SIMO-PEKKA PARVIAINEN

CRYPTOGRAPHIC SOFTWARE EXPORT CONTROLS IN THE EU

UNIVERSITY OF HELSINKI
FACULTY OF LAW

URN:NBN:fi-fe20001230

HELSINGIN YLIOPISTO – HELSINGFORS UNIVERSITET – UNIVERSITY OF HELSINKI

Tiedekunta/Osasto – Fakultet/Sektion – Faculty/Section	Laitos – Institution – Department
Faculty of Law	Department of Public Law

Tekijä – Författare – Author

Parviainen, Simo-Pekka

Työn nimi – Arbetets titel – Title

Cryptographic Software Export Controls in the EU

Oppiaine – Läroämne – Subject

Administrative Law

Työn laji – Arbetets art – Level	Aika – Datum – Date	Sivumäärä – Sidoantal – Number of Pages
Pro-gradu thesis	1. 7.2000	89 pages

Tiivistelmä – Referat – Abstract

Certain software products employing digital techniques for encryption of data are subject to export controls in the EU Member States pursuant to Community law and relevant laws in the Member States. These controls are agreed globally in the framework of the so-called Wassenaar Arrangement. Wassenaar is an informal non-proliferation regime aimed at promoting international stability and responsibility in transfers of strategic (dual-use) products and technology. This thesis covers provisions of Wassenaar, Community export control laws and export control laws of Finland, Sweden, Germany, France and United Kingdom.

This thesis consists of five chapters. The first chapter discusses the *ratio* of export control laws and the impact they have on global trade. The *ratio* is originally defence-related – in general to prevent potential adversaries of participating States from having the same tools, and in particular in the case of cryptographic software to enable signals intelligence efforts. Increasingly as the use of cryptography in a civilian context has mushroomed, export restrictions can have negative effects on civilian trade. Information security solutions may also be took weak because of export restrictions on cryptography.

The second chapter covers the OECD's Cryptography Policy, which had a significant effect on its member nations' national cryptography policies and legislation. The OECD is a significant organization, because it acts as a meeting forum for most important industrialized nations.

The third chapter covers the Wassenaar Arrangement. The Arrangement is covered from the viewpoint of international law and politics. The Wassenaar control list provisions affecting cryptographic software transfers are also covered in detail. Control lists in the EU and in Member States are usually directly copied from Wassenaar control lists. Controls agreed in its framework set only a minimum level for participating States. However, Wassenaar countries can adopt stricter controls.

The fourth chapter covers Community export control law. Export controls are viewed in Community law as falling within the domain of Common Commercial Policy pursuant to Article 133 of the EC Treaty. Therefore the Community has exclusive competence in export matters, save where a national measure is authorized by the Community or falls under foreign or security policy derogations established in Community law. The Member States still have a considerable amount of power in the domain of Common Foreign and Security Policy. They are able to maintain national export controls because export control laws are not fully harmonized. This can also have possible detrimental effects on the functioning of internal market and common export policies. In 1995 the EU adopted Dual-Use Regulation 3381/94/EC, which sets common rules for exports in Member States. Provisions of this regulation receive detailed coverage in this chapter.

The fifth chapter covers national legislation and export authorization practices in five different Member States – in Finland, Sweden, Germany, France and in United Kingdom. Export control laws of those Member States are covered when the national laws differ from the uniform approach of the Community's *acquis communautaire*.

Avainsanat – Nyckelord – Keywords

export control, encryption, software, dual-use, license, foreign trade, e-commerce, Internet

Säilytyspaikka – Förvaringställe – Where deposited

Faculty of Law Library

Muita tietoja – Övriga information – Additional information

Also available online at: http://ethesis.helsinki.fi or http://personal.inet.fi/business/parviainen/thesis.html in .pdf format, for other formats and information email author at Simo-Pekka Parviainen <spp@iki.fi>.

PREFACE

> *"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files."*[1]

Encryption technology regulation may seem, at first glance, as quite a narrow topic in the family of jurisprudence.[2] It may still be so, but one thing is for certain - it is relatively unexplored among legal scholars. Needless to say, this makes the task of the humble law student quite challenging.

Since the triumphant rise of the Information Society, use and distribution of encryption software has been a hot topic in policy discussions. Still classified as a dual-use commodity, governments in major industrial nations want to limit its use, using their export control regimes as an enforcement tool. It seems that the only thing for certain in this field is change – export control regimes are in a state of flux.

Obviously one can see certain trends in the field concerned. One big trend in recent years has been liberalization. Especially in the United States and France governments have been cutting some slack in controls. On the other hand, in those nations especially the export controls have been quite strict in comparison to other industrialized nations. But one trend in the international policy arena has also been quite clear – national governments' willingness to maintain their regimes as intact as possible in spite of liberalization. One must also bear in mind that there are strongly legitimate grounds for maintaining export controls on dual-use goods especially in cases of non-proliferation and trade embargoes. Still one can argue that encryption is defensive in its true nature, used to protect the information from unauthorised access, and cannot be directly used for hostile purposes. Therefore it should not be deemed a dual-use product at all. The future will show us which trend will prevail.

However, the rapid development of technology may render the controls obsolete and the laws may suffer the faith of *desuetudo*. It may well be that controls on encryption products will be abolished in the near future. In my opinion, we can be relatively sure about one thing - governments and intergovernmental organizations are adapting their approach, as they face the new challenges provided by the new information technologies. In the field of export controls this

[1] *Bruce Schneier*; Applied Cryptography: Protocols, Algorithms, and Source Code in C.
[2] Words 'encryption' and 'cryptography' derive from Greek word *kryptikós* (hidden).

means that governments are moving from a gatekeeper model to a surveillance model, [3] because they are unable or unwilling to control certain dual-use exports.

Also it can be considered that when some product is classified as a dual-use product (a strategic product or technology - an item which can be used for both civil and military purposes), it can be used as a part of a weapon or in the manufacturing of weapons. Still almost any item can be used as a weapon if one has the intention, and therefore almost any item could also be classified as a dual-use item. Therefore the whole concept of dual-use products is somewhat problematic and should be used only for products which are mainly used in defence-related fields and only rarely in a civilian setting.

As a general academic remark I should also point out, that this is a legal study in a field filled with myriad technical details. The technical details, however, are beyond the scope of this study.

Finally I would like to thank Jari Puhakka, Päivi Hautamäki, Jari Holmborg and Mikko Maijala, all from the F-Secure Corporation, for giving me the opportunity to do research work for F-Secure Corp. Thank you very much for having confidence in me and my work. Also, I would like to thank Ms Jane Keates M.Sc. for giving me lifesaving guidance in English grammar.

Helsinki, Finland 1. 7.2000

Simo-Pekka Parviainen

[3] *Rotenberg, Marc*, Executive Director of the Electronic Privacy Information Center, interviewed in the New York Times, January 18, 2000.

CONTENTS

REFERENCES

LITERATURE

Baker, Stewart A. & Hurst, Paul R.; The Limits of Trust: Cryptography, Governments and Electronic Commerce, Kluwer Law International, The Hague, The Netherlands 1998.

Baker, Stewart A.; Decoding the OECD's Guidelines for Cryptography Policy, International Lawyer, 1997.

Berg, Jens Petter; Overvakning av kryptert datakommunikasjon på internettet, in publication: Elektronisk handel – rättsliga aspekter, Randi Punsvik (ed.), Nordisk årsbok i Rättsinformatik, Norsteds Juridik, 1997.

Controlling East-West Trade and Technology Transfer; Bertch (ed.), Article: "COCOM: An Appraisal of Objectives and Needed Reforms", 1988.

Cornish, Paul; Joint Action, 'The Economic Aspects of Security' and the Regulation of Conventional Arms and Technology Exports from the EU; in publication: Common Foreign and Security Policy, The Record and Reforms, Holland, Martin (ed.), Pinter, London 1997.

Cryptography and Liberty 1999; An International Survey of Encryption Policy, Electronic Privacy Information Center, Washington D.C., United States of America [http://www.epic.org/ 4. 4.2000].

Cryptography's Role in Securing the Information Society; The Report of the US National Research Council Committee to Study National Cryptography Policy; Dam, Kenneth W. & Lin, Herbert S. (eds.), Committee to Study National Cryptography Policy, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press, Washington, D.C., USA, 1996.

Domeij, Bengt; Fokus på patenträtten: en introduktion till patenträtten, BrandEye Stockholm, Sweden, 1997.

Eeckhout, Piet – Govaere, Inge; On Dual Use Goods and Dualist Case Law: The Aimé Richardt Judgment on Export Controls; in publication: Common Market Law Review 29: 941-965, Kluwer, The Netherlands 1992.

Emiliou, Nicholas; Restrictions on Strategic Exports, Dual-Use Goods and the Common Commercial Policy, on publication: European Law Review 22, Sweet & Maxwell, 1997.

Eurooppaoikeus; Joutsamo, K; Aalto, P; Kaila, H; Maunu, A; 3rd Revised Edition, Lakimiesliiton kustannus, Helsinki 2000.

Eurooppaoikeus; Joutsamo, K; Aalto, P; Kaila, H; Maunu, A; Lakimiesliiton kustannus, Helsinki 1996.

Gladman, Brian; The Wassenaar Arrangement and Controls on Cryptographic Products, FIPR - Foundation for Information Policy Research, Worcester, United Kingdom, August 1998, [http://www.fipr.org/publications/gladmanex.pdf 16. 2.2000].

Govaere Inge; Case C-70/94, Fritz Werner Industrie-Ausrüstungen GmbH v. Federal Republic of Germany, [1995] ECR I-3189 and Case C-83/94, Criminal proceedings against Peter Leifer, Reinhold Otto Krauskopf, Otto Holzer, [1995] ECR I-3231; judgments of the Court of Justice of 17 October 1995; in publication: Common Market Law Review 34, 1019-1037, 1997, Kluwer Law International, The Netherlands.

Hunnings, March; Legal Aspects of Technology Transfer to Eastern Europe and the Soviet Union, in Schaffer (ed.), Technology Transfer and East-West Relations, 1985.

Kapteyn, P. J. G.; Introduction to the law of the European communities: after the coming into force of the Single European Act, 2nd ed., Laurence W. Gormley (ed.), Deventer Kluwer Law and Taxation 1990 (1989).

Koops, Bert Jaap; Crypto Law Survey [http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm 20. 6.2000].

Koutrakos, Panos; Export of Dual-use Goods Under Law of the European Union, European Law Review, June 1998.

Kuyper; Trade Sanctions, Security and Human Rights and Commercial Policy, in Mareceau (ed.), The European Community's Commercial Policy after 1992: The Legal Dimension, 1993.

Lenstra, Arjen K. – Verheul, Eric R.; Selecting Cryptographic Key Sizes, November 24, 1999 [http:www.cryptosavvy.com/ 5. 4.2000].

McDonald, Stuart; Technology and the Tyranny of Export Controls: Whisper Who Dares, 1990.

La Politique Française de Contrôle des Exportations d'Armements et de Biens et Technologies à Double Usage; [http://www.wassenaar.org/docs/fr1_fr.pdf 20. 6.2000].

Proliferation of Weapons of Mass Destruction: Assessing the Risks; U.S. Congress, Office of Technology Assessment, Washington, DC; U.S. Government Printing Office, August 1993.

Ramberg Jan; International Commercial Transactions, Norstedts Juridik, Stockholm 1998.

Schneier, Bruce; Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 1995.

Schroeder–Köchncke; Community Regime For the Control of Exports of Dual Use Goods, International Trade Law Review 1995.

Strategic Export Controls: The Impact On Cryptography; Bohm, Nicholas; Brown, Ian; Gladman, Brian; A Response by The Foundation For Information Policy Research (FIPR) to the Department of Trade and Industry (UK), 1998 [http://www.fipr.org/publications/fexport.html 16. 2.2000].

Tietoturvallisuus ja laki – näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä; Ahti Saarenpää (toim.), Tuomas Pöysti (toim.), Mikko Sarja, Viveca Still, Ruxandra Balboa-Alcoreza.

OFFICIAL DOCUMENTS

European Union

COM (97) 503; Towards A European Framework for Digital Signatures And Encryption, Official Journal of the European Communities, November 4, 1996.

Declaration on Non-Proliferation and Arms Exports; European Council, Luxembourg 29 June 1991.

Échanges Intérieurs Textes; Commission publication, 1987 No 1.

Interception Capabilities 2000; European Parliament, Directorate General for Research, Directorate A, The STOA Programme, Author: Duncan Campbell - IPTV Ltd – Edinburgh, Editor: Mr. Dick Holdsworth, Head of STOA Unit, April 1999, PE Number: PE 168.184/Part 4/4.

KOM (98) 257 lopullinen; Ehdotus Neuvoston asetukseksi (EY) kaksikäyttötuotteiden ja teknologian vientiä koskevan yhteisön valvontajärjestelmän käyttöönottamisesta, Bryssel 15. 5.1998.

KOM (98) 258 lopullinen; Komission kertomus Neuvoston asetuksen 3381/94/EY soveltamisesta.

Poettering Report; Report on the Outlook for a European Security Policy: The Significance of European Security Policy and its Implications for European Political Union, European Parliament Session Documents, A3-0107/91, PE 146.269/fin., 29 April 1991.

SEC (92) final

The Lisbon Criterion; European Council, Lisbon, 1992.

OECD

OECD Adopts Guidelines for Cryptography Policy; Press Release, OECD, Paris, 27 March 1997.

OECD Guidelines for Cryptography Policy; OECD, 27 March 1997.

Report on Background and Issues of Cryptography Policy; OECD 1997 [http://www.oecd.org 4. 4.2000].

Wassenaar Arrangement

Initial Elements; [http://www.wassenaar.org/docs/IE96.html 14. 2.2000].

List of Dual-use Goods and Technologies and Munitions List; [http://www.wassenaar.org/list/WALIST991.zip 14. 2.2000].

WA Public Statement For 1999 Plenary, Vienna, December 3rd , 1999 [http://www.wassenaar.org/docs/press_5.html 14. 2.2000].

Finland

Hakuohjeet ja asiakirjamallit; Kauppa- ja teollisuusministeriö, Suomi [http://www.vn.fi/ktm/2/vientivalvonta/1_6.htm 20. 6.2000].

HE 69/1996 vp; Hallituksen esitys Eduskunnalle laiksi kaksikäyttötuotteiden vientivalvonnasta.

Kaksikäyttötuotteiden vientivalvonta; Kauppa- ja Teollisuusministeriö, Suomi [http://www.vn.fi/ktm/vientiv/ 20. 6.2000].

KK 1430/1998 vp; Written question, Outi Siimes /kok: On Expanding the Wassenaar Arrangement (in Finnish).

KK 1445/1998 vp; Valtiopäivät 1998; Kirjallinen kysymys 1445 N:o 1423 Jaakko Laakso /vas: Salausohjelmien vientivalvontasopimuksesta; N:o 1445 Erkki Pulliainen /vihr: Wassenaar-sopimuksen vaikutuksesta Suomen teollisuuden kilpailukykyyn.

Salauspolitiikassa noudatettavat periaatteet; 30.9.1998, Finnish Ministry of Transportation, memorandum approved by Council of State 7.10.1998 [http://www.vn.fi/lm 13.11.1999].

Valtion etätyön tietoturvallisuussuositus; Valtionhallinnon tietoturvallisuuden johtoryhmä 1/1999, Valtiovarainministeriö.

Vientivalvonta - Exportkontroll; Kauppa- ja teollisuusministeriö, 1999.

Germany

Export Controls - Brief Outline; Bundesausfuhramt (BAFA), 9 April 1999.

Roth, Harald H.; Encryption Controls in Germany [http://www.export-control.com/ 25. 6.2000].

Sweden

Kryptopolitik - möjliga svenska handlingslinjer; En rapport från Regeringskansliets referensgrupp för krypteringsfrågor, Regeringskansliet, Oktober 1997.

Lag och förordning; Inspektionen för strategiska produkter (ISP) [http://www.isp.se/SP/splagar.htm 20. 6.2000].

Regeringens Proposition 1995/96:31; Ny myndighet för kontroll över krigsmateriel och andra strategiskt känsliga produkter.

Tillståndstyper SP; Inspektionen för strategiska produkter (ISP) [http://www.isp.se/SP/tillstndsp.htm 20. 6.2000].

United Kingdom

Annual Report on Strategic Export Controls; Foreign and Commonwealth Office, Department of Trade and Industry, Ministry of Defence, October 1999.

Guidance on Supporting Documentation Needed When Applying For a Standard Iindividual Export Licence (SIEL); Export Control Organization, UK 1999.

Do I need a licence? A brief guide to controls administered by the Export Control Organisation; Export Control Organization, UK 1999 [http://www.dti.gov.uk/export.control/pdfs/briefguide.pdf 25. 6.2000].

Export Controls: A Guide for Business: Supplementary Guidance Notes; Export Control Organization, UK 1999 [http://www.dti.gov.uk/export.control/publications/bizguide/xtec.htm 25. 6.2000].

Supplementary Guidance Note on the End Use Control; Export Control Organization, UK 1999 [http://www.dti.gov.uk/export.control/publications/bizguide/enduse.htm 25. 6.2000].

Appendix C - Suspicious Enquiries; Export Control Organization, UK 1999 [http://www.dti.gov.uk/export.control/ 25. 6.2000].

United States of America

Federal Register / Vol. 65, No. 10 / Friday, January 14, 2000 / Rules and Regulations Part III; Department of Commerce, Bureau of Export Administration, 15 CFR Parts 734, 740, et al., Revisions to Encryption Items; Interim Final Rule.

REFERRED CASES

Court of Justice of the European Communities

Case 6/64, *Costa v. ENEL*, ECR 1964, 585.

Case 74/69, *Krohn & Co*, ECR 1970, 451.

Case 42/71, *Politi*, ECR 1971, 1039.

Case 18/72, *Granaria Graaninkoopmaatschappij*, ECR 1972, 1163.

Opinion 1/75, ECR 1975, 1364.

Opinion 1/78, ECR 1979, 2871.

Case 72/83, *Campus Oil Ltd.*, ECR 1984, 2727.

Case 41/76, *Donckerwolke v Procureur de la République*, ECR 1976, 1921.

Case 50/76, *Amsterdam Bulb*, ECR 1977, 137.

Case 68/76, *Commission v France*, ECR 1977, 515.

Case 53/76, *Procureur de la République v Bouhelier*, ECR 1977, 197.

Case 106/77, *Simmenthal*, ECR 1978, 629.

Case 251/78, *Dencavit Futtermittel v. Minister für Ernährung, Landwirtschaft und Forsten*, ECR 1979, 3369.

Case 292/82, *Merck*, ECR 1983, 3781.

Case 337/82, *St Nicolaus Brennerei*, ECR 1984, 1051.

Case 174/84, *Bulk Oil (Zug) AG v Sun International Limited and Sun Oil Trading Company*, ECR 1986, 559.

Case C-62/88, *Chernobyl*, ECR 1990, I-1527.

Case 117/88, *Trend-Moden Textilhandel.*

Case C-367/89, *Criminal proceedings against Aimé Richardt and Les Accessoires Scientifiques SNC*, ECR 1989, I-4621.

Case C-70/91

Case C-70/94, *Fritz Werner Industrie-Ausruestungen GmbH v Federal Republic of Germany*, ECR 1995, page I-3189.

Case C-83/94, *Criminal proceedings against Peter Leifer, Reinhold Otto Krauskopf and Otto Holzer*, ECR 1995, I-3231.

Case C-120/94, *Commission v Greece (Re FYROM)*, ECR 1995, I-1513.

Case T-194/94, *Carvel*, 1995, II-2765.

Finland

KKO

KKO 1991:81; *Crime against the State*, delivered 4. 6.1991.

GLOSSARY OF ABBREVIATIONS, ACRONYMS AND TERMS

LEGAL

Acquis Communautaire	European Community's legislation in force and case law.
AG	Advocate General
AG	Australia Group, similar international undertaking as WA, in the field of non-proliferation of chemical and biological weapons.
BAFA	Bundesausfuhramt, Federal Export Office (Germany).
BAnz	Bundesanzeiger (Germany)
BXA	Bureau of Export Administration, U.S. Department of Commerce
CCP	Common Commercial Policy
CFSP	Common Foreign and Security Policy, II pillar of the EU.
COCOM	Coordinating Committee on Multilateral Export Controls, preceded WA.
DTI	Department of Trade and Industry
Dual-Use Goods	Goods that have both military and civil applications.
DUD	Dual-Use Decision (94/942/CFSP: Council Decision of 19 December 1994 on the joint action adopted by the Council of the basis of Article [J.3] of the Treaty on European Union concerning the control of exports of dual-use goods; Official Journal L 367, 31/12/1994, p. 8 – 163).
DUR	Dual-use Regulation, Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods.
EAR	Export Administration Regulations (U.S.)
EC	European Communities, I pillar of the EU. EC refers also to the Treaty of the European Communities.
ECJ	European Court of Justice
ECO	Export Control Organization, UK DTI.
EEC	European Economic Community
EU	European Union
FR	Federal Register (U.S.)
GATT	General Agreement on Tariffs and Trade, see WTO.
GCHQ	Government Communications Headquarters (UK)
GSN	General Software Note
GTN	General Technology Note
IPR	Intellectual Property Rights
ISP	Inspektionen för strategiska produkter, National Inspectorate for Strategic Products (Sweden).
ITAR	International Traffic in Arms Regulations
ITU	International Telecommunications Union
IW	Information Warfare. Situation in handling of the societally significant infrastructure, which may be deemed to threaten society's security or public order (source: *Tietoturvallisuus ja laki*, p. 79).
KHO	Korkein hallinto-oikeus (Supreme Administrative Court, Finland)
KKO	Korkein oikeus (Supreme Court, Finland)
MTCR	Missile Technology Control Regime
MTI	Ministry of Trade and Industry
NGO	Non-Governmental Organization
NSA	National Security Agency (U.S.)
NSG	Nuclear Suppliers Group
OECD	Organisation for Economic Co-operation and Development
OJ	Official Journal of the European Communities
QMV	Qualified Majority Voting
Re-Export	Export to third country after initial export.

SCSSI	Service central de la sécurité des systèmes d'information (Central service for the security of information systems), Prime Ministerial department under the authority of the SGDN (France).
SEM	Single European Market
SGDN	Secrétariat Général à la Défense Nationale, Secretary General for National Defence (France).
SIGINT	Signals Intelligence, eavesdropping and monitoring of adversary's communications and other relevant signals.
TEU	Treaty of European Union
TFS	Tullverkets författningssamling (Sweden)
UlkoturvaL	Act on Securing Nations Foreign Trade and Economic Growth 157/1974 (Republic of Finland); (Laki maan ulkomaankaupan ja taloudellisen kasvun turvaamisesta (157/1974)); (Repealed by Act 562/1996).
WA	Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies.
WA-LIST	WA List of Dual-Use Goods and Technologies and Munitions List
WMD	Weapon of Mass Destruction
WTO	World Trade Organisation, the GATT has been merged to WTO negotiations.

TECHNICAL

Algorithm	A formula or set of steps for solving a particular problem. To be an algorithm, a set of rules must be unambiguous and have a clear stopping point. Algorithms can be expressed in any language, from natural languages like English or French to programming languages like C.
Asymmetric Algorithm	A cryptographic algorithm using different, mathematically-related keys for encryption and decryption. Synonym of public key algorithm.
Cryptanalysis	The analysis of a cryptographic system or its inputs and outputs to derive confidential variables or sensitive data, including clear text.
Cryptography	The discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use. Cryptography is limited to the transformation of information using one or more secret parameters (e.g. crypto variables) or associated key management.
DECT	Digital Enhanced Cordless Telecommunications
Diffie-Hellman	The Diffie-Hellman public-key encryption algorithm.
DL	Discrete logarithm
ElGamal	One subgroup of public key algorithms
Elliptic Curve	One subgroup of public key algorithms
Encryption, Strong	Encryption, which is unbreakable or compromised only with very high costs. Secure encryption key recommendations start from 128 bits (symmetric algorithm) and 512 bits (asymmetric algorithm). Recommendations subject to changes in the future.
Encryption, Weak	Encryption, which is easily breakable or breakable with modest costs. Key sizes under 128 bits (symmetric algorithm) and 512 bits (asymmetric algorithm). Recommendations subject to changes in the future.
Evaluation Copy	Commercial software, which is programmed to expire e.g. in 30 or 60 days after the initial computer installation. After expiration it becomes unusable. Before expiration, the program functions as a normal paid copy.
Firmware	The programmable information used to control the low-level operations of hardware. Firmware is commonly stored in read only memory (ROM), which is initially installed in the factory and may be replaced in the field to fix mistakes or to improve system capabilities.
FTP	File Transfer Protocol
GSM	Global System for Mobile Communications

Hardware	The physical components (as electronic and electrical devices) of an apparatus (as a computer).
HTTP	Hypertext Transfer Protocol
Information Security	All the means and functions ensuring the accessibility, confidentiality or integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. This includes cryptography, cryptanalysis, protection against compromising emanations and computer security.
Key Escrow	Third party exceptional access and decryption of encrypted information (synonym to key recovery).
Multilevel Security	A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization. Multilevel security is computer security and not computer reliability which deals with equipment fault prevention or human error prevention in general.
Object Code	An equipment executable form of a convenient expression of one or more processes (source code (or source language)) which has been converted by a programming system, i.e. the 'executable' code of ones and zeros that provides a computer with instructions on what steps to perform. Contrast with source code.
Personalised Smart Card	A smart card containing a microcircuit which has been programmed for a specific application and cannot be reprogrammed for any other application by the user.
PGP	Pretty Good Privacy. Program originally developed by Philip Zimmermann to provide strong cryptographic capabilities freely to unsophisticated end-users all over the world.
PKI	Public Key Infrastructure
RSA Algorithm	The Rivest-Shamir-Adelman public key encryption algorithm.
SDL	Subgroup discrete logarithm systems
Software	Something used or associated with and usually contrasted with hardware: as a: the entire set of programs, procedures, and related documentation associated with a system and especially a computer system; specifically: computer programs.
Source Code	A convenient expression of one or more processes which may be turned by a programming system into equipment executable form (object code (or object language)). The textual form in which a program is entered into a computer (e.g., Pascal or C).
SSH	Secure Shell
Symmetric Algorithm	A cryptographic algorithm using an identical key for both encryption and decryption. A common use of symmetric algorithms is confidentiality of data.
TCP/IP	Transmission Control Protocol/Internet Protocol
UNIX	A popular multi-user, multitasking operating system. UNIX was one of the first operating systems to be written in a high-level programming language, namely C. The emergence of a new version called Linux is revitalizing UNIX across all platforms.
Z/pZ	One subgroup of public key algorithms.

1 INTRODUCTION

1.1 The Problem – Legal Issues Raised by the Democratization of Cryptography

This study is focused on legal problems concerning exportation of encryption software. Export controls imposed on cryptographic software affect the possibilities of individuals and companies of lawfully obtaining cryptographic software, in order to protect themselves against breaches of security. On the other hand, export control regimes constantly face new challenges from non-lawabiding people, who seek to discover new ways and means to circumvent controls. The inherently global nature of information and communication networks makes the task of export control enforcement quite difficult and the difficulties of defining and enforcing jurisdictional boundaries in the international environment become more and more evident.

In order to properly understand the field of cryptography, one must bear in mind that there are three main reasons why a person might want to use cryptography. These are to ensure the confidentiality of data, authenticate data, and to ensure its integrity.[4] Cryptography is used to protect *inter alia* information and communications systems. Also digital signatures are based on encryption algorithms. The importance of information and communications systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored on those systems. At the same time those systems and data are also increasingly vulnerable to a variety of threats, such as unauthorised access and use, misappropriation, alteration, and destruction.

The confidentiality of information that cryptography can provide is useful not only for the legitimate purposes of preventing information crimes (e.g. the theft of trade secrets or unauthorized disclosure of sensitive medical records) but also for illegitimate purposes (e.g., shielding from law enforcement officials a conversation between two terrorists planning to bomb a building). Although strong automatic encryption implemented as an integral part of data processing and communications provides confidentiality for 'good guys' against 'bad guys' (e.g. business protecting information against economic intelligence efforts of foreign nations), it unfortunately also protects 'bad guys' against 'good guys' (e.g. terrorists evading law enforcement agencies). Under appropriate legal authorization law enforcement authorities may gain access to 'bad guy' information for the purpose of investigating and prosecuting criminal activity. Similarly intelligence gathering for national security and foreign policy purposes depends on having access to information of foreign governments and other foreign entities. Because such activities benefit

[4] *Baker 1997*, chapter 'Background' para 5. However, the use of cryptography falls beyond the scope of this study.

society as a whole (e.g. by limiting organized crime and terrorist activities), 'bad guy' use of cryptography used for confidentiality poses a problem for society as a whole, not just for law enforcement.

