Is There a Common Understanding of Dual-Use?: The Case of Cryptography

VERONICA VELLA[1]

Abstract

This article explores the dual-use concept by focusing on the specific case of export controls on cryptographic products. The analysis demonstrates different implementation models and interpretations adopted by states. Although adhering to the same multilateral export control regimes, states employ different approaches when it comes to implementation. The United States and the European Union approach to cryptography are used as case studies to confirm this hypothesis. This paper acknowledges the necessity of revisiting the dual-use concept over time as technology and understanding develop.

Keywords

Dual-use, cryptography, export controls, Weapons of Mass Destruction (WMDs), Wassenaar Arrangement, intangible technology transfer

The Concept of Dual-Use in Practice

An analysis of politically and legally binding documents governing dual-use trade shows the lack of an internationally legally binding definition of dual-use. Existing instruments define the term in different ways, such as being linked to military capabilities, nuclear proliferation, covering the full spectrum of Weapons of Mass Destruction (WMD), or even encompassing the human security approach to dual-use put forward by the European Parliament.[2]

If a common understanding of dual-use in politically and legally binding documents does not exist, then what do these instruments have in common? One answer may be that the lack of an

1 Veronica Vella graduated in Global Politics, European Union, and Euro-Mediterranean Relations at the University of Catania (UC) and the University of Liège (ULg) - Double Master Degree Program. She has worked at the University of Liege in the European Studies Unit (ESU ULg).

2 See Annex I of this article for a full comparative analysis of existing definitions.

internationally legally binding definition has been mitigated or even replaced by lists of dual-use items that have resulted from bargaining and compromise over time. Consequently, lists, in addition to being the commonality of the different instruments employed to control dual-use commerce, have become the dual-use concept itself. In theory, since control lists are similar for all export control regime members, their understanding should be the same as well, and implementation should be uniform and smooth. However, the biggest distinction in the understanding of the dual-use concept lies in the different export control systems employed by states.

The following sections use the case study of cryptography to demonstrate whether a common understanding of dual-use exists from an empirical perspective. The case study aims to verify the conformity of lists governing dual-use trade and attest to a common understanding of dual-use at the implementation level.

Cryptography as a Dual-Use Technology

Cryptography is one of the most complex areas of the security industry. Increasingly, the issue of export controls on cryptographic products has been raised.[3] Several factors, such as the growing international trade of information technology and services, companies' increased interest in high-technology areas, and the centralized storage of personal and sensitive data and its transfer across digital networks have created a greater necessity for information security, whose key component is cryptography.[4]

> *Cryptography is defined as "the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use. Cryptography is limited to the transformation of information using one or more 'secret parameters' (e.g., crypto variables) or associated key management."*[5]

Products that are designed or modified to use cryptography employing digital techniques performing a cryptographic function are ruled by encryption export controls. Most countries, to varying degrees, regulate encryption as a dual-use item, having both civilian and military applications.

The United States was the first country to pioneer efforts to regulate encryption during the Cold War.[6] With the aim of harmonizing regulations on the export and import of dual-use

---

3 Some examples include the case of J. Daniel Bernstein challenging the constitutional validity of the US export system; the struggle against encryption limitations held by international privacy advocates in political debates (such as the Electronic Privacy Information Centre the Electronic Frontier Foundation, Privacy International, Cyber Rights & Cyber Liberties-UK, and the Global Internet Liberty Campaign); the DigitalEurope position on the EU-US Regulatory Cooperation; the issues raised by E. Snowden a couple of years ago; and more recently it has been questioned and reported in the press the possible role that cryptography has had in the Paris terrorist attacks (as if restricting encryption would not have prevented the them).

4 Nathan Saper, "International Cryptography Regulation and the Global Information Economy," *North Western Journal of Technology and Intellectual Property* 11:7 (2013), p. 673.

5 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies, "List of Dual-use Goods and Technologies and Munitions list," WA-LIST (16) 1, December 8, 2016, p. 209.

6 Nathan Saper, "International Cryptography Regulation and the Global Information Economy," *North Western Journal of Technology and Intellectual Property* 11:7 (2013), p. 677.

technologies, many countries have agreed to a set of principles, for example the Wassenaar Arrangement (WA).[7] However, although the WA sets general parameters for import and export control to which its Member States largely adhere, they are not binding and are implemented at the discretion of each country. Thus, until Member States implement these provisions in national legislation, the controls have little effect.

Cryptography is fully regulated by one of the four main export control regimes and partially regulated in two others. The Australia Group (AG) Common Control Lists do not control cryptography, whereas the Missile Technology Control Regime (MTCR) Equipment, Software and Technology Annex refers to "decryption" in Category II Item 11,

> *"Receiving Equipment for Global Navigation Satellite Systems" as "having any of the following characteristics, and specially designed components therefor: [...] 1. Designed or modified for airborne applications and having any of the following: [...] 2. Employing decryption, designed or modified for military or governmental services, to gain access to GNSS secure signal/data [...]."*

The Nuclear Suppliers Group's (NSG) list of Nuclear-related Dual-Use Equipment, Materials, Software, and Related Technology denotes cryptography in Part II under the heading "Uranium isotope separation equipment and components (Other Than Trigger List Items) - 3D Software." It specifies cryptography as "software or encryption keys/ codes specially designed to enhance or release the performance characteristics of equipment." Further, the heading "Test and measurement equipment for the development of nuclear explosive devices, Software 5.D.1" mentions "Software or encryption keys/codes specially designed to enhance or release the performance characteristics of equipment not controlled in Item 5.B.3. so that it meets or exceeds the characteristics specified in Item 5.B.3."

