UACES 45th Annual Conference

Bilbao, 7-9 September 2015

www.uaces.org

Towards a Licence-free Europe?
Impact and Reform of the EU Directive on Intra-Community Transfers of Defence–Related Products

Martin Trybus* and **Luke R. A. Butler****

EU law; free movement of goods; national security; harmonisation

Work in progress: do not cite without permission!

Abstract. *Member State recourse to security derogations has restricted the free movement of defence goods within the Internal Market. Generalised security concerns have also meant that Member States have applied variable national laws and policies on the transfer of defence goods between Member States within the EU on terms equivalent to exports to third countries outside the EU. Consequently, significant costs and delays have been incurred through bureaucratic and restrictive licensing requirements. As part of the Commission's "Defence Package", the Intra-Community Transfers Directive 2009/43/EU ("ICT Directive") was adopted in 2009 introducing a harmonised transfer licensing and certification regime. The ICT Directive will soon be revised but has not yet been the subject of detailed legal analysis. Based on currently available data, this article investigates the ICT Directive's impact with a view to reform. It will be argued, inter alia, that due to insufficient harmonisation, national laws and practices have not changed significantly in form and effect as a result of the ICT Directive's implementation as an export control mentality continues to dictate. Adjustments are necessary to meet the ICT Directive's objectives.*

1. Introduction

Many EU Member States have defence industries[1] which form part of a global defence market in which, in 2013, the top 100 defence producers sold goods and services to an equivalent value of US$402 billion.[2] Companies of the 'Big Six' defence producing Member States[3] sell to their respective governments and, to a lesser extent other Member States, as well as export to third countries. While the regulatory framework of the Internal Market has largely benefitted trade in most goods, the interpretation and application of security derogations in the founding Treaties have largely prevented an Internal Market for armaments. However, a 2008 Editorial for the *European Law Review* introduced the academic community to the then imminent Commission "Defence Package".[4] The Defence Package consists of three elements: the Defence and Security Procurement

*Professor of European Law and Policy and Director of the Institute of European Law at the University of Birmingham and Senior Research Fellow at RAND Europe.

**Lecturer in Law at the University of Bristol.

[1] The European defence industries have an estimated annual turnover of €55 billion and employ 300,000 people. See 2007 figures of the Commission Communication *A Strategy for a Stronger and More Competitive European Defence Industry* COM (2007) 764 final, at 2, also indicating that 20 years ago these figures were almost twice as high. The 2010 *Study on the Impact of Emerging Defence Markets and Competitors on the Competitiveness of the European Defence Sector* (ECORYS, Teknologisk Institut, Cambridge Econometrics, CES Info, DEA Consult: for the European Commission) http://ec.europa.eu/enterprise/sectors/defence/files/study_defence_final_report_en.pdf [accessed 24 March 2015] reports even higher figures. It can be assumed that the 2015 figures are lower.

[2] Stockholm International Peace Research Institute (SIPRI) in their 14 December 2014 press release, see: http://www.sipri.org/media/pressreleases/2014/SIPRI-Top-100-December-2014 [accessed 21 January 2015]. The Top-100 of arms producers list contains many EU-based companies.

[3] These are generally said to comprise France, Germany, Italy, Spain, Sweden and the United Kingdom. For a discussion of this grouping, see M. Trybus, *Buying Defence and Security in Europe: the EU Defence and Security Procurement Directive in Context* (CUP, Cambridge 2014), 26.

[4] P. Koutrakos, 'The Commission's 'defence package' (2008) 33 E.L. Rev. 1-2.

Directive 2009/81/EC ("Defence and Security Procurement Directive"),[5] the ICT Directive[6] and a Commission Communication on the EU Defence Market.[7] The Defence and Security Procurement Directive, arguably the most significant part of the package, has been discussed in numerous publications including those of one of the authors.[8] By contrast, the ICT Directive has not been the subject of similarly detailed legal analysis.[9]

An intra-Community[10] transfer can be conceptualised as the transmission or movement of defence products from a supplier in one Member State to a recipient in another Member State.[11] Transfers may take the form of Member State-Member State, Member State-economic operator (and *vice versa*) and economic operator-economic operator transmissions or movements.[12] Whilst Member States have adopted significant measures outside the framework of EU law to safeguard against uncontrolled re-export of defence material to third countries, they have similarly adopted national laws and policies concerning intra-Community transfers. These include detailed authorisation and licensing measures. Such measures may contain disparities that not only restrict free movement but also distort competition.[13] In practical terms, significant delays and costs are also incurred. Consequently, such measures are said to hamper innovation, industrial cooperation and the competitiveness of the European defence industry.[14] Whilst these measures are *prima facie* subject to the TFEU free movement of goods regime, restrictions may be justified on a case-by-case basis in accordance with art.36 or art.346 TFEU. To the extent that restrictions cannot be justified, direct application of the free movement provisions is not, alone, considered sufficient to abolish such restrictions.[15] The ICT Directive attempts to institute a harmonised licensing and certification regime to eliminate or reduce these restrictions and achieve simplification.[16]

This paper aims to address an important gap in existing literature, offering a first legal analysis of the main provisions of the ICT Directive and their impact on national laws and practices.

---

[5] Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC, [2009] OJ L216/76.

[6] Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community [2009] O.J. L146/1.

[7] *Supra* note 1.

[8] M. Trybus, "The tailor-made EU Defence and Security Procurement Directive: limitation, flexibility, description, and substitution" (2013) 39 E.L. Rev. 3-29. This Directive is also the subject of a more extensive recent monograph of M. Trybus, *Buying Defence and Security in Europe: the EU Defence and Security Procurement Directive in Context* (CUP, Cambridge 2014). See also: B. Heuninckx, "The EU Defence and Security Procurement Directive: Trick or Treat? (2011) 20 P.P.L. Rev. 9; C. Kennedy-Loest and N. Pourbaix, "The New Defence Procurement Directive" (2010) 11 *ERA Forum* 399 T. Briggs, "The New Defence Procurement Directive" (2009) 18 P.P.L. Rev. NA129; A. Georgopoulos, "Legislative Comment: The new Defence Procurement Directive enters into force" (2010) 19 P.P.L. Rev. NA1-3.

[9] For a discussion in the political science/security studies literature, see H Masson, L Marta, P Léger, M Lundmark, 'The "Transfer Directive": perceptions in European countries and recommendations', researches & documents, Fondation pour la reserche stratégique, No. 04/2010. Available at: http://www.frstrategie.org/barreFRS/publications/rd/2010/RD_201004.pdf [accessed 21 January 2015]. For a brief overview of the ICT Directive in a legal context, see Trybus, *Buying Defence and Security in Europe: the EU Defence and Security Procurement Directive in Context*, *supra* note 8, at 139-156.

[10] The (December) 2009 Treaty of Lisbon replaced the term 'European Community' with the term 'European Union'. However, the (August) 2009 ICT Directive still uses the term 'Community'. Since 'Community' is the term used by the legislation which the subject of the article, the authors refer to 'intra-Community transfer'. A revision to the ICT Directive should refer to 'intra-Union transfers' to further symbolise the degree of harmonisation in this field.

[11] Based on the definition of 'transfer' in art.3(2) ICT Directive.

[12] Commission, 'Commission Staff Working Document, Accompanying document to the Proposal for a Directive of the European Parliament and of the Council on simplifying terms and conditions of transfers of defence-related products within the Community, Impact Assessment, SEC (2007), 1593, 11-12.

[13] Recital 3 ICT Directive.

[14] Ibid.

[15] Recital 5 ICT Directive.

[16] Recital 6 ICT Directive.

This article draws extensively on available data in the form of the *UNISYS Study*[17] to discern the *status quo ante*, the 2007 *Commission Impact Assessment* for the *intended* impact,[18] the 2012 *Transposition Report*[19] for the *formal* transposition into national laws, and, most importantly, the *GRIP Study*[20] for *actual* national laws and practices as of 2014.[21] In doing so, the paper reveals certain strengths and shortcomings of the regime, pre-empting an intended review of the ICT Directive's implementation which is due to commence in 2016 and which may, if necessary, be accompanied by a legislative proposal.[22]

The paper begins by situating transfers within the broader framework of EU law (Section 2) and historical context of transfers (Section 3). The article then examines the ICT Directive's general coverage (Section 4), licensing regime (Section 5), certification (Section 6), end use controls (Section 7), licence withdrawals and suspensions (Section 8) and review and remedies (Section 9) before offering some conclusions (Section 10). It will be argued that by moving from individual licences to general and global licenses, the ICT Directive merely lowers but does not remove barriers to trade. It does not create a "license-free" Europe. Moreover, due, *inter alia*, to the absence of sufficient harmonisation, many aspects of national laws and practices remain unchanged and largely replicate the treatment of third country exports. Adjustments will be necessary to enable the ICT Directive to meet is objectives.

2. Armaments under the TFEU

Armaments are goods for the purposes of EU law.[23] It follows that the free movement of goods constitutes the basic framework for determining restrictions to their intra-Community transfer.[24] For instance, it may be argued that licence fees alone constitute charges having equivalent effect to customs duties prohibited by art.30 TFEU.[25] Similarly, licensing requirements that impose significant administrative burdens and long lead times[26] may constitute measures having equivalent effect to quantitative restrictions contrary to art.34 TFEU.[27] However, armaments are subject to art.346(1)(b) TFEU which allows any Member State "to take such measures as it considers

---

[17] See Unisys, 'Intra-Community Transfers of Defence Products', Final Report of the Study 'Assessment of Community initiatives related to intra-community transfers of defence products', Brussels, February 2005 (study commissioned for the European Commission) 65 <http://www.edis.sk/ekes/en_3_final_report.pdf> [accessed October 2013]. This is no longer available at the time of writing but remains on file.

[18] *Impact Assessment*, *supra* note 12, 11-12.

[19] Commission, 'Report from the Commission to the European Parliament and the Council on transposition of Directive 2009/43/EC simplifying terms and conditions for transfer of defence-related products within the EU', COM(2012) 359 final.

[20] L. Mampaey, V. Moreau, Y. Quéau and J. Seniora, Final Report, *Study on the Implementation of Directive 2009/43/EC on Transfers of Defence-related Products*, Group for Research and Information on Peace and Security (GRIP) Commissioned for the European Commission, Brussels, 22 August 2014), see: http://www.grip.org/sites/grip.org/files/RAPPORTS/2014/Study%20on%20the%20implementation%20of%20Directive%20200943EC%20on%20transfers%20of%20defence-related%20products.pdf [accessed 10 March 2014].

[21] This also includes semi-structured interviews conducted with Mr. Ian Bendelow. Department for Business Innovation and Skills, United Kingdom, as well as other informal discussions with officials in certain Member States including Germany.

[22] Recital 41 and art. 17 ICT Directive.

[23] Recital 2 ICT Directive. Armaments can be valued in monetary terms and can be the subject of commercial transactions. See the definition of goods in Case 7/68 *Commission v. Italy ('Arts Treasures')* [1968] ECR 423, 429.

[24] Recitals 1 and 2 ICT Directive.

[25] *Commission v. Italy* (24/68) [1969] E.C.R. 193; [1971] C.M.L.R. 61*; Sociaal Fonds for de Diamantarbeiders v. Brachfeld* (2&3/69) [1969] E.C.R. 211; [1969] C.M.L.R. 335.

[26] See Section 3 of this article, below.

[27] This characterisation was repeatedly highlighted by the Commission, in the *Consultation Paper on the Intra-Community Circulation of Products for the Defence of the Member States* (DG Industry and Enterprise, Brussels, 21 March 2006) http://stopwapenhandel.org/sites/stopwapenhandel.org/files/imported/publicaties/2006/consult_en.pdf [accessed 10 February 2015], at 3 and Commission, 'Proposal for a Directive of the European Parliament and of the Council on simplifying terms and conditions of transfers of defence-related products within the Community' COM(2007) 765 final at 19.

necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material […]".[28] This derogation applies to the Treaty as a whole. In 1958, the Council drew up a list of products to which art.346(1)(b) TFEU applies.[29]

Many Member States had interpreted art. 346 TFEU as a categorical exemption of armaments from the scope of the Treaty and acted accordingly when drafting and applying their licensing rules.[30] This, at least, partly explains the late advent of the ICT Directive and the state of affairs discussed in Section 3 below. However, in *Spanish Weapons*, the ECJ clarified that art.346(1)(b) TFEU does not represent an automatic or categorical exclusion of armaments.[31] As it is a derogation, art. 346(1)(b) TFEU must be interpreted narrowly.[32] Member States must specifically invoke the derogation and prove that a situation justifying its use actually exists. This interpretation was reiterated in a 2006 Commission Interpretative Communication[33] and further refined in subsequent ECJ judgments.[34] As an instrument of secondary EU law, the ICT Directive does not prevent the possibility for Member States to continue to invoke the primary Treaty derogation.[35] However, the ICT Directive aims to harmonise national licensing regimes with the objective to eliminate disproportionate controls of the kind previously imposed by Member States pursuant to art.346 TFEU.[36] Further, even where a Member State considers the need to derogate to impose exceptional licensing measures on essential grounds, the ICT Directive aims to facilitate them within its scope with the objective to limit derogation from the EU Treaties as a whole.

