E/CN.16/2015/CRP.2
17 April 2015

Commission on Science and Technology for Development
Eighteenth session

Geneva, 4-8 May 2015

Mapping of international Internet public policy issues

Table of Contents

1. Introduction

This report presents the main findings of a review of international public policy issues pertaining to the Internet (referred to in this document as Internet policy issues). It was prepared by the secretariat of the Commission on Science and Technology for Development (CSTD) for the Inter-sessional Panel of the Commission, held in Geneva from 26-28 November 2014, in response to a recommendation of the United Nations Economic and Social Council.[1] The work was carried out in August–November 2014, and was supported by independent expert advice and comments from peer reviewers.[2]

The review of Internet policy issues builds on earlier work initiated by the CSTD Working Group on Enhanced Cooperation (WGEC). It continues that Group's work in developing a more comprehensive set of information on international public policy issues pertaining to the Internet, the mechanisms dealing with these issues, and potential gaps in those mechanisms. The information gathered has been included in a database created for this purpose. The report draws on the findings of the database and reviews the international public policy issues in the order in which they are presented in the database.

A provisional version of this report and the database were discussed at the Inter-sessional Panel of the Commission which was held in Geneva from 26-28 November 2014. Following this discussion, the secretariat initiated a period for comments on the document, lasting until 31 December 2014. During that period, written comments were received from the Governments of Brazil, Canada, India, Japan, the Russian Federation, Saudi Arabia, Switzerland and the United States of America as well as from the following organizations and individuals: the European Union, David Allen, the Association for Proper Internet Governance, the Bank for International Settlements, the Council of Europe, Stephen Farrell, ICANN, ICC Basis, INHOPE, the Internet Architecture Board, the Internet Rights and Principles Coalition, ISOC, IT for Change, the ITU, Seth Johnson, OECD, RIPE NCC, UNCITRAL, UNESCO and WTO.

The secretariat revised the report and added information to the database in light of the oral comments received during the Inter-sessional Panel meeting and the written comments submitted to it. The revised report, with the database as its addendum, is presented for the consideration by the Commission at its eighteenth session which will be held in Geneva from 4-8 May 2015. The Commission is invited to consider the document in the context of the ten-

[1] ECOSOC 2014, *Assessment of the progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society* (Resolution E/2014/27).

[2] The work was carried out in collaboration with Jovan Kurbalija. Substantive comments were made by Wolfgang Kleinwächter, Joy Liddicoat, Peter Major, Jimson Olufuye, Phil Rushton, Parminder Jeet Singh and David Souter.

year review of the progress made in the implementation of the outcomes of the World Summit on the Information Society (WSIS).

Background

The CSTD Working Group on Enhanced Cooperation (WGEC) was established by the Chair of the CSTD in 2013 in response to the request of the United Nations General Assembly in its resolution 67/195 of 21 December 2012. Its purpose was to examine the mandate of the World Summit on the Information Society (WSIS) regarding enhanced cooperation as contained in the *Tunis Agenda for the Information Society*, by seeking, compiling and reviewing inputs from all Member States and all other stakeholders, and making recommendations on how to fully implement this mandate. The group was composed of twenty-two Member States and twenty invitees from all other stakeholder communities, that is, from the private sector, civil society, the technical and academic communities, and intergovernmental and international organisations. It held four meetings from May 2013 to May 2014. In its second meeting, held in November 2013, the group agreed to initiate a mapping of international public policy issues pertaining to the Internet. It set up "a Correspondence Group" (CG) which was entrusted to:

> *(a) Review the identified international public policy issues pertaining to the Internet in the spreadsheet that …* [had] *… been developed in the second meeting of the WGEC. …*
>
> *(b) List where there are existing international mechanisms addressing the issues in the list*
>
> *(c) Identify the status of mechanisms, if any,* [and] *whether they are addressing the issues* [and]
>
> *(d) Attempt to identify the gaps in order to ascertain what type of recommendations may be required to be drafted by the WGEC.*[3]

The fourth meeting of the WGEC was held from 30 April-2 May 2014. In this meeting, the work of the CG was presented in a spreadsheet which identified twenty-four broad issue areas. The WGEC took note of the presentation of the CG's work and suggested that the spreadsheet should be considered as "a living document".[4]

---

[3] Chair's summary of the second meeting of the WGEC, available at http://unctad.org/meetings/en/SessionalDocuments/WGEC_2013_Chairmans_summary_en.pdf (accessed 9 April 2015).

[4] The work of the working group is documented at http://unctad.org/en/Pages/CSTD/WGEC.aspx (accessed 9 April 2015).