Finally, the Wassenaar Arrangement controls cryptographic products as dual-use items under Category V, Part II of the "Information Security" section of its List of Dual-use Goods and Technologies and Munition List. The Cryptographic Information Security section states, "Information security systems, equipment and components, as follows: [...] Designed or modified to use cryptography for data confidentiality having in excess of 56 bits of symmetric key length, or equivalent… where that cryptographic capability is usable without cryptographic activation or has been activated." However, some exceptions have been established in the Cryptography Note and in the Note to the Cryptography Note.[8]

---

7 The Wassenaar Arrangement (WA) succeeded the Co-ordinating Committee on Multilateral Export Controls (COCOM), which existed during the Cold War-era. It was established in 1994 in order to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations.

8 Note to the Cryptography Note: 1. To meet paragraph a of Note 3, all of the following must apply: (a) The item is of potential interest to a wide range of individuals and businesses; and (b) The price and information about the main functionality of the item are available before purchase without the need to consult the vendor or supplier. A simple price enquiry is not considered to be a consultation. 2. In determining eligibility of paragraph a. of Note 3, national authorities may take into account relevant factors such as quantity, price, required technical skill, existing sales channels, typical customers, typical use or any exclusionary practices of the supplier. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies, "List of Dual-use Goods and Technologies and Munitions list," WA-LIST (16) 1, December 8, 2016, p. 87.

Different Approaches to Controlling Cryptography: The United States vs. The European Union

This section considers the EU and US implementation approach towards controlling cryptography. This comparison is a useful starting point for any investigation into the global framework for encryption regulation since the two countries have the most developed and documented laws regarding encryption.

United States

The United States is one of the global leaders in encryption technology and therefore has significant influence on international trade and policies on encryption. Accordingly, debates on encryption in the US have an impact far beyond national borders.

US trade of dual-use items is regulated by the Department of Commerce Bureau of Industry and Security (BIS) which implements its authority through the Export Administration Regulations (EAR).[9] The EAR defines dual-use as items as those "[having] civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications."[10] This definition seems to reflect a wider US understanding of dual-use that extends beyond the traditional dichotomy of civilian versus military, including a terrorist dimension.

As noted in 15 CFR 738, the Commerce Control List (CCL) of export controlled items covers ten categories ranging from nuclear materials to space vehicles. Within each category both export controlled physical objects and export controlled digital objects (software and "technology," i.e., information) are controlled. Encryption is covered under Category V, "Telecommunications and Information Security." It is important to note that this particular entry, listed in the CCL under a particular Export Control Classification Number (ECCN), may be controlled for multiple reasons: encryption software and technology are marked as being controlled not only under the special "EI" Reason for Control but also under the more general "NS" (national security) and "AT" (anti-terrorism) Reasons for Control.[11,12]

Although the US is a WA member, it does not apply the General Software Note to "software" controlled by Category V – part II "Information Security" and generally maintains stricter controls than what is required by the arrangement.[13,14,15] The US employs the same definition of cryptography as the WA yet takes a broad view of the scope of the encryption controls given

---

9 The EAR is part of the US Code of Federal Regulations (CFR); more specifically, they are in Title 15 of the CFR, "Commerce and Foreign Trade," Chapter VII, "Bureau of Export Administration, Department of Commerce (Parts 700-799)," Subchapter C, "Export Administration Regulations;" hence the EAR are also sometimes referred to as 15 CFR chapter VII subchapter C or 15 CFR Parts, pp. 730-774.

10 US Department of Commerce, "EAR – Part 730," BIS, January 4, 2017, p. 2.

11 There is an "EI" Reason for Control applied just to encryption items.

12 US Department Of Commerce, "EAR – Part 738," BIS, November 25, 2016.

13 *General Software Note* serves not to control "software" which is (1) generally available to the public, according certain criteria, (2) "in the public domain," (3) the minimum necessary "object code" for the installation, operation, maintenance (checking) or repair of those items whose export has been authorized.

14 US Department Of Commerce, "EAR – Part 774, The Commerce Control List," BIS, September 20, 2016, p. 1.

15 Bert-Jaap Koops, "Crypto Law Survey, Overview per Country," February 2013, <www.cryptolaw.org>.

that it includes controls on products that make calls to the encryption functionality of a third party product, activation codes to activate "dormant" encryption functionality.[16,17]

The US has been one of the most vocal advocates of restrictions on the right to use and export encryption, mainly driven by its prerogative to safeguard national security and foreign intelligence gathering capabilities, and increasingly by terrorist concerns. Initially, cryptographic products were controlled under the International Traffic in Arms Regulations (ITAR).[18] Considering the "commodity jurisdiction" procedure provided by the ITAR, a specific item was considered controlled depending on whether it came under the US Munitions List. If so, the item required a license before it could be exported. Munitions licenses were granted by the Department of State on a case by case basis. It was not until J. Daniel Bernstein challenged the constitutional validity of this licensing system that cryptographic export was transferred to the EAR, which essentially replicates the impugned ITAR controls on cryptographic technologies.[19,20]

The liberalization of US export policies started in 1998, when the Clinton administration announced a new policy to reform the strict export regime. However, during the reform process, the US also proposed domestic controls on the use of encryption which would enable law enforcement officials to legally access encryption keys when necessary.[21]

The US has been a strong advocate of so-called "key escrow and key recovery systems" which involve third party access to private keys or the ability to access data in plain text. Such systems authorize a third party, such as government agency, or a Trusted Third Party, usually connected with the government, to store cryptographic keys and provide them to a government agency when requested.[22] The US strongly pressured the international community to adopt this system. However, doing so provoked a strong reaction from international privacy advocates, security experts and civil liberties groups.[23] The opponents of this system maintained that it would

---

16 The discipline that embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use. "Cryptography" is limited to the transformation of information using one or more "secret parameters" (e.g., crypto variables) and/or associated key management. EAR- Part 772, p. 13. WA-LIST (16) 1, December 8, 2016, p. 209.

