V. Human rights, the European Union and dual-use export controls

MARK BROMLEY

The application of human rights concerns has long been a widely accepted norm in the field of export controls for military equipment and the issue is referenced in the 2008 European Union (EU) Common Position on Arms Exports (EU Common Position), the Wassenaar Arrangement (WA) Best Practice Guidelines and the Arms Trade Treaty (ATT). The EU Common Position, among other things, requires EU member states to take account of human rights issues when granting export licences for military equipment and to deny an arms export licence if 'there is a clear risk that the military technology or equipment to be exported might be used for internal repression'.[1] The WA recommends that exporting states consider whether there is 'a clearly identifiable risk that the weapons might be used to commit or facilitate the violation and suppression of human rights'.[2] Human rights issues also feature in the export assessment criteria included in the ATT.[3]

The application of concerns about human rights violations to dual-use export controls is less clearly established and more uneven than it is to military items. For example, the WA Best Practice Guidelines relating to dual-use export controls make no reference to human rights concerns.[4] This is largely a reflection of the fact that the main priority of dual-use export controls is to prevent the proliferation of weapons of mass destruction (WMD) and their associated delivery systems, issues that do not immediately raise concerns about human rights.[5] However, the EU dual-use list does contain items that

[1] 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*, L335/99, 13 Dec. 2008.

[2] Wassenaar Arrangement, 'Elements for Objective Analysis and Advice Concerning Potentially Destabilising Accumulations of Conventional Weapons', adopted in 2004 and revised in 2011.

[3] United Nations, 'The Arms Trade Treaty', adopted 2 Apr. 2013, entered into force 24 Dec. 2014. Under article 6(3) of the ATT, a state party is required to not authorize an arms transfer if 'it has knowledge at the time of authorization that the arms or items would be used in the commission of genocide, crimes against humanity, grave breaches of the Geneva Conventions of 1949, attacks directed against civilian objects or civilians protected as such, or other war crimes as defined by international agreements to which it is a Party'. Under article 7(1) of the ATT, states parties are also required to 'assess the potential' that the exported arms will be used, among other things, to 'commit or facilitate a serious violation of international humanitarian law' or 'commit or facilitate a serious violation of international human rights law'.

[4] See Wassenaar Arrangement, 'Best Practice Guidelines for the Licensing of Items on the Basic List and Sensitive List of Dual-Use Goods and Technologies' (Agreed at the 2006 Plenary).

[5] The most widely used dual-use control list is the EU dual-use list, which is based on the control lists adopted by the Australia Group (AG), the Chemical Weapons Convention (CWC), the Missile Technology Control Regime (MTCR) and the Nuclear Suppliers Group (NSG), as well as the dual-use list adopted by the WA. The AG, CWC and NSG lists consist of items that raise WMD-related concerns. Annex 1, List of Dual-use Items, Council Regulation 428/2009 of 5 May 2009 setting up

could raise concerns on human rights grounds. In addition, the WA dual-use list consists of items that could be used in conventional weapons as well as several items that might be used by states' intelligence or law enforcement agencies (LEAs).[6] In recognition of this, EU-level controls on the export of dual-use goods make some reference to human rights concerns, for example in the guidance language on the EU General Export Authorization for telecommunications equipment.[7] In addition, article 12 of the EU Dual-use Regulation requires member states to take account of 'all relevant considerations' when assessing export and brokering licences for dual-use goods, including those covered by the EU Common Position.[8]

Nonetheless, the implementation of these concerns by EU member states has been uneven and clear guidance lacking. The EU Common Position and the accompanying User's Guide focus on transfers of military items to military end-users and do not provide specific guidance on the range of human rights issues associated with exports of dual-use goods.[9] The issue of how to better integrate human rights concerns into dual-use export controls has been gaining prominence at the EU level since 2011, largely owing to the expansion in the range of information and communication technology (ICT) surveillance systems covered by WA and EU-level controls on dual-use exports following events connected to the 'Arab Spring'. WA and EU-level controls on dual-use exports have expanded to include a wider range of ICT surveillance systems, and this has driven debates in the EU about how best to integrate human rights concerns into dual-use export controls. The different policy options being discussed as part of the ongoing review of the EU Dual-use Regulation are examined below.