Considered in these terms, it is clear that the development and widespread deployment of cryptography that can be used to deny government access to information ***represents a challenge to the balance of power between the government and the individual***. Historically all governments, under circumstances that further the common good, have asserted the right to compromise the privacy of individuals, e.g. through opening mail, tapping telephone calls, inspecting bank records. Unbreakable cryptography for confidentiality provides the individual with the ability to frustrate assertions of that right.

Export controls imposed on cryptography have generated considerable controversy. Export controls on cryptography have been controversial because they pit the interests of vendors and multinational corporations against the needs of State security. Two members of the Finnish Parliament crystallized the problems of the "cryptography controversy"[5], clearly and in a down-to-earth way, in their parliamentary question, debating Finland's decision to join the WA:

> "Popularly encryption technology can be compared to a lock, it is a method to lock information so, that trespassers cannot access it without a key. Maybe in the past, locks were only in the door of the king's treasury, but can you imagine that modern society could be safe without locks protecting the doors of homes and establishments? So not only doors of WMD -factories need locks. Nowadays we use encryption technology every day in bank cards, in GSM-telephones, in Internet bank connections and so on. Encryption technology also plays a more and more important part in so-called embedded systems, in other words in those computers which control all kinds of equipment and institutions, like factories, power plants, access control systems, telephone networks and power grids. More and more often also the control of embedded systems is handled over open information network. If information moves unencrypted or weakly encrypted, it would be like the doors of those establishments which would be unlocked. Any given hostile party could destroy or paralyze in an instant this nation's vitally important infrastructure."[6]

Encryption functions can be both hardware and software based. Usually the same rules apply to hardware and software, because in Wassenaar Arrangement, which is the principal foundation to all encryption software export control regimes around the world, controlled information security products are controlled or relaxed from controls principally on the basis of the method used. It can also be, in some situations, quite difficult to judge whether some high technology item is software or hardware or a combination of both, because both are used hand in hand in computational processes.[7] One must also bear in mind that this dichotomy is inherently not a legal but technical problem, and should be discussed elsewhere. Of course one can not forget that in the

[5] The term was invented by Bert-Jaap Koops PhD, University of Tillburg, Netherlands scholar, whose PhD -thesis covers cryptography policy issues. See *Koops 2000.*
[6] KK 1445/1998 vp.
[7] The concept of firmware makes things even more complicated.

highly specialized legal field of encryption software export controls, technical and legal expertise is closely linked together. Categorically this marriage of jurisprudence and technical expertise is commonplace in the domain of cyberlaw or jurisprudence linked to emerging technologies.

1.2 The Role of Export Controls

Internationally, export controls are the strongest tool used by governments to limit development of encryption products. Export controls on cryptography and related technical data have been a pillar of cryptography policy for many years. Increasingly, they have generated controversy because they pit the needs of national security to conduct signals intelligence against the information security needs of legitimate businesses and the markets of manufacturers whose products might meet these needs.[8] Export controls reduce the availability of encryption in common programs such as operating systems, electronic mail and word processors. The restrictions make it difficult to develop international standards for encryption and interoperability of different programs. Countries must develop their own local programs, which do not interoperate well (if at all) with other programs developed independently in other countries. They may not be as secure because of a lack of peer review. Because markets are smaller, companies and individuals are not as interested in developing programs because of smaller potential profits. In some Wassenaar member countries export controls are used as a justification to limit the availability of encryption on domestic Internet sites and thus serve as ***indirect domestic controls*** on encryption.[9]

Some countries have taken advantage of the situation by promoting the lack of controls in their countries. One result of this has been the emergence of small companies, in many countries without restrictions, which produce encryption products. Another result has been companies moving their encryption production divisions overseas to countries with fewer controls[10], such as Switzerland or Anguilla, a British self-governing territory in the Caribbean.[11] Switzerland officials have stated according to *Cryptography and Liberty 1999*: "Switzerland will keep its efficient export permit process for cryptographic goods in order to encourage Swiss exports to increase their sales and share worldwide while being mindful of national security interests." Although Switzerland is member of WA, it is pursuing very liberal crypto policy, under full compliance with its provisions. It must be recognized that all the other WA –countries also had

[8] *Cryptography's Role in Securing the Information Society*, chapter 4 paragraph 1.
[9] See *Cryptography and Liberty 1999* for further details. Domestic controls are not examined in this thesis.
[10] *Baker-Hurst*: "... many companies in the United States are considering ways to avoid U.S. controls legally. Some ... have announced relationships with foreign entities that develop encryption and plan to incorporate this encryption into their product line." In U.S. export controls are allegedly even stricter than in the EU region.
[11] There are no cryptography export controls in Anguilla. *Cryptography and Liberty 1999.*

their national economic interests in mind when they joined it. Had they deemed it detrimental to their national interests they probably would not have joined.

The Internet has changed significantly the effectiveness of export controls. Strong, unbreakable encryption programs can instantly be delivered anywhere in the world. It is increasingly difficult for countries to limit digital dissemination, and once a program is released, it is nearly impossible to stop its redissemination, especially if it occurs in one of the many countries around the world with no export controls.

1.3 The Rationale of Encryption Software Export Controls

The ***true ratio*** of export controls on cryptographic products is rather self-evident. It is not publicly stated anywhere in the Wassenaar Arrangement's official documents, but one can add one and one together after some time spent researching nature of the Arrangement. As stated in the *Initial Elements*, the WA is established in order to "prevent the acquisition of ... sensitive dual-use items for military end uses, if the situation in a region or the behaviour of a State is, or becomes, a cause for serious concern to the participating States."[12]

In the case of crypto products, this means that those products should not be exported to a State, which is, or most likely will in the future be, ***an adversary*** of one or more participating States. An export restriction, ***presumably effectively enforced***, will deny a potential adversary the capabilities to secure its military, diplomatic, other official and private sector communications.[13] This means that the adversary's military and civilian infrastructures are prone to effective SIGINT efforts.[14] Also industrial espionage, conducted by private sector operatives, is easier if the subject does not use cryptography.

Laws governing privacy can conflict with laws on cryptography. For example, a law on data privacy may require that certain sensitive data associated with an individual be protected, while a law on cryptography may forbid the use of cryptography. Such laws would obviously conflict if a situation arose in which cryptography were the only feasible tool for protecting such data. In short, policies regarding data export, import, and privacy are an additional dimension of resolving policy with respect to cryptography. EC Data Protection Directive 95/46/EC requires *inter alia* that personal information, such as medical records, should be adequately protected from outside intrusions. However, in the EU, strong crypto products are classified as sensitive, and at

[12] *Initial Elements* I.3.
[13] This aspect of export controls was also recognized in European Commission Communication, COM (97) 503, in chapter 2.1. paragraph 1.
[14] Cryptanalysis for *inter alia* SIGINT purposes is also a part of the techniques of possible *information warfare*, *Tietoturvallisuus ja laki*, p. 86.

present also intra-Community transfers require a license.[15] Therefore protection of personal information is made more difficult, because obtaining protective software or hardware is harder due to export control laws, namely EU Dual-Use Regulation 3381/94 EC. The export authorization procedure established by this EC regulation does not help European public or private entities which seek to acquire best products in order to fulfill the requirements of the Data Protection Directive.

It is important to keep in mind that ***the ultimate goal of export controls on cryptography is to keep strong cryptography out of the hands of potential targets of signals intelligence***.[16] Some WA participating States have very powerful SIGINT bodies, capable of eavesdropping large amounts of communication all over the world.[17] Wide availability of strong unbreakable encryption means a threat to efforts of those intelligence gathering bodies. In small WA countries, like Finland, SIGINT capabilities are quite modest, and therefore interest in limiting the use of cryptography is smaller.

In *Cryptography's Role in Securing the Information Society* it was concluded that the U.S. export control regime on cryptographic products was intended to serve two primary purposes. My understanding is that this can be applied also to WA export controls on cryptography *mutatis mutandis*, as far as WA's rationale is concerned:

> "• To delay the spread of strong cryptographic capabilities and the use of those capabilities throughout the world. Senior intelligence officials recognize that in the long run, the ability of intelligence agencies to engage in signals intelligence will inevitably diminish due to a variety of technological trends, including the greater use of cryptography."
> "• To give the U.S. government a tool for monitoring and influencing the commercial development of cryptography. Since any U.S. vendor that wishes to export a product with encryption capabilities for confidentiality must approach the U.S. government for permission to do so, the export license approval process is an opportunity for the U.S. government to learn in detail about the capabilities of such products. Moreover, the results of the license approval process have influenced the cryptography that is available on the international market."[18]

Also the economic aspects can not be forgotten, because export controls obviously have some effect on the exporters' market position. Especially the European Commission has been concerned about this. Differences between Member States' export controls may adversely affect the functioning of the Single European Market (SEM), by creating obstacles to free circulation of goods within the Community or in relation to non-Member countries. Differences can also lead to distortion of competition.[19]

---

[15] *Cryptography's Role in Securing the Information Society*, Appendix G.3. See also chapter 4.
[16] *Cryptography's Role in Securing the Information Society* chapter 4.2.
[17] Largest of them is the U.S. NSA, which has had historically very close cooperation with its British counterpart GCHQ, *Interception Capabilities 2000*. Russians have similar SIGINT agency called FAPSI.
[18] *Cryptography's Role in Securing the Information Society*, chapter 4.1.1.
[19] COM (97) 503 2.1.

There are also underlying trade policy issues involved. At least for the time being there are some facts to be recognized. Export controls on cryptographic technologies have a negative effect on commercial interests. The global software business is dominated by U.S.-controlled corporations. They hold the largest market shares. The majority of mass-market applications, for example, are created in the U.S. Another fact is that the U.S. has a very large domestic marketplace for encryption software. For an EU software developer it is very important to be able to reach this market.

In the era of free trade and global marketplace, the U.S. Government simply cannot, and probably would not even want to be so protective that it would impose import controls in order to protect US companies. Import restrictions have not even been contemplated in the U.S. or elsewhere, with a few minor exceptions.[20] Therefore, for an EU software developer exporting to the U.S. the only legal obstacles[21] that remain are the export licensing procedures imposed under the EU's or Member States' legal systems. These export regimes can decide the business success right from the start. Too bureaucratic or cumbersome regimes may halt the exports totally to the U.S. and elsewhere.[22] Reseach indicates that at present regimes are not that bureaucratic in the EU region, and if the liberalization and harmonization trend continues in the EU, there is no great cause for concern for European software developer. Finally, although export controls may have significant economic effects, they have not been constructed to enhance foreign trade, but to enforce nations' security and foreign policy interests. Therefore export controls will remain an obstacle to free trade, although a formally legitimate one.

[20] Of EU Member States only France has limited import controls. See chapter 5.4 covering France.
[21] Of course one must comply with possible customs and other laws, national or EC based, but those problems fall beyond the scope of this study.
[22] KK 1430/1998 vp.

2 THE IMPACT OF OECD CRYPTOGRAPHY POLICY

In 1997 OECD released *Guidelines for Cryptography Policy*. Within the OECD it was recognised early on that disparities in laws could create obstacles to the development of national and global information and communications networks.[23] Cryptography is thought to be particularly valuable in fostering global electronic commerce.[24] The OECD recommendation sets out eight principles that should be followed by member nations in establishing their own cryptography policies.[25] OECD Guidelines are only "recommendations"[26] - but because the ***OECD functions as a consensus forum for the most developed countries***, the Guidelines are had ***a significant international impact***.[27] For example the Finnish and Swedish Governments[28] have adopted cryptography policies pursuant to OECD's challenge[29] to national governments to draft national cryptography policies. In fact, many nations have not stated their cryptography policies openly in the past. In the most egregious cases, business users learned the scope of a nation's policy only when the authorities appeared at their hotel or office to confiscate their 'unauthorized' communications equipment. If followed faithfully, this OECD recommendation will move regulation of cryptography out of the shadows and into the normal world of business regulation.[30] It must also be noted that at present all OECD countries, except Iceland and Mexico, are members of WA.[31] Therefore OECD Guidelines have probably influenced somehow respective national policies, which national governments assert *inter alia* in WA-related negotiations.

Guidelines are aimed primarily at governments, though with the expectation that they will be widely read and followed in the private sector as well. The document states that all eight principles are interdependent and should be implemented as a whole. It calls for a 'balance' among the interests at stake, but it provides no further guidance to policymakers, who will understandably feel that the various principles often look in quite contradictory directions. In the end, then, the Guidelines and the integration section can best be seen as creating a series of policy objectives, all of which must be given some gravitational force. Perhaps one can best imagine the principles as fixed points, to which may be attached elastic bands of varying strengths. If all

---

[23] *Report on Background and Issues of Cryptography Policy*, Chapter IV, National Level Activities.
[24] *Baker-Hurst* p. 70.
[25] *Baker-Hurst* p. 49: "The Guidelines do not apply to cryptography that protects military and diplomatic information. Precise scope of this exception is difficult to measure, because different nations treat different kinds of information as "classified" or otherwise protected"
[26] *Berg* p. 80. The Guidelines are not legally binding on its member countries.
[27] *Baker 1997.*
[28] For Finnish national policy, see *Salauspolitiikassa noudatettavat periaatteet* and for Swedish, see *Kryptopolitik – möjliga svenska handligslinjer*.
[29] Governments are to: "state clearly and make publicly available" any national controls on cryptography. See Principle 8 of the *OECD Guidelines for Cryptography Policy*, subparagraph 1, 2nd sentence and *OECD Adopts Guidelines for Cryptography Policy.*
[30] *Baker-Hurst* p. 48.
[31] See chapter 3.

of the bands are joined, the point at which they come to equilibrium will vary depending on the strength of each band. But it is impermissible to give no weight at all to any one of the principles (with the possible exception of the lawful access principle).[32] In the Guidelines it is also stated that they are to be reviewed at least every five years.[33]

Very interesting and significant was the inclusion of a specific recommendation that members avoid policies that create unjustified obstacles to trade and to the development of networks:

> "8. INTERNATIONAL CO-OPERATION
> GOVERNMENTS SHOULD CO-OPERATE TO CO-ORDINATE CRYPTOGRAPHY POLICIES. AS PART OF THIS EFFORT, GOVERNMENTS SHOULD REMOVE, OR AVOID CREATING IN THE NAME OF CRYPTOGRAPHY POLICY, UNJUSTIFIED OBSTACLES TO TRADE.
>
> In order to promote the broad international acceptance of cryptography and enable the full potential of the national and global information and communications networks, cryptography policies adopted by a country should be co-ordinated as much as possible with similar policies of other countries. To that end, the Guidelines should be used for national policy formulation.
>
> If developed, national key management systems must, where appropriate, allow for international use of cryptography.
>
> Lawful access across national borders may be achieved through bilateral and multilateral co-operation and agreement.
>
> No government should impede the free flow of encrypted data passing through its jurisdiction merely on the basis of cryptography policy.
>
> In order to promote international trade, governments should avoid developing cryptography policies and practices which create unjustified obstacles to global electronic commerce. Governments should avoid creating unjustified obstacles to international availability of cryptographic methods.

This language is similar to injunctions contained in WTO agreements. By placing this recommendation on an equal footing with the recommendation that nations adopt the Guidelines, OECD made avoidance of unjustified obstacles to trade an overarching recommendation that is both independent of the Guidelines and a lodestar for interpreting and applying all aspects of the Guidelines.[34] Governments are to co-operate in order to avoid unjustified obstacles to global trade, and even to remove existing obstacles created by cryptography policy if they cannot be justified.[35]

This principle obviously begs the question of how such obstacles can be justified. The language is borrowed from international trade law, where what is unjustified has been defined by usage. The most likely interpretation in this context is that cryptography policy should not be used as a pretext to exclude or discriminate against foreign products. It is not intended to override national security or law enforcement policies if applied in good faith, and ***it clearly does not pro-***

[32] *Baker 1997*. Lawful access principle covers situations where national authorities can have access to plaintext information.
[33] *OECD Guidelines for Cryptography Policy* p. 7.
[34] *Baker-Hurst* p. 47.
[35] *Baker-Hurst* p. 69.

hibit Wassenaar export controls,[36] since several major OECD members maintained such controls on cryptography when the Guidelines were adopted. On the other hand there is a world of difference between "unjustified" and "unjustifiable" obstacles.[37]

The text states further that nations should not impede the free flow of encrypted data passing across their national territory merely on the basis of cryptography policy.[38] This principle is borrowed from a strong ITU rule against actions that impede the flow of international communications across the territory of a member State. This policy against impeding the flow of encrypted data is limited to data transiting a particular country. That is, when encrypted data crosses country A on its way from country B to country C, the cooperation principle calls on country A not to impede the flow of data between B and C.

[36] Likewise it does not prohibit Community or Member State export control regimes. They were also in force when the Guidelines were adopted. The EU Dual-Use Regulation 3381/94 (DUR) came into force on 1. 7.1995. EU export control law will be covered in detail in chapter 4.
[37] *Baker 1997.*
[38] Principle 8 of the *OECD Guidelines for Cryptography Policy*, subparagraph 4.

3 THE WASSENAAR ARRANGEMENT

3.1 History of the WA – From COCOM to the Wassenaar Arrangement

Cryptographic products and technologies have historically been subject to export controls. The history of the multilateral export controls starts after the Second World War. In 1949, seven countries decided to align their systems of export licensing with the aim of having a collective restrictions of exports on strategic and so-called dual-use goods towards the European and Asian communist countries. The seven original members were USA, UK, France, Italy, Belgium, the Netherlands and Luxembourg. The USA and groups of its closest allies in 1949 agreed not to export listed items, including some related to Multilateral Export Controls, missiles and weapons of mass destruction, to Communist countries. Periodically, these lists were adapted as a response to the changing political climate.[39] These COCOM Controls were relaxed after the collapse of the Soviet bloc. COCOM was disbanded on 31 May 1994.

The Co-ordinating Committee for Multilateral Export Controls (COCOM) was created by means of a ”gentlemen’s agreement”, and soon the NATO partners (minus Iceland) plus Japan and Australia joined this initiative.[40] Although COCOM was created by gentlemen’s agreement and has no official existence or recognition, the decisions taken by unanimity within COCOM have proven to be of great importance and have had a considerable impact on trade with the (ex-) communist countries concerned.[41]

The Republic of Finland was not a member of the COCOM, but it implemented the COCOM export restrictions, in order to secure *inter alia* the imports of western high technology products. Cases also exist where Finnish nationals have been convicted of violating the statutes implementing the COCOM controls.[42]

COCOM was unique among supplier agreements in attempting to establish common standards of enforcement of national export controls among the members. However, it is ill-suited to control proliferation-sensitive technology because the very States that were its targets - Communist and ex-Communist States -would have to be members of any nonproliferation export control regime.[43] In the WA this has been corrected because former Warsaw Pact countries have joined

[39] *Eeckhout-Govaere* p. 941.
[40] *Ibid.*
[41] *McDonald.*
[42] The most famous case of them is KKO 1991:81. Two Finnish businessmen were indicted after exporting high technology products (*inter alia* U.S. made computers; facts of the case were sealed on grounds that exposure of the facts may damage Finland’s external relations) to the Soviet Union. Finnish Supreme Court (KKO) rejected treason charges, and in general all criminal charges, but found the defendants violating statute implementing COCOM (UlkoturvaL) and ordered seizure of funds amounting to the sum of the exported goods.
[43] *Proliferation of Weapons of Mass Destruction: Assessing the Risks*, p. 89.

WA. The WA, COCOM's successor, was agreed on 19 December 1995 after over two years of negotiations. It took effect on July 12, 1996. The WA now consists of 33 countries, 15 of them being the EU Member States.[44] The Arrangement controls the export of so-called dual-use goods and technologies, which can be used for both civilian and military end uses. Dual-use products can also be called strategic products. Dual-use items are not classified as arms, but rather as items or technology, which can be used to enhance or promote general military capability. *Inter alia* cryptographic software is classified in WA as a dual-use item.[45]

Ever since the late 1990s the public outcry against export controls on encryption products has been quite loud. Groups such as European software companies and human rights groups have been actively lobbying against them. Other items in the Wassenaar Arrangements Control List have not received similar negative coverage.

The WA is a part of international cooperation in non-proliferation and weapons controls. Other similar arrangements in different product fields are the Nuclear Suppliers Group, the Missile Technology Control Regime and the Australia Group. The latter was established to control the exports of components needed to make chemical or biological weapons.

3.2 The Legal Status of WA

The Wassenaar Arrangement is neither an international treaty nor a law. It is merely designed to exchange views and information on international trade in conventional arms and dual-use goods and technologies. The WA is not a valid agreement, as far as international law is concerned, because it lacks ratification in participating States. It was never meant to be ratifiable and negotiations have been conducted at civil servant level, rather than at political level.

Like its predecessor, COCOM, its character can be best described as a legally non-binding undertaking,[46] a sort of gentleman's agreement among its participating States. The WA does not contain any sanction provisions against States which violate it. In a possible violation situation one or more participating States may resort to diplomatic consultation or pressure measures. However these 'enforcement options' are beyond this legal analysis. Usually the participating States loyally enforce the Control List (WA-LIST) and they obey the provisions of international

[44] The member countries are: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, United Kingdom (all EU Member States); Australia, Japan, New Zealand, Norway, Switzerland, USA, Canada, Argentina, Bulgaria, Czech Republic, Hungary, Poland, Rep. of Korea, Romania, Slovak Republic, Turkey, Ukraine and Russian Federation.
[45] Relevant provisions will be examined in chapter 3.5.
[46] *Koutrakos* p. 248.

law in general, because they want to uphold credible a image in their foreign policy. This is especially true with small or non-influential countries like Finland.

Also, while participating countries commit to adjust their national export control policies to adhere to the Wassenaar Arrangement Control Lists, this commitment is not mandatory. Participating countries implement their encryption export policies through national legislation on a discretionary basis.[47] The decisions made in the Wassenaar Arrangement framework are not binding on participating States under international law.[48] This is one critical difference with COCOM, because in COCOM members had a veto power over individual exports involving member nations.[49]

The provisions of WA are legally based on U.S. trade law, like COCOM was in its time.[50] Therefore some help on interpretation can be obtained from legal publications covering U.S. trade legislation and case law.[51] One must, however, remember that different countries apply WA provisions from their own points of departure.

After this analysis one might come to the conclusion that WA's authority is unclear or its overall significance in the field of export controls is modest compared to strong national policies.[52] It is true that national policies can, under full compliance with WA's provisions, be quite different from one another. It is also true that even inside the EU a large variety of national licensing schemes and practices exist.[53] But it can still be argued that the WA is nevertheless *the forum* where national policies of most prominent industrial nations are compared and forged together to a unified approach. An approach which contains, maybe not all, but probably the most important item categories.

---

[47] *Initial Elements* II.3.: "The decision to transfer or deny transfer of any item will be the sole responsibility of each participating State. All measures undertaken with respect to the arrangement will be in accordance with national legislation and policies and will be implemented on the basis of national discretion."
[48] The legal status is same in NSG, MTCR and AG. *Kryptopolitik* p. 80.
[49] *Cryptography's Role in Securing the Information Society* Appendix G.6.
[50] *Eurooppaoikeus 2000*, p. 795.
[51] U.S. trade law regrettably falls beyond the scope of this study.
[52] Despite the international scope of cryptography policy, the international scene is dominated by national governments. All national governments have certain basic goals in common:
To maintain national sovereignty,
To protect public safety and domestic order,
To look after their nation's economic interests, and
To advance their national interests internationally.
These common goals translate into policy and interests that are sometimes similar and sometimes different between nations. Perhaps the most important point of similarity is that national governments are likely to take actions to mitigate the threat that the use of cryptography may pose to their ability to achieve the goals listed above. *Cryptography's Role in Securing the Information Society*, Appendix G.2.
[53] Some of these will be covered in chapter 5.

3.3 The Aims of the Wassenaar Arrangement

The WA is established in order to contribute to regional and global security and stability, to promote responsible arms and dual-use product trade and non-proliferation of weapons of mass destruction (WMDs). It is also established to prevent arms or dual-use item trade to unstable nations or regions.

In WA *Initial Elements* (I.4) it is stated that the Arrangement will not impede *"bona fide* civil transactions". This can be understood to mean that the WA can not be used to obstruct genuine civil transactions.[54] Genuine civil transactions are transfers of dual-use items which have no links whatsoever to military end use, activity promoting military-related activities or activity leading to regional instability or insecurity. The end use purpose is relevant in judging whether some transfer should be deemed to be genuinely civilian.

It is also stated that the arrangement will not be directed against any State or group of States.[55] Nor will it interfere with the rights of States to acquire legitimate means with which to defend themselves pursuant to Article 51 of the Charter of the United Nations.[56]

In its nature the WA is an evolutionary undertaking,[57] with further measures being developed over time, required by changes in international political climate or technological advances. In the plenary of 1999 it was recognized that circumvention of export controls is a problem[58] and it should be made as difficult as possible by improving the information exchange and other methods of co-operation among participating States.

The WA with its List of Controlled Items (WA-LIST) ***only sets a minimum level for controls and participating States can adopt stricter control regimes***. The lists will be reviewed regularly to reflect technological developments and experience gained by participating States.[59] The participating States will control all items set forth in the WA-LIST, with the ***objective of preventing unauthorised transfers or re-transfers of those items.***[60] Most of the participating States have, at

[54] *Gladman* p. 1.
[55] One can compare WA to its predecessor COCOM, which was clearly directed against Warsaw Pact and communist countries in general.
[56] Article 51 of the Charter of the United Nations: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."
[57] *WA Public Statement for 1999 Plenary*, paragraph 9.
[58] *WA Public Statement for 1999 Plenary*, paragraph 7 mentions specifically terrorist or organised criminal groups that seek to acquire armaments and dual-use items.
[59] *Initial Elements* III.3.
[60] *Initial Elements* III.1.

least in some respect, stricter controls in place than the WA requires.[61] But those national, potentially stricter controls, should not, however, impede *bona fide* civil commerce as explained above. The WA controls are not meant to be used as a tool in enhancing national trade policy objectives and they are ill suited for it anyway, because a nation is unlikely to gain anything positive for itself if it limits its own exports. Export restrictions usually affect the economy negatively.

The WA's true objective is security and foreign policy related: ***to deny certain items or technology from certain end-users or countries***. The *non-grata* countries are not listed,[62] because the Arrangement is not directed against any State.[63] The participating States are free, enjoying their full sovereignty under international law, to decide on the countries to which they would not grant an export license. It is rare that such lists are made openly public or even drafted, with the possible exception of total or partial trade embargoes imposed by the European Union or United Nations Security Council.

It can be argued that modern technology, like encryption software, is widely used in today's military forces, and therefore the dual-use goods would possibly be even more important militarily than in the past. But also the civil use of encryption software has mushroomed, and quite rightly more than in the military setting. Truly effective civil use of encryption became possible only after developments in personal computing, whereas the military has used encryption for many decades.[64]

It can also be argued that completely defensive technology, like encryption, can thus have indirect uses in the operation of offensive weapons.[65] This is surprising, since cryptographic products are defensive in nature and exist only to protect information from unauthorised access, although this information can be used for military purposes. Although cryptographic products are in no sense weapons, they are nevertheless subject to controls under the terms of the Arrangement. Current export controls on cryptography, examined below, make no serious attempt to distinguish between products whose characteristics make them useful for offensive military applications and those intended for civil use. The reason is probably historical: civil applications of cryptography have been very limited in the past, and controls could have a wide scope wit-

[61] Countries like USA and especially France, have maintained stricter controls, in comparison to other countries. But, as stated earlier, there has been some liberalisation in controls. For situation in France see chapter 5.4.
[62] This approach was something of a defeat for the United States, which had hoped the regime would target certain "rogue" countries.
[63] *Initial Elements* I.4.
[64] The Germans had their Enigma crypto machine at the time of the Second World War, when IBM, which created the first PC in the 1970s, was not even founded.
[65] *Gladman* p. 3.

hout having any significant civil impact. However, with the growth of the Internet and the rapidly increasing interest in electronic commerce, cryptographic export controls have come to apply to products of great importance to civil commerce. This raises a serious question about the compatibility of current export controls with the objectives of the Wassenaar Arrangement under which they are apparently justified.[66] It is therefore necessary to consider the wider objectives which such controls may be thought to serve. In support of a more liberal approach a notable U.S. study also presented a very significant conclusion: ***"the advantages of more widespread use of cryptography outweigh the disadvantages"***.[67] Probably only one country in the world, the United States, has a domestic market that can justify the levels of investment needed, and even in the U.S. it is evident that the inability to freely exploit international markets causes much concern in industry.[68]

Since COCOM, member States have been arguing about the dangers of exporting certain dual-use products. This is also the case with encryption commodities.[69] One of the basic difficulties is, that export of arms (defence-related material) is based on different interests, than export of dual-use products.[70] One of the basic facts to be recognized is that WA controls are in practice directed to certain few risk countries or regions which cause security concerns. The Finnish Government gives for example the Middle East or a particular country there, which causes security concerns to the international community at large.[71] Also certain countries in South Asia and countries like North Korea or Libya are countries which cause concern. It is known or suspected that a country or countries in those areas have WMD or ballistic missile programmes. Therefore WA is directed especially to exports of sensitive or strategic items, i.e. heavy weapons or machines or equipment capable of producing weapons.[72]

3.4 Wassenaar Arrangement Co-operative Procedures Pursuant to Initial Elements

3.4.1 Participation, Meetings and Administration

Representatives of the participating States meet regularly, at least once a year[73], to discuss the workings of the Arrangement and to update Control Lists if needed. A Secretariat has been established for administrative purposes.[74] But what is important to note, is the decision-making

[66] See paragraph 1 of this chapter.
[67] *Cryptography's Role in Securing the Information Society*, Executive Summary, Future Trends.
[68] *Strategic Export Controls: The Impact On Cryptography* p. 11.
[69] *Cryptography's Role in Securing the Information Society*, Appendix G.3.
[70] HE 69/1996 vp, chapter 1.2.5.
[71] *Ibid.* This is of course an euphemism for Iraq, which is at present under a United Nations Security Council trade embargo.
[72] HE 69/1996 vp, chapter 1.2.1. and 1.2.5.
[73] *Initial Elements* VII.2. Next plenary will be held in Bratislava, Slovakia in November/December 2000. The agenda for this meeting is at present unknown.
[74] *Initial Elements* VII.4. The Wassenaar Secretariat is in Vienna, Austria.

principle in the framework of the Arrangement: ***all decisions will be reached by consensus of the participating States***,[75] i.e. decisions must be unanimous.

