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

TECHNICAL REPORT

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

ETSI

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 accredidatie-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 Sécurité 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)

ipsecme	IP security maintenance and extensions working group (IETF)
IRAP	Information security Registered Assessors Program (Australia)
IRTF	Internet Research Task Force
ISA	Internal Security Agency (Poland)
ISA	Federal Act on Measures to Safeguard Internal Security (Switzerland)
ISA	Intelligence Service Act (Switzerland)
ISF	Information Security Forum
ISFP	Information Security and Facility Protection (Switzerland)
ISM	Australian government Information and communications technology Security Manual (Australia)
ISMP	Infocomm Security Master Plan (Singapore)
ISO	International Organization for Standardization
IT	Infrastrutture Critiche (Italy)
IT	Information Technology
ITIDA	Information Technology Industry Development Agency (Egypt)
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunication Standardization sector
IWWN	International Watch and Warning Network (Australia)
IXP	Internet eXchange Point
J-CAT	Cybercrime Action Task Force (Europol)
JASPER	Japan-ASEAN Security PartnERship (Japan)
JCPS	Justice, Crime Prevention and Security cluster (South Africa)
JOA	Joint Operating Arrangements of DSD, AFP and ASIO (Australia)
JOCERT	National Computer Emergency Response Team (Jordan)
JP CERT	Japan CERT (Japan)
JRC	Directorate on Joint Research Centre (EC)
JSON	JavaScript Object Notation
JUST	Directorate on Justice and Consumers (EC)
JVN	Japan Vulnerability Notes (Japan)
KCC	Korea Communications Commission (Korea)
KIS	Koordineringsutvalget for forebyggende Informasjonssikkerhet (Norway)
KITS	Koordinierungsstelle IT-Sicherheit
kitten	common authentication technology next generation working group (IETF)
KMIP	Key Management Interoperability Protocol (OASIS)
KMU	Kleine und Mittlere Unternehmen (Austria)
KRITIS	Kritische Infrastrukturen (Germany)
KSZ	Kruispuntbank van de Sociale Zekerheid (Belgium)
LECC	Law Enforcement/CSIRT Cooperation (FIRST)
LI	Lawful Interception
LIBGUIDE	reference library on cybersecurity (NATO)
lisp	locator/ID separation protocol (IETF)
LÜKEX	Länderübergreifende Krisenmanagement Exercise (Germany)
MACCSA	Multinational Alliance for Collaborative Cyber Situational Awareness
MA-CERT	Morocco CERT (Morocco)
MCCD	Joint Cyber Command (Spain)
MAEC	Malware Attribute Enumeration and Characterization
MCI	Ministry of Communications and Information (Singapore)
MCIT	Ministry of Communications and Information Technology (Egypt)
MCIT	Ministry of Communications and Information Technology (Saudi Arabia)
MCIV	Ministerieel Comité voor Inlichting en Veiligheid (Belgium)
MD	Ministry of Defence (Montenegro)
MELANI	Melde- und Analysestelle Informationssicherung (Switzerland)
MHA	Ministry of Home Affairs (Singapore)
MI	Ministry of the Interior (Montenegro)
MIIT	Ministry of Industry and Information Technology (China)
MilCERT	Military Computer Emergency Response Team (Austria)
MilCERT	Militärisches Computer Emergency Response Team (Austria)
milCERT	Military Computer Emergency Response Team (Switzerland)
mile	Managed incident lightweight exchange working group (IETF)
MINDEF	MINistry of DEFence (Singapore)
MIS	Military Intelligence Service (Switzerland)
MISP	Malware Information Sharing Platform & Threat Sharing (Luxembourg)
MIST	Ministry for Information Society and Telecommunications (Montenegro)

MMDEF	Malware Metadata Exchange Format Working Group (IEEE)
MNiSW	Ministry of Science and Higher Education (Poland)
MNiSW	Ministerstwo Nauki i Szkolnictwa Wyzszego (Poland)
MOD	Ministry Of Defence (Latvia)
MoE	Ministry of Economics (Latvia)
MoEPRD	Ministry of Environmental Protection and Regional Development (Latvia)
MoES	Ministry of Education and Science (Latvia)
MOF	Ministry Of Finance (Singapore)
MoFA	Ministry of Foreign Affairs (Latvia)
MoI	Ministry of the Interior (Latvia)
MoJ	Ministry of Justice (Latvia)
MOPAS	Ministry Of Public Administration and Security (Korea)
MoT	Ministry of Transport (Latvia)
Mow	Ministry of welfare (Latvia)
MP	Member of Parliament
MS-ISAC	Multi-State Information Sharing and Analysis Center
MTS	Methods for Testing and Specification (ETSI)
NAF	National Armed Forces (Latvia)
NASK	Research and Academic Computer Network (Poland)
NASK	Naukowej i Akademickiej Sieci Komputerowej (Poland)
NATO	North Atlantic Treaty Organization
NAVONVO	Nord-Atlantische Verdragsorganisatie (Belgium)
NBU	Národný Bezpecnostný Úrad (Slovakia)
NCAC	National Cybersecurity Advisory Council (South Africa)
NCCC	National Cyber Coordination Centre (India)
NCCoE	National Cybersecurity Centre of Excellence (USA)
NCDC	National Centre for Digital Certification (Saudi Arabia)
NCIA	National Computing and Information Agency (Korea)
NCIIPC	National Critical Information Infrastructure Protection Centre (India)
NCP	National Checklist Program
NCPF	National Cybersecurity Policy Framework (South Africa)
NCSC	National Cyber Security Centre (Korea)
NCSC	National Cyber Security Centre (Lithuania)
NCSC	Nationaal Cyber Security Centrum (Netherlands)
NCSC	National Cyber Security Centre (New Zealand)
NCSC	National Cyber Security Coordinating Centre (South Africa)
NCSC	National Cyber Security Centre (U.K.)
NCSP	National Cyber Security Programme (UK)
NCSRA	Nationale Cyber Security Research Agenda (Netherlands)
NCSS	National Cybersecurity Strategie (Netherlands)
NCSS	National Cyber Security Strategies
NCIRC	NATO Communications and Information Agency
NEC	National Encryption Centre (Jordan)
NEOC	National Emergency Operations Centre (Switzerland)
NERC	North American Electric Reliability Corporation
NES	National Economic Supply (Switzerland)
NESAG	Network Equipment Security Assurance Group (3GPP)
NetSafe	Safer Internet Centre of Latvia Net-Safe Latvia (Latvia)
NFSA	National Forensic Science Agency (Pakistan)
NFV	Network Functions Virtualisation (ETSI)
NIACSA	National Information Assurance and Security Agency (Jordan)
NIACSS	National Information Assurance and Cyber Security Strategy (Jordan)
NICI	National Information Security Authority (Slovakia)
NICT	National institute of Information and Communications Technology (Japan)
NIS	Network and Information Security (EU)
NIS	National Intelligence Service (Korea)
NISC	National Information Security Centre (Japan)
NISC	National Infocomm Security Committee (Singapore)
NISE	National Information Security Environment (Saudi Arabia)
NISE	NISE Instructions (Saudi Arabia)
NISED	NISE Directives (Saudi Arabia)
NISEMs	NISE Manuals (Saudi Arabia)

NISS	National Information Security Strategy (Saudi Arabia)
NIST	National Institute of Standards and Technology (USA)
NITC	National Information Technology Centre (Jordan)
NorCERT	Norway CERT (Norway)
NorSIS	Norsk senter for informasjonssikring (Norway)
NPA	National Prosecuting Authority (South Africa)
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen (Germany)
NRAF	National IS Risk Assessment Function (Saudi Arabia)
NRF	National Research Foundation (Singapore)
NSA	National Security Authority (Czech)
NSA	National Security Authority (Hungary)
NSA	National Security Agency (Montenegro)
NSA	National Security Authority (Slovakia)
NSA	National Security Agency (USA)
NSC-CSC	National Security Council Cyber Security Committee (Spain)
NSCS	National Security Coordination Secretariat (Singapore)
NSIS	National Strategy for Information Security in the Slovak Republic (Slovakia)
NSM	Nasjonal SikkerhetsMyndighet (Norway)
NSS	National Security Strategy (Jordan)
NSSIS	National Security Science and Innovation Strategy (Australia)
NTECH	Network Technologies (ETSI)
NTRA	National Telecommunication Regulatory Authority (Egypt)
NV (Storage)	Non-Volatile (shielded location) (TCG)
NVD	National Vulnerability Database (USA)
nvo3	network virtualization overlays working group (IETF)
NZ-CERT	New Zealand Computer Emergency Response Team (New Zealand)
NZSIS	New Zealand Security Intelligence Service (New Zealand)
OAG	Office of the Attorney General (Switzerland)
OASIS	Organization for the Advancement of Structured Information Standards
oauth	web authorization protocol working group (IETF)
OCAD	Coördinatieorgaan voor dreigingsanalyse (Belgium)
OCAM	Organe de Coordination pour l'Analyse de la Menace (Belgium)
OCC	Cybernetics Coordination Office (Spain)
OCP	Operator Cyber security Plan
OCSIA	Office of Cyber Security & Information Assurance (UK)
OFCOM	Federal Office of COMmunications (Switzerland)
OGCIO	Office of the Government Chief Information Office (UK)
OIV	Opérateur d'Importance Vitale (France)
OMB	Office of Management and Budget (USA)
OMG	Object Management Group
OpenC2	Open Command and Control (OASIS)
opsec	operational security capabilities for IP network infrastructure working group (IETF)
OS	Operating System
OSCE	Organization for Security and Co-operation in Europe
ÖSCS	Österreichische Strategie für Cyber Sicherheit (Austria)
ÖSS	Österreichischen SicherheitsStrategie (Austria)
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa (Germany)
OTAN	Organisation du Traité de l'Atlantique Nord (Belgium)
OTS	Ordinance on Telecommunication Services (Switzerland)
OVAL	Open Vulnerability and Assessment Language
PBC	pelnomocnika ds. bezpieczenstwa cyberprzestrzeni (Poland)
PC	Personal Computer
PCA	Privacy CA (TCG)
PCR	Platform Configuration Register (TCG)
PCS	Plenipotentiary for Cyberspace Security (Poland)
PDCA	Plan-Do-Check-Act (Germany)
PHAROS	Platform for Harmonization, Analysis, Cross-check and Orientation of Reportings (France)
PISA	Pakistan Information Security Association (Pakistan)
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PMRM	Privacy Management Reference Model (OASIS)
PPP	Public Private Partnership (Austria)

PRACTICE	Proactive Response Against Cyber-attacks (Japan)
PrivEK	Private Endorsement Key (TCG)
PSN	Public Sector Network
PTA	Police Tasks Act (Switzerland)
PubEK	Public Endorsement Key (TCG)
RAN	subcommittee on Radio Access Network (3GPP)
RCMP	Royal Canadian Mounted Police (Canada)
Restena CSIRT	Research and education CERT (Luxembourg)
RGISSP	Research Group Information Society and Security Policy (Switzerland)
RGS	Référentiel Général de Sécurité (France)
RID	Real-time Inter-network Defense
RoT	Root of Trust (component) (TCG)
RTD	Directorate on Research and Innovation (EC)
RTM	Root of Trust for Measurement (TCG)
RTR	Root of Trust for Reporting (TCG)
RTS	Root of Trust for Storage (TCG)
SA CISRS	Saudi Arabian Critical Security and Resilience Strategy (Saudi Arabia)
SA2	Subcommittee on Architecture (3GPP)
SA3	Subcommittee on Security (3GPP)
SA5	Subcommittee on Telecom Management (3GPP)
sacm	security automation and continuous monitoring working group (IETF)
SAGE	Security Algorithms Group of Experts (ETSI)
SAI	Securing Artificial Intelligence (ETSI)
SAML	Security Services (OASIS)
SAMRISK	Samfunnssikkerhet og risiko (Norway)
SANS	SysAdmin, Audit, Networking, and Security
SAPS	South African Police Service (South Africa)
SAS	Security Assurance Specification (3GPP)
SC27	ISO/IEC JTC1 Committee on Security techniques
SC6	ISO/IEC JTC1 Committee on Telecommunications and information exchange between systems
SC7	ISO/IEC JTC1 Committee on Software and systems engineering
SCADA	Supervisory Control And Data Acquisition (Belgium)
SCAP	Security Content Automation Protocol
SCP	Smart Card Platform
SIG	Special Interest Group
SE	Secure Element
SECAM	Study on Security Assurance Methodology (3GPP)
SeP	Security Police (Latvia)
SERI	Senter for rettsinformatikk (Norway)
SES	Secretariat of State for Security
SESIAD	Secretariat of State for the Information Society and the Digital Agenda (Spain)
SFOE	Swiss Federal Office of Energy (Switzerland)
SG 2	Study Group on Operational aspects (ITU-T)
SG11	Study Group on Protocols and test specifications (ITU-T)
SG13	Study Group on Future networks (ITU-T)
SG17	Study Group on Security (ITU-T)
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale (France)
SGRS	Service Général du Renseignement et de la Sécurité (Belgium)
sidr	secure inter-domain routing working group (IETF)
SIEM	Security Information and Event Management
SIGINT-CYBER	Joint General Intelligence and Security Service Unit (Netherlands)
SIIO	State Internet Information Office (China)
SIM	Subscriber Identity Module, including USIM and ISIM (ETSI, 3GPP)
SIS	State Information Systems (Latvia)
SKKM	Staatliches Krisen- und KatastrophenschutzManagement (Austria)
SLT	Samordning av Lokale kriminalitetsforebyggende Tiltak (Norway)
SN	Standard Norge (Norway)
SNSC	Sistemul |National de Securitate Cibernetica (Romania)
SOC	Security Operations Centre
SOME	Cyber Incident Response Team (Turkey)
SOME	Siber Olaylara Mildahale Ekipleri (Turkey)
SONIA	Special Task Force on Information Assurance (Switzerland)