Expansion of controls on ICT surveillance technologies

ICT surveillance systems, also known as cyber-surveillance technologies or cyber-surveillance systems, enable the monitoring and exploitation of data or content that is stored, processed or transferred using ICTs such as com-

a Community regime for the control of exports, transfer, brokering and transit of dual-use items', *Official Journal of the European Union*, L134, 29 May 2009.

[6] E.g. 'laser acoustic detection equipment'—systems that are used to remotely spy on conversations by measuring vibrations in window glass—are covered by Category 6 of the WA dual-use list. In addition, Category 9 of the WA dual-use list covers 'unmanned aerial vehicles (UAVs)'. Provided they meet the minimum capabilities set by the control list, this would include UAVs fitted with cameras or sounding systems.

[7] Regulation (EU) 1232/2011 of the European Parliament and of the Council of 16 November 2011 amending Council Regulation (EC) 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*, L326, 8 Dec. 2011, pp. 37–38.

[8] 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, 29 Apr. 2009.

[9] Council of the European Union (note 8).

Box 15.1. Types of ICT surveillance system

Mobile telecommunications interception equipment—also know as 'IMSI Catchers'—are used to remotely track, identify, intercept and record mobiles phones.

Intrusion software can be inserted into computers and mobile phones without detection and used to remotely monitor and, in certain cases, control them.

Internet Protocol (IP) network surveillance systems are used to intercept, collect and, in some cases, analyse data as it passes through an IP network.

Data retention systems are used by network operators to comply with legal requirements for the storage of 'meta data' on their users for later potential use by law enforcement agencies (LEAs) or intelligence agencies.

Lawful Interception (LI) systems are used by network operators to enable them to comply with requests from LEAs and intelligence agencies for the provision of their users' communications data.

Monitoring centres are used by LEAs and intelligence agencies to collect, store and analyse different forms of communications data from various surveillance sources.

Digital forensics systems are used by LEAs or intelligence agencies to retrieve and analyse data stored on networks, computers and mobile devices.

Notes: A network operator is a company, such as Vodafone or TeliaSonera, that manages a communications network. Communications data can be: (*a*) meta data—information about the use of a network or the calls that a subscriber has made; (*b*) content data—what is said in a phone call or the content of a text message; or (*c*) location data—information about the movements of a subscriber to a mobile phone network.

Source: Bromley, M. et al., 'ICT surveillance systems: trade policy and the application of human security concerns', *Strategic Trade Review*, vol. 2, no. 2 (2016).

puters, mobiles phones and telecommunications networks (for a description of the different types of ICT surveillance system see box 15.1). Such systems are used by the authorities in virtually all states for law enforcement and intelligence-gathering purposes. However, their export and use raises a range of security concerns (linked to theft of classified data or attacks on critical infrastructure) and human rights concerns (particularly in states that lack effective laws and regulations governing their use). Human rights concerns range from potential violations of the right to privacy or freedom of expression to more serious breaches, such as of the right to freedom from arbitrary arrest and detention, and to freedom from torture and inhuman or degrading treatment.

Prior to 2011 several ICT surveillance systems were indirectly covered by the controls on cryptography under Category 5 of the WA dual-use list.[10] In particular, exports of digital forensics, intrusion software and Lawful Interception (LI) systems have all been made subject to dual-use export controls

[10] Cryptography is used to securely store or transfer information. Since the 1990s, systems that employ a certain standard of cryptography have been covered by the WA dual-use export control list for reasons of national security. See Saper, N., 'International cryptography regulation and the global information economy', *Northwestern Journal of Technology and Intellectual Property*, vol. 11, no. 7 (Fall 2013).

on these grounds.[11] However, after the Arab uprisings in 2011 a series of non-governmental organization (NGO) and media reports highlighted the role of EU- and US-based companies in the supply of security, surveillance and censorship technologies and services to states in the Middle East and North Africa.[12] Most of these systems were not covered by states' export controls. In certain cases the systems supplied were used in connection with violations of human rights by the recipient state's security forces, including cases of torture and arbitrary arrest and detention. EU member states, Members of the European Parliament and NGOs called for steps to be taken to restrict the use of ICT surveillance systems by oppressive regimes and to help dissidents operating in those states to escape monitoring.[13] In response, the EU in particular made a number of commitments to restrict the export and use of ICT surveillance systems.[14] A number of policy options were discussed in the European Commission, the European Parliament and the European Council, such as developing improved corporate social responsibility guidelines for companies that supply ICT surveillance systems and providing dissidents with technologies that would enable them to evade detection by intelligence agencies and LEAs. However, the guidelines produced to date have focused on the whole ICT sector without engaging substantially with the issue of ICT surveillance systems.[15] In addition, the plan to supply dissidents with surveillance-evading technologies was dropped, reportedly over fears about interfering in the internal affairs of states.[16]