The Arrangement will be open, on a global and non-discriminatory basis, to prospective adherent countries, that comply with the agreed export control criteria. To be admitted to the Arrangement, a country must: 1) be a producer and/or exporter of arms or dual-use industrial equipment; 2) maintain non-proliferation policies and appropriate national policies, including adherence to international non-proliferation regimes and treaties; and 3) maintain fully effective export controls.[76] Although the Arrangement does not provide for observer status, an outreach policy is being planned to inform non-member countries about WA objectives and activities and encourage such non-members to adopt WA-compliant national policies on the export of conventional arms and dual-use technologies, including cryptography. Admission of new participants will be based on consensus.

The information exchanged within the framework of Wassenaar Arrangement will remain confidential and be treated as privileged diplomatic communications. This confidentiality will extend to any use made of the information and any discussion among participating States.[77] There is a legitimate interest in securing the sensitive and sometimes difficult negotiations by asserting some confidentiality. However, for the sake of greater transparency it is not very pleasing to note that this transparency does not extend to citizen or NGO level, because of the confidential nature of WA. Freedom of information, or the right to access government documents has been guaranteed to legal and natural persons in the European Community law[78] and in the legal systems of most WA participating States.[79] Because of this there should be little doubt that this *publicity principle* should also be adopted to the rules of the intergovernmental organizations, in which the governments take part. The *openness* of also intergovernmental organizations should be quite obvious now in the 21st century in the era of globalization, when decisions which directly affect peoples lives are often originally drafted in some decision-making body of some intergovernmental organization.

[75] *Initial Elements* VII.5.
[76] *Initial Elements*, Appendix 4.
[77] *Initial Elements* IX.
[78] *Eurooppaoikeus 2000* pp. 224-225. Relevant statute in Community law is first of all Article 255 of the EC Treaty (amended by the Amsterdam Treaty), which guarentees public access to Community documents. A regulation on access to Community documents is also under way (COM (2000) 30 final, 26. 1.2000). The Rules of Procedure of the Council, Commission and Parliament also regulate access to documents. For the Council of Europe there is also Article 255 (3) of the EC Treaty and a case before ECJ (Case T-194/94, *Carvel*, 1995, p. II-2765).
[79] *Inter alia* Finnish Constitution Section 12.2 guarantees *the publicity principle* of official documents.

3.4.2 Procedures for the Information Exchange

The information exchange is one of the most important functions in the WA. Participating States will exchange information on a voluntary basis on arms transfers, as well as on sensitive dual-use goods and technologies.[80] This information exchange does not prevent information requests through normal diplomatic channels.[81]

The effectiveness of information exchange will most likely decide the effectiveness of the whole global control regime. Major differences between WA participating States export controls will quite obviously render the whole regime ineffective. Only by keeping the Control Lists up to date and pursuing fast and efficient communications practices among participant countries can the regime be effective. The information exchange under WA overlaps with the European Union's information exchange under DUR.[82] This is obviously the situation with only those 15 WA -countries which form the European Union.

The information exchange covers transfers and denials of export of the controlled items. The participating States also regularly exchange their export statistics.[83] One of the main purposes for this is to foster mutual transparency and understanding among participants.[84] The notifications apply also to all non-participating States.[85] Participating States will notify licenses denied to non-participants with respect to items on the WA-LIST, where the reasons for denial are relevant to the purposes of the arrangement.[86] It is for individual participating State to decide in which denial situation the reasons for denial are relevant enough. In the abcence of further guidelines it can be added that these reasons can be linked *inter alia* to purpose of the end use, identity of the end-user or situation in country or region of final destination.

As stated earlier,[87] it is at each participating State's discretion, how it sees fit to implement WA controls. Therefore, for example, notification of denial under information exchange of a denial of license will not impose an obligation on other participating States to deny similar transfers.[88] However, a participating State will notify all other participating States – on an early and timely basis, preferably within 30 days, but no later than within 60 days - of an approval of a license which has been denied by another participating State for an "essentially identical transaction"

[80] *Initial elements* IV.1.
[81] *Initial elements* V.6.
[82] Community's export regime is covered in chapter 4.
[83] *Kryptopolitik* p. 80.
[84] See *Initial Elements* I.
[85] *Initial Elements* II.4.
[86] *Initial Elements* V.1.
[87] Chapter 3.2.
[88] *Initial Elements* II.4.

during the last three years.[89] Provided that information exchange works well, one might assume that it should be relatively easy to discover ”essentially identical transactions” after the license has been granted.

Denial notifications are the core of the information exchange under WA.[90] They are similar to ”Wanted” posters of the Wild West. In this milieu they are not hanging on the saloon door, but they appear in the computer systems of the national export authority. A virtual warning flag rises when the authority approves a previously denied similar export, and then, no later than 60 days of the approval, other WA countries' export authorities should have received the approval notification. The *ratio* of the approval notification procedure of WA, is that other WA countries are aware that transfer, which may endanger their national interests, is in progress. The country or countries in question may then take steps to control the damage or possible damage inflicted on their national interests. These steps can include diplomatic negotiations or other course of action towards the exporting country or country of final destination.[91] In future, on the basis of *inter alia* WA's information exchange procedure, further assimilation of the participating States' export control regimes may occur. At least assimilation is one of the WA's main objectives.[92]

Many have argued that notification does not impose effective controls on the international transfer of technology. For instance, by the time one country learns that another country plans to allow a transfer that the first country denied, the transfer may already be complete.[93] As stated earlier, notifications do not impose responsibility on another WA country to deny similar transfers, but the effectiveness of Wassenaar depends on whether member States undercut or support other States' export denial. For this reason, some have argued that member countries should interpret Wassenaar as imposing a ”no undercutting rule” which would require member States at least to consult with other member countries before disregarding a notification of denial.[94] This would be prudent as far as common intrests of WA-countries are concerned, because consultation could make ”license shopping” harder.

According to *Initial Elements* section III. paragraph 2 some items in the WA-LIST are classified as sensitive (Tier 1) and very sensitive (Tier 2). It has been agreed that for those items, more

[89] *Ibid.*
[90] ”... notification is the central provision of Wassenaar.” *Baker-Hurst* p. 75.
[91] This subject can not be examined further here.
[92] *Initial Elements* II.2.: ”... participating States will assist in developing common understanding of the risks associated with the transfer of these items [sensitive dual-use goods and technologies]. On the basis of this information they will assess the scope for co-ordinating national control policies to combat these risks.”
[93] *Baker-Hurst* p. 75.
[94] *Baker-Hurst* p. 76.

stringent information exchange procedures should be used.[95] However, no information security items have been listed in Tier 1 or Tier 2. Therefore those procedures will not be discussed here.

3.5 Relevant Provisions of Wassenaar Arrangement Affecting Encryption Software Transfers

The WA-LIST is at present 188 pages long and covers thousands of items and methods which fall under its control.[96] It lists dual-use items in nine categories[97] and munitions in 22 item categories. It also has two annexes for sensitive (Tier 1) and very sensitive (Tier 2) items.[98] Provisions affecting export of encryption software are Category 5 Part 2 ”Information Security” and General Software and Technology Notes (GSN & GTN). When examining those parts of the WA-LIST one can discover what kind of encryption software falls within the domain of WA export controls. These parts of the WA-LIST will be examined in detail in this chapter of the thesis.[99]

The importance of properly understanding WA-LIST provisions is paramount, because dual-use item provisions of the EU’s control regime are directly copied from the WA-LIST and in the EU-region national control lists, being not completely harmonised, differ usually only little from WA-LIST. The provisions of WA-LIST are obviously quite technical, and therefore their interpretation requires some degree of technical expertise. However, one can find portions from the WA-LIST, which beg interpretation like any other statute. Purely technical facts are covered briefly in this study, and focus is directed to legal analysis. For a lawyer the Arrangement provides very few *travaux préparatoires*. A partial reason for this is, of course, the confidential nature of the Arrangement.[100] However, especially national cryptography policies and national parliamentary documents offer some guidance in interpreting WA-LIST provisions. Still, it would be interesting to know more about positions of different countries concerning information security products.

Interpretation of WA-LIST provisions is conducted nationally, and therefore unified interpretation is not always possible and differing national interpretations occur. The Arrangement provides, however, some definitions and guidelines. If some term is not defined in WA-LIST, its common or dictionary meaning should be used in national legislation.[101] Terms which are de-

[95] *Initial Elements* III.2.
[96] Last amended 3.12.1999.
[97] The categories are: 1. Advanced Materials, 2. Materials Processing, 3. Electronics, 4. Computers, 5. Part 1. Telecommunications, 5. Part 2. ”Information Security”, 6. Sensors and ”Lasers”, 7. Navigation and Avionics, 8. Marine, 9. Propulsion.
[98] See page 18.
[99] Relevant portions of WA-LIST are in Appendix 1 of this thesis.
[100] *Initial Elements* IX. and page 16.
[101] WA-LIST p. 188.

fined are to be used in national legislation in their WA-LIST defined forms. Distinctions are to be preserved ”as far as national languages and legislation allows”.[102] Therefore a participating State can argue that its laws, for instance, do not allow some interpretation of a term to be used. Leeway to members presented here is a yet another aspect of WA’s discretionary nature. And again a country can impose, if it sees fit, stricter controls than required in WA-LIST.

3.5.1 Controlled Encryption Software Items and Related Technology According to WA-LIST Category 5 Part 2 ”Information Security” and GSN & GTN

Category 5 Part 2 of WA-LIST covers information security products and technology. The WA-LIST defines information security as all the means and functions ensuring the accessibility, confidentiality or integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. This includes cryptography, cryptanalysis, protection against compromising emanations and computer security.[103] Also a provision in GTN states that export of technology which is required for the development, production or use of items controlled in the WA-LIST is controlled. This technology remains under control even when applicable to any uncontrolled item.

Cryptography is authoritatively defined as the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use. Cryptography is limited to the transformation of information using one or more secret parameters (e.g. crypto variables) or associated key management.[104] A Technical Note adds that a secret parameter is a constant or key kept from the knowledge of others or shared only within a group.[105] This definition is not authoritative. A technical note defines cryptanalysis as follows: 'Cryptanalysis': the analysis of a cryptographic system or its inputs and outputs to derive confidential variables or sensitive data, including clear text. (ISO 7498-2-1988 (E), paragraph 3.3.18).[106] This definition is not authoritative.

The control status of information security equipment, software, systems, application specific electronic assemblies, modules, integrated circuits, components or functions is determined in Category 5, Part 2 even if they are components or electronic assemblies of other equipment.[107] Software is defined as a collection of one or more programs or microprograms fixed in any tan-

[102] *Ibid.*
[103] WA-LIST p. 171.
[104] WA-LIST p. 166.
[105] *Ibid.*
[106] WA-LIST p. 171.
[107] WA-LIST Category 5 Part 2 Note 1, p. 75.

gible medium of expression.[108] Programs are defined as a sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer.[109] Microprograms are defined as a sequence of elementary instructions maintained in special storage, the execution of which is initiated by the introduction of its reference instruction register.[110]

Electronic assemblies are defined as a number of electronic components (i.e. circuit elements, "discrete components", integrated circuits, etc.) connected together to perform (a) specific function(s), replaceable as an entity and normally capable of being disassembled.[111] Circuit elements are defined as a single active or passive functional part of an electronic circuit, such as one diode, one transistor, one resistor, one capacitor, etc.[112] Discrete components are defined as a separately packaged circuit element with its own external connections.[113]

3.5.1.1 Information Security Items relaxed from controls

3.5.1.1.1 General Software Note (GSN)

The WA-LIST contains General Software Note (GSN), which is intended to restrict the field of control lists in the domain of computer software.[114] Only the Entry 2 of GSN is applicable to cryptographic software.[115] According to Entry 2 the WA-LIST does not control software, which is "in the public domain". This means technology or software which has been made available without restrictions upon its further dissemination.[116] Copyright restrictions do not remove technology or software from the public domain.[117] Thousands of so-called freeware programs can be downloaded from Internet and usually it can be concluded that those programs are in the public domain. Freeware is software which can be used and modified freely, usually the author only wants to be recognized and referred to as the original author. This so-called public domain software is very important, for example, to the global scientific community at large.[118]

Also so-called shareware programs are freely in circulation both on- and off-line. Shareware is software which is offered publicly and shared rather than sold. Those programs usually function for only a couple of days after the initial installation and for further use a fee must be paid in order to obtain a software patch or serial number. Alternatively shareware can in itself be fully

[108] WA-LIST p. 179.
[109] WA-LIST p. 176.
[110] WA-LIST p. 173.
[111] WA-LIST p. 168.
[112] WA-LIST p. 164.
[113] WA-LIST p. 167.
[114] WA-LIST p. 3.
[115] See Appendix 1 of this thesis.
[116] WA-LIST p. 171.
[117] *Ibid.*
[118] KK 1430/1998 vp.

functional, but additional features are provided if a fee is paid. Shareware can be circulated effectively by just putting it into the open network where prospective users can download it.

It is, however, important to recognize that the terms public domain, freeware or shareware can be interpreted differently in different jurisdictions, because the terms are not well established.[119] In 1995 the EU's security group called Senior Officials Group for Information Systems Security concluded that a program called PGP was outside WA controls.[120] PGP is a program which allows use of industry-strength cryptography to anyone with a PC. The program is freely downloadable on-line even from U.S. Internet sites since EAR liberalizations.[121] Many similar and equally effective freeware programs exist, one prominent example of which is a widely distributed program called SSH, which is used *inter alia* to secure UNIX shell accounts.

3.5.1.1.2 General Technology Note (GTN)

According to GTN Wassenaar controls do not apply to technology which is the minimum necessary for the installation, operation, maintenance (checking) and repair of items which are not controlled or whose export has been authorized.[122] Also the controls do not apply to technology in the public domain, to basic scientific research or to the minimum necessary information for patent applications.[123] Basic scientific research is authoritatively defined in WA-LIST as being "experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective".[124] Technology is authoritatively defined as specific information necessary for the development, production or use of a product. The information takes the form of technical data or technical assistance. A Technical Note also unofficially adds that technical data may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories and also that technical assistance may take forms such as instruction, skills, training, working knowledge, consulting services and may involve transfer of technical data.[125]

The situation in which a patent application exemption would come into question is when for instance a European pantent is applied for from the European Patent Office[126] or from the U.S.

[119] *Ibid.*
[120] *Kryptopolitik* p. 37.
[121] *Federal Register / Vol. 65, No. 10 / Friday, January 14, 2000 / Rules and Regulations.*
[122] WA-LIST p. 3.
[123] *Ibid.*
[124] WA-LIST p. 163.
[125] WA-LIST p. 181.
[126] Established by European Patent Convention in 1973, *Domeij* p. 11.

Patent Office. Filing the application may include cross-border technology transfer, which falls into the domain of export controls. Also, nations usually have special statutes in place for inventions which may have importance in the defence-related fields.[127]

3.5.1.1.3 Items Relaxed Pursuant to Cryptography Note

In Category 5 Part 2 information security products are classified in four different paragraphs.[128] Those are:

5. A. 2. Systems, Equipment and Components

5. B. 2. Test, Inspection and Production Equipment

5. D. 2. Software

5. E. 2. Technology

WA-LIST Category 5 Part 2 contains an important provision affecting controls on cryptographic software.[129] According to Cryptography Note systems, equipment and components (5.A.2.) and software (5.D.2.) are not controlled if they meet certain criteria. These criteria list features which classify relaxed products in the ***mass-market*** category.[130] This Cryptography Note does not extend to test, inspection and production equipment (5.B.2.) or to technology (5.E.2) transfers.[131] For those ***niche market***[132] items containing cryptographic software the requirements in the chapter Systems, Equipment and Components (5.A.2.) apply (*inter alia* symmetric keys exceeding 56 bits are controlled).[133] One has to discover if one's products fall under the Test, Inspection and Production Equipment (5.B.2.) or the Technology (5.E.2.) paragraphs. If this is the case, the Cryptography Note does not apply.

In order to be exempted from controls according to the Cryptography Note, items must generally be available to the public by being sold without restriction from stock at retail selling points, from stock by means of over-the-counter transactions, mail order transactions, electronic transactions or telephone call transactions.[134] The requirement of items being generally available to the public means that sales cannot be restricted to a few key customers - anybody must be able, in compliance with national law, to enter the seller's premises and buy the item or order it from the seller.

---

[127] In Finland we have statute called Laki maanpuolustukselle merkityksellisistä keksinnöistä (551/1967), it covers inventions which can be used by defence forces.
[128] WA-LIST pp. 75-78.
[129] WA-LIST Cat. 5 Part 2 Note 3, p. 75.
[130] *Arjen-Lenstra 1999* p. 5.
[131] WA-LIST Cat. 5 Part 2 Note 3, p. 75.
[132] *Ibid.*
[133] See page 27.
[134] WA-LIST Cat. 5 Part 2 Note 3 a., p. 75.

According to *Ramberg*, in international trade sales can be divided into three different main types, namely sales where goods are made available to the buyer at the seller's premises, sales where the seller undertakes to hand over the goods for carriage to the buyer (so-called shipment contracts) and sales where the seller undertakes to carry the goods at his risk and expense to the buyer's destination (so-called destination contracts). These main types are further divided into various subcategories according to specific trade terms.[135] Over-the-counter transactions are therefore sales where goods are available at the seller's premises. Mail order, electronic or telephone call transactions can be shipment contracts or destination contracts depending on specific trade terms. In practice, sale of manufactured goods as distinguished from sale of commodities may often involve various services by the seller. This is particularly common when the contract of sale concerns high technology products.[136] Those services may be deemed technology transfers falling within the domain of export controls.

The Cryptography Note also requires that the cryptographic functionality may not easily be changed by the user.[137] National interpretations may vary, but generally it can be concluded that 'easily' means that, if an average computer user can change the functionality of a program completely, the functionality can be deemed to be easily changeable. Of course the concept of 'easily changeable cryptographic functionality' is also related to the application or program in use. An average user is a person who has not received formal or substantial informal education or experience in - for instance - computer science, software engineering, cryptography, physics or mathemathics. For instance, holders of computer science PhDs, engineers or computer hackers are not average users.

Also, according to the Cryptography Note, an item eligible to be relaxed has to be designed to be installed by the user without further substantial support by the supplier.[138] It can be difficult to judge what kind of action constitutes a 'substantial support', but again some general observations can be made. If for instance, the supplier's employee installs, configures or does both, or gives step by step instructions by phone, the action may usually be deemed as substantial support. As a rule of thumb, a user, again not schooled in computing, should be able to install and configure a program by him- or herself, maybe referring to manuals, read-me files or other instructions provided by the supplier in product documentation.

[135] *Ramberg* p. 38.
[136] *Ramberg* p. 39.
[137] WA-LIST Cat. 5 Part 2 Note 3 b., p. 75.
[138] WA-LIST Cat. 5 Part 2 Note 3 c., p. 75.

The Cryptography Note states that the vendor or exporter must be ready when the national export authority, usually the respective ministry of trade and industry, requests details of the items. The national authority must be able to ascertain compliance with the above conditions.[139] This provision aims to enhance the national authorities' knowledge of the activities of its private sector. According to a U.S. Government Report it is important that authorities know fully the product's internal operations, in order to be aware of latest developments in cryptography technology.[140] Then they may choose the best course of action possible. Obviously this is ample evidence of the fact that governments around the world are adapting the gatekeeper model of controls to a surveillance model.[141]

If items contain ***symmetric cryptographic algorithms the key length may not exceed 64 bits*** in order to be relaxed by the Cryptography Note.[142] As stated earlier, this applies only to Systems, Equipment and Components (5.A.2.) and to Software (5.D.2.). This does not apply to Test, Inspection and Production Equipment (5.B.2.) and to Technology (5.E.2.). In those paragraphs software is controlled if the key length of symmetric algorithms exceeds 56 bits. For asymmetric algorithms see chapter 3.5.1.2.2.

It can be asked why the critical key length was agreed in Wassenaar as being exactly 64 bits. Some guidance to this question is provided in a U.S. National Science Council Report: "Senior Administration officials have said that the limitation to 64 bits is a way of hedging against the possibility of finding easily proliferated ways to break the escrow binding built into software, with the result that U.S. software products without effective key escrow would become available worldwide."[143] So one of the objectives has been the promotion of widespread key escrow systems. The report dates from 1996, and at that time key escrow debate was going on, nowadays this debate has quietly died as proponents of statutory (i.e. mandatory) key escrow have became fewer. The same report also gives another possible reason for the 64-bit limit: "The 64-bit limit is there because we might have a chance of dealing with a breakdown of software key escrow 10 to 15 years down the line; but if the key length implied a work factor of something like triple-DES, we would never be able to do it."[144] So here again, the reason seems to be the

[139] WA-LIST Cat. 5 Part 2 Note 3 e., p. 75.
[140] *Cryptography's Role in Securing the Information Society*, Recommendation 4.1., para 5. In the same paragraph it was stated: "These requirements have two purposes. First, they would enable the U.S. government to validate that the product complies with all of the conditions required for export jurisdiction under the CCL (Commerce Control List). Second, they would allow more cost-effective use of intelligence budgets for understanding the design of exported cryptographic systems."
[141] See Preface to this thesis.
[142] WA-LIST Cat. 5 Part 2 Note 3 d., p. 75. Also Technical Note adds that parity bits are not included in the key length.
[143] *Cryptography's Role in Securing the Information Society*, chapter 5.13.2 para 1.
[144] *Ibid*.

promotion of key escrow and in general limiting the global usage of strong unbreakable encryption. The same report, however, states also that the 64-bit limit also has weaknesses: "... the 64-bit limit is easily circumvented by multiple encryption under some circumstances. Specifically, consider a stand-alone security-specific product for file encryption that is based on DES and is escrowed. ... But disassembly of the object code of the program (to defeat the escrow binding) may also reveal the code for DES encryption in the product. Once the source code for the DES encryption is available, it is a technically straightforward exercise to implement a package that will use the product to implement a triple-DES encryption on a file."[145]

The Cryptography Note as it applies to Software (5.D.2.) is valid until December 3. 2000.[146] Renewal for a successive period will require the unanimous consent of participating countries (a sunset clause[147]).

3.5.1.1.4 Products Accompanying User for the User's Personal Use

Information security products are not controlled if they accompany their user for the user's personal use[148], for instance, if a laptop computer containing cryptographic software is taken on a business trip with its user.[149] However, interpretations of this may vary from country to country. Some countries may even disregard this provision.

3.5.1.2 Controlled Software, Software in Systems, Equipment and Components, Software in Test, Inspection and Production Equipment and Controlled Software Technology

Category 5 Part 2 lists controlled systems, equipment, application-specific electronic assemblies, modules and integrated circuits for information security.[150] Also controlled are other specially designed components therefor which are designed or modified to use cryptography employing digital techniques performing any cryptographic function.[151] This includes equipment designed or modified to use cryptography employing analogue principles when implemented with digital techniques.[152]

Equipment specially designed for the development of equipment or which includes functions of controlled equipment are controlled by Category 5 Part 2.[153] This includes measuring, test, repair or production equipment or controlled functions. Measuring equipment specially designed

[145] *Cryptography's Role in Securing the Information Society*, chapter 5.13.2 para 2.
[146] WA-LIST Statements of Understanding and Validity Notes, Category 5 Part 2, p. 187.
[147] *Koops 2000* chapter 1.
[148] WA-LIST Cat. 5 Part 2 Note 2, p. 75.
[149] Kryptopolitik pp. 26 and 80.
[150] WA-LIST 5.A.2. p. 75.
[151] WA-LIST 5.A.2.a.1.
[152] Note to WA-LIST 5.A.2.a.1.
[153] WA-LIST 5.B.2., p. 78.

to evaluate and validate the information security functions is controlled by the Systems, Equipment and Components (5.A.2) or Software (5.D.2) paragraphs.

Development is authoritatively defined as being related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts.[154] Production is authoritatively defined as meaning all production stages, such as: product engineering, manufacture, integration, assembly (mounting), inspection, testing and quality assurance.[155]

Software specially designed or modified for the development, production or use of equipment or software is controlled by Category 5 Part 2.[156] Software specially designed or modified to support technology[157] is controlled under Category 5 Part 2 paragraph Technology (5.E.2). Specific software,[158] such as software having the characteristics or performing or simulating the functions of the equipment[159] or used to certify[160] software thereof is controlled. The specific software is controlled only if it is related to equipment listed by paragraphs Systems, Equipment and Components (5.A.2) or Test, Inspection and Production Equipment (5.B.2).[161]

Use is authoritatively defined as operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing.[162] However, software is not controlled if software is required to use equipment or provide any functions of equipment, which is excluded from controls in chapter 5.A.2.[163] (for example personal smart cards). Software technology is controlled according to the paragraph Technology (5.E.2) and GTN for the development, production or use of equipment or software controlled by Category 5 Part 2.[164]

3.5.1.2.1 Symmetric Algorithms

A symmetric algorithm employing a ***key length in excess of 56 bits is controlled***.[165] Symmetric algorithm is authoritatively defined as a cryptographic algorithm using an identical key for both encryption and decryption.[166] A Technical Note also unofficially adds, that a common use of

[154] WA-LIST p. 166.
[155] WA-LIST p. 176.
[156] WA-LIST 5.D.2.a., p. 78.
[157] WA-LIST 5.D.2.b., p. 78.
[158] WA-LIST 5.D.2.c, p. 78.
[159] WA-LIST 5.D.2.c.1., p. 78.
[160] WA-LIST 5.D.2.c.2., p. 78.
[161] WA-LIST 5.D.2.c.1., p. 78.
[162] WA-LIST p. 182.
[163] Note to 5.D.2., p. 78.
[164] WA-LIST 5.E.2., p. 78.
[165] WA-LIST 5.A.2.a.1.a., p. 76.
[166] WA-LIST p. 181.

symmetric algorithms is confidentiality of data.[167] If the item in which this algorithm is used fills the requirements of the Cryptography Note, *inter alia* being a mass market item, the limit is 64 bits according to the Cryptography Note. According to the Statement of Understanding in WA-LIST Governments of participating States agree to review this parameter in conjunction with the review of the Cryptography Note, not later than 3 December 2000.[168]

The U.S. influence has been strong also here, because the limit to 56 bits here is exactly what was recommended in a U.S. Government Report back in 1996.[169] The key limit of 56 bits was originally a relaxation from much smaller key size. In the Report it was argued that key sizes must be raised in order to maintain U.S. global market leadership[170] and to allow U.S. multinational corporations to use more secure methods of communication and computing,[171] so that they can defend against *inter alia* economic espionage conducted by business rivals and foreign governments. When these facts are reviewed from a European perspective it seems rather evident that the U.S. has been calling the shots in the Wassenaar Arrangement right from the start. Because the U.S. naturally primarily defends its national interests first, like any other country, the U.S. dominance can have adverse effects on European businesses.