SOSMT	Slovak Standards Institute (Slovakia)
SP	State Police (Latvia)
SPF	Service Public Fédéral (Belgium)
SPIK	Swiss Police IT Congress (Switzerland)
SPOC	Single Point of Contact
SPTA	Surveillance of Postal and Telecommunications traffic Act (Switzerland)
SRDA	State Regional Development Agency (Latvia)
SRK	Storage Root Key (TCG)
SSA	State Security Agency (South Africa)
SSP	Smart Secure Platform
stir	secure telephone identity revisited working group (IETF)
STIX	Structured Threat Information eXpression
TAC	Threat Analysis Centre (Singapore)
TAXII	Trusted Automated eXchange of Indicator Information
TBB	Trusted Building Block (TCG)
TC	Technical Committee
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
tcpinc	TCP increased security working group (IETF)
TEE	Trusted Execution Environment
TISN	Trusted Information Sharing Network for critical infrastructure protection (Australia)
TLP	Traffic Light Protocol
TLS	Transport Layer Security
tls	transport layer security working group (IETF)
TMI	Trusted Multi-tenant Infrastructure (TCG)
TNC	Trusted Network Connect (TCG)
TPM	Trusted Platform Module (TCG)
TPS	Trusted Platform Support services (TCG)
trans	public notary transparency (IETF)
Trust Elevation	electronic identity credential trust elevation methods (OASIS)
TSS	TPM Software Stack -or- TCG Software Stack (TCG)
TSUBAME	International network traffic monitoring project (Japan)
TT CSIRT	Trinidad and Tobago CSIRT (Trinidad & Tobago)
TTA	Telecommunications Technology Association (Korea)
TTC	Telecommunication Technology Committee (Korea)
TTCSA	Trinidad and Tobago Cyber Security Agency (Trinidad & Tobago)
TUVE	turvallisuusverkkohanke (Finland)
UKE	Office of Electronic Communications (Poland)
UKE	Urzedem Komunikacji Elektronicznej (Poland)
UNSW	University of New South Wales
UP KRITIS	Umsetzungsplan KRITIS (Germany)
URI	Uniform Resource Identifier
USOM	National Centre for Cyber Incident Response (Turkey)
USOM	Ulusal Siber Olaylara Mildahale Merkezi (Turkey)
uta	using TLS in applications (IETF)
UTM	Unified Threat Management (Italy)
UVTA	Ulko- ja turvallisuuspoliittinen ministerivaliokunta (Finland)
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä (Finland)
VDRX	Vulnerability Reporting and Data eXchange SIG (FIRST)
VDSG	Ordinance to the Federal Act on Data Protection (Switzerland)
VSSE	Veiligheid van de Staat, Sûreté de l'Etat (Belgium)
W3C	World Wide Web Consortium
websec	web security working group (IETF)
wpkops	web PKI OPS working group (IETF)
WS-SX	Web Services Secure eXchange (OASIS)
XCCDF	eXtensible Configuration Checklist Description Format
XDI	XRI Data Interchange (OASIS)
XML	eXtensible Markup Language
XSPA	Cross-Enterprise Security and Privacy Authorization (OASIS)
YTS	Yhteiskunnan turvallisuusstrategiassa (Finland)
ZNIIS	Центральный научно-исследовательский институт связи (Russia)

4   Global cyber security ecosystem

4.1   Organization of the ecosystem forums and activities

This clause organizes the global cyber security ecosystem as six groups of forums and activities that are fundamental collaborative mechanisms for cyber security and its evolution:

1)   forums that develop techniques, technical standards and operational practices;

2)   major IT developer forums affecting cyber security;

3)   activities for continuous information exchange;

4)   centres of excellence;

5)   reference libraries, continuing conferences; and

6)   heritage sites and historical collections.

In some cases, the same parent organization hosts multiple forums and activities that are attributed to different groups. In other cases, the organization hosts numerous forums where several of them have fully or substantially dedicated cyber security functions - which are indented under the parent. Because of the very large numbers of forums, and in the interests of providing a useful understanding of the ecosystem, only very short descriptions are provided, and the reader is encouraged to use the URI links to fully appreciate the work being done.

This compilation attempts to be an inclusive as possible to expand the collective insight into the extent of the ecosystem. Toward this objective, it includes collaborative mechanisms that are frequently overlooked but enormously significant in the cyber security arena such as developer forums for the major IT platforms, centres of excellence that are rapidly growing in numbers worldwide, and continuing conferences - even hacker major global hacker events that regularly reveal cyber security vulnerabilities that were previously unknown.

This material is augmented by annex A which contains national cyber security ecosystems that have been published in national strategy or other publicly available material. Annex B contains depictions of relationships among these ecosystems.

4.2   Fora that develop techniques, technical standards and operational practices

The forums listed below are well known venues engaging in significant global collaboration to produce techniques, technical standards and operational practices for cyber security. Where the venues operate substantially at a national level, they are placed in annex A.

3GPP - 3rd Generation Partnership Project. 3GPP unites six telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), and provides their members with a stable environment to produce the Reports and Specifications that define the world's principal mobile communication technologies. The scope includes cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security and quality of service. The specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks. http://www.3gpp.org/.

- **SA1 - Services**. Service and feature requirements applicable to mobile and fixed communications technology for 2G, 3G and future communication technologies, evolved industry-wide IP Multimedia Subsystem (IMS), and converged fixed-mobile communication technologies. http://www.3gpp.org/specifications-groups/sa-plenary/sa1-services.

- **SA2 - Architecture**. Identifies the main functions and entities of the network, how these entities are linked to each other and the information they exchange. http://www.3gpp.org/Specifications-groups/sa-plenary/53-sa2-architecture.

- **SA3 - Security**. Determine the security and privacy requirements for mobile systems, and specifies the security architectures and protocols, including the availability of any cryptographic algorithms. SA3 notably includes two significant security assurance activities: SECAM (Study on Security Assurance Methodology) and NESAG (Network Equipment Security Assurance Group). SA3LI also operates as part of SA3 to meet lawful interception security obligations. http://www.3gpp.org/Specifications-groups/sa-plenary/54-sa3-security.

- **SA5 - Telecom Management**. Specifies the requirements, architecture and solutions for provisioning and management of the network (RAN, CN, IMS) and its services. Also the principal venue for coordinating NFV-SDN and 5G activities. http://www.3gpp.org/specifications-groups/sa-plenary/sa5-telecom-management/home.

- **SA6 - Mission-critical Applications**. Responsible for the definition, evolution and maintenance of technical specification(s) for application layer functional elements and interfaces supporting critical communications. http://www.3gpp.org/specifications-groups/sa-plenary/sa6-mission-critical-applications.

5GACIA - 5G Alliance for Connected Industries and Automation. The 5G Alliance for Connected Industries and Automation (5G-ACIA) has been established to serve as the central and global forum for addressing, discussing, and evaluating relevant technical, regulatory, and business aspects with respect to 5G for the industrial domain. It reflects the entire ecosystem, encompassing all relevant stakeholder groups. https://www.5g-acia.org/.

ACDC - Advanced Cyber Defence Centre. Provides a complete set of solutions accessible online to mitigate on-going attacks and targeted both to end-users and to network operators. It also consolidates the data provided by various stakeholders into a pool of knowledge, accessible through the ACDC central clearing house. https://www.acdc-project.eu/.

AIOTI - The European Alliance of IoT Innovation. An inclusive body of IoT industrial players - large companies, successful SMEs and dynamic start-ups - as well as well-known European research centres, universities, associations and public bodies. Its thirteen working groups cover a broad array of IoT sectors including security. https://aioti.eu/.

APCERT - Asia Pacific Computer Security Response Team. Based in Japan, a trusted contact network of computer security experts in the Asia Pacific region to improve the region's awareness and competency in relation to computer security incidents. http://www.apcert.org/about/structure/secretariat.html.

BEREC - Body of European Regulators for Electronic Communications. BEREC facilitates independent, regulation of European electronic communications markets. http://berec.europa.eu/eng/about_berec/what_is_berec/.

CA/B - Certificate of Authority/Browser Forum. The Forum advances industry best practices to improve the ways that digital certificates are used to the benefit of network users and the security of their communications. The Forum produces the specification for Extended Validation Certificates, oversees their implementation, coordinates their recognition through ubiquitous network trust mechanisms. https://cabforum.org/about-us/.

CableLabs®. CableLabs is the principle standards body globally for the providers and vendors in the cable industry. Its standards are republished by ETSI and ITU-T. http://www.cablelabs.com/.

CCRA - Common Criteria Recognition Agreement. The CCRA is an organization among 26 countries to raise the general security of certified information and communications technology products through compliance with sets of security functional and security assurance requirements. https://www.commoncriteriaportal.org/ccra/.

CEN - Comité Européen de Normalisation. Provides a platform for the development of European Standards and other technical documents in relation to various kinds of products, materials, services and processes. Notably it is a member of the CSCG (Cybersecurity Coordination Group) to the EC. https://www.cen.eu/.

CENELEC - European Committee for Electrotechnical Standardization. CENELEC is responsible for standardization in the electrotechnical engineering field. Its cyber security activity relates to coordination on smart grid information security. Notably it is a member of the CSCG (Cybersecurity Coordination Group) to the EC. CEN/CLC/JTC13 on Cybersecurity and Data Protection develops standards for cybersecurity and data protection covering all aspects of the evolving information society. http://www.cenelec.eu/.

CEPOL - European Police College. An EU agency dedicated to providing training and learning opportunities to senior police officers on issues vital to the security of the European Union and its citizens. Activities are designed to facilitate the sharing of knowledge and best practice and to contribute to the development of a common European law enforcement culture. https://www.cepol.europa.eu/education-training/what-we-teach/residential-courses/20141026/132014-cybercrime-vs-cybersecurity.

CIS - Center for Internet Security. The Center is focused on enhancing the cybersecurity readiness and response of public and private sector entities and encompasses two major activities. http://www.cisecurity.org/. Standards to maintain and promote use of the set of Critical Security Controls as recommended actions for cyber defence that provide specific and actionable ways to thwart the most pervasive attacks and the Open Vulnerability and Assessment Language (OVAL) specifications. It also maintains the MS-ISAC - the U.S. DHS mechanism for exchanging cyber threat information among state and local governments, and the EI-ISAC - the U.S. DHS mechanism for securing elections infrastructure.

CSA - Cloud Security Alliance. CSA develops best practices for providing security assurance within Cloud Computing, and provides education on the uses of Cloud Computing to help secure all other forms of computing. https://cloudsecurityalliance.org/.

EC - European Commission. The European Commission is the EU's executive body. Multiple directorates have significant cyber security roles: CONNECT (Communications Networks, Content and Technology; DIGIT (Informatics); GROW (Internal Market, Industry, Entrepreneurship and SMEs) Enterprise and Industry); HR (Human Resources and Security), JRC (Joint Research Centre), JUST (Justice and Consumers); HOME (Migration and Home Affairs); RTD (Research and Innovation). http://ec.europa.eu/about/index_en.htm.

- **CSCG - Cybersecurity Coordination Group**. The CSCG - comprised by CEN, CENELEC, and ETSI - acts as a single point of contact for pan-European interchange on Cyber Security standardization and provides a set of recommendations and advice to the European Commission and EU Member States in the area of Cyber Security standardization. Additionally, the Coordination Group liaises actively with the European Union Agency for Network and Information Security (ENISA) and the Multi-Stakeholders Platform on ICT standardization.

- **ENISA - European Network and Information Security Agency**. ENISA helps the European Commission, the Member States and the business community to address, respond and especially to prevent Network and Information Security problems. Notably it operates the EU-CERT and provides support for the ECRG, NIS activities, including harmonization of national cyber security strategies. https://www.enisa.europa.eu/.

- **EOS - European Organization for Security**. EOS' main objective is the development of a harmonised European security market in line with political, societal and economic needs through the efficient use of budgets. EOS works towards achieving a better level of technology independence for European strategic autonomy and supports the development and use of European reference solutions as well as the growth of a genuine European industry. http://www.eos-eu.com/.

- **ECSO - European Cybersecurity Organization**. ECSO represents an industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote, encourage European cybersecurity. http://www.ecs-org.eu/.

- **ECRG - Electronic Communications Reference Group**. ECRG includes European providers of public electronic communications networks and services (mobile and fixed telecom operators, VoIP providers, ISPs, IXP providers, etc.) and it addresses security topics across the Electronic Communications area - including security measures, incident reporting, data protection, botnet mitigation, interconnection security and other topics. https://resilience.enisa.europa.eu/ecrg.

- **H2020 - Horizon 2020**. H2020 is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness. http://ec.europa.eu/programmes/horizon2020/. It includes a cybersecurity component.

- **Cybersecurity cPPP - Cybersecurity contractual Public Private Partnership**. Signed as part of the EU cybersecurity strategy by the European Commission and the European Cyber Security Organisation (ECSO). The aim of the partnership is to foster cooperation between public and private actors at early stages of the research and innovation process in order to allow people in Europe to access innovative and trustworthy European solutions (ICT products, services and software).

- **NIS - Network and Information Security**. The NIS Platform is part of the European Strategy for Cybersecurity. It serves the 2 priorities of achieving cyber-resilience in the EU and developing industrial and technological resources for cybersecurity https://resilience.enisa.europa.eu/nis-platform.

ETSI - European Telecommunications Standards Institute. ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. Notably, it hosts the Technical Committee for Cybersecurity and is a member of the CSCG (Cybersecurity Coordination Group) to the EC. https://www.etsi.org/.

- **CYBER - Cybersecurity Technical Committee**. CYBER is tasked to develop and maintain the Standards, specifications and other deliverables to support the development and implementation of Cyber Security standardization within ETSI, to collect and specify Cyber Security requirements from relevant stakeholders, to identify gaps where existing standards do not fulfil the requirements and provide specifications and standards to fill these gaps, without duplication of work in other ETSI committees and partnership projects, and to ensure that appropriate Standards are developed within ETSI in order to meet these requirements. https://portal.etsi.org/tb.aspx?tbid=824&SubTB=824. It also hosts the subgroup CYBER QSC which makes assessments and recommendations on the various proposals from industry and academia regarding real-world deployments of quantum-safe cryptography.

- **ESI - Electronic Signatures and Infrastructures**. ESI develops generic standards, guides and reports relating to electronic signatures and related trust infrastructures to protect electronic transactions and ensure trust and confidence. https://portal.etsi.org/tb.aspx?tbid=607&SubTB=607.

- **LI - Lawful Interception technical committee**. Responsible for developing standards that support the requirements of national and international law for lawful interception and retained data of electronic communications. https://portal.etsi.org/tb.aspx?tbid=608&SubTB=608.

- **MTS-SIG - Methods for Testing and Specification Security Special Interest Group**. Responsible generally for the identification and definition of advanced specification and testing methods, and with respect to security, advanced model-based security testing methods, risk-based security testing methods, and security assurance life cycle. https://portal.etsi.org/tb.aspx?tbid=97&SubTB=97.

- **NFV - Network Functions Virtualisation**. NFV is a very large and active Industry Specification Group focused on a broad array of specifications for Network Functions Virtualization, including cyber security techniques and mechanisms through its NFVsec subgroup. https://portal.etsi.org/tb.aspx?tbid=789&SubTB=789,832,831,795,796,801,800,798,799,797,802,828.

- **NTECH - Network Technologies**. Provide detailed architecture and protocol (profile) specifications for use in networks addressing the control, data and management planes in both the service and transport layers of future networks, including security. https://portal.etsi.org/tb.aspx?tbid=785&SubTB=785,808.