17 Jasper Helder, and John F. McKenzie, "Encryption Export Controls: A Comparative Analysis between the EU and the US," Annual International Trade Compliance Conference, Netherlands: November 8, 2013, p. 4, <http://www.hhp.co.id/files/Uploads/Documents/International%20Trade%20&%20Compliance%20Event/Jasper%20Helder%20and%20John%20McKenzie_Encryption%20Export%20Controls_A%20Comparative%20Analysis%20between%20the%20EU%20and%20the%20U.S..pdf>.

18 The ITAR regulates exports of items and services specifically designed for military applications while the EAR regulate exports of commercial items with potential military applications ("dual-use" items).

19 The licensing scheme under ITAR violated his First Amendment right to free speech.

20 See for example Sarah Andrews, "Who Holds the Key? – A Comparative Study of US and European Encryption Policies," *The Journal of Information, Law and Technology (JILT) (*February 2000*),* p. 8-9.

21 The first attempt to restrict domestic use came in 1993 when the government developed the Escrowed Encryption Standard Initiative aimed at providing citizens with a good level of security for communications while at the same time preventing transmission of data in total secrecy.

22 D. Maniotis, M.T. Marinos, A. Anthimos, I. Iglezakis, and G. Nouskalis, *Cyber Law in Greece* (Netherlands: Kluwer Law International, 2011), p. 69.

23 For example, the Electronic Privacy Information Centre the Electronic Frontier Foundation, Privacy International, Cyber Rights & Cyber Liberties (UK), and the Global Internet Liberty Campaign.

present a violation of the right to privacy, besides the fact that such systems are ineffective against criminals who merely use other encryption methods to avoid detection.[24] Moreover, it is important to mention that in the US there is no specific law protecting the right to privacy of personal information. This area is ruled by a piecemeal collection of constitutional and statutory laws and self-imposed industry regulations.[25]

US export controls have been subject to a new wave of liberalization triggered by changes to the EU export regulations.[26] As a consequence, a license exception was introduced for the export of any crypto product to *any* end-user in the EU. Export restrictions to terrorism supporting countries were maintained. In January 2011, a minor amendment was made to the EAR. Publicly available mass-market encryption object code software, and publicly available encryption object code of which the corresponding source code falls under License Exception TSU, are no longer subject to the EAR.[27]

When exporting cryptographic products under the EAR, there are two important factors exporters must consider. First, the attributes of the software to be exported due to concern over key length. Indeed, Category V Part II of the EAR specifies that encryption systems with key lengths of 56 bits or less for symmetric systems, or 512 bits or less for asymmetric systems, can be exported without restriction. Strong encryption systems, which use longer keys, face export restrictions.[28] Moreover, there is an exemption for "mass market" encryption products, according to which if an encryption product is generally available to the public, for home or personal use, without continuing support by the supplier (e.g., a personal email security program), then its export is not restricted. A final important exemption is for products "when accompanying their user for the user's personal use or as tools of the trade […];" this allows users to, for example, travel with laptops and mobile phones that contain encryption capabilities.[29]

In addition, exporters must consider to whom the software is being sold, thus including the specific attributes of the customer's location, which can be problematic. Indeed, the exporter must indicate and ensure that their customers are neither located in an embargoed country nor are "Specially Designated Nationals."[30] However, contrary to other countries' export control regimes, the EAR makes no distinction between the physical shipment of tangible items from the US to a foreign country and the electronic transmission of software or technology from

---

24 Sarah Andrews, "Who Holds the Key? – A Comparative Study of US and European Encryption Policies," *The Journal of Information, Law and Technology (JILT) (*February 2000*),* p. 4.

25 Ibid, 14.

26 Bert-Jaap Koops, "Crypto Law Survey, Overview per Country," February 2013, <www.cryptolaw.org>.

27 Ibid.

28 U.S. Department Of Commerce, "EAR – Category 5 Part 2, "Information Security," BIS, September 20, 2016.

29 Nathan Saper, "International Cryptography Regulation and the Global Information Economy,*" North Western Journal of Technology and Intellectual Property* 11:7 (2013), p. 680-681.

30 The Office of Foreign Assets Control (OFAC), an agency within the US Treasury Department, administers sanctions programs against specific countries, restricting the export of sensitive products and materials—including cryptography software—to those locations. In addition, OFAC administers restrictions against exports to specially designated individuals and entities, known as "Specially Designated Nationals" ("SDNs"); exports to those individuals and entities are generally prohibited.

the US to a person or entity located abroad.[31] For export control purposes, any such physical shipment or electronic transmission is an export that must be performed in accordance with the requirements and restrictions embodied in the EAR. Thus, section 734.2(b)(1) of the EAR defines the term export to include any "actual shipment or transmission of items subject to the EAR out of the United States." All this proves to be problematic when firms that sell encryption software over the internet must adopt measures to screen their customers to assure their location, and it is yet unclear what kinds of steps such firms can take to ensure compliance.[32]

Although its export control system is based on its commitments under multilateral export control regimes, "the US also maintains unilateral controls on a wide range of dual-use items predominantly for anti-terrorism reasons."[33] The US maintains certain "anti-terrorism export controls" on those encryption products that are excluded from controls. Specifically, encryption products that are subject to export controls are generally classified under 5A002 (hardware) and 5D002 (software). Export licenses or other authorizations (such as export license exceptions) are required in order to export those 5A002 and 5D002 encryption products from the US. However, there are certain products with encryption functions and features that are excluded from the controlled categories.[34] Those excluded products are subject to certain "anti-terrorism" export controls. In the encryption provisions of the US CCL, encryption products that are excluded from 5A002 (hardware) and 5D002 (software) are classified for US export control purposes under 5A992 (hardware) and 5D992 (software).[35] Those entries on the CCL indicate that products classified under those 5A992 and 5D992 categories are controlled for "AT" (or anti-terrorism) purposes.[36] Therefore, under both the US Commerce Country Chart and the anti-terrorism provisions of Part 742 of the EAR, the products that are subject to those AT export controls are restricted for export to those countries that have been designated by the United States Government as terrorism supporting countries.[37]

European Union

Article II.I of European Council Regulation (EC) 428/2009, otherwise known as the EU Dual-Use Regulation, defines dual-use 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

---

31 John F., McKenzie, "United States Export Controls on Internet Software Transactions," Baker & McKenzie, August 2010, p. 3.

