ETSI TR 103 306 V1.4.1 (2020-03)

CYBER;
Global Cyber Security Ecosystem

Reference

RTR/CYBER-0051

Keywords

cybersecurity, ecosystem

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document is a basic reference document for undertaking the responsibilities, areas of activity, organization and working methods enumerated in the Terms of Reference for Cyber Security Technical Committee. Cyber security is inherently diverse, dynamic, and spread across a complex array of bodies and activities worldwide, and constitutes a specialized ecosystem. The Committee's effectiveness is predicated in large measure by constantly discovering, analysing, and understanding the diverse requirements and work occurring in this ecosystem in some kind of structured fashion. The present document should also be useful to the many constituents that are part of the cyber security ecosystem.

The present document attempts to discover and assemble enumerated lists in alphabetic order of global cyber security constituents. It attempts to be as inclusive as possible to expand collective insight into the extent and diversity of the ecosystem:

- Fora that develop techniques, technical standards and operational practices.
- Major IT developer forums affecting cyber security.
- Activities for continuous information exchange.
- Global and national centres of excellence.
- Reference libraries, continuing conferences, and publications.
- Heritage sites and historical collections.

The present document is augmented by annex A which contains national cyber security ecosystems that have been published in national cyber security strategies and publicly available material.

Where groups exist within a common organization, they are grouped together. Only brief summaries of bodies are included, and available URLs are provided for further information. Where the body or activity is significantly associated with a national or regional government, that relationship forms the basis of the alphabetic order.

The present document also includes an extensive list of acronym abbreviations and an annex of use cases of the relationships among the different groups.

This ecosystem changes constantly, so URIs provide links to the activities for the latest information. The present document may also be implemented on the ETSI website to allow continuing maintenance both by the ETSI Secretariat research, outreach and cooperation with the included forums.

Introduction

Cyber security consists of a continuing cycle of structured actions to:

- Identify (understand state and risks to systems, assets, data, and capabilities)
- Protect (implement the appropriate safeguards)
- Detect (implement ability to identify a cybersecurity event)
- Respond (implement ability to take action following a cybersecurity event)
- Recover (implement resilience and restoration of impaired capabilities)

All of these activities rely on the trusted, timely sharing of related structured information. See figure 1.

Almost every provider or major user of information or communication of products and services today is involved in a large array of bodies and activities advancing these actions and constitutes a cyber security ecosystem at global regional, national, and local levels down small business, households and individuals.

All those involved in the ecosystem seek solutions to protect the integrity and availability of their communications and information to the extent that is feasible and within cost constraints. As is apparent from the present document, there is so much information and activity, it has created what one notable security community leader describes as "a fog of more". Indeed, some of the activities now ongoing are dedicated to distilling and prioritizing the techniques and mechanisms that have been produced by other groups.

There are so many cyber security activities occurring today in diverse, frequently insular industry, academic, and government groups, that it is beyond the comprehension of any single person's or group's ability to discover and understand them all. The existence of an ecosystem living document in the form of the present document that is structured, regularly updated, and collectively maintained by everyone helps itself to strengthen cyber security.

Especially significant is the recent publication of a large array of formal national cyber security strategy plans and related material in countries worldwide which describe individual national ecosystems that are profiled in annex A. Discovering and providing a common structured understanding of these national ecosystems is ultimately essential to global cyber security work such as that of the Technical Committee for Cyber Security.

Figure 1: Basic components of the cyber security ecosystem

1 Scope

The present document provides a structured overview of cyber security work occurring in multiple other technical forums worldwide. The overview includes global identification of Cyber Security Centres of Excellence, heritage sites, historical collections, and reference libraries. It is intended to be continuously updated to account for the dynamics of the sector.

NOTE: This version is the last publication as Technical Report. The content of the present document is transferred to a wiki available at https://cyberpublicwiki.etsi.org/ and any update will be reflected on the wiki only.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Recommendation ITU-T X.1205 (04/2008): "Overview of cybersecurity".

