harmonize access to justice regulations as swift prosecutions can have a preventive effect on companies that export surveillance technologies.

3.3.3. EU Restrictive Measures and Use of the Anti-Torture Regulation:

Some suggested that while sanctions can be effective in some cases, this measure couldn't be applied to all cases since sanctions are often decided really fast and not much consideration is given to specific technologies. Others suggested that there could also be some scope for a listing of surveillance technologies in the anti-torture regulation, as this mechanism was explicitly decided with human rights in mind and has more objective criteria for problematic human rights violations.

3.4. CREATING GLOBAL PLAYING FIELD

3.4.1 Wassenaar Arrangement is a primary forum for multilateral action, but has limitations:

Important steps have already been taken to update Wassenaar lists, but more work is needed to make sure all relevant technologies are covered. Yet, it is often difficult and time-consuming to reach consensus in this forum. To this end it was suggested that:

- EU countries, which make up for a significant portion of Wassenaar Arrangement membership, should push for a high standard of human rights backed by technical expertise.
- Civil society actors need to be involved in the process and the negotiations need to be more transparent to them.

4.4.2 Other multilateral and multistakeholder forums should be used to promote export controls:

- UN level: with the recent creation of the special rapporteur on privacy, the Human Rights Council could be a forum to broaden participation.
- The Freedom Online Coalition could also be a useful venue for coordination on this topic. Here multiple countries have made joint FOC commitments, although it is unclear to what extent such commitments are actually being implemented.[36]

[36] See https://www.freedomonlinecoalition.com/wp-content/uploads/2014/10/2-FOC-Joint-Statement-on-the-USe-and-Export-of-Surveillance-Technology-October-2014.pdf for further details.

4. POTENTIAL AVENUES FOR INTERNATIONAL POLICY INITIATIVES

Based on the debate at the workshop in Berlin and an evaluation of existing proposals and statements by key organisations, the following avenues for international policy initiatives were developed.

4.1. TRANSPARENCY AND ASSESSING IMPACT

A) **Improve transparency** on exports of surveillance technology from governments and companies. Greater transparency would help to better assess the status quo and consequences of different regulations. Regular statistics[37] allow for deeper analysis by civil society and academia and a better understanding of the impact of policy change.

B) **Conduct broader impact assessments** on the effects of Wassenaar controls on the surveillance technology industry for all participating countries. An Impact Assessment is being carried out at the EU level as part of the on-going review of the EC dual-use regulation and will include work on the export of surveillance technologies. However, further impact assessments will be required to assess consequences for all of the Wassenaar countries.

4.2. SMART REGULATIONS: DEFINITIONS AND SCOPE

C) **Close loopholes in definitions of surveillance technologies** to ensure that all relevant surveillance technologies are caught. CAUSE NGOs note that surveillance products remain on the market that are not currently regulated and thus that existing definitions need to be expanded to cover all relevant surveillance products.[38]

D) **Update definitions of targeted surveillance technologies** to ensure that important security research tools such as Fuzzers are not caught. Updating existing definitions could contribute to the resilience of IT systems and ensure that legitimate security research is not negatively affected by export controls.

[37] See http://www.agnieszka-brugger.de/fileadmin/dateien/Dokumente/Abruestung/Ruestungsexporte/20140808_Antwort_KA_Spaehsoftware_Drs182067_1.pdf.

[38] For further details see www.globalcause.net as well as this list of surveillance technologies by Privacy International: https://docs.google.com/spreadsheets/d/15fL62WjeZ2FaMAIsnG37wFrjxk6Q5LLIlWYWmxkQayg/edit?pli=1#gid=1306600553

4.3. POLICY INSTRUMENTS IN THE EU

E) **Integrate a stronger human rights 'catch-all'** in the updated EU dual use regulation to ensure that new surveillance technologies are caught more effectively.[39] This could also be mixed with other regulatory mechanisms to ensure that where necessary export controls apply while still ensuring that companies exporting technology have as much legal certainty as possible.

F) **Update EU regulation of cryptography exports** through a EU General Export Authorization (GEA) for cryptography, which would allow for easier exports of systems containing cryptography from Europe. The U.S. has developed similar exemptions for encryption[40] and similar steps by the EU would be an important measure to increase resilience of IT systems across the world.

G) **Use the EU Anti-Torture Regulation** to include some of the worst surveillance technologies. On-going criminal proceedings in France against two surveillance vendors suggest a strong link between surveillance technologies and complicity in acts of torture.[41] From a legal perspective the torture regulation was explicitly designed to promote human rights globally and thus could easily integrate additional categories.

4.4. CREATING GLOBAL PLAYING FIELD

H) **Strengthen Human Rights Assessment Criteria** in existing export controls regimes. Current application of existing human rights assessment criteria differs between countries and better coordination between the EU, U.S. and other Wassenaar countries could assist in improving the implementation of existing criteria.

I) **Build additional capacity** of key global export control agencies to improve the implementation of existing export controls both inside and outside of the Wassenaar regime. Given the complexity of the technology and the considerable knowledge gaps that remain capacity building could be a useful tool to promote a uniform approach.

J) **Closer Coordination with key U.N. Special Rapporteurs & U.N. Human Rights Council** who have in the last years repeatedly produced reports which recommended states taking measures "to prevent the commercialization of surveillance technologies" (A/HRC/23/40). Both Human

[39] https://digitalegesellschaft.de/2015/01/ueberwachung-eu-ausfuhrkontrollen/

[40] https://www.federalregister.gov/articles/2011/01/07/2010-32803/publicly-available-mass-market-encryption-software-and-other-specified-publicly-available-encryption

[41] See http://blogs.mediapart.fr/blog/jamesinparis/060914/les-affaires-qosmos-et-amesys-vecues-de-linterieur for further details.

Rights Council and Special Rapporteurs could serve as a key bridge to a global community working on these issues, rather than limiting it to a more focussed European perspective.

CONCLUSION

The expert workshop in Berlin showed clearly that governments, public institutions, civil society and majority of private sector actors share a common concern: preventing surveillance technologies from getting into the hands of oppressive governments. Indeed, effective measures to reduce illegitimate trade are supported by almost everyone except for vendors of surveillance technologies themselves.

Notably there was no complete consensus among participants on which of the measures proposed in this paper are most urgent and effective. However, there was an apparent agreement that many different policy avenues can and should be combined in order to achieve desired result: for example, further updates to the Wassenaar lists, stronger human rights 'catch-alls' and private sector due diligence.

Whatever approach is taken, it needs to be based on evidence about impact of specific measures. This in turn requires greater transparency from public and private actors. Steps forward should also take into consideration interests of legitimate actors and provide clear guidance for companies and for national licensing authorities. In short, moving forward on export controls for surveillance technologies is not just possible but also necessary to ensure that communications networks fulfil their promise of upholding human rights.