- **SAGE - Security Algorithms Group of Experts**. SAGE is responsible for creating reports (containing confidential specifications), draft ETSI deliverables in the area of cryptographic algorithms and protocols specific to fraud prevention/unauthorized access to public/private telecommunications networks and user data privacy. https://portal.etsi.org/tb.aspx?tbid=160&SubTB=160.

- **SAI - Securing Artificial Intelligence**. SAI develops technical specifications that mitigate against threats arising from the deployment of AI, and threats to AI systems, from both other AIs, and from conventional sources. https://portal.etsi.org/tb.aspx?tbid=877&SubTB=877#/.

- **SCP - Smart Card Platform**. SCP is responsible for the development and maintenance of specifications for secure elements (SEs) in a multi-application capable environment, the integration into such an environment, as well as the secure provisioning of services making use of SEs. TC SCP developed the UICC, the smart card platform used for the SIM, and is currently developing the next generation Smart Secure Platform, the SSP. https://portal.etsi.org/tb.aspx?tbid=534&SubTB=534,639,640,714#/.

CERT-EU - Community Emergency Response Team - Europe. A permanent CERT for EU institutions, agencies and bodies made up of IT security experts from the main EU Institutions. It cooperates closely with other CERTs in the Member States and beyond as well as with specialized IT security companies. http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html.

Europol - European Police Office. Located at The Hague, Europol is the EU's law enforcement agency whose main goal is to help achieve a safer Europe for the benefit of all EU citizens through assistance to the Member States in their fight against serious international crime and terrorism, including cyber security investigations. J-CAT (Cybercrime Action Task Force) has been active in dealing with mobile malware. https://www.europol.europa.eu/.

FIDO Alliance. The Fast IDentity Online organization develops technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users and promotes their use. https://fidoalliance.org/.

FIRST - Forum of Incident Response and Security Teams. FIRST is the international organization of CERTs/CSIRTs who cooperatively handle computer security incidents and promote incident prevention programs. FIRST members develop and share technical information, tools, methodologies, processes and best practices. It also promotes the creation and expansion of Incident Response teams globally though global, regional, and national workshops and conferences. http://www.first.org. Through FIRST's Special Interest Groups (SIGs) and BOFs, it develops significant cyber security techniques and standards that include:

- Standards:

    - Common Vulnerability Scoring System (CVSS)

    - Information Exchange Policy

    - Traffic Light Protocol (TLP)

    - Passive DNS Exchange

- Discussion Groups:

    - Internet Infrastructure Vendors

    - Malware Analysis

    - Metrics SIG

    - Industrial Control Systems (ICS)

- Working Groups:

    - Ethics SIG

    - Red Team SIG

    - Vulnerability Reporting and Data eXchange

    - Vulnerability Coordination

    - Information Sharing SIG

GlobalPlatform®. GlobalPlatform is a cross industry, non-profit association which identifies, develops and publishes specifications that promote the secure and interoperable deployment and management of multiple applications on secure chip technology. Its proven technical specifications, which focus on the Secure Element (SE), Trusted Execution Environment (TEE) and system messaging. https://www.globalplatform.org/default.asp.

GSMA™ - GSM Association. GSMA is the global *organization* of GSM and related mobile providers and vendors, and today the largest telecommunication industry entity. GSMA's Fraud and Security Working Group is the global mechanism for exchanging information, developing standards and techniques, and collaborating on mobile cyber security in many other forums. It works closely with 3GPP groups, especially SA3 (Security) - providing support for cyber security information assurance initiatives. http://www.gsma.com/.

- **GSMA™ FASG - GSM Association Fraud and Security Working Group**. The newly integrated FASG group operates through several groups addressing mobile device security and malware, and NESAG (Network Equipment Security Assurance Group) which supports the 3GPP SA3 security assurance platforms. http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group.

ICANN - Internet Corporation for Assigned Names and Numbers. ICANN is responsible for the coordination of maintenance and methodology of several databases of unique identifiers through its operation of the Internet Assigned Numbers Authority (IANA), oversight of key identifier registration and query capabilities, and maintenance of digital certificates for the Domain Name System. https://www.icann.org/.

IEEE Standards Association. The IEEE SA is a leading consensus building organization that nurtures, develops & advances global technologies. Its work drives the functionality, capabilities and interoperability of a wide range of products and services. http://standards.ieee.org/index.html.

- **Industry Connections Security Group (ICSG)**. The Group promotes collaboration and information sharing across the IT security industry. Working group's aim is to help develop an accepted way of traffic inspection, on top of encrypted transport standards. The ICSG has five working groups related to security. http://standards.ieee.org/develop/indconn/icsg/index.html.

  - AMSS - Anti-Malware Support Services Working Group

  - ETI - Encrypted Traffic Inspection Working Group

  - MMDEF - Malware Metadata Exchange Format Working Group

  - Malware Working Group

IETF - Internet Engineering Task Force. The IETF is a global standards making activity of the Internet Society that influences the way people design, use, and manage the Internet. Many of these activities are cyber security related. Its Internet Architecture Board (IAB) also oversees development of cyber security capabilities. IETF groups change frequently and its website should be consulted for the latest activities. https://www.ietf.org.

- **MILE - Managed Incident Lightweight Exchange**. The MILE working group develops standards to support computer and network security incident management; an incident is an unplanned event that occurs in an information technology (IT) infrastructure. Its platforms such as IODEF and RID have been in widespread use by CERTs for many years and new extensions have been produced. https://datatracker.ietf.org/wg/mile/documents/.

- **SACM - Security Automation and Continuous Monitoring**. Standardized protocols to collect, verify, and update system security configurations would allow this process to be automated, which would free security practitioners to focus on high priority tasks and should improve their ability to prioritize risk based on timely information about threats and vulnerabilities. https://datatracker.ietf.org/wg/sacm/charter/.

- Other IETF Security Area and related groups include:

  - ace - Authentication and Authorization for Constrained Environments

  - acme - Automated Certificate Management Environment

  - cose - CBOR Object Signing and Encryption

  - curdle - CURves, Deprecating and a Little more Encryption

  - dots - DDoS Open Threat Signalling

  - emu - EAP Method Update

  - i2nsf - Interface to Network Security Functions

  - ipsecme - IP Security Maintenance and Extensions

  - kitten - Common Authentication Technology Next Generation

  - lake - Lightweight Authenticated Key Exchange

  - lamps - Limited Additional Mechanisms for PKIX and SMIME

  - mls - Messaging Layer Security

  - oauth - Web Authorization Protocol

  - rats - Remote ATtestation ProcedureS

  - secdispatch - Security Dispatch

  - suit - Software Updates for Internet of Things

- teep - Trusted Execution Environment Provisioning

- tls - Transport Layer Security

- tokbind - Token Binding

- trans - Public Notary Transparency

IRTF - Internet Research Task Force. The IRTF focuses on longer term Internet research issues. Its Crypto Forum Research Group (CFRG) is a general forum for discussing and reviewing uses of cryptographic mechanisms, both for network security. https://irtf.org/.

ISF - Information Security Forum. ISF is comprised of major companies dedicated to investigating, clarifying and resolving key issues in information security and risk management, by developing best practice methodologies, processes and solutions that meet the business needs of their Members. https://www.securityforum.org/membership/.

ISO - International Organization for Standardization. The ISO is a Swiss based private international standards development and publishing body composed of representatives from various national standards organizations with multiple committees - several of which have significant cyber security related activity. http://www.iso.org.

- **JTC1/SC27 - Information security, cybersecurity and privacy protection**. SC27 publishes security technique standards. http://www.iso.org/iso/iso_technical_committee?commid=45306. SC27 has five working groups dealing with:

  - Information security management systems

  - Cryptography and security mechanisms

  - Security evaluation, testing and specification

  - Security controls and services

  - Identity management and privacy technologies

- **JTC1/SC7 - Software and systems engineering**. SC 7 publishes software development, testing, and tagging standards. http://www.iso.org/iso/iso_technical_committee%3Fcommid%3D45086.

- **JTC1/SC6 - Telecommunications and information exchange between systems**. SC 6 publishes together with the ITU-T Study Group 17, the legacy X.509 PKI standard that is implemented using IETF, ETSI, and CA/B Forum profiles. http://www.iso.org/iso/iso_technical_committee.html?commid=45072.

ITU - International Telecommunication Union. The ITU is a Swiss based intergovernmental body with three sectors dealing with the development and publication of Recommendations for radio systems (ITU-R), telecommunications (ITU-T), and development assistance (ITU-D). https://www.itu.int.

- **ITU-R - Telecommunication Radiocommunication Sector**. The ITU-R consists of an Assembly that meets every four years to approve its structure and general work areas, six Study Groups that meet annually, and a Secretariat that publishes the materials and maintains several radiocommunication databases. The ITU-R cyber security activity is confined to legacy materials, and contemporary radio cyber security work occurs predominantly in ETSI, 3GPP, and GSMA. https://www.itu.int/en/ITU-R/Pages/default.aspx.

- **ITU-T - Telecommunication Standardization Sector**. The ITU-T consists of an Assembly that meets every four years to approve its structure and general work areas, eleven Study Groups that meet annually, and a Secretariat that publishes the materials and maintains several legacy telecommunications databases. The ITU-T cyber security activity is focussed in Group Q4 of SG17 which produces a series of Recommendations for Cybersecurity Information Exchange (CYBEX). http://www.itu.int/en/ITU-T/studygroups/2017-2020/Pages/default.aspx/.

- The cyber security relevant Study Groups include:

  - SG 2 - Operational aspects

  - SG 9 - Broadband cable and TV

  - SG11 - Protocols and test specifications

- SG13 - Future networks (& cloud)

- SG15 - Transport, Access and Home

- SG16 - Multimedia

- SG17 - Security

- SG20 - IoT and applications, smart cities

- **ITU-D - Development Sector**. Provides technical assistance and in the creation, development and improvement of telecommunications in developing countries. http://www.itu.int/en/ITU-D/Pages/default.aspx. ITU-D has cyber security activity in group Q3 of Study Group 2. ITU-T also maintains Cybersecurity Country Profiles at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Forms/AllItems.aspx.

MITRE - MITRE is a globally active non-profit research and development centre that is responsible for multiple significant global cyber security techniques, standards making and related secretariat activities. The activity occurs through multiple individual on-line activities, frequent workshops, and significant involvement in other global forums listed below. http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-resources/standards.

- **ATT&CK™ - Adversarial Tactics Techniques and Common Knowledge**: a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. It is a structured list of known attacker behaviors that have been compiled into tactics and techniques and expressed in a handful of matrices as well as via STIX/TAXII. The list is a fairly comprehensive representation of behaviors attackers employ when compromising networks, it is useful for a variety of offensive and defensive measurements, representations, and other mechanisms. https://attack.mitre.org/.

- **Cybersecurity Languages/Formats & Protocols**: Malware Attribute Enumeration and Characterization (MAEC™), Common Vulnerabilities and Exposures (CVE®), Common Weakness Scoring System (CWSS™), Common Weakness Risk Analysis Framework (CWRAF™).

- **Cybersecurity Registries**: Common Attack Pattern Enumeration and Classification (CAPEC™), Common Weakness Enumeration (CWE™).

NATO - North Atlantic Treaty Organization. Against the background of increasing dependence on technology and on the Internet, the Alliance is advancing its efforts to confront the wide range of cyber threats targeting NATO's networks on a daily basis. NATO has moved forward with five cyber security actions: developing NATO Policy on Cyber Defence, assisting individual Allies, increasing NATO cyber defence capacity, cooperating with partners, and cooperating with industry. The Allies have also committed to enhancing information sharing and mutual assistance in preventing, mitigating and recovering from cyber attacks. http://www.nato.int/cps/en/natohq/topics_78170.htm.

- **LIBGUIDE - NATO reference library on cybersecurity**. LIBGUIDE provides a few starting points to assist with research on issues related to cyberspace security. Notably, it includes a National Cyber Security Framework Manual. http://www.natolibguides.info/cybersecurity.

- **CCDCOE - NATO Cooperation Cyber Defence Center of Excellence**. CCDCOE is a comprehensive and easy to navigate collection of legal and policy documents adopted by international organizations active in cyber security. https://ccdcoe.org/library/strategy-and-governance/.

OASIS - Organization for the Advancement of Structured Information Standards. OASIS is a major global industry body for developing and publishing worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management, and other areas requiring structured information exchange. Although it began focussed on XML language schema, it has subsequently expanded to JSON.

- The four most significant cyber security specifications activities consist of:

  - Technical Committee for Cyber Threat Intelligence (CTI). https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti. It hosts development and publication of the specifications for Trusted Automated eXchange of Indicator Information (TAXII), Structured Threat Information eXpression (STIX), and Cyber Observable Expression (CybOX).

  - Common Security Advisory Framework (CSAF). https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf. Responsible of the former Common Vulnerability Reporting Framework (CVRF) designed standardize existing practice in structured machine-readable vulnerability-related advisories.

- Collaborative Automated Course of Action Operations (CACAO). https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao. It is developing a standard to implement the course of action playbook model for cybersecurity operations through a sequence of cyber defense actions that can be executed for each type of playbook.

- Open Command and Control (OpenC2). https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=openc2. It is developing documents, specifications, lexicons or other artifacts to fulfill the needs of cyber security command and control in a standardized manner. It has published a language description document (RC4), actuator profiles, and open source prototype implementations.

- OASIS currently hosts other cyber security technical committees listed below. https://www.oasis-open.org/org:

  - Biometric Services (BIOSERV)

  - Cross-Enterprise Security and Privacy Authorization (XSPA)

  - Digital Signature Services eXtended (DSS-X)

  - Electronic Identity Credential Trust Elevation Methods (Trust Elevation)

  - Key Management Interoperability Protocol (KMIP)

  - PKCS 11 TC

  - Privacy Management Reference Model (PMRM)

  - Security Services (SAML)

  - Web Services Secure Exchange (WS-SX)

  - XRI Data Interchange (XDI)

OIC-CERT - Organisation of Islamic Cooperation - Computer Emergency Response Teams. OIC-CERT provides a means for member countries to develop collaborative initiatives and partnerships relating to cyber security. https://www.oic-cert.org/en/.

OMG - Object Management Group®. OMG is a computer industry consortium to develop enterprise integration standards. The Group's principal current cyber security work deals with threat modelling where its System Assurance Task Force Security Fabric Working Group is developing a Unified Modelling Language Threat & Risk Model. http://sysa.omg.org/.

OSCE - Organisation for Security and Co-operation in Europe. (**OSZE Organisation für Sicherheit und Zusammenarbeit in Europa**). The OSCE maintains an informal working group on cyber security and workshops devoted to Confidence Building Measures (CBMs). http://www.osce.org/.

