ICT Surveillance Systems: Trade Policy and the Application of Human Security Concerns

MARK BROMLEY, KEES JAN STEENHOEK, SIMONE HALINK AND EVELIEN WIJKSTRA[1]

Abstract

In recent years, sections of the European Union (EU), EU Member States, non-government organizations (NGOs) and Members of European Parliament (MEPs) have sought to use dual-use export controls to restrict exports of Information Communication Technology (ICT) surveillance systems. This process was driven by revelations in 2011 about the role of EU-based companies in the supply of security, surveillance and censorship technologies and services to states in the Middle East and North Africa and their use in violations of human rights. In response, the Wassenaar Arrangement and the EU have expanded controls on exports of dual-use goods to capture certain ICT surveillance systems and is discussing the adoption of additional measures as part of the ongoing review of the Dual-Use Regulation. This has included discussion about the application of export licensing criteria based on 'human security' considerations in order to better capture the range of concerns raised by the export of these technologies. This article explores the motivations behind these actions, the impact they have had to date, and the ongoing discussion about the adoption of additional measures. It concludes by arguing in favour of a holistic approach which combines export controls with other areas of trade policy, particularly improved standards in corporate social responsibility (CSR). This approach carries the greatest chance for success in restricting the supply of ICT-surveillance systems in situations where they are likely to be used in human rights violations.

Keywords

ICT surveillance systems, human rights, export controls, corporate social responsibility, holistic approach.

Introduction

In recent years, many cases showed that repressive regimes used Information Communication Technology (ICT) surveillance systems to identify and intimidate dissidents and in the commission of other violations of

[1] Mark Bromley is Co-Director of the Dual-Use and Arms Trade Control Programme at the Stockholm International Peace Research Institute (SIPRI) and PhD candidate at the Department of Economic History, Stockholm University; Kees Jan Steenhoek acted as head of the dual-use export control division until July 2015 and is currently deputy head of the nonproliferation and disarmament division, both at the Netherlands Ministry of Foreign Affairs; Simone Halink is Deputy Head of International Cyber Policies at the Netherlands Ministry of Foreign Affairs; Evelien Wijkstra is senior policy officer at the Taskforce International Cyber Policies at the Netherlands Ministry of Foreign Affairs.

international human rights law.[2] These systems have greatly enhanced the surveillance capacities of these regimes allowing them to target people in ways and on a scale not previously possible. Instead of citizens having technology on their side, advanced digital technology has been turned into a tool for surveillance.[3]

Subsequent investigations by NGOs and media organisations have shown that many of the ICT surveillance systems used by these regimes were supplied by companies based in Europe and North America. Prior to 2011, certain ICT surveillance systems were covered by dual-use export controls due to the level of encryption they employed.[4] However, in many instances, existing export controls did not apply. This led to calls from NGOs and Parliamentarians for export controls to be expanded in order to apply greater restrictions on the supply of ICT surveillance systems.

The most coordinated campaign in this regard is the Coalition Against Unlawful Surveillance Exports (CAUSE) which was set up by several leading NGOs.[5] CAUSE called for an effective export control policy to prevent human rights violations by developing regulations requiring export control authorities to take into account human rights implications when making licensing decisions. Other measures promoted by CAUSE include subjecting all relevant ICT surveillance systems to licensing, addressing disparities between national policies, and for security researchers, industry and civil society to be involved in policy processes regarding this issue.[6] In addition, civil society actors have advocated for more transparency from governments about licenses granted and denied in order to develop a clearer overview of relevant actors involved.

In 2012 and 2013, some of these export control gaps were closed through the addition of new categories in the Wassenaar Arrangement's dual-use control list. In particular, 'mobile telecommunications interception or jamming equipment', 'Internet Protocol (IP) network surveillance systems' and 'intrusion software' were added to the Wassenaar Arrangement's dual-use control list.[7] However, NGOs, Parliamentarians and national governments have argued that gaps continue to exist and that a wide range of ICT surveillance systems remain outside the scope of export controls.[8] They have also argued that the issue is not only about

[2] E.g. an Iranian women's rights activist turned to using pay phones when she found out that all her communications were under watch. On her way to meetings with other activists she would be called by police who would tell her they knew where she was headed. Interrogators at Tehran's notorious Evin Prison asked Shojaee about her acquaintances and displayed call records and transcripts going back several months. Ben Elginvand, Vernon Silver, and Alan Katz, "Iranian Police Seizing Dissidents Get Aid Of Western Companies," *Bloomberg Business*, October 31, 2011, <http://www.bloomberg.com/news/articles/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies>. For another example from Libya, see FIDH, "Surveillance Technologies Made in Europe: Regulation Needed to Prevent Human Rights Abuses," Position Paper Presented through FIDH Website, December 2014, <http://fr.scribd.com/doc/251396002/Surveillance-Technologies-Made-in-Europe> .

[3] James Bamford, "The Espionage Economy," *Foreign Policy* (Jan/Feb 2016), pp. 70-72.

[4] The range of activities that states seek to control through national licensing procedures has been expanded beyond exports to include brokering, transit, trans-shipment. Following existing practice within the EU and among EU member states, the terms 'export control' is used here in the broader sense as refering to controls on exports and these other related activities.

[5] CAUSE is made up of the following NGOs: Amnesty International, Digitale Gesellschaft, FIDH, Human Rights Watch, Open Technology Institute, Privacy International, Reporters Without Borders and Access, <http://www.globalcause.net/>.

[6] Coalition Against Unlawful Surveillance (CAUSE), "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

[7] Sibylle Bauer et al., "Dual-use and Arms Trade Controls," *SIPRI Yearbook* (Oxford: Oxford University Press, 2013); and Sibylle Bauer et al., "Dual-use and Arms Trade Controls," *SIPRI Yearbook* (Oxford: Oxford University Press, 2014). The Wassenaar Arrangement seeks to prevent 'destabilizing accumulations' by states of conventional arms and related dual-use goods and technologies and to prevent the acquisition of such items by terrorist groups, organizations and individuals. See <www.wassenaar.org/>.

[8] See Coalition Against Unlawful Surveillance (CAUSE), "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>, European Parliament, "Resolution on 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries," September 8, 2015, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0288+0+DOC+XML+V0//EN>, and Catherine Strupp, "Germany Leaves Brussels Behind on

the items that are subject to control, but also the mechanisms through which controls are exercised. In particular, they have argued that states need to develop better criteria for assessing licences for the export of ICT surveillance systems.[9]

Discussions about additional control list categories have taken place within the Wassenaar Arrangement and the EU. However, discussions about the development of improved criteria for assessing export licences have exclusively taken place at the EU-level. Since 2011, the EU has made a number of commitments to restrict exports of ICT surveillance systems that might be used in human rights violations.[10] A range of different policy options have been discussed, including developing improved guidelines for supplier companies and providing dissidents with technologies that would enable them to evade detection. However, most of the concrete steps and substantive discussions have focused on the use of export controls.