[i.2] ISO/IEC JTC-1 SC 27: "Standing Document 6 (SD6): Glossary of IT Security Terminology", N12806 (2013.10.03).

[i.3] NIST SP 800-70: "National Checklist Program for IT Products: Guidelines for Checklist Users and Developers".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

centre of excellence: educational or research & development organization recognized as a leader in accomplishing its cyber security mission

cyber environment: users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks [i.1]

cyber security (or cybersecurity): collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets

NOTE: Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability.
- Integrity, which may include authenticity and non-repudiation.
- Confidentiality [i.1].

cybersecurity: preservation of confidentiality, integrity and availability of information in the Cyberspace [i.2]

cyberspace: complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form [i.2]

heritage site: place (such as a building or complex) that is listed by a recognized accrediting body as a place where significant cyber security innovations occurred

historical collection: place, both real and virtual, dedicated to the structured gathering and availability of cyber security materials of historical significance; frequently denominated as a museum

information exchange mechanism: real or virtual activity established for providing continuing structured exchange of cyber security information content

reference library: collection of available published material useful for consultation for cyber security purposes

NOTE: The present document also includes significant dedicated publications in this category.

techniques, technical standards and operational practices forum: any continuing body established for the purposes of reaching agreement on techniques, technical standards or operational practices for enhancing cyber security

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

NOTE: Not all abbreviations are used in the present document. Some are included purposely to provide a unique global reference set of cyber security abbreviations.

3GPP	3rd Generation Partnership Project
A*STAR	Agency for Science, Technology and Research (Singapore)
ABW	Agencja Bezpieczenstwa Wewnetrznego (Poland)
AC	Authentication Code (TCG)
ACDC	Advanced Cyber Defence Centre
ACE-CSR	Academic Centres of Excellence in Cyber Security Research (UK)
ACI	Austrian Critical Infrastructure (Austria)
ACI	Österreichische kritische Infrastruktur (Austria)
ACMA	Australian Communications and Media Authority (Australia)
ACSS	Austrian Cyber Security Strategy (Austria)
ADCC	Algemene Directie Crisiscentrum (Belgium)
ADIV	Algemene Dienst Inlichting en Veiligheid (Belgium)
AEPD	Spanish Data Protection Agency (Spain)
AFNOR	Association Française de Normalisation (France)
AFP	Australian Federal Police (Australia)