The Chair of WGEC gave an account of the work carried out by his group at the seventeenth session of the CSTD in May 2014. In his report, the Chair concluded that "the complexity and political sensitivity of the topic did not allow the group to finalize a set of recommendations on fully operationalizing enhanced cooperation."[5] The CSTD recommended to the United Nations Economic and Social Council (ECOSOC) that the work that had been initiated by the Working Group – the collection of relevant information, the review of international public policy issues, and the identification of gaps carried out in the CG – should be continued by the secretariat of the Commission.

Subsequently, in its resolution E/RES/2014/27 of 16 July 2014, the ECOSOC noted:

> […] *the work initiated by the Working Group* [on Enhanced Cooperation] *to review the identified international public policy issues pertaining to the Internet, list where there are existing international mechanisms addressing these issues, identify the status of mechanisms, if any, and whether they are addressing the issues and attempt to identify gaps in order to ascertain what type of recommendations may be required;*

and recommended that:

> *this work may be further continued by the secretariat of the Commission with a view to the submission of the findings to the Commission at its intersessional meeting for further discussion and their integration into the 10-year review of the progress made in the implementation of the outcomes of the World Summit, to be prepared for consideration by the Commission at its eighteenth session.*[6]

This report presents the work that was carried out to continue the work initiated in WGEC, in compliance with the above mentioned resolution.

Methodology

The mandate that was given by ECOSOC to the CSTD secretariat has been addressed through the following steps:

1. *Review the identified international public policy issues pertaining to the Internet.*

---

[5] See Chair's summary of the WGEC (E/CN.16/2014/CRP.3), available at http://unctad.org/meetings/en/SessionalDocuments/ecn162014crp3_en.pdf (accessed 13 April 2015).

[6] ECOSOC, 2014, *Assessment of the progress made in the implementation of and follow-up to the World Summit on the Information Society* (Resolution E/RES/2014/27).

The information that was initially gathered through the CG was reviewed and reorganised. Adjustments were made in the listing of issues to allow more detailed information to be included concerning relevant mechanisms.[7] The issues were then classified under the following seven broad clusters according to their main attributes:

- infrastructure and standardisation;
- security;
- human rights;
- legal;
- economic;
- development; and
- sociocultural issues.

It should be noted, however, that this classification into seven broad clusters is only indicative. Its purpose is to assist readers in their understanding of the complex field of Internet public policy. Many issues are intersectoral, cutting across the dividing lines between these clusters or incorporating elements of two or more of them. As a result, many issues could be classified in more than one cluster, depending on the context.

2. *List where there are international mechanisms addressing these issues, and identify the status of these mechanisms, if any.*

The spreadsheet that was prepared by the CG included many different types of mechanisms such as organisations, policy processes and instruments. Most of these mechanisms, which are marked as OLD in the database, were retained in the continuation of the work. NEW mechanisms were added, where appropriate. For example, some general mechanisms identified by WGEC (giving the name of the organisation) were supplemented by more specific mechanisms describing the activities of the organisations mentioned (such as consultation mechanisms, conventions and events). Some mechanisms identified by the CG were dropped because they were considered national rather than international. Regional mechanisms were retained and some new mechanisms at regional level have been added.

Altogether, the database includes over 680 mechanisms, classified into 41 issues, which are themselves classified into seven clusters. A number of mechanisms, such as the Internet Governance Forum (IGF), are listed in more than one issue category in the database.

As noted by several respondents commenting on the provisional documents, the database is not and does not attempt to deliver an exhaustive list of Internet governance mechanisms. This would not have been possible, given the breadth and constant evolution of the field of Internet public policy.

[7] Refer to the annex for a detailed comparison between the general description of the issues identified through the CG and the list of issues presented in the database.

The status of each mechanism is evaluated using the following criteria:

a) What is the TYPE of the specific Internet public policy mechanism? The following main types are identified:
   - Processes (events, negotiations, consultations, coordination, monitoring);
   - International agreements and other binding and non-binding instruments (conventions, standards, regulations, recommendations, court judgements, and other documents);[8]
   - Programmes (capacity development, training, research projects).

b) What is the FUNCTION of the specific Internet public policy mechanism? The following criteria are used:
   - To DISCUSS: includes non-decision-making mechanisms such as policy discussions, academic research, and coordination.
   - To DECIDE: includes all mechanisms that result in policy decisions, including legally binding mechanisms (e.g. conventions and treaties) and legally non-binding ones (e.g. resolutions, standards, guidelines).
   - To IMPLEMENT: includes all mechanisms that implement, enforce, or monitor adopted policy, including policy enforcement, monitoring, dispute resolution, and capacity development.

c) What is the level of PARTICIPATION in specific Internet public policy mechanisms? What opportunities exist for participation by concerned stakeholders? The analysis is conducted around the following indicators:
   - Participation only by members of the organisation;
   - Participation open to others as observers;
   - Open participation with limited intervention (submission of documentation, exceptional interventions);
   - Full participation (suggesting agenda items and tabling proposals, interventions, and deliberations).

d) Is an INTERSECTORAL approach used? Do the mechanisms used take into consideration the intersectoral nature of Internet public policy issues? For example, are online privacy and data protection issues addressed from all relevant perspectives including human rights, trade, standardisation and security? The following criteria are used:
   - Exclusive coverage in, or mandate for, one policy community (e.g. technical, legal, economic).