In 2011 and 2012, the EU added a broad range of ICT surveillance to its sanctions on Iran and Syria. The main focus of debate since has been about how the EU Dual-Use Regulation can be used as a means of further expanding controls on transfers of ICT surveillance systems. The EU Dual-Use Regulation is currently undergoing a review and the issue of expanding controls on ICT surveillance systems has become a central part of the process.[11] In November 2014 Cecilia Malmström, the EU Commissioner for Trade, stated that 'the export of surveillance technologies is an element—and a very important element—of our export control policy review.'[12]

As part of the review process, the Commission is examining the possibility of controlling ICT surveillance systems that are not included in the Wassenaar Arrangement's controls list. The EU maintains its own list of dual-use goods and in the 2014 update, Wassenaar Arrangement control list categories in the field of ICT surveillance systems were added. As of now, the EU list is drawn exclusively from the Wassenaar Arrangement and other multilateral control regimes. The EU is also discussing the development of new criteria for assessing exports of ICT surveillance technologies, including the possible application of concepts from the human security field.

A number of commentators have argued that the application of export controls to the field of ICT surveillance systems is at best insufficient and at worst counter-productive. In particular, they have argued that the expansion of controls in this area risks creating unnecessary regulatory burden for the ICT sector, particularly for companies and individuals working in the field of IT security.[13] Others have argued that more work needs to be devoted to exploring other mechanisms besides export controls through which the supply of ICT surveillance systems can be regulated. This includes the application of other tools in the field of trade controls, particularly the development and implementation of improved standards in Corporate Social Responsibility (CSR).[14]

Surveillance Tech Export Controls," Euractiv.Com, July 10, 2015, <http://www.euractiv.com/section/digital/news/germany-leaves-brussels-behind-on-surveillance-tech-export-controls/>.

[9] Ibid.

[10] Council of the European Union, "EU Strategic Framework and Action Plan on Human Rights and Democracy," June 25, 2012, <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/131181.pdf> and Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline," May 12, 2014, < http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf>.

[11] "Joint statement by the European Parliament, the Council and the Commission on the Review of the Dual-use Export Control System," April 16, 2014, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.173.01.0079.01.ENG&toc=OJ:L:2014:173:TOC>.

[12] Malmström, Cecilia, EU Commissioner for Trade, "Debate at European Parliament in Strasbourg," November 24, 2014, <http://www. europarl.europa.eu/sides/getDoc.do?pubRef=-//ep//text+cre+20141124+item-018+doc+xml+v0//en>.

[13] Joe Uchill, "Industry Warns Proposed Arms Export Rule Will Thwart Basic Cyberdefenses," *Christian Science Monito*r, June 26, 2015, <http://www.csmonitor.com/World/Passcode/2015/0626/Industry-warns-proposed-arms-export-rule-will-thwart-basic-cyberdefenses>; and Dennis Fisher, "Coalition of Security Companies Forms to Oppose Wassenaar Rules," *Threat Post*, n.d., <https://threatpost.com/coalition-of-security-companies-forms-to-oppose-wassenaar-rules/113794>.

[14] See Centre for Internet and Human Rights (CIHR), "Export Controls of Surveillance Technologies," 2015, <https://www.

During the Global Conference on CyberSpace (GCCS 2015) on the 16th and 17th of April 2015 in The Hague, one session brought together experts in the field of ICT surveillance systems from the European Parliament, the European Commission, NGO's, the OECD and national governments.[15] The panellists compared notes on latest policy developments and agreed that unlawful interception and subsequent human rights infringements are 'a problem worth solving'. They highlighted several options for improvement of export control policy from different angles, ranging from the provision of more transparency by States about licenses granted and denied, to creating more awareness about the issue and the need for smart regulation. The panel concluded that a flexible, effective and comprehensive solution could be found through a balanced approach, which might include a list-based regime, end-user controls and vendor due diligence (as required, for example, by the OECD Guidelines for Multinational Enterprises and the UN Guiding Principles on Business and Human Rights).[16]

This article presents an overview of recent debates about the use of both export controls and CSR standards in order to exert greater control over exports of ICT surveillance systems Section II presents an overview of the range of ICT surveillance systems that have been the subject of debate because of their use in alleged human rights violations and highlights the factors that speak for and against the application of export controls as a means of exerting control on their use. Sections III and IV discuss the way in which existing export controls apply to these systems, how these powers have expanded in recent years, and debates about widening them further, looking at developments at both the Wassenaar Arrangement and EU level. In particular, Section III focuses on debates about expansions in the range of ICT surveillance systems that should be subject to control while Section IV focuses on debates about the criteria states should use when assessing licences for their export. Section V highlights the important role that other tools in field of trade controls can play in controlling transfers of ICT surveillance systems, particularly improved standards in CSR. It lays out the range of existing CSR mechanisms that already exist and the gaps and challenges that remain. Section VI presents conclusions, arguing that export controls and improved standards in CSR are both necessary elements of an effective policy response to the challenges posed by the export and use of ICT surveillance systems.

ICT Surveillance Systems: Different Risks, Different Challenges

The debate about controls on exports of ICT surveillance systems encompasses a wide range of systems and technologies. Its boundaries and sub-categories are often unclear and subject to different views and interpretations. In particular, it is difficult to clearly mark the technological boundaries of the various technologies. Not only because it is a rapidly developing field, but also because it's not always possible to define when the items are "used" and when they are "abused".

This article defines 'ICT surveillance systems' as systems that enable the monitoring and exploitation of data or content that is stored, processed or transferred via ICTs, including computers, mobiles phones and telecommunications networks. It pays particular attention to systems that were subject to export controls prior to 2011, that have since become subject to export controls, or have been the subject of debate in this area. This includes, but is not limited to: mobile telecommunications interception equipment; intrusion software; IP network surveillance systems; monitoring centres; lawful interception (LI) systems; data retention systems; digital forensics; probes; and deep packet inspection (DPI) (see box 1).

gccs2015.com/sites/default/files/documents/Export%20Controls%20of%20Surveillance%20Technologies_DEF_BW.pdf>.

[15] Global Conference on Cyberspace 2015 programme (link also directs to a video registration of the panel discussion and a background document): <https://www.gccs2015.com/programme?programme=2>.

[16] Global Conference on Cyberspace 2015, "Chair's Statement," April 2015, <https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf>.

