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.