DOI : 10.14746/pp.2015.20.3.11

Ben WAGNER, Joanna BRONOWICKA

Frankfurt (Oder), Germany

Between International Relations and Arms Controls: Understanding Export Controls for Surveillance Technologies[1]

Abstract: Export Controls are becoming an increasingly important dimension of international relations, however there is still relatively little literature on their usage and implementation. The following article attempts to show the development and problems surrounding export controls in a new area: surveillance technologies. These have recently been integrated into international frameworks for export controls, bringing with them a row of challenges and questions for policy makers. Based on extensive conversations with practitioners and key experts in the field, this paper attempts to sketch out key ideas and solutions in this area as well as important responses that have been developed to (perceived) challenges.

Key words: export controls, surveillance technology, international relations, global governance

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. The following article intends to provide an overview over the key points of the debate. How has the debate on surveillance technologies developed in recent years, what problems have been identified by experts within this debate and what are the main policy solutions they suggested?

The first section 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 section, 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 various key experts is included in section three and we are particularly grateful for the participants of the expert workshop organise on 5 February 2015 at the Netherlands Embassy in Berlin whose input was key in developing the third section. Finally the conclusion provides some ideas on how to move the debate forward and perspectives for the future.

---

[1] This research 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) and funded by the Netherlands Ministry of Foreign Affairs.

1. The 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.

The cases of human rights abuses are very diverse and include serious human rights challenges in many different countries. For example Anita Gohdes argues that in Syria the Internet is being used as a weapon of war with Internet disconnection (Gohdes, 2015). Her research suggests that: “regimes implement large-scale disruptions selectively and purposely in conjunction with launching larger battles. Evidently, not all battles are accompanied by outages, but when they are, they tend to be preceded by a substantial increase in violence” (Gohdes, 2015, p. 13). There is a clear link in here research between the Syian disconnection of networks and surveillance, which is has repeatedly been suggested are externally sourced (Waleed, 2011).

This however is not the only case of European or North American surveillance technologies being used for targeted and mass surveillance purposes. Indeed Companies in Finland, Sweden, Denmark, Ireland, United Kingdom, France, Germany and Italy developed surveillance technologies used in Iran, Syria, Bahrain and Tunisia (Wagner, 2012). There are even specific company names that have been presented, with products developed by European companies Gamma, Trovicor, Hacking Team and Amesys reported to have been used to commit violations of human rights (Benedek, Kettemann, 2014).

Also it should be noted that these challenges are by no means restricted to the Middle East, indeed 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 (Citizen Lab, 2013). Moreover these technologies need to be seen in the context of a 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 (Silver, 2011).

There are also clear and evident regulatory failures in this process. 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 (Wagner, Guarnieri, 2014). Yet at the same time the spread across the world of these surveillance technologies has been a considerable challenge for many actors, as it is unclear what regulatory responses could be effective (Hosein, Palow, 2013). Thus authors such as

Wagner (2012) have proposed a variety of measures that might constitute effective responses to the problem, while also noting that none of these measures are likely to be fully effective but that all represent limited responses to a challenging problem.

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:

But what are surveillance technologies? While the understanding of surveillance technologies that can be used to harm human rights has developed over time to encompass the following technologies:

1) **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” (Hosein, Palow, 2013);
2) **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” (Bauman et al., 2914);
3) **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 (Maras, 2013).

Thus these definitions will be used in the following discussion when the types of surveillance and negative effects on human rights are discussed further.

2. Reactions from Experts: 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

2.1.1. 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.[2] The Wassenaar Arrange-

[2] For further details see: *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, http://www.wassenaar.org/participants/index.html.

ment 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." (Commission Delegated Regulation (EU) No 1382/2014, p. 132–133). These measures adopted by the Wassenaar Arrangement entered into force in the EU on 31 December 2014.

2.1.2 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."[3]

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.

2.2.1. EU Restrictive Measures

In reaction to media reports about European companies delivering surveillance technologies to Iran and Syria, the European Union reacted by updating existing sanctions to include embargo on telecommunications monitoring and interception equipment in 2012 (Council Decision 2012/168/CFSP) and 2013 (Council Decision 2013/255/CFSP) respectively. Moreover, the EU also prohibits export of equipment that might be used

[3] For further details see *Freedom Online Coalition: Statement on the Use and Export of Surveillance Technology*, Freedom Online Coalition, 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 internal repression as part of measures targeting Belarus, Cote d’Ivoire, Republic of Guinea, Libya, Myanmar (Burma), and Zimbabwe (*European Union Restrictive measures*).