TCG - Trusted Computing Group®. TCG develops, defines and promotes open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. Its platforms provide for authentication, cloud security, data protection, mobile security, and network access & identity. TCG presently has twelve working groups. http://www.trustedcomputinggroup.org/:

- Cloud Work Group

- CYRES - Cyber Resilient Technologies Work Group

- DICE - Device Identifier Composition Engine Architectures Work Group

- ESWG - Embedded Systems Work Group

- Industrial Work Group

- IWG - Infrastructure Work Group

- IoTWG - Internet of Things Work Group

- MPWG - Mobile Platform Work Group

- Network Equipment Work Group

- PCCWG - PC Client Work Group

- SWG - Server Work Group

- TWG - Storage Work Group

- TSSWG - TSS Software Stack Work Group

- TNCWG - Trusted Network Communications Work Group

- TPM - Trusted Platform Module Work Group

- VPWG - Virtualized Platform Work Group

W3C® - World Wide Web Consortium. W3C develops protocols and guidelines for WWW services. It maintains four cyber security groups. http://www.w3c.org/:

- Web Authentication Working Group

- Web Application Security

- Web Payments

- Privacy Interest Group

- Technical Architecture Group (TAG)

- Hardware Based Secure Services Group

- XML Security

4.3   Major IT developer forums affecting cyber security

Amazon Web Services® Forum. A developer forum for services hosted on the Amazon data centre platforms. https://forums.aws.amazon.com/forum.jspa?forumID=30.

Android™ Developers Forum. A developer forum for applications running on the Android OS. http://developer.android.com/develop/index.html.

Apple® iOS Dev Center. A developer forum for applications running on the iOS OS. https://developer.apple.com/devcenter/ios/index.action.

Apple Safari®. A developer forum for applications operating via the Safari browser. https://developer.apple.com/devcenter/safari/index.action.

BlackBerry® Dev Zone. A developer forum for applications operating on the Blackberry OS. http://developer.blackberry.com/.

BMC Software®. A developer forum for applications running on OS. http://www.bmc.com/solutions/cloud-computing/cloud-computing-management/Cloud-Computing-Management-CCM.html.

Broadcom. A set of developer forums for Broadcom platforms. https://community.broadcom.com/communities/allcommunities.

Cisco Developer Network. A developer forum for applications running on Cisco OS platforms. http://developer.cisco.com/.

FreeBSD®. A developer forum for applications running on FreeBSD Unix. http://www.freebsd.org/projects/.

GitHub®. A developer software exchange forum. https://github.com/.

Google Chrome™. A developer forum for applications running on the Chrome browser.
https://www.google.com/chrome/dev/.

Google Developers. A developer forum for applications running on the Google platforms.
https://developers.google.com/.

HP Cloud Services. A developer forum for applications running on HP cloud platforms.
https://www.hpe.com/us/en/solutions/cloud.html.

IBM developerWorks®. A developer forum for applications running on IBM platforms generally.
http://www.ibm.com/developerworks/aboutdw/contacts.html.

IBM z/OS®. A developer forum for applications running on IBM's Z/OS.
https://developer.ibm.com/mainframe/2017/12/06/exploring-the-new-ibm-system-automation-for-zos/.

iCloud for Developers. A developer forum for applications running on the Apple Cloud platform.
https://developer.apple.com/icloud/index.php.

Intel® Cloud Builders. A developer forum for applications running on Intel cloud platforms.
http://www.intel.com/content/www/us/en/cloud-computing/cloud-builders-provide-proven-advice.html?cid=sem116p9128.

Jive apps developers. A developer forum for applications running on Jive. https://developer.jivesoftware.com/.

Linux Foundation. A developer forum for applications running on the Linux OS. http://www.linuxfoundation.org/.

Microsoft Azure® Community. A developer forum for applications running on the Microsoft cloud Azure OS.
http://azure.microsoft.com/en-us/solutions/dev-test/.

Microsoft Internet Explorer®. A developer forum for applications running on the Microsoft IE browser.
https://msdn.microsoft.com/en-us/.

Microsoft Windows®. A developer forum for applications running on Microsoft Windows OS.
https://dev.windows.com/en-us.

Mozilla®. A developer forum for applications running on the Mozilla platforms. https://developer.mozilla.org/en-US/.

OpenShift® Developer Community. A developer forum for applications running on the OpenShift Cloud OS.
https://openshift.redhat.com/app/platform.

OpenStack Developer Community. A developer forum for applications running on the OpenStack OS.
http://www.rackspace.com/blog/.

Opera Software. A developer forum for applications running on the Opera browser platform.
http://www.opera.com/developer.

Oracle® Cloud Computing. A developer forum for applications running on the Oracle Cloud platform.
http://www.oracle.com/us/technologies/cloud/index.html.

Oracle Java®. A developer forum for applications running on the Java OS.
http://www.oracle.com/technetwork/java/index.html.

Oracle® Solaris/Trusted Solaris. A developer forum for applications running on Solaris OS.
http://www.oracle.com/us/sun/index.htm.

ProgrammableWeb. A developer forum for applications running on the Programmable Web platform.
http://www.programmableweb.com/.

Qihoo 360. A developer forum for applications running on the Qihoo 360 browser. http://se.360.cn/.

SourceForge. A developer software exchange forum, http://sourceforge.net/.

TopCoder™. http://www.topcoder.com/.

VMware® Community. A developer forum for applications running the VMware OS.
http://communities.vmware.com/groups/.

XDA Developers Forum. A developer software exchange forum. http://forum.xda-developers.com/.

4.4   Activities for continuous information exchange

ACSC - Australian Cyber Security Centre. Australia-based, the ACSC in the Defence Signals Directorate is a Defence capability serving whole of government cyber security needs to detect and defeat sophisticated cyber threats. The ACSC provides cyber situational awareness and an enhanced ability to facilitate coordinated responses to, and management of, cyber security events of national importance. https://www.asd.gov.au/.

CERT-FR. The French CERT is the principal governmental centre for watch, warning and response to computer attacks, and operated by ANSSI and SGDSN. https://www.cert.ssi.gouv.fr/.

CCIRC - Canadian Cyber Incident Response Centre. Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber events. It does this by providing authoritative advice and support, and coordinating information sharing and event response. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx.

China National Vulnerability Database of Information Security. China based. CNNVD Identifier allows responsible researchers, vendors, and incident response teams to include CNNVDs in the initial public announcement of a vulnerability. It ensures that a CNNVD number is instantly available to all CNNVD users and makes it easier to track vulnerabilities over time. Cross referenced to CVEs where possible. http://www.cnnvd.org.cn/.

CVE™ Numbering Authorities. U.S. based with global centres. CVE Identifier (CVE-ID) reservation allows responsible researchers, vendors, and incident response teams to include CVE-IDs in the initial public announcement of a vulnerability. It ensures that a CVE-ID number is instantly available to all CVE users and makes it easier to track vulnerabilities over time. https://cve.mitre.org/cve/cna.html.

GSMA™ - GSM Association. GSMA operates several cyber security related databases, including the global IMEI (International Mobile Station Equipment Identity) database for authoritative determination of mobile phone integrity. https://imeidb.gsma.com/imei/index#.

FS-ISAC. The Financial Services Information Sharing and Analysis Center, is the global financial industry's go to resource for cyber and physical threat intelligence analysis and sharing. FS-ISAC is unique in that it was created by and for members and operates as a member-owned non-profit entity. https://www.fsisac.com/about.

JVN - Japan Vulnerability Notes. Operated under the JPCERT/CC, vulnerability information and mitigations for software products reported in Japan. https://jvn.jp/en/.

MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing - Luxembourg. MISP, via CIRCL, is driving both some of the largest communities and the development of the MISP threat intelligence sharing platform. The purpose of the platform is to allow its user-base to exchange and collaborate on a wide range of threat data, ranging from technical indicators of compromise, through financial fraud indicators to threat actor information. MISP encompasses a complete and extensive data-model and exchange format to support the standardisation of information exchange within IETF and MISP standard initiative. CIRCL being an OASIS member is actively sharing their experiences in building the next information exchange formats. The communities utilizing Luxembourg operated MISP instances host over 1 200 organizations from various sectors from within the CERT community, the financial sector, military and international organizations, security vendors and various private organizations. https://www.circl.lu/services/misp-malware-information-sharing-platform/ https://github.com/MISP/.

MELANI - Reporting and Analysis Centre for Information Assurance. Swiss based. Within MELANI, the Reporting and Analysis Centre for Information Assurance, partners work together who are active in the area of security of computer systems and the Internet and protection of critical national infrastructures. http://www.melani.admin.ch/.

Nationales Cyber-Abwehrzentrum. In view of the growing cyber dangers, the federal authorities dealing with the relevant facets of this issue are working together more closely - the joint cyber-defense centre (Cyber-AZ). https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html.

National Checklist Program Repository. U.S. based. The National Checklist Program (NCP), defined by the NIST SP 800-70 [i.3], is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. http://web.nvd.nist.gov/view/ncp/repository.

National Council of ISACs. https://www.nationalisacs.org/.

National Cyber Security Center. The NCSC acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents. Multiple nations now operate NCSC organizations for information exchange, although the most prominent is in the UK. https://www.ncsc.gov.uk/. See individual national cyber strategy subclauses in annex A.

National Vulnerability Database. U.S. based. NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. https://web.nvd.nist.gov/view/vuln/search.

PHAROS - Platform for Harmonization, Analysis, Cross-check and Orientation of Reportings. http://www.internet-signalement.gouv.fr.

4.5 Centres of excellence

ACCS - Australian Centre for Cyber Security. ACCS is an interdisciplinary cyber security centre that brings together experts from UNSW Sydney and Canberra campuses and recognized by the Ministry of Defence. http://www.accs.unsw.adfa.edu.au/.

ARCSI - Association des Réservistes du Chiffre et de la Sécurité de l'Information. ARCSI is one of the main French associations in the field of digital security. Created in 1928 and with nearly 350 members, it brings together a considerable sum of talents and skills always ready to exchange on the most advanced subjects: mathematicians and cryptologists, engineers, teachers, researchers and technicians specialists in cryptology and/or cybersecurity but also lawyers, historians or journalists. Its activity is multiple: permanent updating of this website, daily exchanges on the association's mailing lists, edition of newsletters, organization of symposia or exhibitions, or participation in major events in the field. https://www.arcsi.fr/.

ACE-CSRs - Academic Centres of Excellence in Cyber Security Research. The NCSC and the Engineering and Physical Sciences Research Council (EPSRC) jointly recognize Academic Centres of Excellence in Cyber Security Research (ACE-CSR) and Centres for Doctoral Training (CDT). https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research. Nineteen universities are presently recognized at https://epsrc.ukri.org/research/centres/acecybersecurity/.

CCD COE - Cooperative Cyber Defence Centre of Excellence. CCD COE is an activity within NATO based in Estonia with a mission to enhance the capability, cooperation and information sharing among NATO, its member nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation. https://ccdcoe.org/.

European Cybersecurity Centres of Expertise. The EC is providing under Horizon 2020 a means to facilitate collaboration among European Cybersecurity Centres. https://ec.europa.eu/jrc/en/publication/european-cybersecurity-centres-expertise-map-definitions-and-taxonomy.

INRIA - Institut national de recherche en sciences et technologies du numérique. INRIA is France's principal national research institute for digital science and technology and consists of facilities at ten sites in France and includes the Carnot Institute. For more than 50 years it has served as a crossroads between the academic world and industry, positioned on the new frontiers of digital research, pioneer to bring out new disciplines from applied mathematics and computer science, pioneer to support the dynamics of technology start-ups in France and in Europe, the institute has been a visionary and pioneer in many fields (scientific computing, Internet, Web). https://www.inria.fr/fr/inria-son-ecosysteme.

NCCC - National Cyber Coordination Centre. Based in India, NCCC helps protect its critical ICT infrastructures. The NCCC comes under the National Information Board and is responsible for all forms of cyber intelligence and cyber security. The NCCC is expected to screen all forms of meta-data, ensure better coordination between various intelligence agencies and "streamline" intelligence gathering. To that end, it expands the charter of the Computer Emergency Response Team, India, (CERT-IN), which has the bulk of the government, public-private and private sectors under its jurisdiction. It is also the duty of the NCCC alert all relevant agencies during a cyber-attack and ensure better cyber intelligence sharing. https://www.cert-in.org.in/s2cMainServlet?pageid=PRESSLIST.

NCCoE - NIST National Cybersecurity Center of Excellence. The CCoE hosted by NIST provides businesses with real-world cybersecurity solutions-based on commercially available technologies. The centre brings together experts from industry, government and academia to demonstrate integrated cybersecurity that is cost-effective, repeatable and scalable. https://nccoe.nist.gov/.

SANS™ Institute - SysAdmin, Audit, Networking, and Security Institute. SANS is a source for information security training and security certification, as well as related available resources that include the Internet Storm Center, a weekly news digest (NewsBites), a weekly vulnerability digest (@RISK), and more than a thousand information security research papers. http://www.sans.org.

SERENE-RISC - Smart Cybersecurity Network. SERENE-RISC is a Canadian based mechanism for facilitating exchange of cyber security information. http://www.nce-rce.gc.ca/NetworksCentres-CentresReseaux/NCEKM-RCEMC/SERENE-RISC_eng.asp.

US National IA Education & Training Programs (NIETP). NSA and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cyber Defense (CD) Education (CAE-CDE), Two-Year Education (CAE-2Y) and Research (CAE-R) programs. The goal of these programs is to reduce vulnerability in US national information infrastructure by promoting higher education and research in CD and producing a growing number of professionals with CD expertise in various disciplines. http://www.iad.gov/NIETP/aboutCAE.cfm. Additionally, a CyberCorps®: Scholarship for Service program initially established in 2001 by the National Science Foundation has been expanded significantly. https://www.sfs.opm.gov/Overview-History.aspx.

4.6   Reference libraries, continuing conferences, and publications

ARCSI - Association des Réservistes du Chiffre et de la Sécurité de l'Information. ARCSI Bulletins contain an extensive history relating to cryptology and hosts cybersecurity conferences. https://www.arcsi.fr/bulletin.php.

Black hat® conference. An annual global conference begun in 1997 usually held in Las Vegas that provides attendees with the very latest in information security research, development, and trends in a strictly vendor-neutral environment. Smaller regional Black Hat conferences also exist. https://www.blackhat.com/.

Chaos Computer Club conference. An annual global conference begun in Berlin in 1981 and usually held in Hamburg that is dedicated to discovering cyber security exploits. http://www.ccc.de/en/.

Cryptologia. A journal in cryptography published quarterly since January 1977. Its remit is all aspects of cryptography, but there is a special emphasis on historical aspects of the subject. http://www.tandfonline.com/toc/ucry20/current#.VKGmTdTABA. An archive is also maintained as part of the ACM Digital Library at http://dl.acm.org/citation.cfm?id=J192&picked=prox&cfid=613942318&cftoken=65391965.