AGCOM	Autorità per le Garanzie nelle Comunicazioni (Italy)
AGIMO	Australian Government Information Management Office (Australia)
AIK	Attestation Identity Key (TCG)
AIOTI	Alliance of IOT Innovation
AISI	Australian Internet Security Initiative (Australia)
AMSS	Anti-Malware Support Services Working Group (IEEE)
ANS	Autorité Nationale de Sécurité (Belgium)
ANSAC	ASEAN Network Security Action Council
ANSES	Ambient Network Secure Eco System (Singapore)
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (France)
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (Luxembourg)
APCERT	Asia Pacific Computer Emergency Response Team (Japan)
APCIP	Austrian Programme for Critical Infrastructure Protection (Austria)
APCIP	Österreichisches Programm zum Schutz kritischer Infrastruktur (Austria)
APT	Advanced Persistent Threat
ARCSI	Association des Réservistes du Chiffre et de la Sécurité de l'Information (France)
ARF	Assessment Results Format or Asset Reporting Format
ARIB	Association of Radio Industries and Businesses (Japan)
ASD	Australian Signals Directorate (Australia)
ASEAN CERT	Association of Southeast Asian Nations CERT
ASIO	Australian Security Intelligence Organisation (Australia)
A-SIT	Secure Information Technology Centre - Austria (Austria)
A-SIT	Zentrum für sichere Informationstechnologie - Austria (Austria)
ASS	Austrian Security Strategy (Austria)
ATIS	Alliance for Telecommunications Industry Solutions
ATT&CK™	Adversarial Tactics Techniques and Common Knowledge (MITRE)
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Germany)
BBK	Biuro Badan Kryminalistycznych (Poland)
BCM	Business Continuity Management (Germany)
BCSS	Banque Carrefour de la Sécurité Sociale (Belgium)
Belac	Organisme belge d'accréditation (Belgium)
Belac	Belgische accreditatie-instelling (Belgium)
Belnet	Belgian national research network (Belgium)
BelNIS	Belgian Network Information Security (Belgium)
BEREC	Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelin (Finland)
BEREC	Body of European Regulators for Electronic Communications (Norway)
BfV	Bundesamt für Verfassungsschutz (Germany)
BLOB	Binary Large OBject (TCG)
BIPT	Belgisch Instituut voor Postdiensten en Telecommunicatie (Belgium)
BIS	Department for Business, Innovation and Skills (UK)
BMI	Bundesministerium des Innern (Germany)
BORE	Break Once Run Everywhere (TCG)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Germany)
BSI	British Standards Institute (UK)
BYOD	Bring Your Own Device
C3	Computer Competence Certificate (Egypt)
C3	Cybersecurity Competence Center (Luxembourg)
CA	Certification Authority
CA/B	Certificate of Authority/Browser Forum
CACAO	Collaborative Automated Course of Action Operations (OASIS)
CAE	Centers of Academic Excellence (UK)
CAK	Communications Authority of Kenya (Kenya)
CAN	Computer Network Attack (Italy)
CAPEC	Common Attack Pattern Enumeration and Classification
CASES	Cyberworld Awareness and Security Enhancement Services (Luxembourg)
CBM	Confidence Building Measures
CBPL	Commissie voor de Bescherming van de Persoonlijke Leverssfeer (Belgium)
CCC	Chaos Computer Club
CCDB	Common Criteria Development Board
CCDCOE	NATO Cooperation Cyber Defence Center of Excellence
CCE	Common Configuration Enumeration
CCIP	Centre for Critical for Infrastructure Protection (New Zealand)

CCIRC	Canadian Cyber Incident Response Centre (Canada)
CCN	National Cryptologic Centre (Spain)
CCN-CERT	Spanish Government National Cryptologic Center - CSIRT (Spain)
CCRA	Common Criteria Recognition Agreement
CCSA	China Communications Standards Association
CCSB	Centre pour Cyber Securité Belgique (Belgium)
CCSB	Centrum voor Cyber Security Belgie (Belgium)
CD	Cyber Defense
CDT	Centres for Doctoral Training (UK)
CDU	Cyber Defence Unit of the National Armed Forces (Latvia)
CEEE	Common Event Expression Exchange
CEN	Comité Européen de Normalisation
CENELEC	European Committee for Electrotechnical Standardization
CEPOL	European POLice College
CERT	Computer Emergency Response Team (Belgium)
CERT Poland	(Poland)
CERT.at	Computer Emergency Response Team - Austria (Austria)
CERT.GOV.PL	Governmental Computer Security Incident Response Team (Poland)
CERT.GOV.PL	Rzadowego Zespolu Reagowania na Incydenty Komputerowe (Poland)
CERT.LU	Grouping of all Luxembourg CERTs
CERT.LY	Information Technology Security Incident Response Institution (Latvia)
CERT-AU	CERT Australia (Australia)
CERT-EU	CERT Europe
CERT-FR	CERT France
CERT-in	National Level Computer Emergency Response Team (India)
CERT-LT	National Electronic Communications Network and Information Security Incidents Investigation Service (Lithuania)
CERT-PA	Computer Emergency Response Team of the Public Administration (Italy)
CERT-PA	CERT - Pubblica Amministrazione (Italy)
CERT-SA	CERT Saudi Arabia (Saudi Arabia)
CERT-SI	Computer Emergency Response Team for Security and Industry (Spain)
CERT-SPC	CERT Sistema Pubblico de Connettività (Italy)
CERT-UK	CERT United Kingdom
CERT-US	CERT United States
CESG	Communications-Electronics Security Group (UK) (now NCSC)
CFRG	Crypto Forum Research Group
CHOD	Chief of Defence (Netherlands)
CI	Critical Infrastructure
CIC	Critical Infrastructure Council (Saudi Arabia)
CII	Critical Information Infrastructures (Austria)
CII	Kritische Informationsinfrastrukturen (Austria)
CIIP	Critical Information Infrastructure Protection
CII-SA	Critical Infocomm Infrastructure Security Assessment (Singapore)
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPMA	Critical Infrastructure Protection Modelling and Analysis (Australia)
CIRCL	The Computer Incident Response Center Luxembourg
CIRT	Computer Incident Response Team
CIS	Center for Internet Security
CISA	Civilian Intelligence Service (Switzerland)
CISA	Cybersecurity and Infrastructure Security Agency (US)
CiSP	Cyber-security Information Sharing Partnership (UK)
CISR	Comitato interministeriale per la sicurezza della Repubblica (Italy)
CloudAuthZ	Cloud Authorization (OASIS)
CMK	Certified Migration Key (TCG)
CMRS	Comité Ministériel du Renseignement et de la Sécurité (Belgium)
CN	subcommittee on Core Network (3GPP)
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastructure Critiche (Italy)
CNC	National Cyber Security Council (Spain)
CNCERT/CC	National Computer Network Emergency Response Technical Team/Coordination Center (China)
CND	Computer Network Defence (Italy)
CNDP	National Commission for Data Protection (Morocco)