Box 1 – Different Types of ICT Surveillance Systems

Mobile telecommunications interception equipment – Also known as 'IMSI Catchers,' mobile telecommunications interception equipment are used to remotely track, identify, intercept and record mobiles phones.

Intrusion software – A type of malware that can be inserted on computers and mobile phones without detection and used to remotely monitor and in certain cases control them.[17]

IP Network Surveillance - Used to intercept, collect and, some cases analyse data as it passes through an Internet Protocol (IP) network.

Monitoring centres – Monitoring centres are used by law enforcement and intelligence agencies to collect, store and analyse difference forms of communications data from various surveillance sources.[18]

Lawful Interception (LI) systems – Used by network operators to enable them to comply with requests from law enforcement or intelligence agencies for the provision of their users' communications data.[19]

Data retention systems - Used by network operators to comply with legal requirement for 'meta data' storage of their users for potential later use by law enforcement or intelligence agencies.

Digital forensics – Enable law enforcement or intelligence agencies to retrieve and analyse data stored on networks, computers and mobile devices.[20]

Probes – Used to collect data as it passes through a communications network.[21] They are used in several ICT surveillance systems but also have a range of non-surveillance applications.

Deep Packet Inspection (DPI) – Used to examine the content of data as it passes through a communications network.[22] They are used in several ICT surveillance systems but also have a range of non-surveillance applications.

A 'network operator' is a company that manages a communications network, such as Vodafone or TeliaSonera. 'Communications data' can be: (a) 'meta data,' meaning information about the use of a network or the calls that a subscriber has made; (b) 'content data,' meaning what is said in a phone call or the content of a text

[17] "The Little Black Book of Electronic Surveillance: 2015," *Insider Surveillance*, January 30, 2015, < https://insidersurveillance.com/the-little-black-book-of-electronic-surveillance-2015/>.

[18] Edin Omanovic and Matthew Rice, "Monitoring Centers: Force Multiplier From the Surveillance Industry," Privacy International, April 29, 2014, <https://www.privacyinternational.org/?q=node/439>.

[19] See Frost and Sullivan, "Lawful Interception: A Mounting Challenge for Service Providers and Governments," 2011, < https://www.wikileaks.org/spyfiles/docs/FROSTSULLIVAN-LawfInteA-en.pdf>; and Vodaphone, "Law Enforcement Disclosure Report," February 2015, <http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html>.

[20] UK Government, "Assessing Cyber Security Export Risks," TeckUK, 2014, p. 15, <https://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf>.

[21] Passive probes collect data indiscriminately as it moves through the communications network. Actives probes collect data from specific individuals using their identifiers (e.g. IP address) or based on specific signatures (e.g. specific semantic content). See "Catalyst 6500 Series Switches Lawful Intercept Configuration Guide," CISCO, August 2007, <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/lawful/intercept/book.pdf>.

[22] Duncan Geere, "How Deep Packet Inspection Works," *Wired*, April 27, 2012, <http://www.wired.co.uk/news/archive/2012-04/27/how-deep-packet-inspection-works>.

message; or (c) 'location data,' meaning information about the movements of a subscriber to a mobile phone network.

ICT surveillance systems differ significantly in many ways. These differences include the type, size and location of the companies engaged in their production. Some of the producers are large defence contractors such as Thales and BAE Systems that produce a range of ICT surveillance systems for law enforcement and intelligence agencies as part of a broad portfolio of defence and security products and solutions. Others are large ICT companies, particularly Nokia and Ericsson, that produce telecommunications networks and are legally required to have LI systems 'built in' to their products or to enable their inclusion.

Other companies are smaller ICT firms such as Gamma International and Hacking Team that specialize exclusively in the production of certain types of surveillance technologies, such as IMSI catchers or intrusion software.

There are also differences with regards to the types of human rights abuses that have been connected to the use of different ICT surveillance systems and the nature of that connection. In certain cases, the connection is fairly direct. For example, by analysing the content of malware found on the target's computer, Citizen Lab have shown how Hacking Team intrusion software has been used by the UAE authorities to monitor the communications of a human rights activist.[23] Moreover, documents found in the Libyan intelligence files following the overthrow of Colonel Gadaffi show that, prior to 2012, the Libyan authorities used Amesys' Eagle IP Network Surveillance system to monitor phone and email conversations of government opponents on a 'massive scale.'[24]

In other cases, a clear connection between a particular ICT surveillance system and abuses of human rights is less clear or harder to establish. For example, digital forensics systems can potentially be used by law enforcement agencies to recover personal data from individuals who are under investigation for political reasons.[25] However, there are no clearly documented cases where this has happened. Meanwhile, certain ICT surveillance systems raise both human rights and security concerns. For example, IMSI catchers and intrusion software can be used in the theft of commercial and government secrets.[26]

Certain aspects of the production and supply of ICT surveillance systems make them a suitable target for export controls. For instance, ICT surveillance systems, particularly intrusion software, require regular software updates in order to remain undetected and to function effectively, meaning that they can be effectively 'switched off' by the supplier.[27] Moreover, existing regulations mean that many ICT surveillance systems are sold exclusively to national governments, making it possible to target end-user based controls effectively.[28]

At the same time, there is a significant level of internationalization in the industry, which creates challenges for nationally implemented, list-based export control systems. Many of the companies involved maintain

[23] Citizen Lab, "Backdoors are Forever: Hacking Team and the Targeting of Dissent?," October 10, 2012, <https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/>.

[24] Mattieu Aikins, "Jamming Tripoli, Inside Moammar Gadhafi's Secret Surveillance Network," *Wired*, May 18 2012, <http://www.wired.com/2012/05/ff_libya/all/>.

[25] Ibid.

[26] Jeff, Stein, "New Eavesdropping Equipment Sucks All Data Off Your Phone," *Newsweek*, June 22, 2014, <http://www.newsweek.com/2014/07/04/your-phone-just-got-sucked-255790.html> and James Clapper, Director of National Intelligence, "Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence," US Government, March 23, 2013.

[27] Kenneth Page, "Six Things We Know from the Latest FinFisher Documents," Privacy International, August 15, 2014, <https://www.privacyinternational.org/?q=node/371>.