32 Nathan Saper, "International Cryptography Regulation and the Global Information Economy," *North Western Journal of Technology and Intellectual Property* 11:7 (2013), p. 681.

33 Office of the Coordinator for Counter-terrorism, The Global Challenge of Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism, 2011, <https://www.state.gov/j/ct/rls/crt/2013/224827.htm>.

34 Examples of those excluded products include (i) products that use a very weak encryption algorithm only (e.g., a symmetric encryption algorithm with a key length of 56 bits or less); (ii) products that qualify as "mass market" encryption items; and (iii) products that use encryption exclusively for authentication, password protection or other forms of access control to digital resources, but do not provide any data encryption functionality

35 US Department of Commerce, "EAR – Category 5 Part 2 - Information Security," BIS, September 20, 2016.

36 US Department of Commerce, "EAR – Part 742, Control Policy - CCL Based Controls," BIS, January 2017.

37 US Department of Commerce, "EAR - Supplement No. 1 to Part 738 – Commerce Country Chart," BIS, November 4, 2016; US Department of Commerce, "EAR – Part 742, Control Policy - CCL Based Controls," BIS, January 15, 2017.

non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices."[38] This definition cumulates "purposive" understanding of this term because it first refers to military and non-military purposes (WA, AG, MTCR definitions), and then refers to nuclear and non-nuclear purposes (NSG definition), including nuclear terrorism.[39]

However, especially after the Arab Spring began in 2010, and considering the deep instability of the African continent and the Middle East, the concern of dual-use trade has expanded in the EU towards a concern for human rights in the export control context. By way of illustration, the European Parliament (EP) proposed a legislative resolution in 2012 to extend the scope of dual-use.[40] Debates on this particular issue, mainly linked to dual-use technologies, are still ongoing as part of the review of the Regulation. Members of the EP as well as members of the Commission call for "taking into consideration human rights as a new dimension of export controls," suggesting establishing human rights as a reason for control and possibly denial of export.[41] These debates arose after the discovery that during the uprisings in Tunisia and Egypt, information and communication technologies provided by European companies played a role in aiding and assisting the government's violation of the freedom of expression, freedom of press and access to information.[42]

The recent European Commission proposal to amend Council Regulation No. 428/2009 has introduced the issue of preventing human rights violation associated with certain cyber-surveillance technology.[43] The proposal adds to the definition of dual-use, in Article II, a paragraph as follows,

> *"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."*[44]

As far as cryptography is concerned, generally, EU Member States are unified in their commitment to a liberal framework for encryption regulations, even though there has not yet been formal

---

38 Council Regulation (EC) No. 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union (L 134/1) of May 29, 2009.

39 Quentin Michel, Sylvian Paile, Maryna Tsukanova and Andrea Viski, *Controlling the Trade of Dual-Use Goods - A Handbook*, (Brussels, Peter Lang, 2013) p. 81.

40 "Export Controls of Dual-use Items," CRE 24/11/2014 - 18, European Parliament, February 18, 2015, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20141124+ITEM-018+DOC+XML+V0//EN>.

41 Ibid.

42 "Inquiry into Role of European Companies in Violation of Human Rights," European Parliament, March 9, 2011, <http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2011-002212&language=SL>.

43 EU 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, Brussels, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf>.

44 Ibid.

harmonization of encryption policies among them.[45] The export control laws of Member States regarding encryption products are uniformly regulated under European law, although each state may have additional regulations concerning the import, supply, use or export of encryption items.

At present, the governing legislation is the Commission Delegated Regulation (EU) 2015/2420 of October 2015 amending Council Regulation (EC) No. 428/200.[46] Before this amendment, the Commission Delegated Regulation (EU) No. 1382/2014 of October 2014 replaced and updated the EU control list to reflect decisions take in export control regimes in 2011, 2012 and 2013.[47] The update incorporated some 400 changes, including the addition of new controls, the removal of some controls, changes to certain technical parameters and other amendments.[48] Among the most significant changes is the inclusion of an additional "note to cryptography note" in order to be in line with the WA and other international agreements.[49]

In addition, the EU has adopted a General Technology Note and a General Software Note that excludes information and software within the public domain from the Control List. Cryptography and information security products are included in Annex I of the control list and are subject to a licensing regime as regard exports from the European Union.

Similarly to the US, the EU takes a broad view of the scope of encryption controls. Indeed, it also includes activation codes to activate "dormant" encryption functionality, but unlike the US, it has always controlled components for "mass market" encryption items.[50] However, encryption products specially designed or modified for military use are subject to export control under national regulations of EU Member States with respect to military items.

The most significant difference between EU and US encryption export controls lies in their respective clarity in defining what is and what is not controlled. Indeed, generally EU controls are very clear whether an item is to be controlled or not and there is no equivalent to US anti-terrorism controls on an EU level even if some Member States can introduce national controls beyond the EU Regulation.[51,52] Nonetheless, if the US employs the "exceptionalism" of anti-terrorism, the EU applies the "exceptionalism" of human rights. In this regard, Article VIII of the EU Regulation clarifies that "a Member State may prohibit or impose an authorization

---

45 Sarah Andrews, "Who Holds the Key? – A Comparative Study of US and European Encryption Policies," *The Journal of Information, Law and Technology (JILT),* February 2000, p. 13.

46 European Commission Delegated Regulation No. 2420/2015 amending Council Regulation (EC) No. 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union, October 12, 2015.

47 Commission Delegated Regulation (EU) No. 1382/2014 of 22 October 2014 Amending Council Regulation (EC) No. 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union (L 371/1), December 30, 2014.