3. Intra-Community transfers prior to the ICT Directive

For many years, the Commission has prioritised intra-Community transfers alongside procurement, competition, standardisation and export control as areas for the development of an EU defence market.[37] However, there had been no general EU-wide intra-Community transfer regime. Each of

[28] On art.346 TFEU in detail: M. Trybus, *Buying Defence and Security in Europe*, *supra* note 8 at 87-128; M. Trybus, *European Union Law and Defence Integration* (Hart: Oxford, 2005), Chapter 5 and M. Trybus, "The EC Treaty as an instrument of European defence integration: judicial scrutiny of defence and security exceptions", (2002) 39 C. M. L. Rev. 1347-1372. See also the interpretations of P. Koutrakos, "The Application of EC law to Defence Industries—Changing Interpretations of Article 296 EC" in Catherine Barnard and Okeoghene Odudu (eds.), *The Outer Limits of European Union Law* (Hart: Oxford, 2009), 307-328 and N. Pourbaix, "The Future Scope of Application of Article 346 TFEU" (2011) 20 P.P.L. Rev. 1-8.

[29] According to art.346(2) TFEU. See Council-Decision 298/58 of 15 April 1958 (not published).

[30] Whilst difficult to empirically validate, this assessment was made in the UNISYS study *supra* note 16 at 70-72.

[31] C-414/97 *Commission* v. *Spain* [1999] E.C.R. I-5585, [2000] 2 C.M.L.R. 4.

[32] *Johnston* (222/84) [1986] E.C.R. 1651, [1986] 3 C.M.L.R. 240, para. 26. See also *Salgoil* (C-13/98) [1968] E.C.R. 453, 463, [1969] C.M.L.R. 181, 192 and *Commission* v. *Italy* (C-7/68) [1968] E.C.R. 633, 644.

[33] Commission, 'Interpretative Communication on the Application of Article 296 of the Treaty in the field of defence procurement' (Communication) COM (2006) 779 final.

[34] See the *Agusta* judgments (*Commission* v. *Italy* (C-337/05) [2008] E.C.R. I-2173 and *Commission* v *Italy* (C-157/06) [2008] E.C.R. I-7313); the *Military Exports* judgments (*Commission* v. *Finland* (C-284/05) [2009] E.C.R. I-11705; *Commission* v. *Sweden* (C-294/05) [2009] E.C.R. I-11777; *Commission* v. *Italy* (C-387/05) [2009] E.C.R. I-11831; *Commission* v. *Greece* (C-409/05) [2009] E.C.R. I-11859; *Commission* v. *Denmark* (C-461/05) [2009] E.C.R. I-11887; *Commission* v. *Portugal* (C-38/06) [2010] E.C.R. I-1569; *Commission* v. *Italy* (C-239/06) [2009] E.C.R. I-11913) and *Finnish Turntables* (*Insinööritoimisto InsTiimi Oy* (C-615/10), n.y.r., 7 June 2012)

[35] Recitals 5, 13 and art.1(3) ICT Directive.

[36] See the *Impact Assessment*, *supra* note 12, at 4: "[t]his patchwork of licensing requirements - and the corresponding administrative burden – clearly appear to be *out of proportion* with actual control needs", and even more clearly at 13: "Intra-community transfers of defence-related goods hindered by cumbersome and *disproportionate* procedures*"*. (emphasis added).

[37] See COM (1996) 10 final, at 19; COM(1997)583 final, Annex I: Draft Common Position on Framing a European Armaments Policy, Article 5;, Annex II: Action Plan for the defence-related industries at 3 and timetable on page 10; COM(2003)113final, was another initiative; see also Council Regulation 428/2009/EC setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (recast) [2009] O.J. L134/1, Annex I: Draft Common Position on Framing a European Armaments Policy, Article 5;, Annex II: Action Plan for the defence-related industries at 3 and timetable on page 10; COM(2003)113final, was another initiative; see also Council Regulation

the 28 Member States instituted their own national legislation and policies to regulate the import, export and transit of armaments.[38] As part of an extensive consultation, in 2005, the EU commissioned a study on intra-Community transfers. *UNISYS* conducted this study based on extensive data collected through questionnaires and structured interviews which revealed significant obstacles to effective internal transfers arising as a result of national licensing regimes.[39] Through national laws, policies and practices, Member States had formally treated the internal transfer of defence products within the EU and their export to third countries without distinction.[40] National *ex ante* export licences would be required in both instances.[41] To this extent, national rules were not specifically adapted to differentiate EU internal market law obligations and any other legal obligations with regard to export. Thus, measures that might otherwise be appropriate for application where there was a risk of export and diversion to third parties involved in conflict or terrorism were equally applied to transfers to relatively peaceful Member States within an otherwise deeply integrated EU. This situation was criticised in many quarters not least the European defence industries.[42] Whilst it has been suggested that, in practice, export applications to other EU or NATO countries were probably subject to less scrutiny than exports to other third countries,[43] the formal application of variable national export regimes had a number of consequences. According to *UNISYS*, the simple existence of many different laws was, in itself, "a serious burden for intra-community transfers" resulting in a lack of knowledge on the part of many traders, the absence of a common information system, and language variations, all of which created considerable administrative burdens.[44]

The *UNISYS* study identified numerous barriers to trade.[45] In certain Member States, licences could be obtained for several years whereas in other Member States, licences were required for every single shipment.[46] Time limits for licence expirations also varied.[47] Renewals were often possible but requirements for renewal and the length of permissible renewals also varied.[48] Member States used different armaments lists to determine the scope of coverage of licences,[49] often containing idiosyncratic modifications to reflect national laws and cultures.[50] This also meant that companies had to comply with variable regimes when transferring components between subsidiaries located in several countries.[51] Most national laws did not specify detailed or transparent licensing criteria.[52] Determinations were, therefore, at the absolute discretion of licensing authorities.[53] Further, the allocation of responsibility was not always clear.[54] More than one body could be

---

428/2009/EC setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (recast) [2009] O.J. L134/1.

[38] *UNISYS*, *supra* note 16, at 12; *Impact Assessment*, *supr*a note 12, at 4.

[39] *UNISYS*, *supra* note 16.

[40] *Impact Assessment*, *supra* note 12, at 4.

[41] *UNISYS*, *supra* note 16, at 12-14; *Impact Assessment*, ibid., at 13.

[42] See the President of the European Defence Industries Group Corrado Antonini: "Political Harmonisation and Consolidation", EMP conference on the Future of the European Defence Industry, Brussels, 10-11 December 2003 as cited in *UNISY*S, ibid., at 80.

[43] See, for instance, the German practice prior to the adoption of the ICT Directive in H. Masson, L. Marta, P. Leger, M. Lundmark, 'The "Transfer Directive"', *supra* note 9 at 18. For a useful analysis of national licensing regimes prior to the Directive, see ibid 15-32 and *UNISY*S, supra note 16, at 8-36 and Annex D.

[44] *UNISYS*, *supra* note 16, at 12 also at 59 and 64.

[45] For a detailed discussion, see *UNISYS*, *supra* note 16, Ch.4.

[46] ibid 62.

[47] ibid

[48] ibid.

[49] ibid at 9 citing: the 1958 list / art.[346]; the 1991 list on European embargoes; the 1998 EU common list/ EU Code of Conduct on Arms Exports; the 2003 list/ customs regulation [2003] OJ C-314/1, the Wassenaar list (the most recent version of which is cited at note 93 of this article, and individual lists referred to in the national legislation.

[50] C. Mölling, "Options for an EU regime on intra-Community transfers of defence goods" in David Keohane (ed.), *Towards a European Defence Market*, Chaillot Paper 113 (EU Institute of Security Studies: Paris, 2008), 51, at 58.

[51] *Impact Assessment*, *supra* note 12, at 4.

[52] *UNISYS*, *supra* note 16, at 61.

[53] *Impact Assessment*, note 12, at 14.

[54] *UNISYS*, *supra* note 16 at 13 and 60-61.

designated with licensing approval responsibility and, in many cases authorities were obliged to consult with others prior to approval.[55] This could result in a need to obtain multiple additional licenses.[56] Stages in licensing procedures also varied.[57] Moreover, certain national laws required that additional (pre-)licenses be obtained or a fee paid before export/import/transit licenses could be approved.[58] Finally, the processes for certifying reliable defence exporters were also based on varying national practices.[59]

These issues resulted in significant administrative burdens for companies, generating long lead times, in some cases up to several months.[60] On the basis of available evidence, it is difficult to assess the indirect costs.[61] According to *UNISYS*, the estimated direct costs for the 12,627 licences procedures conducted in 2003 amounted to €238 million.[62] In 1998, the European Defence Industries Group ("EDIG") estimated their direct costs for export control measures at €107.1 million or 0.22 per cent of annual turnover of defence related activities.[63] The 2007 Communication *A Strategy for a Stronger and More Competitive European Defence Industry* reported "red tape" costing industry €400 million per year.[64]

These costs are rendered even more stark when it is considered that licences were rarely refused. According to *UNISYS*, 12,627 license applications were made in 2003 for conventional defence products delivery between the then 25 EU Member States, with an overall value of €8.9 billion.[65] This represents approximately 31.4 per cent of all transfers, with the remainder being exports to third countries.[66] Out of this total, only 15 licences were refused, all in the Baltic States.[67] There were no refusals anywhere else in the Union, including in the 'Big Six' major defence producing Member States. This provides a clear indication that disproportionate licencing regimes were not justified in light of limited internal control needs.[68]

Based on the findings of the UNISYS study, in 2006, a public debate was launched with a *Consultation Paper*.[69] This precipitated the 2007 *Impact Assessment*[70] and proposal for a Directive.[71] The *Impact Assessment* had considered alternatives, including taking no action, various licence and certification combinations and even a centralised EU licencing agency. Most of these alternatives will be discussed below to the extent otherwise considered viable. The *status quo* was rejected due to the perceived disadvantages: the continued fragmentation of the market along national lines, the delay of necessary defence industry consolidation, the risks of discrimination between operators covered by intergovernmental regimes outside the EU and other EU operators, the difficulty of integrating Small and Medium Sized Enterprises ("SMEs") from new Member States in supply chains, the gradual technological decline as the critical mass of industries remained insufficient, the progressive exclusion from the highest value-added market segments, and, finally,

[55] ibid and *Impact Assessment*, supra note 12 at 13.
[56] *UNISYS*, *supra* note 16,at 15-16..
[57] ibid, at 17-24 on the different procedures. See also: Mölling, *supra* note 49, at 58.
[58] *UNISYS*, *supra* note 16, at 61; *Impact Assessment*, *supra* note 12, at 14.
[59] Mölling, *supra* note 49, at 59.
[60] *UNISYS*,, *supra* note 16, at 5; *Impact Assessment*, *supra* note 12, at 14 and Mölling, *supra* note 49 at 61-62 and 68.
[61] *UNISYS*, *supra* note 16 at 112 estimates the indirect costs related to the obstacles to intra-Union transfers at €2.73 billion.
[62] ibid.
[63] ibid.
[64] *Impact Assessment*, *supra* note 12, at 4.
[65] *UNISYS*, *supra* note 16, at 94.
[66] ibid, 95. The UNISYS Study reports that this percentage is in line with the turnover reported by large European enterprises: e.g. Thales reports a military turnover of 30 per cent inside the EU and 70 per cent outside. Ibid at fn 79 citing "Interview D. L. August 2004".
[67] ibid., at 94: six in Estonia and Latvia each, and three in Lithuania.
[68] *Impact Assessment*, *supra* note 12, at 4.
[69] Commission, Consultation Paper on the Intra-Community Circulation of Products for the Defence of Member States, 21 March 2006, Brussels, ENTR/C.
[70] *Supra* note 12.
[71] *Proposal*, *supra* note 27.

the resulting erosion of competitiveness, sanctioned by loss of market share in both EU and third countries.[72]

Until the ICT Directive, transfer licences had only been the subject of one serious intergovernmental initiative, namely the 1998 Letter of Intent ("LoI"), to which an exclusive number of EU Member States are currently signatories.[73] The LoI created a *Framework Agreement*, one objective of which was to simplify transfer licences.[74] Attempts were made *inter alia* to introduce the 'Global Project Licence' which was designed to remove the need for specific authorisations to destinations permitted by the licence between LoI partners participating in collaborative projects.[75]

The co-existence of supranational EU law and intergovernmental LoI initiatives may become increasingly contentious as the speed of harmonization continues to vary between Member States. Whilst it has been observed that the LoI proposals have not been fully executed in practice and with limited results,[76] the LoI remains an important forum for consultation not only for Member States seeking greater harmonization than is currently provided by the ICT Directive but as a means to further inform and influence the future development of the ICT regime.[77] For instance, art.1(4) ICT Directive appears to acknowledge the continued possibility for Member States to pursue and further develop intergovernmental cooperation whilst complying with provisions of the Directive.[78] Similarly, art.4(3)(c) ICT Directive provides for a Member State or the Commission to add intergovernmental cooperation as one of the circumstances which are exempt from a requirement of prior authorization. However, from an EU law perspective, EU Member States may not confer powers to organisations outside the EU which have already been conferred to the EU as this would *inter alia* violate the loyalty clause in art.4(3)TEU.[79] The ICT Directive now confirms Internal Market competence in the field of intra-Community transfers and licensing. Therefore, it is likely that any framework outside this instrument can only be used after a successful invocation of art.346(1)(b)TFEU which is likely to be extremely limited for the reasons indicated in the preceding Section. Therefore, it is submitted that while Member States may exceptionally impose specific requirements for transfer licenses which result from policies determined within organisational frameworks outside the EU, general and abstract licensing regimes outside the TFEU are difficult to reconcile with EU law. Moreover, the limited membership of the LoI risks potential discrimination against excluded Member States which may, in turn, dis-incentivise their efforts to cooperate.[80] Member States must invoke art.346 TFEU to exempt licensing requirements that do not comply with the ICT Directive, the permitted circumstances for which are likely to be highly exceptional. This apparent tension should be kept firmly in mind when considering the extent to which the ICT Directive strikes an effective balance between the internal harmonization objective and the continuation of intergovernmental initiatives outside this framework.