3.5.1.2.2 Asymmetric Algorithms

Asymmetric algorithm is authoritatively defined as a cryptographic algorithm using different, mathematically-related keys for encryption and decryption.[172] A Technical Note also unofficially adds that a common use of asymmetric algorithms is key management.[173] According to the Statement of Understanding in WA-LIST, Governments of participating States agree to review this parameter in conjunction with the review of the Cryptography Note, not later than 3 December 2000.[174]

---

[167] *Ibid.*
[168] WA-LIST p. 187.
[169] *Cryptography's Role in Securing the Information Society*, Recommendation 4.1, para 2: "Products providing confidentiality at a level that meets most general commercial requirements should be easily exportable. Today, products with encryption capabilities that incorporate the 56-bit DES algorithm provide this level of confidentiality and should be easily exportable. A collateral requirement for products covered under Recommendation 4.1 is that a product would have to be designed so as to preclude its repeated use ***to increase confidentiality beyond the acceptable level*** (i.e., today, it would be designed to prevent the use of triple-DES)." (emphasis added).
[170] *Cryptography's Role in Securing the Information Society*, Recommendation 4.1, para 9: "Relaxation of export controls in the manner described in Recommendation 4.1 will help the United States to maintain its worldwide market leadership in products with encryption capabilities."
[171] *Cryptography's Role in Securing the Information Society*, Recommendation 4.1, para 8: "The ability to use 56-bit DES abroad will significantly enhance the confidentiality available to U.S. multinational corporations conducting business overseas with foreign partners, suppliers, and customers..."
[172] WA-LIST p. 162.
[173] *Ibid.*
[174] WA-LIST Statement of Understanding and Validity Notes, Category 5 Part 2, Statement of Understanding, p. 187.

3.5.1.2.2.1 Classical Asymmetric Systems

An asymmetric algorithm is controlled, when the security of the algorithm is based on factorisation of integers in excess of 512 bits (e.g., RSA).[175] Also other classical asymmetric systems exist, of which the most notable are the Diffie-Hellman scheme and ElGamal.[176] Both the maximal RSA modulus size and the maximal field size allowed are 512 bits. Subgroup discrete logarithm (SDL) systems are like traditional discrete logarithm systems. The maximum SDL field size allowed is 512 bits – there is no maximum allowed key size. A popular subgroup size is 160 bits. That choice is used in the US Digital Signature Algorithm, with field sizes varying from 512 to 1024 bits.[177]

3.5.1.2.2.1.1 Discrete Logarithms (DLs) in a Multiplicative Group

One type of cryptographic asymmetric algorithms are discrete logarithms, in which computation discrete of logarithms in a multiplicative group occur in a finite field (e.g. Diffie-Hellman over Z/pZ). This kind of algorithms are ***controlled if finite field size is greater than 512 bits***.[178]

3.5.1.2.2.1.2 Elliptic Curve Systems

An asymmetric algorithm is controlled, when a group of discrete logarithms, ***other than*** computation of discrete logarithms in a multiplicative group of a finite field (e.g. Diffie-Hellman over Z/pZ stated above), is in excess of 112 bits (e.g. Diffie-Hellman over an elliptic curve).[179] Field size is unspecified.[180] Elliptic curve systems are quite advanced:

> "Variants of the RSA and Diffie-Hellman asymmetric cryptographic systems have been proposed that use elliptic curves instead of modular multiplication as the fundamental group operation. Today the elliptic curve variants have the advantage that the best-known algorithms for cryptanalyzing them have computational requirements that grow exponentially in the size of the modulus, as opposed to subexponential behavior for RSA and Diffie-Hellman. If this exponential behavior continues to hold, asymmetric cryptographic systems can have significant safety margins, comparable to those obtainable with conventional cryptographic systems, without undue economic or time cost to legitimate users. Caution is warranted, however, since the elliptic curve systems are fairly recent and therefore not nearly as well studied as RSA and Diffie-Hellman."[181]

3.5.1.2.3 Software Performing Cryptanalytic Functions

The systems, equipment and components designed or modified to perform cryptanalytic functions are controlled.[182] Technical Note defines cryptanalysis as follows: 'Cryptanalysis': the analysis of a cryptographic system or its inputs and outputs to derive confidential variables or sensitive data, including clear text. (ISO 7498-2-1988 (E), paragraph 3.3.18).[183] This definition is not authoritative.

---

[175] WA-LIST 5.A.2.a.1.a.1., p. 76.
[176] *Arjen-Lenstra 1999* p. 6.
[177] *Arjen-Lenstra 1999* pp. 6 & 10.
[178] WA-LIST 5.A.2.a.1.a.2., p. 76.
[179] WA-LIST 5.A.2.a.1.a.3., p. 76.
[180] *Arjen-Lenstra 1999* p. 12.
[181] *Cryptography's Role in Securing the Information Society* Appendix C.6.8.
[182] WA-LIST 5.A.2.a.2., p. 76.
[183] WA-LIST p. 171.

3.5.1.2.4 Software to Reduce Compromising Emanations of Information-Bearing Systems

The systems, equipment and components specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards are controlled.[184]

3.5.1.2.5 Software for Spread Spectrum Systems Use

The systems, equipment and components designed or modified to use cryptographic techniques to generate the spreading code for spread spectrum systems, including the hopping code for frequency hopping systems are controlled.[185] Spread spectrum system is authoritatively defined as the technique whereby energy in a relatively narrow-band communication channel is spread over a much wider energy spectrum.[186] Frequency hopping system is authoritatively defined as a form of spread spectrum in which the transmission frequency of a single communication channel is made to change by a random or pseudo-random sequence of discrete steps.[187]

3.5.1.2.6 Software to Provide Multilevel Security

The systems, equipment and components designed or modified to provide certified or certifiable "multilevel security" or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) or equivalent are controlled.[188] Multilevel security is authoritatively defined as a class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.[189] A Technical Note also unofficially adds that multilevel security is computer security and not computer reliability, which deals with equipment fault prevention or human error prevention in general.[190]

3.5.1.2.7 Software to Detect Surreptitious Intrusion in Communications Cable Systems

The systems, equipment and components for communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion are controlled.[191]

---

[184] WA-LIST 5.A.2.a.4., p. 76.
[185] WA-LIST 5.A.2.a.5., p. 76.
[186] WA-LIST p. 180.
[187] WA-LIST p. 169.
[188] WA-LIST 5.A.2.a.6., p. 76.
[189] WA-LIST p. 174.
[190] *Ibid.*
[191] WA-LIST 5.A.2.a.7., p. 76.

3.5.1.2.8 Software for Decryption in Global Navigation Satellite Systems Receiving Equipment

Global navigation satellite systems (i.e. GPS or GLONASS)[192] receiving equipment containing or employing decryption are controlled under Category 7.A.5.[193]

3.5.1.3 Exemptions from Control of Software, Software in Systems, Equipment and Components, Software in Test, Inspection and Production Equipment and Controlled Software Technology

3.5.1.3.1 Exemption for Cryptography Used for Certain Authentication or Digital Signature Functions

Items are not controlled if systems, equipment and components are designed or modified to use cryptography employing digital technologies performing any cryptographic function for authentication or digital signature purposes.[194] Technical Note defines that authentication and digital signature functions include their associated key management function, authentication includes all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorised access.[195] Also cryptography does not include fixed data compression or coding techniques.[196] These definitions are not authoritative. Fixed is authoritatively defined as being the coding or compression algorithm that cannot accept externally supplied parameters (eg. cryptographic or key variables) and cannot be modified by the user.[197]

3.5.1.3.2 Restricted Audience Broadcast Equipment

Receiving equipment for radio broadcast, pay television or similar restricted audience broadcast of the consumer type, without digital encryption except that exclusively used for sending the billing or programme-related information back to the broadcast providers are relaxed from WA controls.[198]

3.5.1.3.3 Cryptographic Software Protecting IPR-rights

Equipment where the cryptographic capability is not user-accessible and which is specially designed and limited to allow execution of copy-protected software or access to any of the following: copy-protected read-only media, information stored in encrypted form on media (e.g. in connection with the protection of intellectual property rights) when the media is offered for sale

[192] GPS and GLONASS are global navigation systems, the former maintained by U.S. Department of Defence (DoD) and the latter by Government of Russian Federation.
[193] France, the Russian Federation and Ukraine view this list (only WA-LIST Category 7) as a reference list drawn up to help in the selection of dual-use goods which could contribute to the indigenous development, production or enhancement of conventional munitions capabilities. WA-LIST pp. 104-105.
[194] WA-LIST 5.A.2.a.1., p. 76.
[195] Technical Notes 1 & 2 to WA-LIST 5.A.2.a.1., p. 76.
[196] Technical Note 3 to WA-LIST 5.A.2.a.1., p. 76.
[197] WA-LIST p. 169.
[198] Note b. to 5.A.2., p. 77.

in identical sets to the public or one-time copying of copyright-protected audio or video data.[199] Therefore, for example, Digital Versatile Disks (DVDs) and their players are not subject to Wassenaar controls. They would not be controlled anyhow, because they allegedly employ encryption algorithms with only 40-bit key.[200]

3.5.1.3.4 Banking Exemption

Cryptographic equipment specially designed and limited for banking use or money transactions is relaxed from export controls.[201] A non-authoritative Technical Note adds that the concept of 'money transactions' includes the collection and settlement of fares or credit functions.[202] The banking exemption is probably the most important exemption from export controls, with public domain exemption being also equally important. It allows banks and securities and exchange-related institutions to use strong virtually impenetrable cryptography to secure money, shares, bonds or other securities and exchange-related transactions. Exemption covers machines for banking use or money transactions, such as automatic teller machines, self-service statement printers or point of sale terminals. By allowing this exemption the Arrangement tacitly recognizes cryptography's paramount importance in securing society's critical infrastructures such as banking.

In a U.S. National Science Council Report[203] the importance of secure banking practices was stressed. It stated that the flow of currency is largely digital in banking systems. Funds are transferred from account to account, from customer to vendor, from bank to bank - all without trade of tangible property. Banks and financial service institutions have had a long history of being a target of nefarious elements in society and thus traditionally have been willing to spend money on security measures (e.g. safes). This history, coupled with their dependence on information technology and their capability for networked communication among themselves, has led to a relatively high degree of concern within the banking and financial services sector for information security. Given the importance of banks in the world economy, large banks with multinational connections have needs for security that are quite stringent.

Banking is extensively international today and will become more so in the future. Moreover, it has moved relatively quickly to bring customers (both individual and institutional) on-line in an attempt to reduce costs. For these reasons, ***the banking industry may represent the leading***

[199] Note c. to 5.A.2., p. 77.
[200] DVD copy protection has been breached and nowadays it is possible to copy these disks. This breach is partly due to DVD technology using only 40-bit keys other factors were also involved.
[201] Note d. to 5.A.2., p. 77.
[202] Technical Note to 5.A.2. Note c., p. 77.
[203] *Cryptography's Role in Securing the Information Society* Appendix I.1.

edge of information security needs as far as other increasingly internationalized and electronically interconnected industries are concerned.[204] To date, losses due to electronic penetration of banking systems have been a relatively small fraction of the sums written off every year in bad loans, unrepayable debt, and the like.[205]

Given the central importance of banking systems in the EU economy, a major disruption of service in these systems could have cataclysmic consequences for global economy. Finally, customer and patron trust is at the heart of modern financial systems around the world, and such trust, once lost, is difficult to regain. Even small bank losses - if made widely known - could adversely affect customer trust in banks, and the result could be a significant and widespread loss of trust leading to enormous financial disruption and chaos.[206]

3.5.1.3.5 Exemption for Portable and Mobile Radiophones

Portable or mobile radiotelephones for civil use (e.g. for use with commercial civil cellular radiocommunications systems) that are not capable of end-to-end encryption are not controlled.[207] Therefore, for instance, GSM cellular telephony is exempted from controls, because only the wireless part of the communications is encrypted,[208] and GSM is used only in a civilian environment. GSM's encryption is so-called link encryption, in which the encryption is performed on data traffic after it leaves one of the end-users; the traffic enters one end of the link, is encrypted and transmitted, and then is decrypted upon exit from that link. Link encryption refers to the practice of encrypting information being communicated in such a way that it is encrypted only in between the node from which it is sent and the node where it is received; while the information is at the nodes themselves, it is unencrypted. In the context of link encryption for cellular communications, a cellular call would be encrypted between the mobile handset and the ground station. When carried on the landlines of the telephone network, the call would be unencrypted (GSM and DECT networks).[209]

On the other hand, end-to-end encryption involves a stream of data traffic (in one or both directions) that is encrypted by the end-users involved before it is fed into the communications link; traffic in between the end-users is never seen in plaintext, and the traffic is decrypted only upon receipt by an end-user. Link encryption is encryption performed on data traffic after it leaves

---

[204] *Ibid.*
[205] *Ibid.*
[206] *Ibid.*
[207] Note e. to 5.A.2., p. 77.
[208] *Salauspolitiikassa noudatettavat periaatteet,* para 12.
[209] *Cryptography's Role in Securing the Information Society* Box 7.4.

one of the end-users; the traffic enters one end of the link, is encrypted and transmitted, and then is decrypted upon exit from that link.[210]

Thus, for purposes of protecting sensitive information on an open network accessible to anyone (the Internet is a good example), ***link encryption is more vulnerable than end-to-end encryption***, which protects sensitive information from the moment it leaves party A to the moment it arrives at party B. However, from the standpoint of law enforcement, link encryption facilitates legally authorized intercepts, because the traffic of interest can always be obtained from one of the nodes in which the traffic is unencrypted.[211]

3.5.1.3.6 Cordless Telephony Exemption

Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (i.e. a single, unrelayed hop between terminal and home base station) is less than 400 metres, according to the manufacturer's specifications, is not controlled.[212] For instance cordless phones using DECT encryption standard are freely exportable according to WA.[213]

3.5.1.3.7 Exemption for Certain Personalized Smart Cards

Personalised smart cards meeting certain criteria are not controlled.[214] A personalised smart card is a card containing a microcircuit which has been programmed for a specific application and cannot be reprogrammed for any other application by the user.[215] If a personalised smart card has multiple functions, the control status of each function is assessed individually.[216] The card's cryptographic capability must be restricted for use in equipment or systems excluded from control under some of the following exemptions: exemption for receiving equipment for restricted audience broadcast (5.A.2 Note b.); exemption for IPR-protective cryptography (5.A.2 Note c.); exemption for banking and money transactions (5.A.2 Note d.), like bank, credit and debit cards; exemption for portable or mobile radiotelephones for civil use (5.A.2 Note e.); or exemption for cordless telephony (5.A.2 Note f.).[217]

3.5.2 The Dichotomy – Tangible and Intangible Transfers

It has been considered an inherent weakness in export controls that intangible transfers are not by law controlled in some participating States or the control is in real life situations very diffi-

[210] *Ibid.*
[211] *Ibid.*
[212] Note f. to 5.A.2., p. 77.
[213] For definitions on link and end-to-end encryption see above chapter.
[214] Note a. to 5.A.2., p. 77.
[215] WA-LIST p. 176.
[216] Note a. to 5.A.2., p. 77.
[217] *Ibid.*

cult to enforce because of the open information network's global and unrestricted nature. In the WA environment Governments are expected to excercise controls on intangible technology as far as their legislation will allow.[218] Also Governments agree that the transfer of software, for production or development of items on WA-LIST shall be treated with vigilance in accordance with national policies and the aims of the regime.[219] However, Wassenaar does not obligate member States to control intangible exports, such as downloading encryption software off the Internet; in this area national practices often differ - for instance, the U.S. has a history of controlling these transfers quite aggressively.[220]

So then, exactly what kind of transfers are to be considered intangible? First of all, intangible transfers are digital, or in transfer process digital techniques have to be employed. Intangible items do not have a physical form. The basic case of intangible transfer nowadays is when a customer goes to an exporter's website and downloads software to his computer. In the transfer process i.e. FTP- or HTTP-protocols based on TCP/IP can be used; the software can be sent as an email attachment, using a modem or even a facsimile. For instance, the source code can be sent using a fax, the transfer of items is intangible, although the recipient gets the source code in physical paper format.

Nowadays corporate or other intranets can be extended over an open network (such as Internet) to include users outside the entity's network. In these virtual private networks, which by the way are usually protected by cryptography, data are easily transmitted across borders, also intangible transfers of software or technology data is indeed very easy. Intangible transfer can even be completed using communication satellites as a relay, common usage is i.e. satellite telephones. One must note that, for instance, transfers of floppy diskettes, CD-ROMs or books containing software code are deemed to be tangible transfers, hence the physical storage medium.

As far as technology transfers are concerned, the know-how, working knowledge, education, instructions, skills, or other information on controlled technology can even be transmitted orally in the form of a scientific or other kind of presentation like a consulting service or in a meeting. This presentation can be given abroad or it can be given via telephone or video conferencing

[218] WA-LIST GTN revision (WG2 GTN TWG/WP1 Revised 2) p. 186.
[219] GSN revision NF (95) CA WP 1, WA-LIST p. 186. Also in the *WA Public Statement For 1999 Plenary* it was stated that: "Participating States recognised it is important to have comprehensive controls of listed "software" and "technology", including controls on intangible transfers. Participating States also recognised that it is important to continue deepening WA understanding of how and how much to control those transfers. In this context, participating States agreed that the possibility of taking national measures should be considered."
[220] *Baker-Hurst* pp. 74-75.

system or via some other form of correspondence. It depends on the facts of the individual case whether this kind of activity can sometimes be deemed as technology transfer controlled pursuant to WA provisions. Generally it can be concluded that in the technology transfer field the defining of boundaries to determine whether some act is to be controlled or not is most difficult compared to other fields of controlled transfer, like pure software transfers or transfers of physical equipment.

3.5.3 Some Final Conclusions

The Arrangement does not specifically define exactly what kind of export control regimes participating States should uphold, it merely states that export controls should be fully effective[221] and pursued vigorously.[222] The Arrangement does not include provision of different types of licenses, they are left to be defined by participating States. The relevant provisions in WA concern notifications and information exchange in general and management and upholding of the WA-LIST. A member Government can approach another member Government formally or informally if they are concerned, for instance, about the activities of some foreign national in his native country.[223]

Programs using symmetric keys under 56 bits (in some cases 64 bits)[224] and asymmetric keys under 512 bit are not controlled by WA. They are freely exportable and license-free according to WA-LIST. The only thing is that prospective buyers resent using such weak encryption methods. Due to the nature of the Wassenaar Arrangement, it is not surprising that it turns out that these key sizes do not provide for adequate protection of the majority of commercial applications.[225]

Usually prospective end-users are sophisticated enough to know that weak encryption is breached with relative ease and modest costs. Quite a few academic studies have been published to show this, and they demonstrate this clearly. Also, for example, the Finnish Government's information security recommendation suggests that a symmetric key of at least 128 bits should be used in government computer systems.[226]

The fact that weak encryption methods are license-free, does not mean much, because there is no real market demand for weak crypto products***. They are economically insignificant as an***

[221] *Initial Elements*, Appendix 4.
[222] WA-LIST p. 186.
[223] *Cryptography's Role in Securing the Information Society*, Part II, Chapter 4.
[224] WA-LIST 5.2 *"Information Security"* Note 3 (Cryptography Note) and WA-LIST 5.A.2.a.1.a. & WA-LIST 5.A.2.a.1.b., pp. 75-76.
[225] *Lenstra-Verheul 1999* p. 4.
[226] *Valtion etätyön tietoturvallisuussuositus* chapter 2.5.

information security products. It can therefore be concluded that the only relevant control exemptions are GSN, banking or other exemptions provided for in the WA-LIST, but not the Cryptography Note.

4 EXPORT CONTROL LAWS IN THE EUROPEAN UNION

4.1 Introduction into the Community's Legal Activity in the Domain of Export Controls

Like export controls everywhere, export controls in the European Union are in a constant state of flux. The Dual-Use Regulation 3381/94 (EC) (hereinafter referred to as DUR) and Dual-Use Decision 94/942/CFSP (hereinafter referred to as DUD) came into force on 1 July 1995.[227] Since then the DUD has been amended many times, and major changes to DUR, based on Commission Communication COM (98) 257 final, have been pending since 1998. Before adoption of DUR and DUD, the Court of Justice of the European Communities (ECJ) established case law in the domain of export controls with two preliminary rulings given together in 1995.[228] These rulings strengthen Community's Common Commercial Policy (CCP) in the domain of export controls.

4.2 Wassenaar Arrangement from the European Union Perspective

Member States of the European Union can conduct foreign policy freely according to Community law. However, they may not do so in disregard of their Community obligations under the EC Treaty. This is an important statement of principle which will most likely not be limited to the issue of dual-use goods.[229] Such an approach is indispensable in order to shield the *acquis communautaire* from any attempts to transfer subject-matters from Community to intergovernmental channels. Articles 1 and 2 TEU specifically stipulate that the *acquis communautaire* should be fully maintained, respected and further built upon. Article 47 TEU further states that "nothing in this Treaty shall affect the Treaties establishing the European Communities".[230] As far as Community law is concerned, Wassenaar does not have a very significant position. From a strictly legal viewpoint it does not exist since WA is not an international organization and operates only as an intergovernmental arrangement and its decisions must be implemented by national legislation.[231]

Controls are seen in Community law as national measures, because WA controls are implemented on a discretionary and national basis.[232] Since the WA commitments are observed only informally by the Member States, no obligation in international law arising out of a convention

---

[227] Joint action procedure ,TEU Article 13, was used to great effect in drawing up and publishing the control lists in DUD relating to EU DUR, *Cornish* p. 77.
[228] These cases were C-70/94 *Werner* and C-83/94 *Leifer*.
[229] *Govaere* p. 1031.
[230] *Ibid.*
[231] Some arguments in this chapter are from the COCOM era, but in the view of the author of this thesis, those arguments can be used *mutatis mutandis* because the WA, is if possible, even more informal in nature than COCOM was. In COCOM States had, for instance, *right of veto* to other States' licensing decisions. This is not the case with WA. See chapter 3.
[232] Report for the Hearing, Case C-367/89, *Criminal proceedings against Aimé Richardt and Les Accessoires Scientifiques SNC*, ECR 1989, I-4626, para 20.

or other rule of law binds the Member States in that connection.[233] It must also be kept in mind that political considerations are not alien to WA, or subsequently to the national implementation measures. Export restrictions can be imposed by way of retaliation against a third State rather than to safeguard the security of the participating States of WA.[234] The basis of WA is an informal one and its decisions have to be implemented by the participating States in order to take effect in national law. The need to implement legislation means that the classes of products which are subject to export restrictions in different participating States might not coincide precisely at a given moment.[235] Although, since adoption of DUR, this possibility of differing national lists exists and it can lead to problems, especially in intra-Community transfers.

The fundamental question as far as export controls on strategic dual-use products are concerned, is *delimitation of competences between the Community and the Member States*. The answer to this question bears upon the extent to which WA rules can jeopardize both the proper functioning of the internal market and the CCP.[236] Controls agreed in the WA framework are subject to judicial review by the ECJ. The ECJ can examine whether national measures are compatible with DUR's provisions and whether they possibly breach the CCP and, if they do, whether they can be justified under Export Regulation Article 11 and the Community's *proportionality principle*.[237]

It can hardly be maintained that WA has primacy over the Community legal order and that therefore national measures taken to give effect to those decisions should fall outside the scope of judicial review by the European Court of Justice. At the time of COCOM, the status of dual-use goods was still mainly determined by it, thus implicitly raising questions about the possible effect of the latter in the Community legal order.[238] Nowadays in this respect the legal situation is clear, because the Community has adopted DUR. The question arises whether the WA commitments could be qualified as "obligations accepted for the purpose of maintaining peace and international security", so as to benefit from the room for derogation given by Article 297 EC. That does not seem to be the case. The WA is not a genuine international organization, and WA members have never agreed to any binding obligations under international law. From a legal point of view, WA hardly exists, and export controls carried out in the WA framework have to be considered as purely national measures.[239] Furthermore, WA decisions are not legally bin-

[233] Report for the Hearing, Case C-367/89 *Richardt*, I-4627, para 25.
[234] *Controlling East-West Trade and Technology Transfer* pp. 417-441. As an example, author of this text cited Siberian pipeline affair, which occurred in the early 1980s.
[235] Opinion of AG *Jacobs*, Case C-367/89 *Richardt*, I-4638, para 12.
[236] *Eeckhout-Govaere* p. 944.
[237] See chapters 4.3.2.1. and 4.3.2.3.
[238] *Eeckhout-Govaere* pp. 941-943 & 950.
[239] *Eeckhout-Govaere* p. 956.

ding on the Member States. Therefore the WA does not come under the scope of Article 297 of the Treaty.[240] The Commission had argued that the WA is of an informal nature and that, consequently, there were no obligations in the sense of Article 297 resulting from it.[241] Also in the Commission's view WA controls are not obligations which the Member States have 'accepted' within the meaning of Article 297 of the EEC Treaty.[242]

Article 296 allows a Member State to derogate from the EC Treaty, when it is necessary to secure its vital security interests in production or trade in defence-related items. Like Article 297 EC, this Article is by nature wholly exceptional. According to *Eeckhout-Govaere*, there can be little doubt that the WA list of dual-use goods is not covered by this provision.[243] Those goods are certainly not arms or munitions; neither are they war material, since they are by their very nature goods produced for civilian application, but which could be adapted and used for military purposes.

4.3 Relevant Acquis Communautaire

4.3.1 European Community's Common Commercial Policy

The question of strategic export controls is one of the most interesting issues in the sphere of common commercial policy.[244] The CCP is one of the most fundamental instruments on which the Community is based. In ECJ case law[245] it has been established, that since full responsibility for commercial policy has been transferred to the Community by Article 133 EC, national measures of commercial policy, like export controls, were permissible only if they were specifically authorized by the Community.[246] The basic question is obviously one of competence: what is the division of powers between the Community and the Member States concerning controls on exports to third countries of goods considered to be of a strategic nature?[247]

Article 133(1) EC

> 1. The common commercial policy shall be based on uniform principles, particularly in regard to changes in tariff rates, the conclusion of tariff and trade agreements, the achievement of uniformity in measures of liberalisation, export policy and measures to protect trade such as those to be taken in the event of dumping or subsidies.

The common commercial policy, as an indispensable aspect of the customs union on which the Community is based, is no less vital for the functioning of the Community than the Treaty provisions on the internal market. It will be obvious that restrictions imposed by Member States on

[240] *Hunnings*, section 4.
[241] Report for the Hearing, *Richardt* C-367/89, I-4627, para 25; and *Eeckhout-Govaere* p. 955.
[242] Report for the Hearing, *Richardt* C-367/89. See also chapter 4.3.2.4.
[243] *Eeckhout-Govaere* p. 956.
[244] *Emiliou* p. 68.
[245] Case 41/76 *Donckerwolke*, para 32; Case 174/84 *Bulk Oil*, para 31.
[246] Judgments in Case 41/76 *Donckerwolke v Procureur de la République* ECR 1976, p. 1921, para 32, and Case 174/84 *Bulk Oil v Sun International* ECR 1986, p. 559, para 31.
[247] *Eeckhout-Govaere* p. 955.

exports to non-Member States are liable to affect intra-Community trade, as for example where the goods transit through another Member State. The fact that the Treaty itself does not lay down the basic rules of the common commercial policy does not mean there are no such basic rules. In the field of export policy the basic rule is contained in the Export Regulation: ***exports from the Community shall be free***.[248]

The concept of the common commercial policy provided for in Article 133 EC must not be interpreted restrictively, so as to avoid disturbances in intra-Community trade by reason of the disparities to which a narrow interpretation of that policy would give rise in certain sectors of economic relations with non-member countries.[249] Article 133 of the EC Treaty is to be interpreted as meaning that rules restricting exports of dual-use goods to non-member countries fall within the scope of that article and that in this matter the Community has exclusive competence, which therefore excludes the competence of the Member States save where the Community grants them specific authorization.[250] A Member State may not restrict the scope of Article 133 EC by freely deciding, in the light of its own foreign policy or security requirements, whether or not a measure is covered by it.[251]

Export policies might affect the internal management of the single market, where a large proportion of internal trade is in goods which could be classified as dual-use. The single market requires there to be no internal barriers or idiosyncratic export control systems which might make way for unfair competitive advantage. However, much as they accepted the EC's CCP, if Member States were adamant in their wish to control traffic in dual-use technology on grounds of national security, the result could be anti-competitive practices where the civilian use of the technology or commodity was concerned. If controlled dual-use items could not be traded freely within the EC, without the delays and costs associated with the obtaining of licenses, it would represent a significant barrier to civil trade.[252] Dual-use items listed in DUD, Annex IV, *inter alia* ***all significant cryptographic products***,[253] are still subject to licensing in intra-Community transfers. The situation is not at all satisfactory at present, when the provisions in Article 29 EC reads as follows: "Quantitative restrictions on exports, and all measures having equivalent effect, shall be prohibited between Member States."

[248] Opinion of AG *Jacobs*, Cases *Werner* C-70/94 and *Leifer* C-83/94, ECR 1995, I-3205-3206, para 38.
[249] Summary of the Judgment, *Leifer* C-83/94, I-3232 para 1.
[250] *Leifer*, C-83/94, I-3253-3254 para 1.
[251] ECJ Case C-70/91, para 11.
[252] *Cornish* p. 83.
[253] See chapter 4.4.3.

The conduct of commercial policy, needless to say, is indeed an exclusive Community competence.[254] The ECJ stated in its opinion of 11 November 1975:[255]

> "It cannot be accepted that in a field covered by export policy and more generally by the Common Commercial Policy, the Member States should exercise a power concurrent to that of the Community, in the Community sphere and in the international sphere... To accept that the contrary were true would amount to recognizing that, in relations with third countries, Member States may adopt positions which differ from those which the Community intends to adopt, and would thereby distort the institutional framework, call into question the mutual trust within the Community and prevent the latter from fulfilling its task in the defence of the common interest."