Dual-use export controls

Most of the concrete steps and substantive discussions have focused on the use of dual-use export controls—an area in which the EU has a clear mandate to act and a focus for NGOs working on human rights and privacy issues.[17] In 2014 the Coalition Against Unlawful Surveillance Exports (CAUSE) was set up by several leading NGOs to call for the EU to make ICT surveillance

[11] Privacy International, 'British government admits it started controlling exports of Gamma International's FinSpy', 10 Sep. 2012.

[12] See e.g. Elgin, B., Silver, V. and Katz. A., 'Iranian police seizing dissidents get aid of Western companies', Bloomberg Business, 31 Oct. 2011; and FIDH, *Surveillance Technologies 'Made in Europe': Regulation Needed to Prevent Human Rights Abuses*, Position paper (Dec. 2014).

[13] European Parliament, Trade for change: The EU Trade and Investment Strategy for the Southern Mediterranean following the Arab Spring revolutions, Resolution (2011/2113(INI)), 10 May 2012.

[14] See Kroes, N. (Vice-President of the European Commission responsible for the Digital Agenda), 'ICT for Democracy: Supporting a Global Current of Change', SPEECH/11/866, 9 Dec. 2011; and Council of the European Union, EU Human Rights Guidelines on Freedom of Expression Online and Offline, Foreign Affairs Council meeting, Brussels, 12 May 2014.

[15] See European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013).

[16] See Stupp, C., 'EU Internet freedom programme endangered by Commission muddle', Euractiv, 12 Feb. 2016.

[17] The Dual-use Regulation forms part of the EU's 'common commercial policy', one of the areas of 'exclusive' EU competence.

systems subject to export controls and oblige member states to take human rights issues into account when making licensing decisions.[18]

Citing both security and human rights concerns connected to their use, the WA and the EU have expanded their dual-use export controls since 2011 to directly capture a wider range of ICT surveillance systems. In 2011 and 2012 the EU arms embargoes on Iran and Syria were expanded to include a wide range of ICT surveillance systems.[19] In addition to capturing all the ICT surveillance systems (see box 15.1), the expanded coverage of these two embargoes also created restrictions on the supply of telecommunications networks and related services.[20] Particular types of ICT surveillance systems have also been added to the WA and, subsequently, to the EU dual-use control lists. Controls on mobile telecommunications interception equipment were added to the WA's dual-use control list in December 2012 and the EU's list in December 2014. Controls on intrusion software and IP network surveillance systems were added to the WA's export control list in 2013 and to the EU list in 2014. Discussions are ongoing in the WA about controls on data retention systems and monitoring centres and in the EU about controls on digital forensics systems and LI systems. As a result, most of the ICT surveillance systems that LEAs and intelligence agencies use to intercept and analyse electronic communications are subject to WA or EU dual-use export controls or may become subject to control in the future.

The application of these measures has varied among EU member states, reflecting their different priorities when implementing dual-use export controls, particularly when the normative implications of a particular export extend beyond questions of WMD non-proliferation to include issues related to human rights. The companies involved have also responded differently to being made subject to export controls. At least one company that produces intrusion software—Gamma Group—is reported to have moved its work in this area to offices in countries not in the WA.[21] Most companies appear to have accepted the new regulations, however, although the varied composition of the producers of the different types of ICT surveillance systems makes a uniform response unlikely. Some of the companies involved are

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

[19] Council Decision 2011/782/CFSP of 1 Dec. 2011 concerning restrictive measures against Syria and repealing Decision 2011/273/CFSP, *Official Journal of the European Union*, L319, 2 Dec. 2012, pp. 56–70; and Council Decision 2012/168/CFSP of 23 Mar. 2012 amending Decision 2011/235/CFSP concerning restrictive measures directed against certain persons and entities in view of the situation in Iran, *Official Journal of the European Union*, L87, 24 Mar. 2012, pp. 85–89.

[20] Stecklow, S., 'Special report: Chinese firm helps Iran spy on citizens', Reuters, 22 Mar. 2012.

