sipri

EXPORT CONTROLS, HUMAN SECURITY AND CYBER-SURVEILLANCE TECHNOLOGY

Examining the Proposed Changes to the EU Dual-use Regulation

MARK BROMLEY

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

SIPRI is an independent international institute dedicated to research into conflict, armaments, arms control and disarmament. Established in 1966, SIPRI provides data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.

The Governing Board is not responsible for the views expressed in the publications of the Institute.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

EXPORT CONTROLS, HUMAN SECURITY AND CYBER-SURVEILLANCE TECHNOLOGY

Examining the Proposed Changes to the EU Dual-use Regulation

MARK BROMLEY

December 2017

sipri

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

Contents

Acknowledgements

The author would like to thank SIPRI intern Johanna Trittenbach for her detailed background research. The author would also like to thank Machiko Kanetake, Edin Omanovic and the anonymous reviewers for providing comments on draft versions of the paper, and Ralf Kuhne and Felix A. Lutz for their feedback on the sections detailing the legislative procedure of the EU.. All errors are the responsibility of the author alone. Finally, SIPRI would like to thank the Swedish Ministry of Foreign Affairs for its generous support in covering the costs associated with the production of this paper.

Abbreviations

AFET	European Parliament Committee on Foreign Affairs
AG	Australia Group
ASD	Aeronautic, Space, Defence and Security Industries in Europe
ATT	Arms Trade Treaty
BDI	Bundesverband der Deutschen Industrie (Federal Association of German Industry)
CAUSE	Coalition Against Unlawful Surveillance Exports
Cefic	European Chemical Industry Council
CFSP	Common Foreign and Security Policy
CJEU	Court of Justice of the European Union
CSR	Corporate social responsibility
CWC	Chemical Weapons Convention
DPI	Deep Packet Inspection
DUCG	Dual-use Coordination Group
EFA	European Free Alliance
EU	European Union
EUGEA	EU General Export Authorisation
FPI	Foreign Policy Instruments
ICT	Information and communications technology
IHL	International humanitarian law
INTA	European Parliament Committee for International Trade
IP	Internet protocol
LEA	Law enforcement agency
LI	Lawful interception
MEP	Member of the European Parliament
MTCR	Missile Technology Control Regime
NSG	Nuclear Suppliers Group
STEG	Surveillance Technology Expert Group
WMD	Weapons of mass destruction

Executive summary

In September 2016, the European Commission published a proposed 'recast' of the EU Dual-use Regulation, the main regulatory instrument for EU member states' controls on the trade in dual-use items. The proposal, which is currently being examined by the European Parliament and Council of the European Union, is part of a review of the Regulation which was launched in 2011. The review is expected to conclude with the adoption of a new version of the Regulation in late 2018 or early 2019. One of the most controversial aspects of the Commission's proposal is a series of amendments to the Regulation that would give human rights, international humanitarian law (IHL) and terrorism a more central role in member states' dual-use export controls and create an expanded set of controls on exports of so-called cyber-surveillance technology. Many of these aspects of the Commission's proposal have been broadly welcomed by the European Parliament and NGOs, which have been pushing for tighter EU controls on the trade in cyber-surveillance technology since 2011. However, other stakeholders—particularly the sections of EU industry affected by dual-export controls—have warned of the potential for confusion and unintended side-effects to be generated by the language used.

This paper seeks to inform discussion about these aspects of the Commission's proposal. In particular, the paper outlines the existing relationship between human rights, IHL, terrorism and dual-use export controls, details the origins of the discussion about applying export controls to cyber-surveillance technology and describes the measures that have been adopted to date within the Wassenaar Arrangement and the EU. The paper then analyses those aspects of the Commission's proposal which are focused on human rights, IHL, terrorism and cyber-surveillance technology while also detailing the responses and alternative formulations put forward by key stakeholders. The paper ends by presenting some conclusions and recommendations, focused particularly on the issues that should be addressed as the review process continues. Although well-advanced, the process may not conclude until late 2018 or early 2019, which means that there is still time to ensure that the approach taken by the EU on this important issue can contribute effectively to a more responsible trade in cyber-surveillance technology and a Dual-use Regulation that reflects EU values and continues to act as a model for other parts of the world.

1. Introduction

The European Union (EU) has had a common legal framework for dual-use export controls—controls on the trade in items which have the potential to be used for both military and civilian purposes—since the 1990s. In 2011 the European Commission launched a review of the EU Dual-use Regulation—the main regulatory instrument in this area. Following a series of consultations, it published a proposal in the form of a draft 'recast' of the regulation in September 2016. One of the most controversial aspects of the Commission's proposal is a series of amendments that would give concerns related to human rights, international humanitarian law (IHL) and terrorism a more central role in member states' dual-use export controls while also creating an expanded set of controls on so-called cyber-surveillance technology. In 2018, the Commission's proposal will be the subject of trilogue negotiations between the Commission, the Council of the European Union and the European Parliament. The negotiating process will begin once the European Parliament and the Council have adopted their proposed amendments to the Commission's proposal. The European Parliament is expected to adopt its proposed amendments in January 2018 but it is unclear when the Council will do so. It is hoped that the whole process will conclude in 2018 or early 2019.

The issue of exerting control over the export and use of cyber-surveillance technology became prominent in EU thinking after the so-called Arab Spring of 2011. In the months that followed a series of NGO and media reports detailed the role that EU-based—as well as US and Israeli-based—companies had played in supplying cyber-surveillance technology to some of the affected states in the Middle East and North Africa, which had then used them in connection with violations of human rights. Partly in response, the Wassenaar Arrangement's participating states added certain types of cyber-surveillance technology to its dual-use control list in 2012 and 2013. These items were added to the EU dual-use list in 2014. The EU also took unilateral steps in this area, particularly by including a range cyber-surveillance technology in the EU sanctions on Iran and Syria, and made commitments to take additional measures. Although other avenues were explored—such as promoting systems of industry self-regulation—the Dual-use Regulation and the review process have emerged as the primary focus for discussions about how stronger controls could be created at the EU level.

The Commission's proposal contains a wide range of modifications to the Dual-use Regulation. These include measures aimed at reducing the administrative burden of licensing processes on business and authorities, particularly by expanding the range of facilitated licensing procedures for certain transfers through the use of new EU General Export Authorizations (EUGEAs). It also includes measures aimed at harmonizing the application of controls at the national level, particularly by increasing the amount of information EU member states share with each other about how controls are implemented. These aspects are beyond the scope of this paper, which focuses on the parts of the proposal that are aimed at giving human rights, IHL and terrorism-related concerns a more prominent position in the Dual-use Regulation and creating expanded controls on cyber-surveillance technology. In this regard, the Commission's proposal contains four key changes. First, it would expand the definition of dual-use items to capture cyber-surveillance technology. Second, it would create an EU list of controlled cyber-surveillance technology. Third, it would give human rights and IHL a more central place in the set of criteria that member states apply when assessing export licences. Fourth, it would create a new 'catch-all clause' that would allow member states to apply controls to exports of non-listed dual-use items

that may be used in serious violations of human rights or IHL or acts of terrorism, and an accompanying obligation on companies to assess the risk that their exported items will be used in this way.

These four aspects of the Commission's proposal have been the subject of considerable discussion and debate. In particular, industry associations, NGOs, national parliaments, and Members of the European Parliament (MEPs) have argued that they have the potential to generate confusion and unintended side-effects, as well as an increased regulatory burden for both companies and national authorities. However, other NGOs and MEPs, as well as political groups in the European Parliament have argued that the proposals do not go far enough by leaving important categories of cyber-surveillance technology outside the scope of the Dual-use Regulation and failing to ensure consistent, restrictive and transparent implementation of the controls at the national level. A number of alternative formulations have been proposed that would either narrow or broaden the focus of these measures. Despite the intensity of the debate, there is still a significant lack of clarity about the implications of the Commission's proposal and the alternatives put forward. This paper seeks to clarify the issues under discussion, assess the implications of what has been proposed, and provide a sound basis for a focused discussion of these topics as debates about the content of the new version of the Dual-use Regulation continue in 2018 and—potentially—2019.

Section 2 provides detailed background to the current discussions. First, it outlines the existing relationship between human rights, IHL, terrorism and dual-use export controls. Second, it details the origins of the discussion about creating stronger controls on the export of cyber-surveillance technology. Third, it details the set of controls that has been created in this area at the Wassenaar Arrangement and outlines available assessments of how these have been implemented by EU member states. Fourth, it outlines the history of the debate about the need to create EU-level controls in this area and describes the measures that have been introduced to date. Section 3 provides an overview of those aspects of the Commission's proposal which are focused on human rights, IHL and terrorism-related concerns, and on expanding the controls on exports of cyber-surveillance technology. The section details the content and potential implications of the four key changes outlined above. For each of these changes, the section also outlines some of the responses and alternative formulations that have been put forward by different stakeholders, particularly the European Parliament, industry associations, national parliaments, NGOs, and political groups in the European Parliament. Section 4 presents some conclusions and recommendations, focused particularly on the issues that might be addressed during the trilogue process. Given that this process may not conclude until early 2019, there is still the potential to further develop and refine these important aspects of the Commission's proposal. Having language that is clear and works as intended would help to ensure that the EU Dual-use Regulation fills important gaps in the measures that have been created for controlling the trade in cyber-surveillance technology and establish standards that could act as a model for other parts of the world.

2. Background to the current discussion

Human rights, IHL, terrorism and dual-use export controls

International human rights law—referred to here as human rights—is the set of protections to which all individuals are entitled. Its parameters are detailed in a number of international conventions, most notably the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[1] Human rights include the right to privacy, freedom of expression, freedom of association, the right to life, freedom from arbitrary arrest and detention, and freedom from torture and inhuman or degrading treatment. Certain of these rights are considered inviolable while others may be restricted in certain defined circumstances.[2] Moreover, certain violations of human rights are viewed as 'serious violations' or as constituting a case of 'internal repression' while others are not, although there is a lack of consensus on the exact coverage of these categories.[3] The application of human rights-related concerns to export controls on military goods is a well-established international practice. For example, criterion 2 of the 2008 EU Common Position on Arms Exports (EU Common Position) requires EU member states to deny an export licence for military goods if 'there is a clear risk that the military technology or equipment to be exported might be used for internal repression'.[4] It also requires member states to exercise 'special caution and vigilance' when issuing licences for exports to countries where 'serious violations of human rights have been established by the competent bodies of the United Nations, by the European Union or by the Council of Europe'.[5] Human rights concerns are also referenced—albeit in less detail—in other arms export control instruments, such as the Wassenaar Arrangement's Best Practice Guidelines and the Arms Trade Treaty (ATT).[6]

International humanitarian law—also known as the 'laws of war' or 'the law of armed conflict'—is the international legal framework that governs situations of armed conflict or occupation. Its parameters are detailed in a number of international conventions, most notably the 1907 Hague Regulations and the four Geneva conventions and their Additional Protocols.[7] Examples of serious violations of IHL include wilful

[1] Office of the United Nations High Commissioner for Human Rights, Universal Declaration of Human Rights, <http://www.un.org/en/documents/udhr/>; and International Covenant on Civil and Political Rights, <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

[2] For example, the right to privacy, freedom of expression and freedom of association may be restricted for certain legitimate reasons, the right to life and to freedom from arbitrary arrest and detention 'must be protected from arbitrary or unlawful deprivation or interference by the State', while the right to freedom from torture and inhuman or degrading treatment can never be limited or restricted. Government of the United Kingdom, *Assessing Cyber Security Export Risks: Cyber Growth Partnership Industry Guidance* (Techuk: London, 2015).