The ECJ has also stated in its opinion of 4 October 1979:[256] "... the fact that a product may have a political importance ... is not a reason for excluding that product from the domain of the Common Commercial Policy." Implementation of such a Common Commercial Policy requires a non-restrictive interpretation of that concept, so as to avoid disturbances in intra-Community trade by reason of the disparities which would then exist in certain sectors of economic relations with non-member countries.[257]

CCP requires that a Member State should not be able to restrict its scope by freely deciding in the light of its own foreign policy or security requirements, whether the measure is covered by Article 133 EC.[258] A national measure cannot be treated as falling outside the scope of the common commercial policy on the grounds that it has foreign policy and security objectives.[259] The Court says, in essence, that it does not suffice to point to foreign policy and security considerations in order to take a subject-matter outside the scope of the EC Treaty and, in so doing, also to shield it from judicial review.[260] Pursuant to Art. 46 TEU the Court of Justice has no jurisdiction insofar as the second pillar of the TEU, the Common Foreign and Security Policy, is concerned. Moreover, national export restrictions fly in the face of the objective of achieving a truly integrated internal market and establishing a complete common commercial policy.[261]

Under Art. 301 EC common positions and joint actions are adopted to give effect to economic sanctions decided within the framework of intergovernmental foreign and security policy co-operation. Article 133 EC is no longer used as a legal basis for such decisions.[262] Sanctions imposed by the UN Security Council are implemented at Community level by a common position under Article 12 TEU and a Council Regulation under Article 300 EC. It has been argued that

[254] Opinion 1/75, ECR 1975, 1364.
[255] Opinion 1/75, ECR 1975, 1355.
[256] Opinion 1/78, ECR 1979, 2871.
[257] *Ibid.*
[258] *Werner*, C-70/94, ECR 1995, I-3226.
[259] *Werner*, Case C-70/94, para 10.
[260] *Govaere* p. 1024.
[261] *Emiliou* p. 68.
[262] *Emiliou* p. 70.

Article 301 EC is also applicable with regard to strategic export controls.[263] Undoubtedly, strategic export controls are one way of reducing economic relations. However, such controls are not necessarily imposed as a matter of urgency.[264] In the light of the above considerations, it can be argued that Article 301 EC covers strategic export controls only to the extent that they are imposed *as a matter of urgency* following a common position or a joint action within the framework of the CFSP.[265]

Exports of dual-use goods are viewed as falling within a broadly construed CCP and hence as covered by the Community's exclusive competence. Secondly, Member States enjoy considerable discretion under the public security proviso to impose export restrictions on the basis of their foreign policy. Thirdly, in doing so they must conform with the principles of proportionality and less restrictive alternative means.[266] National authorities are, because of the vagueness of the EU legislation, able to manipulate the control system established by DUR to protect national exports and hence accommodate national concerns of an essentially economic nature. It follows that the legal protection of the individual exporter is at risk.[267] The material interdependence between DUR and DUR is so close that they cannot operate as an "integrated system" if the legal guarantees enjoyed by the former are denied to the latter. In any case, under Article 10 EC, the validity of a legal formula which seriously undermines the effectiveness of a Community instrument is questionable.[268] The rigid distinction between trade and foreign policy objectives and national and Community competence is legally problematic.[269] The ECJ put forward such an approach after *Werner* and *Leifer* that trade and foreign policy can no longer be understood as entirely distinct areas. The Court held that interdependence between trade and foreign policy precludes a rigid distinction between them.[270]

4.3.1.1 Interpretation of Article 1 of the Export Regulation 2603/69

Common Commercial Policy is implemented by Export Regulation 2603/69. The Export Regulation establishes common rules for exports.[271] In Art. 1 of said Regulation, the so-called 'Basic Principle' is set out: "The exportation of products from the [EEC] to third countries shall be free, that is to say, they shall not be subject to any quantitative restriction, with the exception of those restrictions which are applied in conformity with the provisions of this Regulation." The

[263] *Kuyper* pp. 404-405.
[264] *Emiliou* p. 70.
[265] *Emiliou* p. 70.
[266] *Koutrakos* p. 244.
[267] *Koutrakos* p. 243.
[268] *Ibid.*
[269] *Koutrakos* p. 244.
[270] *Koutrakos* p. 245.
[271] Council Regulation 2603/69 [1969] OJ L 324/25 (last amended by Council Regulation 3918/91, OJ 1991 L 372/31).

ECJ ruled in *Leifer,* that Article 1 confers on individuals rights which they may assert before the courts.[272] Before *Leifer,* in case *Bulk Oil v. Sun International* the ECJ ruled that: "The fact that no Community institution challenges the legality of a policy adopted by a Member State cannot in itself have any effect on the compatibility with Community law of a policy imposing quantitative restrictions on exports of ... to non-member countries."[273] A Member State cannot argue that the Community's inactivity implicitly means that a national measure is legal under Community law. Article 1 must be interpreted as prohibiting national measures which have the effect of precluding the export of certain categories of goods to non-Member States.[274]

The Article mentions quantitative restrictions, but not does not expressly mention measures having equivalent effect. Employing the contextual method of interpretation,[275] the Court concluded that: "A regulation based on Article [113] (present Art. 133 EC) of the Treaty, whose objective is to implement the principle of free exportation at the Community level, as stated in Article 1 of the Export Regulation, cannot exclude from its scope measures adopted by the Member States whose effect is equivalent to a quantitative restriction where their application may lead... to an export restriction."[276] The Court had already indicated that Article 1 of the Export Regulation covered not only export licenses but all measures having an equivalent effect which may lead to an export prohibition. It remains to be seen whether, in so doing, the Court intended to establish exhaustive criteria with the respect to the application of the Export Regulation or whether also other measures having equivalent effect may be held to come within its scope.[277]

In cases C-70/94, *Fritz Werner Industrie-Ausruestungen GmbH v Federal Republic of Germany* and C-83/94, *Criminal proceedings against Peter Leifer, Reinhold Otto Krauskopf and Otto Holzer,* the ECJ stated that, according to Art. 133 EC, CPP is based on uniform principles, especially when tariff rates, the conclusion of tariff and trade agreements, the achievement of uniformity in measures of liberalisation, and measures to protect trade are concerned.[278] According to the ECJ there should not exist disparities in trade relations in different sectors, which can cause disturbance to the functioning of the EU's internal market. Therefore, national rules

[272] *Leifer* C-83/94, ECR 1995, I-3255.
[273] *Bulk Oil (Zug) AG v Sun International Limited and Sun Oil Trading Company*, Case 174/84, ECR 1986, para 5 of the judgment.
[274] Opinion of AG *Jacobs*, C-367/89 *Richardt*, ECR 1989, I-4644.
[275] The Court, referring to its case law, stated: "in interpreting a provision of Community law it is necessary to consider not only its wording but also the context in which it occurs and the objectives of the rules of which it is part". See Case 292/82 *Merck* ECR 1983. 3781, para. 12; Case 337/82 *St Nicolaus Brennerei* ECR 1984. 1051, para. 10.
[276] *Emiliou* p. 71 and *Werner* C-70/94, ECR 1995, I-3226 para 22.
[277] *Govaere* p. 1033.
[278] This was also stated in *Bulk Oil (Zug) AG v Sun International Limited and Sun Oil Trading Company*, Case 174/84, ECR 1986, 559.

which are meant to deny or limit exports are subject to Art. 133 EC. For instance, export controls of dual-use items are subject to Art. 133 EC, when it is investigated whether those controls are legal under Community law. The fact that the goods in question are dual-use goods is irrelevant. The usage or quality of goods in question is irrelevant to this investigation.

The *Werner* and *Leifer* cases also bring important clarifications with respect to the scope of Article 133 EC in general and of Article 1 of the Export Regulation in particular.[279] One aspect is non-restrictive interpretation of CCP. Prior case law with respect to Article 133 EC points out that the common commercial policy is to be based on uniform principles, and is not to be interpreted restrictively, in order to avoid disturbances in intra-Community trade.[280] For the first time it is specified that neither the nature of dual-use goods nor the fact that foreign policy objectives are pursued may be successfully invoked in order to take measures outside the scope of Article 133 EC. This may seem surprising considering that, strictly speaking, competence for conducting foreign policy has not been transferred to the Community.[281]

It is important to recognize the differences between EC customs law and export control law, because export controls involve quite different policy goals from customs law. In customs matters an item which is imported outside the Community through one or more Member States, is controlled usually in the originating Member State. From the point of view of customs law item has never been imported into Member States it passes through in transit. The Community transit procedure merely aims at avoiding a succession of national customs procedures and therefore lays down a procedure which only applies to customs formalities.[282] Legal fiction applies only with regard to customs formalities which have been fulfilled in accordance with the Community Transit Regulation (222/77). In the framework of export controls such an assumption is inappropriate.[283] In order to attain their objectives, export controls have to be applied to all goods that are present on national territory, whether produced there or physically imported. In some situations these different approaches may lead to a paradoxical situation, when various competent authorities deem the same goods to be imported or not imported.

Export controls are viewed in Community law as being export restrictions, and they have to be justified and proportional in order to be legal in the Community. A licensing system, the object

[279] *Govaere* p. 1032.
[280] Opinion 1/78, 1979 ECR 2871, para 45.
[281] *Eeckhout-Govaere* p. 950-960, where a parallel is drawn with the judgment in the *Chernobyl* case, C-62/88, ECR 1990, I-1527.
[282] Ex. Council Regulation No. 222/77 2nd recital, where it is submitted that establishment of a customs union as provided in chapter 1 Title I of Part two of the Treaty lies at the basis of the Community Transit procedure. See also Case 117/88, *Trend-Moden Textilhandel.*
[283] *Eeckhout-Govaere* pp. 953.

and effect of which is to prevent all exports of certain products to certain States, must be regarded as running counter to the principle that the exportation of products from the Community should be free and fall within the prohibition of Article 1 of the regulation unless it is justified under other provisions of the regulation.[284]

The requirement to obtain a license constitutes a quantitative restriction. That finding is supported by Article XI of the General Agreement on Tariffs and Trade, which can be considered to be relevant for the purposes of interpreting a Community instrument governing international trade. That article, headed 'General Elimination of Quantitative Restrictions', refers in its first paragraph to 'prohibitions or restrictions other than duties, taxes or other charges, whether made effective through quotas, import or export licenses or other measures'.

4.3.2 Member State's Possibility to Derogate from Common Commercial Policy

4.3.2.1 Article 11 of the Export Regulation 2603/69

Where national measures fall within the prohibition contained in Article 1 of the Export Regulation, the question arises whether they can be justified under Article 11 of that regulation.[285] Notwithstanding the exclusive competence of the Community in the commercial policy field, Member States may take action unilaterally on grounds of public security. Under Article 11 a Member State may exceptionally adopt national measures restricting the export of dual-use goods to non-member countries on the ground that this is necessary in order to prevent the risk of a serious disturbance to its foreign relations or to the peaceful coexistence of nations which may affect the public security of a Member State within the meaning of that article.[286]

Such measures, in so far as they affect exports to third countries, must be justified. The discovery of possible justification is the task of Member State's national courts. Although in the context of the Common Commercial Policy Article 1 lays down the principle of freedom to export goods, Article 11 of that regulation provides that it does not preclude the adoption or application by a Member State of quantitative restrictions on exports that are justified, *inter alia*, on grounds of public security. The Article 11 of the Export Regulation states that:

> "Without prejudice to other Community provisions, this regulation shall not preclude the adoption or application by a Member State of quantitative restrictions on exports on grounds of public morality, public policy or public security; the protection of health and life of humans, animals or plants; the protection of national treasures possessing artistic, historic or archaeological value, or the protection of industrial and commercial property."

[284] Opinion of AG *Jacobs*, *Werner*, C-70/94, ECR 1995, I-3203, para 31.
[285] Opinion of AG *Jacobs*, *Richardt*, C-367/89, para 27, I-4642.
[286] Judgment of the Court in *Leifer* C-83/94, ECR 1995, I-3254.

The derogation provided in Article 11 must be understood as applying also to measures having equivalent effect and as referring to both internal and external security of a Member State. Where the decision whether or not to award a license is taken on a case-by-case basis in the light of all the prevailing circumstances, *with the result that it cannot in advance be said with certainty whether a license will be granted*, the system in question will amount to a measure of equivalent effect.[287] Member State's measures of commercial policy must be specifically authorized by the Community in order to be lawful. The problem with Article 11 according to *Eeckhout-Govaere* is that it is not specific at all. It does not mention which measures can be taken; neither does it mention any industrial sectors or product categories to which it applies.[288] The conclusion to be drawn from the case law is that the scope of the various provisions depends not on the formulation used, but on their context and purposes.[289]

AG *Jacobs* noted that the protection of health and human life, mentioned in Article 11, referred not only to nationals of Member States, but to "the loss of life in general". He added that if a strictly legal approach were to prevail over a humanitarian one, it might be more difficult to maintain that there is a similarly close link between the potential loss of human life abroad and in the Community.[290] The Court apparently did not consider it necessary to determine whether or not it could additionally be justified on the ground of the other higher interests, such as the protection of human life, also mentioned in Article 11 of the Export Regulation.

Article 11 is to be considered as a provision delineating the field of commercial policy. It may only exceptionally be invoked.[291] It should be interpreted without prejudice to other Community provisions. It merely allows national legislation to derogate from the fundamental rule of freedom of export, and as an exception to a fundamental rule it should be interpreted strictly.[292] If one looks at the substance of the problem, it is rather evident that measures genuinely serving the purpose of protecting the security of a Member State cannot be qualified as commercial policy measures. It is reasonable, therefore, to acknowledge the competence of the Member States to take such measures.[293] Some degree of Community supervision is required, however,

[287] Opinion of AG *Jacobs* in *Richardt* C-367/89, I-4641. He referred to prior case law in cases: *Donckerwolcke*, C-53/76; *Procureur de la République v Bouhelier* C-53/76; *Commission v France* C-68/76.
[288] *Eeckhout-Govaere* p. 957.
[289] Opinion of AG *Jacobs*, *Richardt* C-367/89, I-4641.
[290] AG *Jacobs*, *Werner*, C-70/94, para 59.
[291] *Leifer* C-83/94, para 30.
[292] AG *Jacobs*, *Werner*, C-70/94, I-3205, para 37. Since Article 11 forms an exception to the principle of the freedom to export goods laid down in Article 1 of the Export Regulation, it must be interpreted in a way which does not extend its effects beyond what is necessary for the protection of the interests which it is intended to guarantee.
[293] *Eeckhout-Govaere* p. 958.

so that Member States cannot hide measures of downright commercial policy behind the public security screen.[294]

In order to assess the compatibility of national export restrictions with EC law, due regard should be given to the type of dual-use goods concerned, the specific country of destination and the specific circumstances in the material time.[295] The concept of dual-use goods implies that those goods are suitable for military use despite the fact that such use is not necessarily intended when the goods are produced or exported.[296] And as far as final destinations are concerned, can Germany, for instance, justify its exports to Iraq while another Member State justifies its authorising exports of the same product to the same country?[297] Moreover, if all Member States, or at least the Member States concerned, have similar rules as regards export to a third country, it should become more difficult, in view of the internal market, for one particular Member State to claim that its public security is put at risk where another Member State has given its consent to the exportation.[298]

4.3.2.1.1 Similarities Between Article 30 EC and Article 11 of the Export Regulation

Even if it should not be taken for granted that Article 11 of Export Regulation should necessarily be interpreted in the same way as Article 30 EC,[299] it is clear that the two provisions have a lot in common.[300] As long as export controls are not fully harmonized and Member States are allowed to maintain national export controls, there exists a possibility that Community law may be breached. The public security proviso of Article 11 of the Export Regulation has, according to the ECJ the same scope as the same proviso in Article 30 EC.[301] This is to ensure that Member States could not restrict intra-Community trade more than external trade.[302] AG *Jacobs* took the view in *Werner* that Article 11 of the Export Regulation is to be interpreted in much the same way as Article 30 of the EC Treaty, ***at least in an area such as strategic export controls***, where one and the same objective is at stake: namely to safeguard the external security of a Member State, either through restrictions on intra-Community trade or on exports to third

---

[294] *Ibid*.
[295] *Govaere* p. 1035.
[296] AG *Jacobs*, *Werner*, C-70/94, I-3215, para 68.
[297] *Koutrakos* p. 241.
[298] *Eeckhout-Govaere*, p. 951.
[299] Article 30 EC: "The provisions of Articles 28 and 29 shall not preclude prohibitions or restrictions on imports, exports or goods in transit justified on grounds of public morality, public policy or public security; the protection of health and life of humans, animals or plants; the protection of national treasures possessing artistic, historic or archaeological value; or the protection of industrial and commercial property. Such prohibitions or restrictions shall not, however, constitute a means of arbitrary discrimination or a disguised restriction on trade between Member States."
[300] *Govaere* p. 1034.
[301] The general principles governing Article 30 EC were established in case *Campus Oil*. (Case 72/83 *Campus Oil Ltd.*)
[302] *Werner,* C-70/94 at para 28, *Leifer,* C-83/94 at para 29.

countries.[303] In *Richardt*[304] the ECJ held that the concept of public security within the meaning of Article 30 of the EC Treaty covers both a Member States internal security and its external security. To interpret the concept more restrictively when it is used in Article 11 of the Export Regulation would be tantamount to authorizing the Member States to restrict the movement of goods within the internal market more than movement between themselves and non-member countries. Also in conformity with the above provisions in Article 19 (6) of DUR[305] it is stated that: "Application of this Article may in no case result in consignments of a specific product from one Member State to another being subject to more restrictive conditions than those imposed for exports of the same product to non-member countries." Dual-use goods also fall within the scope of the Export Regulation.[306]

Furthermore, it is established case law that Member States may only invoke the exceptions provided for in Art. 30 EC to the extent that no harmonization has been achieved.[307] The Court did not have the opportunity, in the *Werner* and *Leifer* cases, to rule on the compatibility of national export restrictions on dual-use goods with the Community regime for the export of dual-use goods as the latter only entered into force on 1 July 1995. Judging from its objectives and content, it is not likely that the existence of a Community regime at the material time would have fundamentally altered the outcome of the cases under discussion.

If Article 11 is to be considered as a provision delineating the field of commercial policy, this would fit in with the rule-of-reason approach to the concept of commercial policy, as advocated by *Timmermans*.[308] This approach starts from the observation that there has to be some degree of parallelism between the scope of the powers of the Member States concerning the regulation of intra-Community trade and the concept of commercial policy. It would indeed not be logical to deny the Member States certain powers relating to trade with third countries, whereas they retain the same powers in respect of intra-Community trade.[309] However, it cannot *a priori* be excluded that they could in reality be measures of downright commercial policy, simply hiding behind the public security screen. Therefore, some degree of Community supervision of their use is required.[310]

[303] AG *Jacobs*, *Werner,* C-70/94, I-3206 at para 39.
[304] Case C-367/89 *Richardt,* ECR 1991, I-4621 at para 22.
[305] DUR Article 19 covers procedures which are in force in the interim period. The length of this period is unspecified and it is still running.
[306] Opinion of AG *Jacobs* in *Werner,* C-70/94, I-3203, para 28: "I do not think that there is any reason to exclude dual-use goods from the scope of the regulation."
[307] Case 251/78 *Dencavit Futtermittel v. Minister für Ernährung, Landwirtschaft und Forsten*, ECR 1979, 3369.
[308] *Eeckhout-Govaere* p. 958, note 43.
[309] *Eeckhout-Govaere* p. 958.
[310] *Ibid.*

The parallelism with export controls is as follows, according to *Eeckhout-Govaere*. Suppose the Community had not acted to prevent importation of contaminated agricultural products after the Chernobyl accident. Would the Member States then have lacked the necessary powers to take action themselves, in order to protect public health, because such action is a matter of commercial policy coming under the Community's exclusive competence? Surely, negating their competence is hardly tenable, as much as it is untenable that the Member States cannot take measures aimed at protecting their national security.[311] But this does not exclude the competence of the Community to take such measures of its own, because such Community measures do not only protect public health, or – in the case of export controls – national security. They also create uniform conditions of importation or exportation, thus preventing deflections of trade or distortions of competition within the common market. It should be remembered that this is one of the basic aims of the Common Commercial Policy.[312]

4.3.2.2 The Concept of Public Security Under Community Law

Article 11 states that exports may be restricted on grounds of protecting the public security of a Member State. In this chapter I try to clarify how the concept of public security is defined in Community law. Increasingly, moreover, the security of a State cannot be looked at in isolation. It is closely linked to the security of the international community at large, and of its various components. The ECJ has concluded that the security of a State is closely linked to the security of the international community at large. A Member State may invoke the public security derogation even when its own security is not directly endangered.[313] The ECJ recalled that, in the *Richardt* case, it had already adopted the view that the exportation of goods capable of being used for military purposes to a country at war with another country may affect the public security of a Member State.[314]

The ECJ acknowledged that the public security exception may be invoked to restrict external as well as intra-Community trade without there being a need to prove that the security of a Member State is directly endangered.[315] A measure taken by a Member State is justified if it aims to protect the external security of at least one Member State.[316] The notion of security should be understood as extending to the security of the international community in general.[317] Use of Article 11 can be justified even when safeguarding the security of the international community

[311] *Eeckhout-Govaere* p. 960.
[312] *Ibid.*
[313] *Govaere* p. 1027.
[314] *Werner* C-70/94, para 28; *Leifer* C-83/94, para 29.
[315] *Govaere* p. 1034.
[316] AG *Jacobs*, *Werner*, I-3208.
[317] AG *Jacobs*, *Werner*, I-3211.

at large.[318] The measure is also justifiable if it is aimed at avoiding serious disruption of its foreign relations. These disruptions may affect the operation of international agreements concerning the security of a State, as well as its room for manoeuvre in conducting foreign policy interests.[319]

In the *Werner* and *Leifer* cases, the Court points out that adopting a more restrictive interpretation of the same concept in the Export Regulation would entail the paradoxical result that Member States could restrict intra-Community trade more than trade with third countries.[320] This is not tantamount to opening the door to unlimited use by Member States of the public security derogation. As far as the external security of a Member State is concerned, AG *Jacobs* pertinently remarked that: ”the latter is more likely to be affected by exports of strategic products to third countries than by intra-Community trade in such products.[321] In *Werner* an earlier incident was cited. It was the so-called Rabta case – German companies participated in the construction of a Libyan factory producing poisonous gas. The incident seriously disrupted Germany’s relations with the US and Israel.[322]

It is difficult to draw a hard and fast distinction between foreign policy and security policy considerations, not least because a disruption of foreign relations can have serious security implications. In any event, it is clear that Community law leaves Member States a large measure of freedom, subject always to the application of the principle of proportionality. In the field of restrictions on export to third countries, Article 11 of the Export Regulation seems designed to recognize that freedom, without any need to examine too closely whether ’public policy’ or ’public security’ is at issue. The European Commission also took the view that national measures can be justified on the basis of a combined application of public policy and public security grounds.[323] It is questionable, however, whether measures could be based only on maintaining the reputation of a Member State.[324] The Commission’s view, on the other hand, was that mere disruption of Germany’s foreign relations could justify the refusal to issue a license.[325]

Clarification brought by the *Werner* and *Leifer* cases is that the public security exception of Article 11 of the Export Regulation should not be interpreted more restrictively than the same

[318] AG *Jacobs*, *Werner,* I-3208.
[319] *Ibid.*
[320] *Werner* C-70/94, para 25; *Leifer* C-83/94, para 26.
[321] AG *Jacobs*, *Werner*, C-70/94, para 37.
[322] AG *Jacobs*, *Werner*, C-70/94, I-3209.
[323] AG *Jacobs*, *Werner*, C-70/94, I-3206 at para 41.
[324] *Werner*, C-70/94, I-3222: ”According to the Verwaltungsgericht, arguments put forward by the Federal Export Office seem to be based more on grounds concerning the reputation of the Federal Republic of Germany than on considerations of public security.”
[325] AG *Jacobs*, *Werner*, C-70/94, I-3206 at para 40.

concept used in Article 30 EC. This is not necessarily tantamount to acknowledging that Article 11 of the Export Regulation should always be interpreted in the same way as Article 30 EC. AG *Jacobs* had argued that a difference in interpretation may not be based on the fact that the former provides for a derogation from secondary legislation whereas the latter provides for a derogation from a fundamental principle laid down in the EC Treaty. He underlined the vital role of the CCP, as an indispensable component to the customs union, for the functioning of the Community.[326]

It was for the first time in the *Richardt* case that the Court clarified that the scope of the concept 'public security' extends to both the internal and external security of a Member State. Without further analysis, the Court then held that the importation, exportation or transit of goods which can be used for strategic purposes may indeed affect the public security of a Member State, which is therefore entitled to protect its interest under Article 30 EC. Hence, the Member States can make the transit of goods, qualified as strategic material, subject to a specific transit license. Since not all dual-use goods are always considered to prejudice public security, objective reasons should be forwarded to come to a justification, under Article 30 of the Treaty, with regard to restrictions on the movement of a specific type of dual-use goods.[327]

The concept of public security, referred to in Article 11 of the Export Regulation, is in principle broad enough to embrace restrictions on the transfer of goods or technologies of strategic importance to countries which are thought to pose a military threat. It will be recalled that Article 11 permits restrictions on exports to third countries by the same countries with regard to which Article 30 of the Treaty permits restrictions on imports, exports or goods in transit between Member States. Similar principles should, as AG *Jacobs* suggests, govern the interpretation of both provisions, and guidance can therefore be provided by the judgment of the ECJ in *Richardt*, which examined whether the confiscation of the microetch, as a restriction, was compatible with Article 30 of the EC Treaty.

The Court first recalled that the purpose of Article 30 EC is not to resolve certain matters under the exclusive jurisdiction of the Member States, but merely to allow national legislation to derogate from the principle of the free movement of goods. Since Article 30 EC is an exception to a fundamental principle of the Treaty, it must be interpreted in such a way that its scope is not extended any further than is necessary for the protection of the interests which it is intended to

[326] *Govaere* p. 1033.
[327] *Hunnings*, p. 157, where he argues that: "dual-use items would have to be very close to the armaments end of the spectrum to benefit from the 'public security' exemption".

secure.[328] It can be concluded that in the absense of Community legislation competent national authorities may decide which dual-use items may endanger the security of a Member State. Judicial review is confined to ensuring that no manifest errors of appraisal have occurred and national authorities have not abused Article 11.[329]

The ECJ seems to consider that a requirement to obtain export licenses which may be refused could in fact amount to a quantitative restriction. The apparent approval of unilateral measures in the area of strategic export controls does little to encourage Community co-operation and solidarity in the face of common external threats. The concept of external security should be further elaborated in order to minimise the scope and opportunity for abuse. [330]

Issues raised by considerations of foreign policy and security policy are, in general, not readily susceptible to judicial review. It is not easy for the ECJ, or for a national court, to examine the reality of the threat posed to the security of the Member State by the exportation of dual-use goods.[331] In some respects, indeed, Community law is less well placed to consider such questions than national law, since security concerns may differ substantially between different Member States.[332] Security concerns may also be indirect: exported goods may pose an indirect threat, because they may be used to manufacture military goods, may be adapted to military use or the manufacture of military goods, rather than being immediately suited for military purposes. The risk that certain exports may pose for the security of a State is often assessed on the basis of intelligence, the accuracy of which cannot be checked by the courts. The nature and gravity of that risk are likely to determine the tightness of the export restrictions. The subjective point of view of the Member State is of central importance in the assessment of foreign policy considerations.[333] National courts cannot dictate how their governments conduct foreign policy.[334] The role of the national courts should therefore be confined to exercising only a limited judicial review in order to ensure that no manifest errors of appraisal have occurred and that national authorities have not abused their powers under Article 11 of the Export Regulation.[335]

4.3.2.3 Proportionality Principle Considerations

Export controls are viewed in Community law as being export restrictions, and they have to be justified and honor the proportionality principle of Community law in order to be legal in the

[328] AG *Jacobs*, *Werner*, C-70/94, I-3205.
[329] AG *Jacobs*, *Werner*, C-70/94, I-3207.
[330] *Govaere* p. 1026.
[331] Opinion in Case C-120/94 *Commission v Greece* concerning the Greek embargo against the former Yugoslav Republic of Macedonia, delivered 6 April 1995.
[332] AG *Jacobs*, *Werner*, C-70/94, I-3207.
[333] Opinion of AG *Jacobs* in paras 54-56 in case *Commision v. Greece*, C-120/94.
[334] AG *Jacobs*, *Werner*, C-70/94, I-3214.
[335] Opinion of AG *Jacobs*, *Werner*, C-70/94, para 45.