[8] These are referred to as "Instruments" in the database.

- Ad hoc coordination across policy sectors based on informal contacts in the preparation of events and implementing projects without any formal structure or requirement for intersectoral coordination).
- Structured coordination across policy sectors (e.g. coordination groups).
- Full intersectoral coverage of Internet governance issues.

3. *Attempt to identify gaps, if any, in order to ascertain what type of recommendations may be needed.*

Based on the criteria mentioned above, the review attempts to identify possible gaps in the governance of the international public policy issues pertaining to the Internet. References to the initial gaps identified by the CG are included in the database. Other possible gaps were identified while the work continued and are also presented in the database. This report gives a brief account of some of the possible gaps in each issue area. It also briefly describes some areas of ambiguity and some issues which have been debated at the international level but which remain unresolved.

Through a number of analytical iterations, the review identified four major groups of gaps, which can be summarised as:

- knowledge gaps (insufficient data or awareness of the impact of the Internet on public policy issues);
- policy gaps (lack of policy instruments such as norms and guidelines, and lack of mechanisms for identifying and adopting policy instruments);
- implementation gaps (lack of guidelines and other mechanisms for implementing existing policies and rules); and
- capacity gaps (lack of capacity of stakeholders and actors to actively participate in international Internet public policy mechanisms).

Structure of the report

The report is structured according to the classification of the issues in the seven broad clusters mentioned above. Chapters 2–8 therefore present the main findings of the review. Each chapter presents the analysis of issues included in the appropriate cluster, including a description of the issues, the status of mechanisms addressing these, and a description of areas of ambiguity, unresolved issues and possible gaps identified in those mechanisms. It should be remembered in reading these chapters that the clusters are indicative and that many issues are cross-cutting (see above). Chapter 9 sets out the main conclusions, describes the principal challenges encountered in the course of the work, and discusses potential areas for continuation.

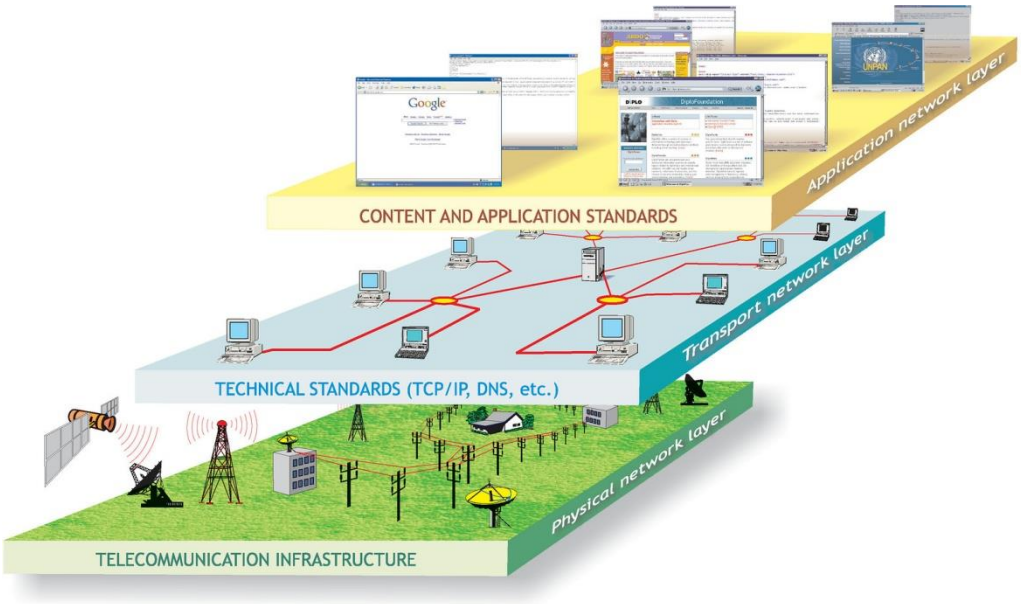
The annex provides a comparison of the issues that were identified by the Correspondence Group and the issues which are presented in the database. The addendum[9] presents the review of the public policy issues, the mechanisms which address them, the status of those mechanisms and possible gaps in Excel spreadsheet format.

