International Telecommunication Union

ITU-T X.1500.1

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Overview of cybersecurity

Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange

Recommendation ITU-T X.1500.1

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	**X.1500–X.1519**
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1500.1

Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange

Summary

Recommendation ITU-T X.1500.1 provides for the registration of OID arcs which enable coherent, unique and global identification of cybersecurity information as well as for organizations exchanging that information and associated policies. This Recommendation specifies the information and justification to be provided when requesting an OID for cybersecurity information exchange purposes, and the procedures for the operation of the Registration Authority.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1500.1	2012-03-02	17

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1500.1

Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange

1 Scope

This Recommendation specifies the procedures for operating the registration of OID arcs to identify cybersecurity information, organizations exchanging that information, and associated policies under the Cybersecurity Information Exchange object identifier arc `{joint-iso-itu-t(2) cybersecurity(48)}`.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.660] Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2011, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree.*

[ITU-T X.680] Recommendation ITU-T X.680 (2008) | ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.

[ISO 3166-1] ISO 3166-1:2006, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*.

[ISO/IEC 10646] ISO/IEC 10646:2003, *Information technology – Universal Multiple-Octet Coded Character Set (UCS).*

NOTE – Recommendation ITU-T T.55 recommends the use of [ISO/IEC 10646] for the representation of the languages of the world.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 object identifier [ITU-T X.660]: An ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node.

3.1.2 OID internationalized resource identifier [ITU-T X.660]: An ordered list of Unicode labels from the root of the international object identifier tree that unambiguously identifies the node in that tree.

3.1.3 primary integer value [ITU-T X.660]: A primary value of type integer used to unambiguously identify an arc of the international object identifier tree.

3.1.4 primary value [ITU-T X.660]: A value of a specified type assigned to an arc of the OID tree that can provide an unambiguous identification of that arc within the set of arcs from its superior node.

3.1.5 registration [ITU-T X.660]: The assignment of an unambiguous name to an object in a way which makes the assignment available to interested parties.

3.1.6 registration authority [ITU-T X.660]: An entity such as an organization, a standard or an automated facility that performs registration of one or more types of objects.

3.1.7 registration procedures [ITU-T X.660]: The specified procedures for performing registration and amending (or deleting) existing registrations.

3.1.8 secondary identifier [ITU-T X.660]: A secondary value restricted to the characters forming an (ASN.1) identifier (see [ITU-T X.680]), assigned either in an ITU-T Recommendation, an International Standard or by some other Registration Authority to an arc of the OID tree.

NOTE – An arc of the international object identifier tree can have zero or more secondary identifiers.

3.1.9 secondary value [ITU-T X.660]: A value of some type associated with an arc that provides additional identification useful for human readers, but that does not in general unambiguously identify that arc, and is not normally included in computer communications.

3.1.10 Unicode character [ITU-T X.660]: A character from the Unicode character set.

3.1.11 Unicode character set [ITU-T X.660]: The set of coded characters specified in [ISO/IEC 10646].

NOTE – This is the same character set as that specified in the Unicode Standard.

3.1.12 Unicode label [ITU-T X.660]: A primary value that consists of an unbounded sequence of Unicode characters that does not contain the SPACE character (see [ITU-T X.660], clause 7.5 for other restrictions) used to unambiguously identify an arc of the OID tree.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 administrative role (of a Registration Authority): Assigning and making available unambiguous names according to this Recommendation.

NOTE – This definition is consistent with [ITU-T X.660].

3.2.2 cybersecurity information: Any of the categories of information identified in [ITU-T X.1500].

3.2.3 cybersecurity organization: Any organizational entity using the model for information exchange specified in [ITU-T X.1500].

3.2.4 relevant Question(s): The ITU-T Question(s) responsible for the maintenance of this Recommendation.

NOTE – At the time of approval of this Recommendation, the relevant Question is ITU-T Q.4/17.

3.2.5 technical role (of a Registration Authority):Verifying that an application for registration of an OID arc is in accordance with this Recommendation.

NOTE – This definition is consistent with [ITU-T X.660].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CYBEX Cybersecurity Information Exchange

OID Object Identifier

OID-IRI OID Internationalized Resource Identifier

RA Registration Authority

5 Conventions

None.