[28] Privacy International, "Privacy International BIS Submission," [N/D], <https://www.privacyinternational.org/sites/default/files/Privacy%20International%20BIS%20submission.pdf>.

offices in different countries, including ones that are inside and outside of the Wassenaar Arrangement, and can move production from one country to the other.[29] In addition, many of the technologies involved have legitimate non-surveillance applications, meaning that there is significant potential for creating unintended consequences for other parts of the ICT sector. Probes and DPI systems have a wide range of non-surveillance applications, including in quality of service, network diagnostics and IT security.[30]

There is also significant overlap between the techniques used in certain areas of ICT surveillance and IT security, which risks unintended consequences when crafting list-based control systems. For example, there are concerns that the attempts to place controls on intrusion software have inadvertently captured, and will have a chilling effect upon, the processes of 'responsible disclosure' through which software vulnerabilities are identified and reported. Finally, many of the ICT surveillance systems states use are composites of several different sub-systems provided by different suppliers.[31] Concerns have been raised that the controls created on IP surveillance systems could be effectively bypassed by sourcing different elements of the system from different vendors and assembling it in the recipient country.[32]

Export Controls: Expansions in Coverage

To date, debate on how to restrict transfers of ICT surveillance systems through the application of export controls has centered on two sets of issues. First, there has been a debate about which systems and technologies should be made subject to controls. This debate has taken place at the Wassenaar Arrangement and the EU levels and within different national capitals in Europe and North America. It has focused on where and how controls should be implemented and the best way to avoid generating unintended consequences for the IT security sector and the telecommunications industry. Second, there has been a debate about what standards national export licensing authorities should use when assessing licences for the export of ICT surveillance systems. This debate has largely been confined to the EU level and has focused on the application of existing human rights standards and the potential development of new standards based around notions of 'human security.' Both debates are ongoing and in some cases expand to involve other issue areas.

Certain ICT surveillance systems were already covered by export controls prior to 2011. For example, exports of IMSI Catchers were controlled by certain states on the grounds that they were covered by '5A001 - Telecommunications systems, equipment, components' or '5D002 - Software', while exports of certain types of intrusion software and digital forensics were covered by '5A002 - Cryptography'.[33] However, these controls were largely indirect in nature and not intentionally targeted on ICT surveillance systems. In late 2011 and early 2012, the EU arms embargoes on Iran and Syria were updated to include prohibitions on the sale of ICT surveillance systems.[34] The language used in both cases was broad in scope, covering any

[29] Henry Habegger, "Bund Verscheucht Hersteller von Spionagesoftware Aus Der Schweiz [Bund Chases manufacturer of spy software from Switzerland]," *Schweiz Am Sonntag*, August 1, 2015, <http://www.schweizamsonntag.ch/ressort/politik/bund_verscheucht_hersteller_von_spionagesoftware_aus_der_schweiz/>.

[30] Hewlett Packard manufactures several types of probes and DPI systems that can be used for both surveillance and non-surveillance purposes. "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," Coalition Against Unlawful Surveillance (CAUSE), June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

[31] Collin, Anderson, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies," *Access*, March 13, 2015, <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

[32] Adam Weber, et al, "IP Network Communications Surveillance Systems: Deciphering Wassenaar Arrangement Controls," *World ECR*, April 2015.

[33] Privacy International, "British Government Admits it has Already Started Controlling Exports of Gamma International's FinSpy," September 9, 2012, <https://www.privacyinternational.org/news/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma>.

[34] Council of the European Union, "Council Decision 2011/782/CFSP of 1 December 2011 Concerning Restrictive Measures against Syria and Repealing Decision 2011/273/CFSP," Official Journal of the European Union, December 2, 2011; Council of the European Union, "Council Decision 2012/168/CFSP of 23 March 2012 Amending Decision 2011/235/CFSP Concerning

‘equipment or software intended primarily for use in the monitoring or interception […] of the Internet and of telephone communications on mobile or fixed networks,’ as well as associated services.[35] The sanctions cover the export of a wide range of ICT surveillance systems but have also had implications for the supply of telecommunications networks and services from EU-based companies. Since their implementation, Ericsson and Nokia have reduced sales of communications networks to Iran.[36]

In 2012 and 2013 certain types of ‘mobile telecommunications interception or jamming equipment,’ ‘IP network surveillance systems’ and ‘intrusion software’ were added to the Wassenaar Arrangement’s dual-use control list. In all cases, these additions were justified, at least in part, on the national security concerns associated with their use. For example, the controls on intrusion software were justified on the grounds that they ‘may be detrimental to international and regional security and stability.’[37] In December 2014, these items were added to the EU’s Dual-Use control list. In 2015, Germany imposed national controls on the export of certain types of data retention systems and monitoring centres and is seeking to promote their adoption at the EU and Wassenaar Arrangement.[38]

Since 2014, an ongoing discussion has taken place within both the EU and the Wassenaar Arrangement about if and how additional ICT surveillance systems should be made subject to dual-use export controls. In particular, a number of Members of European Parliament (MEPs) and NGOs have called for existing controls to be expanded and additional ICT surveillance systems to be included.[39] One EU-level option under discussion is the adoption of a dedicated ‘catch-all’ control for exports of unlisted ICT surveillance systems that might play a role in human rights abuses. The proposal for such a control was made by the European Parliament in October 2012 but was not adopted.[40] At the time, the Council Working Group on Dual-use Goods - the EU level body where EU Member States discuss the legal and political aspects of Dual-use export controls through the Dual-use Regulation - was of the opinion that the new procedures for amending the control lists should be implemented as quickly as possible. Some delegations were concerned that a policy debate on substantive matters would postpone European implementation of the changes to the control lists agreed in the export control regimes in 2010 and 2011.[41]

Making further expansions in the range of ICT surveillance systems that are subject to control is likely to involve focusing on systems that are mainly of interest because of their human rights concerns, given that most of the systems that have been made subject to control on national security grounds are already covered. This is likely to be more achievable at the EU rather than at the Wassenaar Arrangement level.

Restrictive Measures Directed against Certain Persons and Entities in View of the Situation in Iran,” Official Journal of the European Union, March 25, 2012, p. 85.

[35] Ibid.

[36] Steve Stecklow, “Special Report: Chinese Firm Helps Iran Spy on Citizens,” *Reuters*, March 22, 2012, <http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322>.

[37] Wassenaar Arrangement, “Public Statement 2013. Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies,” December 4, 2013, <http://www.wassenaar.org/publicdocuments/index_PS_PS.html/>.

[38] BMWI, “Anlage AL zur Außenwirtschaftverordnung [Annex AL to the German Foreign Trade Regulations],” July 2015, <http://www.bmwi.de/BMWi/Redaktion/PDF/A/anlage-al-zur-aussenwirtschaftsverordnung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf>.

[39] Coalition Against Unlawful Surveillance (CAUSE), “A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation,” June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

[40] European Parliament, «Legislative Resolution on the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) no. 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, (COM(2011)0704 – C7-0395/2011 – 2011/0310(COD)), October 23, 2012.

[41] Tweede Kamer, vergaderjaar 2012–2013, 33 400 V, nr. 152 [Proceedings of Dutch Parliament, 33 400 V: approval of the budget of the Ministry of Foreign Affairs (V) and the budget for Foreign Trade and Development Cooperation for the year 2013, no. 152: letter from the Minister for Foreign Trade and Development Cooperation.], <https://zoek.officielebekendmakingen.nl/kst-33400-V-152.html>.