[21] Omanovic, E., 'Surveillance companies ditch Switzerland, but further action needed', Privacy International, 5 Mar. 2014; and Habegger, H., 'Bund verscheucht Hersteller von Spionagesoftware aus der Schweiz' [Federation chases manufacturer of spy software from Switzerland], *Schweiz am Wochenende*, 18 July 2015.

large military contractors, such as Thales and BAE Systems, which produce a wide range of ICT surveillance systems for LEAs and intelligence agencies. Others are large ICT companies, such as Nokia and Ericsson, which produce telecommunications networks and are legally required to have LI systems 'built in' to their products or to enable their inclusion. Finally, smaller ICT firms, such as Gamma International and Hacking Team, specialize exclusively in the production of certain types of surveillance technologies, such as mobile telecommunications interception equipment and intrusion software.

Controls on intrusion software

The most controversial aspect of the expansion of controls on ICT surveillance systems has been the implementation of controls on intrusion software. Following the adoption of the WA and EU controls, companies and researchers voiced concern that the language used described both the intrusion software used by LEAs and intelligence agencies and the systems and processes that are essential to IT security, particularly systems used for 'penetration testing' and processes of 'vulnerability disclosure'.[22] This debate grew more heated after the United States published proposed implementation language in May 2015 that implied the controls might also capture so-called zero days.[23] Definitions vary, but zero days are generally understood to be vulnerabilities in a computer program that are unknown to the software vendor or users.[24] Zero days have been used to insert ICT surveillance systems into target devices, particularly intrusion software, and also in the deployment of offensive cyberwarfare tools, such as the Stuxnet virus.[25] However, the ability to freely exchange information about zero days across national boundaries is also a key aspect of processes of vulnerability disclosure.[26] The strength of the pushback by the IT sector led the USA to

[22] Bratus, S. et al., 'Why Wassenaar Arrangement's definitions of intrusion software and controlled items put security research and defense at risk: and how to fix it', 9 Oct. 2014. 'Penetration testing' systems are used to test the security of a network by simulating attacks against it in order to locate vulnerabilities. Processes of 'vulnerability disclosure' are the means through which software vulnerabilities are identified and reported. Others have argued that, if properly applied, the controls should not have any effect in these areas. See Anderson, C., 'Considerations on Wassenaar Arrangement control list additions for surveillance technologies', Access, 13 Mar. 2015.

[23] Uchill, J., 'Industry warns proposed arms export rule will thwart basic cyberdefenses', *Christian Science Monitor*, 26 June 2015.

[24] See Fidler, M., 'Regulating the zero-day vulnerability trade: a preliminary analysis', *I/S: A Journal of Law and Policy for the Information Society*, vol. 11, no. 2 (Dec. 2015).

[25] Zetter, K., 'Hacking team leak shows how secretive zero-day exploit sales work', *Wired*, 24 July 2015; Murchu, L. O., 'Stuxnet using three additional zero-day vulnerabilities', Symantec Official Blog, 14 Sep. 2010; and Nakashima, E. and Warrick, J., 'Stuxnet was work of US and Israeli experts, officials say', *Washington Post*, 2 June 2012.

[26] The issue of whether and, if so, how governments should seek to regulate the trade in zero days and software vulnerabilities more generally has been a topic of debate in several states. It is also one that has seen agencies from the same state focused on intelligence-gathering or IT network security take opposing sides. See Shear, M. D. and Sanger, D. E., 'Competing interests on encryption divide top Obama officials', *New York Times*, 5 Mar. 2016.

both delay the adoption of the controls and, unusually, to seek to substantially amend the control list language at the WA.[27] However, amendments to existing WA control list categories can only be adopted by consensus and, owing to resistance from other states, only minor adjustments to the controls on intrusion software were adopted.[28]

In 2016, the WA also examined proposals to further expand the range of ICT surveillance systems that are subject to control. Germany adopted national-level controls on monitoring centres and data retention systems in 2015 and has proposed their adoption at the WA.[29] None of these proposals were adopted in 2016 and their chances for inclusion in the WA dual-use list may have suffered owing to a combination of the intrusion software controversy and the lack of a clear mandate for the WA to address human rights concerns through its dual-use export controls. To date, the inclusion of ICT surveillance technologies on the WA's lists has been based 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'.[30] Monitoring centres and data retention systems are largely of interest because of human rights concerns.