6 General

6.1 This Recommendation defines procedures for the registration of arcs under the Cybersecurity Information Exchange OID arc `{joint-iso-itu-t(2) cybersecurity(48)}`.

6.2 According to the requirements and rules of [ITU-T X.660], this Recommendation is the RA for allocation of arcs under the Cybersecurity Information Exchange OID arc (by the progression of amendments to this Recommendation). The RA is operated by the relevant Question(s).

6.3 As the RA for the Cybersecurity Information Exchange OID arc, this Recommendation records the primary integer value, secondary identifiers and Unicode labels assigned to each subsequent arc identifying cybersecurity information (see Annex A).

6.4 Each RA being assigned a subsequent arc by this Recommendation is then responsible for the allocation of further subsequent arcs in accordance with [ITU-T X.660].

7 Responsibilities of the Registration Authority (RA)

7.1 The relevant Question(s) play both the technical role and the administrative role of the RA in accordance with the provisions of this Recommendation.

7.2 With regards to the assignment of arcs, the responsibilities of the relevant Question(s) shall be as follows:

a) to receive applications for the allocation of an arc (the required content of the application is specified in clause 9.1);

b) for each assigned arc, to produce an amendment to (or a new edition of) this Recommendation (see clause 9.3.1), in order to add to Annex A, a record of the assigned primary value, any secondary values and the specification of the category of cybersecurity information that is being registered.

NOTE – In the case of the national RAs mentioned in Annex B and of the RA mentioned in Annex C, this Recommendation is not updated but the assigned arc is added to a web-based registry (see clauses B.4 and C.3).

7.3 If the application is accepted according to the criteria of clause 8, the arc shall be allocated and a registration announcement shall be sent to the applicant as specified in clauses 9.2 and 9.3.2.

7.4 If the application is not accepted, the application shall be rejected by sending a notice of rejection as specified in clauses 9.4 and 9.3.2. The appeals process is specified in clause 10.

8 Criteria for acceptance

8.1 An application is accepted if, in the technical judgment of the relevant Question(s), the requested OID will identify cybersecurity information as described in [ITU-T X.1500] and be used on a worldwide basis.

8.2 The application shall identify the time-scale within which the relevant cybersecurity information is to be used within applications or services. The application shall be rejected if the time-scale exceeds 12 months, and can be voided if it is not in use within that time-scale.

NOTE – The primary integer value of a voided application shall not be reused within the next five years.

9 Detailed procedures for the operation of the RA

9.1 Registration application

The application shall include at least the following information:

a) name of any legally constituted and verifiable organization involved in the exchange of cybersecurity information, and submitting the application;

b) name, postal mail address, e-mail address, and optionally telephone and facsimile numbers for the contact point within the requesting organization;

c) full identification of the person submitting the application (including their role in the organization);

d) a specification (or a reference to it) of the cybersecurity information for which an arc is being requested;

e) (optionally) any desired secondary identifier(s); and

f) (optionally) any desired Unicode label(s).

9.2 Registration announcement

The relevant Question(s) shall send a registration announcement to an applicant when the amendment adding the new arc to this Recommendation (see clause 7.2 b) has been approved. The registration announcement shall include at least the following information:

a) the name of the organization submitting the application and the reference number of the application;

b) the name, postal/electronic mail address and telephone/facsimile number for the contact point within the requesting organization;

c) full identification of the person submitting the application (including their role in the organization);

d) a specification (or a reference to it) of the cybersecurity information for which an arc was requested;

e) the primary value assigned;

f) any confirmed secondary identifier(s); and

g) any confirmed Unicode label(s).

9.3 Time-scale for processing applications and publication

9.3.1 The technical evaluation by the relevant Question(s) is expected to be completed within eight weeks of receipt of the application by the RA. If the application is acceptable, the relevant Question(s) produce a draft amendment to (or a new edition of) this Recommendation (see clause 7.2 b) and publish it as a temporary document (TD) for consideration at the next plenary meeting of the ITU-T study group responsible for the maintenance of this Recommendation.

NOTE – In the case of the national RAs mentioned in Annex B and the RA mentioned in Annex C, this Recommendation is not updated but the assigned arc is added to a web-based registry (see clauses B.4 and C.3).