2. Infrastructure and standardisation cluster

The cluster of issues concerned with infrastructure and standardisation, identified in the review, includes three issue areas that are concerned with the core functionality of the Internet. These are:

- the communications infrastructure that facilitates digital communication;
- technical issues related to standards and critical Internet resources (technical and web standards), Internet protocol (IP) numbers, the domain name system (DNS), and the root zone; and
- a group of content and application issues including net neutrality, cloud computing and the Internet of Things, that concern aspects of policy that may shape and determine future Internet developments.

Figure 1: Issue areas in the infrastructure and standardization cluster



Source: *DiploFoundation, graphic library.*

[9] Available only in electronic format at http://unctad.org/en/pages/MeetingDetails.aspx?meetingid=606.

2.1 Communications infrastructure

The communications infrastructure facilitates electronic communication, including Internet traffic as well as voice and other data traffic. This infrastructure includes wired (i.e. copper wires, fibre-optic cables, connection equipment, servers, user devices) and wireless space and terrestrial links (satellite radio communication systems, fixed and mobile radio communication systems, etc.). Fibre-optic cables, which carry 95 per cent of international Internet traffic, are among the most important elements within this infrastructure. Technological development and innovations are likely to introduce new infrastructure types, including drones and balloons. The governance of the communications infrastructure has an important impact on how the Internet is developed and used.

Status of mechanisms concerning communications infrastructure

The communications infrastructure is managed and overseen by a wide variety of public and private organizations. The principal international organization involved in the facilitation of telecommunications networks is the International Telecommunication Union (ITU), which provides a global framework for the coordination of national telecommunication systems. The ITU plays an important role in the allocation of radio spectrum, which is relevant to wireless communications, including wireless Internet. The World Trade Organization (WTO) has played an important part in the liberalisation of telecommunication markets worldwide. Prominent professional and technical organizations include the Institute of Electrical and Electronic Engineers (IEEE), which develops standards such as the WiFi standard (IEEE 802.11b), and the GSM Association (GSMA) which develops standards for mobile networks.

With growing demand to develop local content and keep Internet traffic closer to users (e.g. Internet Exchange Points), the question of global interconnection amongst a large number of networks with differing characteristics will be important for the future growth of the Internet. Reliable telecommunications networks, including fibre-optic cables and other types of infrastructure, also facilitate wider access to the Internet in developing countries.

How communications infrastructure is governed has implications for other Internet policy issues including technical standards, the Internet of Things, cyber security, data protection, jurisdiction, cloud computing, and intermediary liability. Governance of the communications infrastructure is related to net neutrality, in particular when it comes to the prioritization of Internet traffic.

Areas of ambiguity, unresolved issues and possible gaps in dealing with the communications infrastructure

The complexity of the Internet creates ambiguity in understanding of the interface between telecommunications policy and Internet public policy. This becomes particularly pronounced in cases which involve content issues. For example, when providers of telecommunications services manage traffic or try to detect spam and viruses, they could interfere with the content

on the Internet. Should such activities be considered as a telecommunications issue or an Internet public policy issue?

The mechanisms analysed indicate a gap concerning the implementation of existing policies and rules which reflects the ambiguity of the regulatory border zone between telecommunications and Internet public policy. This could be addressed through different measures such as regulation, guidelines, practices and capacity building.

2.2 Technical standards

The Internet's architecture is based on a set of technical standards. The IETF defines an Internet standard as "a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognisably useful in some or all parts of the Internet."[10] The most important technical standard is the Internet Protocol suite (TCP/IP - Transmission Control Protocol/Internet Protocol), which is fundamental to the routing and addressing of Internet traffic.

Status of mechanisms concerning technical standards

Many Internet technical standards are set by the Internet Engineering Task Force (IETF) in the form of Request for Comments (RFC). These are voluntary standards developed in working groups open to all interested parties. The IETF makes decisions through an open and consensus-based process which is often described as "rough consensus and running code." Standardization work is also undertaken in the Internet Research Task Force (IRTF), which is overseen by the Internet Architecture Board (IAB). In addition to this oversight, the IAB handles external liaison relationships for the IETF and IRTF, and has some oversight responsibilities for them. The IAB and the IETF have their institutional home within the Internet Society (ISOC).