Having considered several policy options, the Commission opted for a Directive rather than a Regulation based on the "primary responsibility" of Member States for simplification of licencing

[72] ibid., at 44.

[73] Letter of Intent between the Defence Ministers of the UK, France, Germany, Italy, Spain and Sweden on Measures to facilitate the Restructuring of the European Defence Industry signed in London, 6 July 1998. For a general discussion of the LoI, see Trybus, *Buying Defence and Security in Europe*, *supra* note 8, at 225-231.

[74] Framework Agreement between The French Republic, The Federal Republic of Germany, The Italian Republic, The Kingdom of Spain, The Kingdom of Sweden and The United Kingdom of Great Britain and Northern Ireland Concerning Measures to Facilitate the Restructuring and Operation of the European Defence Industry signed during the Farnborough Air Show on 27 July 2000. The Framework Agreement entered into force on 2 October 2003.

[75] Article 7, Framework Agreement.

[76] See *Impact Assessment*, *supra* note 12, 9 and 18.

[77] We are grateful to Mr. Ian Bendelow for elaborating on the continuing role of the LoI in this regard.

[78] See also Recital 8 ICT Directive. It is understood that Article 1(4) ICT Directive was introduced to ensure the continuation of the LoI initiative in this field. We are grateful to Mr. Ian Bendelow for this observation.

[79] Trybus, *Buying Defence and Security in Europe*, *supra* note 8, at 227 citing at fn 241 observations by Dr. Baudouin Heuninckx.

[80] *Impact Assessment*, *supra* note 12, at 6.

and the general sensitivity of defence.[81] On 6 May 2009, the ICT Directive was adopted. Member States were given until 30 June 2011 for transposition.[82] However, national provisions did not have to enter into effect until 30 June 2012, allowing for a period of deferral in which to "foster mutual trust".[83] In 2012, the Commission published a *Transposition Report*.[84] According to the Report, twenty Member States had transposed the ICT Directive fully, one had transposed partially, six Member States expected transposition in 2012 and one had not communicated transposition.[85] The Commission initially launched infringement proceedings for non-communication against seven Member States.[86] At the time of writing in 2015, the ICT Directive has been formally transposed by all Member States.[87]

4. General coverage of the ICT Directive

Art.1 ICT Directive identifies its aim to simplify the rules and procedures applicable to intra-Community transfers of defence related products.[88] At the outset, it is important to acknowledge, therefore, that the ICT Directive does not purportedly affect Member State policies regarding the transfer of defence-related products[89] nor discretion as regards policy on export of defence related products.[90] An overarching concern, which has not been fully acknowledged, is the extent to which it is possible to fully realise the ICT Directive's harmonisation and simplification objectives given that Member States continue to retain competence to determine policy not only on intra-Community transfers but also exercise discretion in relation to export control policy. This paper does not address the legal compatibility or coordination of these regimes. However, as the very least, fundamental issues of respective competences signal a further tension that the ICT Directive may either exacerbate or reduce to a degree which remains uncertain.

4.1. Scope

According arts.2 and 3(1), the ICT Directive applies to defence-related products.[91] These are set out in its Annex, which must correspond with the EU Common Military List ("CML")[92] adopted in the context of Council Common Position 2008/944/CFSP,[93] and updated annually by the Council.[94]Art. 13(1) ICT Directive requires the Commission to update the list set out in its Annex in order to

[81] *Proposal*, *supra* note 70, at 8.
[82] Article 18(1) ICT Directive.
[83] See Recital 40, Articles 17(1) and 18(1) ICT Directive.
[84] In accordance with art.17(1) ICT Directive. See *Supra* note 18.
[85] ibid, at 15-19.
[86] ibid, at 5.
[87] Thanks to our colleagues Marcin Spyra (University of Krakow), Dacian Dragos (Babes Bolaj University of Cluj Napoca), Kirsi-Maria Halonen (University of Turku), Baudouin Heuninckx (University of Nottingham and Belgian Military Academy) Roberto Caranta (University of Turin), Pedro Telles (University of Swansea), and Steen Treumer (University of Copenhagen) for assistance in locating the relevant laws of the Member States that had not fully transposed in 2012. Croatia only joined the Union in 2013 in full compliance with the entire *acquis*.
[88] Article 1(1) ICT Directive.
[89] Recital 6 ICT Directive. Of course, this is only to the extent that Member State policies are not otherwise affected by the ICT Directive's rules and procedures.
[90] Article 1(2) ICT Directive. See also Recital 30 ICT Directive.
[91] The ICT Directive does not apply to defence-related products which only pass through the territory of the Community. See Recital 9 ICT Directive.
[92] Common Military List of the European Union [2007] O.J. L88/58. See also Recital 10 ICT Directive. This list must not be confused with that of Council Decision of 1958 (art.346(2) TFEU list), *supra* note 28, which determines the material scope of art.346(1)(b)TFEU.
[93] Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment [2008] O.J. L335/99-103.
[94] It is updated usually as a consequence of an amendment to the 'Munitions List' adopted in the framework of the Wassenaar Arrangement. The latest version is 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 (14) 2* 25 March 2015.

strictly correspond to the CML[95] and which has, to date, already been amended three times.[96] Therefore, whilst Member States continue to operate national military lists, the ICT Directive's application to products corresponding to the CML is intended to address the criticism concerning the variable use of national lists identified in the *UNISYS* Study. However, the attempt to coordinate lists has exposed the difficulties of ensuring harmonisation. Firstly, the *Transposition Report* singles out the Annex as creating legal and administrative divergences which go against the ICT Directive's legislative intention.[97] The Annex should be identical to the CML at all times but the procedure for amendment of the Annex has, in practice, taken at least seven months followed by a further transposition of the amendment by Member States.[98] Thus, the Annex does not fully correspond to the CML for at least seven months of the year. The Commission therefore considers it necessary to simplify the procedure for aligning Annex and CML.[99] Secondly, Member States ultimately determine the type of products covered by a licence prescribed under the ICT Directive.[100] Thus, there is a risk that some Member States may adopt a very short list of products or relevant lists of products may vary thereby prohibitively discouraging use of the ICT regime. Therefore, the success of general transfer licences under the ICT Directive may depend, to a significant extent, on how Member States define their scope.[101]

These concerns are confirmed by the *GRIP* Report.[102] According to *GRIP*, the danger of short lists appears to be a lesser problem but Member States practice in defining the scope of lists in terms of products covered "varies greatly […] and patterns are difficult to establish".[103] While many Member States use the CML as a reference point, national exclusions lead to significant differences.[104] Certain other Member States use their own lists or different lists for different general transfer licences.[105] Member States also appear to define the scope of their general transfer licences case-by-case and based on factors such as the recipient in question, the sensitivity of the product, risk assessment and diversion risk.[106] This apparent 'diversity' of scope is further exacerbated by the lack of consensus between Member States as to how to define or classify "sensitive" products which legitimate their exclusion from the scope of a general licence.[107] In terms of the practical effects, *GRIP* identifies a lack of "visibility and clarity" of different national lists,[108] making the use of general transfer licences less attractive for companies, especially in the case of licences for those companies certified under the ICT Directive's certification regime.[109]

It is submitted that if Member States continue to retain national lists, visibility and clarity can be improved in various ways, either by harmonising certain requirements in a revised ICT Directive or by soft means, such as a guidance note, seminars or information exchange between the Commission and Member States.[110] For instance, these requirements should include increased

[95] Recitals 37 and 45 and art.13(1) ICT Directive.
[96] Commission Directive 2010/80/EU [2010] O.J. L308/11; Commission Directive 2012/10/EU [2012] O.J. L85/3; Commission Directive 2014/108/EU [2014] O.J. L359/117.
[97] *Transposition Report*, *supra* note 18, at 13.
[98] ibid.
[99] ibid. See also *GRIP Report*, *supra* note 19, at 64.
[100] See Section 5 below. According to the *Transposition Report*, *supra* note 18, at 9, several Member States had already communicated their general licences list to the Commission.
[101] According to the *Transposition Report*, ibid,, at 9 only six Member States had communicated their respective lists to the Commission.
[102] *GRIP Report*, *supra* note 19, at 23-27.
[103] ibid, at 27. According to the *GRIP Report*, at fn21, it seems that some countries have allowed a greater scope for "temporary transfers" (demonstration, evaluation, repair, maintenance) under general licences.
[104] Ibid, at 29.
[105] Ibid., at 23-27. According to the *GRIP Report* at 25, Luxembourg appeared to be the only country referring to the most recent version of the Annex of the ICT Directive in the definition of defence-related products covered by its general transfer licences.
[106] ibid, at 23.
[107] ibid, at 38.
[108] Ibid., at 27.
[109] Ibid, at 39. Certification under the ICT Directive is discussed in Section 6 below.
[110] Exchanges of information are already expressly envisaged by art.12 ICT Directive.

visibility of, and access to, national websites identifying national lists and could include publication of lists in English. A more fundamental question concerns the scope of national discretion left to Member States. At present, the diversity of national practices could be indicative of a need felt, in practice, to retain flexibility in defining the scope of licences to ensure that as many general transfer licences can be issued as possible. However, as indicated, the ability of Member States to exclude products from a list creates considerable uncertainty which may favour further harmonisation.

To this extent, it is argued that the ICT Directive should include a harmonised list of covered products using the CML as an already widely used reference point with clearer correspondence to the Wassenaar List.[111] Ideally, a harmonised list would be comprehensive and based on a common understanding of "sensitive products" that should be definitively included or excluded from the list. As will be discussed below, the ICT Directive has already sought to define the "sensitivity of transfer" in relation to components.[112] However, as the *GRIP Report* has observed, it appears impossible at this stage to recommend a detailed list of categories of sensitive or defence-related products to be excluded that would be accepted by all Member States.[113] Therefore, The *GRIP Report* recommends that a positive or minimum list should be adopted.[114] Whilst it must be acknowledged that such an approach could result in the "lowest common denominator" this could, at least, reduce routine exclusions. Several Member States and companies have called for the feasibility of such a list "while taking into account national limitations".[115] It is unclear whether a revised ICT Directive would need to include specific provisions identifying precisely what these "national limitations" are. If so, the ICT Directive could similarly ensure that these national limitations are not applied to circumvent the objectives of the ICT Directive. At the very least this would increase clarity and thereby encourage the use of general transfer licences in practice.

4.2. Transfers

A fundamental innovation of the ICT Directive is the qualitative differentiation of transfers from exports so that the former can no longer be treated as generally equivalent to the latter through disproportionate controls. Whilst all Member States enjoy relatively sustainable peace and security, there are crisis regions in many third countries. Transfers to the former do not generally involve the same political and strategic concerns as exports to the latter, necessitating a lighter regime to facilitate an Internal Market for armaments. The ICT Directive now provides for a legal definition of "transfers" and does not define the term "exports". Article 3(2) ICT Directive defines a 'transfer' as "any transmission or movement of a defence-related product from a supplier[116] to a recipient[117] in another Member State".[118]

Whilst as indicated below, a transfer will generally be subject to prior authorisation, no further authorisation must be imposed on an authorised transfer for "passage through".[119] "Passage through" is defined as a "transport through one or more Member States other than the originating and receiving Member States".[120] Similarly, no further authorisation must be imposed for entrance

[111] The *GRIP Report*, *supra* note 19 at 63 places particular emphasis on design of the List based specifically on the Wassenaar List.
[112] See Section 5 below and which may further evidence the difficulty of determining what is "sensitive" for the purposes of determining the scope and application of the ICT Directive.
[113] *GRIP Report*, *supra* note 20, 39.
[114] Ibid 63.
[115] Ibid 48 and 63.
[116] Article 3(3) ICT Directive defines a supplier as the legal or natural person established within the Community who is legally responsible for a transfer.
[117] Article 3(4) ICT Directive defines a "recipient" as a legal or natural person established within the Community who is legally responsible for the receipt of a transfer.
[118] Article 3(2) ICT Directive.
[119] art.4(1) ICT Directive.
[120] Recital 17, art.3(7) and art.4(1) ICT Directive.

onto the territory of a Member State where the recipient is located.[121] Crucially, however, the prohibition on further authorisation is without prejudice to provisions necessary on public policy or public security grounds such as, *inter alia*, the safety of transport.[122] A Recital to the ICT Directive also refers to safety of storage, the risk of diversion and the prevention of crime.[123] According to the *Transposition Report*, no Member State which had transposed the ICT Directive permits passage and entrance licences other than on the basis of the above exceptions contained in the ICT Directive.[124] The *Report* is not unequivocal in this regard. For instance, it states that Germany will require a general licence for entrance and passage licences only for "war weapons".[125] The Netherlands will adopt a "previous notification system".[126] Hungary will require passage licences for certain categories of products and maintain entrance licences.[127] The above suggests that the legal basis for imposing prior authorisation for passage through and the types of measures used continues to remain unclear. It is submitted that a revised ICT Directive should clarify these grounds to enable a further degree of harmonisation.