[3] See Geneva Academy, 'What amounts to "a serious violation of international human rights law"?', Aug. 2014.

[4] 'Internal repression', in turn, is defined as including 'inter alia, torture and other cruel, inhuman and degrading treatment or punishment, summary or arbitrary executions, disappearances, arbitrary detentions and other major violations of human rights and fundamental freedoms as set out in relevant international human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights'. Council of the European Union, 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.

[5] Council of the European Union, Common Position 2008/944/CFSP (note 4). The EU Common Position goes on to specify that 'Internal repression includes, inter alia, torture and other cruel, inhuman and degrading treatment or punishment, summary or arbitrary executions, disappearances, arbitrary detentions and other major violations of human rights and fundamental freedoms as set out in relevant international human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights'.

[6] The Wassenaar Arrangement 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 and fundamental freedoms'. Wassenaar Arrangement, 'Elements for Objective Analysis and Advice Concerning Potentially Destabilising Accumulations of Conventional Weapons', adopted in 2004 and revised in 2011. Under Article 7(1) of the ATT, states parties are required to 'assess the potential' for the exported arms to be used, among other things, to 'commit or facilitate a serious violation of international human rights law'. United Nations, 'The Arms Trade Treaty', adopted 2 Apr. 2013, entered into force 24 Dec. 2014.

[7] See International Justice Resource Centre, International Humanitarian Law, [n.d.], <http://www.ijrcenter.org/

killing, torture or inhuman treatment, wilfully causing great suffering, and the extensive destruction or appropriation of property not justified by military necessity.[8] The application of IHL-related concerns to export controls on military goods is a well-established international norm. Indeed, all states have an obligation under Article 1 common to the Geneva conventions of 1949 to 'respect and ensure respect' for IHL. This is widely viewed as creating a requirement that all states take steps to assess whether their arms exports will be used in violation of IHL.[9] Criterion 2 of the EU Common Position requires EU member states to deny an export licence for military goods if 'there is a clear risk that the military technology or equipment to be exported might be used . . . in the commission of serious violations of international humanitarian law'.[10] Similar wording appears in other arms export control instruments, most notably the Wassenaar Arrangement's Best Practice Guidelines and the ATT.[11]

At the EU level, terrorist acts have been defined as acts committed with the aim of 'seriously intimidating a population', 'unduly compelling a government or international organisation to perform or abstain from performing any act', or 'seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation'.[12] Similar wording is employed in the User's Guide of the EU Common Position, which provides guidance on how its eight criteria should be applied.[13] There is no universally agreed definition of terrorism or terrorist acts at the international level.[14] Still, that states should seek to ensure that their exports of military goods do not facilitate acts of terrorism is well-established international practice. Criterion 6 of the EU Common Position requires EU member states to 'take into account' the buyer country's 'support for or encouragement of terrorism' when assessing export licences for military goods.[15] Language on terrorism-related concerns also appears in the Wassenaar Arrangement Best Practice Guidelines and the ATT.[16] Nonetheless, the lack of an internationally agreed definition of terrorism or terrorist acts means that the meaning and consequences of these commitments are less clearly established than those for human rights and IHL.

The application of concerns about human rights, IHL and terrorism to export controls on dual-use items is less clearly established and more uneven than it is for military goods. The main focus of the Dual-use Regulation—and dual-use export control more generally—is to prevent the supply of goods and technologies that might contribute to

international-humanitarian-law/>.

[8] International Committee of the Red Cross (ICRC), *Arms Transfer Decisions: Applying International Humanitarian Law and International Human Rights Law Criteria, a Practical Guide* (ICRC: Geneva, Aug. 2016), p. 24.

[9] See ICRC (note 8).

[10] Council of the European Union, Common Position 2008/944/CFSP (note 4).

[11] The Wassenaar Arrangement 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 ...the laws of armed conflict'. Wassenaar Arrangement (note 6). Under Article 6(3) of the ATT, states parties are obliged to not authorize exports of military goods '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'. In addition, under Article 7(1) of the ATT, states parties are required to 'assess the potential' that the exported arms will be used, among other things, to 'commit or facilitate a serious violation of international human rights law'. United Nations, 'The Arms Trade Treaty' (note 6).

[12] Council of the European Union, Common Position 2001/931/CFSP of 27 December 2001 on the application of specific measures to combat terrorism, *Official Journal of the European Communities*, L344/93, 28 Dec. 2001.

[13] 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, p. 106.

[14] European Parliament, 'Understanding definitions of terrorism', Nov. 2015.

[15] Council of the European Union, Common Position 2008/944/CFSP (note 4).

[16] The Wassenaar Arrangement recommends that exporting states consider the recipient state's 'record of compliance . . . with regard to international obligations and commitments, in particular on the suppression of terrorism' when considering exports of SALW. Wassenaar Arrangement, 'Best Practice Guidelines for Exports of Small Arms and Light Weapons (SALW)', adopted in 2002. 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 an act constituting an offence under international conventions or protocols relating to terrorism to which the exporting State is a Party'. United Nations, 'The Arms Trade Treaty' (note 6).

illegal Weapons of Mass Destruction (WMD) programmes by nation states. The initial push behind the creation of a common EU legal framework in this area was provided by revelations about the role that European companies had played in providing material that assisted the development of Iraq's WMD programmes in the 1990s.[17] Moreover, the EU dual-use list is based on the control lists adopted by the export control regimes—the Australia Group (AG), the Missile Technology Control Regime (MTCR), the Nuclear Suppliers Group (NSG) and the Wassenaar Arrangement dual-use list—and the Chemical Weapons Convention (CWC).[18] The AG, MTCR, NSG and CWC lists consist of items that raise WMD-related concerns. Finally, human rights and IHL do not feature prominently in discussions about the application of dual-use export controls. For example, the Wassenaar Arrangement Best Practice Guidelines relating to dual-use export controls make no reference to human rights or IHL concerns.[19]

Nonetheless, the Dual-use Regulation—and dual-use export controls in general—have always looked beyond issues related to the proliferation of WMD among nation states to both reflect and address broader questions in the fields of national, regional and international security. In particular, the idea that export controls on dual-use items can play a role in preventing acts of terrorism has become firmly established since the terrorist attacks on the United States of 11 September 2011, primarily through the adoption and implementation of UN Security Council Resolution 1540.[20] In addition, the Wassenaar Arrangement dual-use list covers items that could be used in conventional weapon systems as well as several items that are more or less exclusively used by intelligence agencies or law enforcement agencies (LEAs).[21] Moreover, EU-level controls on the export of dual-use items include references to human rights concerns. For example, the guidance language for the EUGEA for telecommunications equipment states that it may only be used if the items in question are not intended 'for use in connection with a violation of human rights, democratic principles or freedom of speech'.[22] In addition, Article 8 of the Dual-use Regulation enables EU member states to place controls on dual-use items not covered by the EU dual-use list 'for reasons of public security or human rights considerations'.[23]

The most substantive link between the Dual-use Regulation and human rights, IHL and terrorism is through Article 12 of the Dual-use Regulation. Article 12 requires EU member states to take account of 'all relevant considerations' when assessing export and brokering licences for dual-use items, including those covered by the EU Common Position.[24] The implication is that all of the concerns detailed in the EU Common

[17] See Davis, I., SIPRI, *The Regulation of Arms and Dual-use Exports: Germany, Sweden and the UK* (Oxford University Press: Oxford, 2002).

[18] Council of the European Union, Council Regulation 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, Annex 1, List of Dual-use Items, *Official Journal of the European Union*, L134, 29 May 2009.

[19] See Wassenaar Arrangement, 'Best Practice Guidelines for the Licensing of Items on the Basic List and Sensitive List of Dual-use items and Technologies', Agreed at the 2006 Plenary.

[20] In particular, UN Security Council Resolution 1540 obliges all states to 'adopt and enforce appropriate laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes'. UN Security Council Resolution 1540, 28 Apr. 2004.

[21] For example, '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, unmanned aerial vehicles (UAVs) are covered by Category 9 of the WA dual-use list. Depending on whether they meet the specifications detailed, this would include UAVs fitted with cameras or sounding systems.

[22] Council of the European Union and European Parliament, 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.

[23] Council of the European Union, Council Regulation (EC) 428/2009 of 5 May 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*, 29 May, 2009.

[24] 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.

Box 2.1. Types of cyber-surveillance technology

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

Intrusion software are used to remotely monitor and, in certain cases, control computers and mobile phones without detection.

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 requirement to store their users' communications data for potential later use by intelligence agencies or LEAs.

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

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

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

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

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).

Position—including those in the fields of human rights, IHL and terrorism—should be taken into account when EU member states are assessing licences for the export of dual-use items. Nonetheless, there is a certain lack of clarity about EU member states' obligations in this area. In particular, Article 6 of the EU Common Position states that exports of dual-use items should be subject to assessment under the EU Common Position criteria, but only 'where there are serious grounds for believing that the end-user of such goods and technology will be the armed forces or internal security forces or similar entities in the recipient country'.[25] This indicates a narrower focus than is implied in the Dual-use Regulation. In addition, the criteria of the EU Common Position and its accompanying User's Guide focus on transfers of military goods to military and security end-users.[26] They do not provide specific guidance on the range of human rights, IHL and terrorism-related concerns that could potentially be raised by exports of dual-use items and exports to civilian end-users.

Human rights, IHL and terrorism-related concerns are being taken into account by EU member states when assessing exports of dual-use items, and particularly exports of items covered by the controls on cyber-surveillance technology that were adopted by the Wassenaar Arrangement in 2012 and 2013 (see below). In 2015, for example, 6 of the 10 EU member states that responded to a survey about the topic indicated that Criterion 2 of the EU Common Position, and particularly 'respect for human rights', was among the criteria most frequently applied when licences for the export of cyber-surveillance technology were denied.[27] However, the lack of clarity about when human rights, IHL and terrorism-related concerns should be applied when assessing exports of dual-use items—and the limited guidance about how this should be done—allows for inconsistencies in EU member states' practices. These inconsistencies appear to encompass both the processes and the outcomes of EU member states' decision-making (see below).