48 Ibid.

49 Ibid.

50 Jasper Helder and John F. McKenzie, "Encryption Export Controls: a Comparative Analysis between the EU and the US," Annual International Trade Compliance Conference, Netherlands: November 8, 2013, p. 18.

51 There is no equivalent to US anti-terrorism controls such as 5A992, 5D992, 5E992.

52 Jasper Helder and John F. McKenzie, "Encryption Export Controls: a Comparative Analysis between the EU and the US," Annual International Trade Compliance Conference, Netherlands: November 8, 2013, p. 22.

requirement on the export of dual-use items not listed in Annex I for reasons of public security or *human rights consideration*."[53]

Indeed, as far as cryptography is concerned, many EU licensing authorities consider encryption for governmental use to be a potential human rights issue. A few examples of encryption related human rights impact are, for example: (1) German unilateral controls for certain hardware and software for Terrestrial Trunked Radio (TTR) for Sudan, (2) increased scrutiny by Dutch authorities of encryption exports to Lebanon, (3) the exception for the supply of certain encryption items to Iran under EU sanctions, (4) Netherlands brokering controls requiring individual pre-notification of brokering for the supply of controlled items for "sensitive countries," and (5) UK license refusals for encryption communications equipment.[54,55]

The UK presents an exception to the overall EU approach towards this issue. Indeed, the UK has specific requirements relating to the export of certain cryptographic items when exported from the UK under a EU General Export Authorization (GEA). These requirements consist in providing "details of information, which is in a person's possession, or other information as that person can be reasonable be expected to obtain."[56] Such information should be submitted to the UK Export Control Organization (ECO) via email within 30 days of first export.

Overall, despite the EU common framework, Member States implement encryption controls differently and still have dissimilar national laws in some cases.[57] The EU approach towards cryptography reflects its understanding of dual-use as also related to human rights violations in this regard. Moreover, the EU does not have equivalent to US anti-terrorism controls such as 5A992, 5D992, 5E992. Indeed, "anti-terrorism export controls" has proved to be a unique feature of US implementation.

What about 'International Competitiveness'?

As shown above, the EU and US approach towards cryptography, and more generally to the dual-use concept, is not the same, nor does it seems to be coherent. These different understandings may damage *inter alia* international competitiveness. In this regard, and as a further demonstration of the inconsistency of these two approaches, it is useful to mention the point of view of an important stakeholder, namely DigitalEurope, a European organization that represents the digital technology industry and seeks to ensure industry participation in the development and implementation of EU policies.[58] In the framework of the much-discussed *Transatlantic Trade*

---

53 Council Regulation (EC) No. 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union (L 134/1) of May 29, 2009.

54 Afghanistan, Angola, Belarus, Burma, Congo, Egypt, Eritrea, Guinea, India, Iraq, Iran, Israel Ivory Coast, Lebanon, Liberia, Libya, North-Korea, Pakistan, Sudan, Syria, Zimbabwe, South Sudan.

55 Jasper Helder and John F. McKenzie, "Encryption Export Controls: a Comparative Analysis between the EU and the US," Annual International Trade Compliance Conference, Netherlands: November 8, 2013, p. 24.

56 "Additional UK Requirements for Cryptography Items Exported under an EU GEA," EU General Export Authorizations, <https://www.gov.uk/european-union-general-export-authorisations>.

57 *See* Figure 2 in Annex II.

58 "About Us," DigitalEurope, <http://www.digitaleurope.org/Aboutus.aspx>.

and Investment Partnership (TTIP) between the EU and the US, DigitalEurope addresses a paper containing its comments and suggestions about it.

The organization underlines the divergent policy approaches adopted by the EU and the US towards the ICT industry. The two systems demonstrate differences in their regulatory systems and in their approaches to risk management, making the achievement of a certain level of harmonization difficult. Even when principal regulatory objectives are equivalent, in practice product requirements imposed by the EU and US technical regulations in certain cases diverge.[59] Indeed, given that the ICT industry generally operates on a global scale, dissimilarities in standard requirements involve the implementation of more than one standard for the same functionality, and hence lead to duplicated implementation efforts and costs. DigitalEurope members offer products, such as hardware or software with cryptographic capabilities, classified as dual-use items. It argues that EU and US export control regulations require that every export of dual-use item shall be performed according these regulations, which envisage either an export authorization/license or a license exception. Nevertheless, because the implementation of export controls is a national responsibility, the administrative procedures for compliance and the method for controlling dual-use items differ between the controlling countries.[60] Hence a problem arises of damaged international competitiveness.

The latter may be further proved by glancing at other countries' approaches to cryptography. Figure II in Annex II provides a general view of international engagements towards import and export controls, and domestic law and regulations on crypto use.[61] If on the one hand nothing new emerges from this figure (since the weaknesses of dual-use export controls—i.e., the lack of uniformity in implementation and even acceptance of these systems by states—are well known), on the other hand it suggests that a strong dual-use export control system is needed worldwide in order to be effective and assure competitiveness and security.

China is one of the most challenging environments for cryptography use and regulations.[62] Both import and export of cryptographic products are highly regulated, and, specifically, encryption is regulated by the National Commission on Encryption Code Regulations (NCECR).[63] Encryption products cannot be sold or imported in China without prior approval by NCECR, and individuals and firms can only use cryptographic products approved by NCECR. This restriction also applies to foreign individuals and firms operating in China as they must receive approval to use their encryption systems. China is not a member of the WA, which means WA Member States are not allowed to export chip technology to China.

Unlike in the US and the EU, all encryption products in China, regardless of key strength or other factors, are fully regulated.[64] Nevertheless, importing encryption products and equipment

---

59 "Digitaleurope Position on the EU-US Regulatory Cooperation," Digital Europe, November 5, 2013, Brussels, p. 1.

60 Ibid, 15.

61 However, it is important to note that it is updated to 2013.

62 Nathan Saper, "International Cryptography Regulation and the Global Information Economy," *North Western Journal of Technology and Intellectual Property* 11:7 (2013), p. 683.