Because they underpin the working of the Internet, Internet technical standards have an impact on other Internet public policy issues.[11]They may influence, for example, the way the Internet is used (access and interaction), how digital assets are safe-guarded (intellectual property rights and data protection), and how human rights are protected (freedom of expression and online privacy). For example, IETF standard RFC 6409 sets a standard

---

[10] Bradner, S., 1996, *The Internet Standards Process - Revision 3.* Request for Comments: 2026. IETF Network Working Group. Available at https://www.ietf.org/rfc/rfc2026.txt (accessed 4 April 2015).

[11] Policy decisions in the non-technical sphere can also have significant impacts on the technical operation of the Internet.

separating mail submission from message relay. This standard has direct relevance for all operators of e-mail systems, including intermediaries who have flexibility to set their own rules in handling the security of e-mail communication.

Internet technical standards concerned with e-mail authentication can influence the level of anonymity on the Internet with a direct impact on cyber security and cybercrime (anonymity increases the complexity of identifying perpetrators of cyber attacks), freedom of expression (in some cases anonymity can facilitate freedom of expression), and privacy protection.

Internet standards are also related to the following Internet public policy issues: net neutrality**,** encryption**,** e-commerce**,** access**,** the digital divide**,** content policy**,** and the Internet as a global public good.

Areas of ambiguity, unresolved issues and possible gaps in dealing with technical standards

Some submissions to the WGEC suggested the desirability of more involvement from the part of governments and/or non-technical entities, for instance, consumer representatives, in the development of technical standards. Even though participation is open to all stakeholders, the effect of this is constrained by factors such as lack of awareness, interest, or capacity. Lack of broad participation may lead to insufficient attention to non-technical implications, such as human rights, competition policy, and security, in the development of standards. The IETF has recognized this challenge and has taken steps to enhance participation of non-technical stakeholder representatives.

2.3 Web standards

The main web standard is HTML (HyperText Markup Language). It facilitates sharing of information, display of content, and web interaction. HTML has been regularly upgraded with new features, and the current version is HTML 5.0. While basic HTML only handled text and images, HTML 5.0 provides more features for managing databases and advanced display of video and animation. With the emergence of a wide variety of web applications, web standards ensure that Internet content can be accessed and properly viewed by the majority of Internet applications. Another important web standard is XML (Extended Markup Language), which provides flexibility in setting standards for Internet content.

Status of mechanisms for web standards

Web standards are set by the World Wide Web Consortium (W3C), whose membership is open to all types of organizations and individuals. The standards are developed through an elaborate consensus-based process, and published as W3C Recommendations.

W3C standards have high economic relevance, which has led to active participation by Internet industry and software developers in the development of the W3C standards. They

can have direct impact on many Internet policy issues, including multilingual content on the Internet, access for people with disabilities, and e-commerce.

Areas of ambiguity, unresolved issues and possible gaps in dealing with web standards

As in the case of Internet technical standards, possible gap in the development of web standards concerns the sufficiency of participation by governments and non-technical entities, and the extent to which non-technical aspects (e.g. human rights, competition policy, and security) are integrated in their development. Web standards have an even stronger impact on non-technical aspects than technical standards since, more so than technical standards, they shape the way the Internet is accessed and used.