[25] Council of the European Union, Common Position 2008/944/CFSP (note 4).

[26] Council of the European Union, Common Position 2008/944/CFSP (note 4); and Council of the European Union (note 24).

[27] SIPRI and Ecorys, *Final Report: Data and Information Collection for EU Dual-use Export Control Policy Review* (European Commission: Brussels, Nov. 2015), p. 181.

The demand for controls on cyber-surveillance technology

The term 'cyber-surveillance technology' is defined in this paper as referring to the software and hardware used by intelligence agencies and LEAs—or by network operators acting under their direction—to covertly monitor and/or exploit communications data that is stored, processed or transferred via information and communications technologies (ICTs). This includes monitoring the communications of large numbers of people—so-called bulk surveillance—and of individuals or small groups—so-called targeted surveillance. The ICTs might be devices such as computers and mobiles phones or telecommunications networks. There is a range of software, hardware and technology that could be considered as covered by this definition (see box 2.1). However, there is no agreed definition of 'cyber-surveillance technology' and many NGOs, companies and government officials would challenge the one proposed in this paper for being either too wide or too narrow. Some would also argue that other terms, such as 'hacking tools', 'ICT surveillance systems' or 'surveillance tools', provide a more meaningful framework for a policy-focused discussion than 'cyber-surveillance technology' and would either increase or reduce the range of items covered. However, the intention of this paper is to pay particular attention to the software, hardware and technology that have been included in the Wassenaar Arrangement dual-use list since 2012, or have been the subject of serious discussion for inclusion in either that list or the coverage of the Dual-use Regulation. For this reason, the definition excludes 'offensive' forms of malware that are designed to disrupt or damage ICT devices or networks.[28] On these grounds, it also excludes social media analytics, Internet content filtering and blocking systems, probes and Deep Packet Inspection (DPI).[29]

Intelligence agencies and LEAs have always sought to use regulatory and technical tools to ensure that they have the ability to access communications data for law-enforcement and intelligence-gathering purposes. The best established of these regulatory and technical tools are related to Lawful interception (LI). LI is the process by which a network operator is required by a judicial or administrative order to provide communications data on one or more of its users to a monitoring centre operated by an LEA or intelligence agency.[30] Most states have laws in place that require network operators to comply with LI requests, and 'LI systems' are used by network operators to assist with meeting these requests.[31] Most states also require network operators to store certain types of communications data for potential later use. 'Data retention systems' are used by network operators to assist with meeting these obligations.[32] International and national standards have been developed that specify how LI systems and data retention systems should operate.[33] Some of these technical standards

[28] The use of offensive malware is regulated by other legislative tools and, to date, they have not been considered for inclusion in dual-use export controls at the Wassenaar Arrangement or EU level.

[29] Probes are used to collect data as it passes through a communications network. DPI is used to examine the content of data as it passes through a communications network. Probes and DPI are used in a range of both surveillance and non-surveillance systems. See CISCO, *Catalyst 6500 Series Switches Lawful Intercept Configuration Guide* (CISCO: San Jose, CA, 2007); and Geere, D., 'How Deep Packet Inspection works', Wired, 27 Apr. 2012. DPI is included in the EU sanctions on Iran, Syria and Venezuela (see below). However, there are currently no discussions about including DPI—or social media analytics, Internet content filtering and blocking systems, and probes—in the Wassenaar Arrangement dual-use list or the Dual-use Regulation.

[30] See Frost & Sullivan, 'Lawful interception: A mounting challenge for service providers and governments', Press release, 16 May 2011; and Vodafone, 'Law enforcement disclosure report', Feb. 2015.

[31] See Utimaco, *Utimaco LIMS: Lawful Interception of Telecommunication Services* (Utimaco Safeware AG: Aachen, Germany: Feb. 2011).

[32] See Utimaco (note 31).

[33] These include international standards drawn up by the European Telecommunications Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP), as well as national standards, such as the 'Technical Guideline for implementation of legal measures for monitoring telecommunications and to information requests for traffic data' (TR TKÜV) standards developed in Germany, the American National Standards Institute (ANSI) standards developed in the USA and the System of Operative Investigative Measures (SORM) standards developed in Russia.

provide some level of protection against human rights abuses.[34] Moreover, certain LI systems have in-built capabilities that can help to prevent human rights abuses.[35] However, these technical standards do not specify which government agencies should be able to use these powers or the mechanisms that should govern their use. In addition, states sometimes require a network operator to provide them with some form of 'direct access' to all communications data.[36] In such cases, international and national standards on how LI systems and data retention systems should operate are effectively bypassed.[37]

It is widely agreed that something fundamental has changed in recent years with regard to the way in which intelligence agencies and LEAs collect and use communications data. However, there is a lack of agreement about the precise nature of this change.[38] Intelligence agencies and LEAs argue that the key change has been the growing use of 'over-the-top' messaging services, such as Skype and WhatsApp, default end-to-end encryption and the so-called dark web, all of which have made traditional LI processes ineffectual.[39] This is often referred to in the USA as the 'going dark' problem, a scenario in which the government has the legal power but not the technical ability to access a target individual's communications data.[40] In response, intelligence agencies and LEAs are seeking to force companies—including providers of over-the-top messaging services and device manufacturers—to decrypt encrypted communications data.[41] They are also becoming increasingly reliant on different methods of 'device compromise', such as intrusion software, IMSI catchers and digital forensics, which allow direct access to a target individual's mobile phone or computer.[42] Conversely, NGOs and civil rights activists tend to argue that the key change has been the exponential growth in the volume of communications data that individuals are generating and sharing about themselves—both consciously and unconsciously—through their use of mobile telephones, social media and other Internet-based tools.[43] This has been coupled with a significant expansion in the range of tools that intelligence agencies and LEAs have for collecting and analysing this data. As a result, through the use of IP network surveillance systems and monitoring centres, governments are able to identify and track target individuals in a way that would have been unthinkable 10 years ago.[44]

[34] In particular, ETSI technical standards on LI state that 'Law Enforcement Network systems' should never be integrated 'directly into the public network architecture'. In contrast, SORM technical standards on LI do not contain these types of safeguards and are generally seen as being more prone to facilitating human rights abuses. ETSI, 'Lawful interception (LI): Concepts of interception in a generic network architecture (ETSI TR 101 943 V2.2.1)', Nov. 2006; and Privacy International, *Private Interests: Monitoring Central Asia*, Special report (Privacy International: London, Nov. 2014).

[35] E.g., Ericsson's 'Lawful Interception Solution' is designed to limit the number of people who can be intercepted simultaneously. Purdon, L., *Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems*, Case Study—Ericsson (IHRB: London, Nov. 2014).

[36] EU-based network operators have been criticized for allowing the states where they operate to have direct access to their communication networks. See Galperin, G., 'Swedish telecom giant Teliasonera caught helping authoritarian regimes spy on their citizens', Electronic Frontier Foundation, 18 May 2012.

[37] See Privacy International, *Study on Telecommunications and Internet Access Sector*, Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Privacy International, Nov. 2016).

[38] See Anderson, D., *A Question of Trust: Report of the Investigatory Powers Review* (Her Majesty's Stationery Office: London, June 2015).

[39] See Hess, A., Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, 'Statement before the House Oversight and Government Reform Committee, Subcommittee on Information Technology', 9 Apr. 2015.

[40] Taylor, J. M., 'Shedding light on the "going dark" problem and the encryption debate', *University of Michigan Journal of Law Reform*, vol. 50, no. 2 (2016).

[41] See Acosta, L., *Government Access to Encrypted Communications: Comparative Summary* (US Library of Congress, Washington, DC, May 2016).

[42] Anderson, D. (note 38).

[43] Anderson, D. (note 38).

[44] Anderson, D. (note 38).

The cyber-surveillance technologies listed in box 2.1 are widely used by the authorities in virtually all states—including EU member states—for intelligence-gathering or law enforcement purposes. For example, in 2015 it was reported that government agencies in Cyprus, the Czech Republic, Germany, Hungary, Italy, Luxembourg, Poland and Spain were using intrusion software.[45] In addition, EU-based companies are market leaders in the development, production and sale of all of these cyber-surveillance technologies. However, leading producers can also be found in the USA, Israel and—increasingly—China.[46] Among the EU-based companies are: (*a*) large military contractors, such as Thales and BAE Systems, which produce a wide range of cyber-surveillance technology, including IP network surveillance systems and monitoring centres, for intelligence agencies and LEAs; (*b*) large ICT companies, such as Nokia and Ericsson, which produce telecommunications networks for network operators and are legally required to have LI systems and data retention systems 'built in' or to enable an interface for their use; and (*c*) smaller ICT firms, such as Gamma International and Hacking Team, which specialize in the production of certain types of cyber-surveillance technology, such as IMSI catchers and intrusion software, for intelligence agencies and LEAs. These companies are diverse in terms of their size and level of exposure to export controls. In addition, they do not form any kind of coherent 'sector' and there is no single industry association at either the national or the EU level to which they all belong.[47]

It is generally accepted that in a well-functioning state with effective measures of oversight and control most of the cyber-surveillance technologies listed in box 2.1 can play an important role in counterterrorism and crime fighting. However, the use of cyber-surveillance technology raises a range of security concerns. For example, in the USA concerns have been raised about the actual or potential use of intrusion software and IMSI catchers in the theft of government and commercial secrets.[48] In addition, all of the cyber-surveillance technologies listed in box 2.1 have been linked with violations of human rights. The most concrete examples involve violations of the right to privacy. Indeed, the use of most of these systems by states that lack effective measures of oversight and control can—in itself—be seen as constituting a potential violation of the right to privacy. Numerous allegations have also been made about more serious violations of human rights, including freedom from unlawful detention and freedom from torture.[49] However, many of these allegations are based on evidence that the intelligence agencies or LEAs in the states where these abuses occur are using these systems, rather than any explicit direct connection. Indeed, given the nature of the systems and the states involved, establishing clear links can be extremely difficult.[50] Examples of cyber-surveillance technology being used in connection with violations of IHL and acts of terrorism are even harder to establish. The cyber-surveillance technologies listed in box 2.1 could be used in these ways but no documented cases have come to light.

[45] Privacy International, 'Surveillance company hacking team exposed', 7 July 2015.

[46] See Anderson, C., 'Considerations on Wassenaar Arrangement Control List additions for surveillance technologies', Access, 13 Mar. 2015; and Insider Surveillance, *The Little Black Book of Electronic Surveillance, 2015* (Insider Surveillance: Feb. 2015).

[47] Instead, some of the companies are members of ICT-focused associations, such as Digital Europe, IT-focused associations, such as BitKom, or defence and security associations, such as ASD, while others are not members of any association.

[48] Clapper, J. R., Director of National Intelligence, Statement for the Record, 'Worldwide Threat Assessment of the US Intelligence Community', US Senate Select Committee on Intelligence, 23 Mar. 2013; and Stein, J., 'New eavesdropping equipment sucks all data off your phone', *Newsweek*, 22 June 2014.