9.3.2 When the amendment to (or the new edition of) this Recommendation is approved, the allocation and the results of the application are sent to the applicant (see clause 9.2) and will be part of the amended Annex A. The applicant is also informed if the amendment (or the new edition) does not pass the approval process (see clause 9.4).

9.4 Notice of rejection

The relevant Question(s) shall send a notice of rejection to an applicant when the assignment of a new arc has been rejected. The notice of rejection shall include at least the following information:

a) the name of the organization submitting the application and the reference number of the application;

b) the name, postal/electronic mail address and telephone/facsimile number for the contact point within the requesting organization;

c) full identification of the person submitting the application (including their role in the organization);

d) a specification (or a reference to it) of the cybersecurity information for which an arc was requested;

e) the desired secondary identifier(s);

f) the desired Unicode label(s); and

g) the reason for rejection.

9.5 Change of registration information

The cybersecurity information identified by an allocated OID shall not change significantly from the cybersecurity information identified in the original application, but supporting information, such as the information provided in clause 9.1 b, may change from time to time. The relevant Question(s) shall be notified of all such changes, and shall update Annex A, maintaining an audit trail of earlier information.

10 Appeals process

10.1 In response to a notice of rejection, the applicant can submit to the relevant Question(s) a supplement to its original application that responds to the reason(s) for rejection.

10.2 Any subsequent appeal shall be resolved by the ITU-T study group responsible for the maintenance of this Recommendation.

NOTE – At the time of approval of this Recommendation, the study group responsible for the maintenance of this Recommendation is ITU-T SG 17.

Annex A

Register of arcs allocated under the Cybersecurity OID arc

(This annex forms an integral part of this Recommendation.)

Allocation of arcs for other cybersecurity information will be done by the addition of further tables in this register by way of publishing an amendment to (or a new edition of) this Recommendation (see clause 7.2).

NOTE – It is recommended to also update the OID repository at http://www.oid-info.com/get/2.48.

Cybersecurity information to which the OID arc is assigned	ITU Member States
Contact information for the RA of this OID arc	The relevant Question(s) (see clause 3.2.4)
Reference to where the cybersecurity information is specified	Annex B to this Recommendation
Assigned primary integer value	1
Confirmed secondary identifier(s)	country
Confirmed Unicode label	Country
Date of allocation	2012-03-02
Resulting OID	{joint-iso-itu-t(2) cybersecurity(48) country(1)}
Resulting ASN.1 OID-IRI	/Cybersecurity/Country

Cybersecurity information to which the OID arc is assigned	Cybersecurity international organizations
Contact information for the RA of this OID arc	The relevant Question(s) (see clause 3.2.4)
Reference to where the cybersecurity information is specified	Annex C to this Recommendation
Assigned primary integer value	2
Confirmed secondary identifier(s)	international-org
Confirmed Unicode label	International-Org
Date of allocation	2012-03-02
Resulting OID	{joint-iso-itu-t(2) cybersecurity(48) international-org(2)}
Resulting ASN.1 OID-IRI	/Cybersecurity/International-Org

Annex B

Rules for allocation of arcs under the country arc

(This annex forms an integral part of this Recommendation.)

B.1 The primary integer values (and hence the integer-valued Unicode labels) assigned to arcs under the `country` arc are the values of the numeric-3 codes of [ISO 3166-1] (without leading zeros). Secondary identifiers and non-integer Unicode labels are assigned that are the (two-letter) alpha-2 code elements of [ISO 3166-1] (in capitals for the Unicode labels).

NOTE – The existence of a country code in [ISO 3166-1] does not necessarily imply that there is an agency in that country which can allocate subsequent OIDs for the identification of national cybersecurity information. [ISO 3166-1] also assigns codes to regions or areas, but for the purpose of this Recommendation, an arc shall only be assigned to an ITU Member State.