4.3. Transfer licences

The ICT Directive facilitates the progressive replacement of individual *ex-ante* control through strict licensing of internal transfers by instituting a broader licensing regime containing reduced controls which are also compensated through *ex-post* monitoring.[128] However, in light of opposition by both Member States and most of industry to the alternative of a European "licence-free zone",[129] the ICT Directive continues to subject transfers to at least some prior authorisation through 'transfer licences' which, for the reasons explained in Section 4.2 above, must be distinguished from 'export licences'.[130] The *Impact Assessment* identified two principal reasons for retaining a licensing regime. The first concerns the relative infancy of a common foreign policy and "uneven levels of trust" concerning the extent to which certain external borders are capable of maintaining sufficient control.[131] The second concerns the incompatibility of total liberalisation with existing national and EU commitments in the field of international control regimes.[132] Therefore, licensing was still considered necessary as a "vehicle" to carry possible re-exportation limitations.[133] Importantly, this further reinforces that export control continues to be an equal, if not overriding, concern in the ICT Directive's design.[134]

Before and after the adoption of the ICT Directive, three types of transfer licence were, and continue to remain, in place for both intra-Community transfers and exports of armaments: general,

---

[121] Article 4(1) ICT Directive.
[122] Ibid.
[123] Recital 14 ICT Directive. It is not clear to what extent these grounds similarly correspond to the sorts of measures accepted on security grounds in cases such as Case C-367/89 *Criminal Proceedings against Aimé Richardt and Les Accessoires Scientifiques SNC* [1991] ECR I-4621. See generally, Trybus, *European Union Law and Defence Integration* note 28, at 137-8.
[124] *Transposition Report*, *supra* note 18, 7. The Report does not precisely identify these exceptions.
[125] ibid.
[126] ibid.
[127] ibid.
[128] Recital 29 ICT Directive.
[129] *Impact Assessment*, *supra* note 12, at 74.
[130] Recital 16 and art.4(1) ICT Directive. Art. 3(5) ICT Directive defines a 'transfer licence' as: "an authorisation by a national authority of a Member State for suppliers to transfer defence-related products to a recipient in another Member State." Art. 3(6) ICT Directive defines an 'export licence' as: "an authorisation to supply defence-related products to a legal or natural person in any third country."
[131] *Impact Assessment*, *supra* note 12, at 24.
[132] Ibid. identifying Wassenaar and the Missile Technology Control Regime. Also acknowledged in Recital 28 ICT Directive.
[133] *Impact Assessment*, *supra* note 12, at 24-25.
[134] As the *GRIP Report*, *supra* note 19 observes at 60: "Member States have used the opportunity given by the Directive to impose specific restrictions in their general transfer licences in order to maintain the coherence of their arms export control policy."

global, and individual.[135] According to the *Transposition Report*, all Member States who had transposed the ICT Directive incorporated all three types of licence.[136] Whilst retaining the same general categories of licence, the significant point of departure for the ICT Directive is an attempt to change the *type* of licence predominantly used in practice away from restrictive individual licences towards broader general licences.

4.4. Licence exemptions

Before examining each type of licence, it should be emphasised that art.4(2) ICT Directive provides that Member States *may* exempt five forms of transfer from prior authorisation. Exemptions are an important feature in determining the ICT Directive's scope given that Member States retain the option whether or not to provide for these exemptions in their transposition.[137] These circumstances also provide preliminary indications as to potential future areas in which a license free space may be possible.[138] The first two circumstances are where the supplier or recipient is a governmental body or part of the armed forces and where the EU, NATO, the International Atomic Energy Agency or other intergovernmental organisations send supplies in the performance of their tasks.[139] Whilst supplier or recipient status as a governmental body or armed forces does not automatically eliminate security and export diversion risks, these risks are likely to be limited in transfers between allies in comparison to transfers where the supplier and/or recipient is a private economic operator. The *Transposition Report* indicates that not all Member States have transposed or made use of this exemption.[140] It is submitted that the ICT Directive should be amended to provide that such transfers are mandatorily excluded from prior authorisation, perhaps subject only to exceptional use of a general licence (unless a further justification can be provided for use of global or individual licences) on a public policy or security ground. As will be discussed below, art. 5(2)(a) ICT Directive prescribes the mandatory use of the general licence subject to prior authorisation in similar circumstances. The stated rationale appears to be to "greatly increase security of supply".[141] However, it is suggested that whilst a general licence may provide a formal guarantee of security of supply, an unrestricted transfer provides optimal security of supply for operational efficiency without need for a formal guarantee. Exceptional recourse to a general or other licence for such transfers could then provide for a formal guarantee of security of supply but only where absolutely necessary.

A third exemption concerns a transfer necessary for the implementation of a cooperative armament programme between Member States.[142] The importance attributed to cooperative programmes under the Defence Package is reflected in the provisions of both its Directives. The Defence and Security Procurement Directive contains a specific provision permitting the exclusion

[135] *Impact Assessment*, *supra* note 12 at 4. See also art. 4(4) ICT Directive.
[136] Citation.
[137] H. Ingels, "The Intra-EU Defence Trade Directive: Positive Goals" in Alyson J. K. Bailes, Sara Depauw, and Tomas Baum (eds.), *The EU Defence Market: Balancing Effectiveness with Responsibility* (Flemish Peace Institute: Brussels, 2011), 61, at 65.
[138] Article 4(3) ICT Directive further provides for the Commission on its own initiative or at a Member State's request to amend the Directive to exempt three additional circumstances: (1) where the transfer takes place under conditions which do not affect public policy or public security, (2) where the prior authorisation obligations have become incompatible with Member States' international commitments subsequent to the Directive's adoption, and (3) where the exemption is necessary for intergovernmental cooperation. According to this provision, these measures are designed to amend "non-essential elements" of the Directive and must be adopted in accordance with the procedure prescribed in art.14(2) ICT Directive.
[139] Article 4(2)(a) and (b) ICT Directive.
[140] *Transposition Report*, *supra* note 18, at 6.
[141] Recital 22 ICT Directive.
[142] Article 4(2)(c) ICT Directive. An example includes the *Eurofigher/Typhoon* fighter aircraft programme For a discussion of EU armaments collaboration, see B. Heuninckx, "A Primer to Collaborative Procurement in Europe: Troubles, Achievements and Prospects" (2008) 17 P. P. L. Rev. 123-145 and *The Law of Collaborative Defence Procurement Through International Organisations in the European Union*, Ph.D. thesis submitted to the University of Nottingham and the Belgian Royal Military Academy, July 2011 (on file).

of cooperative programmes based on research and development ("R&D") from its contract award procedures to ensure flexibility when procuring under, and executing, such programmes.[143] An exemption from prior authorisation for transfers is broadly consistent with this objective. Again, however, similar to the armed forces exemption, a question arises as to whether such transfers should not be subject to prior authorisation through licencing subject to exceptional use of a general or other licence only on public policy or security grounds One difficulty is that the ICT Directive may seek to differentiate between forms of cooperative programme. For instance, in contrast to possible exemption of cooperative armament programmes between Member States from prior authorisation, art.5(3) ICT provides that a Member State *may* publish a general transfer licence where Member States participate in an "intergovernmental cooperation programme concerning the development, production and use of one or more defence-related products". Any *prima facie* distinction is exacerbated by the fact that either form of cooperative programme could fall within the classification of the other.

Notwithstanding, under a revised ICT Directive, it is nevertheless possible to distinguish forms of cooperative programme which could be presumptively excluded from prior authorisation subject to authorisation in exceptional cases and those forms of cooperation which may *prima facie* be subject to prior authorisation or not at the option of Member States. For example, cooperative armaments programmes involving common purchases off-the-shelf equipment are not particularly complex[144] and could fall within the former category. By contrast, cooperative programmes involving R&D could fall within the latter category. This would align cooperative armament programmes based on R&D with intergovernmental cooperation programmes currently subject to optional prior authorisation and which, in light of their "development" component are likely to share certain similarities in this regard. This also corresponds to the fact that the ICT Directive already envisages that a Member State or the Commission may request an amendment to the ICT Directive to add intergovernmental cooperation to one of the five categories exempt from prior authorization discussed above.[145]

At present, whilst the ICT Directive attempts to offer relative flexibility between no prior authorisation and mandatory or optional minimum prior authorisation, it appears ambivalent as to how to approach these circumstances. This is exemplified by the vague provision stating that mandatory publication of general licences is "without prejudice" to the provisions enabling optional exemption.[146] Whatever the approach, the starting principle should be against prior authorisation to the extent possible.

A fourth exemption is where "the transfer is linked to humanitarian aid in the case of disaster or as a donation in an emergency."[147] In addition to enabling expeditious transfer, references to disasters and donations suggest that the material in question will not raise major security concerns. This exemption is also consistent with the EU's humanitarian obligations.[148]

The final exemption is where the transfer is necessary for or after repair, maintenance, exhibition or demonstration.[149] This exemption reflects a level of risk commensurate with the generally more limited capability of a product at the pre-production stage or that a product may have already been subject to licensing requirements after initial production. A number of Member

[143] See art.13(c) Directive 2009/81/EC. For a discussion of this provision, see Trybus, *Buying Defence and Security in Europe*, *supra* note 8, at 283-288.
[144] This is further reflected in the fact that contracts awarded under such programmes must generally be awarded in accordance with the Defence and Security Procurement Directive (in contrast to cooperative programmes based on R&D) under art.13(c) Defence and Security Procurement Directive.
[145] Article 4(3)(c) ICT Directive cited *supra* note 139. Curiously, art.4(3)(c) cross-references to art.1(4) ICT Directive which simply provides that Member States must ensure that suppliers wishing to transfer may use general, global or individual licences in accordance with the provisions which govern each type.
[146] Article 5(2) ICT Directive.
[147] Article 4(2)(d) ICT Directive.
[148] Articles 4(4) ICT Directive and 208-211 TFEU.
[149] Article4(2)(e) ICT Directive.

States have made use of this exception.[150]

According to the *Transposition Report*, out of the twenty Member States who had already fully implemented the ICT Directive in 2012, thirteen had used the first exception; eleven had used the second exception; twelve had used the third exception and nine had used the fourth exception.[151] While *GRIP* is silent on this matter, it can be said that although certain Member States have been prepared to formalise these exceptions, the combined effect of optional exclusions which have not been adopted by all Member States further inhibits the potential for harmonisation.

5. Licences under the ICT Directive

Member States are free to determine the appropriate choice of licence.[152] However, for reasons that will be explained in the remainder of this paper, the ICT Directive signals a clear emphasis on general transfer licences as the least restrictive. For the purposes of the ICT Directive, a general transfer licence is a specific authorisation granted to suppliers established in one Member State to perform transfers of defence-related products to be specified in the general transfer licence to categories of recipients located in another Member State.[153] The main distinguishing feature is that a Member State must publish it directly, granting authorisation to a supplier fulfilling its terms and conditions without requiring a specific request for each individual transfer.[154] Prior to the adoption of the ICT Directive, Member States, with the notable exception of the United Kingdom, did not provide for extensive use of general licences.[155] Thus, the ICT Directive has largely adopted the British model.[156] The Commission had considered a regime exclusively comprising the general transfer licence.[157] Whilst this regime could have minimised bureaucracy and significantly improved security of supply, such a regime was not considered acceptable EU-wide. For Member States with only limited defence industries, the costs of issuing general transfer licences might exceed those for individual licenses.[158] More importantly, the general transfer licence is not suitable for all types of equipment especially the most sensitive items.[159] Deprived of any flexibility in the use of other licences, Member States might have also sought to invoke art.346 TFEU thereby taking licensing outside the scope of EU law, undermining the ICT Directive's objectives. Whilst the ICT Directive therefore is a compromise also permitting use of global and individual licences, , the introduction of general transfer licences is an innovation offering at least the theoretical possibility for reduced administrative burdens and improved security of supply.

5.1. Circumstances requiring general licences

Article 5(2)(a)-(d) ICT Directive identifies a list of "at least" four circumstances in which publication of a general transfer licence is mandatory. To this extent, the ICT Directive envisages

[150] Bulgaria, Estonia, Greece, France, Malta, Austria, Slovenia, Slovakia and Sweden. See *Transposition Report*, *supra* note 18, 7.
[151] Ibid at 6 and 7.
[152] Article 4(5) ICT Directive.
[153] Article 5(1) ICT Directive.
[154] Article 5(1) and Recital 21 ICT Directive.
[155] *Impact Assessment*, *supra* note 12, at 15 and 34. The United Kingdom has widely implemented a general licence for military goods under Open General Export Licences ("OGELs"). For a useful discussion of British practice in this regard, see H. Masson et al, *The "Transfer Directive" supra* note 00 at 15-19. See also on the German practice with regard to general licences at 19.
[156] According to one respondent interviewed for this article, Mr. Ian Bendelow, this has enabled an effective transposition in the UK with relatively few adjustments to UK licensing practice. The Directive was implemented into UK legislation on 10 August 2012 via an amendment to the Export Control Order 2008, the UK's main export control legislation. The amendment is published as the Export Control (Amendment) (No 2) Order 2012 (SI 2012/1910).
[157] *Impact Assessment*, *supra* note 12, at 34-35.
[158] Ibid., at 35.
[159] *Impact Assessment*, *supra* note 12, at 35.

use of general licences in a wider range of circumstances.[160] Some Member States have published general transfer licences for other types of transfer, for example, in France for transfers to the police, customs, border guards, and coast guards.[161] A revised ICT Directive could further expand the list of circumstances for mandatory publication of a general transfer licence.