David Kahn Collection. Located in the United States, Ft. Meade, Maryland, as part of the National Cryptologic Museum. It contains the largest known collection of books (2 800) and notes on cryptology. It contains the first printed book on cryptology, Johannes Trithemius's Polygraphiae of 1518. The library also holds some of the oral histories taken by NSA's Center for Cryptologic History. https://cryptologicfoundation.org/visit/museum/acquisitions/special_acquisition_items/acquisitions_special.html.

DEF CON conference. An annual global conference begun in 1993 usually held in Las Vegas that is dedicated to discovering cyber security exploits. https://www.defcon.org/.

Forum International de la Cybersécurité (FIC). FIC is dedicated to exchanges of views and professional meetings, and becomes a leading European event on cybersecurity security and digital trust. Its mixes reflection and exchanges among the European cybersecurity ecosystem and vendors of cybersecurity solutions. https://www.forum-fic.com/en/home/discover/what-is-the-fic.htm.

ETSI Security Week. An annual global conference addressing key cybersecurity standardization challenges in the short, medium and longer term. The event look at the different aspects of cybersecurity underpinning the digital world. https://www.etsi.org/securityweek.

IEEE/ACM International Conference on Cyber-Physical Systems (ICCPS). An annual conference held at diverse global locations devoted in part to cyber-physical security research. http://iccps.acm.org/2020/.

IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. The Japan Institute of Electronics, Information and Communication Engineers aims at the investigation and exchange of knowledge on the science and technology of electronics, information and communications, and contributes to the progress of technologies and to the development of industries. https://www.ieice.org/eng/shiori/mokuji_ess.html.

International Journal of Engineering and Technology. International Journal of Engineering and Technology (IJET) is a scholarly open access, peer-reviewed, interdisciplinary, quarterly and fully refereed journal focusing on theories, methods and applications in Engineering and Technology. http://www.enggjournals.com/ijet/.

Meridian Conference. The Meridian process aims to exchange ideas and initiate actions for the cooperation of governmental bodies on Critical Information Infrastructure Protection (CIIP) issues globally. https://www.meridianprocess.org/About/.

Munich security conference (MSC). A global forum for debating international security policy, its Cyber Security and Technology Series, focuses on the impact of technological changes and the chances and risks in a digital world. https://securityconference.org/en/topics/cyber-security/.

PrivSec. PrivSec conferences are part of Data Protection World Forum's series of global events. https://london.privsec.info/.

RSA® conference. An annual global conference begun in 1991 usually held in San Francisco that is dedicated to presentations and discussion of current a cryptography and information security-related developments. Regional RSA conferences also exist. http://www.rsaconference.com/.

World Congress of the International Federation of Automatic Control (IFAC). Annual conference begun in 1960 devoted in part to cyber security research. http://www.ifac-control.org/events/congresses.

4.7   Heritage sites and historical collections

ARCSI - Association des Réservistes du Chiffre et de la Sécurité de l'Information. In addition to other roles and activities, ARCSI provides for a historical and account of cryptologic history for the French national security community. It hosts special programs and events in the field. https://www.arcsi.fr/.

Bletchley Park. Located in United Kingdom, Milton Keynes, Buckinghamshire, it maintains several museums detailing the fundamental advancements in cryptographic technologies, signals analysis, and programmable computational techniques and devices that occurred between 1936 and 1946. The collection includes a reconstructed Turing Bombe decoding machine and the Colossus computer. http://www.bletchleypark.org.uk/.

Center for Cryptologic History (CCH). As part of the National Security Agency, the CCH provides a historical and objective account of cryptologic history for the U.S. Intelligence Community, the Department of Defense, other government agencies, academia, and the general public. It hosts special programs and events explores the impact of history on current issues and operations. Its most prominent event is the open global biennial symposium. https://www.nsa.gov/about/cryptologic-heritage/center-cryptologic-history/.

Crypto Museum. Located in the Netherlands, it maintains an extensive collection of cryptographic materials. http://www.cryptomuseum.com/.

Deutsches Museum. Located in Munich Germany, it maintains a collection of encryption devices and machines that fundamentally advanced telecommunication security using cryptographic techniques. http://www.deutsches-museum.de/de/ausstellungen/kommunikation/informatik/kryptologie/.

Musée des Transmissions. Located in Cesson-Sévigné near Rennes, Paris, and honouring radio pioneer and WW-1 signals intelligence leader Gustave-Auguste Ferrié, the Museum of the Army, the Museum of Transmissions - Espace Ferrié contains collections and exhibits dedicated to military telecommunication and intelligence. http://www.espaceferrie.fr/.

National Cryptologic Museum. Located in the United States, Ft. Meade, Maryland, it is the U.S. National Security Agency's principal gateway to the public. https://www.nsa.gov/about/cryptologic-heritage/museum/. It shares the USA, as well as NSA's, cryptologic legacy and place in world history. The Museum houses a collection of thousands of artefacts that collectively serve to sustain the history of the cryptologic profession. The National Cryptologic Museum Foundation is undertaking the creation of a new Cyber Center for Education and Innovation as part of its master plan for the future. http://cryptologicfoundation.org/visit/goal/.

4.8   Additional exchange sources and methods

4.8.1   Twitter accounts

Some individual social media accounts dealing with cyber security have substantial followings and effects to justify inclusion as part of the larger ecosystem:

- Dejan Kosutic (Croatia) - @Dejan_Kosutic

- Chris Roberts (US) - @Sidragon1

- Eugene Kaspersky - @e_kaspersky

- Nicolas Caproni (FR) - @ncaproni

- Charles Ibrahim - @Ibrahimous

- Jean-Marc Manach (FR) - @manhack

- Ken Westing (US) - @kwestin

- Bruce Schneier (US) - @schneierblog

- Team Cymru - @teamcymru

- Kristin Paget (US) - @KristinPaget

- Mathieu Destrian (France) - @MathieuDestrian

- Troy Hunt (Australia) - @havibeenpwned

- Lukasz Olejnik - @lukOlejnik

4.8.2   Web sites

Some web sites dealing with cyber security have substantial followings and effects to justify inclusion as part of the larger ecosystem:

- ANSSI (https://www.ssi.gouv.fr)

- CLUSIF (http://www.clusif.fr/)

- DEFCON (https://media.defcon.org)

- Heise Security (https://www.heise.de/security/)

- Insinuator (https://insinuator.net/)

- Kaspersky blog (http://blog.kaspersky.com/)

- Krebs on Security (https://krebsonsecurity.com/)

- NORSE (https://norse-corp.com/map/)

- OWASP (https://www.owasp.org/index.php/Main_Page)

- Qualys® SSL Labs (https://www.ssllabs.com/ssltest/)

- Schneier blog (https://www.schneier.com/)

- The Hacker News™ (http://thehackernews.com/)

- Threat post (https://threatpost.com/)

- Wired (https://www.wired.com/)

4.8.3   Diffusion lists

Some diffusion lists dealing with cyber security have substantial followings and effects to justify inclusion as part of the larger ecosystem:

- Industrial Control Systems Cyber Emergency Response Team (https://ics-cert.us-cert.gov/ics-archive)

- IGF Bpf (http://intgovforum.org/mailman/listinfo/bpf-cybersecurity_intgovforum.org)

- CERT-EU (http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html)

- CISA - CERT-US (https://www.us-cert.gov/)

- GSMA™ Fraud and Security Group (http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group)

- Hunton Privacy & Information Security blog (https://www.huntonprivacyblog.com/)

- Security Mailing List Archive (http://seclists.org/)

- The Hacker News™ (http://thehackernews.com/)

Annex A:
National cyber security ecosystems

The national ecosystems described in this annex have been either described in their national cyber security strategies or available material. See NATO Cooperative Cyber Defence Center of Excellence. See also, ITU-D National Cybersecurity Strategies Repository at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx. See also Cybersecurity Country Profiles at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Forms/AllItems.aspx. ENISA also maintains a repository of EU member strategies and related materials at https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

Afghanistan

Afghanistan's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence and its Ministry of Communications and Information Technology. See https://mcit.gov.af/node/7082.

Albania

Albania's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Australia

Australia's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

ACMA - Australian Communications and Media Authority. http://www.acma.gov.au/.

- **AFP - Australian Federal Police**. http://www.afp.gov.au/.

- **AGD - Attorney-General's Department**. The AGD delivers programs and policies to maintain and improve Australia's law and justice framework, strengthen its national security and emergency management. The CERT Australia is located in the AGD. http://www.ag.gov.au/about/Pages/default.aspx.

- **AGIMO - Australian Government Information Management Office**. http://www.finance.gov.au.

- **AISI** - **Australian Internet Security Initiative**

- **ASIO - Australian Security Intelligence Organisation**. ASIO's main role is to gather information and produce intelligence that will enable it to warn the government about activities or situations that might endanger Australia's national security. http://www.asio.gov.au/.

- **CIPMA** - **Critical Infrastructure Protection Modelling and Analysis**

- **CSPC - Cyber Security Policy and Coordination Committee**. CSPC is the Australian Government interdepartmental committee that coordinates the development of cyber security policy for the Australian Government.

- **Department of Communications**. http://www.communications.gov.au/.

- **DSD - Defence Signals Directorate**. Within the DOD (Department of Defence), the DSD is the national authority on the security of ICT across government. DSD, through the CSOC, is responsible for maintaining a comprehensive national picture of cyber security threats, through monitoring and analysis of all information sources. DSD works with ASIO and AFP to protect the National Information Infrastructure (NII) under the Joint Operating Arrangements (JOA). This includes the ACSC (Australian Cyber Security Centre), CSOC (Cyber Security Operations Centre) and ISM (Australian Government Information and Communications Technology Security Manual). http://www.asd.gov.au/.

- **GovCERT.au - Australian Government's Computer Emergency Readiness Team**

- **IAAGs - Infrastructure Assurance Advisory Groups**

- **IRAP - Information Security Registered Assessors Program**

- **IWWN - International Watch and Warning Network**

- **NSSIS - National Security Science and Innovation Strategy**

- **TISN - Trusted Information Sharing Network for Critical Infrastructure Protection**

Austria

Austria's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **ACI - Austrian Critical Infrastructure (Österreichische kritische Infrastruktur)**

- **ACSS - Austrian Cyber Security Strategy (Österreichische Strategie für Cyber Sicherheit (ÖSCS))**

- **APCIP - Austrian Programme for Critical Infrastructure Protection (Österreichisches Programm zum Schutz kritischer Infrastruktur)**

- **A-SIT - Secure Information Technology Centre - Austria (Zentrum für sichere Informationstechnologie - Austria)**

- **ASS - Austrian Security Strategy**

- **CERT.at - Computer Emergency Response Team - Austria**

- **CII - Critical Information Infrastructures (Kritische Informationsinfrastrukturen)**

- **GovCERT - Governmental Computer Emergency Response Team (Staatliches Computer Emergency Response Team)**.

- **MilCERT - Military Computer Emergency Response Team (Militärisches Computer Emergency Response Team)**.

Azerbaijan

Azerbaijan's Cybersecurity Strategy and additional material are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

Bangladesh

Bangladesh's Cybersecurity Strategy and additional material are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

Belgium

Belgium's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **ADCC - Algemene Directie Crisiscentrum**

- **ADIV - Algemene Dienst Inlichting en Veiligheid**

- **ANS - Autorité National de Sécurité**

- **BCSS - Banque Carrefour de la Sécurité Sociale**

- **Belac - Organisme belge d'Accréditation (Belac Belgische Accredidatie-instelling)**

- **Belnet - Belgian national research network**

- **BelNIS - Belgian Network Information Security**

- **BIPT - Belgisch Instituut voor postdiensten en telecommunicatie**

- **CBPL - Commissie voor de bescherming van de persoonlijke leverssfeer**

- **CCSB - Centre pour Cyber Sécurité Belgique (Centrum voor Cyber Security Belgie)**

- **CERT - Computer Emergency Response Team**

- **CMRS - Comité ministériel du renseignement et de la sécurité**

- **CPVP - Commission de la protection de la vie privée**

- **DGCC - Direction Générale Centre de Crise**

- **ESA - European Space Agency**

- **FCCU - Federal Computer Crime Unit**

- **Fedict - FOD - voor informatie-en Communicatietechnologie**

- **Fedoct - SPF Technologie de l'Information et de la Communication**

- **FOD - Federal Overheidsdienst**

- **IBPT - Institut belge des services postaux et des télécommunications**

- **KSZ - Kruispuntbank van de Sociale Zekerheid**

- **MCIV - Ministerieel Comité voor inlichting en veiligheid**

- **OCAD - Coördinatieorgaan voor dreigingsanalyse**

- **OCAM - Organe de coordination pour l'analyse de la menace**

- **SGRS - Service Général du Renseignement et de la Sécurité**

- **SPF - Service Public Fédéral**

- **VSSE - Veiligheid van de Staat, Sûreté de l'Etat**

Bosnia and Herzegovina

Bosnia and Herzegovina's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Botswana

Botswana's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Brazil

Brazils Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Bulgaria

Bulgaria's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Canada

Canada's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **CSEC - Communications Security Establishment Canada**. CSEC is the Government of Canada's cryptologic agency responsible for the collection of cyber foreign intelligence and Canada's interface with the international cryptologic community. It undertakes classified research and development for cyber security. CSEC monitors and defends Government of Canada networks by detecting, discovering and responding to sophisticated cyber threats to the Government, and provides mitigation and recovery advice and guidance to Government departments to help them recover from cyber incidents. https://www.cse-cst.gc.ca/.

- **CSIS - Canadian Security Intelligence Service**. CSIS conducts national security investigations, reports to and advises the Government of Canada of activities constituting a threat to the security of Canada as defined in the Canadian Security Intelligence Service Act. It provides analysis to assist the Government of Canada in understanding cyber threats, and the intentions and capabilities of cyber actors operating in Canada and abroad who pose a threat to the security of Canada. https://www.canada.ca/en/security-intelligence-service.html.

- **DRDC - Defence Research and Development Canada**. DRDC leads the development of military cyber security science and technology (S&T). The DRDC Centre for Security Science (DRDC CSS) leads, in partnership with Public Safety Canada, cyber security S&T efforts that are not specifically assigned to another department or agency. These activities fall under the Canadian Safety and Security Program (CSSP). http://www.drdc-rddc.gc.ca/.

- **ISEDC - Innovation, Science and Economic Development Canada**. IC is responsible for fostering a robust and reliable telecommunications system. It develops policies to ensure a safe and secure online marketplace and helps to ensure the continuity of telecommunications during an emergency. http://www.ic.gc.ca/.

- **PSC - Public Safety Canada**. PSC houses the Government Operations Centre as the hub of the National Emergency Response System (NERS). The Canadian Cyber Incident Response Centre (CCIRC) escalates cyber incidents of national significance to the Government Operations Centre which then helps coordinate a national response. http://www.publicsafety.gc.ca/.