B.2 Each ITU Member State has an arc automatically allocated under the `country` arc. However, to be able to use it, the ITU Member State shall nominate a national RA for that arc and inform the relevant Question(s) by sending a letter based on the following template:

> The signatory below, representing [*give the name of the administration representing the ITU Member State*[1]] for the country [*give the name of your country*] has agreed that [*give the name and postal address of the organization that will be the national RA as well as the name, email address and phone number of a contact person*] will operate the Registration Authority for object identifiers (OIDs) under the country arc
>
> {`joint-iso-itu-t(2) cybersecurity(48) country(1)` *xx*(*nn*)}
>
> [*complete the lowercase 2-letter code* *xx*[2] *and the numeric code* *nn*[3] *in accordance with ISO 3166-1*]
>
> in accordance with the provisions of Recommendation ITU-T X.1500.1.
>
> It is agreed that this information will be recorded by ITU-T, and can be made publicly available in the OID repository at http://www.oid-info.com/get/2.48.1.
>
> It is further agreed that if this information is changed, the relevant Question(s) (currently ITU-T Q.4/17) will be informed.
>
> Signed: *<add signature and official stamp as necessary>*

B.3 Each national RA shall assign an arc to a national organization which requests one. The national RA shall follow a process similar to what is described in clauses 7 to 10 (in particular, it plays both the technical role and the administrative role).

B.4 Each national RA shall make its best effort to provide a publicly available webpage detailing entries in the register, with email addresses protected against robot harvesting.

B.5 It is recommended that each national organization assigns subsequent arcs (of its arc) as depicted in Figure B.1.

---

1 See http://www.itu.int/GlobalDirectory/search.html.

2 See http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm.

3 See http://unstats.un.org/unsd/methods/m49/m49alpha.htm.

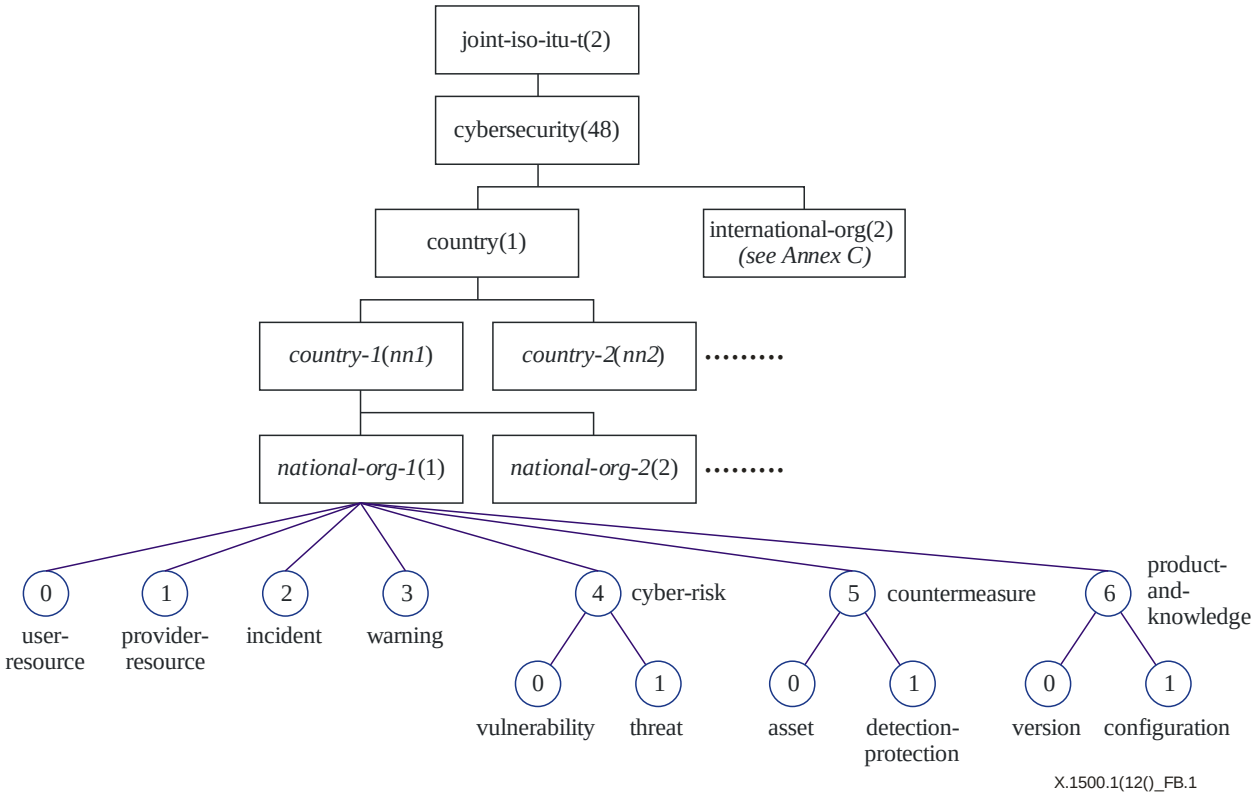

Figure B.1 – Subsequent arcs under the arc allocated to a country

Annex C

Rules for allocation of arcs under the international-org arc

(This annex forms an integral part of this Recommendation.)