[49] Citizen Lab, 'Mapping hacking team's "untraceable" spyware', 17 Feb. 2014; Marquis-Boire, M. et al., 'You only click twice: FinFisher's global proliferation', Citizen Lab, 13 Mar. 2013; and Human Rights Watch (HRW), *They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia* (HRW: New York, 2014).

[50] McKune, S. A., 'Human rights and technologies: The impact of digital surveillance and intrusion systems on human rights in third countries', Hearing of the European Parliament, 21 Jan. 2015.

The manufacture and export of cyber-surveillance technology by EU-based companies gained public attention in 2009 following reports that Nokia Siemens Networks (NSN) had supplied LI systems to one of the main mobile phone network operators in Iran.[51] The communications data collected, in conjunction with information assembled from other cyber-surveillance technologies, was reportedly used by the Iranian Government to identify and monitor opposition activists who were later subjected to torture and unlawful detention.[52] However, the issue gained a greater level of attention in the wake of the Arab Spring in 2011. A series of NGO and media reports highlighted the role of EU-based companies in the supply of cyber-surveillance technology to a number of affected states, such as Bahrain, Libya and Syria.[53] These systems were allegedly used in connection with violations of a range of human rights by the recipient state's security forces.[54] In the years since, there have been continuing reports of national authorities in a number of states using cyber-surveillance technology in ways that appear to violate human rights.[55] In response, EU member states, MEPs and NGOs have called for steps to be taken to restrict the export and use of cyber-surveillance technology.[56]

The expansion of controls in the Wassennar Arrangement

The Wassenaar Arrangement was established in 1996 and aims to promote 'transparency and greater responsibility' regarding transfers of military goods and dual-use items. It maintains detailed control lists in both areas.[57] Since the 1990s, systems that employ a certain standard of encryption have been covered by Category 5 of the Wassenaar Arrangement's dual-use list.[58] Prior to 2011 several cyber-surveillance technologies, including digital forensics and intrusion software, were covered by Category 5 of the Wassenaar Arrangement dual-use list on these grounds.[59] LI systems and data retention systems also employ a level of encryption that can make them subject to dual-use export controls.[60] However, as detailed above, the end-user for LI systems or data retention systems is usually a network operator in the recipient country. As a result, it is unclear whether—and if so how—human rights, IHL and terrorism-related concerns are being addressed when assessing these exports, particularly in the case of EU member states that view the EU Common Position criteria as only applicable to exports to military and security-related end-users.

After 2011, several cyber-surveillance technologies were added to the Wassenaar Arrangement dual-use list. Controls on IMSI catchers were added in December 2012 and controls on intrusion software and IP network surveillance systems in December 2013. In December 2014 these items were added to the EU dual-use control list. The

[51] Roome, B., 'Provision of lawful intercept capability in Iran', Nokia, 22 June 2009.

[52] Rhoads, C. and Chao, L., 'Iran's web spying aided by western technology', *Wall Street Journal*, 22 June 2009.

[53] Silver, V. and Elgin, B., 'Torture in Bahrain becomes routine with help of Nokia Siemens', Bloomberg, 23 Aug. 2011; Business and Human Rights Resource Centre, 'Amesys lawsuit (re Libya)', [n.d.], accessed 2 Aug. 2015; and Silver, V., 'Italian firm exits Syrian monitoring project, Republica says', Bloomberg, 28 Nov. 2011.

[54] Several studies have also argued that access to advanced telecommunications networks—and particularly social media tools—operated as a 'source multiplier' that contributed to the size of the Arab Spring. See e.g. Eriksson, M. et al., *Social Media and ICT During the Arab Spring* (FOI: Stockholm, July 2013).

[55] See Omanovic, E., 'Macedonia: Society on Tap', Privacy International; Scott-Railton, J. et al., 'Reckless III: Investigation into Mexican mass disappearance targeted with NSO spyware', Citizen Lab, 10 July 2017; and Human Rights Watch, 'Ethiopia: New Spate of Abusive Surveillance', 6 Dec. 2017.

[56] 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.

[57] Wassenaar Arrangement, 'Introduction', <http://www.wassenaar.org/>.

[58] See Saper, N., 'International cryptography regulation and the global information economy', *Northwestern Journal of Technology and Intellectual Property*, vol. 11, no. 7 (Fall 2013).

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

[60] See Utimaco (note 31).

controls on IMSI catchers and IP network surveillance systems do not appear to have generated a significant amount of debate or confusion. However, following the adoption of the controls on intrusion software companies and researchers working in IT security began to voice concerns that the language used describes not just the types of systems used by intelligence agencies and LEAs, but also systems and processes that are essential to IT security, particularly systems used for 'penetration testing' and processes of 'vulnerability disclosure'.[61] However, others have argued that, if properly applied, the controls should not have any significant effects in these areas.[62] Moreover, companies in the EU that export the kind of systems that were the originally intended target of the controls are aware that they are covered and are applying for export licences.[63]

The debate grew more intense after the USA published proposed implementation language in May 2015 that appeared to confirm some of the fears of the IT security community.[64] The strength of the response from its domestic IT sector led the USA to delay adopting the intrusion software controls. This was in spite of the fact that national implementation of the control lists is one of the obligations associated with being a Wassenaar Arrangement participating state.[65] In 2016 and 2017 the USA also proposed amendments to the content of the intrusion controls at the Wassenaar Arrangement.[66] In 2016 opposition from other participating states meant that only minor changes were agreed.[67] However, in 2017 more detailed explanatory notes were added to the controls on intrusion software, specifying that they did not apply to items that are designed to provide 'software updates' as well as 'vulnerability disclosure' and 'cyber incident response'.[68] At the time of writing it is unclear whether these clarifications will meet the concerns raised by companies and researchers working in IT security.

Separate to the debate about the clarity of the controls has been a discussion on how they have been applied by EU member states, particularly in relation to decisions to approve or deny export licences. Figures released in early 2017 indicate that EU member states have issued 317 licences for the export of IMSI catchers, IP network surveillance and intrusion software since the beginning of 2014 and denied 14 applications.[69] The fact that 30 per cent of the approved licences were for exports to countries classed as 'not free' by the Freedom House index has been held up as evidence of the need for EU member states to take a more restrictive approach.[70] Particular decisions by EU member states have also been criticized by NGOs, such as Denmark's reported approval of an export of IP network surveillance systems to Qatar and the UK's reported approval of the export of IMSI catchers to Turkey.[71] Questions have also

[61] 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 tools' are used to test the security of a network by simulating attacks against it in order to locate vulnerabilities. 'Vulnerability disclosure' is the means through which software vulnerabilities are identified and reported.

[62] See Anderson, C. (note 46).

[63] See 'Hacking team complies with Wassenaar Arrangement Export Controls on Surveillance and Law Enforcement/Intelligence Gathering Tools', Hacking Team, 25 Feb. 2015.

[64] See e.g., 'Google, the Wassenaar Arrangement, and vulnerability research', Google Online Security Blog, 20 July 2015.

[65] Wassenaar Arrangement, 'Public Documents Volume 1: Founding Documents', Feb. 2017.

[66] Cardozo, N. and Galperin, E., 'Victory! State Department will try to fix Wassenaar Arrangement', Electronic Frontiers Foundation, 29 Feb. 2016. However, due to resistance from other participating states, only minor adjustments to the controls were adopted. Thomson, I., 'Wassenaar weapons pact talks collapse leaving software exploit exports in limbo', The Register, 21 Dec. 2016.

[67] Thomson (note 66).

[68] Wassenaar Arrangement, 'List of Dual-use Goods and Technologies and Munitions List', 7 Dec. 2017.

[69] See Gjerding, S. and Skou Andersen, L., 'How European spy technology falls into the wrong hands', The Correspondent, 23 Feb. 2017. The figures only cover 17 EU member states, since 11 did not provide the requested data.

[70] See Gjerding and Skou Andersen (note 69).

[71] Skou Andersen, L., 'Dansk firma sælger internetovervågning til oliediktatur' [Danish company sells Internet

been asked about the consistency of EU member states' application of the controls, in terms of both whether to approve particular licences and the type of export licence companies are required to use when submitting applications. In particular, reports have indicated that while Germany has been controlling exports of intrusion software using individual licences, Italy has used global licences that are valid for multiple shipments, years and destinations.[72]

EU-based producers of cyber-surveillance technology have responded in different ways to the new licensing requirements, possibly due to the significant variations in their size, previous experience with export controls and the potential sensitivities of their exports. FinFisher, which produces intrusion software, is reported to have moved its work in this area to offices in states that are not members of the Wassenaar Arrangement.[73] Amseys, which produces IP network surveillance systems, is also reported to have moved its operations, but it is unclear whether this was in response to the application of export controls.[74] Reports also indicate that certain EU-based producers of cyber-surveillance technology have been actively seeking to bypass the new controls and—in certain cases—offering to supply systems to states that are subject to EU sanctions.[75] As noted above, however, other companies appear to be seeking to abide by the new controls and have not moved.[76] One EU-based producer of IP network surveillance systems has even noted that being subject to export controls has certain advantages.[77] In particular, it creates a greater potential for political and economic support from the exporting company's national government should a contract need to be cancelled due to changing conditions in the recipient state.

In 2015 Germany—citing Article 8 of the Dual-use Regulation—adopted national controls on monitoring centres and data retention systems.[78] The controls apply to supplies of complete systems and to technical assistance, which means that services provided for previously installed systems might also be subject to control. Germany stated that the controls would only affect a small number of companies, most of which were already subject to export controls.[79] Germany also stated that these controls were intended to prevent the use of this technology for 'internal repression' and the suppression of human rights, and that it would promote their wider adoption within the Wassenaar Arrangement.[80] However, they have not been added to the Wassenaar Arrangement dual-use list. A number of EU member states and NGOs have called for consideration to be given to making other cyber-surveillance technologies subject to dual-use export controls at the Wassenaar Arrangement, such as 'undersea fibre-optic cable taps, monitoring centres, and mass voice / speaker recognition technologies'.[81]

surveillance to oil dictatorship], Information, 26 Aug. 2016; and Cox, J., 'The UK granted spy tech export to Turkey amid its massive crackdown on dissent', Vice Motherboard, 19 July 2017.

[72] Page, K., 'Six things we know from the latest FinFisher documents', Privacy International, 15 Aug. 2014; and Currier, C. and Marquis-Boire, M., 'A detailed look at hacking team's emails about its repressive clients', The Intercept, 7 July 2015.

[73] 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 Sonntag, 1 Aug. 2015.

[74] Paquette, E., 'Les mercenaires de la cyber-guerre', L'express, 22 Nov. 2014.

[75] Boazman, S., 'How we revealed the surveillance world's illegal trades', Al Jazeera, 10 Apr. 2017.