Community. With regard to the conditions for the application of Article 30 EC, the Commission takes the view that, in order to be compatible with the EC Treaty, the national measures adopted within the framework of Wassenaar Arrangement must be susceptible of actual judicial review, on the application of those concerned, in order to avoid errors and abuses owing to the lack of transparency in the legal situation for traders and their lack of other means of defence.[336]

Community law allows national rules to impose on the applicant the whole burden of proving that the goods are for civil use as a condition for the grant of an export license, allowing for the refusal of an export license if the goods are objectively suitable for military use and imposing penalties, including imprisonment.[337] In *Richardt* the Court set out the following principle: "... in order to verify the nature of goods described as strategic material, the Member States are entitled under Article [36] of the Treaty to make their transit subject to the grant of a special authorisation."[338] As regards the penalties laid down for failure to comply with the obligation to obtain such authorization, it should be stated that a measure involving seizure or confiscation may be considered disproportionate to the objective pursued, and thus incompatible with Article 30 of the Treaty, in a case where the return of the goods to the Member State of origin could suffice.[339] Since confiscation or seizure constitutes a penalty, it may, where goods of high value are concerned, be considered disproportionate and thus incompatible with Article 28, 29 or 30 of the EC Treaty,[340] provided that the infringement committed by the trader is relatively insignificant or of a merely formal nature. It is highly possible that seizure or confiscation of dual-use goods could be considered disproportionate, because they are usually quite expensive. The right to impose criminal penalties for any breach of that procedure is a matter falling within the competence of the Member States. However, although Community law does not therefore preclude national rules from making the failure to comply with that obligation a matter subject to penalties, the penalties laid down may not be disproportionate to the public security aim pursued. It is for the national court to determine whether the criminal penalties applicable comply with the principle of proportionality, taking account of all the elements of each case, such as the nature of the goods capable of endangering the security of the State, the circumstances in which the

[336] *Richardt*, C-367/89, I-4629.
[337] AG *Jacobs*, *Werner*, C-70/94, I-3214.
[338] C-367/89 *Richardt*, paras 23-25.
[339] *Ibid.*
[340] Article 28 EC: "Quantitative restrictions on imports and all measures having equivalent effect shall be prohibited between Member States." Article 29 EC: "Quantitative restrictions on exports, and all measures having equivalent effect, shall be prohibited between Member States." Article 30 EC: "The provisions of Articles 28 and 29 shall not preclude prohibitions or restrictions on imports, exports or goods in transit justified on grounds of public morality, public policy or public security; the protection of health and life of humans, animals or plants; the protection of national treasures possessing artistic, historic or archaeological value; or the protection of industrial and commercial property. Such prohibitions or restrictions shall not, however, constitute a means of arbitrary discrimination or a disguised restriction on trade between Member States."

breach was committed and whether or not the trader who has illegally exported the goods was acting in good or bad faith.

It is for the national court to determine whether the system established complies with the principle of proportionality, taking into account all the elements of each case, such as the nature of the goods capable of endangering the security of the State, the circumstances in which the breach was committed and whether or not the trader seeking to effect the transit and holding documents for that purpose issued by another Member State was acting in good faith. AG *Jacobs* stated in *Richardt*: "The application of the principle of proportionality in specific cases is a matter for the national courts. It should not be assumed that that principle produces the same effect in relation to both Article 11 of the regulation and Article 36 of the Treaty, to which it also applies."[341]

However, depending on the circumstances, the competent national authorities have a certain degree of discretion when adopting measures which they consider to be necessary in order to guarantee public security in a Member State within the meaning indicated above. When the export of dual-use goods involves a threat to the public security of a Member State, those measures may include a requirement that an applicant for an export license show that the goods are for civil use and also, having regard to specific circumstances such as *inter alia* the political situation in the country of destination, that a license be refused if those goods are objectively suitable for military use. An obligation on the applicant to prove that the goods will be used exclusively for civil purposes or a refusal to issue a license if the goods can objectively be used for military purposes can be consistent with the principle of proportionality.

It is for the national court to consider whether national security or other interest listed in Art. 11 of the Export Regulation is in jeopardy, because there is an absence of Community legislation. This is the opinion of AG *Jacobs* in *Werner* case. *Jacobs* continues: "... judicial review is confined to ensuring that manifest errors of appraisal have not occurred and that national authorities have not abused the powers conferred by the exceptional provision in question."[342] The Court's function is to ensure that manifest errors or abuse of power has not occurred. The *acquis communautaire* is to be safeguarded.[343] In the light of the fundamental role of the principle of "full effectiveness of Community law" (*effet utile*) in the development of the Community legal order, the Court may exercise its jurisdiction over the interpretation of the guidelines set by DUD as a

[341] Opinion of AG *Jacobs* in C-367/89 *Richardt*, paras 28-29.
[342] Para 45 of his opinion in *Werner* C-70/94.
[343] *Koutrakos* p. 248.

matter of Community law.[344] The fact that foreign or security policy considerations are also in question, does not mean that Member States have in principle more leeway.[345] Member States may only rely on Article 11 of Export Regulation where the principle of proportionality has been respected. This means that Member States must not seek to enforce a national measure which is capable of being justified under that provision by steps which go further than is necessary to achieve the objective of the measure.

It should not be assumed that that principle produces the same effect in relation both to Article 11 of the regulation and to Article 30 of the EC Treaty, to which it also applies. Nevertheless, where failure to comply with national rules such as those at issue in the main action may lead to confiscation of the goods in question, such matters as the state of mind at the material time of the owner of the goods seized and the value of the goods should be taken into account. If there exists a risk of military use, it cannot be disproportionate to require the applicant for an export authorization to demonstrate that the goods will only be put to civil use. Nor it is necessarily disproportionate to refuse an export license if the goods are objectively suitable for military use. Much depends on the specific circumstances of each case.

Article 133 of the EC Treaty, as implemented by the Export Regulation, does not preclude a Member State from requiring a license for the export to a non-Member State of a product capable of being used for military purposes or the refusal of such a license on the ground that refusal was necessary to protect the security of the Member State owing to the risk of a serious disruption of its external relations.[346] Also pursuant to DUR Article 19 with some products deemed sensitive, a license can be required even in intra-Community transfers.[347] National rules restricting exports to a non-Member State of products capable of being used for military purposes in order to prevent a substantial disturbance of the peaceful coexistence of nations or to prevent the external relations of the Member State concerned from being seriously disrupted are justified on the basis of Article 11 in so far as those aims are linked to the external security of the Member State concerned, or in so far as the restrictions serve to protect the health and life of humans, as in cases where the country of destination is at war. Plain refusal to grant an export license without taking into account the specific circumstances prevailing in the country of destination would fail *the proportionality test*. Whether or not an export license may be refused will depend not only on the type of dual-use goods concerned but also on the specific country of destination

[344] See page 69.
[345] *Koutrakos* p. 249.
[346] *Werner*, C-70/94, I-3216.
[347] Regrettably cryptographic software is listed as sensitive in DUD Annex IV, see also chapter 4.4.

and the specific circumstances prevailing at the time of request.[348] The fact that the prejudice to public security is evaluated differently according to the country of destination of the goods shows that in this particular case the problem posed by the transit of the dual-use goods is intrinsically linked with their exportation to a particular non-Member State.[349]

The transit of goods destined to a non-Member State will only in rare cases lead to a distortion of trade between Member States.[350] Theoretically, at least, it is possible to envisage that a Member State restricts the transit of dual-use goods on the basis of the public security provision of Article 30 EC while allowing the exportation to the same country of destination of similar or comparable domestic goods fulfilling the same purpose. Similarly, it is not excluded that export controls are aimed at serving the commercial interests of a State rather than its public security.

Read literally, the *Werner* and *Leifer* cases seem to indicate that all measures containing instruments regulating trade would fall within the exclusive competence of the Community by virtue of Article 133 EC. Nevertheless, such a conclusion does no seem to accord with either the Treaties or the political realities. On a closer examination, these judgments seem to imply that the Community enjoys concurrent powers in that area, meaning that as long as the Community has not acted, Member States remain competent to adopt the necessary measures aimed at safeguarding their external security – provided those genuinely serve the objectives in question. However, once the Community has adopted measures harmonising the conditions of exportation, then Member States are naturally obliged to respect the relevant Community rules.[351]

4.3.2.4 Applicability of Articles 296 and 297 EC

If a national measure, *inter alia* export control regime, cannot be justified with Article 11 of the Export Regulation, the question arises whether it could be justified under Article 296 or 297 EC.[352] For a number of practical as well as legal reasons the relevance of the named provisions

[348] *Govaere* p. 1029.
[349] *Eeckhout-Govaere* p. 950.
[350] *Eeckhout-Govaere* p. 952.
[351] *Emiliou* p. 68.
[352] Article 296 EC: ”1. The provisions of this Treaty shall not preclude the application of the following rules: (a) no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security; (b) any Member State may take such measures as it considers 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; such measures shall not adversely affect the conditions of competition in the common market regarding products which are not intended for specifically military purposes. 2. The Council may, acting unanimously on a proposal from the Commission, make changes to the list, which it drew up on 15 April 1958, of the products to which the provisions of paragraph 1(b) apply.”
Article 297 EC: ”Member States shall consult each other with a view to taking together the steps needed to prevent the functioning of the common market being affected by measures which a Member State may be called upon to take in the event of serious internal disturbances affecting the maintenance of law and order, in the event of war, serious international tension constituting a threat of war, or in order to carry out obligations it has accepted for the purpose of maintaining peace and international security.

in the sphere of strategic export controls is rather limited.[353] Similarly, it is not clear whether Article 297 EC could be successfully invoked in relation to dual-use goods. In cases *Werner* and *Leifer* the Court concluded that national measures could be justified pursuant to Article 11 of the Export Regulation, and therefore did not find it necessary to engage in an analysis of Articles 296 and 297 EC.[354] If a Member State resort to these provisions, it would mean quite drastic measures against the Community and its Common Commercial Policy. Also, applicability of these provisions to dual-use goods is questionable, because those goods are not arms, but rather civilian products with possible military applications.

In Art. 296 of the EC Treaty a possibility is given for Member States to deviate from EC Treaty *inter alia* when trading or producing defence-related products. This provision allows a Member State to take measures *inter alia* in the event of war and serious international tension constituting a threat of war, or in order to carry out obligations for the purpose of maintaining peace and international security. It is commonly accepted that the first ground mentioned refers to crisis situations.[355] This Article is in by nature a wholly exceptional provision,[356] and it applies only to products listed exhaustively in the decision given on 15 April 1958 pursuant to Art. 296 (2) EC. This list has not been amended since 1958 and is very much outdated.[357] Since the scope of Art. 296 EC applies only to this list, dual-use items are not covered by this Article of the EC Treaty.[358] Member States cannot justify their possibly unproportional or otherwise unjustified export controls with this provision. It has to be established that the Member State needs to take the contested measure in order to comply with international obligations. It does not suffice to invoke resolutions or to refer to other non-binding statements of principle. For instance, in the *Werner* case, AG *Jacobs* pointed out that the German Government failed to argue that the UN Security Council Resolutions, which it invoked, entailed an obligation to adopt the contested measure.[359] The *Werner* and *Leifer* cases nonetheless have the merit of clarifying that Articles 296 and 297 EC do not need to be taken into consideration when a measure is already covered by a specific authorization such as Article 11 of the ER. If the discussion on the potential application of Articles 296 and 297 EC to dual-use goods may still be relevant from the theoretical point of view, in practice most problems are resolved now that dual-use goods have, at last, been classified within the realm of the Common Commercial Policy.[360]

---

[353] *Kapteyn*, pp. 406-407.
[354] Case C-83/94 *Leifer*, paras 14 and 31.
[355] *Eeckhout-Govaere*, p. 956.
[356] *Koutrakos* p. 248.
[357] Opinion of AG *Jacobs* in *Werner*, ECR 70-94, I-3200: "In 1958, the Council indeed drew up such a list. The Council's decision was never published, but its text is annexed to the Commission's observations. The products at issue in the present case are not mentioned in that list, ..."
[358] *Ibid.*
[359] AG *Jacobs*, para 52.
[360] *Govaere* pp. 1036-1037.

If it were necessary to examine Article 296 EC it would be necessary to resolve that issue and also to consider whether it can be construed so broadly as to encompass dual-use goods generally.[361] Uncertainty remains as to whether Articles 296 and 297 EC could at all apply to dual-use goods. Moreover, the Court has implicitly confirmed in its *Richardt* judgment that Articles 296 and 297 EC cannot be invoked in the context of export controls on dual-use goods, for it refrained from dealing with the applicability of those Articles whereas the AG had taken them into consideration. This points to the fact that the Court did not consider those Articles to be relevant to the case. As AG *Jacobs* pointed out, the issue of whether those provisions can be construed so broadly as to encompass dual-use goods is still not resolved.[362]

4.4 Export Control Regime in the Community

4.4.1 Some Remarks on Interpretation of Dual-Use Regulation

The Commission first began to examine the issue of export controls on sensitive and dual-use goods in the 1980s.[363] In the summer of 1989, a Political Committee (PoCo) working group was convened to examine the problems which the Single European Market (SEM) might pose for national arms export controls. The Dutch floated the idea of using a Benelux-style system, where the original supplier's export policies and licenses would be honoured throughout the Community.[364] It became apparent that a single market with no internal customs barriers would require a Community-wide policy for the export of sensitive or strategic goods which would not be exempted under Article 296 EC and which were therefore vulnerable to EC industrial, commercial and competition policies.[365] DUR drew its authority from Article 133 EC and was therefore a matter for qualified majority voting (QMV); several governments argued that QMV would not be an appropriate way to deal with the lists, given their foreign and security policy implications. Late in 1993 the Belgian government offered a compromise which was subsequently adopted. The solution was to seek agreement on the context of the lists through the joint action process, and to publish the list as annexes to an intergovernmental CFSP decision rather than include them in the Commission regulation.

Unless all EC members had comparable export policies and standards of implementation, license-free trade in dual-use technology within the single market area could enable unscrupulous exporters to evade controls in their home State by exporting first to a customer in another EC

[361] AG *Jacobs*, *Werner* C-70/94, I-3213.
[362] AG *Jacobs*, *Werner*, C-70/94, para 63.
[363] *Cornish* p. 82. For an overview see *Schroeder–Köchncke* p. 101-104.
[364] *Cornish* p. 79.
[365] *Cornish* p. 82.

State with more lax controls before re-exporting to the final, perhaps otherwise proscribed, destination.[366] The object of the exercise was to ensure that free and flexible intra-EC trade did not make possible the diversion of sensitive goods to third countries via the weakest link in the EC 'fence'.[367] In the long term, it could also be that States with more lax controls could, unfairly, attract additional investment for the manufacture of dual-use goods. The winding-down of COCOM posed another problem, since those EC members which were also COCOM participants had introduced simplified licensing systems for exports of sensitive goods to other COCOM partners and COCOM cooperation countries.[368]

Among many issues of concern was whether the regulation should adopt the COCOM consultative model, or whether some central licensing body should be created. Member States examined in microscopic detail the various legal, timetable and voting questions raised by the proposed legislation. One concern was whether licenses issued by one Member State would be valid throughout the Community, or whether Member States should have a *droit de regard* over exports from their ports under licenses issued by another Member State.[369] Some members called for a catch-all clause, and others for a 'safeguard' clause which could operate when national security was considered to be at stake, even in the case of exports to other EC States.

Reflecting deep misgivings about the integrity of the boundary between Community competence and national prerogative, the most difficult issue was the content and purpose of the lists which would support the regulation. Some members argued that lists of sensitive technologies, favoured or proscribed destinations and guidelines for making export decisions came too close to foreign and security policy-making to be placed under Community competence and could not therefore form part of a Commission-based regulation and system. In late 1992 the Commission accepted that these three key lists should indeed be a matter for governments.[370] The decision to implement material control provisions was indeed agreed under EU's Common Foreign and Security Policy pillar and not under a pillar of the European Communities. At this stage, the Community competence is restricted to the harmonisation of export control policies in order to establish a uniform external trade regime. The Community does not have the competence to deal with purely security issues. This explains the fact that the lists of goods and destinations subject to controls, which are essentially strategic in nature and therefore part of national com-

[366] *Ibid.*
[367] *Cornish* p. 83.
[368] *Cornish* p. 83.
[369] *Cornish* p. 84.
[370] *Ibid.*

petence, have been drawn up by the Member States within the framework of the intergovernmental co-operation in CFSP.[371]

DUD has been drafted in such a way that it would not give rise to any Community competence claims not acceptable to the Member States. The EU's export control regime established by DUR, falls completely within the domain of the CCP, although export controls do have additional foreign and security policy considerations and national authorities have considerable amount of room for manoeuvre in the Community export framework. Member States are obligated to implement, at a minimum, the EU's export controls and they may maintain additional controls as well.[372] The additional export control measures must be 'compatible' with DUR's objectives.[373]

Traditionally in the domain of the Community's CCP, exports have not been as problematic as imports. Therefore, there has been little need to regulate exports. For many years Council Regulation 2603/69[374] (so-called Export Regulation) was the only statute affecting exports from Community.[375] The current Community regime for dual-use goods essentially endorses the principle that, ***whereas in intra-Community trade the free movement of dual-use goods should prevail, the export of dual-use goods to third countries should be subject to effective control***.[376] In some respects it can be regarded as formulating established principles formulated earlier in ECJ case law explained in above chapters.

The basic aim of the regulation is to ensure that the export from the customs territory of the Community of certain dual-use goods[377] does not take place without authorization. Intra-EU trade in these goods and in other unlisted dual-use goods is controlled only with respect to certain sensitive goods. For instance cryptographic software is deemed to be sensitive, and its intra-Community transfers are to be controlled.[378] The Commission's proposal to update DUR is regrettably not likely to lift this intra-EU requirement in the future.[379] Annex IV lists goods such as nuclear reprocessing plant, stealth technology and rocket propulsion systems along with encryption technology which, although already listed in Annex I, are considered by some States to be so sensitive that, for the duration of the 'transitional period', all intra-EU exports will require

[371] *Cornish* p.75.
[372] *Baker-Hurst* p. 115.
[373] DUR Preamble, at Recital 10.
[374] OJ L 324, 27.12.1969, p. 25. Amended by Council Regulation 3918/91 OJ L 372/31.
[375] *Eurooppaoikeus 2000*, p. 794.
[376] *Govaere* p. 1035.
[377] Listed in DUD Annex I.
[378] DUR 19 (1) (b) and DUD Annex IV, where cryptographic software is listed as being sensitive.
[379] COM (98) 257final, p. 5.

national authorization. Annex V lists those goods which some Member States continue to define as military, rather than dual-use, and which are therefore excluded from the regulation under Article 297 EC. Annexes IV and V, it would seem, provide a counter-weight to the Commission's earlier insistence that Article 297 EC should be applied restrictively.[380]

One of the problems of the Community's export control regime is that it does not include so-called 'black list' countries to which dual-use exports are deemed implicitly as counterproductive to international stability. The omission of a list of sensitive or proscribed destinations could prove to be a grave weakness in the overall regulation, by giving governments significant discretion in deciding whether the proliferation risk associated with a prospective recipient country is outweighed by the benefits of exporting controlled items to that country. Such discretion could limit the effectiveness of an agreement among EU Member States on a common list of controlled goods and technologies.

The EU now ranks as one of the most sophisticated multilateral export control organizations in the world. As far as arms exports are concerned, the level of cooperation which has so far been achieved begins to give the EU a unified 'personality' in a nationally and internationally sensitive area, and begins to address the practical problems posed by the export of jointly developed and manufactured weapons and military equipment from the EU. As for the control of dual-use technology exports, the combination of an Article 113/QMV regulation with a set of CFSP joint action / unanimous lists is a notable and imaginative achievement.[381]

4.4.2 Controlled Encryption Software

Material dual-use item provisions are based on the Wassenaar Arrangement Control List – the WA-LIST.[382] The DUD, last amended on 19 May 1999,[383] implemented the latest changes in WA. The ***controls are limited to tangible forms of transfer***.[384] In the Commission's draft on updating DUR, it was suggested that controls at Community level should be extended to cover also intangible transfers.[385] The export outside the EU of goods in categories listed in Annex I to DUD is to be specifically authorized, unless the destination appears in Annex II to the joint action, a list of destinations for which 'simplified formalities may be applicable'.[386]

[380] *Cornish* p. 86, see also chapter 4.3.2.4 covering Articles 296 and 297 EC.
[381] *Cornish* p. 87.
[382] See chapter 3.
[383] Decision 1999/193/CFSP, OJ L 73 19. 3.1999.
[384] DUD Annex 1, General Notes to Annex 1 (3). See discussion on tangible/intangible transfers in chapter 3.5.2.
[385] COM (98) 257 final, p. 5.
[386] See p. 66.

In many Member States intangible transfers are controlled pursuant to national export control laws.[387] Some Member States, like Finland, control even the transfer of services, like education or consulting services. ***Services do not, however, fall within the scope of the EU's control regime.*** Once the Community has adopted measures harmonising the conditions of exportation, then Member States are naturally obliged to respect the relevant Community rules, but in this special case they are, however, allowed to maintain stricter controls. One must also bear in mind, that relevant control lists are updated regularly, usually few times a year and the field of export controls is very prone to changes in political climate and technology advances.

4.4.3 Transfers Inside Community Boundaries

Almost all dual-use item transfers inside the Community are relaxed from controls. DUD Annex IV classifies some items as sensitive. Article 19 DUR states that in the transition period also intra-Community transfers of those sensitive items are subject to licensing. Regrettably also information security items are classified in Annex IV as sensitive. Therefore ***intra-Community transfers of cryptographic software must be authorized***. Also in DUR Article 19 (b) it is stated that Member States cannot give general authorizations to sensitive transfers. Competent national authorities can give sensitive items only global authorizations or individual authorizations even in transfers inside the Community.

These intra-Community restrictions are meant to be in force only for a transitional period and after that they are obviously meant to be lifted. The original idea, when drafting DUR, was that when the EU's export regime was functioning efficiently and harmonized sufficiently, the intra-Community authorizations could be lifted permanently.[388] However, the transitional period has been running since 1995 and the length of this transition period is unspecified in DUR.[389]

The transfer authorization must be applied for in the Member State from which the dual-use goods are transferred.[390] A Member State may require an authorization for the transfer of dual-use goods from its territory to another Member State in cases where, at the time of transfer, the operator knows that the final destination of the goods concerned is outside the Community and export of those goods to that destination is subject to a license pursuant to DUR Article 3, 4 or 5. In some of those situations it is required that no processing or working as defined in the Community Customs Code is to be performed on the goods in the Member State to which they

[387] See chapter 5.
[388] *Baker-Hurst* p. 115: "The intent of these regulations is to remove the **internal** border controls on dual-use goods and technology..." (emphasis added). Also COM (97) 503 IV 2.(ii): "progressively dismantling intra-Community controls..."
[389] See DUR Art. 19 and *Baker-Hurst* p. 116.
[390] DUR Article 19 (3) (b).

are being transferred.[391] These measures shall not involve the application of internal frontier controls within the Community, but solely controls which are performed as part of the normal control procedures applied in a non-discriminatory fashion throughout the territory of the Community.[392]

For a transitional period, in respect of consignments dispatched from one Member State to another for dual-use goods listed in DUD, the relevant commercial documents shall indicate clearly that they are subject to control if exported from the Community.[393] For instance, the following formulation may be used: ”This product is subject to export control if exported out of the European Union.”[394] Documents and records of consignments of dual-use goods listed in DUD must be kept for at least three years from the end of the year in which a transaction took place and must be presented to the competent authorities on request. Any natural or legal person who engages in intra-Community trade in the dual-use goods listed DUD must, before or within 30 days of the first such transaction, provide details to the competent authorities of his name and the address where the documents and records can be inspected.[395]

4.4.4 Controls of Items Not Listed in DUD

The EU Control List for dual-use goods and technologies is not exhaustive. It is expressly provided that a Member State may impose additional restrictions with respect to the export of other dual-use goods and to countries which are not listed (DUR Art. 3). With a view to pursuing the objectives of DUR effectively in terms of export controls, a Member State may prohibit or make subject to authorization the export of dual-use goods not listed in DUD.[396] Those restrictions are published in the OJ.[397]

One major aspect of the EU’s export control regime has been the introduction of ”Know Your Customer” burden to the exporter.[398] DUR Art. 4 contains a so-called Catch-All clause. It is a central element of the regulation, a feature which aroused some controversy during negotiations.[399] Vendors are to report to competent national authorities, when they suspect *inter alia* possible WMD end use. But in some cases it can be, if not practically impossible as *Gladman* argues,[400] very difficult for the vendor to know to which purpose a dual-use product will be put.

[391] DUR Article 19 (3) (a).
[392] DUR Article 19 (4).
[393] DUR Article 19 (1) (a).
[394] *Tillståndstyper SP.*
[395] DUR Article 19 (2).
[396] DUR Article 5 (1).
[397] DUR Article 5 (4).
[398] DUR Article 4.
[399] *Cornish* p. 85.
[400] *Gladman* p. 2.

Items can be resold or re-exported and the end-user may remain virtually anonymous to the exporter. Article 4 states that the exports even of unlisted goods must be licensed if the exporter is informed by his national authorities, or is simply 'aware', that the goods are intended for use in Weapons of Mass Destruction or missile manufacture. It is left to member governments to decide how to legislate in the potentially controversial matter of establishing an exporter's knowledge, or mere grounds for suspecting that a given export is intended to be misused. An authorization shall be required for the export of dual-use goods not listed in DUD, if the exporter has been informed by his authorities that the goods in question are or may be intended, in their entirety or in part, for WMD end-use (DUR 4 (1)).

Also if the exporter is aware that the goods in question are intended, in their entirety or in part, for WMD-related purposes, he must notify his authorities, which will decide whether or not it is expedient to make the export concerned subject to authorization (DUR 4 (2)). By giving this provision, the Community authorities require the exporter to "know his customer", at least in some part.[401] This provision means that the exporter must maintain some degree of awareness in his business contacts. If, for intanse, in normal business negotiations, the exporter learns about possible WMD-related end-use, he should report this to his country's competent national export authorities. DUR Art. 4 (2) does not, however, establish any active or broad investigation duty to the exporter. In unclear situations, it is wisest to consult national export authorities.[402]

Member States may adopt or maintain national legislation stipulating that the exporter has to notify his authorities where he has grounds for suspecting that the goods concerned are intended. wholly or in part, for WMD-purposes, and that in such a case the export operation may be made subject to authorization.[403] By making this provision the Community authorizes Member States to extend the exporter's "Know Your Customer" duty to situations where there exists only suspicion of WMD end-use.

So, what kind of things should make the exporter suspicious? Of course much depends on the case and no clear pointers can be given.[404] However, the exporters should be suspicious about an enquiry or order if the customer is reluctant to offer information about the end use of the goods; the customer is reluctant to provide clear answers to commercial or technical questions which are routine in normal negotiations; an unconvincing explanation is given as to why the goods

[401] COM (98) 258 final p. 2.
[402] *Lag och förordning.*
[403] DUR Article 4 (3).
[404] *Supplementary Guidance Note to the End Use Control.*

are required, in view of the customer's normal business or the technical sophistication of the goods; routine installation, training or maintenance services are declined; unusually favourable payment terms such as higher price and/or lump-sum cash payment are offered; unusual shipping, packaging or labelling arrangements are requested; the customer is new to exporter and his knowledge about him/her is incomplete; the installation site is in an area under strict security control or is in an area to which access is severely restricted, or is unusual in view of the type of equipment being installed; there are unusual requirements for excessive confidentiality about final destinations, or customers, or specifications of items; there are requests for excessive spare parts or lack of interest in any spare parts; the dealer exporter is selling to is new, or has been evasive about customers; the customer or end-user is a military or government research body; the order is itself unusual in any way, e.g. the quantity or performance capabilities of the goods ordered significantly exceed, without satisfactory explanation, the amount or performance normally required for the stated end use.[405]

4.4.5 Types of Authorizations When Exporting Outside the Community

According to DUR Article 6 (1) all controlled items (which are listed in DUD) are subject to individual authorization. Individual authorization means that every transfer must be separately authorized by the competent national authority. However, regarding some transfers simplified procedures are provided. One must note that Member States are not by law obliged to allow simplified procedures. At present all Member States have adopted global authorizations, but there still exist Member States that have not adopted general authorizations, although they are likely to adopt them in the future.