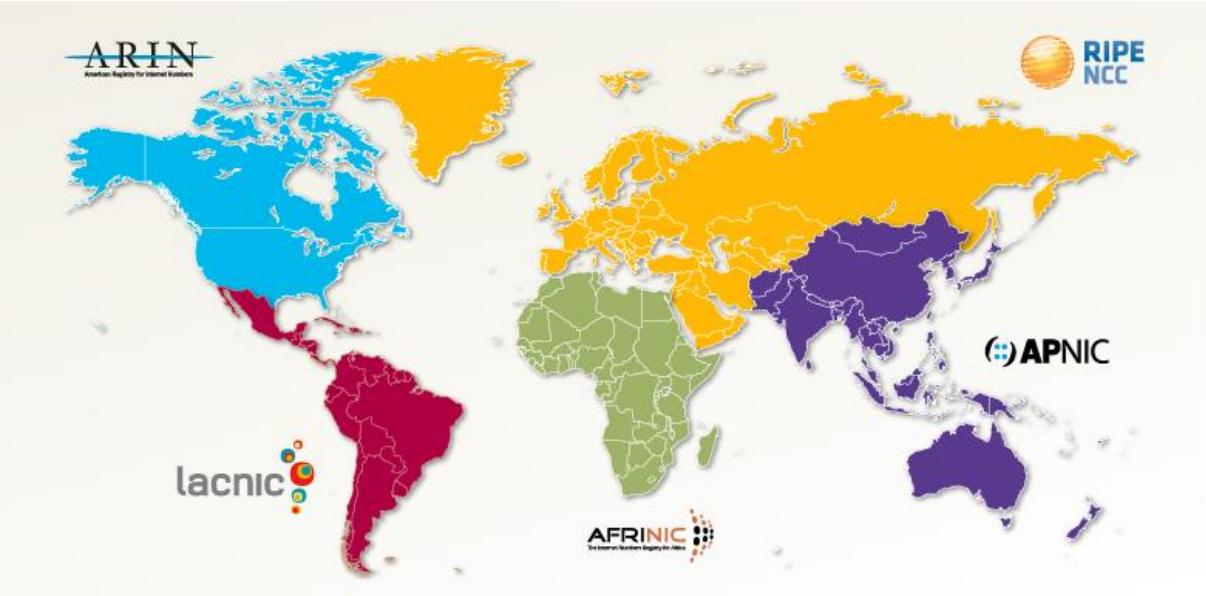
2.4 Internet protocol numbers

Internet protocol (IP) numbers are numeric addresses that are used to identify computers and other devices connected to the Internet. The fast growth of the number of Internet-enabled devices (including mobile phones, personal organisers, tablets and home appliances) has increased the level of demand for IP numbers and made them a potentially scarce resource. IP version 6 (IPv6) was introduced partly in order to overcome the limited pool of IP version 4 (IPv4) numbers. The transition to IPv6 has been progressing more slowly than many consider necessary to address the limitations of IPv4.

Status of mechanisms concerning Internet protocol numbers

The governance of IP numbers is coordinated by the Internet Assigned Numbers Authority (IANA) - a set of functions provided by the Internet Corporation for Assigned Names and Numbers (ICANN). IANA distributes blocks of IP numbers to the five Regional Internet Registries (RIRs). RIRs distribute IP numbers to local Internet registries (LIRs), which in turn distribute them to smaller Internet Service Providers (ISPs), companies, and individuals.

Figure 2: Geographic coverage of the five Regional Internet Registries



Source: *The Number Resource Organization (https://www.nro.net/about-the-nro)*

The Number Resource Organisation (NRO) coordinates the work of the five RIRs. The Address Supporting Organisation (ASO) reviews and develops recommendations on global IP address policy and advises the ICANN Board.

The governance of IP numbers is particularly relevant for the development of the Internet of Things (IoT), which will substantially increase the number of devices connected to the Internet, and, consequently, the demand for IP numbers.

Areas of ambiguity, unresolved issues and possible gaps in dealing with Internet protocol numbers

Various organisations are engaged in capacity building and development regarding the transition to IPv6. Despite ongoing efforts, there appears to be a knowledge gap related to awareness, data, and research on transition to IPv6.

Some submissions to the WGEC/CG also point to a possible policy gap in mechanisms for coordination and facilitation of the transition from IPv4 to IPv6. The adoption of IPv6 is considered critically important to ensure that the Internet continues to serve users and spur innovation. Governments, regional organisations and other institutions can play an important role in enhancing adoption of IPv6.

Another policy gap discussed in some submissions to WGEC/CG concerns the status of governments in the decision-making structure of ICANN. However, there is no consensus on this issue. While some submissions view the Governmental Advisory Committee (GAC) of

ICANN as providing insufficient role for governments (and point out that, formally speaking, their role is only advisory), others believe that, in practice, governments play an important role (and point out that there are formal procedures to address instances where the ICANN Board disagrees with GAC advice).

2.5 Domain name system

The domain name system (DNS) is often defined as the Internet "address book", which enables the mapping of host names to IP addresses. The DNS functions include mechanisms to take language-based Internet names and convert them to numeric IP addresses. Internet-connected devices use IP numbers to communicate with one another. DNS names are hierarchically organized using a series of labels separated by a stop (“.”). The top level in domain names consists of the “root”, and points to the relevant top-level domain (TLD), such as .com or .org. Each of these TLDs is (or is potentially) independently administered. Under each TLD are pointers to second-level domains (SLDs), again each potentially independently administered, while under each SLD there may pointers to third-level domains, and so on. At each level in the DNS hierarchy for a particular name, one or more potentially independently operated name servers will respond to queries about names, either providing information about the name, a referral to other name servers that might know about it, or an indication that the name does not exist. The DNS ensures that accurate information may be found about any address at any time, from anywhere and, with the deployment of security protocols known as DNS Security (DNSSEC), with confidence as to its veracity. The DNSSEC authenticates DNS response data.

The DNS includes two types of TLDs: generic (gTLD) and country code (ccTLD), with gTLDs being characterized as sponsored (sTLD) or unsponsored. Unsponsored gTLDs include domains that can be obtained by anyone (.com, .info, .net, and .org). Since 2014 many other gTLDs have been added such as .pub, .بازار (bazaar), .rentals, .ngo, and .游戏 (game). sTLDs are limited to a specific group. For example, the sTLD .aero is open for registration only for the air-transport industry. ccTLDs designate specific countries or territories (.uk, .cn, .in).