- **RCMP - Royal Canadian Mounted Police**. RCMP leads the criminal investigative response to suspected criminal cyber incidents, such as the unauthorized use of a computer and mischief in relation to data. It leads the investigative response to suspected criminal national security cyber incidents and assists domestic and international partners with advice and guidance on cyber crime threats. http://www.rcmp-grc.gc.ca/.

- **Cyber Centre - Canadian Center for Cyber Security**. The Centre is Canada's authority on cyber security. It unites existing operational cyber security expertise from Public Safety Canada, Shared Services Canada, and the Communications Security Establishment in to one high-functioning, responsive organization. It includes the National CERT and the Government of Canada CIRT. https://cyber.gc.ca/en/about-cyber-centre.

Chile

Chile's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

China

China's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **CNCERT/CC - National Computer Network Emergency Response Technical Team/Coordination Center**. CNCERT is the coordination team for China's cybersecurity emergency response community. CNCERT strives to improve China's cybersecurity posture, and protect critical infrastructure cybersecurity. CNCERT leads efforts to prevent, detect, warn and coordinate the cybersecurity threats and incidents. http://www.cert.org.cn/publish/english/index.html.

- **MIIT - Ministry of Industry and Information Technology**. MIIT is a state agency responsible for regulation and development of the postal service, Internet, wireless, broadcasting, communications, production of electronic and information goods, software industry and the promotion of the national knowledge economy. MIIT and its various bodies represent China in international activities dealing with cyber security. http://www.miit.gov.cn/n11293472/index.html.

- **CAC - Cyberspace Administration of China or Office of the Central Leading Group for Cyberspace Affairs**. The CAC includes an Internet Security Emergency Command Center, an Agency Service Center, and an threat information reporting centre. http://www.cac.gov.cn/.

- **CCSA - China Communications Standards Association**. CCSA TC8 (Network and Information Security) corresponding to ITU-T SG17, 3GPP SA3, IETF, etc. http://www.ccsa.org.cn/english/.

- **TC260 - National Information Security Standardization Technical Committee**. A standardization group in charge of security standards development that includes the security guidelines for cloud security. http://www.tc260.org.cn/.

- **SAC - Standardization Administration of China**. SAC has responsibilities by management and coordination of ISO and IEC standardization work in China. http://www.sac.gov.cn/sacen/.

- **CAICT - China Academy of Information and Communication Technology**, previously known as China Academy of Telecommunication Research (CATR), it is responsible for a broad array of security standards and development of techniques. http://www.catr.cn/.

- **CESI - China Electronics Standardization Institute**. A professional institute for standardization in the field of electronics and IT industry under the Ministry of Industry and Information Technology (MIIT). The core business of CESI is standardization work in the field of electronics and information technology. By developing scientific research for standards, testing, measurement, certification and information evidences provides professional support for the government's strategic study, industry management and strategic decision, and provides technical service in standardization field to the society. http://www.cesi.cn.

- **ISC - Internet Society of China**. ISC has more than 400 members which are legal companies, research institutes, academic associations, universities and other organizations engaged in various activities related with Internet. The main mission of ISC is to promote development of Internet in China and make efforts to construct an advanced information society. http://www.isc.org.cn/english.

Colombia

Colombia's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Costa Rica

Costa Rica's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Croatia

Croatia's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Cyprus

Cyprus' Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Czech Republic

Czech Republic's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Denmark

Denmark's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Egypt

Egypt's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **ITIDA - Information Technology Industry Development Agency**

- **MCIT - Ministry of Communications and Information Technology**

- **NTRA - National Telecommunication Regulatory Authority**

Estonia

Estonia's Cybersecurity Strategy and additional material are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

Finland

Finland's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **FICORA - Finnish Communications Regulatory Authority**. The National Cyber Security Centre Finland (NCSC-FI) at FICORA issues alerts, Information security articles and vulnerability reports. https://www.viestintavirasto.fi/en/cybersecurity.html.

- **TUVE - turvallisuusverkkohanke (Network security project)**

- **UVTA U - lko- ja turvallisuuspoliittinen ministerivaliokunta (Committee on Foreign and Security Policy)**

- **VAHTI - Valtionhallinnon tietoturvallisuuden johtoryhmä (Government Information Security Management Board)**

- **YTS - Yhteiskunnan turvallisuusstrategiassa Cyber security strategy**

France

France's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **AFNOR - Association Française de Normalisation (French Association of standardization)**. AFNOR is one of France's principal standards development bodies - representing it especially in ISO/IEC. http://www.afnor.org/.

- **ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information (National agency for information systems security)**. As such it is responsible for proposing rules for the protection of state information systems and verify the implementation of measures adopted. In the field of defense information systems, it provides capabilities to monitor, detect, alert and reaction to computer attacks, including state networks. https://www.ssi.gouv.fr/.

- **ARCSI - Association des Réservistes du Chiffre et de la Sécurité de l'Information**. ARCSI serves as an educational and collegial mechanism in conjunction with government agencies.

- **COMCYBER - Commandement de cyberdéfense**. COMCYBER exists under the Chief of Staff of the Armed Forces unites all of the cyber defense forces of the French armies under a common operational, permanent and joint authority. The COMCYBER is responsible for the protection of information systems placed under the responsibility of its Chief, the conduct of the defense of the information systems of the Ministry (excluding those of the DGSE and DRSD) and the design, planning and conduct of military cyber defense operations, under the authority of the Deputy Chief of Staff of operations. https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation.

- **DGSE - Direction générale de la Sécurité extérieure**. DGSE is the external intelligence service of France. It works in cooperation with the DGSI in order to protect the vital interests of the nation, in the counter-terrorist and paramilitary fields, including economic intelligence. https://www.defense.gouv.fr/dgse.

- **DRSD - Direction du renseignement et de la sécurité de la Défense**. DRDE has responsibility for the security of defense sensitive personnel, information, equipment and facilities. https://www.drsd.defense.gouv.fr.

- **Ministère de l'Intérieur**. The Ministry of the Interior is responsible for ensuring national public safety, and includes the gendarmerie, the police and intelligence services in the cybersphere on a daily basis to combat threats directed at Internet users. https://www.interieur.gouv.fr/.

- **SGDSN - Secrétariat Général de la Défense et de la Sécurité Nationale (General secretariat of defence and national security)**. Ensures cyber defence. http://www.sgdsn.gouv.fr/.

- **Office of Strategic Coordination**.

    - **SDLC - Sub directorate against Cybercrime**

    - **OIV - Opérateur d'importance vitale (Critical Infrastructure operator)**

    - **RGS - Référentiel général de sécurité (General security framework)**

Gambia

Gambia's Cyber Security Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Georgia

Georgia's Cyber Security Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Germany

Germany's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **BBK - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe**. BBK has the task of providing information on the significance of KRITIS for the State and for society, of creating an awareness among enterprises and in the public, of describing the structures, functioning and interdependences of critical infrastructures, of establishing and intensifying cooperation between authorities and enterprises, of developing and refining analysis and protection concepts for KRITIS, and of proposing short-, medium- and long-term measures to protect critical infrastructures. https://www.bbk.bund.de/.

- **BfV - Bundesamt für Verfassungsschutz**. Nationales Cyber-Abwehrzentrum (National Cyber Response Centre) has been established in Germany. It began its work in April 2011 and aims at optimizing the co‑operation of state authorities e.g. through the co-ordination of protective and response measures taken against IT incidents. BfV is one of the partners contributing to the Response Centre. http://www.verfassungsschutz.de/.

- **BMI - Bundesministerium des Innern**. https://www.bmi.bund.de/.

- **BSI - Bundesamt für Sicherheit in der Informationstechnik**. https://www.bsi.bund.de/.

- **BCM - Business Continuity Management**

- **DIN - Deutsches Institut für Normung**. DIN is a national standards body that represents German interests in European and international standards organizations. Notably, it serves as the ISO/IEC JTC1 SC27 secretariat. http://www.din.de/en.

- **KITS - Koordinierungsstelle IT-Sicherheit**. The coordination office for IT-Security assigned to the DIN presidential committee FOCUS.ICT. http://www.kits.focusict.de/.

- **KRITIS - Kritische Infrastrukturen**

- **LÜKEX - Länderübergreifende Krisenmanagement Exercise**

- **NPSI - Nationaler Plan zum Schutz der Informationsinfrastrukturen**

- **PDCA - plan-do-check-act**

- **UP KRITIS - Umsetzungsplan KRITIS**

Ghana

Ghana's Cyber Security Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Greece

Greece's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Grenada

Grenada's Cyber Security Strategy and additional material are available through the https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Grenada.pdf.

Hungary

Hungary's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **NSA - National Security Authority**

Iceland

Iceland's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

India

India's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **CERT-in - National Level Computer Emergency Response Team**

- **DeitY - Department of Electronics & Information Technology**

- **NCIIPC - National Critical Information Infrastructure Protection Centre**

- **NCCC - National Cyber Coordination Centre**

Ireland

Ireland's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Italy

Italy's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **AGCOM - Autorità per le Garanzie nelle Comnicazioni**

- **CAN - Computer Network Attack**

- **CERT-PA - Computer Emergency Response Team of the Public Administration**

- **CERT-PA - CERT - Pubblica Amministrazione**

- **CERT-SPC - CERT Sistema Pubblico de Connettività**

- **CISR - Comitato interministeriale per la sicurezza della Repubblica**

- **CNAIPIC - Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastructure Critiche**

- **CND - Computer Network Defence**

- **CNE - Computer Network Exploitation**

- **CNO - Computer Network Operations**

- **CPS - Cyber Physical System**

- **CSBM - Confidence and Security Building Measures**

- **DF - Digital Forensics**

- **ICE - Infrastrutture Critiche Europe**

- **IT - Infrastrutture Critiche**

- **UTM - Unified Threat Management**

Jamaica

Jamaica's Cyber Security Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Japan

Japan's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **JPCERT/CC - the Japan Computer Emergency Response Team Coordination Center**. JPCERT/CC coordinates with network service providers, security vendors, government agencies, as well as the industry associations, acting as a "CSIRT of CSIRTs" for the Japan in the Asia Pacific region. https://www.jpcert.or.jp/english/about/.

- **APCERT - Asia Pacific Computer Emergency Response Team**

- **ARIB - Association of Radio Industries and Businesses**

- **CSSC - Control System Security Center**

- **ICPO - International Criminal Police Organization**

- **JASPER - Japan-ASEAN Security PartnERship**

- **NICT - National Institute of Information and Communications Technology**

- **NISC - National Information Security Center**

- **PRACTICE - Proactive Response Against Cyber-attacks**

- **TSUBAME - International network traffic monitoring project**

Jordan

Jordan's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **CNIP - Critical National Infrastructure Protection Program**

- **CSOC - National Cyberspace Security Operations Centre**

- **JOCERT - National Computer Emergency Response Team**

- **NEC - National Encryption Centre**

- **NIACSA - National Information Assurance and Security Agency**

- **NIACSS - National Information Assurance and Cyber Security Strategy**

- **NITC - National Information Technology Center**

- **NSS - National Security Strategy**

Kenya

Kenya's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **CAK - Communications Authority of Kenya**

Korea (South)

Korea's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **KCC - Korea Communications Commission**

- **MOPAS - Ministry of Public Administration and Security**

- **NCIA - National Computing and Information Agency**

- **NCSC - National Cyber security center**

- **NIS - National Intelligence Service**

- **TTA - Telecommunications Technology Association**

- **TTC - Telecommunication Technology Committee**

Latvia

Latvia's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **CDU - Cyber Defence Unit of the National Armed Forces**

- **CERT.LY - Information Technology Security Incident Response Institution**

- **CPB - Constitution Protection Bureau**

- **DISS - Defence Intelligence and Security Service**

- **DSI - Data State Inspectorate**

- **FCMC - Financial and Capital Market Commission**

- **MOD - Ministry of Defence**

- **MoE - Ministry of Economics**

- **MoEPRD - Ministry of Environmental Protection and Regional Development**

- **MoES - Ministry of Education and Science**

- **MoFA - Ministry of Foreign Affairs**

- **MoI - Ministry of the Interior**

- **MoJ - Ministry of Justice**

- **MoT - Ministry of Transport**

- **Mow - Ministry of welfare**

- **NAF - National Armed Forces**

- **NetSafe - Safer Internet Centre of Latvia Net-Safe Latvia**

- **SeP - Security Police**

- **SIS State information systems**

- **SP - State Police**

- **SRDA - State Regional Development Agency**

Lithuania

Lithuania's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **CERT-LT - National Electronic Communications Network and Information Security Incidents Investigation Service**

- **CTWIN - Critical Infrastructure Warning Information Network**

- **Litnet CERT - computer emergency response team**. https://cert.litnet.lt/en/.

- **NCSC** - National Cyber Security Centre. NCSC at the Ministry of National Defence is the main Lithuanian cyber security institution, responsible for unified management of cyber incidents, monitoring and control of the implementation of cyber security requirements, accreditation of information resources. https://www.nksc.lt/en/.

Luxembourg

Luxembourg's Cyber Security Strategy and additional material are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **ANSSI** - Agence nationale de la sécurité des systèmes d'information. ANSSI is the national authority with respect to security of classified and unclassified information systems established and operated by the government and the operators of critical infrastructures for their own purposes. Its mission is to define policies and guidelines for the security of classified and unclassified information, and to ensure that the necessary measures regarding the security of information systems are implemented and that their application is guaranteed. ANSSI operates the national and governmental CERT.

- **CERT.LU** - Grouping of all Luxembourg CERTs.

- **CNPD - The National Commission for Data Protection** (Commission Nationale pour la Protection des Données - CNPD) is an independent authority created by the Act of 1 August 2018 on the organization of the National Data Protection Commission and the general data protection framework. It verifies the legality of the processing of personal data and ensures the respect of personal freedoms and fundamental rights with regard to data protection and privacy. Its mission also extends to ensuring the respect of the amended Act of 30 May 2005 regarding the specific rules for the protection of privacy in the sector of electronic communications.

- **CSSF - Commission de surveillance du secteur financier**. CSSF is the competent authority for the security of networks and information systems covering the sectors of credit institutions and financial market infrastructures, as well as the digital services provided by an entity falling under the supervision of the CSSF.

- **GovCERT** - CERT gouvernemental du Grand-Duché de Luxembourg (GOVCERT.LU). GOVCERT is the single point of contact dedicated to the treatment of all significant computer related incidents jeopardizing the information systems of the government and defined critical infrastructure operators operating in Luxembourg, whether they are public or private. As national CERT it acts as the official national point of contact for natural and legal persons, entities and bodies, both national and international.

- **HCPN - The High Commission for National Protection** (Haut-commissariat à la Protection nationale, HCPN) is a body that falls under the responsibility of the Prime Minister and Minister of State. Its main mission is to ensure that the nation is always and in all circumstances protected against threats that could seriously infringe upon the country's sovereignty and independence, the free functioning of its institutions, the safeguarding of its national interests and the safety of the population. The ANSSI and the GOVCERT is attached to the High Commission for National Protection.