63 Article 4 of Shangyong Mima Guanli Tiaoli (商用密码管理条例), "Regulation of Commercial Encryption Codes," State Council, Directive No. 273, Oct. 7, 1999, China, <http://newmedia.cityu.edu.hk/cyberlaw/gp3/pdf/law_encryption.pdf>.

64 Ibid.

containing encryption technology is restricted in China because of the focus on protecting information security, strengthening commercial encryption management, and safeguarding national security interests.[65] China has pursued a policy of favoring the development of domestic cryptography systems, for example with the creation of a new Chinese standard for wireless Wi-Fi security (WAPI). This kind of approach could be damaging to international competitiveness since foreign companies hoping to sell wi-fi devices to China would have to co-produce their product with designated Chinese firms.[66]

Furthermore, the WAPI standard raises fear that the domestic cryptography standard would create a functional key escrow system that would allow the Chinese Government easier access to encrypted communications. More recently, China's legislature approved an anti-terrorism law which requires companies to hand over technical information and help with decryption when the police or state security agents demand it for investigating or preventing terrorist cases.[67] This provision has created concern among human rights groups about the Chinese government's increasingly intrusive powers and has also created a warning for international companies that use encrypted technology in China such as Cisco, IBM and Apple, all of which have big stakes there.

Interestingly, multinationals are not the only advocates of more relaxed provisions concerning encryption. The Dutch government, for example, published a position paper in which it "endorses the importance of strong encryption for internet security, for supporting the protection of citizens' privacy, for confidential communication by the government and companies, and for the Dutch economy."[68] The paper also states that

> *"The ability to use encryption strengthens the international competitiveness of the Netherlands, and promotes an attractive climate for businesses and innovation […]. Trust in secure communication and storage of data is essential for the (future) growing potential of the Dutch economy, that mainly resides in the digital economy."*

Although the same technology is an obstacle in legitimate investigations, the Dutch paper calls for a "search for new solutions" and opposes the introduction of backdoors in encryption products. Similarly, the French government has rejected crypto backdoors as "the wrong solution." The Deputy Minister for Digital Affairs Axelle Lemaire, speaking on behalf of the French government, rejected an amendment to the new "Law for the Digital Republic," calling for computer companies to provide backdoors to encrypted systems.[69]

---

65 Yu, Xia and Murphy, Mattew (MMlC Group), "The Regulation of Encryption Products in China," *Bloomberg Law Reports – Asia Pacific* 4:2 (2011), p. 1.

66 This clearly suggests a protectionist tool used by Chinese government to promote domestic technology production.

67 Chris Buckley, "China Passes Anti-terrorism Law That Critics Fear May Overreach," *The New York Times*, December 27, 2015, <https://nyti.ms/1ZvqB5L>.

68 G.A. van der Steur, Minister van Veiligheid en Justitie, H.G.J. Kamp, Minister van Economische Zaken, Brief regering, January 4, 2016.

69 Glyn Moody, "French Government Rejects Crypto Backdoors as the Wrong Solution," *Ars Technica*, January 14, 2016, <https://arstechnica.co.uk/tech-policy/2016/01/french-government-rejects-crypto-backdoors-as-the-wrong-solution/>.

To conclude, in the specific case of cryptography, varying regulations and implementations worldwide are considerable obstacles to information technology and security firms' willingness to expand into new markets. Therefore, multinational firms may suffer from this lack of understanding at the international level.[70] At the same time, the right to privacy is at stake since the only way to protect the privacy of digital information is by encryption.

Is a New Definition Necessary?

This article has argued for a common understanding of the dual-use concept. In this regard, one may wonder if the adoption of a new, global definition may be a fundamental condition to achieve this purpose. Yet, this leads to another question in turn: If export control regime guidelines set the standards for national export controls, are they uniformly implemented by Member States? As this article has shown, they are not. Beyond this, catch-all clauses or different perceptions of a dual-use item, as in the case of cryptography, suggest it is not just a matter of standards. By analogy, the same reasoning may be applied to justify the uselessness of a new common definition of dual-use. There is no room to think that a new definition will lead to a homogeneous and global implementation of dual-use export controls. Inevitably, different interpretations, investigation and enforcement structures, borderline cases, end-user concerns, and levels of information or intelligence among states lead to different export control decisions.

However, if on the one hand the adoption of a new definition is far from being the solution to the current weak international export control system, on the other hand it may be valid and useful to propose a modern and consistent definition that incorporates the different understandings of the concept and reflects the evolution it has undergone. Any new definition proposal should clearly touch on the following: (1) which "items" are to be controlled, (2) which purposive nature, and (3) which scope/security.

For instance, considering the subcategory "items," and the confused way in which they are used by different instruments (see Annex I), dual-use may refer to "item" in the sense of goods, including software and technologies. Moreover, to consider the dual-use concept in the life-sciences, "items" should also refer to "information." However, information should not be interpreted in the *sensu stricto* of "technology," which many lists already refer to. Rather, it should be meant as the information issues related to dual-use arising from research.

In addition, in light of the multiplication of items with uncertain dual-use features (due also to the increasingly blurry lines between civilian and defense technology and industrial bases), and with the multiplication of dual-use items with no predominately military use (e.g., surveillance technology, encryption), a question remains concerning the traditional dichotomy between civil vs. military.

Finally, in view of the dissimilar scopes of several international instruments governing dual-use commerce (see Annex I), a valuable scope to include in the new definition may be "*peaceful and non-peaceful"* in order to comprehend the purpose of every instrument. However, this umbrella definition approach would not take into account the shift from national security interests to human security interests since the concept of peaceful vs. non-peaceful originates

70 In this regard, the DigitalEurope position on the EU-US regulatory cooperation is illustrative.

in the international concept of war and peace. Therefore, given that, (1) the concept of dual-use seems to have shifted from state's concern for security to consideration also of human security (e.g., the EU understanding of dual-use as related to human rights violation; the US understanding of dual-use as related to terrorism), (2) taking into account the dual-use research of concern area, (3) and the case of cryptography which underlines the possible threats to human rights to privacy (therefore to political security), the definition may refer to items which threaten *human security,* used as umbrella concept that includes political security. These are suggestions which aim to open the way for further studies in this direction.