CNE	Computer Network Exploitation (Italy)
CNI	National Intelligence Centre (Spain)
CNIP	Critical National Infrastructure Protection Program (Jordan)
CNO	Computer Network Operations (Italy)
CNO	Computer Network Operations (Switzerland)
CNPIC	National Centre for Critical Infrastructure Protection (Spain)
CNSS	Committee on National Security Systems (USA)
COMCYBER	Commandement de cyberdéfense (France)
CONNECT	Directorate on Communications Networks, Content and Technology (EC)
COSC	Consiliul Operativ de Securitate Cibernetica (Romania)
CPB	Constitution Protection Bureau (Latvia)
CPE	Common Platform Enumeration
CNPD	Commission Nationale pour la Protection des Données (Luxembourg)
CPNI	Centre for the Protection of National Infrastructure (UK)
CPS	Cyber Physical System (Italy)
CPVP	Commission de la Protection de la Vie Privée (Belgium)
CRP	Cyberprzestrzen Rzeczypospolitej Polskiej (Poland)
CRTM	Core Root of Trust for Measurement (TCG)
CSA	Cloud Security Association
CSAF	Common Security Advisory Framework (OASIS)
CSBM	Confidence and Security Building Measures (Italy)
CSBN	Cyber Security Beeld Nederland (Netherlands)
CSC	Council on Cyber Security (now the Centre for Internet Security)
CSCG	Cyber Security Coordination Group
CSCP	Cyber Security Cooperation Program (Canada)
CSEC	Communications Security Establishment Canada (Canada)
CSIAC	Cyber Security and Information Systems Information Analysis Center (USA)
CSIRT	Computer Security Incident Response Team (South Africa)
CSIRT.SK	National centre for computer security incidents.Slovakia (Slovakia)
CSIS	Canadian Security Intelligence Service (Canada)
CSN	National Security Council (Spain)
CSO	Armed Forces Command Support Organisation (Switzerland)
CSOC	Cyber Security Operations Centre (Australia)
CSOC	National Cyberspace Security Operations Centre (Jordan)
CSOC	National Cyber Security Operations Centre (Netherlands)
CSPC	Cyber Security Policy and Coordination Committee (Australia)
CSSC	Control System Security Centre (Japan)
CSSF	Commission de Surveillance du Secteur Financier (Luxembourg)
CTI	Cyber Threat Intelligence (OASIS)
CTWIN	Critical Infrastructure Warning Information Network (Lithuania)
CVE	Common Vulnerabilities and Exposures
CVE-ID	CVE IDentifier
CVRF	Common Vulnerability Reporting Format
CVSS	Common Vulnerability Scoring System
CWC	Cyber Watch Centre (Singapore)
CWE	Common Weakness Enumeration
CWRAF	Common Weakness Risk Analysis Framework
CWSS	Common Weakness Scoring System
CYBER	Cybersecurity Technical Committee (ETSI)
CYBEX	Cybersecurity Information Exchange (ITU-T)
CybOX	Cyber Observable Expression
CYCO	Cybercrime Coordination unit Switzerland (Switzerland)
CYIQL	Cybersecurity Information Query Language
DAA	Direct Anonymous Attestation (TCG)
DCE	Dynamic root of trust for measurement Configuration Environment (TCG)
DCEC	Defence Cyber Expertise Centre (Netherlands)
D-CRTM	Dynamic Core Root of Trust for Measurement (TCG)
DDoS	Distributed Denial of Service
DDPS	Federal Department of Defence, civil Protection and Sport (Switzerland)
DeitY	Department of electronics & information technology (India)
DETEC	Federal Department of Environment, Transport, Energy and Communications (Switzerland)
DF	Digital Forensics (Italy)