The first circumstance under art.5(2)(a) is where the recipient is part of a Member State's armed forces or a defence contracting authority, purchasing for the exclusive use by that Member State's armed forces.[162] The general rationale for this circumstance has been discussed above in relation to optional exemption from prior authorisation.[163]

The second circumstance under art.5(2)(b) is where the recipient is certified in accordance with the ICT Directive's certification provisions.[164] Certification is examined further below.

The third and fourth circumstances under art.5(2)(c) and (d) respectively are where the transfer is made for the purposes of demonstration, evaluation or exhibition or for the purposes of maintenance and repair if the recipient is the original supplier. It is recalled from the discussion on optional exemption from prior authorisation above that this provision reflects the level of risk attending pre- and post-production transfers. It is therefore questioned whether the control needs in such circumstances justify even a general licence. It is submitted that these circumstances could rather be the subject of exclusion from prior authorisation unless exceptional circumstances justify prior authorisation.

Additionally, it is recalled that art.5(3)ICT Directive provides that Member States participating in an intergovernmental cooperation programme *may* publish a general transfer licence for transfers necessary for the programme's execution.[165] According to the *Transposition Report*, some Member States have transposed this option.[166] Prior to the adoption of the Defence Package, the use (albeit limited) of general transfer licences was most common in cooperative programmes between larger countries, in particular, signatories to the LoI FA.[167] As indicated in Section 4.4 above, a revised ICT Directive may retain the option for Member States to require prior authorisation for transfers in intergovernmental cooperation programmes through the use of general licences but subject to certain clarifications in terms of scope of application.

Beyond the intended savings in terms of administration and cost, the mandatory use of general licences is also intended to have a specific impact on defence procurement, particularly on improving the ability of an EU economic operator's to provide a comparable guarantee of security of supply to that of a domestic economic operator when tendering for a defence contract. For instance, art23(a) Defence and Security Procurement Directive provides that in order to ensure security of supply, a contracting authority can require a tenderer to demonstrate that it will be able to honour its obligations regarding the export, transfer and transit of goods associated with the contract. It is usually the case that at the time of tender preparation, the authorisation to transfer

[160] Some indication is provided in Recital 25 ICT Directive which states: "[m]ember States should be able to publish further general transfer licences where the risk for the preservation of human rights, peace, security and stability is very low in view of the nature of the product and the recipients.

[161] Arrêté du 6 janvier 2012 relatif à la licence générale de transfert dans l'Union européenne de produits liés à la défense à destination de la police, des douanes, des gardes-frontières et des gardes-côtes d'un Etat membre dans un but exclusif d'utilisation par ces destinataires, JORF n°0008 of 10/01/2012, at 419. For other types of general licence identified as used in a range of Member States, see *GRIP Report supra* note 00, 19-22.

[162] See also Recital 22 ICT Directive which refers to the role of general transfer licences to "greatly increase security of supply" to armed forces. Security of supply is discussed in more detail below.

[163] Section 4.4. above.

[164] Article 9 ICT Directive concerns the certification of recipients of defence-related products, on which see below. See also Recital 23 ICT Directive.

[165] Recital 24 and art.5(3) ICT Directive as discussed in Section 4.4 above.

[166] *Transposition Report*, *supra* note 18, at 6. According to the *Grip Report*, *supra* note 19 at 19, the Flemish Region and Spain have published general licences on intergovernmental cooperation, in the latter case, concerning transfers which are the result of the participation of the Spanish Ministry of Defence and Spanish companies in its activities and operations of NATO and its agencies.

[167] *UNISYS, supra* note 17, 15. The LoI FA is discussed in Section 3 above and which is not to be confused with the global project licence under that initiative.

equipment will not yet have been granted, thereby possibly raising questions in some instances as to the non-domestic economic operator's ability to guarantee security of supply.[168] The Guidance Note on Security of Supply published to assist in the transposition of the Defence and Security Procurement Directive[169] suggests that this uncertainty is now removed in light of possible recourse to general transfer licences which will have already been published with the necessary authorisation.[170] However, the United Kingdom has indicated that whilst general transfer licences should provide some degree of security of supply, they can be withdrawn or granted with end-use restrictions that may continue hinder security of supply.[171] More fundamentally, it may be questioned to what extent security of supply can be guaranteed whatever licence is used an issue which the ICT Directive itself cannot fundamentally resolved. Notwithstanding, it is submitted that the ICT Directive could at least contribute significantly to enhancing security of supply through widespread uptake and use of general licences.

5.2. Licence terms and conditions and conditions for registration prior to first use

The ICT Directive contains general provisions applicable to all types of transfer licences with regard to their terms and conditions. For instance, it is recalled from Section 4.1 that visibility and clarity in the use of general licences has been affected by 'diversity' in the *condition*s imposed by Member States on the users of their general transfer licences.[172]

Article 4(6) provides that Member States shall determine all the terms and conditions of transfer licences, including any limitations on the export of defence-related products to persons in third countries. In this regard, Member States can "avail themselves of the possibility to request end-use assurances, including end-user certificates.[173] According to the *GRIP* Report there are several types of limitations on re-transfer and re-export. These include: non-re-export clauses in the licence itself imposing a total ban on export outside the EU or an obligation to ask for consent of the Member State of origin, or even a separate non-re-export certificate.[174] In this regard, certain Member States have exempted certain exports to allied third countries, EEA, NATO or other relevant intergovernmental organisations.[175] It is submitted that there is scope for harmonisation in a revised ICT Directive by introducing a standard form of export limitation and one list of 'allied countries' for all Member States.

Similarly, according to art.4(7), Member States shall determine the terms and conditions of transfer licences for components on the basis of an assessment of the sensitivity of the transfer.[176] The ICT Directive does not define 'components' but does prescribe two criteria according to which the sensitivity of the transfer is determined. The first is the "nature of the components in relation to the products in which they are to be incorporated and any end-use of the finished products which might give rise to concern".[177] The second is the "significance of the components in relation to the products in which they are to be incorporated".[178] Whilst the *GRIP Report* is silent on these potentially subjective criteria, it is recalled from Section 4.1 that the *GRIP Report* identified the difficulty of reaching a consensus on the issue of "sensitive" products for the purposes of the lists used for coverage of general licences. It may therefore be inferred that there is likely to be

[168] Guidance Note *Security of Supply*, http://ec.europa.eu/internal_market/publicprocurement/docs/defence/guide-sos_en.pdf [accessed 18 August 2015], at 10

[169] There is no comparable Guidance Note for the implementation of the ICT Directive although it must be observed that the issuance of such guidance is rare.

[170] Guidance Note *Security of Supply*, *supra* note 168, at 10.

[171] The Defence and Security Public Contract Regulations, Chapter 12 – Security of Supply, 7, para. 38.

[172] *GRIP*, *supra* note 19, at 38.

[173] ibid.

[174] Ibid. 33. For instance, the French certificate de non-reexportation en dehors de la l'UE-CNR.

[175] Ibid. citing the UK, Walloon, Estonia, Luxembourg, Spain, the Flemish Region and Denmark.

[176] See also Recital 18.

[177] Article 4(7)(a) ICT Directive.

[178] Article 4(7)(b) ICT Directive.

considerable variation regarding national assessments of the sensitivity of transfers with regard to components. According to art.4(8), where Member States do not consider the transfer of components, Member States must refrain from imposing export limitations for components where the recipient provides a declaration of use to the effect that the components are or will be integrated into its own products and cannot subsequently be transferred or exported except for maintenance or repair.[179] According to the GRIP Report, general licences may incorporate integration clauses or declarations, or statements certifying to this effect.[180] Certain Member States have used these sorts of statements as an alternative to the non-re-export clause discussed above,[181] probably because their industries only produce parts to be integrated into larger systems.

In addition to these conditions, general licences may incorporate technical clauses requiring either the supplier or the recipient to make specific alterations to the product before shipping it.[182] General licences may also incorporate specific conditions attached to each category of product under the licence in the form of the clauses discussed above.[183] It is submitted that in order for the functions and use of general licences to be optimised, such licences must be subject to the fewest specific terms and conditions possible. A revised ICT Directive could contain a provision which provides an illustrative list of the types of permissible terms and conditions. A Recital could indicate the types of terms and conditions which are to be generally discouraged or which have been used only by a limited number of Member States such as technical clauses, for example.

Finally, general licences may include a host of other obligations. For example, even before granting a general licence, art.5(4) provides that a Member State is permitted to lay down the conditions for registration prior to first use.[184] Therefore, Member States retain considerable discretion to define procedures for registration and de-registration, the latter of which is not mentioned at all in the ICT Directive. Further, art. 8(2) also provides that Member States may determine additional information that may be required regarding products transferred under a general transfer licence prior to first use. Certain Member States may therefore require more detailed information than others. Other requirements include: informing certified recipients about the existence of specific restrictions and conditions;[185] notification to the national authority prior to first use of the licence,[186] to keep records of each transfer under the licence[187] including reporting requirements to be determined by Member States.[188] It is submitted that most, if not all, of these conditions appear excessive and are susceptible to variable national applications. However, the lack of harmonisation of these requirements in a first iteration of ICT Directive could be considered sensible in respecting differences in administrative practice and other priorities between the Member States at this transitional stage. A shift from individual transfer licences to general licences in practice is an ambitious objective, would constitute a major success, and needs time. However, the data provided by *GRIP* indicates that national differences in the use of variable conditions has

[179] See also Recital 19
[180] *GRIP*, *supra* note 19, at 36.
[181] ibid Walloon Region, Flemish Region and Luxembourg.
[182] Ibid., at 36, although the GRIP Report only identifies the use of this clause in France.
[183] *GRIP*, *supra* note 19, at 37, although, again the GRIP Report only identifies the use of this practice in France.
[184] In the UK, for example, most Open General Export Licences ("OGEL's") require the exporter or trader to register with the Export Control Organization ("ECO") before they make use of them and registered companies are subject to compliance visits from the ECO to ensure that all the conditions are being met. See Lundmark report, *supra* note 9, at16.
[185] Recital 31 and art.8(1) ICT Directive. Ibid. 37-38.
[186] Article 8(2) ICT Directive. According to the GRIP Report, this is often accompanied by an obligation to prove that the user of the general licence is authorised to manufacture and trade in equipment which, the GRIP Report identifies as seeming to be automatically introduced in the general licence (with France reserving the right to call potential suppliers for a preliminary interview). In most cases, notification means registering with the national authorities to await confirmation of notification prior to shipping the product.
[187] Article 8(3) and (4) ICT Directive.
[188] Article 8(3) ICT Directive. *GRIP*, *supra* note 19, at 37. According to the Report, these reporting requirements can be seen as creating a new "administrative burden" on the user of the general licence which could contribute to the current limited use of the general licences. The Report indicates that Germany is the only Member State requiring an electronic 'zero-report' when there were no transfers under the general transfer licence during the reporting period.

impacted on the regime and which may require more detailed harmonization through a revised ICT Directive.

In addition to the specific issues discussed above, *GRIP* made a number of general observations regarding the implementation of the general transfer licence regime in practice. First, general licences are often difficult to access or not available through the official websites of the relevant national authorities and are regularly only published in the respective national language.[189] Second, the number of general transfer licences in the Member States varies, while some have published one or several of the mandatory circumstances, not all Member State use them for all four circumstances; some Member States are still in the process of preparing their first such licences, and others have not published any.[190] Third, there appears to be no specific documentary format. For example, some general licences comprise only one page while others comprise a complex series of documents.[191] A revised ICT Directive can address issues such as the publication of general transfer licences in English[192] and possibly a common format or template for licences in the form of a "European General Licence Document". User-friendly websites can be established by softer means, such as seminars, guidance notes or information exchange. As discussed in Sections 4.4 and 5.1 above, the circumstances mandating and permitting use of general licences is a more complex issue that would require more extensive consultation informed by observation in practice.