4.4.5.1 Types of Simplified Procedures

4.4.5.1.1 General Authorization

First of all, a general authorization can be given. It can concern some type or category of dual-use goods.[406] A general authorization is directed to all prospective exporters in a Member State. No applications for authorization are needed in the field covered by a general authorization. According to DUD Annex II general authorizations are applicable only to certain destinations, which are adherents to, or fully cooperating with, all relevant regimes on non-proliferation and control of sensitive goods. In particular, the following non-EU countries are listed in DUD as being such destinations: Australia, Canada, Japan, Norway, Switzerland, and the United States of America. If a Member State wishes to give general authorizations to other destinations, it must inform other Member States and Commission about it.[407] As far as cryptographic software

[405] *Appendix C – Suspicious Enquiries*.
[406] DUR Article 6 (1) (a).
[407] DUD Annex II (2) & (3).

controlled pursuant to WA is concerned, general authorization is not available. According to DUR Art. 19 (1) (b), cryptographic software (classified as sensitive in DUD Annex IV) may not be exported giving general authorizations.[408]

4.4.5.1.2 Global Authorization

Global authorization can be given to a specific exporter in respect of a type or category of dual-use goods which may be valid for exports to one or more specified countries.[409] When exporting cryptographic software this type of authorization is very important, because general authorizations are not available. The applying of individual authorizations for every transfer could have devastating effects on, for instance, an exporting company's business prospects, although intangible technology transfers, like web downloads, fall beyond the scope of the Community's export regime. Regrettably, the Commission has proposed that also intangible transfers should be controlled in the future.[410]

4.4.5.1.3 Simplified Procedures

Article 5, the 'safeguard clause', allows governments to prohibit the export of any other, unlisted dual-use goods, provided any prohibitions are notified to the Commission and other governments. When a Member State controls an item which is not listed in the DUD control list pursuant to DUR Art. 5,[411] it can employ simplified procedures when giving authorization to export this item.[412] Simplified procedures may be employed when, for instance, a recipient country is listed in Annex II to DUD.[413]

As stated before, unlisted items can be controlled if control of those items is in harmony with the objectives of DUR. For instance in Finland, intangible technology transfers are controlled by law, even though this is not required in Community law. The Finnish Government has argued that control of intangible transfers is necessary in order to guarantee the effectiveness of export controls.[414] In this type of situation simplified procedures can be employed. For instance in web downloads it can be ruled that an end-user bookkeeping requirement is sufficient and individual authorizations are not needed if buyers are identified as being nationals of a country where the exporter has a valid export license. In fact this is the current situation under Finnish export regulations. Buyer identification in the Internet environment is not, according to techical experts,

[408] *Baker-Hurst* p. 116.
[409] DUR Article 6 (1) (b).
[410] COM (98) 257 final p. 5.
[411] See p. 64.
[412] DUR 6 (1) (c).
[413] See above chapter covering global authorization.
[414] HE 69/1996 vp, Yksityiskohtaiset perustelut 2 §. Also in COM (98) 257 final p. 5 this opinion has been stated as a principal reason to control intangible transfers.

100 percent accurate and impersonation and 'spoofing'[415] is relatively easy for skilled individuals. Still, Finnish authorities have concluded, that the above-mentioned simplified procedures are sufficient. This is probably because making individual licenses compulsoty would be too cumbersome to exporters conducting e-commerce across borders.

4.4.5.1.4 End Use and Re-Export Statements and Other Requirements and Conditions for Export

An export authorization may be subject, if appropriate, to certain requirements and conditions. In particular, the competent authorities of a Member State may require a statement of end use and may impose other conditions concerning the end use and/or the re-export of the goods.[416] An end use statement is a statement from the end-user of a dual-use product, which ascertains that the product is used solely in a civilian context, for peaceful, non-military use. Usually re-export restrictions or prohibitions are also included in licencing conditions, when an end-user statement is required.

End use statements are important tools in enforcement when WMD or other defence-related end-use is suspected. If an end use statement, signed by the end-user or his representative is required by the competent national authority, it is hard for the exporter to argue that he did not know or suspect malicious end use. The same applies to re-export restrictions which, if imposed, preclude re-export from a country to which an export authorization was originally given. A re-export restriction violation or a failure to file an end use statement when required should be punishable in Member States, because this is required by Article 17 of DUR. If the suspect is a foreing national the enforcement can be difficult.

One other question, which needs to be discussed here are the re-export controls imposed by U.S. authorities. In many situations they may have significant effects to product's transferability, because parts of the dual-use product in question may contain American parts which are already subject to U.S. re-export restrictions or prohibitions. Not all U.S. re-export controls are considered illegal in Europe pursuant to provisions of international law. It is seen as legal that the U.S. (like other nations do) issues licenses under certain restrictions and conditions which are binding for the end-user who has signed the appropriate statement of end use. What is seen as contradicting international law, because of extra-territoriality, is the imposition of fines against the foreign re-exporter who is including U.S. products into his foreign products. Also so-called *de minimis* rules for parts and components are seen as contradicting generally accepted customs

[415] The changing or masking of designated IP-addresses, by which the computer can be identified as located in a certain country or region.
[416] DUR Article 6 (2).

rules. U.S. rules are - in general - accepted by those companies, who fear for their reputation or who have an exposure because of necessary US imports or exports. Most managers who have to deal with U.S. re-export controls would qualify extraterritorial U.S. re-export controls - especially those based on unilateral controls as 'blackmail' if asked unofficially but would nonetheless comply with them.[417] Also a Member State's legislation may contain provisions which can be used to prohibit the export, if the goods or parts thereof have been imported with re-export restrictions. This is completely legal according to Community provisions mentioned above.

4.4.6 The Validity of Export Authorizations

In Article 6 (3) of DUR the fundamental principle is laid down - ***export authorizations shall be valid throughout the Community***. Once issued any individual, general or global authorization is to be valid throughout the EU. But if the goods to be exported are located elsewhere in the EU, the relevant government is granted a brief period in which to object to the export.[418] Competent national authorities, for instance DTIs or customs agencies, are to recognize authorizations given by their counterparts in other Member States. Article 3 (3) states that dual-use goods which only pass through the territory of the Community, whether or not subject to a transit procedure fall outside the provisions of the Regulation. A Member State may take appropriate measures in respect of such goods according to its national law.

4.4.7 Some General Remarks About Export Authorization Procedure

It can be concluded that DUR does not establish enforcement provisions. Instead, each Member State is required to take appropriate measures to ensure proper enforcement of all provisions of the regulation.[419] In deciding whether or not to grant an export authorization, the competent authorities shall take into consideration the common guidelines set out in Annex III to DUD (DUR Article 8). DUD Annex III, so-called *Agreement of Member States on Guidelines*, lists the following criteria in deciding whether to grant an export authorization: (a) their commitments under international agreements on non-proliferation and the control of sensitive goods; (b) their obligations under sanctions imposed by the UN Security Council or agreed in other international fora;[420] (c) considerations of national foreign and security policy, including, where relevant, those covered by the criteria they agreed at the European Council in Luxembourg in June 1991 and in Lisbon in June 1992 with regard to the export of conventional arms;[421] (d)

[417] *Roth*.
[418] See chapter 4.4.9.
[419] *Baker-Hurst* p. 120.
[420] At present, according to DUD Annex III the following countries are subject to a general UN trade embargo (excluding humanitarian aid): Iraq, Serbia and Montenegro. The following countries, while not subject to a general trade embargo or an embargo on dual-use goods, are subject to UN or EU arms embargoes: Angola (specific buyers), China, Liberia, Libya (plus an embargo on aircraft and aircraft spares and certain refinery equipment), Myanmar, Rwanda, Somalia, Sudan, Zaïre, and the former Socialist Federal Republic of Yugoslavia.
[421] The EU Arms Export Criteria (The Luxembourg criteria, June 1991). *Inter alia* the existence of a risk that the equipment will be diverted within the buyer country or re-exported under undesirable conditions should be taken into

considerations about intended end use and the risk of diversion. Member States will exchange views on these guidelines as appropriate, in order to review them as necessary. Basically, what Annex III does is remind Member States of their international commitments. In any decentralised system of control, the interpretation of the applicable guidelines is of central importance. This is even more so in the case of DUR and DUD, because of the broad scope for manoeuvre left to the Member States and the general character of the criteria themselves.[422]

An export authorization shall be granted by the competent authorities of the Member State in which the exporter is established.[423] If the dual-use goods in respect of which an application has been made for an individual export authorization to a destination not specifically mentioned in Annex II to Decision DUD or to all destinations in the case of very sensitive dual-use goods referred to in Annex IV to the said Decision are or will be located in a different Member State, this shall be indicated on the application.

If exported goods are or will be located in a different Member State, the licensing authorities of the Member State to which the application for authorization has been made, shall immediately consult the licensing authorities of the Member State(s) in question and provide the relevant information. The Member State(s) consulted shall make known, following receipt of the information gathered under the exporter's bookkeeping requirement[424] and of any supplementary information required, within 10 working days, any objections to it they may have to the granting of such an authorization, ***which shall bind the Member State in which the application has been made***. If no objections are received within the above period, the opinion of the Member State consulted shall be regarded as positive.[425] This other Member State's *right of veto* and the consultation procedure are intended to prevent "forum shopping" among different EU countries. Nevertheless, it is in practice not uncommon for exporters to "shop around" for the most favourable EU country from which to export their goods.[426]

If an exportation might prejudice its essential interests, a Member State may request another Member State not to grant an export authorization or, if such authorization has been granted, request its annulment, suspension, modification or revocation. The Member State receiving such a request shall immediately engage in consultations of a non-binding nature with the requesting

consideration when granting licenses. (European Council, Declaration on Non-Proliferation and Arms Exports, Luxembourg, 29 June 1991).
[422] *Koutrakos* p. 242.
[423] DUR Article 7 (1).
[424] See chapter 4.4.8.
[425] DUR Article 7.
[426] *Baker-Hurst* p. 160.

Member State, to be terminated within 10 working days. This consultation procedure provided in DUR Article 7 (3) is expressly of a non-binding nature.[427]

4.4.8 Exporter's Duties Under DUR

Exporters shall supply the competent authorities with all relevant information required for their applications for authorization.[428] Failure to give accurate information or giving knowingly false information is punishable in Member States' penal codes pursuant to DUR Article 17:

> "Each Member State shall take appropriate measures to ensure proper enforcement of all the provisions of this Regulation. In particular, it shall determine the penalties to be imposed in the event of breach of the provisions of the Regulation or of those adopted for its application. Such penalties must be effective, proportionate and dissuasive.
> In particular, for the implementation of Article 4 (2), each Member State shall lay down and specify the nature of the breach of national law and shall determine the nature of the penalty to be imposed."

Penalties for infringing Art. 4 (2) DUR are for failing to notify the export authority of possible WMD end-use. Article 17 can be regarded as formulating established principles in Community law, namely in *Werner* and *Leifer* cases, which make it possible to punish for a breach of the export control laws, taking in account proportionality principle considerations.[429]

When completing the export formalities at the customs office responsible for handling the export declaration, the exporter shall furnish proof that the export has been duly authorized.[430] A translation may be required of the exporter of any documents furnished as proof into the official language or one of the official languages of the Member State where the declaration is presented.[431]

The exporters must keep detailed registers or records of their transactions, in accordance with the practice in force in the respective Member States. Such registers or records must include in particular commercial documents such as invoices, manifests and transport and other dispatch documents containing sufficient information to allow the following to be identified: the description of the dual-use goods, the quantity of the dual-use goods, the name and address of the exporter and of the consignee, where known, the end use and end-user of the dual-use goods. The recipient, in other words, is the 'first line buyer' of product in question. The relevant commercial documentation are e.g. a sales contact, order information, an invoice or a dispatch note. If known, the end-user information (the real end-user, name, adress) must be kept. The registers and records and the documents must be kept for at least three years from the end of the calendar

[427] *Koutrakos* p. 239.
[428] DUR Article 9 (1).
[429] See chapter 4.3.2.3.
[430] DUR Article 10 (1).
[431] DUR Article 10 (2).

year in which the export took place. They must be presented to the competent authorities on request.[432]

Member States shall take whatever measures are needed to permit the competent authorities to gather information on any order or transaction involving dual-use goods and to establish that the control measures are being properly applied. These measures may include, in particular, the power to enter the premises of persons with an interest in an export transaction.[433]

4.4.9 A Member State's Right to Stop a Dual-Use Item Transfer Already Authorized in Another Member State

Without prejudice to any powers conferred on it under, and pursuant to, the Community Customs Code, a Member State may also suspend the process of release for export from its territory or, if necessary, otherwise prevent the export of dual-use goods listed in DUD and covered by a valid authorization from leaving the Community via its territory, where it has grounds for suspicion that relevant information was not taken into account when the authorization was granted, or circumstances have materially changed since the issue of the authorization. The suspension period may not exceed 10 working days.[434]

In such cases, the competent authorities of the Member State which granted an export authorization in the first place shall be consulted forthwith in order that they may take action.[435] Should these authorities decide to maintain the authorization or if no reply has been received within 10 working days, the dual-use goods shall be released immediately unless the consulting Member State has recourse to exceptional circumstances provided for in DUR Art. 10 (4).

According to DUR Art. 10 (4), in exceptional circumstances, where a Member State considers an exportation would be contrary to its essential foreign policy or security interests or to the fulfillment of its international obligations or commitments, it may prevent the dual-use goods from leaving the Community via its territory even though the export was duly authorized in another Member State. When a Member State takes action under this paragraph, the goods concerned shall be put at the disposal of the exporter. The competent authorities of the Member State which issued the authorization shall be duly informed. Although foreign and security policy is largely the business of Member States, some analogy can perhaps be drawn from interpretation of Article 30 EC – a Member State which relies on a requirement provided for in Article

[432] DUR Article 14.
[433] DUR Article 15.
[434] DUR Article 10 (3).
[435] DUR Article 10 (3) and also DUR 9 (2).

30 EC must prove that the specific conditions in its country are different from those in the State which authorized the movement of the product.[436]

4.5 Common Foreign and Security Policy Considerations

The *Werner* and *Leifer* cases are extremely important as they implicitly raise the issue of the interface between the first and second pillars of the Maastricht Treaty and, in particular, the extent to which the latter may encroach upon the former.[437] Article 46 TEU specifies that the Court has no jurisdiction with respect to the CFSP. Article 133 EC, in conjunction with Article 301 EC[438], could serve as the legal basis for a Community export control regime also for military (not dual-use) goods. That would be only logical, since an agreement on the common export control regime for military goods should not be unduly difficult within the framework of a common foreign and security policy.[439] Some unofficial sources from the Council of the European Union even indicate that there exist proposals to harmonize arms trade and bring it fully subject to EC competition and other provisions. If arms trade is harmonized in the EU region there exists strong impetus to fully harmonize dual-use item trade and remove room for national derogations.

The modern arms trade has to be understood as involving weapons of varying sophistication, tangible technology of both military and civil origin, and intangible know-how.[440] Naturally Member States might be reluctant to make trade in military goods subject to rules of Community law. Nevertheless, it should be pointed out that there is no doubt any common position or a joint action agreed in the CFSP involving export controls for military goods will need to be effected through Community action (by qualified majority) under Article 301 EC. Thus, unilateral national or even intergovernmental action in areas where there are clear links with Community mechanisms, such as those established under Article 300 EC,[441] would probably deal quite a serious blow to the integrity and coherence of the Community legal order.[442] Member States should undertake coordinated steps with a view to cutting off supplies of war material to third countries whose military capability is sufficient for their own defence.[443] In SEC (92) final key elements for an operational and effective system at Community level were set out: a com-

[436] Commission publication: Échanges Intérieurs Textes 1987 No 1, pp. 73-74.
[437] *Govaere* p. 1030.
[438] Article 301 EC: "Where it is provided, in a common position or in a joint action adopted according to the provisions of the Treaty on European Union relating to the common foreign and security policy, for an action by the Community to interrupt or to reduce, in part or completely, economic relations with one or more third countries, the Council shall take the necessary urgent measures. The Council shall act by a qualified majority on a proposal from the Commission."
[439] *Govaere* p. 1030.
[440] *Cornish* p. 74.
[441] Article 300 EC contains Community's foreign relations provisions.
[442] *Cornish* p. 74.
[443] *Poettering Report* p. 65.

mon list of dual-use goods and technologies which are subject to control; a common list of destinations, altough the nature of this list; i.e. whether it should be a list of 'proscribed' or of 'special facilities' destinations, will require further reflexion; common criteria for the issuing of licenses for exports from the EC; a forum or mechanism in which to coordinate licensing and enforcement policies and procedures for administrative cooperation. Until the determination to achieve closer political integration is felt, it is difficult to see defence industry collaboration, common defence procurement and a fully integrated export control system as attainable objectives.[444]

[444] *Cornish* p. 88.

5 EXPORT CONTROLS IN SOME RELEVANT EU MEMBER STATES

The export control regimes of Finland, Sweden, Germany, France and United Kingdom are covered in this chapter. However, all these countries are covered in this chapter *only to the extent that they differ from the EU's uniform export control regime*. Usually, according to well established principles of Community law, Member States are not allowed to legislate on a subject that is already covered by Community regulations.[445] Regulations like DUR are applicable in Member States directly, without any national implementing measures.[446] Member States are not even allowed to pass legislation implementing Community regulations, because such regulations are directly applicable in Member States pursuant to Article 249 of the EC Treaty. And also, if the provisions of a national statute and a Community regulation conflict, the courts and national authorities in Member States are required to apply the provisions of the Community regulation, ***because Community law has primacy over national law***.[447] Community regulations also have ***replacing effect***: if a national provision does not directly conflict with the text of the regulation, it can still hinder the aims and objectives of the regulation and it must not be applied.[448]

However, in the domain covered by DUR, according to Recital 10 of its Preamble, national measures that are 'compatible' with the objectives of DUR are allowed. This is an exceptional case when national measures are allowed. Member States are allowed to pass legislation on a subject covered by a Community Regulation, when this possibility is stated in the regulation itself.[449] This legislation cannot, however, affect the direct applicability of a regulation, its uniform interpretation in different Member States or the validity of the regulation.[450] Also national measures cannot establish broad exceptions to regulation, if those exceptions are not compatible with the objectives of the regulation.[451]

Finally, this is a question of interpretation, and it must be decided separately in the case of each particular regulation, which national measures are compatible with the objectives of the regulation in question.[452] National measures are also legal, when: (i) a Community entity has not acted, when it should have done according to a regulation, (ii) or in the case when subject is not

---

[445] *Eurooppaoikeus* p. 70.
[446] This fundamental doctrine of Community law was established *inter alia* in Case 42/71 *Politi,* ECR 1971 p. 1039.
[447] This doctrine was established by the landmark case of Community law - Case 6/64 *Costa v. ENEL*, ECR 1964, p. 585. ECJ stated also in Case 106/77 *Simmenthal,* ECR 1978, p. 629: "Directly applicable Community statutes prevent automatically the interpretation of conflicting national law."
[448] Case 50/76 *Amsterdam Bulb*, ECR 1977, p. 137 para 9: "... not only the express provisions of Regulations, but also of their aims and objectives."
[449] Relevant case law is for instance Case 74/69 *Krohn & Co,* ECR 1970, p. 451.
[450] *Eurooppaoikeus* p. 71.
[451] Case 18/72 *Granaria Graaninkoopmaatschappij,* ECR 1972, p. 1163, paras 14-18.
[452] *Eurooppaoikeus* p. 71.

covered exhaustively by regulation and national measures serve the objectives of the regulation, (iii) or when some arrangement mentioned in the regulation is not within the scope of the Community law in question.[453]

5.1 Finland

5.1.1 Overview

Finnish strategic export controls on dual-use goods are implemented by three different statutes: Act on Control of Exports of Dual-Use Goods (laki kaksikäyttötuotteiden vientivalvonnasta 562/96) and Decree thereof (asetus kaksikäyttötuotteiden vientivalvonnasta 645/96), with detailed provisions in Decision of the Ministry of Trade and Industry on the Goods and Technologies Subject to Export Licensing (kauppa- ja teollisuusministeriön päätös kaksikäyttötuotteiden vientilisensioinnista 54/97). The national export authority is the Ministry of Trade and Industry under the Council of State. Compared to the EU regime, Finland's controls are broader in two important areas. First, Finland restricts the export of services and technology.[454] Thus, Finland restricts the export of technical assistance and other services. Second, Finland controls intangible transfers,[455] e.g. via electronic mail or the Internet.

5.1.2 Export Control Procedure

Well before actually exporting goods which are possibly of dual-use nature, the exporter must discover whether they are subject to export control, because this is not possible when declaring goods to customs.[456] This is principally the duty of the exporter or manufacturer.[457] The characteristics of the product are of key relevance, when assessing its possible dual-use nature. MTI can, when requested, give prior information on some particular products dual-use nature. This does not, however, free the exporter from the duty to apply for export authorization.[458]

As a principle, freedom to export is recognized in Finnish law. Only in cases listed in § 3 of Act 562/96 may an authorization be refused. It is important to recognize that exports can be banned if the goods have been exported to Finland with re-export restrictions. Goods or software may include foreign parts which are subject to foreign export controls. Finland has adopted legislation, pursuant to Art. 19 (3) (a), that an authorization for the transfer of dual-use goods from its territory to another Member State is required in cases where, at the time of transfer, the operator knows that the final destination of the goods concerned is outside the Community and export of

[453] *Eurooppaoikeus* p. 72.
[454] Act 562/96 § 2.
[455] HE 69/96 vp. See also page 34.
[456] *Hakuohjeet ja asiakirjamallit*.
[457] *Vientivalvonta* p. 10.
[458] *Vientivalvonta* p. 1.

those goods to that destination is subject to a license.[459] Pursuant to DUR Article 4 (3), national exporter's duty to inform MTI has been extended to cover situations where the exporter has grounds to suspect that goods are intended for WMD end-use.[460] Also the bookkeeping requirement in DUR Art. 14 has been extended in national legislation to last five years.[461]

There are no fees payable by exporters when applying for licenses. This is of course good news for exporters, but also for the economy and the control regime as a whole, because burdensome or bureaucratic licensing schemes could adversely affect export trade. The principal format for export authorization is the individual license, which is usually in force for a period of one year.[462]

Global authorizations may also be issued to companies which have frequent exports to certain destinations. MTI has imposed *inter alia* the following requirements for recipients of global authorizations: the company must previously have frequently exported dual-use goods, it must have functional internal export controls in place, products must be for civil end-users and for civil end-use purposes. More buyers or recipients can later be added to a global authorization. End use statements obtained from foreign recipients must be sent to MTI one month after the initial export.

From end-user statements the MTI must be able to ascertain the final end use purpose, final end-user and the final destination country, it must also be signed or otherwise approved by the final end-user.[463] A global license is usually valid for two years. The conditions and requirements can be changed later by MTI, also re-export prohibitions or restrictions may be imposed.[464] MTI can also request the exporter to show a so-called import certificate issued by the destination country's export control authority. In intra-EU transfers, an import certificate can be requested only when DUD IV or V goods are concerned (e.g. crypto software). Decisions made by MTI can be appealed to the Supreme Administrative Court. Appeals may be made on grounds that the decision is illegal.[465]

MTI may request information on a legal entity's exports when it sees it fit. Also reporting in electronic form may be introduced to streamline export controls in some cases. Reporting in

[459] Act 562/96 § 4. See page 63.
[460] Act 562/96 § 4.
[461] Decree 645/96 § 5. See also page 71.
[462] *Vientivalvonta* p. 8.
[463] *Vientivalvonta* p. 12 and *Kaksikäyttötuotteiden vientivalvonta*.
[464] *Vientivalvonta* p. 9.
[465] Hallintolainkäyttölaki § 7.

electronic form may be required yearly or even quarterly. Failure to inform MTI is a criminal offence. Penalties are imposed on persons who knowingly or negligently fail to inform MTI when this is required by law. Also violation of DUR is a criminal offence pursuant to DUR Art. 17.[466]

5.1.3 MTI's Garden Variety Licensing Practices When Exporting Cryptographic Software

This chapter covers some aspects of the control regime which affects exporters of strong crypto products. To be eligible for these licenses, the exporting entity must be eligible to receive global authorizations. Because licensing is decided on a case-by-case basis, much remains to be judged on the facts of the individual export and character of the exporter.

When exporting crypto software to EU countries MTI does not usually require end-user statements. This applies only to so-called shrink wrap products which incorporate strong encryption controlled by Wassenaar. For exports to certain non-EU countries listed in DUD Annex II (Australia, Japan, Canada, Norway, Switzerland, New Zealand and the United States) MTI has issued a general export license for civil end-use purposes only (so-called FIN 0). No end-user statements are required for exporting shrink wrap cryptography products incorporating strong encryption.

When exporting to Wassenaar countries not mentioned above MTI may issue a global export license for those countries. The end use statement is usually required from the first line buyer, e.g. distributor. The Ministry will request information when needed. Also, a quarterly report in electronic form once a year is usually required.

Export to other countries which are not Wassenaar countries is usually a little more complicated. Applicable countries are for example India, Pakistan, China or Cuba. The exporting entity can apply for global authorization. The end use statement is required from the first line buyer, e.g. from distributor. Usually also, at MTI's request, in these countries importers undertake not to re-export cryptography products, even though the national export licensing authority could authorize the re-export in question. MTI can impose special reporting requirements in export licensing provisions. Also, a quarterly report in electronic form is usually required.

When exporting crypto products to countries like Libya, North Korea, Iran, Iraq, Sudan, Syria, and any country subject to United Nation's and/or the European Union's total or partial trade sanctions or embargoes, an individual license is the only option possible. The real (final) end-

[466] Rikoslaki 46:9, 46:1-3 and Act 526/96 § 9. See also chapter 4.4.8.

user must be discovered and decisions are taken on case-by-case basis in MTI. The review process may take several weeks from the date of filing the application. MTI usually requires that, if the license is granted, importers and end-users undertake not to re-export cryptography products, even though the national export licensing authority could authorize the re-export in question. Also, a quarterly report in electronic form is usually requested.

5.2 Sweden

5.2.1 Relevant Legislation and National Export Control Authority

Sweden maintains export controls on encryption pursuant to the Wassenaar Arrangement and the EU Dual-Use Regulation. The Swedish Government is committed to maintaining the export controls on cryptography.[467] Export controls are governed by the Strategic Products Act (1991:341) and the Ordinance Relating to Strategic Products (1994:2060). They are drafted much the same way as in Finland, although some differences exist. The licensing authority is the National Inspectorate of Strategic Products (ISP - Inspektionen för strategiska produkter), a component of the Ministry of Foreign Affairs. It was established on February 1st 1996. The objectives of Swedish export controls are as follows: protection of Sweden's security interests; preventing terrorist organizations and organized crime groups from acquiring advanced crypto technology and enabling Swedens's industry to have the latest crypto technology available.[468]

5.2.2 Export Control Procedure

Export of a product included in the Control List requires an authorization from ISP. Anyone wanting to export a cryptographic product from Sweden must submit prior written application to ISP. Three types of licenses exist: general, global and individual. This is of course pursuant to DUR Art. 6. When ISP is considering the application it usually consults the Swedish Ministry of Defence's experts. In crypto matters Försvarets Radioanstalt (FRA) is usually consulted.[469] FRA is an intelligence agency, tasked with SIGINT missions. Authorizations are granted on a case-to-case basis;[470] global and general authorizations seem to be used a little more rarely than in Finland.

When an individual authorization is applied for, ISP requires an end-user statement. Usually it includes the name of the end-user, the name of the relevant product, the purpose of use (end use), re-export restriction (re-export not allowed without Swedish Government's written consent). In special situations it may also include an affirmation from the distributor or from the exporter's subsidiary in the end use country. In unclear situations ISP must be consulted in or-

[467] *Kryptopolitik* p. 149.
[468] *Kryptopolitik* p. 55.
[469] *Kryptopolitik* p. 55.
[470] *Kryptopolitik* p. 57.

der to find out what kind of end-user statement is required. When very sensitive dual-use products are exported ISP may require that the end-user's home country's authorities affirm the end use. ISP can also lay down other terms and conditions for end use, such as requirements concerning physical location or usage of product.[471] For dual-use products a form called "Commitment concerning re-export and peaceful use" is to be used. ISP accepts end-user statements in all Scandinavian languages, English, French and German. If another language is used ISP requires a translation from an authorized translator.

Swedish companies and those who permanently live or have permanently been established in Sweden cannot, without authorization from ISP, enter into a contract which includes transferring abroad the production right for a dual-use product.[472] Also, any change or amendment to these kinds of contracts must usually be authorized.[473]

In the ISP licensing procedure freedom to export is a presumption. This principle is reflected in § 4.1 of the Strategic Products Act, which states that: "Authorization shall be given ... if it does not adversely affect Sweden's foreign, security, or defence policy interests." An authorization is given if there is no evidence of possible military end-use. Only in exceptional situations is the authorization refused. War material export authorizations have a different character, principally prohibiting export without proper authorization from ISP.[474] Cabinet (*Regeringen)* decides case involving important decisions of principle or which are otherwise especially important.[475]

DUD Art. 4 (3) gives Member States the possibility to adopt or maintain national legislation stipulating that the exporter has to notify his authorities where he has grounds for suspecting that the goods concerned are intended, wholly or in part for, WMD-related purposes, and that in such a case the export operation may be made subject to authorization. Sweden has used this possibility. In the Strategic Products Act duty to notify is triggered in the following situations: (a) ISP has in an individual case notified the exporter that some product is or can be used for WMD-related purposes and an authorization from ISP is required; or (b) an exporter who knows that his product can in some individual case be used for WMD-related purposes must notify ISP at once; the ISP decides if an authorization has to be applied for.[476] The exporter can request from ISP prior information about some item's exportability. A positive prior information is not

[471] *Ibid.*
[472] Strategic Products Act § 10.
[473] Strategic Products Act § 11.
[474] *Kryptopolitik* p. 55.
[475] Strategic Products Act § 5.2.
[476] *Lag och förordning* and Strategic Products Act § 7.

an export authorization. It does not liberate the exporter from the duty to apply for an authorization if such is needed.