[76] See Hacking Team (note 63).

[77] SIPRI and Ecorys (note 27), p. 181.

[78] BMWI, 'Anlage AL zur Außenwirtschaftverordnung' [Annex AL to the German Foreign Trade Regulations], July 2015.

[79] BMWI, 'Verordnung der Bundesregierung Vierte Verordnung zur Änderung der Außenwirtschaftsverordnung' [Regulation of the Federal Government: Fourth Regulation amending the Foreign Trade Regulations], 17 July 2015.

[80] BMWI, 'Gabriel: Export von Überwachungstechnik Wird Starker Kontrolliert' [Gabriel: Export of Surveillance Technology Under Strong Controls], 8 July 2015; and Stupp, S., 'Germany leaves Brussels behind on surveillance tech export controls', EurActiv, 10 July 2015.

[81] Amnesty International, Digitale Gesellschaft, FIDH (International Federation for Human Rights), Human Rights Watch, Open Technology Institute (at New America), Privacy International and Reporters sans frontiers, 'An open letter to the members of the Wassenaar Arrangement', 2 Dec. 2014.

However, it does not appear that these items have been the subject of serious discussion within the Wassenaar Arrangement.

In early 2017 the Head of the Wassenaar Arrangement indicated that surveillance systems and other 'new technologies'—such as drones and artificial intelligence—would remain on the regime's agenda due to their 'potentially disrupting impacts'.[82] This indicates that there may be scope for additional cyber-surveillance technologies to be included on the Wassenaar Arrangement dual-use list. However, the inclusion of cyber-surveillance technology on the list has, to date, been justified on the basis of national security concerns. For example, the controls on intrusion software were proposed on the grounds that these tools 'may be detrimental to international and regional security and stability'.[83] Monitoring centres, data retention systems and the other items proposed by NGOs for inclusion on the Wassenaar Arrangement dual-use list are almost exclusively of interest because of their human rights-related concerns. Adding these systems to the list on these grounds alone would be potentially problematic. The regime's mandate for including items on the dual-use list on human rights grounds is unclear and doing so would probably be opposed by certain participating states. This leaves the EU as the primary location for a potential expansion of controls on cyber-surveillance technology.

The expansion of controls in the EU

Since 2011 EU member states, MEPs and NGOs have called for steps to be taken to place restrictions on the export and use of cyber-surveillance technology.[84] A number of policy options have been discussed in different parts of the Commission, the European Parliament and the Council. These include developing improved corporate social responsibility (CSR) guidelines for companies supplying cyber-surveillance technology, and providing dissidents with systems that would enable them to evade detection by intelligence agencies and LEAs. However, the CSR guidelines produced to date have focused on the ICT sector as a whole without engaging substantially with the issue of cyber-surveillance technology.[85] In addition, the plan to supply dissidents with surveillance-evading systems was dropped, reportedly over fears about interfering in the internal affairs of states.[86] Increasingly, the focus has shifted to using dual-use export controls to address this set of challenges.

The focus on dual-use export controls reflects the clear mandate that the EU has to act in this area. EU member states have delegated powers in the field of dual-use export controls to the EU level through two legislative instruments: EU sanctions and the Dual-use Regulation. EU sanctions form part of the EU's Common Foreign and Security Policy (CFSP), one of the areas of 'special' EU competence.[87] Most EU sanctions cover the trade in military goods. Some, including those on Iran and Russia, also cover the trade in certain dual-use items. The Dual-use Regulation forms part of the EU's 'common commercial policy', one of the areas of 'exclusive' EU competence.[88] In addition, the use of dual-use export controls as a tool for restricting the

[82] Cercle Diplomatique, 'Global risks have greatly expanded', no. 1 (2017).

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

[84] European Parliament (note 55).

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

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

[87] Measures adopted in areas of 'special' EU competence are legally binding on member states. However, member states are free to determine their mechanisms of implementation and the EU has no legal powers to sanction non-compliance.

[88] The EU alone is able to legislate in areas of 'exclusive' EU competence—except where member states have been specifically empowered to do so—and any measures adopted are legally binding and directly applicable throughout the EU.

supply of cyber-surveillance technology has become a focus for NGOs working on human rights and privacy issues. In 2014 the Coalition Against Unlawful Surveillance Exports (CAUSE) was set up by Amnesty International, Digitale Gesellschaft, the International Federation for Human Rights, Human Rights Watch, the New America Foundation's Open Technology Institute, Privacy International and Reporters without Borders.[89] CAUSE has called for the EU to make cyber-surveillance technology subject to export controls and to oblige member states' authorities to take account of human rights issues when taking licensing decisions.

In 2011 the EU sanctions on Iran and Syria were expanded to include cyber-surveillance technology.[90] The accompanying Council Regulations listed the technology covered. In addition to capturing many of the cyber-surveillance technologies in box 2.1, they placed restrictions on a number of sub-systems that are used in both surveillance and non-surveillance systems, including DPI.[91] However, rather than banning exports of these systems, the sanctions created a requirement for companies to apply for licences for their export to Iran and Syria, and an obligation on EU member states to deny such licences in certain circumstances.[92] In November 2017 a similar set of controls was included in the EU's newly adopted sanctions on Venezuela.[93] However, while the list of cyber-surveillance technologies is the same as for the Iran and Syria sanctions, the scope of the controls for Venezuela is narrower. In particular, the Iran and Syria sanctions state that denials should be issued if the EU member state has 'reasonable grounds to determine that the equipment, technology or software in question would be used for monitoring or interception . . . of internet or telephone communications'.[94] By contrast, the Venezuela sanctions state that denials should be issued if the EU member state has 'reasonable grounds to determine that the equipment, technology or software in question would be used for internal repression'.[95] In addition, while the Iran and Syria sanctions state that the list of surveillance technologies shall cover 'equipment, technology or software which may be used for the monitoring or interception of internet or telephone communications', the Venezuela sanctions state that it shall cover 'equipment, technology or software intended primarily' for these uses.[96]

The review of the Dual-use Regulation began in 2011. In 2014 the European Commission issued a Communication setting out proposals for the review, building on an earlier green paper and round of stakeholder consultation.[97] In 2015 a public consultation and a data collection and analysis project were conducted on the current impact of the Dual-use Regulation and the potential impact of the various review options

[89] See Omanovic, E., *NGO Coalition Calls on EU to Update Dual Use Regulation to Protect Human Rights* (Privacy International: London, June 2015).

[90] Council of the European Union, Council Decision 2011/235/CFSP of 12 April 2011 concerning restrictive measures directed against certain persons and entities in view of the situation in Iran, *Official Journal of the European Union*, L100/51, 14 Apr. 2011; and 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*, L319/55, 2 Dec. 2011.

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

[92] Council Regulation (EU) 359/2011 of 12 April 2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran, *Official Journal of the European Union*, L100/1, 14 Mar. 2011; and Council Regulation (EU) 36/2012 of 18 January 2012 concerning restrictive measures in view of the situation in Syria and repealing Regulation (EU) 442/2011, *Official Journal of the European Union*, L16/1, 19 Jan. 2012.

[93] Council Decision (CFSP) 2017/2074 of 13 November 2017 concerning restrictive measures in view of the situation in Venezuela, *Official Journal of the European Union*, L295/60, 14 Nov. 2017; and Council Regulation (EU) 2017/2063 of 13 November 2017 concerning restrictive measures in view of the situation in Venezuela, *Official Journal of the European Union*, L295/21, 14 Nov. 2017.

[94] Council Regulation (EU) 359/2011 of 12 April 2011; and Council Regulation (EU) 36/2012 of 18 January 2012 (note 92) [emphasis added].

[95] Council Regulation (EU) 2017/2063 of 13 November 2017 (note 93) [emphasis added].

[96] Council Regulation (EU) 359/2011 of 12 April 2011 (note 92); Council Regulation (EU) 36/2012 of 18 January 2012 (note 92); and Council Regulation (EU) 2017/2063 of 13 November 2017 (note 93) [emphasis added].

[97] 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.

being considered.[98] These fed into an assessment of the social and economic impact of the Dual-use Regulation and the review options.[99] The Commission presented its draft regulatory proposal in September 2016 in the form of a 'recast' of the Dual-use Regulation.[100] Early in the process, strong commitments were made to use the review to introduce stronger controls on the export of cyber-surveillance technology. 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'.[101] In 2014 the Commission also established a sub-group of the EU's Dual-use Coordination Group (DUCG)—the Surveillance Technology Expert Group (STEG)—to examine issues related to controls on the export of cyber-surveillance technology.[102] During the review process the Commission proposed that the concept of 'human security' should be introduced into the Dual-use Regulation in order to encompass a wider range of human rights and security-related issues.[103] However, both industry associations and NGOs voiced concerns about this approach, noting in particular that human security has never been integrated into regional or international legal instruments and lacks any kind of universally agreed definition.[104]

The Commission's proposal contains several changes that would give human rights, IHL and terrorism-related concerns a more central role in the Dual-use Regulation while also expanding controls on cyber-surveillance technology. First, it would expand the definition of dual-use items to capture cyber-surveillance technology. Second, it would create an EU list of controlled cyber-surveillance technology. Third, it would give human rights and IHL a more central place in the set of criteria that member states apply when assessing export licences. Fourth, it would create a new 'catch-all clause' that would allow member states to apply controls to exports of non-listed dual-use items that may be used in serious violations of human rights or IHL or acts of terrorism, and an accompanying obligation on companies to assess the risk that their exported items will be used in this way.

Since the review of the Dual-use Regulation is subject to the ordinary legislative procedure of the EU, the Commission's proposal will go through a process of trilogue involving the European Commission, the Council and the European Parliament.[105] The European Parliament is preparing a set of amendments to the Commission's proposal, which will form the basis for a negotiating mandate. The Committee for International Trade (INTA) was appointed the Committee responsible for drafting these amend-

[98] European Commission, 'EU Export Control Policy Review: online public consultation report', 23 Nov. 2015; and SIPRI and Ecorys (note 27), p. 181.

[99] European Commission, Commission Staff Working Document, Impact Assessment, Report on the EU Export Control Policy Review, Accompanying the document 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) SWD(2016) 314 final, 28 Sep. 2016.

[100] 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.

[101] Malmström, C., EU Commissioner for Trade, 'Debate at European Parliament in Strasbourg', 24 Nov. 2014. In 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. European Parliament, Report on human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries, 2014/2232(INI).

[102] Coalition Against Unlawful Surveillance (CAUSE), 'A critical opportunity: bringing surveillance technologies within the EU Dual-Use Regulation', 2 June 2015.

[103] 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. According to the European Commission, this would potentially involve 'a clarification of control criteria to take into consideration broader security implications, including the potential effect on the security of persons e.g. through terrorism or human rights violations'. European Commission, *The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World* (European Commission: Brussels, 24 Apr. 2014).