Adding technologies to the Wassenaar Arrangement list on purely human rights grounds would likely be opposed by other participating states, and all list additions have to be made by consensus. However, adopting EU-level controls on items that are not included in the control lists of the various multilateral export controls regimes is something that industry and EU member states seek to avoid. This is due both to the impact it might have on the competitiveness of EU-based companies and the confusion it may generate for non-EU states who value the EU dual-use control list as a synthesis of the multilateral regime's control lists and implement it nationally.

The expansion of controls on ICT surveillance systems has generated concerns about unintended side-effects. This has been particularly apparent in relation to the controls on 'intrusion software' adopted by the Wassenaar Arrangement in 2013.[42] Specifically, significant concerns have been raised about the impact of the controls on intrusion software on 'vulnerability coordination' or 'vulnerability disclosure', the process by which individuals or organizations make ICT companies aware of software vulnerabilities and exploits. A number of papers have argued that the control list language effectively describes a software exploit and thereby makes the process of identifying and reporting them subject to control.[43] A number of articles have argued that the controls, if properly applied, should not have an effect in these areas.[44] Guidance language released by the UK government , who originally proposed the control language at the Wassenaar Arrangement, has also sought to make this point.[45]

However, concerns have persisted, fed largely by the US Bureau of Industry and Security (BIS) language on its proposed national implementation of the intrusion software controls, published in May 2015.[46] The language included a number of phrases that alarmed academics and individuals working in IT security, implying, in particular, that vulnerability disclosures would be covered by the controls.[47] The debate in the United States has since grown particularly heated. A coalition of IT security companies and researchers have successfully delayed the US adoption of the intrusion software controls and sought to press the US government to propose revisions to the control list language at the Wassenaar Arrangement.[48]

Regardless of whether the concerns raised in relation to the intrusion software controls are justified, they highlight the need for clarity when drafting control list language and the potential risks when export controls are expanded into a new areas and engage with communities that do not have experience of being subject to their coverage.

Export Controls: New Criteria and the EU Dual-Use Regulation

Much of the debate about how to assess licences for the export of ICT surveillance systems has been confined to the EU. Under the EU Dual-Use regulation, member states already have an obligation to take

[42] Uchill, Joe, "Industry Warns Proposed Arms Export Rule Will Thwart Basic Cyberdefenses," *Christian Science Monitor*, June 26, 2015, <http://www.csmonitor.com/World/Passcode/2015/0626/Industry-warns-proposed-arms-export-rule-will-thwart-basic-cyberdefenses>.

[43] Sergey Bratus, D.J. Capelis, Michael Locasto, and Anna Shubina, "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, <http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf>.

[44] See Collin Anderson, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies," *Access*, March 13, 2015, <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

[45] UK Department for Business Innovation & Skills, "Intrusion Software Tools and Export Control," August 10, 2015, <http://blogs.bis.gov.uk/exportcontrol/uncategorized/eco-issues-guidance-on-intrusion-software-controls/>.

[46] Uchill, Joe, "Industry Warns Proposed Arms Export Rule Will Thwart Basic Cyberdefenses," *Christian Science Monitor*, June 26, 2015, <http://www.csmonitor.com/World/Passcode/2015/0626/Industry-warns-proposed-arms-export-rule-will-thwart-basic-cyberdefenses> and Dennis Fisher, "Coalition of Security Companies Forms to Oppose Wassenaar Rules," *Threat Post*, n.d., <https://threatpost.com/coalition-of-security-companies-forms-to-oppose-wassenaar-rules/113794>.

[47] For example, see "Google, the Wassenaar Arrangement, and Vulnerability Research," Google Online Security Blog, July 20, 2015, <http://googleonlinesecurity.blogspot.se/2015/07/google-wassenaar-arrangement-and.html>.

[48] Kevin Carty, "Lawmakers Assail Cybersecurity Provisions in International Treaty," *Morning Consult*, January 12, 2016, <https://morningconsult.com/alert/lawmakers-assail-cybersecurity-provisions-in-international-treaty/>.

into account human rights considerations when considering exports of certain ICT surveillance systems.

For example, the EU general export authorisation (GEA) for telecommunications equipment (EU 005) allows the export of a range of dual-use items covered under category 5 of the control list to nine countries, including China, Russia and Turkey. This authorisation cannot be used if the exporter has been told by the licensing authority or is otherwise aware that the export will be used ‘in connection with a violation of human rights, democratic principles or freedom of speech’ through the use of ‘interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of Internet use.’[49]

More broadly, Article 12 of the EU Dual-use Regulation requires member states to take into account ‘all relevant considerations’ when assessing export and brokering licences for dual-use goods, including those covered by Council Common Position 2008/944/CFSP defining common rules governing control of exports of military technology and equipment (EU Common Position).[50] The Council Common Position lays down eight criteria that EU Member States should apply when assessing license applications for the exports of conventional arms. Many of the human rights and security concerns associated with the export and use of ICT surveillance systems are addressed in the eight criteria of the EU Common Position and the accompanying User’s Guide which provides guidance on how the Common Position should be implemented.[51]

In particular, criterion 2 of the Common Position requires member states to deny an export licence if there is a ‘clear risk’ that the goods ‘might be used ‘for internal repression’ or ‘in the commission of serious violations of international humanitarian law.’[52] The guidelines for criterion 2 in the User’s Guide note that ‘communications/surveillance equipment can have a strong role in facilitating repression.’[53] Meanwhile, criterion 5 requires member states to take into account the impact of the potential export on their own and other member states’ defence and security interests.[54] A number of EU Member States have denied licences for the export of ICT surveillance systems on human rights grounds. For example, in 2009 it was reported that the UK denied a licence for the export of IMSI Catchers to a country in the Asia Pacific region because of the risk that the goods would be used to commit human rights abuses.[55]

However, other human rights concerns relating to the export and use of ICT surveillance systems are not referenced in the EU Common Position. For example, potential threats to the right to privacy and freedom of expression are not mentioned. Also not mentioned is the need for recipient states to have effective regulatory and oversight mechanisms that regulate the performance of investigative and surveillance duties and the powers of law enforcement and intelligence agencies and their use of ICT surveillance systems. There are also no references to the specific security threats associated with the use of ICT surveillance systems, such as the theft of government and commercial information and attacks on critical infrastructure.

[49] Regulation (EU) No. 1232/2011 of the European Parliament and of the Council of 16 November 2011 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, 8 December 2011, pp. 37-38.