5.3. Global transfer licence

According to art.6(1) a global transfer licence is a specific authorisation granted in response to an individual request to transfer products to authorised recipients in one or more other Member States. Again, Member States must determine the products or categories of products covered and the authorised recipients.[193] The Commission opted against a 'global licences only' scenario on the basis that a combination of general and global licences would enable use of general licences for routine non-sensitive transfers while at the same time accommodating the necessary flexibility for more sensitive transfers through global licences.[194]

According to the Commission, the main simplification potential of the global licence is that it is not specific to a precise shipment and, thus, can be used several times to cover similar transfers. Further, global transfer licences are typically not subject to quantitative limits and are valid over a long period.[195] Global transfer licences are said to be particularly helpful in cases of routine shipments to habitual customers or for SMEs with a limited catalogue.[196] Their potential has already been realised in certain Member States.[197] In 2002, France introduced global licences based on a catalogue of participating companies, specifically targeting SMEs.[198] The first 35 licences replaced 1,250 individual licences, a reduction in administrative bureaucracy by a ratio of 36.[199] Similarly, during the ICT Directive's preparatory phase, Romania indicated that it had replaced 700 individual licences with 7 global licences.[200]

Whilst the Commission has emphasised the simplification potential of global licences, it is submitted that the ICT Directive expresses ambivalence as to the intended role of global licences under this regime and which may reflect the view that global licences are intended merely as a

[189] *GRIP*, *supra* note 19, at 19.
[190] Ibid., at 19-20.
[191] *GRIP*, *supra* note 19, at 20.
[192] At 63, GRIP recommends that general licences should be published and accessible in a common language such as English which could ease the decision-making process to become certified.
[193] art. 6(2) ICT Directive.
[194] *Impact Assessment*, *supra* note 12, at 36
[195] *Impact Assessment*, ibid., at 35.
[196] Ibid. See also *GRIP*, *supra* note 19, at 39.
[197] *GRIP*, ibid.
[198] *Impact Assessment*, *supra* note 12, at 36.
[199] Ibid.
[200] Ibid.

transitional measure until general licences are fully operational.[201] Notwithstanding, this does generate uncertainty in the short-medium term, assuming that global licences are also likely to continue to feature in a revised ICT Directive. For instance, whilst the ICT Directive does not adopt a formal prioritisation of licenses by reference to any defined criteria, the ICT Directive at the very least prescribes circumstances in which general licences and individual licences are required or permitted. By contrast, whilst it is clear that the ICT Directive generally views global licences as a 'second best' option, the ICT Directive does not prescribe any circumstances in which a global licence could be used. Rather, a Recital simply states that "[w]here a general transfer licence cannot be published, Member States *should*, upon request, grant a global transfer licence […] except in the case set out in this Directive […]" Further, according to the ICT Directive a global licence must be granted for a period of three years but may be renewed.[202] It is open to debate whether or not the global licence period should be set higher or lower than 3 years. However, arguably more significant is the fact that the ICT Directive does not prescribe a minimum or maximum period of renewal, an issue which, it is recalled from the Unisys Study discussed in Section **X**, has proven to result in variable national practices. A revised ICT Directive could, at the very least, provide an illustrative list of circumstances in which a global licence must or could be used. This would bring the global licence provision into closer conformity with the general format of the general licence and individual licence provisions. Further, a revised ICT Directive could determine a minimum and/or maximum period of renewal. The Commission could also issue additional guidance on these matters.

While the introduction of the global transfer licence through the ICT Directive is likely to have more limited impact on Member States already using general licences, it is estimated that the regime would reduce red tape by a factor of 10 where newly introduced and by 50 per cent overall within the EU.[203] The Commission has acknowledged a small risk that Member States may define global licences in such restrictive terms as to be equivalent to individual licences, but states that there is little reason to fear such abuses as a Member State would compromise the competitive position of its industries for no reason.[204] However, this does presuppose that competition will be a primary determinant when making licensing decisions. The Commission also suggested a risk that Member States already using general transfer licences of backtracking.[205] However, on the Commission's own logic, this could also compromise a Member State's competitive position. Further, there is no indication in countries such as the UK where general licensing is most well established that global licensing has significantly increased.

GRIP reports that according to several stakeholders, global licences could be a useful transition tool until the general licence regime is fully operational.[206] However, extensive use of global licences could also compromise the general licence regime when the former are used in cases more suited to the latter. For example, it appears that recipients favour this type of licence to avoid the perceived burdens of certification.[207] Again, this reinforces the need for a clearer delimitation of the circumstances in which global licences are generally permitted where general licences cannot be used.

5.4. Individual transfer licence

As indicated in Section **X**, prior to the ICT Directive, individual transfer licences were the most commonly used type of licence.[208] In contrast to general and global licences, an individual transfer

---

201 *GRIP*, *supra* note 19, at 39.
202 Ibid.
203 *Impact Assessment*, *supra* note 12, at 36.
204 ibid.
205 *Impact Assessment*, *supra* note 12, at 36.
206 *GRIP*, *supra* note 19, at 39.
207 Ibid.
208 *Impact Assessment*, *supra* note 12, at 36.

licence provides a limited authorisation to transfer qualified by quantity of products and the number of authorised recipients. An individual licence concerns only one specific authorisation granted to a supplier at its request, permitting only one transfer of a specified quantity of specified products to be transmitted in one or several shipments to only one recipient.[209] Prior to the ICT Directive, individual licences were typically subject to limited duration, for example, expiring after 12 months or on fulfilment of a specified quantity.[210]

While individual transfer licences are still possible, art.7 ICT Directive confines their use to four exhaustively defined circumstances: (1) where the request is limited to one transfer, (2) where it is necessary for compliance with international obligations and commitments, (3) where it is necessary for the protection of essential security interests or on grounds of public policy, and (4) where a Member State has "serious reason" to believe that the supplier will not be able to comply with all the terms and conditions necessary to grant it a global transfer licence. The first circumstance is unlikely to be particularly problematic given that the limitation is at the request of the licence user as opposed to being imposed by the Member State. It also appears to be superfluous given that the definition of individual transfer licence expressly states that it only concerns a single transfer. A revised ICT Directive should delete this circumstance. The second circumstance reflects the ICT Directive's general approach to ensuring Member State compliance with other international obligations and commitments.[211] However, invocation of this circumstance is likely to be subject to certain implied limitations such as the need for international obligations to exist at the time of transfer and use of an individual licence must be necessary.

The third circumstance aims to address national security interests inside the ICT Directive thereby limiting the need to invoke arts.36, 52 and 346 TFEU.[212] This is comparable to many of the security based adaptations in the Defence and Security Procurement Directive.[213] However, the reference to public policy is not defined. Recital 14 refers to safety of transport, safety of storage, the risk of diversion and the prevention of crime as public policy grounds. As indicated in Section **X**, the breadth of these grounds is likely to require careful judicial scrutiny of the necessity of the decision to use an individual licence.

The final circumstance further reinforces an attempt by the ICT to institute a hierarchy of licences but, again, without providing a clear basis on which to guide national authorities in differentiating between use of a global licence and an individual licence. For instance, it is not clear what "serious reasons" may justify use of an individual transfer licence. As essential national security concerns are already accommodated in one of the other circumstances discussed above, a question arises as to what serious reasons other than those related to national security could exist in an armaments transfer context. It appears that such reasons are likely to concern lesser security reasons than "essential" security or serious non-security reasons or combination thereof. An inability to comply with export limitations is likely to be capable of constituting a sufficiently "serious reason". Further, whilst a "serious reason" appears to require a substantial justification, this may be weakened by the fact that the authority only has to "believe" that the supplier will not be able to comply. There is also a difficulty in verifying or evidentially substantiating any reason given. In addition, there is no provision enabling authorities to determine whether the imposition of alternative terms or conditions could allow for the use of a global transfer licence. Therefore, it is submitted that this circumstance could be susceptible to abuse undermining the effectiveness of the ICT Directive as a whole. It is therefore suggested that a revised ICT Directive should delete this circumstance or, at least, clarify its definition with additional safeguards. In any event, based on an analogous interpretation of the existing ECJ jurisprudence on exceptions under the TFEU, it is

[209] Article 7 ICT Directive.
[210] *UNISYS*, supra note 17, at 14.
[211] Recital 7 ICT Directive.
[212] See also Recital 14 ICT Directive.
[213] Trybus, "The tailor-made EU Defence and Security Procurement Directive: limitation, flexibility, description, and substitution", *supra* note 8 and, more extensively, in *Buying Defence and Security in Europe*, *supra* note 8, chapters 6-10.

argued that these circumstances have to be interpreted narrowly.[214]

Whilst the continued availability of individual licences poses a risk to the successful transition to general licences, the decision to retain individual licences must be put into perspective. Firstly, an ICT Directive would have been unlikely to have garnered sufficient support for its passing had it not permitted at least the possibility of the exceptional use of individual licences.[215] Secondly, individual licences are only allowed in four exhaustively defined circumstances and which could be further reduced through appropriate deletion and revision of at least one circumstance. Thirdly, the inability to grant an individual licence under the ICT Directive might have lead Member States to grant the same outside the ICT Directive by invoking art.346 TFEU.[216] Finally, retention of the use of individual licences may offer an opportunity to study their effects in more detail. In principle, there can be no objection to individual licences if they serve a legitimate function in practice.

It should be observed that the *GRIP* Report did not focus extensively on individual licences but reported continuing use and validity of existing individual licences.[217]

6. Certification

The second major innovation of the ICT Directive is the introduction of a certification regime. A particular concern is the reliability of recipient companies of intra-Community transfers of armaments in, particular, in respecting limitations on re-exports outside the EU.[218] To the extent that reliability can ever be formally demonstrated or guaranteed, certification can contribute to addressing these concerns. Certification involves the formal assessment of the reliability of a company receiving products by the Member State in which it is registered before any transfer to that recipient company takes place. This is designed to facilitate the building of mutual trust between Member States as it is said to reduce the risk of illicit transfers and enhance the traceability of products transferred under general transfer licences and thus incentivise their use. A key component of mutual trust is mutual recognition. Consequently, art.9(6) ICT Directive provides that Member States must recognise any certificates issued in another Member State. It should be observed that certain Member States had already operated their own national certification or equivalent systems.[219] However, an EU-wide certification regime based on common principles and mutual recognition requires a fundamental overhaul of existing national processes.

Having considered two other options, the legislator decided to establish a regime based on optional rather than mandatory certification.[220] A significant argument against mandatory certification concerned the diversity of national defence industries. The manageable but still considerable costs of certification make the economic trade-offs decisive.[221] A large system integrator situated in one of the Big Six defence producing Member States is likely to benefit from certification on a cost-benefit analysis. For instance, a Recital to the ICT Directive has indicated that transfers within a group of undertakings should benefit from a general transfer licence in cases where the members of the group are certified in their respective Member States of establishment.[222] By contrast, for an SME with only limited activities in the military market, certification is likely to

[214] See the case law in *supra* notes 31, 32 and 34.
[215] *Impact Assessment*, *supr*a note 12, at 36.
[216] *Ibid*.
[217] *GRIP*, *supra* note 19, 20.
[218] Recitals 33 and 34 ICT Directive.
[219] For example, French companies must obtain a "licence for manufacturing and trading – autorisation de fabrication et de commerce" whilst United Kingdom companies are invited to implement a "compliance programme for exporters". See *Impact Assessment*, *supra* note 12, 37.
[220] *Impact Assessment*, ibid., at 26-27 and 37-40.
[221] Data collected during the consultation phase also from stakeholders suggests that there would be annual costs of about €10,000.00 per company if that company is already certified under ISO9001: *Impact Assessment, supra* note 12, at 38-40.
[222] Recital 32 ICT Directive.

incur disproportionate costs, in particular, given fewer transfers. Optional certification provides an incentive to grant the "least burdensome" licence to companies of now certified reliability, through the "additional guarantees pertaining to certification" which result from general licences.[223] The ICT Directive also recognises that, ultimately, it should be for undertakings to decide whether the benefits of general licences and certification justify the effort.[224] As will be discussed below, concerns continue to be prevalent amongst SMEs as to the perceived risks in relation to certification, although concerns are not exclusively confined to SMEs, suggesting that as yet untested risks continue to create a sense of inertia as to whether the uptake of licensing and certification will yield benefits that outweigh the costs.

According to art.9(1) ICT Directive, Member States must designate competent authorities to certify recipients of defence-related products on their territory under general transfer licences published by other Member States. This requirement corresponds to one of the mandatory circumstances in which a general transfer licence must be issued and which was discussed in Section **X** above.[225] The 20 Member States who had implemented the ICT Directive in 2012 had attributed the role of certification authority to different institutions ranging from the ministry of defence to ministries of industry or the economy.[226] The fact that in several Member States it is not the ministries of defence in charge of these acts was also an argument against the adoption of a transfer regime under the auspices of the European Defence Agency ("EDA") which is seen as an agency of Member States' ministries of defence.[227]

Article 9(2)(a)-(f) ICT Directive provides that certification must establish the recipient's reliability on the basis of prescribed criteria which appear to be exhaustive, any addition to which could potentially compromise the objective of harmonising certification based on common criteria. These criteria are: (1) proven experience, taking into account, in particular, the undertaking's record of compliance with export restrictions; (2) relevant defence industrial activity, in particular capacity for (sub)system integration; (3) the appointment of a senior executive personally responsible for transfers and exports; (4) a written commitment of the recipient that it will take all necessary steps to observe and enforce conditions relating to the end-use and export of any specific component or product received; (5) a written commitment that it will provide detailed information in response to requests and inquiries concerning the end-use(rs) of all products exported, transferred or received; and (6) a description of the recipient's internal compliance programme or transfer and export management system. Whilst none of the above criteria appear to be disproportionate to their objective, it is difficult to discern to what extent such criteria are any lighter in their touch than reliability assessments concerning exports.

In order to ensure a further degree of convergence in the ICT Directive's application, the Commission issued Recommendation 2011/24 which sets out further common certification guidelines.[228] It is suggested that the absence of comparable licensing guidance could be indicative of the priority accorded to certification as the primary control mechanism. However, it is open to question whether the ICT Directive should have included more detailed certification provisions within the text of the Directive to reflect this status. The Commission probably became aware of the need for more detailed interpretation during the transposition period to which a non-legally binding instrument is a practical response in the interim before the ICT Directive is reassessed in 2016.