[104] 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 (note 102).

[105] European Parliament, Briefing, EU Legislation in Progress, Review of dual-use export controls, 24 July 2017.

ments by the European Parliament in October 2016, with Klaus Buchner (Greens/EFA, Germany) acting as rapporteur. In addition, the Committee on Foreign Affairs (AFET) was also asked to issue an opinion, with Marietje Schaake (ALDE, the Netherlands) acting as rapporteur.[106] AFET published a Draft Opinion on the proposal in April and May 2017.[107] In total 152 amendments were tabled in AFET. AFET adopted its final Committee Opinion on 31 May 2017, reducing the number of proposed amendments to 38.[108] INTA also published its Draft Report on the proposal in April and May 2017.[109] In total 424 amendments were proposed in INTA. INTA adopted its final Committee Report on 23 November, reducing the number of proposed amendments to 98.[110] INTA also voted against the 'decision to enter into negotiations'. This means that the INTA report will be debated in plenary at the European Parliament and that additional amendments could still be proposed and adopted.[111] The discussion in plenary is due to take place in January 2018. During 2017, the European Commission's proposal was also discussed in the Council, where EU member states have been seeking to agree their own proposed amendments to the Commission's proposal.[112] Once both co-legislators have established their position, discussions can begin between the European Parliament and the Council on how to merge their amendments.

Since the proposal was published other stakeholders have given their views on its content and put forward alternative formulations. The national parliaments of seven EU member states have examined the proposal.[113] Finally, several key stakeholders—particularly NGOs, political groups in the European Parliament and industry associations—have published analyses of the Commission's proposal.

[106] European Parliament/Legislative Observatory, 'Procedure file 2016/0295(COD), Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items, Recast', 3 Oct. 2017.

[107] European Parliament, Committee on Foreign Affairs, Draft Opinion of the Committee on Foreign Affairs to the Committee on International Trade on the 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)0616—C8-0393/2016—2016/0295(COD)), 10 Apr. 2017; and European Parliament, Committee on Foreign Affairs, Amendments 27–152, Draft opinion, Marietje Schaake (PE602.925v01-00), Setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast), Proposal for a regulation (COM(2016)0616—C8-0393/2016—2016/0295(COD)), 9 May 2017.

[108] European Parliament, Committee on Foreign Affairs, Opinion of the Committee on Foreign Affairs for the Committee on International Trade on the 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)0616—C8-0393/2016—2016/0295(COD)) , 31 May 2017.

[109] European Parliament, Committee on International Trade, Draft Report on the 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)0616—C8-0393/2016—2016/0295(COD)), 4 Apr. 2017; European Parliament, Committee on International Trade, Amendments 58–348, Draft report Klaus Buchner (PE602.808v01-00) on the 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), Proposal for a regulation (COM(2016)0616—C8-0393/2016—2016/0295(COD)), 16 May 2017; and European Parliament, Committee on International Trade, Amendments 349–424, Draft report Klaus Buchner (PE602.808v01-00) on the 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), Proposal for a regulation (COM(2016)0616—C8-0393/2016—2016/0295(COD)), 16 May 2017.

[110] European Parliament, Report on the 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)0616—C8-(0393/2016—2016/0295COD)), Brussels, 5 Dec. 2017.

[111] European Parliament, Committee on International Trade, 'Results of roll-call votes: 23/11/2017', 23 Nov. 2017, p. 4; and European Parliament, 'Ordinary legislative procedure. Interinstitutional negotiations for the adoption of EU legislation', [n.d.].

[112] European Commission, 'Dual-use export controls', [n.d.].

[113] The 7 national parliaments that have examined the proposal are those of Finland, Germany, Ireland, Poland, Slovakia, Sweden and the UK.

3. The Commission's proposal and the responses made

Expanding the definition of 'dual-use items'

The definition of 'dual-use items' used in the proposal retains the existing framing language from the Dual-use Regulation. This defines dual-use items as 'items, including software and technology, which can be used for both civil and military purposes and shall include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices'. However, the definition in the proposal states that the term also includes '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'.[114] The proposal later defines cyber-surveillance technology as:

> items specially designed to enable the covert intrusion into information and telecommunication systems with a view to monitoring, extracting, collecting and analysing data and/or incapacitating or damaging the targeted system. This includes items related to the following technology and equipment: (*a*) mobile telecommunication interception equipment; (*b*) intrusion software; (*c*) monitoring centers; (*d*) lawful interception systems and data retention systems; and (*e*) digital forensics.[115]

An earlier draft of the proposal, which was leaked in the summer of 2016, also included biometrics, location tracking devices, probes and DPI in this definition.[116] This provoked concern from industry and a number of EU member states about the potential impact on EU-based companies, particularly in the ICT sector. These categories did not appear in the September version of the proposal.[117]

However, even the narrower definition of cyber-surveillance technology includes a number of items that have not been subject to control at the Wassenaar Arrangement, such as LI systems and digital forensics. As a result, the proposed definition has been the subject of considerable debate. Including LI systems in the EU's definition of cyber-surveillance technology could have a significant impact on the EU's ICT sector. As noted above, a company supplying a telecommunications network to a network operator is obliged either to include an LI system or to enable one to be installed. As such, any standards applied to the export of LI systems could potentially apply to exports of telecommunications networks. Industry representatives have argued that such a step would place EU-based suppliers at a competitive disadvantage in comparison with suppliers outside the EU.[118] Nor would it necessarily enhance human rights in the recipient, since LI systems—potentially with fewer restrictions in place—can be provided by suppliers based outside the EU. The EU is home to three of the world's five manufacturers of telecommunications networks: Ericsson, Nokia and Alcatel-Lucent. The other two are Huawei and ZTE Corp in China.

Several stakeholders have also voiced concern that the definition of cyber-surveillance technology included in the Commission's proposal might inadvertently capture items that are either vital to IT security or are used by human rights defenders to evade surveillance when operating in repressive regimes. In this context, NGOs have drawn

[114] European Commission (note 100), p. 19.

[115] European Commission (note 100), pp. 22–23.

[116] 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>.

[117] 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.

[118] SIPRI and Ecorys (note 27), p. 193.

attention to the inclusion of digital forensics in the definition of cyber-surveillance technology, arguing that the term could capture systems and processes that are essential to IT security.[119] AFET has also indicated that digital forensics should be deleted from the definition of cyber-surveillance technology.[120] Moreover, the Greens/EFA group in the European Parliament has argued that 'technologies capable of promoting and protecting human rights as well as security testing tools without criminal intent' should be exempted from control under the Dual-use Regulation.[121]

The lack of consistency in the definition put forward in the Commission's proposal has also been raised. For example, the reference to cyber-surveillance technology is a potential source of confusion. In the context of export controls 'technology' generally refers to items that are used 'for the "development", "production" or "use" of goods under control'.[122] The implication is that the language in the proposal would mean that controls do not apply to the actual cyber-surveillance software and hardware, but only to items used in their development, production or use. Industry associations have urged that the focus should remain on 'dual-use products, as they have been defined traditionally and in the current Regulation'.[123] However, the Wassenaar Arrangement dual-use list already includes a number of items that are predominantly used by intelligence agencies and LEAs. It could therefore be argued that the focus of dual-use export controls has already shifted beyond the civilian- or military-use paradigm to encompass systems used by intelligence agencies and LEAs. The definition in the proposal goes some way towards reflecting this shift but there is a lack of consistency in the approach. In particular, it retains the overall framing language of the current definition of dual-use items, which states that they are items that 'can be used for both civil and military purposes'. However, the definition of cyber-surveillance technology includes systems that are predominantly used by intelligence agencies and LEAs. Intrusion software and IMSI catchers, for instance, are seldom if ever used for either civilian or military purposes. In addition, the definition also includes items that are mainly used for civilian purposes, particularly LI systems and data retention systems, which are primarily used by network operators and are also seldom if ever used for military purposes.

Creating an EU list of controlled cyber-surveillance technology

The proposal also includes the adoption of an EU control list for 'Other items of cyber-surveillance technology' and creates the potential to add items to this list at the initiative of the Commission through the use of delegated powers. The only items that would initially be included on this new EU list are monitoring centres and data retention systems, which are defined using the same language as Germany used when it added these items to its national controls in 2015. However, the proposal states that additional cyber-surveillance technologies can be added 'due to risks that the export of such items may pose as regards the commission of serious violations of human rights or international humanitarian law or the essential security interests of the Union and its Member States.'[124] The range of items that could be added would presumably be those covered by the definition of cyber-surveillance technology provided elsewhere

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

[120] European Parliament (note 108), p. 11.

[121] The Greens / EFA group in the European Parliament, 'No spyware for dictators', [n.d.].

[122] Council of the European Union (note 18), p. 20.

[123] Digital Europe, 'European Commission proposed recast of the European Export Control Regime: Making the rules fit for the digital world', 24 Feb. 2017.

[124] European Commission (note 100).

in the proposal and which aren't already included in the dual-use list—LI systems and digital forensics.

This would, for the first time, create an EU control list for dual-use items that is not drawn from one of the multilateral export control regimes, and give the Commission the ability to take the lead on adding items to the EU dual-use list. It would also make the risk of misuse grounds for including items on the EU dual-use list. The multilateral regimes tend to balance concern about misuse against other factors when adding items to their control list, such as the ability to accurately describe the item and its wider availability.[125] Including items on the EU dual-use list that are not drawn from the control lists of the multilateral export control regimes is something that EU member states and industry have previously sought to avoid. Their key concerns are that this might have a negative impact on the competitiveness of EU-based companies, and that it might generate confusion among non-EU states that value the EU dual-use list as a synthesis of the regimes' control lists and implement it nationally. However, as noted above, the prospect of the Wassenaar Arrangement adopting additional controls on cyber-surveillance technology beyond those that have been created to date looks limited at present.

NGOs and the European Parliament have broadly welcomed the idea of creating an EU control list for cyber-surveillance technology. The Greens/European Free Alliance (EFA) group in the European Parliament has called for 'a broad list of technology' to be created that covers 'all relevant software and hardware elements that could facilitate human rights abuses . . . particularly technologies used for mass-surveillance, monitoring, intrusion, tracking, tracing and censoring'.[126] However, Access Now and other NGOs have emphasized the need for an open and transparent process that takes account of the expertise of all relevant stakeholders, including civil society and experts in human rights, when adding new items to the list.[127] INTA has also highlighted the need to ensure that the process of drafting new control list items is carried out in an inclusive manner that involves 'relevant international bodies and particularly civil society'.[128] Regardless of whether the concerns raised about the unintended consequences of the controls on intrusion software are justified, the case definitely highlights the complexity of seeking to establish new export controls in this area, and the need to consult with all relevant stakeholders when drafting language. However, AFET has argued that any procedures that are put in place need to allow for items to be added to the EU list rapidly, potentially through the use of urgency procedures 'to allow for quick responses to changes on the ground in third countries or in terms of new technological developments requiring scrutiny', while INTA have also indicated that such measures may be relevant in certain circumstances.[129]

In contrast, industry associations have voiced concerns about the creation of EU controls that deviate from the lists established in the different export control regimes. In particular, Business Europe has argued that adopting an EU list that is not implemented by non-EU member states could 'harm the competitiveness of EU companies'.[130] Citing similar concerns, the European Chemical Industry Council (Cefic), Digital Europe and Aeronautic, Space, Defence and Security Industries in Europe

[125] According to the Wassenaar Arrangement, when adding items to the list, 'dual-use items should also be evaluated against the following criteria: Foreign availability outside Participating States, The ability to control effectively the export of the goods, The ability to make a clear and objective specification of the item, [and whether it is] Controlled by another regime.' Wassenaar Arrangement, 'Criteria for the selection of dual-use items', 2005.