[50] Council of the European Union, “User’s Guide to Council Common Position 2008/944/CFSP Defining Common Rules Governing the Control of Exports of Military Technology and Equipment,” Brussels, April 29, 2009, <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209241%202009%20INIT>.

[51] Ibid.

[52] Council of the European Union, Council Common Position 2008/944/CFSP of 8 Dec. 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment, Official Journal of the European Union, L335.

[53] Council of the European Union, User’s Guide to Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment., Brussels, 20 July 2015, p. 38.

[54] Council of the European Union, Council Common Position 2008/944/CFSP of 8 Dec. 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment, Official Journal of the European Union, L335.

[55] Matthew Rice, “Collaborating Companies: Shady Moves in a Secretive Sector,” Privacy International, May 27, 2015, <https://www.privacyinternational.org/node/587>.

The European Commission has raised the prospect of filling this gap by applying a 'human security approach' to exports of dual-use goods. This forms one of a range of potential policy proposals that the Commission is considering proposing in order to expand the application of export controls on ICT surveillance systems within the context of the ongoing review of the Dual-Use Regulation. The European Commission has announced that it will put forward proposed amendments to the Dual-Use Regulation in the first half of 2016. This legislative step is the last in a series that started with the publication of the Green Paper on dual-use exports in 2011.[56]

It is widely expected that the proposals will include measures aimed at preventing the misuse of European cyber systems for human rights infringements as various communications of the European Commission, the European Parliament and the Council have flagged the importance of addressing this issue. Upon amending the Dual-Use Regulation on 16 April 2014 to accelerate the procedure to update the list of dual-use items, the European Parliament, the Council and the Commission jointly acknowledged that the export of certain ICT systems can be used in connection with human rights violations and have the potential to undermine the EU's security. They also noted that options would be explored to address this issue in the context of the ongoing review of EU dual-use export control policy.

On 24 April 2014, the European Commission published a communication on the export control policy review. It laid out a range of 'concrete policy options' for the review with regards to export controls of ICT surveillance systems, such as adopting an EU-level control list, adopting an EU-level catch-all mechanism, making joint proposals for additions to the Wassenaar Arrangement control list, and developing new export assessment criteria. The communication also included potentially evolving towards a 'human security' approach to take into account broader security implications, including human rights violations.[57]

Under the Italian Presidency in the second half of 2014, the Council adopted conclusions that reconfirmed the April 2014 statement.[58] On 8 September 2015, the European Parliament adopted a non-binding resolution urging the Commission to put forward a proposal to regulate the export of dual-use technologies, addressing potentially harmful exports of ICT products and services to third countries.[59]

The next stage in the review of the Dual-Use Regulation will arrive in early 2016 when the Commission presents an impact assessment. This will be followed by a legislative proposal. As part of its preparation for the impact assessment, the Commission funded the production of a data collection project, conducted by SIPRI and ECORYS, to examine the current and potential economic, social and security costs and benefits of the Dual-Use Regulation. The study included a section focusing on the recent expansion of controls on ICT surveillance technologies and the potential for further action in this area.[60]

According to the European Commission, the adoption of a 'human security' approach would potentially involve 'a clarification of control criteria to take into consideration broader security implications, including

[56] European Commission, "Green Paper: The Dual-Use Export Control System of the European Union: Enduring Security and Competitiveness in a Changing World," COM(2011)393 final, June 30, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>.

[57] European Commission, "Communication for the Commission to the Council and the European Parliament: The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World," COM(2014)244 final, <http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf>.

[58] Council of the European Union, "Outcome of the Council Meeting, 21 November 2014, 15792/14," <http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/145922.pdf>.

[59] European Parliament, "Report 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=REPORT&mode=XML&reference=A8-2015-0178&language=EN>.

[60] SIPRI and Ecorys, "Data and Information Collection for EU Dual-use Export Control Policy Review," November 6, 2015, <http://www.egadd.org.uk/wp-content/uploads/sites/25/2015/12/FINAL-REPORT.pdf, pp. 219-221>.

the potential effect on the security of persons e.g. through terrorism or human rights violations.'[61] Industry associations and NGOs have both voiced concerns about its application to export licensing decision-making.[62] Unlike human rights and international humanitarian law (IHL), 'human security' has never been integrated into regional or international legal instruments and lacks any kind of universally agreed upon definition.[63]

While the discussion regarding the adoption of human security criteria for assessing exports of dual-use goods has taken place largely in response to the recent debate about exports of ICT surveillance systems, it can be assumed that any standards developed would be applicable to all exports of other controlled items as well. This has generated concerns about the potential unintended effects of such a move. In particular, an attempt to create a set of human security considerations for states to take into account when assessing dual-use exports may have implications for other areas of the 'dual-use industry' and generate calls for further additions in the range of items that are subject to control.

It will be up to European legislators and regulators to strike the balance between the commercial interests of European cyber companies and their commitments to address this issue and adopt effective measures.

CSR and the Potential Benefits of a More Holistic Approach

The development and implementation of improved standards in CSR has always been part of the EU's discussion about the range of policy responses to the challenges posed by the export of ICT surveillance technologies. In May 2012 the European Parliament adopted a non-legislative resolution calling on the European Commission to 'produce guidelines for EU companies to act in a manner consistent with the Union's fundamental principles in such situations.'[64] The Commission has requested information on stakeholders' views regarding the creation of standards on 'due diligence and self-regulation by industry' within the context of a possible adoption of a 'human security approach' under the review of the Dual-Use Regulation.[65]

However, this aspect of the potential policy response to exports of ICT surveillance systems has been largely set to one side in the discussion about the application of export controls. Indeed, in the heat of the European debate about whether or not to amend export control regulations to include restrictions for ICT surveillance systems, it is easy to forget that CSR is a trade policy objective that already seeks to deal with the issues at hand.

CSR is a policy objective that, like export control policy, aims at mitigating the risks of international trade in an increasingly globalised world economy. Where export controls are aimed at non-proliferation and security objectives, CSR focuses on the impact of business operations on people, the environment and society. In addition, the role of government in these policies differs; where export controls are mainly driven by internationally developed legal obligations (hard law), like authorization requirements and end-

[61] European Commission, "The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World," April 2014.

[62] "ASD Position Paper on the Review of the Dual-Use Export Control System of the European Union," ASD, 22 Oct. 2014; and "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," Coalition Against Unlawful Surveillance (CAUSE), June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

[63] Oscar A. Gomez and Des Gasper, "Human Security: A Thematic Guidance Note for Regional and National Human Development Report Teams," UNDP, n.d., <http://hdr.undp.org/sites/default/files/human_security_guidance_note_r-nhdrs.pdf.>.