C.1 The RA for this arc is the relevant Question(s) (see clause 3.2.4).

C.2 The RA for this arc shall assign an arc to any cybersecurity international organization which requests one. The RA shall follow a process similar to what is described in clauses 7 to 10 (in particular, it plays both the technical role and the administrative role).

C.3 Each arc under the `international-org` arc has a primary integer value (and hence an integer-valued Unicode label) which is the next available number (beginning at 1). Secondary identifiers and non-integer Unicode labels can be assigned if requested by the applicant. It is recommended that secondary identifiers be different from any other secondary identifier used at the same level of the OID tree. It is mandatory that Unicode labels be different from any other Unicode label used at the same level of the OID tree.

C.4 The RA shall make its best effort to provide a publicly available webpage detailing entries in the register, with email addresses protected against robot harvesting.

C.5 It is recommended that each international organization assigns subsequent arcs (of its arc) as depicted in Figure C.1 (based on the types of information specified in [ITU-T X.1500]).

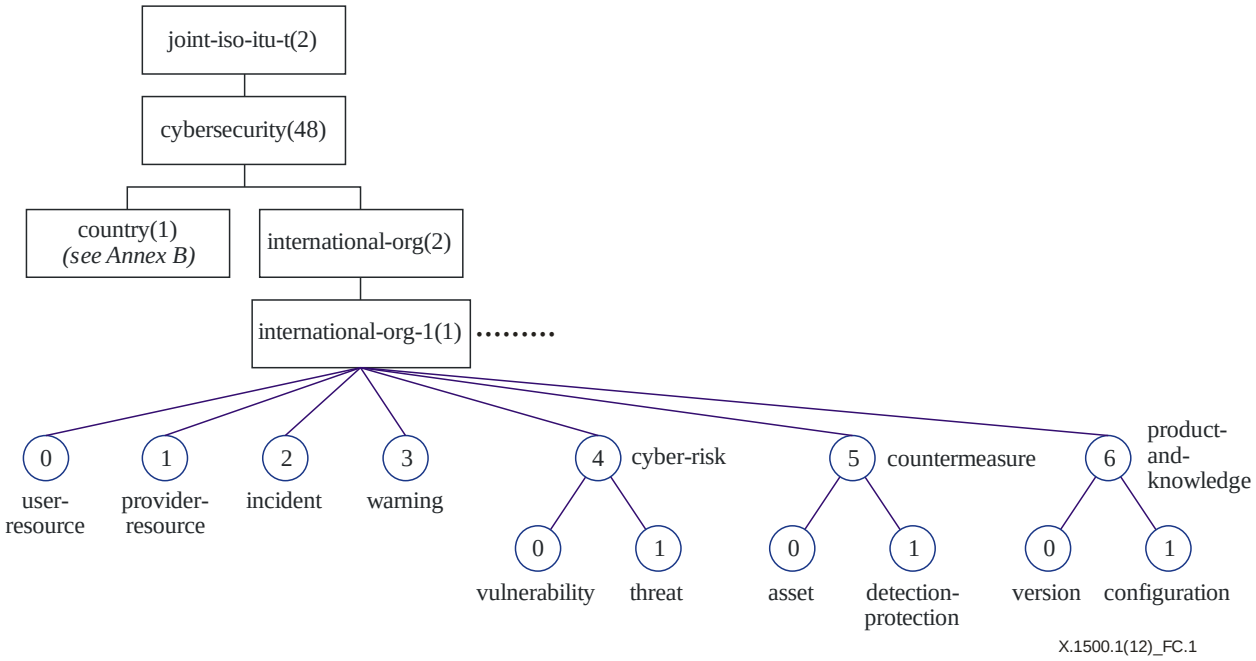

Figure C.1 – Subsequent arcs under the arc allocated to a cybersecurity international organization

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012