2.2.2. 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 (Council Regulation (EC) No 428/2009). 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.” (Regulation (EU) No 599/2014) 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.

2.2.3 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”. The Communication published on 24 April 2014, explicitly discusses a regulation of “cybertools for mass surveillance, monitoring, tracking and interception.” (*The Review of export*, 2014, p. 3).

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” (*Commission updates*, 2014). The updates to the EU list entered into force on 31 December 2014 (Commission Delegated Regulation (EU) No 1382/2014).

2.2.4. 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 (European Parliament amendments) call-

ing 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)” (European Parliament amendments).

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” (*Freedom of expression*, point 17). Export controls were also discussed at a public hearing organized jointly by the Subcommittee on Human Rights and the Committee on International Trade (Joint Public Hearing).

2.2.5. 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 (Outcome of the Council Meeting). 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.

2.3. EU Member State 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 (Information Note). 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 (*The Export Control Order*, 2008).

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 (*Assessing Cyber*).

2.4. 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.[4] The paper states that members “have introduced due diligence programs, applied range of policies and processes, and integrated human rights into 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.

2.5. 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)[5] has played an important role by compiling and analysing available evidence and urging governments to take action.[6]

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 (FIDH, 2014). Yet, the impact of civil society actors is lim-

---

[4] For further details see: DIGITALEUROPE position paper on the review of export control policy in the EU Brussels, October 2014, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/droi/dv/412_digitaleurope_position_paper_/412_digitaleurope_position_paper_en.pdf.

[5] The CAUSE initiative includes Privacy International, Human Rights Watch, Amnesty International, Digitale Gesellschaft e.V., Open Technology Institute, FIDH and Reporters Without Borders.

[6] For further details see: Coalition Against Unlawful Surveillance Exports, http://www.globalcause.net for further details.

ited by lack of access to information about licenses requested and approved and the list of companies supplying surveillance technologies.

3. Analysing Existing Measures

There are numerous challenges and difficulties with existing implementations of export controls. This may perhaps stem from the fact that they stem from a historical attempt to regulate arms and limit the access of countries outside the west to advance technologies. As a result the way in which the system works presumes easily defined and categorised products. While there have been arguments that it is technically impossible to regulate software, most surveillance vendors on the market typically also sell training and software updates while also developing a long term relationship with their customers. This suggests that surveillance vendors are seldom one off transactions. Indeed many are in a strong position to know more about their clients and the nature of the their use of the tools as recent documents provided during the recent massive leak of documents by surveillance technology vendor Hacking Team suggest (Hern, 2015).

3.1. Transparency

However this does not mean on the flip side that export controls are the perfect solution for this problem. One of the greatest problems dealing with existing export control provisions is transparency. Many actors in this debate have suggested that more information is needed to ensure that existing and future measures are effective. They also argue that 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. This is particularly problematic as much of the publicly available information about the surveillance technology trade needed to be attained through FOIA requests and parliamentary questions. What little information is available is obtained through these ad-hoc means rather than stable and systematic information and documentation systems.[7]

This problem is not uncommon for export controls of dual-uset techonologies more generally, as transparency to the general public remands a key issue (Holtom et al., 2013; Bromley et al., 2012). This has led even the OECD to call for greater transparency of export controls in arguing that:

> “when a government is considering introducing an export restriction, it should publish sufficient information letting experts know about the initiative so that they can act upon the information. So that experts are in a position to adjust to change in

[7] For further details see: Kleine Anfrage der Abgeordneten Agnieszka Brugger, Dr. Konstantin von Notz, http://www.agnieszka-brugger.de/fileadmin/dateien/Dokumente/Abruestung/Ruestungsexporte/20140808_Antwort_KA_Spaehsoftware_Drs182067_1.pdf and Case No: CO/4089/2013 In the High Court of Justice Queen’s Bench Division Administrative Court, Royal Courts of Justice Strand, London, WC2A 2LL Date, 12/05/2014 18th and 19th March 2014, Approved Judgment, https://www.privacyinternational.org/sites/default/files/Privacy%20International_v_HMRC%20Judgment.pdf.

> policy, the government should publicise the planned action widely, give interested experts an opportunity to express their views and take such views into consideration. Following enactment of an export restriction, information should be published well in advance of its entry into force. The measure should be implemented and enforced in a transparent manner assuring all experts affected equal treatment and include a right to contest decisions and procedures” (Fliess, 2014).

Finally it should be noted that lack of transparency impedes independent research on the subject, accurate impact assessment of existing regulations and better public understanding of the issue. public institutions also need to be more supportive of systematic research into the subject by voluntarily sharing data about licences they grant and reject.