DGCC	Direction Générale Centre de Crise (Belgium)
DGSE	Direction Générale de la Sécurité Extérieure (France)
DHS	Department of Homeland Security (USA)
DIGIT	Directorate on Informatics (EC)
DIN	Deutsches Institut für Normung
DISS	Defence Intelligence and Security Service (Latvia)
DISS	Defence Intelligence and Security Service (Netherlands)
DL	Dynamic Launch (TCG)
DLME	Dynamically Launched Measured Environment (TCG)
DNS	Domain Name System
DoC	Department of Communications (South Africa)
DOD	Department Of Defence (Australia)
DoD&MV	Department of Defence and Military Veterans (South Africa)
DOJ&CD	Department Of Justice and Constitutional Development (South Africa)
DoS	Denial of Service
dots	DDoS open threat signaling (IETF)
DRDC	Defence Research and Development Canada (DRDC)
DRSD	Direction du Renseignement et de la Sécurité de la Défense (France)
D-RTM	Dynamic Root of Trust Measurement (TCG)
DSD	[See ASD] (Australia)
DSG	Federal Act on Data Protection (Switzerland)
DSI	Data State Inspectorate (Latvia)
DSN	National Security Department (Spain)
DSS-X	Digital Signature Services eXtended (OASIS)
DST	Department of Science and Technology (South Africa)
E2NA	End-to-End Network Architectures (ETSI)
EAP	Extensible Authentication Protocol
EAPC	Euro-Atlantic Partnership Council (Switzerland)
EBIOS	Expression of Needs and Identification of Security Objectives
EC	European Commission
ECI	European Critical Infrastructure
EI-ISAC	Elections Infrastructure Information Sharing and Analysis Center
ECRG	Electronic Communications Reference Group (EC)
EMAD	Chiefs of the Defence Staff (Spain)
ENFSI	European Network of Forensic Institutes
ENISA	European Network and Information Security Agency
EOC	Electronic Operations Centre (Switzerland)
EPCIP	European Programme for Critical Infrastructure Protection
ESA	European Space Agency (Belgium)
ESI	Electronic Signatures and Infrastructures (ETSI)
ESPCERTDEF	Computer Emergency Response Team in the field of the Ministry of Defence (Spain)
ESRIM	European Security Research & Innovation forum
ETI	Encrypted Traffic Inspection working group (IEEE)
ETSI	European Telecommunication Standards Institute
EU	European Union
EU CSS	EU CyberSecurity Strategy (EU)
Europol	European Police Office
EVCERT	Extended Validation Certificate
FASG	GSM Association Fraud and Security Working Group
FCC	Federal Communications Commission (USA)
FCCU	Federal Computer Crime Unit (Belgium)
FCMC	Financial and Capital Market Commission (Latvia)
FCP	Federal Criminal Police (Switzerland)
FDEA	Federal Department of Economic Affairs (Switzerland)
FDF	Federal Department of Finance (Switzerland)
FDJP	Federal Department of Justice and Police (Switzerland)
FDPIC	Federal Data Protection and Information Commissioner (Switzerland)
Fedict	FOD voor informatie-en communicatietechnologie (Belgium)
Fedoct	SPF Technologie de l'Information et de la Communication (Belgium)
fedpol	federal office of police (Switzerland)
FIA	Federal Investigation Agency (Pakistan)
FIC	Forum International de la Cybersécurité (Europe)