[126] The Greens / EFA group in the European Parliament (note 121).

[127] Access Now, Amnesty International et al., 'Open NGO letter to EU member states and institutions regarding the export of surveillance equipment', July 2017.

[128] European Parliament (note 110), p. 57.

[129] European Parliament (note 108), p. 3; and European Parliament (note 110), p. 139.

[130] Business Europe, 'Key points for Communication on Export Controls on Dual-Use Items', 27 June 2017.

(ASD) have also argued that the only items that should be included on the EU dual-use list are those that have already been adopted in one of the multilateral export control regimes.[131] Digital Europe noted that: 'any update of the EU list of dual-use items must conform to commitments that Member States have with export control regimes in countries located outside the EU'.[132] In addition, the House of Commons Select Committee on European Security in the UK has voiced concerns about the adoption of an EU list, noting that it represents a 'significant departure from the established position where control lists are derived from the various international export control regimes'.[133] The committee has also indicated that it is sceptical about the extension of Commission powers that would be created by an ability to propose additions to the list.[134]

Including human rights and IHL in the assessment criteria

The Commission's proposal also includes new language on the range of concerns that EU member states must address when assessing dual-use export licences. It notes 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'.[135] If this language is adopted, it will create an explicit reference to human rights and IHL issues in the Dual-use Regulation. However, the current draft also removes any reference to the Common Position, which means that the Dual-use Regulation would not include a link to the Common Position's criteria or the guidance provided by its accompanying User's Guide. The proposal also states that the Council and the European Commission will produce 'guidance and/or recommendations to ensure common risk assessments by the competent authorities of the Member States for the implementation of those criteria'.[136] However, the proposal does not indicate how detailed this guidance will be or when and how it will be produced.

NGOs have strongly supported the inclusion of concerns related to human rights and IHL in EU member states' assessment criteria for exports of dual-use items in general—and cyber-surveillance technology in particular—but have called for greater specificity in the content of both the criteria in the Dual-use Regulation and any accompanying guidance. Access Now and other NGOs have argued that the Dual-use Regulation should state that EU member states 'are required to deny export licenses where there is a substantial risk that those exports could be used to violate human rights, where there is no legal framework in place in a destination governing the use of a surveillance item, or where the legal framework for its use falls short of international human rights law or standards'.[137] In 2014 a group of NGOs launched a set of 'necessary and proportionate principles' intended to ensure that states' surveillance powers are in line with human rights law that could form the basis for accompanying guidance.[138] INTA and AFET have responded positively to the Commission's decision

[131] European Chemical Industry Council (Cefic), 'Cefic views on the Recast of the EU Dual Use Goods legislation', Jan. 2017; Digital Europe, 'European Commission Proposed Recast of the European Export Control Regime: Making the rules fit for the digital world', 24 Feb. 2017; and Aeronautic, Space, Defence and Security Industries in Europe (ASD), 'Defence Market'.

[132] Digital Europe (note 131).

[133] British House of Commons, 'Control of Exports of Dual-Use Items', 18 Jan. 2017.

[134] British House of Commons (note 133).

[135] European Commission (note 100).

[136] European Commission (note 100).

[137] Access Now, Amnesty International et al. (note 127).

[138] 'Necessary and proportionate: International principles on the application of human rights to communications surveillance', necessaryandproportionate.org, May 2014.

to incorporate human rights and IHL considerations into the EU's export control criteria for dual-use items and made several amendments that give would give greater specificity to the factors that member states should take into account when making their licensing assessments. Overall, AFET has called for a more restrictive approach, indicating that licences should be denied if 'the legal framework or technical arrangements in the destination country fail to provide adequate safeguards against serious human rights abuse'.[139] In the INTA amendments, the legal framework in the recipient country is among the issues that must be taken into account in member states' assessment processes, but only in connection with exports of cyber-surveillance technology. In addition, licences should only be denied if the export is likely to lead to 'serious violations of human rights'.[140] INTA has also called for accompanying 'guidelines'—rather than 'guidance'—to be produced and both INTA and AFET have indicated that this material should be ready as soon as the new Dual-use Regulation enters into force.[141] INTA have specified that these guidelines should draw upon the User's Guide of the EU Common Position and be produced in a way that involves 'external expertise from academics, exporters, brokers and civil society organizations.'[142] In contrast, several stakeholders have argued against criteria-based assessments and in favour of having either a 'black list' of prohibited recipients or a 'white list' of approved recipients. For example, Digital Europe has called on the EU to publish 'a list of excluded end-users'.[143] Meanwhile, the Greens/EFA group in the European Parliament has argued that exports should be limited 'to a very restrictive and short list of highly stable and mature democracies'.[144]

Certain stakeholders have noted the potentially negative implications of applying more restrictive, human rights-based standards to the export of cyber-surveillance technology. During the review process, one industry representative noted that if the application of restrictive policies on the export of cyber-surveillance technology leads to these companies leaving the EU, this could have negative security implications for EU member states. In particular, states could lose their ability to cooperate with the intelligence agencies of states in Africa and the Middle East, which provides a means of sharing intelligence, and influencing and improving the policies and practices of the states involved.[145] However, others have noted that the impact of applying human rights concerns in this area should be thought of not just in terms of measureable outcomes, but also in relation to the need to align polices and practices in this area with EU values. For example, AFET has noted that the application of stronger, human rights-based, controls in this area would add 'coherence between the EU's foreign and security policies and its economic and commercial interests'.[146]

Creating a new catch-all control and 'due diligence' requirements

Catch-all controls make dual-use items that do not feature on the EU dual-use list subject to control because they are being shipped for a particular end use or to a particular end-user. The Dual-use Regulation includes catch-all controls that allow EU member states to impose licensing requirements on exports of non-listed dual-use items that are, or may be, intended for a military end-user in an embargoed state or for use in a WMD programme or as spare parts for illegally supplied military goods. Companies

[139] European Parliament (note 108), p. 19.
[140] European Parliament (note 110), p. 37.
[141] European Parliament (note 110), p. 38; and European Parliament (note 108), p. 19.
[142] European Parliament (note 110), p. 38.
[143] Digital Europe (note 131).
[144] The Greens / EFA group in the European Parliament (note 121).
[145] SIPRI and Ecorys (note 27), p. 207.
[146] European Parliament (note 108), p. 3.

are also obliged to notify their national authorities if they are 'aware' that an export of non-listed dual-use items is intended for any of these end-users or purposes. Under the proposal a new catch-all control would be established allowing EU member states to impose controls on exports of non-listed dual-use items that are, or may be, intended 'for use by persons complicit in or responsible for directing or committing serious violations of human rights or international 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'.[147] Companies would also be obliged to inform their national authorities if—having performed 'their obligation to exercise due diligence'—they become aware that an export of non-listed dual-use items is intended for any of these purposes. The European Parliament proposed adding a dedicated catch-all control for exports of unlisted cyber-surveillance technology to the Dual-use Regulation in October 2012 but it was not adopted.[148] The Commission's proposal goes beyond the 2012 language by including a reference to terrorism and covering all non-listed dual-use items as opposed to just cyber-surveillance technology.

A number of responses to the Commission's proposal have noted that the concrete implications of the new catch-all control are hard to assess. In particular, its full parameters would be determined by the scope of the definitions of 'dual-use items' and cyber-surveillance technology that are included in the revised Dual-use Regulation. The Federal Association of German Industry (Bundesverband der Deutschen Industrie, BDI) has highlighted that a broadly defined catch-all control is likely to generate differences in national implementation and confusion among companies about which products and transactions are covered.[149] 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.[150] Cefic has indicated that companies may respond to any lack of clarity in the catch-all control by increasing the number of export authorizations they submit.[151] The Finnish Government has also highlighted that companies, particularly smaller enterprises, may find it hard to determine when their exports are covered by the proposed catch-all control.[152] Finally, Business Europe has highlighted that Article 8 already allows EU member states to impose controls on unlisted cyber-surveillance technology because of human rights concerns associated with their use.[153] In contrast, INTA and AFET have welcomed the Commission's inclusion of a new catch-all control in its proposal.[154] However, INTA has indicated that the scope of what is being proposed should be narrowed by deleting the reference to acts of terrorism and having the catch-all apply only to cyber-surveillance technology rather than all unlisted dual-use items.[155] AFET has indicated that the coverage of the reference to terrorism should be narrowed but that other aspects of the catch-all control put forward by the Commission should remain

[147] European Commission (note 100).

[148] 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), 23 Oct. 2012.

[149] Bundesverband der Deutschen Industrie (BDI), Position Paper, EU Dual-Use-Reform: EC Proposed Regulation COM(2016) 616, Apr. 2017; and BDI, 'Why BDI supports dual-use reform but not the new catch-all rules', May 2017.

[150] 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).

[151] Cefic (note 131).

[152] Finland Government, 'Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi kaksikäyttötuotteiden vientiä, siirtoa, välitystä, teknistä apua ja kauttakulkua koskevan unionin valvontajärjestelmän perustamisesta (kaksikäyttötuoteasetus) [Government statement to the Parliament on the proposal for a regulation of the European Parliament and of the Council establishing a European Union supervisory regime for the export, transfer, brokering, technical assistance and transit of dual-use items (Dual-Use Regulation)]', Helsinki, 10 Nov. 2016.

[153] Business Europe (note 130).

[154] European Parliament (note 110), p. 57.