The review of the EU Dual-use Regulation

Inside the EU, the main focus of attention when it comes to further expanding controls on the export of ICT surveillance systems has been the ongoing review of the EU's Dual-use Regulation (see section IV). 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'.[31] On 8 September 2015, the European Parliament adopted a non-binding resolution urging the European 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.[32] As part of this discussion, the Commission

[27] Cardozo, N. and Galperin, E., 'Victory! State Department will try to fix Wassenaar Arrangement', Electronic Frontiers Foundation, 29 Feb. 2016.

[28] Thomson, I., 'Wassenaar weapons pact talks collapse leaving software exploit exports in limbo', *The Register*, 21 Dec. 2016.

[29] German Federal Ministry of Economic Affairs and Energy, 'Anlage AL zur Außenwirtschaftverordnung [Annex AL to the German Foreign Trade Regulations]', July 2015.

[30] Wassenaar Arrangement, 'Public statement: 2013 Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies', Vienna, 4 Dec. 2013.

[31] Malmström, C. (EU Commissioner for Trade), 'Debate at European Parliament in Strasbourg', 24 Nov. 2014.

[32] European Parliament, 'Report on human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries', 2014/2232(INI), 3 June 2015.

has proposed evolving dual-use export controls towards a 'human security' approach in order to encompass a wider range of human rights issues.[33] Both industry associations and NGOs have voiced concerns about the application of a human security approach to export-licensing decision-making.[34] In particular, unlike human rights, human security has never been integrated into regional or international legal instruments and lacks any kind of universally agreed definition.[35] The draft revision of the EU Dual-use Regulation, published in September 2016, contains a range of steps that would expand controls on ICT surveillance systems. These steps are embedded in a wider set of measures that could serve to expand both the range of items that are subject to dual-use export controls at the EU level and the range of normative concerns that EU member states are required to take into account when assessing their exports. These measures consist of four main elements: a proposed expansion of the definition of dual-use goods; the proposed adoption of an EU-level control list for ICT surveillance systems; a proposed new catch-all control; and new language on the range of concerns that EU member states must address when assessing dual-use export licences.

1. *A proposed expansion of the definition of dual-use goods*. This would include 'cyber-surveillance technology which can be used for the commission of serious violations of human rights or international humanitarian law, or can pose a threat to international security or the essential security interests of the Union and its Member States'.[36] The draft revision also provides a definition of cyber-surveillance technology, which lists '(a) mobile telecommunication interception equipment; (b) intrusion software; (c) monitoring centers; (d) lawful interception systems and data retention systems; and (e) digital forensics'.[37] An earlier draft of the proposal, which was leaked in the summer, included a number of sub-systems that are used in ICT surveillance systems, such as probes and deep packet inspection.[38] The definition provoked concern from industry and a number of EU member states about

[33] European Commission, 'Communication from 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, 24 Apr. 2014.

[34] AeroSpace & Defence Industries Association of Europe, 'ASD position paper on the review of the dual-use export control system of the European Union', 22 Oct. 2014; and CAUSE, 'A critical opportunity: bringing surveillance technologies within the EU Dual-use Regulation', June 2015.

[35] Gomez, O. A. and Gasper, D., 'Human security: a thematic guidance note for regional and national human development report teams', United Nations Development Programme, [n.d.].

[36] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)', COM(2016) 616 final, 28 Sep. 2016, p. 19.

[37] European Commission (note 36), pp. 22–23.

[38] Probes are used to collect data as it passes through a communications network; deep packet inspection is used to examine the content of data as it passes through a communications network. Both systems are used in several ICT surveillance systems but also have a range of non-surveillance applications.

the impact such a proposal might have on sections of the ICT sector.[39] However, even the narrower definition of cyber-surveillance technology includes a number of systems that have not been subject to control at the WA level, such as LI systems and digital forensics, and this is likely to be a focus of debate. For example, several NGOs—such as Privacy International, which is part of the CAUSE coalition—have voiced concern about the impact of adopting controls on digital forensics, arguing that they have the potential to affect IT security.[40] The recast retains the current overall framing language, which defines dual-use items as 'items, including software and technology, which can be used for both civil and military purposes'. However, it includes cyber-surveillance technology within that definition; and in its definition of cyber-surveillance technology it includes items that are predominantly used by LEAs and intelligence agencies. The proposed language therefore has the potential to shift dual-use export controls beyond the civilian-use or military-use paradigm that currently frames the range of goods controlled to explicitly encompass systems used by LEAs and intelligence agencies.[41]