[223] *Impact Assessment*, *supra* note 12, at 40.
[224] Recital 32 ICT Directive.
[225] Article 5(2)(b) ICT Directive.
[226] *Transposition Report*, *supra* note 18 at 10. In Germany this is the responsibility of the Federal Office for Economy and Export Control (*Bundesamt für Wirtschaft und Ausfuhrkontrolle BAFA*) which is operating under the supervision of the Federal Ministry for Economy and in the United Kingdom the Exports Control Organisation under the Department for Business, Innovation and Skills.
[227] *Impact Assessment*, *supra* note 12, at 18.
[228] See Commission Recommendation of 11 January 2011 on the certification of defence undertakings under Article 9 of Directive 2009/43/EC of the European Parliament and of the Council simplifying terms and conditions of transfers of defence-related products within the Community [2011] O.J. L11/62. The Recommendation was developed by the working group established under the Committee procedure in art.14 ICT Directive.

However, it will need to be considered whether a revised ICT Directive should delete the Recommendation and incorporate more detailed substantive provisions drawing on the Recommendation to the extent necessary. Otherwise, co-existence of a legally binding and non-legally binding instrument may further compromise the harmonisation and simplification objectives.

Article 9(3)(a)-(d) ICT Directive prescribes the minimum mandatory information to be contained in certificates. Recommendation 2011/24 provides a standard certificate template specifying the contents of the certificate in accordance with art.9(3) ICT Directive. However, it should also be observed that certificates may also contain further conditions relating to the provision of information required to verify compliance with the reliability criteria and concerning suspension or revocation of the certificate.[229] Further, the validity of a certification must not exceed five years.[230] In addition, authorities must monitor the recipient's compliance at least every three years. [231] It appears, therefore, that there is a risk that Member States may vary in terms of additional conditions imposed as well as issuing certificates for less than five years and exceeding the minimum three year compliance monitoring requirement.

If a competent authority determines that a certified recipient on its territory is no longer compliant, it must take "appropriate measures", which may include revoking the certificate.[232.] It follows that measures other than revocation may be used. Whilst the ICT Directive contains limited references to the possibility of suspension, it does not specify any other appropriate measures. Recommendation 2011/24 is slightly more specific, although does not specify which kinds of measures may be more or less appropriate in relation to certain instances of non-compliance. For instance, Recommendation 2011/14 states that when non-compliance is of "minor importance", the authority should require the recipient to take "corrective action" within a specified period.[233] Uncertainty in determining what might constitute an instance of non-compliance and appropriate action may also have the consequence that authorities simply opt for automatic revocation or suspension, irrespective of the gravity of the violation and the possibility of less severe corrective action. There is no mechanism in the ICT Directive for Member States to achieve a relative degree of uniformity in approach, other than an obligation to inform the Commission and other Member States of the decision taken.[234] When deciding whether to lift a suspension, Recommendation 2011/24 specifies use of the same measures identified for verifying implementation of corrective measures, namely site visits, meetings with senior officers or inspection of written documentation.[235] Within one month of its verification, the authority must issue a new decision confirming that the suspension will be lifted, maintained pending further verification, or that the certificate is revoked. Again, this could potentially result in variable national treatment and enforcement.

According to art.9(8), Member States must publish and regularly update a list of certified recipients and inform the Commission, the European Parliament and the other Member States. Further, the Commission must make publicly available on its website a central register of recipients certified by Member States.[236] The Commission's Register of Certified Defence-related Enterprises (CERTIDER) [237] provides information about enterprises certified under the ICT Directive. CERTIDER contains a list of the competent national authorities designated to deal with certification, the list of certified enterprises, details about the certificates and links to relevant national legislation. According to the *GRIP Report*, most but not all Member States refer to the

[229] Article 9(4)(a) ICT Directive.
[230] Article 9(3) paragraph 2 ICT Directive.
[231] Article 9(5) ICT Directive. This provides an additional safeguard to that provided in art.8(3) ICT Directive which requires Member States to regularly check that suppliers keep detailed and complete records of their transfers.
[232] Article 9(7) ICT Directive
[233] Section 4(4.1) Recommendation 2011/24.
[234] Article 9(7) ICT Directive.
[235] Section 4(4.3.) Recommendation 2011/24.
[236] Ibid.
[237] http://ec.europa.eu/enterprise/sectors/defence/certider/ [accessed 16 March 2015].

EU's list of certified recipients and several Member States specifically require the supplier to verify, on the EU website, whether the beneficiary holds a valid certificate.[238] It is submitted that either a guidance note or a revised ICT Directive could specify that all references should refer to the EU list of certified recipients. Modifications to the overall design and update of CERTIDER would also be a necessary addition to improve information content.[239]

According to the *Transposition Report*, the 20 Member States that had fully transposed in 2012 have put in place the framework to certify recipients as well as appointed competent authorities, established reliability criteria, "in general" foresee mutual recognition of certificates in their national legislation, and instituted the mechanisms to monitor compliance with the certification criteria and apply the necessary corrective measures.[240] Beyond formal transposition of certification regime however, *GRIP* reports a limited impact on certification *practice* in the Member States.[241] Only a small number of companies were certified in 2014 and the generally slow pace of the publication of general licences suggests that the certification regime lacks visibility.[242] Stakeholders from the Member State governments and from both certified and non-certified companies interviewed by the GRIP study team or responding to its questionnaire saw the certification regime as a step in the right direction but expressed "serious doubts" about the practical benefits of certification, in particular given the time, risks in terms of intellectual property, security breaches and negative findings, and organisational and financial requirements necessary to prepare procedures, controls and audits for compliance, especially for SMEs.[243] This includes the risks of assigning personal responsibility to any one individual in the form of a senior executive.[244] Further, the consequences (in particular legal) for a company of not being certified were considered unclear.[245] In addition, the lack of visibility and availability (in English) of general transfer licences in all Member States had a negative impact on the certification process, in particular, in light of the general complexity of general licences, their scope of application and requirements for certification which do not appear to be harmonised notwithstanding Commission Recommendation 2014/24/EU and which require additional criteria, different lists and processes.[246]

It appears therefore that four main and interrelated factors have limited the use of the certification regime and, therefore, its impact in practice. Firstly, the certification process is perceived to create cost and risk, especially where the recipient is an SME.[247] Secondly, even if it is possible to estimate the known costs and risks, there are potentially unknown costs and risks, for example, the legal consequences of certification or non-certification and any exposure to liability, for example, within the organisational structure of a recipient company. Thirdly, the relative lack of harmonisation and potential for variability in national practices concerning the scope of general licences and the certification criteria create uncertainty.[248]

---

[238] *GRIP*, *supra* note 19, 33 indicating, however, that the British authorities refer to a list of certified companies available on a UK website.
[239] *GRIP*, ibid, 63.
[240] *Transposition Report*, *supra* note 18, at 11. Ten Member States incorporated the provisions to provisionally suspend a general licence with regard to a certified recipient in another Member State in certain specific cases and under certain conditions in their national legislation.
[241] *GRIP*, *supra* note 19, at 43.
[242] *GRIP*, *supra* note 19, at 43.
[243] Ibid., at 40 and 44.
[244] This had been identified as an increasing issue within the export community as compliance programmes become increasingly mandatory and sophisticated. Thanks to Mr. Ian Bendelow for discussions on this point, although this was not expressed as a UK specific concern. This is also reiterated in the *GRIP* Report, *supra* note 19, at 44.
[245] Ibid., at 44.
[246] *GRIP*, *supra* note 19, at 45. It has been suggested that the language issues have been a predominant factor. Thanks to Mr. Ian Bendelow for discussions on this point.
[247] Ibid., at 44. According to the GRIP Report at 46, the administrative burdens and lack of information on general licences lead some SMEs to use individual and global licences in the alternative.
[248] Ibid., at 45. This criticism is expressed by the defence companies who participated in the study. The Member States were more cautious due to concerns about the effect of further harmonisation on their national policies on defence transfers.

Recognising the inherent reluctance of stakeholders to trial licensing and certification beyond a preliminary cost/benefit risk assessment, there are various ways in which this situation could be addressed. Firstly, a principal motivation for this article has concerned the relative absence of information and communication on the ICT regime which could be improved, at the Member State and Commission levels.[249] Within the regime itself, greater uniformity of understanding of how the regime functions in practice could be enhanced via publication of general transfers licences in English. Secondly, Member States and prime contractors can use their stronger position as customers of the defence industries to drive more extensive certification down the supply chain.[250] Thirdly, certain changes and adjustments to the regime including Recommendation 2011/24 could be considered as discussed above.

Ultimately, however, it is suggested that certain realities must be accepted which further changes or adjustments to the ICT regime are unable to mitigate. For instance, it is inevitable that certification will introduce a new administrative burden for its users. Further, aside from further standardisation of the permissible scope, terms and conditions of general transfer licences, by nature, licensing is a complex process reliant on the exercise of sound decision-making by users. In addition, Member States with small defence industrial bases cannot expect to derive the same benefits from general licences and certification and cannot, therefore, be expected to use the regime to the same extent.[251] Similarly, certain problems facing SMEs are not specific to licensing but are symptomatic of problems experienced by SMEs in the defence sector generally.[252] It is therefore submitted that even with improved communication, pressure and legislative adjustments, certification and general transfer licences will be used by those companies who can most benefit from them: primes rather than subcontractors, large companies rather than SMEs, and companies from the 'Big Six' rather than those from the other Member States. Within these limits, and with further observation, institutional adaptation and application in practice, it can be assumed that the certification regime will eventually progress towards its objectives with a corresponding impact on the uptake of general licences. Each aspect of the equation inevitably affects the other.

7. End-use controls: compensatory control of third country exportation risks

As the ICT Directive indicates, and as discussed above, even though Member States cooperate within the framework of Council Common Position 2008/944/CFSP defining common rules governing the control of military exports, the ICT Directive does not prevent Member States from determining all the terms and conditions of transfer licences, including limitations on export.[253] This reflects the fact that Member States have always expressed concern regarding a risk of "re-export" of goods into 'rogue hands', reinforced through existing export control commitments undertaken through international control regimes.

Concerning limitations imposed in licences prior to transfer, according to the *GRIP* Report, as a result of different regulatory procedures applied to the issue of end-use(r) on a case-by-case basis at the time of authorisation, end-use obligations and the type/format of documentation vary greatly.[254] Most Member States require so called end-use certificates ("EUC") in the context of individual and global licences, although these can have different names and forms.[255] In their EUCs, most Member States refer to the minimum mandatory provisions of the *User Guide* to Council Common Position 2008/944/CFSP, although there are variations in the formulation of these provisions, in the details of minimum elements required and in the optional elements recommended

[249] *GRIP*, *supra* note 19, at 46-47.
[250] Ibid., at 46.
[251] See *GRIP*, *supra* note 19, at 47.
[252] Ibid.
[253] Article 4(6) and Recital 30.
[254] *GRIP*, *supra* note 19, at 54-55.
[255] *GRIP*, *supra* note 19, at 55 and 60.

by the *User Guide*.[256] It is submitted that there is scope for harmonisation on this issue by means of a common EUC comprising one standard form referring to end-use and based on the *User Guide*.[257]

Further, most Member States include a non-re-export clause.[258] However, the formulations vary between clauses prohibiting re-export with or without the prior written consent of the Member State of origin, with varying lists of 'friendly' countries where written consent for re-export is not required on the one hand and outright prohibitions especially for nuclear, biological and chemical weapons on the other.[259] In case of re-exports to 'friendly' countries the EUC was often replaced by an International Import Certificate ("IIC") certified by the importing country (as opposed to end-user) as proof that the authorities are aware of the future re-export and agree to it.[260] Again, there may be scope for harmonisation by means of a common prior consent to export clause and common lists of 'friendly countries' and 'prohibited weapons'. According to the *GRIP* Report, a majority of Member States would like to harmonise EUCs but do not share a common vision on how to approach the issue.[261] Ideas suggested by Member States include: a common model format of EUC annexed to the ICT Directive; a list of minimum essential elements to be included in an EUC on the basis of the guidelines of the User's Guide for example; or common rules on the use of EUCs, for example, when an EUC should be required and for which type of intra-Community transfers under general, global and individual licences.[262] Harmonisation does appear conceivable in light of relative agreement already achieved most notably in the *User Guide.*

In addition, the *GRIP* Report identifies that practices on *ex-post* controls vary between Member States, with a majority requiring a delivery verification certificate ("DVC") from the end-user as proof that the military items have successfully been imported, although, a DVC is often optional.[263] Further, several Member States do not require DVCs for transfers within the EU and, where required, these are only used under individual licences.[264] A minority of Member States have procedures for post-shipment end-use monitoring, often allowing the Member State of origin on-site inspections, although clauses to this effect are not included systematically and are quite rare in practice.[265] A crucial issue leading to many of these differences in law and practice is the lack of a common definition of what constitutes a 'sensitive product', since for these items the controls tend to be tighter and more diverse.[266] As indicated in Section **4** above, initiatives towards a common list of sensitive products or at the least clearer definition of a product's sensitivity could lead to greater harmonisation.