When looking at empirical reality it is evident that while some countries have taken steps to improve transparency, access to data about what licences were granted or rejected is limited. Also 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. Many are considering how to improve transparency and provide more information about licensing decisions to the public. To make matters even more puzzling the European Commission obtains considerable data about export licenses from the Member States, but cannot share it under current regulations. Last of all 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.

This is all happening under the backdrop of increasing private sector transparency. 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. Clearly 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. Accurately Defining Scope of Regulation

As mentioned above one of the main challenges and debates about defining the scope of export control regulations. This question is particularly hotly debated, as many actors argue that not all surveillance technologies require an authorisation under current export control regimes. 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. At the same there are some bright spots on the Horizon. It seems possible that the EU group 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.

At the same time swift and effective responses are particularly problematic as they can hurt legitimate actors. The potential regulation of Fuzzers[8] in the Wassenaar list, intended to control FinFisher trojans, has proved controversial among security researchers who are concerned it might hinder their work (Bratus, et al., 2014). These concerns are taken seriously by many governments and regulatory agencies, who emphasised their intention to implement existing and future controls in a manner that does not negatively affect security research. Yet questions still remain if these commitments are also backed up by law and the extent to which governments can be held to such commitments.

Another challenge that appears frequently relates to 'legacy' encryption controls that governments have kept on-going for decades with very few strong justifications. Mainly they argue that it allows them to be able to observe 'interesting' exports without actually being able to provide compelling evidence for their military or security relevance. This is particularly the case as encryption has become so common that its use is basically ubiquitous across almost all generic computing technologies. To try to regulate encryption is to try to regulate most computing. Despite this 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.

3.3. Policy Instruments in the EU

Another key aspect that needs to be analysed are the role of policy instruments in the EU. The EU has the ability to create a regulatory model that is effective and based on high human rights standard. The EU can also provide regulation that is a template for similar regulatory measures in third countries. In this context the current review process of export control regulation is an important process, albeit lengthy and slow.[9] Data collection and impact assessment are crucial, so maybe worth the wait: we need to get it right, so it is 'future-proof' (Rajan, 2009; Director, Levi, 1956). One of the main challenges with the Regulation is ensuring uniform implementation across Member States. Subsidiaries take advantage of lack of uniformity. It has also been suggested that the reviewed regulation will have a direct reference to human rights. Also, so it can be used as a model for non-EU countries.

At the same time it should also be noted that the EU also has other mechanisms to restrict access to products which could lead to negative human rights consequences, the most notable of which is the anti-torture regulation. Some parties have 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

---

[8] For further details see: Newly Controlled Items Under the Wassenaar Arrangement, http://dymaxion.org/essays/wa-items.html.

[9] For further details see: Public online consultation on the export control policy review (Regulation (EC) No 428/2009), http://trade.ec.europa.eu/consultations/index.cfm?consul_id=190.

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.

Conclusion

Export controls of surveillance technologies remain a heavily contested topic. Current debates about the issue suggest 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. Sadly there is at this point little agreement on which measures are most urgent and effective in implemented these concerns.

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 urgently necessary to ensure that communications networks fulfil their promise of upholding human rights.

Bibliography

Assessing Cyber Security Export Risks, http://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_ website_FINAL_3.pdf.

Bauman Z. et al. (2014), *After Snowden: Rethinking the Impact of Surveillance*, “International Political Sociology”, 8(2), pp. 121–144.

Benedek P. W., Kettemann D. M. C. (2014), *Freedom of expression and the Internet*, Council of Europe.

Bratus S., Capelis D. J., Locasto M., Shubina A. (2014), *Why Wassenaar Arrangement’s Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk–And How To Fix It*, October 9, 2014, www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf.

Bromley M., Cooper N., Holtom P. (2012), *The UN Arms Trade Treaty: arms export controls, the human security agenda and the lessons of history*, International Affairs.

Citizen Lab (2013), *You Only Click Twice: FinFisher’s Global Proliferation – Citizen Lab*.

Commission Delegated Regulation (EU) No 1382/2014 of 22 October 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*, Official Journal of the European Union, L 371 Volume 57, English edition, Legislation 30 December 2014.

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

Council Decision 2012/168/CFSP of 23 March 2012 *amending Decision 2011/235/CFSP concerning restrictive measures directed against certain persons and entities in view of the situation in*

Iran, http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:087:0085:0089:EN:PDF.

Council Decision 2013/255/CFSP of 31 May 2013 *concerning restrictive measures against Syria*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:147:0014:0045:EN:PDF.