Status of mechanisms concerning domain name system

The organisation and management of DNS is based on Internet standards and recommendations (Requests for Comments adopted by the IETF). For country domains, the IETF refers to the ISO 3166 which is the International Standard for country codes and codes for their subdivisions. ICANN, through a number of stakeholder groups and constituencies, provides overall coordination of the DNS by establishing agreements and accrediting registries and registrars.12 For each gTLD there is one registry that maintains information

[12] Internet registry (IR) is an entity that assigns and manages Internet numbers assigned to IT systems, autonomous systems and/or organizations. Registrar is an entity, commercial or non-commercial, that manages

related to the second-level domains delegated within the TLD. For example, the .com gTLD is managed by Verisign, which maintains the file that includes pointers (referrals) to all names within the .com TLD. Final users purchase specific domain names (the part in front of the dot in each TLD) from registrars.

To date, ICANN has performed the so-called IANA[13] functions, on behalf of the United States government, through a contract with the United States Department of Commerce's National Telecommunications and Information Administration (NTIA). These functions include the coordination of the assignment of technical Internet protocol parameters; the administration of certain responsibilities associated with Internet DNS root zone management; the allocation of Internet numbering resources; and other services related to the management of the .arpa and .int top-level domains. The ICANN community also decides on the introduction of new gTLDs (such as .city, .wine, etc.). A process to transition the IANA contract was initiated by the NTIA on 14 March 2014, when it announced its intention to transition the contract to the global multi-stakeholder community.[14]

The policy development function for the DNS lies within the Country Code Names Supporting Organisation (CCNSO) for country code TLDs and the Generic Names Supporting Organization (GNSO) for gTLDs. The main dispute resolution mechanism for the names in contention in the DNS is the Uniform Domain-Name Dispute-Resolution Policy (UDRP).[15] In addition to the WIPO Arbitration and Mediation Center, there are four other regional UDRP service providers.

Areas of ambiguity, unresolved issues and possible gaps in dealing with the domain name system

The importance of policy concerning the DNS intensified with the introduction of the new gTLDs. For example, this aroused policy debate on the right to register names such as .amazon (which is both the name of a company (who owns a trademark) and a river system which is used as a term for countries in Amazon basin. Other debates have concerned generic names such as .book. It has also been noted that new domains such as .doctor or .lawyer could mislead Internet users should individuals who, for example, do not have appropriate medical and/or legal qualifications register under these domains.

---

the reservation of Internet domain names with the authorisation of and in accordance with the guidelines of the designated domain name registries.

[13] Internet Assigned Numbers Authority.

[14] NTIA's press release is available at http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions (accessed 9 April 2015).

[15] See Chapter 5.2.

Some submissions to the WGEC/CG have suggested that the most important policy gap in this issue area derives from the way in which the DNS has been coordinated through the IANA contract by ICANN. Following its announcement to transition the contract to the global multi-stakeholder community, the NTIA requested ICANN to convene a multi-stakeholder dialogue which could develop a proposal "to transition the current role played by NTIA in the coordination of the … DNS," including "the procedural role of administering changes to the authoritative root zone file," thereby potentially ending the oversight role exercised by the NTIA. Following a consultation process, ICANN has established a Consultation Group, representing its diverse stakeholder communities, to develop proposals concerning future management of the IANA function. The current IANA contract expires in September 2015.[16]

Another policy gap discussed in some submissions to WGEC/CG concerns the status of governments in the decision-making structure of ICANN. However, there is no consensus on this issue. While some submissions view the Governmental Advisory Committee (GAC) as providing insufficient role for governments (and point out that, formally speaking, their role is only advisory), others believe that, in practice, governments play an important role (and point out that there are formal procedures to address instances where the ICANN Board disagrees with GAC advice).

2.6 Root zone

The root zone is the top level of the hierarchically organised DNS (the so-called Internet address book). The root zone maintains a list of all top-level domains in use on the public Internet and is implemented through a set of root servers. There are thirteen root servers - ten located in the United States, and one each in Sweden, the Netherlands and Japan. The IP addresses of the thirteen root servers are built into the software that performs DNS look-ups of domain names. Hundreds of machines respond to DNS queries sent to the root server IP addresses through a technique known as "any cast". This technique ensures global accessibility of root zone data.

Status of mechanisms concerning root zone

Twelve independent organizations administer the root servers mentioned above, located in four countries.