Conclusion

This investigation of legally and politically binding instruments referring to the dual-use concept has demonstrated the lack of a common definition and identified and compared similarities and differences in national understandings of dual-use. The article has analyzed to what extent the international community has confusingly worded the concept of dual-use.

One of the most significant findings is that the concept of dual-use has evolved from state proliferation concerns to encompass also non-state proliferation concerns, thus shifting from national security interests to human security interests. In this regard, the US and EU approach are empirical evidence. On the one hand, the US maintains unilateral controls on a wide range of dual-use items predominantly for anti-terrorism reasons, such as anti-terrorism export controls on 5A992 and 5D992 categories, to which there is no EU equivalent. On the other hand, the EU has shown a human rights approach to the dual-use concept by appealing to Article VIII of the EU Dual-Use Regulation and maintaining ongoing dialogue through regulatory reform discussions within the EU. Although the EU and the US adhere to the same multilateral export control regimes and have a lot in common (i.e., defining dual-use as having both civil and military applications), they employ different approaches when it comes to implementation.

The common denominator for all export controls regimes consists of lists of dual-use items. Nevertheless, the consideration of the case of cryptography has revealed a lack of conformity among these international instruments. This, however, does not imply that lists are not the most practical way to achieve common and objective guidance.

Besides the harmonization of lists and systems, a reconceptualization of dual-use may be useful. There is a need for a modern and consistent definition to incorporate the different understandings of the concept and to reflect the evolution it has undergone, as technology and interpretations are constantly changing. This investigation has paved the way for new studies and literature focused on the meaning itself of dual-use that can benefit the international community.

ANNEX I

Figure 1: Matrix of the terms used to refer to dual-use, articulated in the 3 subcategories of items, and the scope of each instrument.

	ITEMS			SCOPE
	GOODS = Tangibility	**TECHNOLOGY**	**SOFTWARE**	
International Regimes, General	Not formally and directly defined.	General consensus on the meaning of the term when it is used.	Same definition in the dual-use export control systems and regimes 'worldwide.'	
BWC & CWC	Do not refer to these 3 categories but, respectively, to *"the agents, toxins, weapons, equipment or means of delivery specified in Article I of this Convention"* and the *"chemical weapons and related activities."* [71,72]			Prohibition of *chemical and biological weapons* to facilitate general and complete disarmament.
NPT	Article III.2 does not mention any of the 3 categories but only the *"equipment and materials"* which can serve proliferation purposes.			Prevention of wider dissemination of *nuclear weapons* – Development of the applications of atomic energy for peaceful purposes.
Zangger Committee	Designates under the term items *"equipment or material especially designed or prepared for the processing, use or production of special fissionable material."*			Stems from Article II.2 of the NPT. Same objectives.
Nuclear Suppliers Group	Targeting *"certain equipment, materials, software, and related technology* that could *make a major contribution* to a *"nuclear explosive activity,"* an *"unsafeguarded nuclear fuel-cycle activity."* (It does not propose a formal definition of the "equipment" and "materials").	"Specific information required for the *development, production,* or *use* of any item. This information may take the form of *technical data* or *technical assistance."*	"A collection of one or more "programs" or "microprograms" fixed in any tangible medium of expression."	Prevent a *major contribution to a nuclear explosive activity, an unsafeguarded nuclear fuel-cycle activity or acts of nuclear terrorism*.

71 BWC Article III.

72 CWC Article I.

	ITEMS			SCOPE
The Australia Group	*"Materials, equipment, technology and software that could contribute to CBW activities,"* (thus suggesting that the sub-category of "goods" may be further divided between "materials" and "equipment"). However, the control list adopted by this *forum* only refers—without defining it—to the "equipment."			Fulfill the obligations under the CWC and BWC.
Missile Technology Control Regime	*Items* and *equipment* are indifferently used, but they are opposed to technology.	Same definition of NSG.	Same definition of NSG.	Prevent *missile development, production and operation*.
The Wassenaar Arrangement	It does not provide any definition of "goods," though it use the term in the title of its Initial Elements and the section dedicated to the scope of its controls.	Same definition of NSG. Annex I. General Technology Note & General Software Note (ex. Controls do not apply to "technology" "in the public domain," to "basic scientific research" or to the minimum necessary information for patent applications).	Same definition of NSG.	Controlling *military* capabilities
Resolution 1540 (2004)	*Items* refer to *materials* related to the "proliferation of nuclear, chemical or biological weapon and their means of delivery."			In response to *global terrorism* and the risk that *non-state actors* may acquire, develop traffic in or use *nuclear, chemical and biological weapons* and their means of delivery.
EU Regulation 428/2009	"Dual-use items shall mean 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."[73] (It seems that the definition of *items, goods* but also *technology* and *software* as dual-use ones is subjected to both aspects of principles and opportunity).[74] European parliament legislative resolution states: "…for use in connection with a *violation of human rights, democratic principles or freedom of speech* […], by using *interception technologies* and *digital data transfer devices for monitoring mobile phones and text messages* and *targeted surveillance of internet use*, such as via monitoring centers or lawful interception gateways."[75]	Provides a definition similar to the definition provided by the international systems. General Technology Note (GTN), General Software Note (GSN), Nuclear Technology Note (NTN). Despite the existence of a definition at the EU level, the MS have inserted a definition of "technology" in their national implementing legislation. (ex. In the British Export Control Order, technology means information that is "capable"—and not compulsorily "necessary"—to be used for such purposes, which enlarges the possibilities of control).	Same definition of NSG – Annex I. General Software Note (GSN).	Cumulates WA, AG, MTCR and NSG objectives. Effort to extend the original scope to protection of human rights and democratic principles, to torture or other cruel inhuman or degrading treatment or punishment.