- **Healthnet CSIRT** - HealthNet is a telematics platform dedicated to the health sector, which aims to provide health professionals and institutions in the sector: infrastructure allowing them to communicate securely, electronic basic services like email exchanges and internet access, specialized applications for the exchange of results of medical tests, the double reading and program coordination mammography and the future of telemedicine applications such as teleradiology, telepathology and telemonitoring.

- **ILNAS** - The Luxembourg institute for standardisation, accreditation, safety, and quality of goods and services (ILNAS, "Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services") is the national standards body, representing the Luxembourg interests in European and international standards organizations. In the frame of the national ICT Technical Standardization Policy (https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/orientations-strategiques/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2015-2020/policy-ict-technical-standardization-2015-2020.pdf), ILNAS is developing and supporting the promotion of digital trust domain and related technical standardization (https://portail-qualite.public.lu/content/dam/qualite/publications/confiance-numerique/white-paper-digital-trust-september-2017.pdf).

- **ILNAS**, via the "Digital trust department", is also charged with the supervision of QTSPs (Qualified Trust Service Providers) that are established in the Grand Duchy of Luxembourg and offer qualified trust services, and of PSDCs ("Prestataires de services de dématérialisation ou de conservation") that are established in the Grand Duchy of Luxembourg and offer services related to digitization or e-archiving of documents.

- **ILR - Institut Luxembourgeois de Régulation**. ILR is the competent authority for the security of networks and information systems in the following fields: Energy, Transport, Health, Drinking water supply and distribution and Digital infrastructure as well as digital services. ILR is also the regulation authority for security and integrity of networks and services in the electronic communication sector.

- **Restena CSIRT** - RESTENA CSIRT represents the research and educational community of Luxembourg. The RESTENA Foundation brings together all types of research and teaching bodies, as well as the ministries for education, research and of finance. The primary objective is to provide network services for all public and private institutions involved in the field of education, research and administration, providing them with cutting-edge solutions for their communication needs. The Foundation also co-ordinates Internet resources nationally, by managing the registry for .LU domain names and by actively participating in the operation of the neutral platform for the exchange of Internet traffic LU-CIX.

- **SECURITYMADEIN.LU** - As an agency of the Ministry of the Economy SECURITYMADEIN.LU serves the private sector in all questions related to cybersecurity. Its activities cover the full spectrum from technical expertise, digital forensics and incident response (DFIR), via its CIRCL department, through organizational security, aka governance, risk and compliance (GRC), via the CASES department, not to forget the human aspects with the Cybersecurity Competence Center (C3), the third department of SECURITYMADEIN.LU:

  - **CIRCL - The Computer Incident Response Center Luxembourg** (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg. CIRCL provides a reliable and trusted point of contact for any users, companies and organizations of its constituency, for the handling of attacks and incidents.

  - **CASES - Cyberworld Awareness and Security Enhancement Services**. The mission of CASES is to promote information security. CASES is mainly dedicated to the development of tools and services to prevent and manage security risks within Luxembourg administrations and SMEs. CASES also offers security trainings for various audiences.

  - **C3 - Cybersecurity Competence Center**. C3 brings together under one roof three fundamental pillars of digital security: an observatory for current threats and vulnerabilities; a training centre and simulation platform; a laboratory to test new products and digital solutions.

Malaysia

Malaysia's Cyber Security Strategy and additional material are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

Malta

Malta's Cybersecurity Strategy and additional material are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

Mauritania

Mauritania's Cyber Security Strategy and additional material are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

Mauritius

Mauritius's Cyber Security Strategy and additional material are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

Mexico

Mexico's Cyber Security Strategy and additional material are available through [the NATO Cooperative Cyber Defence Center of Excellence](#).

Mongolia

Mongolia's Cyber Security Strategy and additional material are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

Montenegro

Montenegro's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **MD - Ministry of Defence**

- **MI - Ministry of the Interior**

- **MIST - Ministry for Information Society and Telecommunications**

- **NSA - National Security Agency**

Morocco

Morocco's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **CNDP - National Commission for Data Protection**

- **MA-CERT - Morocco CERT**

Netherlands

The Netherlands's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **CHOD - Chief of Defence**

- **CSBN - Cybersecurity Beeld Nederland**

- **CSOC - Nationaal Cyber Security Operations Center**

- **DCEC   - Defence Cyber Expertise Centre**

- **DISS - Defence Intelligence and Security Service**

- **GISS - General Intelligence and Security Service**

- **NCSC - Nationaal Cyber Security Centrum**

- **NCSRA - Nationale Cyber Security Research Agenda**

- **NCSS - National Cybersecurity Strategie**

- **SIGINT-CYBER - Joint General Intelligence and Security Service Unit**

New Zealand

New Zealand's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **CCIP - Centre for Critical for Infrastructure Protection**

- **NCSC - National Cyber Security Centre**

- **NZ-CERT - New Zealand Computer Emergency Response Team**

- **NZSIS - New Zealand Security Intelligence Service**

Nigeria

Nigeria's Cyber Security Strategy and additional material are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

Norway

Norway's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **KIS - Koordineringsutvalget for forebyggende informasjonssikkerhet** (Information Security Coordination Council. https://www.regjeringen.no/globalassets/upload/FAD/Vedlegg/IKT-politikk/Handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf.

- **NorCERT - Norway CERT**

- **NorSIS - Norsk senter for informasjonssikring (Norwegian Centre for Information Security)**

- **NSM - Nasjonal sikkerhetsmyndighet (National Security Authority)**

- **SAMRISK - Samfunnssikkerhet og risiko**

- **SERI - Senter for rettsinformatikk (Norwegian Research Center for Computers and Law)**

- **SLT - samordning av lokale kriminalitetsforebyggende tiltak (coordination of local crime prevention measures)**

- **SN - Standard Norge**

Pakistan

Pakistan's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the [NATO Cooperative Cyber Defence Center of Excellence](#).

- **FIA - Federal Investigation Agency**

- **NFSA - National Forensic Science Agency**

- **PISA - Pakistan Information Security Association**

Panama

Panama's Cyber Security Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Poland

Poland's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **ABW - Agencja Bezpieczeństwa Wewnętrznego (ISA - Internal Security Agency)**

- **BBK - Biuro Badań Kryminalistycznych (Bureau of Forensic Laboratory)**

- **CERT Poland**

- **CERT.GOV.PL - Governmental Computer Security Incident Response Team (Rządowego Zespołu Reagowania na Incydenty Komputerowe)**

- **CRP - Cyberprzestrzeń Rzeczypospolitej Polskiej (Cyberspace Polish Republic)**

- **MNiSW - Ministerstwo Nauki i Szkolnictwa Wyższego (Ministry of Science and Higher Education)**

- **NASK - Naukowej i Akademickiej Sieci Komputerowej (Research and Academic Computer Network)**

- **PBC - pełnomocnika ds. bezpieczeństwa cyberprzestrzeni (PCS - plenipotentiary for cyberspace security)**

- **UKE - Urzędem Komunikacji Elektronicznej (Office of Electronic Communications)**

Portugal

Portugal's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Qatar

Qatar's Cyber Security Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Romania

Romania's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **COSC - Consiliul operativ de securitate cibernetică (Operational Cybersecurity Council)**

- **SNSC - Sistemul Național de Securitate Cibernetică (National Cyber Security System)**

Russia

Russia's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **ZNIIS - Центральный научно-исследовательский институт связи (Central Research Institute of Communications)**

Samoa

Samoa's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Saudi Arabia

Saudi Arabia's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **CERT-SA - CERT Saudi Arabia**

- **CIC - Critical Infrastructure Council**

- **MCIT - Ministry of Communications and Information Technology**

- **NCDC - National Center for Digital Certification**

- **NISE - National Information Security Environment**

- **NISE - NISE Instructions**

- **NISED - NISE Directives**

- **NISEMs - NISE Manuals**

- **NISS - National Information Security Strategy**

- **NRAF - National IS Risk Assessment Function**

- **SA CISRS - Saudi Arabian Critical Security and Resilience Strategy**

Singapore

Singapore's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **A*STAR - Agency for Science, Technology and Research**

- **ANSES - Ambient Network Secure Eco System**

- **CII-SA - Critical Infocomm Infrastructure Security Assessment**

- **CWC - Cyber Watch Centre**

- **IDA - Infocomm Development Authority of Singapore**

- **ISMP - Infocomm Security Master Plan**

- **MCI - Ministry of Communications and Information**

- **MHA - Ministry of Home Affairs**

- **MINDEF - Ministry of Defence**

- **MOF - Ministry of Finance**

- **NISC - National Infocomm Security Committee**

- **NRF - National Research Foundation**

- **NSCS - National Security Coordination Secretariat**

- **TAC - Threat Analysis Centre**

Slovakia

Slovakia's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **CSIRT.SK - national centre for computer security incidents**. **Slovakia**

- **NICI - National Information Security Authority**

- **NSA - National Security Authority (NBU - Národný bezpečnostný úrad)**

- **NSIS - National Strategy for Information Security in the Slovak Republic**

- **SOSMT - Slovak Standards Institute**

Slovenia

Slovenia's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

South Africa

South Africa's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **DoC - Department of Communications**

- **DoD&MV - Department of Defence and Military Veterans**

- **DOJ&CD - Department of Justice and Constitutional Development**

- **DST - Department of Science and Technology**

- **ICASA - Independent Communications Authority of SA**

- **JCPS - Justice, Crime Prevention and Security Cluster**

- **NCAC - National Cybersecurity Advisory Council**

- **NCPF - National Cybersecurity Policy Framework**

- **NCSC - National Cyber Security Coordinating Centre**

- **NPA - National Prosecuting Authority**

- **SAPS - South African Police Service**

- **SSA - State Security Agency**

Spain

Spain's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **AEPD - Spanish Data Protection Agency**

- **CCN - National Cryptologic Centre**

- **CCN-CERT - Spanish Government National Cryptologic Center CSIRT**

- **CERT-SI - Computer Emergency Response Team for Security and Industry**

- **CNI - National Intelligence Centre**

- **CNPIC - National Centre for Critical Infrastructure Protection, as part of the CNPIC:**

  - **OCC - Cybernetics Coordination Office**

- **CSN - National Security Council, two specific specialized committees assist the CSN with the operation of the Cyber Security Strategy:**

  - **CNC - National Cyber Security Council**

- **Specialised Situation Committee**

- **DSN - National Security Department**

- **EMAD - Chiefs of the Defence Staff**

- **ESPCERTDEF - Computer Emergency Response Team in the field of the Ministry of Defence**

- **INCIBE - Spanish National Cybersecurity Institute**

- **MCCD- Joint Cyber Command**

- **SES - Secretariat of State for Security**

- **SESIAD- Secretariat of State for the Information Society and the Digital Agenda**

Sweden

Sweden's Cybersecurity Strategy is available at its Ministry of Justice.

Switzerland

Switzerland's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **CISA - Civilian Intelligence Service**

- **CSO - Armed Forces Command Support Organisation**

- **CYCO - Cybercrime Coordination Unit Switzerland**

- **DDPS - Federal Department of Defence, Civil Protection and Sport**

- **DETEC - Federal Department of Environment, Transport, Energy and Communications**

- **DSG - Federal Act on Data Protection**

- **EOC - Electronic Operations Centre**

- **FCP - Federal Criminal Police**

- **FDEA - Federal Department of Economic Affairs**

- **FDF - Federal Department of Finance**

- **FDJP - Federal Department of Justice and Police**

- **FDPIC - Federal Data Protection and Information Commissioner**

- **fedpol - Federal Office of Police**

- **FIS - Federal Intelligence Service**

- **FITO - Federal IT Ordinance**

- **FITSU - Federal IT Steering Unit**

- **FOCA - Federal Office of Civil Aviation**

- **FOCP - Federal Office for Civil Protection**

- **FOITT - Federal Office of Information Technology, Systems and Telecommunication**

- **FONES - Federal Office for National Economic Supply**

- **GovCERT - Government Computer Emergency Response Team**

- **ISA - Federal Act on Measures to Safeguard Internal Security**

- **ISA - Intelligence Service Act**

- **MELANI - Melde- und Analysestelle Informationssicherung (Reporting and Analysis Centre for Information Assurance)**

- **milCERT - Military Computer Emergency Response Team**

- **MIS - Military Intelligence Service**

- **NEOC - National Emergency Operations Centre**

- **OAG - Office of the Attorney General**

- **OFCOM - Federal Office of Communications**

- **OTS - Ordinance on Telecommunication Services**

- **PT - Police Tasks Act**

- **RGISSP - Research Group Information Society and Security Policy**

- **SFOE - Swiss Federal Office of Energy**

- **SONIA - Special Task Force on Information Assurance**

- **SPIK - Swiss Police IT Congress**

- **SPTA - Surveillance of Postal and Telecommunications Traffic Act**

- **VDSG - Ordinance to the Federal Act on Data Protection**

Tanzania

Tanzania's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Trinidad & Tobago

Trinidad & Tobago's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **TT CSIRT - Trinidad and Tobago CSIRT**

- **TTCSA - Trinidad and Tobago Cyber Security Agency**

Turkey

Turkey's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **SOME - Siber Olaylara Mildahale Ekipleri (Cyber Incident Response Team)**

- **USOM - Ulusal Siber Olaylara Mildahale Merkezi (National Center for Cyber Incident Response)**

Uganda

Uganda's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

Ukraine

Ukraine's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

United Arab Emirates

UAE's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.

United Kingdom

United Kingdom's Cybersecurity Strategy and additional material that treat the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

- **BSI - British Standards Institution**. BSI is the UK's National Standards Organization and represents UK interests in CEN, CENELEC, ISO, IEC as well as writing national standards.one of UK's principal standards development bodies - representing it especially in ISO/IEC. http://www.bsigroup.com/.

- **CGSD - Cyber and Government Security Directorate**. CGSD supports Cabinet Office ministers in determining priorities in relation to securing cyberspace; coordinates the National Cyber Security Programme (NCSP) and is responsible for Personal, Physical and Information Security Policy across government and internationally. The CGSD works with other lead government departments and agencies. https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance.

- **CPNI - Centre for the Protection of National Infrastructure**. CPNI protects UK national security by providing protective security advice. Its advice covers physical security, personnel security and cyber security/information assurance. http://www.cpni.gov.uk/.

- **DCMS - Department for Digital, Culture, Media and Sports**. DCMS leads UK government policy on digital issues for industry and society. This includes cyber security issues and digital/ICT technical standards. https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport/about and https://www.gov.uk/government/policies/cyber-security.