[64] European Parliament, "Trade for Change: The EU Trade and Investment Strategy for the Southern Mediterranean following the Arab Spring Revolutions, 2011/2113(INI) Resolution, May 19, 2012, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0201+0+DOC+XML+V0//EN>.

[65] See European Commission, "Consultation on the Export Control Policy Review (Regulation (EC) No 428/2009)," July 2015, <http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153629.pdf>.

user verification, CSR is a responsibility of enterprises and merely promoted by the government (soft law).

In 1976 the Organisation for Economic Co-operation and Development (OECD) first adopted the Guidelines for Multinational Enterprises. The Guidelines are recommendations by governments covering all major areas of business ethics, including corporate steps to obey the law, observe internationally-recognised standards and respond to other societal expectations.[66]

In 2011, the Guidelines were amended to include a chapter on human rights. This amendment anticipated the endorsement by the UN General Assembly of the UN Guiding Principles on Business and Human Rights that were proposed by UN Special Representative on business & human rights John Ruggie.[67,68] Both the UN Guiding Principles and the OECD Guidelines prescribe that enterprises should respect human rights, avoid causing or contributing to and seek ways to mitigate human rights infringements and provide remediation in case of 'causing' or 'contributing.' Although these instruments are non-binding in nature, non-observance of the guidelines can have serious consequences for enterprises. The OECD guidelines have a built-in grievance mechanism through National Contact Points (NCP). Adherent governments are required to set up an NCP, whose main role is to further the effectiveness of the Guidelines by undertaking promotional activities, handling enquiries, and contributing to the resolution of issues that arise from the alleged non-observance of the guidelines in specific instances (case law in a soft-law system).

In February 2013 a group of NGOs led by Privacy International submitted a complaint to the UK NCP against Gamma International. It alleged that the company had supplied an intrusion software product, Finfisher, to agencies of the Bahrain government that had used it to target pro-democracy activists. In December 2014, the UK NCP concluded that Gamma had not acted consistently with the provisions of the OECD Guidelines and made a number of recommendations, including that the company become more transparent and cooperate to remedy the misuse of its products.[69]

After the GCCS 2015, Professor Roel Nieuwenkamp, one of the panellists and chair of the OECD working group on responsible business conduct, commented on the developments in this area, including the UK NCP ruling.[70] He argued that although the NCP rulings represent "soft" law, their conclusions and recommendations might have "hard" consequences, as they may cause significant reputational damage to involved companies. Companies might lose government contracts, no longer receive export credit insurance or lose their governments' commercial diplomatic support. In addition, commercial investors might withdraw from companies that do not comply with OECD guidelines.

Implementing CSR in enterprises can be challenging, especially when it comes to understanding the impact of operations by suppliers or subcontractors. Luckily for exporters, there is guidance available with recommended measures companies can take to mitigate the risk that their products will be used to abuse human rights. These include the 'Guiding Principles on Business and Human Rights' produced by

[66] Organisation for Economic Co-operation and Development, "OECD Guidelines for Multinational Enterprises," May 25, 2011, <http://www.oecd.org/daf/inv/mne/48004323.pdf>.

[67] United Nations General Assembly, "Human Rights and Transnational Corporations and Other Business Enterprises," A/HRC/RES/17/4, July 6, 2011.

[68] UN Human Rights Council, "Guiding Principles on Business and Human Rights," June 2011, <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

[69] UK National Contact Point for the OECD Guidelines for Multinational Enterprises, "Privacy International & Gamma International UK Ltd: Final Statement after Examination of Complaint," December 2014, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/402462/BIS-15-93-Final_statement_after_examination_of_complaint_Privacy_International_and_Gamma_International_UK_Ltd.pdf>.

[70] Roel Nieuwenkamp, "Responsible Business Conduct in Cyberspace," April 30, 2015, <https://friendsoftheoecdguidelines.wordpress.com/2015/05/05/responsible-business-conduct-in-cyberspace/>.

the UN; the 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights' produced by the European Commission; and the "Know Your Customer" Standards for Sales of Surveillance Equipment' produced by the Electronic Frontiers Foundation.[71,72,73] Several ICT companies have also developed their own due diligence policies. For example, Ericsson and Nokia have systems for vetting potential sales that include a range of potential human rights risks.[74]

In 2014, the UK industry association TechUK published a set of guidelines about the risks associated with the export and use of 'cyber security' systems that included detailed guidance on the particular concerns associated with ICT surveillance systems.[75] This guide identifies specific human rights, such as the right to privacy and freedom of expression that could be affected by these systems. It provides examples of non-intended consequences of technology exports illustrated with real life examples and highlights specific actions companies can take to address human rights risks. These actions include pre-sale and post-sale scrutiny to identify customers of concern as well as potential technical and contractual options to mitigate potential risks if the company wants to go ahead with a specific transaction.

Improved CSR standards can act as an effective complement to export controls by strengthening the human rights policy objective without introducing a large licensing burden for the companies involved. However, like export controls, industry self-regulation alone is unlikely to solve the challenges related to the export of ICT surveillance systems. As noted, a wide range of companies produce these systems. These companies are likely to differ significantly in terms of their willingness and ability to develop and implement effective self-regulation processes. In addition, unlike in other sectors such as nuclear, chemical or defence, no EU or national industry associations exist that represent all companies producing ICT surveillance technologies and which could act as a coordinator for the development self-regulation standards.[76]

Moreover, companies that have publicly stated that they have developed systems of self-regulation have been faulted for the way they have been applied in practice. Since 2013, Hacking Team has taken steps to develop and implement a system of self-regulation for assessing its exports of intrusion software. However, following the theft and release of Hacking Team's internal emails, the content of their ICP was criticised on the grounds that it did not appear to be preventing the company from doing business with governments with 'controversial human rights records.'[77]

Conclusions

Efforts to apply export controls to ICT surveillance systems highlight an expansion in the range of policy objectives that states and NGOs seek to pursue through the use of these tools. Traditionally, dual-use

[71] UN Human Rights Council, "Guiding Principles on Business and Human Rights," June 2011, <http://shiftproject.org/sites/default/files/GuidingPrinciplesBusinessHR_EN.pdf>.

[72] European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights," June 2013, <http://shiftproject.org/sites/default/files/ECHRSG.ICT_.pdf>.

[73] Cindy Cohn and Jillian York, "Know Your Customer' Standards for Sales of Surveillance Equipment," Electronic Frontier Foundation, October 24, 2011, <https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment>.

[74] Nokia, "Nokia Human Rights Policy," February 25, 2015, <http://company.nokia.com/sites/default/files/download/nokia_human_rights_policy_1.pdf>; and Ericsson, "ICT and Human Rights: An Eco-System Approach," 2013, <http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/2012/human_rights0521_final_web.pdf>.