	ITEMS			SCOPE
US internal regulations	*The term 'dual- use' is often used to describe the types of items subject to the EAR. A 'dual-use' item is one that has civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications.*[76] The term goods is not used. However, an *item* means "commodities, software, and technology."[77] The term commodity is defined as "any article, material or supply except technology and software." (An item shall be reviewed with the light of the Commerce Control List and the provisions of the Regulations.)	*"Basic Scientific Research."* (GTN) – "Experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective." GSN.	Same definition of NSG.	Controlling *terrorism, military or WMD*-related items.
WHO definition of dual-use in life sciences[78]	"Initially used to refer to the aspects of certain materials, information and technologies that are useful in both *military and civilian* spheres. The expression is increasingly being used to refer not only to military and civilian purposes, but also to *harmful misuse* and *peaceful activities*."			From *military and civilian* sphere it extended to *harmful misuse* and *peaceful activities*.

73 Council Regulation (EC) No. 428/2009 of 5 May 2009, Article 2.1.

74 Quentin Michel, Sylvian Paile, Maryna Tsukanova, and Andrea Viski, *Controlling the Trade of Dual-Use Goods- A Handbook*, (Brussels, P.I.E. Peter Lang, 2013), p. 79.

75 Position of the European Parliament adopted at first reading on 23 October 2012 with a view to the adoption of Regulation (EU) No. .../2012 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.

76 US Department of Commerce, "EAR – Part 730, General Information," BIS, May 21, 2015.

77 US Department of Commerce, "EAR – Part 772, Definition of terms," BIS, May 21, 2015.

78 In respect to life sciences research that have dual-use potential, it is useful to the present work to mention at least one reference to it made by an international instrument.

ANNEX II

Figure 2: Overview per Country of Cryptography Laws[79]

COUNTRY	IMPORT CONTROLS	EXPORT CONTROLS	DOMESTIC LAWS AND REGULATIONS
Antigua and Barbuda	X	X	X
Argentina[80]	O		O
Australia	X	X	X
Austria	X	X	X
Bahrain			X
Bangladesh			O
Belarus	X	X	X
Belgium	X	X	X
Brazil	O		O
Bulgaria			
Burma	X	X	X
Cambodia	O		O
Canada	X	X	O
Chile	O		O
People's Republic of China	X	X	X
Colombia	O		O
Costa Rica			
Czech Republic	X	X	O
Denmark	X	X	O
Egypt	X	O	
Estonia	O	X[81]	
Finland	O	X	X
France	X	X[82]	X[83]
Germany	X	X	X
Ghana	O		O
Greece	O	X	X
Hong Kong	X	X	O[84]

Legend: X = Yes; O = No; Blank = no reliable data source found

79 *Cfr.* Bert-Jaap, Koops, "Crypto Law Survey, Overview per country," (February 2013), <www.cryptolaw.org>

80 Argentina has signed the Wassenaar Arrangement, so export controls should be regulated according to the pre-December 1998 Arrangement, including the General Software Note.

81 There are no import controls, but export is controlled along the Wassenaar model.

82 France has signed the Wassenaar Arrangement for *export* controls, with the exception of the (pre- December 1998) General Software Note.

83 France used to restrict the domestic use and supply of cryptography for a long time. This restrictive legislation (authorization and declaration were required for almost all cryptography) was slightly liberalized since 1996.

COUNTRY	IMPORT CONTROLS	EXPORT CONTROLS	DOMESTIC LAWS AND REGULATIONS
Hungary	X	X	X
Iceland			O
India	X		X
Indonesia	O		
Iran			X
Ireland	O	X	X
Israel	X	X	X
Italy	X	X	X
Japan		X	O
Kazakhstan	X	X	X
Kenya	O		O
Kyrgyzstan		O	
Latvia	X	X	O
Lithuania	X	X	O
Luxembourg	X	X	O
Malaysia	O	O	O
Mauritius	O	O	O
Mexico	O	O	O
Moldova	X	X	O
Morocco	X	X	X
Netherlands	X	X	X
New Zealand	X	X	O
North Korea[85]			
Norway	O	X	O
Pakistan			X
Peru	O	O	O
Philippines			O

Legend: X = Yes; O = No; Blank = no reliable data source found

84 There are no regulations on the use of encryption. Crypto products that are to be connected to the public telecoms network, however, must comply with the relevant Telecommunications Authority's network connection specifications.

85 When requested to provide information about its encryption laws, the government of the Democratic People's Republic of Korea stated that they never release such information.

Figure 2: Overview per Country of Cryptography Laws Continued

COUNTRY	IMPORT CONTROLS	EXPORT CONTROLS	DOMESTIC LAWS AND REGULATIONS
Poland	X	X	O
Portugal		X	O
Puerto Rico	O		O
Romania	O		
Russia			O
Rwanda			
Saudi Arabia	O	O	X
Singapore	O	X	O
Slovakia		X	
Slovenia			X
South Africa	X[86]	X[87]	X
South Korea	X	X	X
Spain		X	X
Sweden	O	X	X
Switzerland	O	X	O[88]
Syria			O
Thailand			X
Tonga			X
Trinidad & Tobago			X
Tunisia	X		X
Turkey			
Ukraine	X	X	X
United Kingdom	X	X	X
United States of America	O	X[89]	X
Uruguay	O		O
Venezuela			O
Vietnam	O		

Legend: X = Yes; O = No; Blank = no reliable data source found

86 There are import and export controls for military cryptography. Otherwise crypto import and export is free.

87 Use of encryption is free for commercial or private organizations.

88 Apart from these two specific regulations, there are no domestic crypto regulations.

89 The US has signed the Wassenaar Arrangement, but does not implement the (pre-December 1998) General Software Note and generally maintains stricter controls.