- **GCHQ - Government Communications HeadQuarters**. GCHQ is the hundred years old intelligence and security organization responsible for providing signals intelligence and information assurance in the United Kingdom. The UK's cyber security mission is led by the National Cyber Security Centre (NCSC), which is a part of GCHQ. https://www.gchq.gov.uk/.

- **GSS - Government Security Secretariat**. The GSS provides coordination on security and intelligence issues of strategic importance across government. https://www.gov.uk/government/organisations/national-security.

- **Home Office**. The Home Office leads works to ensure visible, responsive and accountable policing in the UK. It a ministerial department, supported by 25 agencies and public bodies. https://www.gov.uk/government/organisations/home-office.

- **MI5 Security Service**. MI5, together with the other UK's intelligence agencies, works to tackle the cyber threat along with other Government Departments and industry. https://www.mi5.gov.uk/cyber.

- **MOD - Ministry of Defence**. The MOD protects the security, independence and interests of the UK at home and abroad. Its aim is to ensure that the armed forces have the training, equipment and support necessary for their work. MOD is a ministerial department, supported by 29 agencies and public bodies. https://www.gov.uk/government/organisations/ministry-of-defence.

- **Ofcom**. Ofcom is the communications regulator in the UK. It regulates the TV, radio and video-on-demand sectors, fixed-line telecoms, mobiles and postal services, plus the airwaves over which wireless devices operate. https://www.ofcom.org.uk/.

- **NCSC - National Cyber Security Centre**. NCSC provides advice and guidance to the UK government on the security of communications and electronic data, in partnership with industry and academia, including the Centers of Academic Excellence (CAE) programme. It also hosts the UK National Computer Emergency Response Team, CERT-UK. http://www.ncsc.gov.uk.

- **NICC® - UK Interoperability Standards**. NICC is a technical forum for the UK communications sector that develops interoperability standards for public communications networks and services in the UK. http://www.niccstandards.org.uk/publications/.

United States

United States Cybersecurity Strategy and additional material that treat in part the bodies listed below are available through the NATO Cooperative Cyber Defence Center of Excellence.

DHS - Department of Homeland Security. DHS has multiple largely domestic security missions and works with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems. It plays a significant role within Analyses and reduces threats and distributes warnings. http://www.dhs.gov/.

- **CISA - Cybersecurity and Infrastructure Security Agency**. CISA is responsible for enhancing the security, resilience, and reliability of the US cyber and communications infrastructure. https://www.dhs.gov/cisa/cybersecurity-division.

  - **NCC - National Coordinating Center for Communications**. NCC continuously monitors national and international incidents and events that may impact emergency communications . NCC is the US Information Sharing and Analysis Center (ISAC) for Telecommunications. http://www.dhs.gov/national-coordinating-center-communications.

  - **NCCIC - National Cybersecurity and Communications Integration Center**. Within CISA, the NCCIC is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. It issues Joint Indicator Bulletins (JIBs) to more than 130 countries. https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center.

  - **ICS-CERT - Industrial Control Systems Cyber Emergency Response Team**. ICS-CERT helps reduce risks in all critical infrastructure sectors by partnering with law enforcement and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, it collaborates with international and private sector CERTs to share control systems-related security incidents and mitigation measures. https://ics-cert.us-cert.gov/.

  - **IP - Office of Infrastructure Protection**. IP leads and coordinates national programs and policies on critical infrastructure security and resilience, including the implementation of its Strategic Plan that includes multiple activities for information collection, compliance, coordination, protective security, and outreach. http://www.dhs.gov/office-infrastructure-protection.

  - **US-CERT - US Community Emergency Response Team**. US-CERT responds to major incidents, analysing threats, and exchanging critical cybersecurity information with trusted partners around the world, and facilitates the development of new information sharing capabilities. https://www.us-cert.gov/. It hosts the Software Assurance (SwA) Communities program. https://www.sei.cmu.edu/about/divisions/cert/index.cfm.

- S&T - Science and Technology Directorate

  - **CSD - Cyber Security Division**. CSD enhances the security and resilience of critical information infrastructure and the Internet by:

    1) developing and delivering new technologies, tools and techniques to defend, mitigate and secure current and future systems, networks and infrastructure against cyber attacks;

    2) conduct and support technology transition; and

    3) lead and coordinate research and development community. http://www.dhs.gov/science-and-technology/cyber-security-division.

DOD - Department of Defense. http://www.defense.gov/.

- **DISA - Defense Information Systems Agency**. DISA provides, operates, and assures command and control and information-sharing capabilities and a globally accessible enterprise information infrastructure. It supports cyberspace operations, serving as the experts in the DoD Strategy for Operating in Cyberspace (DSOC), the DoD Strategy for Defending Networks, Systems, and Data (DDNSD), and exploiting the DoD Cyberspace Workforce Strategy. http://www.disa.mil/Services/Cybersecurity.

- **CSIAC - Cyber Security and Information Systems Information Analysis Center**. CSIAC is a Department of Defense (DoD) Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC). The CSIAC is a consolidation of three predecessor IACs: the Data and Analysis Center for Software (DACS), the Information Assurance Technology IAC (IATAC) and the Modelling & Simulation IAC (MSIAC), with the addition of the Knowledge Management and Information Sharing technical area. https://www.csiac.org/groups/cybersecurity/.

DOS - Department of State. http://www.state.gov/.

- **CIP - International Communications and Information Policy**. The division works with other government agencies, foreign governments, U.S. businesses, and civil society to promote competitive and secure networks and lead U.S. delegations to international meetings. It consists of three offices - Bilateral and Regional Affairs, Multilateral Affairs, and Technology and Security Policy.

DOJ - Department of Justice. http://www.justice.gov/.

- **CCIPS - Computer Crime and Intellectual Property Section**. CCIPS is responsible for providing the legal support for combating computer and intellectual property crimes worldwide. http://www.justice.gov/criminal/cybercrime/.

- **FBI - Federal Bureau of Investigation**. The FBI has broad domestic investigative roles within the DOJ. Its Cyber Division is a focal point for cyber related matters. The Internet Crime Complaint Center (IC3) collects reports from private industry and citizens about online fraud schemes, identifies emerging trends, and produces reports. The Cyber Initiative and Resource Fusion Unit (CIRFU) maximizes and develops intelligence and analytical resources received from law enforcement, academia, international, and critical corporate private sector subject matter experts to identify and combat significant actors involved in current and emerging cyber-related criminal and national security threats. Similarly, its InfraGard program maintains partnerships and working relationships with private sector, academic, and other public-private entity subject matter experts for the protection of critical national infrastructure. http://www.fbi.gov/about-us.

- **NCIJTF - National Cyber Investigative Joint Task Force**. Supported by the FBI, the NCIJTF serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations. https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

FCC - Federal Communications Commission. The FCC assists in:

1) identifying and prioritizing communications infrastructure;

2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and

3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends. www.fcc.gov.

- **CISRIC - Communications Security, Reliability and Interoperability Council**. CISRIC provides recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety. http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council.

GSA - Government Services Administration. The General Services Administration, in consultation with DOD, DHS, and other departments and agencies as appropriate, provides and supports government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure. http://www.gsa.gov/.

NIST - National Institute of Standards and Technology. NIST is responsible for cybersecurity research and the development of standards for use by the Federal government, and which may also be useful for broader public sector use such as the National Vulnerability Database. http://www.nist.gov.

- **FIPS Federal Information Processing Standards**. Includes Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE).

- **FISMA - Federal Information Security Management Act**. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. NIST plays an important implementation role in developing the required standards, while the GSA facilitates their implementation.

- **Cybersecurity Framework Information Reference Catalog**. https://csrc.nist.gov/Projects/Cybersecurity-Framework/Informative-Reference-Catalog.

NSA - National Security Agency. The NSA which also consists of the Central Security Service (CSS) maintains both signals intelligence and cybersecurity missions. https://www.nsa.gov/what-we-do/cybersecurity/.

- **CNSS - Committee on National Security Systems**. CNSS sets national-level Information Assurance policies, directives, instructions, operational procedures, guidance and advisories for United States Government (USG) departments and agencies. https://www.cnss.gov/cnss/.

Zimbabwe

Zimbabwe's Cybersecurity Strategy and additional material are available through the NATO Cooperative Cyber Defence Center of Excellence.
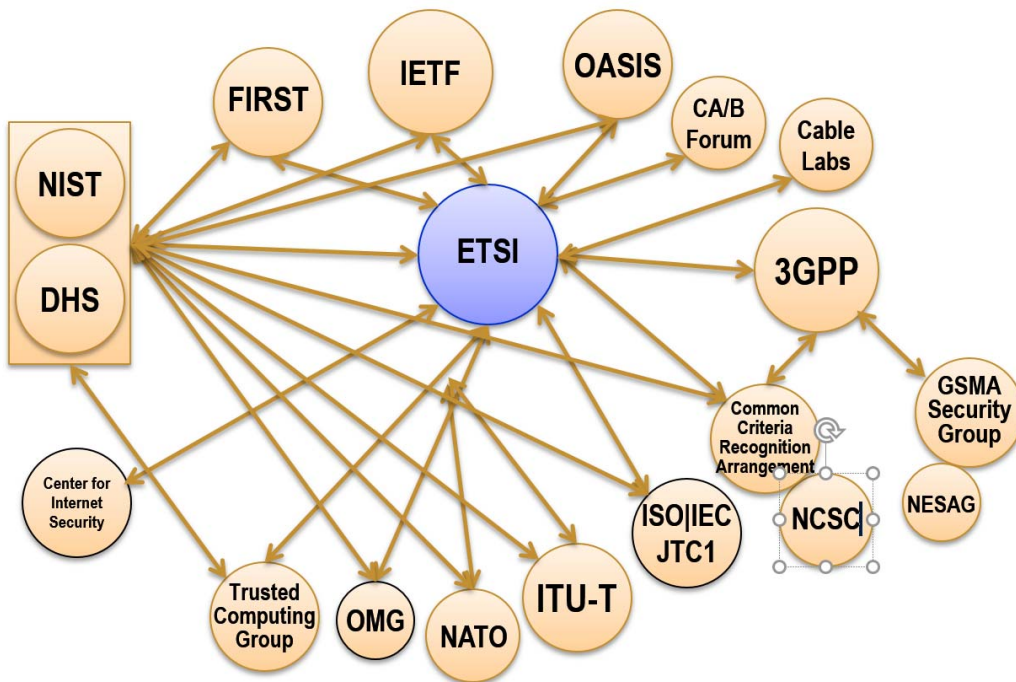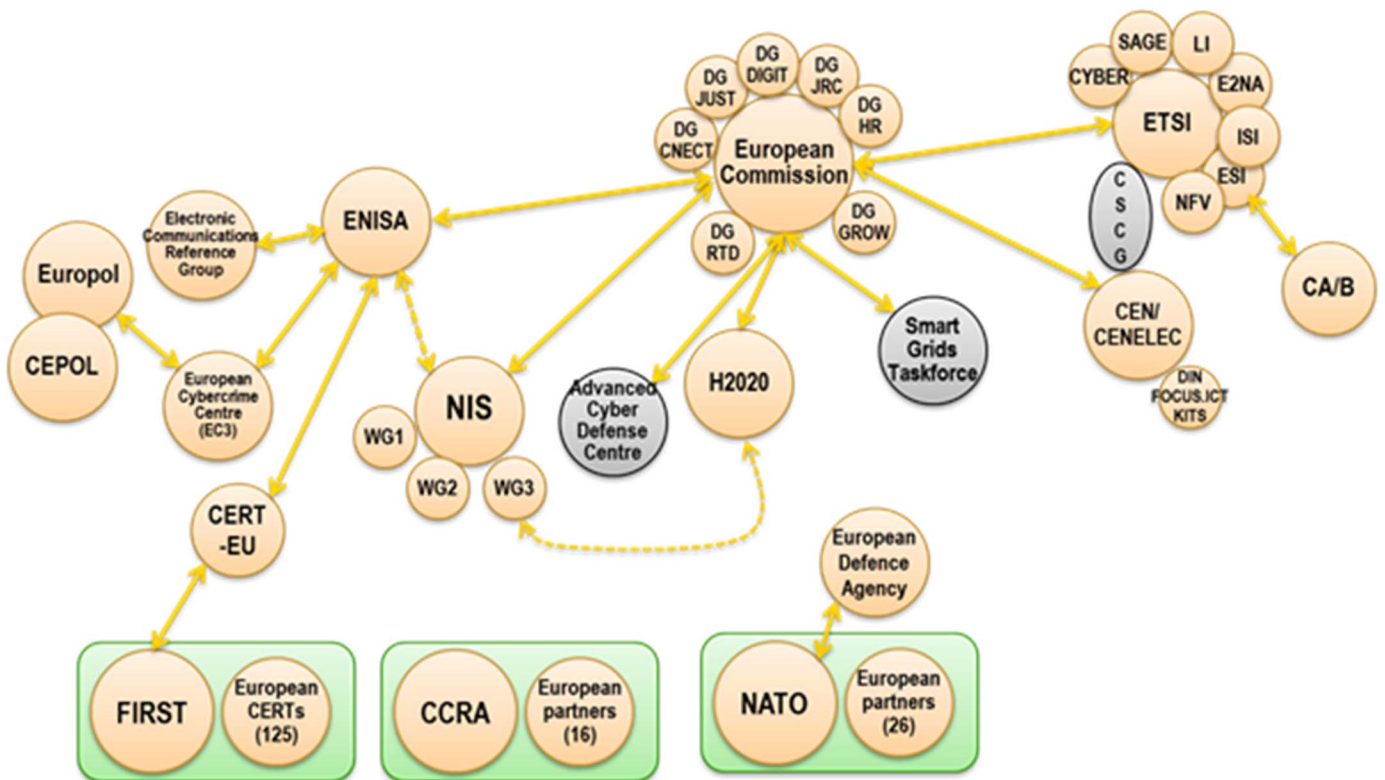
Annex B:
Relationship diagrams

Figure B.1

Figure B.2

Annex C:
Bibliography

ENISA: "National Cyber Security Strategies in the World", 2 February 2013.

> NOTE: Available at https://www.enisa.europa.eu/publications/cyber-security-strategies-paper/at_download/fullReport.

ETH Zurich: "International CIIP Handbook 2008/2009".

> NOTE: Available at http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf.

NATO CCDOE: "National Cyber Security Strategies".

> NOTE: Available at https://ccdcoe.org/library/strategy-and-governance/?category=cyber-security-strategies.

Software Engineering Institute, Technical Note: "Generalized Criteria and Evaluation Method for Center of Excellence: A Preliminary Report", December 2009.

> NOTE: Available at http://resources.sei.cmu.edu/asset_files/TechnicalNote/2009_004_001_15053.pdf.

History

Document history		
V1.1.1	November 2015	Publication
V1.2.1	March 2017	Publication
V1.3.1	August 2018	Publication
V1.4.1	March 2020	Publication