[75] Cyber Growth Partnership Industry Guidance, "Assessing Cyber Security Export Risks," November 26, 2014, <http://www.ihrb.org/publications/reports/human-rights-guidance-for-cyber-security-companies.html>.

[76] Some companies are members of ICT-focussed associations (e.g. Digital Europe), IT-focussed associations (e.g. BitKom), and/or defence industry associations (e.g. ASD), while others are not members of any association.

[77] James Lee, "Hacking Team Leak Highlights the Need to Implement Human Rights Due Diligence," *Tech UK*, July 14, 2015, <https://www.techuk.org/insights/news/item/5123-hacking-team-leak>.

goods have been understood as goods and technologies that have both military and civilian applications.[78] Expanding controls to encompass ICT surveillance systems where the end-user may be a law enforcement or intelligence agency indicates an expansion of this notion. Meanwhile, states have sought to control exports that pose a threat to national or regional security or that may be used in violations of human rights or international humanitarian law. Adopting criteria based on notions of human security would represent an expansion in the range of concerns that states take into account when assessing export licences.

The subsequent debate about the implementation of these controls reflects the challenges facing export controls as they are applied to a sector that is rapidly evolving, international, and highly mobile. At least one of the companies that was the intended target for controls, Gamma Group, moved its work on FinFisher intrusion software to offices in countries that are outside of the Wassenaar Arrangement.[79] Moreover, questions have been raised about the ability of list-based control systems to keep pace in a field where new systems are developed on a regular basis. At the same time, there is concern that the adoption of catch-all controls will generate confusion for ICT companies about whether their systems and technologies are covered.[80]

That said, these issues are not unique to the field of ICT surveillance systems but confront many areas of export controls. Many of the goods and technologies subject to export controls are rapidly evolving and produced by mobile companies. Moreover, the vast majority of the companies that produce ICT surveillance systems have chosen to remain in place and make themselves subject to controls.

In most of the areas where it applies, export controls are never a silver bullet that can solve a particular challenge but rather present one of a range of different policy tools that can affect change. Export controls may not prevent questionable exports of ICT surveillance technologies from taking place. However, in states where information is published about the granting of export licences, they can help to shed light on the secretive trade in ICT surveillance systems and generate debate about the best way to respond effectively.[81] As this article argues, industry self-regulation and the application of CSR guidelines forms a useful complement to export controls in the effort to create improved standards in the export of ICT surveillance systems. Indeed, as European legislators and regulators continue their legislative process to amend the Dual-Use Regulation to include legal measures aimed at preventing human rights abuse through the use of ICT surveillance systems, they should bear in mind that multinational enterprises have the responsibility to respect human rights. Legal measures should be aimed at clarifyng these responsibilities. At the same time, widely accepted principles can be adopted into legislation to create a level playing field while creating and maintaining a high ethical standard.

One challenge facing the effective implementation of CSR guidelines and export controls is the lack of clear standards for how ICT surveillance systems should be effectively governed. Almost all of the ICT surveillance systems that have been the focus of debate in recent years – including IMSI Catchers and intrusion software - are also widely used by EU and other Western law enforcement and intelligence agencies.[82] However, there

[78] The term 'dual-use' is also used to refer to items that have nuclear and non-nuclear applications as well as items that have WMD and non-WMD applications. See Quentin Michel, "Dual-use Exports Require a Common Definition," Dual-use Technologies in the European Union - Prospects for the Future, Friends of Europe, 2015, < http://www.friendsofeurope.org/security-europe/dual-use-exports-require-common-definition/>.

[79] Edin Omanovic, "Surveillance Companies Ditch Switzerland, but Further Action Needed," March 5, 2014, <https://www.privacyinternational.org/?q=node/377>; and Henry Habegger, "Bund Verscheucht Hersteller von Spionagesoftware Aus Der Schweiz [Bund Chases manufacturer of spy software from Switzerland]," *Schweiz Am Sonntag*, August 1, 2015, <http://www.schweizamsonntag.ch/ressort/politik/bund_verscheucht_hersteller_von_spionagesoftware_aus_der_schweiz/>.

[80] SIPRI and Ecorys, "Data and Information Collection for EU Dual-use Export Control Policy Review," November 6, 2015, <http://www.egadd.org.uk/wp-content/uploads/sites/25/2015/12/FINAL-REPORT.pdf, pp. 219-221>.

[81] Griffin, Andre, "Government has been Allowing UK Firms to Sell Invasive Spying Equipment to Countries Including Saudi Arabia, Records Show," *The Independent*, January 27, 2016, <http://www.independent.co.uk/life-style/gadgets-and-tech/news/government-has-been-allowing-uk-firms-to-sell-invasive-spying-equipment-to-countries-including-saudi-a6836651.html>.

[82] Eric King and Matthew Rice, "Behind the Curve: When Will the UK Stop Pretending IMSI Catchers Don't Exist," Privacy

is nothing in the way of agreed standards either at the EU level or elsewhere for how these systems should be used or how this use should be effectively governed and controlled.

Standards have been developed for LI systems and data retention systems.[83] However, these are primarily technical standards that do not stipulate the mechanisms that should govern the use of these powers, the government agencies that should be able to utilize them, or the way they should be employed in practice. Moreover, nothing has been developed for other ICT surveillance systems, such as IMSI Catchers, intrusion software and monitoring centres. Several EU member states do have legislation in place that governs the use of these systems or are currently putting legislation in place.[84] However, this is the exception rather than the rule and the standards that do exist vary significantly. Moreover, these discussions have not yet 'moved upwards' to the EU level.

The measures discussed in this article can contribute to preventing cases where exported ICT surveillance systems are used in human rights violations. However, when taking steps in this area, legislators and regulators should be careful to not introduce measures that form a disproportionate burden for the companies involved. A holistic approach, which combines export controls with improved standards for industry self-regulation and the application of CSR principles, carries the greatest chance of success for promoting change. List-based trade controls allow for legal certainty and transparency, end-use controls allow for flexibility and adaptability and industry self-regulation, and CSR allows companies to take initiative and demonstrate responsibility to their shareholders and customers.

International, November 5, 2014, <https://www.privacyinternational.org/?q=node/454>.

[83] See "Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture," ETSI TR 101 943 V2.2.1, ETSI, November 2006, < http://www.etsi.org/deliver/etsi_tr/101900_101999/101943/02.01.01_60/tr_101943v020101p.pdf>.

[84] Eric King and Matthew Rice, "Behind the Curve: When Will the UK Stop Pretending IMSI Catchers Don't Exist," Privacy International, November 5, 2014, <https://www.privacyinternational.org/?q=node/454>.