2. *The proposed adoption of an EU-level control list for ICT surveillance systems*. In the draft proposal the only items included on the proposed list are monitoring centres and data retention systems, using the definitions that Germany used when it added these items to its national controls in 2015. However, the proposal leaves open the option of adding new items in the future, at the initiative of the Commission through the use of delegated powers. This would, for the first time, create a set of EU-level list-based controls that are not drawn from one of the multilateral export control regimes. Adopting EU-level controls on items that are not included on the control lists of the multilateral export control regimes is something that EU member states and industry have always sought to avoid. Their argument is that it might have a negative impact on the competitiveness of EU-based companies and generate confusion for non-EU states that value the EU dual-use control list as a synthesis of the multilateral regimes' control lists and implement it nationally.

3. *A proposed new catch-all control covering exports of unlisted dual-use items*. Among other things, 'the items in question are or may be intended, in their entirety or in part . . . for use by persons complicit in or responsible for directing or committing serious violations of human rights or international

[39] Stupp, C., 'Commission plans export controls on surveillance technology', EurActiv, 22 July 2016. The leaked proposal is available at <http://www.euractiv.com/wp-content/uploads/sites/2/2016/07/dual-use-proposal.pdf>. Stupp, C., 'Tech industry, privacy advocates pressure Commission on export control bill', EurActiv, 3 Aug. 2016; and Stupp, C., 'Juncker postpones controversial export control bill on surveillance technology', EuroActiv, 20 Sep. 2016.

[40] Omanovic, E., 'Landmark changes to EU surveillance tech export policy proposed, leaked document shows', Privacy International, 28 July 2016.

[41] See Bauer, S. and Bromley, M., 'The dual-use export control policy review: balancing security, trade and academic freedom in a changing world', Non-Proliferation Paper no. 48 (Mar. 2016).

humanitarian law in situations of armed conflict or internal repression in the country of final destination . . . [or] for use in connection with acts of terrorism'.[42] Companies would be required to apply for an export licence if their national authority informs them that the items are, or may be, intended for these purposes. They are also obliged to inform their national authorities if—after having carried out processes of 'due diligence'—they become aware that the items are or may be intended for these purposes. The European Parliament proposed a dedicated catch-all control for exports of unlisted ICT surveillance systems in October 2012 but it was not adopted.[43] The Commission's proposal goes beyond the 2012 language by including a reference to terrorism and covering all unlisted dual-use items. What this would mean in practice is unclear, but a catch-all control is potentially better able than an exclusively list-based approach to keep pace with technology developments in the ICT surveillance sector. Moreover, existing regulations mean that most ICT surveillance technologies of interest are sold exclusively to national governments, making it possible to target controls effectively.[44] However, a broadly defined catch-all is likely to generate differences in national implementation and confusion among companies about which products and transactions are covered. These are already issues for the EU-level WMD and embargo-related catch-all controls, even though agreed practices and shared standards have been developed over several years.[45]

4. *New language on the range of concerns that EU member states must address when assessing dual-use export licences.* The new language states that, in deciding whether to grant a licence, member states 'shall take into account . . . respect for human rights in the country of final destination as well as respect by that country of international humanitarian law' and commit to not export any items that 'would provoke or prolong armed conflicts or aggravate existing tensions or conflicts in the country of final destination'.[46] If this language is adopted, it will be an explicit mention of human rights issues in the EU Dual-use Regulation. However, the current draft also removes the reference to the Common Position, meaning that the guidance it provides is no longer connected to the Dual-use Regulation. As noted above, the guidance provided by the EU Common Position and the accompanying User's Guide were in many ways poorly suited to the concerns raised by the export of dual-use items in general and of ICT surveillance systems in particular. Nonetheless, it did provide some points of relevance and it will

[42] European Commission (note 36), pp. 23–24.

[43] European Parliament, 'Legislative resolution on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items', COM (2011), 23 Oct. 2012.

[44] Privacy International, 'Privacy International BIS submission', [n.d.].

[45] Bauer and Bromley (note 41).

[46] European Commission (note 36).

need to be replaced by something detailed if the requirements on human rights are to be interpreted by EU member states in a clear and consistent manner. The proposed revision states that 'guidance and/or recommendations to ensure common risk assessments by the competent authorities of the Member States for the implementation of those criteria' will be produced by the European Council and the European Commission, but it is unclear how detailed they will be and when or how they will be produced.[47]

[47] European Commission (note 36).