DUR Art. 19 (2) lays down a bookkeeping requirement. Exporters must keep detailed registers or records of their transactions and keep those records for at least three years from the end of the calendar year in which the export took place. In Swedish national legislation this bookkeeping requirement is extended to last five years.[477]

ISP can also issue global authorizations pursuant to DUR Art. 6 and Ordinance 1999:681 Section 8.[478] Global authorizations are valid for two years. To be eligible to receive a global authorization, an exporter must fulfill the following criteria: knowledge of relevant legislation, functioning internal export control routines and due diligence in bookkeeping of export transactions (fulfilling the 5 year bookkeeping requirement).[479] Global authorizations can be used only in civil end-use situations. The exporter must be able to show to ISP that this is the case. There is no formal requirement to obtain end-user statements, but obtaining these statements may help to document civil end-use. Re-export to countries which are not on the country list in the global authorization in question, is prohibited.

Internal export control routines may be formed in many different ways, depending on the company's business practices. However, ISP requires that the following elements be included: company policy, which is known by personnel dealing with export matters; an internal control organization with responsible persons; a product classification system; end use control system; authorization application procedures in place; and a system to acknowledge suspect inquiries.[480] Swedish customs officials will visit the company premises in order to ascertain these requirements before a global authorization is granted.

Appeals can be made against ISP decisions. They are directed to a general administrative court. From there one can appeal to *kammarrätten*, if an appeal authorization is received.[481]

5.2.3 Licensing Practices Concerning Cryptographic Software

Act 1991:341 was amended on 21st August 1997; new legislation allows PC users to use cryptographic software in their computers, while they are travelling in the EU region, without the need

[477] *Tillståndstyper SP* and Strategic Products Act § 21.
[478] See chapter 4.4.5.1.2 covering global authorizations.
[479] *Tillståndstyper SP.*
[480] *Ibid.*
[481] Strategic Products Act § 29 and Regeringens Proposition 1995/96:31 chapter 9. If a decision is taken in Cabinet appeals are directed to *Regeringsrätten* (Supreme Administrative Court) pursuant to Act 1988:205; it can only judge on law interpretation questions and not factual questions.

to acquire authorization from ISP.[482] Intangible dual-use transfers are controlled,[483] as in Finland. In Sweden there have been no cases when the WA's GSN should have been interpreted.[484]

ISP can issue general authorizations pursuant to Section 8a of the Ordinance Relating to Strategic Products (1994:2060). On 1st July 1999 ISP issued a general authorization for some cryptographic products[485], which came into force on 1st August 1999. According to this authorization mass-market crypto products, i.e. items which fulfill the requirements of WA-LIST Cryptography Note,[486] can be exported to named countries.[487] However in this authorization symmetric cryptographic algorithms not exceeding 128 bits are eligible for export, compared to the categorical 64-bit limit in the Cryptography Note. ISP's general authorizations are published in the Swedish Government's publication called *Tullverkets författningssamling (TFS)*. No applications for authorization are needed in the field covered by a general authorization.

5.3 Germany

5.3.1 National Authority and Relevant Legislation

As a member of Wassenaar and the EU, Germany's export restrictions on encryption follow both regimes. In strategic export control matters the competent national authority is the Federal Export Office (*Bundesausfuhramt* - BAFA). The BAFA is subordinate to the Federal Ministry of Economics and Technology.[488] An influential federal government agency - *Bundesamt für Sicherheit in der Informationstechnik* (BSI)[489] - must also be mentioned here. BSI is very influential and widely consulted in cryptography matters, since it is responsible for the German Government's information security efforts. As far as export controls are concerned, the relevant national statutes are *Außenwirtschaftsgesetz* (AWG) and *Außenwirtschaftsverordnung* (AWV) – German Act and Ordinance on Foreign Economic Relations.[490] The basic freedom of transactions in the field of foreign trade can be restricted only within narrow legal limits.

---

[482] *Ibid*.
[483] *Baker-Hurst* p. 218.
[484] *Kryptopolitik* p. 26.
[485] TFS 1999:40.
[486] See chapter 3.5.1.1.3.
[487] USA, Argentina, Australia, Bahrain, Bangladesh, Brazil, Bolivia, Brunei, Bulgaria, Canada, Chile, Cyprus, Ecuador, Egypt, Estonia, Philippines, United Arab Emirates, India, Indonesia, Iceland, Israel, Japan, Jordan, China, Kuwait, Rep. of Korea, Lithuania, Lebanon, Latvia, Macedonia, Malaysia, Morocco, Mauritius, Mexico, Norway, New Zealand, Oman, Pakistan, Poland, Qatar, Romania, Russia, Saudi-Arabia, Switzerland, Singapore, Slovakia, Slovenia, Sri Lanka, South Africa, Taiwan, Thailand, Czech Republic, Tunisia, Turkey, Ukraine, Hungary, Venezuela, Vietnam.
[488] *Baker-Hurst* p. 145.
[489] BSI was established in December 17, 1990 (*BSI-Errichtungsgesetz*, BGBl. I 1990, S.2834.). It is an offshoot of the German foreign intelligence service (*Bundesnachrichtendienst* or *BND*).
[490] BGBl. I S. 481, April 28, 1961, BGBl. I S.1936, November 22, 1993, amended on December 12, 1995, BAnz. S. 12797.

Appendix AL (*Anlage AL*) to the AWV contains the ”Export Control List” (*Ausfuhrliste*), a list of dual-use goods. It is virtually identical to the list contained in the EU’s DUD. German export control law as it relates to the export of encryption is both highly detailed and depends very much on the facts in each individual case.[491]

5.3.2 Export Authorization Procedure

The Federal Export Office's decision to grant or deny an export license depends on the assessment of intended use, country of destination, purchaser and end-user, type, and in some cases the quantity, of the goods for which a license is required and on the information available about the exporter's reliability. The BAFA requires authorization for the export of dual-use goods, including cryptography, and reviews license applications on a case-by-case basis. The duty to obtain a license is broad enough that it should be assumed that a particular product falls under it, unless the product can be fitted into one of the exceptions.[492]

All license applications for dual use encryption software are referred to the BSI.[493] Typically, BAFA will not issue a general license for cryptographic goods. These restrictions do not apply to generally available software and public domain software and technology pursuant to the General Software Note and the General Technology Note. The controls are administered in an industry-friendly fashion.[494]

AWG § 2.1 states that contracts and activities may be subject to a licensing requirement or may be precluded. AWG § 2.2 contains a proportionality rule, indicating that restrictions shall not exceed what is necessary and that they should interfere as little as possible with the freedom of economic activity. It also states that restrictions may only affect existing contracts if the objectives pursued are seriously threatened. According to AWG § 7.1.2 and § 7.1.3 contracts and activities in the sphere of foreign trade may be curtailed in order to guarantee the security of the Federal Republic of Germany, prevent a disturbance of peaceful coexistence or prevent the external relations of the FRG from being seriously disrupted.

The legal situation can vary greatly depending on the country to which an encryption product is to be exported. While it cannot be said with certainty how long the application for an export license will take in a particular case, the BAFA tries to decide on most license applications for exports to OECD countries within two weeks; exports to non-OECD countries may take consi-

[491] *Baker-Hurst* p. 157.
[492] *Baker-Hurst* p. 159.
[493] *Roth.*
[494] *Baker-Hurst* p. 145.

derably longer, as it may be necessary for the BAFA to consult with various Government ministries. Exports to non-OECD countries often require consultation between the BAFA and other government entities.[495]

The burden of discovering whether a license is needed lies with the exporter.[496] It is sometimes difficult to determine whether an export license is necessary for a particular product. In these cases, the exporter may apply for a *Negativbescheinigung* (NB) (or in more complicated cases *Voranfrage*), which is a legally binding determination by the BAFA that the goods do not fall within the duty to obtain a license. However, the BAFA requires strict proof of the necessary facts before it may issue a NB.[497] While individual licenses and determinations only apply to the particular case for which they have been granted, generally speaking, once one has been granted for a particular good and destination, the BAFA will often rely on it in the future, thus giving the exporter some legal certainty that further exports will be possible.[498] The bit length of the encryption product is not of major importance in the decision whether or not to grant a license.[499]

It should also be noted that under AWV § 4b transmissions of software on-line (intangible transfer) are considered to be exports, which would mean that, for example, the transmission of software with encryption functions over the Internet could be considered an export. However, Germany has fully implemented the General Software Note, so no export licenses need to be obtained for software which is ”freely available”. Since software distributed over the Internet is likely to be regarded as being ”freely available”, no license is generally required for encryption distributed on-line. Under the GSN, samples of encryption may also generally be distributed in trade fairs. However, the BAFA takes the position that it is not applicable to distribution of encryption software with a restricted customer pool, such as software that is merely an add-on to particular hardware, or to complex software which cannot be installed by an unsophisticated end-user.[500]

There are also a number of so-called ”general exceptions” (*allgemeine Genehmigungen*) which allow for the export of products without the necessity of applying for a license in advance. With regard to encryption products, general exceptions N:o 10 (computers) and N:o 16 (telecommunications) are of particular interest, and should be closely examined in each particular case. If

[495] *Baker-Hurst* p. 158.
[496] *Export Controls – Brief Outline* p. 17.
[497] *Roth*.
[498] *Baker-Hurst* p. 161.
[499] *Baker-Hurst* p. 161.
[500] *Baker-Hurst* p. 161.

applicable, these exceptions may free the exporter from the need to obtain a license for exports to most countries, and may also allow the on-line distribution of encryption even in circumstances when it would not fall under GSN. However, there are no ”general licenses” available as may exist in some other countries, so that an export license must generally be obtained for each individual export of encryption.[501]

Pursuant to § 45 AWV, a license is required for the transfer of, not generally accessible knowledge about the production of goods or technologies included in the Export List. Knowledge that is not generally accessible means that it is accessible to a restricted number of persons only.

Instead of applying for several individual licenses, certain exporters may be granted a collective export license. This license permits the export of a group of goods to several consignees.[502] In the case of specific export transactions it is necessary to assign a person responsible for exports. He/she is personally responsible for compliance with the export control regulations and must be a member of the board of directors or executive management.[503] For the transfer of listed goods subject to authorization an end use certificate must be enclosed with the application (AWV § 17). The submission of end use documents is normally not required in bagatelle situations.[504]

The time required for the processing of a license application for dual-use goods to non-sensitive countries is about two weeks. In the case of exports to other countries the processing takes about one month. The processing time of applications for exports, where critical and sensitive cases are involved, may exceed one month. In these cases detailed inquiries and, if necessary, the participation of the competent ministries are required.[505]

All licenses contain certain re-export conditions stating that re-exports require a license by the BAFA. If a good is licensed for a certain end use at a certain destination, change of end use or destination - even within the same country - should trigger the re-export license requirement. The German exporter is not held responsible for change of end use or destinations if he was not aware of this. If he knows that the software is bought for re-export he is supposed to indicate that in his license application. German authorities have no possibility of bringing a foreign company to court for violation of end use. But a new export license application for the same foreign company or similar cases will definitely run into problems.[506]

[501] *Baker-Hurst* p. 161.
[502] *Export Controls – Brief Outline* p. 13.
[503] *Export Controls – Brief Outline* p. 18.
[504] *Export Controls – Brief Outline* p. 19.
[505] *Export Controls – Brief Outline* p. 20.
[506] *Roth*.

§ 7 AWV states, pursuant to DUR 19 (3) (a), that transfers to EU Member States of controlled encryption software or technology which do not require a license for shipments to final destinations within the EU will require a license if the German exporter knows that the final destination of the transfer will be outside the EU. A shipment of decontrolled encryption software for use e.g. in Italy or France or within Germany with the knowledge that the software will be used for criminal purposes does not require an export license but may constitute aiding or abetting of the buyer's crime by the seller of the software.

5.4 France

5.4.1 Overview

As a member of Wassenaar and the European Union, France controls the export as well as the import and use of encryption products. Of EU Member States only France has limited import controls,[507] and it has globally the most comprehensive regulations in place concerning cryptography. French encryption controls are administered by the Service Central de la Sécurité des Systèmes d'Information (SCSSI), Central Service for the Security of Information Systems, an office reporting to the Prime Minister through the Secrétariat Général à la Défense Nationale (SGDN), Secretary General for National Defence. This reflects a general French view that technology and industrial policy are critical elements of national defence.[508]

France has a long history of regulating the use of cryptography. Prior to 1990, France considered cryptographic products “war materials” and generally prohibited their use with some exceptions.[509] As to export controls for dual-use goods, they were introduced in France by a decree of 1944. Since July 1994, export controls for dual-use goods are implemented in accordance with rules defined by a European regime established by DUR and DUD. By means of a national licensing system, France controls exports of goods that are not military equipment but whose export it regards as extremely important in accordance with the European criteria. All actions conducted by France in the field of exports of arms and dual-use goods and technologies thus take place within a regulatory and political framework incorporating the laws and obligations agreed at European and international level. The commitments given by France in respect of

[507] *Koops 2000*. Of EU countries only France controls crypto imports. Use is controlled to a limited extent in France, Italy, Austria and in Belgium (which maintains laws requiring decryption for law enforcement purposes in certain situations.).
[508] *Baker-Hurst* p. 130.
[509] *Baker-Hurst* p. 131.

arms control are an integral part of its export policy which is subject to one of the most stringent national control procedures.[510]

5.4.2 Export Licensing Procedures

The French regime regulating cryptography export is based on Act No. 96-659 and Decree No. 98-101. In those statutes encryption products are classified into three different categories. The first category is products that are not capable of confidentiality. SCSSI requires that a 'declaration' be submitted one month before the export. The second category is key recovery products. The export of those products is controlled by SCSSI in much the same way as products in the first category.

The third category is all remaining crypto products, primarily those providing confidentiality. For export of products that employ encryption to ensure confidentiality, a "prior authorization" must be obtained from SCSSI. As usual, SCSSI may request that the applicant provides technical documentation or copies of the software involved. SCSSI will take a decision within four months of receipt of the completed authorization request, and failure to respond within this time will be deemed an approval. Authorizations can be revoked or abrogated under certain conditions, and, in cases of urgency, may be suspended with immediate effect. In most cases SCSSI is unlikely to approve an "authorization" for a non-key recovery product that uses strong encryption for confidentiality purposes.[511] For the French economy in general and French software developers in particular, this is bad news, because foreign trade is likely to be hampered by SCSSI strictness. Encryption products that are to be exported exclusively for development, validation or demonstration purposes are exempt from the authorization requirements but SCSSI must be notified at least two weeks in advance.

5.5 United Kingdom

5.5.1 National Authority and Relevant Legislation

UK export control is imposed by statutory instruments made either under the Import, Export and Customs Powers (Defence) Act 1939 or under the European Communities Act 1972 pursuant to the requirements of the DUR. The 1939 Act does not specify or limit the purposes for which its powers may be used. The licensing authority is the Export Control Organization of the Department of Trade and Industry.

[510] *La Politique Française de Contrôle des Exportations d'Armements et de Biens et Technologies à Double Usage* p. 3.
[511] *Baker-Hurst* p. 133.

5.5.2 Authorization Procedure

It is a criminal offence to export goods specified in the controlled lists from the UK without a license. The controls apply only to goods, i.e. tangible physical property. The 1939 Act gives no power to impose any wider controls. Where the controls apply to software, therefore, they apply only to software embodied in some tangible medium, such as an application-specific integrated circuit, a CD or a listing on paper of source code or machine code.[512] However, there are provisions covering the export of technology by intangible means contained in the United Nations Act 1946, Official Secrets Act 1989 and the Patents Act 1977 and legislation under these Acts. Where this is the case, the exporter is not totally free from obligations. The Government is well aware of the scope for abuse in this area and would discourage any undermining of the controls through transmission by electronic or other intangible means.[513]

Goods subject to control on cryptographic grounds may not be exported from the UK to any destination without a license (inside or outside the EU). Licenses are granted more readily, and with fewer conditions (relating to the scope of permitted use by the end-user, for example), for exports to other Member States of the European Community or to Australia, Canada, Japan, New Zealand, Norway, Switzerland or the United States of America pursuant to DUR and DUD Annex II.

An export license may be obtained by applying to the DTI. In practice, however, UK vendors of crypto goods also send a fax of their applications to the Communications and Electronics Security Group (CESG), simultaneously with the transmittal of the application to DTI so as to speed up the decision-making process. CESG is part of GCHQ, the UK's NSA equivalent, but has a separate identity to facilitate work with unclassified commercial entities. CESG reviews the application and advises DTI of its view. In practice, DTI generally follows the CESG recommendation and does not approve an export item that CESG finds unacceptable.[514]

There are four main types of license: Standard Individual Export Licences (SIELs), Open Individual Export Licences (OIELs), Special categories of OIELs and Open General Export Licences (OGELs).[515] Standard Individual Export Licences (SIELs) generally allow shipments of specified goods to a specified consignee up to the quantity specified by the license. Such licenses are generally valid for two years where the export will be permanent; where the export is temporary, for example for the purposes of demonstration, trial or evaluation, the license is ge-

[512] *Strategic Export Controls: Impact on Cryptography.*
[513] *Export Controls: A Guide for Business: Supplementary Guidance Notes.*
[514] *Cryptography and Liberty 1999.*
[515] *Annual Report on Strategic Export Controls* p. 7.

nerally valid for one year only and the goods must be returned before the license expires.[516] An Open Individual Export Licence (OIEL) is specific to an individual exporter and covers multiple shipments of specified goods to specified destinations and/or, in some cases, specified consignees. OIELs are generally valid for three years.[517] Open General Export Licences (OGELs) allow the export of specified controlled goods by any company, removing the need for exporters to apply for an individual license, provided the shipment and destinations are eligible and the conditions are met. Exporters must register with the Export Control Organisation before they make use of most OGELs. All Open General Licences remain in force until they are revoked.[518] The DTI seem not to have issued OGELs for any significant crypto products. On January 28 1998, the DTI authorized an OGEL for personal computers accompanying their users that contain encryption. On-line voice encryption and decryption programs are not covered by the special permit.[519] The Export Control Organisation also responds to requests from exporters for advice on whether or not a license is required to export particular goods of which the exporter has provided full technical details.[520]

In almost all circumstances, the application form must be accompanied by an appropriate end-user undertaking.[521] These must be drafted in English or, if written in a foreign language it must be accompanied by an English translation. English translations must be verified by the proprietor of the company applying for a license, or a partner, director or company secretary of that firm, or by a member of the Institute of Translators, or a Notary Public.[522]

A license may or may not be issued. Among the factors taken into account will be the destination, the parties involved and the nature of the goods or technology concerned, and the use to which they could be put. If application is refused an appeal can be made. An appeal must be written to the ECO within 28 days of receiving the refusal letter.[523]

[516] *Do I Need a Licence?* p. 2.
[517] *Annual Report on Strategic Export Controls* p. 100.
[518] *Annual Report on Strategic Export Controls* p. 124.
[519] *Cryptography and Liberty 1999.*
[520] *Annual Report on Strategic Export Controls* p. 126.
[521] *SIEL* p. 1.
[522] *SIEL* p. 2.
[523] *Do I Need a Licence?* p. 3.

APPENDIX 1

RELEVANT PORTIONS OF THE WA-LIST

GENERAL TECHNOLOGY NOTE AND GENERAL SOFTWARE NOTE

DUAL-USE LIST – CATEGORY 5 PART 2 – ”INFORMATION SECURITY”

STATEMENTS OF UNDERSTANDING AND VALIDITY NOTES

DUAL-USE LIST

Note *Terms in "quotations" are defined terms. Refer to 'Definitions of Terms used in these Lists' annexed to this List.*

GENERAL TECHNOLOGY NOTE

The export of "technology" which is "required" for the "development", "production" or "use" of items controlled in the Dual-Use List is controlled according to the provisions in each Category. This "technology" remains under control even when applicable to any uncontrolled item.

Controls do not apply to that "technology" which is the minimum necessary for the installation, operation, maintenance (checking) and repair of those items which are not controlled or whose export has been authorised.

N.B. *This does not release such "technology" controlled in entries 1.E.2.e. & 1.E.2.f. and 8.E.2.a. & 8.E.2.b.*

Controls do not apply to "technology" "in the public domain", to "basic scientific research" or to the minimum necessary information for patent applications.

GENERAL SOFTWARE NOTE

The Lists do not control "software" which is either:

1. Generally available to the public by being:

    a. Sold from stock at retail selling points without restriction, by means of:
        1. Over-the-counter transactions;
        2. Mail order transactions; or
        3. Telephone call transactions; and

    b. Designed for installation by the user without further substantial support by the supplier; or

    N.B. *Entry 1 of the General Software Note does not release "software" controlled by Category 5 - Part 2.*

2. "In the public domain".

Part 2 - "INFORMATION SECURITY"

Note 1 *The control status of "information security" equipment, "software", systems, application specific "electronic assemblies", modules, integrated circuits, components or functions is determined in Category 5, Part 2 even if they are components or "electronic assemblies" of other equipment.*

Note 2 *Category 5 – Part 2 does not control products when accompanying their user for the user's personal use.*

Note 3 *Cryptography Note*

5.A.2. and 5.D.2. do not control items that meet all of the following:

a. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
   1. Over-the-counter transactions;
   2. Mail order transactions;
   3. Electronic transactions; or
   4. Telephone call transactions;

b. The cryptographic functionality cannot easily be changed by the user;

c. Designed for installation by the user without further substantial support by the supplier;

d. Does not contain a "symmetric algorithm" employing a key length exceeding 64 bits; and

e. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs a. to d. above.

Technical Note

In Category 5 - Part 2, parity bits are not included in the key length.

5. A. 2. SYSTEMS, EQUIPMENT AND COMPONENTS

a. Systems, equipment, application specific "electronic assemblies", modules and integrated circuits for "information security", as follows, and other specially designed components therefor:

N.B. *For the control of global navigation satellite systems receiving equipment containing or employing decryption (i.e. GPS or GLONASS), see 7.A.5.*

5. A. 2. a. 1. Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature having any of the following:
Technical Notes
1. Authentication and digital signature functions include their associated key management function.
2. Authentication includes all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorised access.
3. "Cryptography" does not include "fixed" data compression or coding techniques.

Note *5.A.2.a.1. includes equipment designed or modified to use "cryptography" employing analogue principles when implemented with digital techniques.*

5. A. 2. a. 1. a. A "symmetric algorithm" employing a key length in excess of 56 bits; or
b. An "asymmetric algorithm" where the security of the algorithm is based on any of the following:
1. Factorisation of integers in excess of 512 bits (e.g., RSA);
2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
3. Discrete logarithms in a group other than mentioned in 5.A.2.a.1.b.2. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);

2. Designed or modified to perform cryptanalytic functions;

3. Deleted;

4. Specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;

5. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, including the hopping code for "frequency hopping" systems;

6. Designed or modified to provide certified or certifiable "multilevel security" or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) or equivalent;

7. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion.

Note *5.A.2. does not control:*

a. "Personalised smart cards" where the cryptographic capability is restricted for use in equipment or systems excluded from control under entries b. to f. of this Note. If a "personalised smart card" has multiple functions, the control status of each function is assessed individually.

b. Receiving equipment for radio broadcast, pay television or similar restricted audience broadcast of the consumer type, without digital encryption except that exclusively used for sending the billing or programme-related information back to the broadcast providers;

c. Equipment where the cryptographic capability is not user-accessible and which is specially designed and limited to allow any of the following:
1. Execution of copy-protected software;
2. Access to any of the following:
a. Copy-protected read-only media; or
b. Information stored in encrypted form on media (e.g. in connection with the protection of intellectual property rights) when the media is offered for sale in identical sets to the public; or
3. One-time copying of copyright protected audio/video data.

d. Cryptographic equipment specially designed and limited for banking use or money transactions;
Technical Note
'Money transactions' in 5.A.2. Note d. includes the collection and settlement of fares or credit functions.

e. Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radiocommunications systems) that are not capable of end-to-end encryption;

f. Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (i.e., a single, unrelayed hop between terminal and home basestation) is less than 400 metres according to the manufacturer's specifications.

5. B. 2. TEST, INSPECTION AND PRODUCTION EQUIPMENT

a. Equipment specially designed for:

1. The "development" of equipment or functions controlled by Category 5 - Part 2, including measuring or test equipment;
2. The "production" of equipment or functions controlled by Category 5 - Part 2, including measuring, test, repair or production equipment.

b. Measuring equipment specially designed to evaluate and validate the "information security" functions controlled by 5.A.2. or 5.D.2.

5. C. 2. MATERIALS - None

5. D. 2. SOFTWARE

a. "Software" specially designed or modified for the "development", "production" or "use" of equipment or "software" controlled by Category 5 - Part 2;
b. "Software" specially designed or modified to support "technology" controlled by 5.E.2.;
c. Specific "software", as follows:
   1. "Software" having the characteristics, or performing or simulating the functions of the equipment controlled by 5.A.2. or 5.B.2.;
   2. "Software" to certify "software" controlled by 5.D.2.c.1.

Note *5.D.2. does not control:*
a. "Software" required for the "use" of equipment excluded from control under the Note to 5.A.2.;
b. "Software" providing any of the functions of equipment excluded from control under the Note to 5.A.2.

5. E. 2. TECHNOLOGY

a. "Technology" according to the General Technology Note for the "development", "production" or "use" of equipment or "software" controlled by Category 5 - Part 2.

STATEMENTS OF UNDERSTANDING AND VALIDITY NOTES

MUNITIONS LIST

ML 10 (NF (95) WG2/2)

Absence of items from the Munitions List and absence of configuration for military use would mean that an aircraft would not be considered military.

DUAL-USE LIST OF GOODS AND TECHNOLOGIES

General Technology Note (NF (95) CA WP 1)

Governments agree that the transfer of "technology" according to the General Technology Note, for "production" or "development" of items on this list shall be treated with vigilance in accordance with national policies and the aims of this regime.

General Technology Note (WG2 GTN TWG/WP1 Revised 2)

It is understood that Member Governments are expected to exercise controls on intangible "technology" as far as the scope of their legislation will allow.

General Software Note (NF (95) CA WP 1)

Governments agree that the transfer of "software", for "production" or "development" of items on this list shall be treated with vigilance in accordance with national policies and the aims of this regime.

Statement of Understanding - medical equipment (NF (96) DG PL/WP1)

Participating countries agree that equipment specially designed for medical end-use that incorporates an item controlled in the Dual-Use List is not controlled.

Category 2

2.B.1.

Validity Note 2.B.1. is valid until 5 December 2000 and renewal of the agreed parameters will require unanimous consent.

2.E.3.f.

Validity Note The control of diamond-like carbon technology in 2.E.3.f. is valid until 1 December 2000 and its renewal for an additional one-year period will require unanimous consent.

Category 4

4.A.3.b.

Statement of Understanding

Governments agree to review 4.A.3.b. six months after the date of entry into force of the amendments to the List of Dual-Use Goods and Technologies, taking into account, inter alia, relevant acquisition patterns and transfer data.

4.D.3.b.

Validity Note 4.D.3.b. is valid until 1 November 2000 and its renewal for each successive two-year period will require unanimous consent.

Category 5, Part 2

Validity Note Cryptography Note, paragraph d., as it applies to "software", is valid until 3 December 2000, and renewal for a successive period will require the unanimous consent of participating countries.

Statement of Understanding

Governments agree to review the parameters of 5.A.2.a.1.a. and 5.A.2.a.1.b., in conjunction with the review of the parameter of paragraph d. of the Cryptography Note, not later than 3 December 2000.

Category 9

9.E.2.

Statement of Understanding

"Development" or "production" "technology" controlled by 9.E. for gas turbine engines remains controlled when used as "use" "technology" for repair, rebuild and overhaul. Excluded from control are: technical data, drawings or documentation for maintenance activities directly associated with calibration, removal or replacement of damaged or unserviceable line replaceable units, including replacement of whole engines or engine modules.

ANNEX 1

4.A.3.b.
Statement of Understanding

Governments agree to review 4.A.3.b. six months after the date of entry into force of the amendments to the List of Dual-Use Goods and Technologies, taking into account, inter alia, relevant acquisition patterns and transfer data.

DEFINITION OF TERMS USED IN THESE LISTS

Statement of Understanding

Participating States note that, in these Lists, words and terms appearing under 'Definitions of Terms used in these Lists', if used in their undefined forms, take their common or dictionary meanings. Governments are expected to preserve these distinctions, as far as national languages and legislation allow, when the Lists are translated into national legislation.
(See also Note 2 to 'Definitions of Terms used in these Lists').

N.B. *The references in this section refer to the List of Dual-Use Goods and Technologies and the Munitions List approved by the Plenary Meeting in Vienna on 1st to 3rd December 1999.*