[155] European Parliament (note 110), p. 24.

largely unchanged.[156]

The inclusion of a requirement for companies to carry out due diligence has generated a significant amount of discussion and debate among stakeholders. BDI has argued that this language could create a number of serious legal problems since the obligations are not clearly defined but failure to comply could incur serious penalties, including prison sentences.[157] Meanwhile Cefic has argued that 'companies will most likely tend to strive for zero-risks, either by requesting increasing export authorizations, or abstaining from exporting certain goods to certain regions'.[158] In contrast, INTA and AFET have indicated that some form of due diligence requirement in connection with the new catch-all control should be retained. They have also proposed that due diligence should be defined as 'the process through which enterprises can identify, prevent, mitigate and account for how they address their actual and potential adverse impacts as an integral part of business decision-making and risk management systems'.[159] However, INTA has indicated that the reference to due diligence being an 'obligation' for companies should be removed.[160] In contrast AFET has recommended keeping the reference to due diligence as an 'obligation'.[161] Both AFET and INTA have sought to define what 'due diligence' would mean with references inter alia to the UN Guiding Principles for Business and Human Rights and the OECD Guidelines for Multinational Enterprises.[162]

[156] European Parliament (note 108), p. 14.
[157] BDI (note 149).
[158] Cefic (note 131).
[159] European Parliament (note 110), p. 23.
[160] European Parliament (note 110), p. 23.
[161] European Parliament (note 108), p. 14; and European Parliament (note 110), p. 12.
[162] European Parliament (note 108), pp. 12–13.

4. Conclusions and recommendations

Assess the current and potential impact of controls

Although the European Commission has carried out an impact assessment, this was performed before the more specific language contained in the proposal had been drafted. Now that concrete language is on the table there is potentially a need to reconnect with stakeholders to try to identify the costs and benefits that will be generated if the language in the proposal is adopted. The need to carry out this kind of assessment has been highlighted by a number of stakeholders. For example, the House of Commons Select Committee on European Security has asked whether 'the financial and administrative costs of implementing the new controls have been adequately mapped out by the Commission'.[163] Any assessment that is carried out should also examine how the controls adopted by the Wassennaar Arrangement in 2012 and 2013 are being applied by EU member states. In particular, it would be useful to assess how EU member states are assessing exports of the cyber-surveillance technologies that have been made subject to control: which criteria are being applied, how they are being applied, which sources of information are being used and which exports have been approved or denied. It should also examine how the aspects of the EU sanctions on Iran and Syria that cover cyber-surveillance technology have been implemented by EU member states. There is no formalized mechanism for assessing national implementation of EU sanctions within the EU, as there is for UN sanctions. However, the narrowing of the focus of controls on cyber-surveillance technology in the EU sanctions on Venezuela implies that the experience gained from the controls on Iran and Syria has been noted and taken into account. Foreign Policy Instruments (FPI)—a part of the Commission—oversees the implementation of EU sanctions. There is no formal role for DG Trade—the part of the Commission responsible for overseeing the Dual-use Regulation—in this process. However, it should be possible to ensure that the experience gained from implementing the EU sanctions on Iran, Syria and Venezuela is properly documented and fed into the review of the Dual-use Regulation.

Create links with the wider range of EU policy tools

A wide range of policy instruments—many of which are at the disposal of different branches of the EU—can be used in seeking to control the transfer and use of cyber-surveillance technology. EU member states' use of the controls adopted by the Wassenaar Arrangement in 2012 and 2013 clearly demonstrates that dual-use export controls have—in certain circumstances—a role to play in meeting the challenges posed by the export and use of cyber-surveillance technology. However, they are not a panacea and cannot resolve all of the challenges in this complex area. In particular, they can only be used to control the international movement of hardware, software and technology and do not have any kind of direct role to play in ensuring that network operators, LEAs and intelligence agencies act responsibly when collecting, transferring or using communications data. Making progress on these fronts is essential if the challenges posed by the use of cyber-surveillance technology are to be properly addressed. These are also areas in which significant achievements have been made in recent years. In particular, network operators have sought to create greater transparency and accountability with regard to the way communications data is collected and transferred to governments, and to push governments to develop more standardized processes in

[163] British House of Commons (note 133).

this area.[164] The lessons learned from these and other experiences need to be properly mapped and understood so they can feed into a broader discussion of the full range of human rights, IHL and terrorism-related concerns associated with the export and use of cyber-surveillance technology.[165] This, in turn, would help to achieve greater coherence between dual-use export controls and other areas of EU policymaking.

Address the complexities of drafting criteria and guidelines

Generating clear and effective criteria and guidelines for assessing exports of cyber-surveillance technology is likely to be a challenging process that would involve bringing together technologists, legal experts and policymakers. The EU Common Position and its accompanying User's Guide illustrate the complexities involved in such a process. Work on drafting the criteria in the EU Common Position began in 1991 with a comparison of national practices and a discussion about the potential for harmonization, and concluded in 1998 with the adoption of the EU Code of Conduct on Arms Exports, the predecessor to the EU Common Position.[166] The User's Guide is a 150-page document that has been developed and expanded over many years. A first step would be to establish an EU-wide understanding of the legitimate uses of cyber-surveillance technology, and the regulatory powers and checks and balances that would need to be in place in order to ensure that abuses do not occur. The EU has agreed standards for certain types of cyber-surveillance technology, such as data retention systems. In such cases, there is the potential to create criteria and guidelines that are grounded in established EU legal standards. However, national practices—in terms of which authorities can use these powers and how they are governed—vary significantly, even among EU member states (see below). In addition, there are no agreed standards at the EU level with regard to the use of other cyber-surveillance technologies, such as IMSI catchers, intrusion software and monitoring centres. Several EU member states have passed legislation governing the use of these systems or are currently putting such legislation in place.[167] However, the standards that exist vary significantly and these discussions have not yet 'moved upwards' to the EU level. A number of CSR standards have been produced that can provide useful material when drafting guidance.[168] However, these are either largely focused on the ICT sector or cyber-surveillance technology in general—without discussing the particular risks associated with each particular system—or only cover certain types of technologies.

Create mechanisms for transparency and reporting

One issue that was not addressed in the Commission's proposal is public transparency. The proposal includes a number of mechanisms that would increase the amount

[164] See 'TeliaSonera Transparency Report January 2015', TeliaSonera, Jan. 2015; 'CREDO Transparency Report: Q2 2015', CREDO, 24 July 2015; the Global Network Initiative (GNI), <http://globalnetworkinitiative.org/principles/index.php>; and the Telecommunications Industry Dialogue, <http://www.telecomindustrydialogue.org/about/>.

[165] For a fuller overview of the range of policy options available see McKune, S. and Deibert, R., *Who's Watching Little Brother: A Checklist for Accountability in the Industry Behind Government Hacking* (The Citizen Lab: University of Toronto, Mjunk School of Global Affairs, Mar. 2017).

[166] Council of the European Union, 'European Union Code of Conduct on Arms Exports', 8675/2/98 Rev. 2, 5 June 1998.

[167] King, E. and Rice, M., 'Behind the curve: When will the UK stop pretending IMSI catchers don't exist', Privacy International, 5 Nov. 2014.

[168] These include United Nations, Office of the High Commissioner, Human Rights, Guiding Principles on Business and Human Rights (United Nations: New York and Geneva, 2011); OECD, Guidelines for Multinational Enterprises, n. d.; Shift and Institute for Human Rights and Business, ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights (European Commission: Brussels, June 2013); Cohn, C. and York, J., '"Know your customer": Standards for sales of surveillance equipment', Electronic Frontier Foundation, 24 Oct. 2011; and British Government and TechUK, Assessing Cyber Security Export Risks, Cyber Growth Partnership Industry Guidance (TechUK: London, 25 Nov. 2014).

of information that EU member states share with each other about how controls are applied, but no requirements for EU member states to make any of this information publicly available. A small number of EU member states have systems in place for publishing data on export licences issued and denied for dual-use items, but the majority do not release any data in this area. AFET argues that 'Member States should make available all licensing information, to enhance accountability and oversight'.[169] Access Now and other NGOs have also recommended that greater transparency and reporting should be made mandatory under the Dual-use Regulation.[170] This could have a significant impact on improving public understanding of the way export controls on cyber-surveillance technology operate while also helping to improve and harmonize national standards on the issuing of licences. If it is judged that publishing data on all dual-use licences would generate an undue level of regulatory burden, then consideration could be given to focusing attention on licences issued and denied for the export of cyber-surveillance technology.

Clearly define the human rights, technologies and end-users of interest

One of the key challenges of the long-running discussion about applying dual-use export controls to the trade in cyber-surveillance technology is the lack of clarity about which human rights, technologies and end-users are of interest. Certain stakeholders indicate that there should be an emphasis on 'internal repression' which, while poorly defined, would imply a focus on more serious breaches of human rights, such as of the right to life, freedom from arbitrary arrest and detention, and freedom from torture and inhuman or degrading treatment. Others emphasize—either explicitly or implicitly—a focus on a wider range of human rights, including potentially the right to privacy, freedom of expression, and freedom of assembly and association. However, as noted above, the very use of some of the cyber-surveillance technologies that are already controlled—or which may be made subject to control—by a state that lacks adequate systems of oversight could be considered a violation of some of these rights, particularly the right to privacy. Many states—including some in the EU—have been accused of lacking such systems of oversight. Indeed, a recent survey of 21 EU member states argued that all of them maintained standards relating to the types of data retention systems that network operators are required to maintain that are in breach of rulings by the Court of Justice of the European Union (CJEU) concerning violations of the right to privacy.[171] There is also a lack of clarity about the cyber-surveillance technologies that are the focus of interest. While many would like to see the scope widened beyond those featured in this paper, others would like to see it narrowed. One way to achieve clarity on this point would be to clearly define the end-users that are of interest. As noted above, the proposal defines dual-use items as items that have 'both civil and military purposes' but then lists items that are only ever used by civilian end-users, particularly network operators. Clearly mapping out the options on each of these points—and assessing their potential costs and benefits—would help to frame discussions as the review process continues.

Although the process of reviewing the Dual-use Regulation is well advanced, it is still continuing and may not conclude until early 2019. As such, there is still time to ensure that the Regulation as a whole—and particularly the sections focused on human rights, IHL and terrorism-related concerns and cyber-surveillance technology—are framed in a balanced and effective manner. As the revelations that emerged

[169] European Parliament (note 108), p. 3.
[170] Access Now, Amnesty International et al. (note 127).
[171] Privacy International, *National Data Retention Laws since the CJEU's Tele-2/Watson Judgment*, Sep. 2017.

during the 2011 Arab Spring and events since have demonstrated, the unregulated use of cyber-surveillance technology poses a threat to human rights in many parts of the world. In addition, if framed effectively, dual-use export controls have the potential to contribute to greater oversight and responsibility in the trade in these items. At the same time, important regulatory gaps remain which the Dual-use Regulation can help to narrow. There is the potential do this in a way that both reflects EU values and allows the Dual-use Regulation to continue to act as a model for other parts of the world. However, this can only be achieved if the implications of the language being proposed are properly assessed and if the views of all relevant stakeholders are taken into account.

About the author

Mark Bromley **(United Kingdom)** is the Director of the SIPRI Dual-Use and Arms Trade Control Programme. His areas of research include arms acquisitions in Latin America, transparency in the field of international arms transfers and the efforts to combat the illicit trafficking of small arms and light weapons (SALW).

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org