FICORA	Finnish COmmunications Regulatory Authority (Finland)
FIDO	Fast IDentity Online
FIPS	Federal Information Processing Standards (USA)
FIRST	Forum of Incident Response and Security Teams
FIS	Federal Intelligence Service (Switzerland)
FISMA	Federal Information Security Management Act (USA)
FITO	Federal IT Ordinance (Switzerland)
FITSU	Federal IT Steering Unit (Switzerland)
FOCA	Federal Office of Civil Aviation (Switzerland)
FOCP	Federal Office for Civil Protection (Switzerland)
FOD	Federal OverheiDsdienst (Belgium)
FOITT	Federal Office of Information Technology, systems and Telecommunication (Switzerland)
FONES	Federal Office for National Economic Supply (Switzerland)
FS-ISAC	Financial Services Information Sharing and Analysis Centre
GFCE	Global Forum on Cyber Expertise
GCHQ	Government Communications HeadQuarters (UK)
GISS	General Intelligence and Security Service (Netherlands)
GovCERT	CERT gouvernemental du Grand-Duché de Luxembourg
GovCERT	Governmental Computer Emergency Response Team (Austria)
GovCERT	Staatliches Computer Emergency Response Team (Austria)
GovCERT	Government Computer Emergency Response Team (Switzerland)
GovCERT.au	Australian Government's Computer Emergency Readiness Team (Australia)
GROW	Directorate on Internal Market, Industry, Entrepreneurship and SMEs (EC)
GSA	Government Services Administration (USA)
GSMA	GSM Association
GSS	Government Security Secretariat (UK)
H2020	Horizon 2020
HCPN	Haut-Commissariat à la Protection Nationale (Luxembourg)
Healthnet CSIRT	Healthsector CERT (Luxembourg)
HOME	Directorate on Migration and Home Affairs (EC)
HR	Directorate on Human Resources and Security (EC)
i2nsf	interface to network security functions (IETF)
IA	Information Assurance
IAAGs	Infrastructure Assurance Advisory Groups (Australia)
IAB	Internet Architecture Board
IAD	Information Assurance Directorate (USA)
IANA	Internet Assigned Numbers Authority
IBPT	Institut Belge des services Postaux et des Télécommunications (Belgium)
ICANN	Internet Corporation for Assigned Names and Numbers
ICASA	Independent Communications Authority of SA (South Africa)
ICASI	Industry Consortium for Advancement of Security on the Internet
ICE	Infrastructure Critiche Europe (Italy)
ICE	European Critical Infrastructure
INCIBE	Spanish National Cybersecurity Institute (Spain)
ICPO	International Criminal Police Organization (Japan)
ICSG	Industry Connections Security Group (IEEE)
ICT	Information and Communication Technology
IDA	Infocomm Development Authority of Singapore (Singapore)
IE	Internet Explorer
IEEE	Institute for Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGF-Bpf	Internet Governance Forum Best Practice Forum on Cybersecurity
ILNAS	Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services
ILP	Initiating Logical Processor (TCG)
ILR	Institut Luxembourgeois de Régulation
IMEI	International Mobile station Equipment Identity
IMS	IP Multimedia Subsystem (3GPP)
INRIA	Institut national de recherche en sciences et technologies du numérique (France)
IODEF	Incident Object Description Exchange Format
IP	Internet Protocol
IPC	International Police Cooperation (Switzerland)