In addition, according to the *GRIP* Report, Member States do not seem to require an EUC for transfers under a general licence.[267] However, general licences are frequently subject to end-use limitations under art.10 ICT Directive. Article 10 provides that when a recipient of transferred defence-related products under licence applies for an export licence to export those transferred goods outside the EU, the exporting Member State must ensure that the recipient declares that it has complied with export limitations attached to the licence[268] to the extent that any export limitations

[256] Ibid., at 55-56.
[257] According to the *GRIP* Report , *supra* note 19, at 55, at least two countries (the Walloon Region and Austria) out of 19 Member States have designed a specific EUC for intra-Community transfers in which an authentication of the foreign end-user is included. According to this form, the end-user certifies that as end-user it will not transmit or export the goods without prior written approval of the originating EU government and that the goods are destined to be integrated into its own manufactured products.
[258] *GRIP*, *supra* note 019, at 57.
[259] Ibid.
[260] Ibid., at 57-8.
[261] Ibid, at 60 referring to 14 Member States out of 21.
[262] Ibid., at 61.
[263] *GRIP*, *supra* note 019, at 58.
[264] Ibid.
[265] Ibid., at 58-59.
[266] *GRIP*, *supra* note 19, at 59.
[267] Ibid., at 55.
[268] Recitals 34, 35, 36 and art.10 ICT Directive. This obligation corresponds with a prior obligation to ensure that suppliers inform recipients of limitations relating to end-use or export. See Recital 31 and Article 8(1).

are included.[269] More specifically, the recipient may be required by the originating Member State to obtain prior consent for export.[270] Thus, any export restriction on the defence good issued by the Member State of origin "follows the transferred good",[271] so that at the point of export at the common external frontier of the Community, the Member State in question knows and enforces the original export restriction. These export limitations include non-re-export clauses or notification clauses, "in order to maintain the coherence of their arms export policy".[272] Article 10 ICT Directive, and not surprisingly the implementing laws and practices of the Member States, do not appear to differentiate between the different situations in which general licences are to be used. Most importantly, in cases in which the end-user is a certified company without prospect of export, an end-use guarantee should not be needed.[273] Any such requirement is arguably disproportionate. It is submitted that art.10 ICT Directive should differentiate between the general licence situations on the basis of the understanding of certification as an alternative to end-use controls and be revised accordingly, for example, by adding the following sentence: "[n]o export limitations of any kind shall be attached to general licences in which the end-user is a certified undertaking."[274] Apart from facilitating administrative procedure and reducing delays, this would also strengthen the under-used certification regime of the ICT Directive discussed above by providing an additional incentive to get certified.

More generally, it has been argued that the ICT Directive lacks any systematic means by which receiving Member States are routinely informed about relevant re-export conditions.[275] Whilst it is the Member State's obligation to implement the provision, the recipient must ensure compliance and inform the authority of any export limitations. Consequently, the ICT Directive fails to safeguard against the risk of unauthorised export in cases where recipients intentionally or inadvertently neglect to inform their authorities.[276] Further, previous versions of the ICT Directive proposal had proposed consultation between Member States in the event that consent to re-export was required by the originating Member State but not obtained. However, the inclusion of a consultation obligation recognises the possibility for the re-exporting Member State to overrule an export limitation. The absence of a consultation requirement suggests that a re-exporting Member State cannot override export limitations.[277] However, it has been advised that in order to completely safeguard against the risk of re-exportation, the originating Member State should specify a consultation requirement in the case of sensitive transfers in order to avoid the possibility of an export limitation being overridden.[278] It has been suggested that such a requirement is necessary to prevent export decisions being focused in Member States that host companies working on system assembly.[279] It should be observed that the Commission also originally considered an I.T.

[269] According to art.4(8) ICT Directive, Member States must not impose any export limitations for components where a declaration of use confirming component integration is provided, except where Member States consider that the transfer of components is sensitive. To this extent, generally, transfer licences for components should not include exportlimitations. For a discussion in this regard, see above.
[270] Ibid.
[271] *Impact Assessment*, *supra* note 12, at 41.
[272] *GRIP*, *supra* note 19, at 55 and 60.
[273] According GRIP, ibid., at 60, only one Member States expressed this opinion.
[274] According to GRIP, ibid., there is currently no consensus on treating certification as an alternative to end-sue controls but "this should be discussed".
[275] C. Taylor, EC Defence Equipment Directives, Standard Note SN/IA/4640 3 June 2011, House of Common Library, 20 citing at fn 49 Committee on Arms Export Controls, *Scrutiny of Arms Export Controls 2009,* HC 178, Session 2008-09.
[276] Ibid.
[277] S. Depauw, "Risks of the Ict-directive in terms of transparency and export control", in Alyson J. K. Bailes, Sara Depauw, and Tomas Baum (eds.), *The EU Defence Market: Balancing Effectiveness with Responsibility*, *supra* note 137, at 72.
[278] Ibid.
[279] Ibid. According to Depauw, at 72-3, such a position would, in turn create: "the spectre of less public and parliamentary control in the supplier nations and a greater influence for economic pressures, threatening to undermine a balanced assessment – taking full account of the criteria in the Common Position on arms exports - of export licence applications for the final product. Such a development may be attractive from an economic point of view, but also risks

traceability database that would track all licences and their eventual export restrictions. However, this option was considered to be less cost-efficient than the information requirements finally adopted.[280]

Whilst the current uncertainty of art. 10 ICT Directive may be criticised, this provision must not be seen in isolation as the only available safeguard. As indicated in Section 6 above, certification is one means of addressing export control concerns. In addition, the ICT Directive contains provisions on customs procedures to ensure a further final check on exports and their conformity with relevant administrative formalities before leaving the EU.[281] Article 16 ICT Directive also requires Member States to lay down penalties for infringements, in particular, in the event of false or incomplete information being provided as regards export limitations.[282] Concerning the latter, one criticism raised by *UNISYS* was that whilst the penalties prescribed by national legislation for export violations generally took the form of a fine or imprisonment (or both) in all Member States, the amount of the fines and duration of imprisonment differed considerably, as did their enforcement. Thus, characteristic of the absence of enforcement machinery in the ICT Directive, Member States continue to exercise considerable discretion on an important issue which continues to remain within the field of national procedural autonomy.

8. Safeguard measures: withdrawals, suspensions and limitations

The ICT Directive envisages the possibility for a Member State to enact suspensory measures in a number of scenarios. Firstly, as indicated in Section **6**, the Member State of a certified recipient may take corrective action which includes suspension of a certificate where an instance of non-compliance has been determined to affect its reliability.[283] Secondly, art.4(9) is a general provision applicable to all licences according to which Member States may withdraw, suspend or limit the use of transfer licences issued at any time on four grounds: protection of their essential security interests; public policy; public security; and non-compliance with licence terms and conditions. Thirdly, art.15 which is solely applicable to general licences provides for a "safeguard measure" in which suspension may be imposed but only after a prior verification of the situation. Specifically, a Member State must first "consider" that one of three circumstances exists. These circumstances are: where there is a "serious risk" that a certified recipient in another Member State will not comply with a condition attached to a general transfer licence; public policy could be affected; public security could be affected; or essential security interests could be affected. Where a Member State considers one (or presumably more) of the circumstances to exist, they must first inform the Member State of the recipient and request verification of the situation. Importantly, therefore, whilst art.4(9) appears to apply where one of the above circumstances *are* present, art.15(1) is pre-emptive, concerning circumstances where there is a risk or possibility of one of the circumstances eventuating. Where "doubts" (i.e. a "reasonable doubt"[284]) "persist" a Member State may then impose a provisional suspension. The suspending Member State must then inform the other Member States and the Commission of the reasons. The suspending Member State may also decide to lift the suspension where it considers that it is no longer justified. Again, similar to issues concerning measures to be applied to non-compliant certified recipients, variable national approaches may result to the determination of suspension. For instance, it is not clear what is meant by a "serious risk" and whether it must be possible or probable as well as what constitutes a "reasonable doubt" which "persists". Further, it is unclear to what extent verification will satisfy the licensing Member State especially if the recipient Member State has limited understanding of the

underplaying the security threats. We have not yet reached the stage where full confidence in the export control policy of all member states can be endorsed. A system of checks and balances for arms export controls - not only for denials, but also for approvals - is therefore to be welcomed."

[280] See CSWD, at 47.

[281] Article 11(1) ICT Directive.

[282] See also Recital 38 ICT Directive.

[283] As referenced in art.9(4)(b) ICT Directive.

[284] Recital 39 ICT Directive.

circumstances. There is also a risk that verification simply becomes a formality, suspension having already been determined on the basis of risk rather than evidence. In addition, the ICT Directive does not prescribe measures which may result after verification but which fall short of provisional suspension. Member States may also fundamentally differ as to when suspension, withdrawal or limitation of a licence is appropriate. Finally, art.15(2) authorises a Member to lift a suspension on a *general* licence where it considers that suspension is no longer justified. However, the ICT Directive contains no comparable provision with regard to the lifting of suspensions on global or individual licences. *GRIP* does not provide data on such measures but there is a risk of abuse which may be further exacerbated by the lack of a review system, to which this article now finally turns.

9. Review and remedies

National legal systems have traditionally provided a means to bring judicial review for the purposes of challenging export licensing decisions.[285] However, beyond existing provision under national law, the ICT Directive contains no specific provisions enabling, for example, a licensee to challenge decisions such as a Member States choice to only grant a particular type of licence, to refuse to grant a licence or the basis for suspending or revoking a licence or certificate. Rather, a Recital to the ICT Directive simply encourages the determination by Member States of effective and sufficient measures to ensure enforcement.[286] Whilst not entirely unequivocal, another Recital to the ICT Directive also indicates that Member States should determine the "recipients of transfer licences" in a non-discriminatory way unless necessary for the protection of their essential security interests.[287] To this extent, the ICT Directive appears to envisage the possibility to challenge a Member State's decision where a recipient has been chosen on grounds which are discriminatory.[288]

By contrast, the Defence and Security Procurement Directive, has its own review and remedies system to challenge procurement decisions.[289] However, the review and remedies systems of the procurement Directives are a rare deviation from the EU principle of national procedural autonomy and which was not, in fact, originally included in the initial proposal. The position is also not directly comparable given that the review and remedies system is not new but modelled on the pre-existing provisions under the Public Sector Procurement Remedies Directive 89/65/EEC. Therefore, the harmonisation of review and remedies provision under the ICT Directive would have been new and ambitious.

Notwithstanding, it is submitted that existing national judicial review proceedings indicate that a basis for challenge potentially exists. The Defence and Security Procurement Directive indicates the potential for harmonisation of review and remedies in the field of defence trade. The courts can accommodate the special national security context of these challenges, as the Court of Justice has shown in the case law discussed above.[290] Further, the ICT Directive expressly incorporates reference to the use of penalties for violations which presupposes a basis for challenging those penalties. It is therefore suggested that progress be undertaken towards assessing the feasibility of incorporating specific provisions on review and remedies in a revised or future ICT Directive in order to further the "progressive building of mutual trust and confidence".[291].

[285] Some Member States provide for challenges. In Germany, for example, the rejection of an application for a global transfer licence or its withdrawal would always take the form of an 'administrative act' (*Verwaltungsakt*) and could therefore be challenged in the administrative courts with the possible annulment of the administrative act by that court. Similarly, export licensing decisions in the UK can be challenged by way of traditional judicial review in public law.
[286] Recital 38 ICT Directive.
[287] Recital 20 ICT Directive.
[288] Recital 20 ICT Directive.
[289] See in detail: M. Trybus, "The hidden Remedies Directive: review and remedies under the EU Defence and Security Remedies Directive" (2013) 22 P.P.L. Rev. 135-155
[290] *Supra* notes 31, 32 and 34.
[291] Recital 38 ICT Directive.

10. Conclusions

Through the ICT Directive, the EU legislator has provided a series of options for both the national legislators of the Member States and their authorities in charge of armaments transfer licences. The latter are offered (1) a selection of general, global and individual licences, (2) certification, and (3) re-exportation controls. It is the introduction of global transfer licences and British-style general transfer licences which represent the main innovation of the instrument as they are likely to reduce costs and red tape and significantly improve security of supply. However, this paper has demonstrated that an export control mentality continues to permeate the very structure of the ICT Directive from limitations on mandatory exemptions from prior authorisation to export control limitations. Consequently, the ICT Directive is restrained in clearly defining the circumstances in which general, global and individual licences are required, permitted and prohibited, in turn creating a sense of ambivalence that is unlikely to instil confidence in its user communities. Beyond the legislative design, national practice post-transposition has raised or perhaps exposed for the first time a number of further divergences in national practice and which a revised ICT Directive should consider as institutional learning hones in on areas in need of greater harmonization through the Directive. These include: the scope of munitions lists, definitions of sensitive products under licence, the use of common licence conditions, common approaches to certification and remedial measures concerning suspension and revocation. Fundamentally, however, a key concern continues to be a sense of stalemate between Member States that are accustomed to their own licensing cultures and anxious to safeguard against re-exportation risks and the private sector cautious to calculate the costs, benefits and risks associated with a wholescale transition to general licences. Whilst changes to the legal framework cannot address these pressures, a bold approach towards harmonisation in a revised ICT Directive backed with institutional measures towards improved visibility and communication could at least go some way towards a more “licence friendly Europe.”