Council Regulation (EC) No 428/2009 of 5 May 2009 *setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items*, http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF

Director A., Levi E. (1956), *Law and the future: Trade regulation*, Nw. UL Rev.

European Parliament amendments adopted on 5 April 2011 *to the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology* (COM(2008)0854 – C7-0062/2010 – 2008/0249(COD)), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference= P7-TA-2011-0125.

European Union Restrictive measures (sanctions) in force (Regulations based on Article 215 TFEU and Decisions adopted in the framework of the Common Foreign and Security Policy), http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf.

FIDH (2014), *Surveillance Technologies “Made in Europe”. Regulation Needed to Prevent Human Rights Abuses*.

Fliess B. (2014), *Transparency of Export Restrictions*.

Freedom of expression and assembly in Egypt, European Parliament resolution of 17 July 2014 *on freedom of expression and assembly in Egypt* (2014/2728(RSP)), P8_TA- PROV(2014)0007, http://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/provisoire/2014/07-17/P8_TA-PROV%282014%2907-17_EN.doc.

Gohdes A. R. (2015), *Pulling the plug: Network disruptions and violence in civil conflict*, “Journal of Peace Research”.

Hern A. (2015), *Hacking Team hacked: firm sold spying tools to repressive regimes*, documents claim, http://www.theguardian.com/technology/2015/jul/06/hacking-team- hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim, July 29, 2015.

Holtom P. et al. (2013), *Trends in international arms transfers, 2012*.

Hosein G., Palow C. (2013), *Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques*, Ohio St. LJ.

Information Note, Council Regulation (EC) No 428/2009 *setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items: Information on measures adopted by Member States in conformity with Articles 5, 6, 8, 9, 10, 17 and 22 2012/C 283/05*, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2012.283.01.0004.01.ENG.

Joint Public Hearing On Human rights and technologies: the impact of digital surveillance and intrusion systems on human rights in third countries, Subcommittee on Human Rights Committee on International Trade, Wednesday 21 January 2015, www.europarl.europa.eu/meetdocs/2014_2019/documents/inta/dv/hearingdigitalsurv_ prog_/hearingdigitalsurv_prog_en.pdf.

Maras M.-H. (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. B. J. Goold, D. Neylan, Routledge.

Outcome of the Council Meeting, 3348th Council meeting, Foreign Affairs, Trade, Brussels, 15792/14 (OR. en), Presse 598, PR CO 60 21 November 2014, www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/145922.pdf.

Rajan R., (2009), *Cycle-proof regulation*, “The Economist”.

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 ex-*

ports, transfer, brokering and transit of dual-use items, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0599&from=EN.

Silver V. (2011), *Spies Fail to Escape Spyware in $5 Billion Bazaar for Cyber Arms*, Bloomberg Business.

The Export Control Order 2008, http://www.legislation.gov.uk/uksi/2008/3231/schedule/3/made.

The Review of export control policy: ensuring security and competitiveness in a changing world, Communication from the Commission to the Council and the European Parliament, Brussels, 24.4.2014 COM(2014) 244 final, http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf.

Wagner B., Guarnieri C. (2014), *German Companies Are Selling Unlicensed Surveillance Technologies to Human Rights Violators – and Making Millions*, Global Voices.

Wagner B. (2012), *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy*, Brussels, Belgium.

Waleed K. (2011), *What was Iraq’s role in the export of banned US-made web watching gear to Syria? Niqash: briefings from inside and across Iraq*.

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, http://www.wassenaar.org/participants/index.html.

Kontrola eksportu technologii nadzoru w ujęciu pomiędzy stosunkami międzynarodowymi a kontrolą zbrojeń

Streszczenie

Kontrole eksportu stają się coraz ważniejszym wymiarem stosunków międzynarodowych. Stale jest jeszcze jednak stosunkowo mało literatury na temat ich wykorzystania i wdrażania. Niniejszy artykuł jest próbą ukazania rozwoju i problemów związanych z kontrolą eksportu w nowym obszarze: technologiach nadzoru, które niedawno zostały włączone do struktur międzynarodowych w zakresie kontroli eksportu, przynosząc ze sobą szereg wyzwań i pytań dla decydentów. Na podstawie przeprowadzonych rozmów z praktykami i kluczowymi ekspertami w tej dziedzinie autorzy artykułu próbują nakreślić najważniejsze pomysły i rozwiązania w tym obszarze, jak również istotne odpowiedzi, które zostały opracowane w kontekście (dostrzegalnych) wyzwań.

Słowa kluczowe: kontrola eksportu, technologia nadzoru, stosunki międzynarodowe, global governance

Article submitted: August 10, 2015; accepted: August 27, 2015