Changes to the root zone are currently administered by ICANN through the IANA function pursuant to the contract administrated by NTIA. VeriSign performs the related root zone

[16] ICANN's website concerning the process to develop the proposal is available at https://www.icann.org/resources/pages/process-next-steps-2014-06-06-en (accessed 9 April 2015).

management functions[17] pursuant to a cooperative agreement with NTIA which ensures that the procedure of making changes to the root zone is properly followed and observed.

Areas of ambiguity, unresolved issues and possible gaps in dealing with the root zone

Governance of the root zone has been one of the most controversial issues in the international Internet policy debate. The main point raising divergent views has been about the historical role of the United States in the stewardship of changes to the root zone as administered through the IANA process by ICANN. Some inputs to WGEC/CG also highlighted the oversight of the IANA function as one of the main policy gaps in the current arrangement for the root zone.

As explained above, the United States government announced that it intended to transfer its oversight responsibilities under the IANA contract to the global multi-stakeholder community. The process of transition, which the NTIA entrusted to ICANN, includes a wider array of consultations with the multi-stakeholder community, which are currently underway.

2.7 Net neutrality

As a principle, net neutrality requires equal treatment of Internet traffic, regardless of the type of service, the sender, or the receiver of said traffic. In practice, however, the Internet service providers conduct a degree of appropriate traffic management (i.e., reasonable differentiation) aimed at avoiding congestion, and delivering a reliable quality of service.

Discussions about net neutrality mainly concern definitions of (in)appropriate and (un)reasonable management and discriminatory practices, especially those that are conducted for commercial (e.g. anti-competitive behaviour) or political reasons (e.g. censorship).

Net neutrality has three important dimensions: a technical dimension (impact on Internet infrastructure), an economic dimension (influence on Internet business models), and a human rights dimension (possible discrimination in the use of the Internet).

Status of mechanisms concerning net neutrality

Net neutrality features prominently in Internet policy debates at national level in many countries. At regional level, the European Union leaves the enforcement power concerning net neutrality to national regulatory authorities (NRAs) and their European association, BEREC (Body of European Regulators of Electronic Communications). The Council of Europe emphasises the human rights dimension of the issue. Its Committee of Ministers has

[17] These include the management of the root zone "zone signing key" (ZSK), as well as implementation of changes to and distribution of the DNS authoritative root zone file. See http://www.ntia.doc.gov/other-publication/2014/iana-functions-and-related-root-zone-management-transition-questions-and-answ (accessed 9 April 2015).

adopted a *Declaration of the Committee of Ministers on network neutrality* in 2010. The OECD approaches the issue from an economic perspective, through forums and analytical work related to Internet traffic exchange, including competition and consumer protection issues.

Among others, net neutrality has been discussed at the Internet Governance Forum, within its Dynamic Coalition on net neutrality. A number of Internet principles initiatives by global NGOs and other civil society entities, such as the Internet Rights and Principles Coalition, include net neutrality among their fundamental principles (either directly or through a non-discriminatory principle).

Areas of ambiguity, unresolved issues and possible gaps in dealing with net neutrality

The debate on net neutrality has focused on whether network operators and/or Internet service providers should be allowed to have more control of the content that passes through their networks.

Net neutrality is a complex issue which requires careful consideration in order to avoid the implementation of "solutions" which then turn into problems. In particular, it poses challenges due to the need to balance various technical, economic and human rights perspectives. Other areas of complexity in the context of net neutrality include issues related to access, choice and transparency, competition as well as consumer information and user choice.

Some submissions to the WGEC/CG indicated a lack of a global forum where net neutrality issues can be addressed as a possible policy gap. Others suggested that net neutrality issues are best handled at the national and regional level.

The analysis of mechanisms shows a knowledge gap resulting from a lack of data and research on traffic management practices and their effects on quality of service, competition, innovation, investments, and protection of human rights.

Likewise, there are no established mechanisms that can evaluate the effects of various regulatory approaches on investments, innovations, diversity, and online freedoms.

2.8 Cloud computing

Cloud computing has emerged with the major shift of data from personal computers and local servers to server farms collectively referred to as "the cloud". Early application of public cloud services include web mail (Gmail, Yahoo!), social media applications (Facebook, Twitter), and other online applications (Wikis, blogs, Google docs). Apart from everyday applications, cloud computing is extensively used for business software. Cloud services can be divided in the following three main groups: 1) Software as a Service (SaaS); 2) Platform

as a Service (PaaS); and 3) Infrastructure as a Service (IaaS). Leading players in the cloud economy include Google, Microsoft, Apple, Amazon Web Services, and Facebook.[18]

Status of governance mechanisms concerning cloud computing

As a policy issue cloud computing is mainly addressed at national level by laws and regulations that either target cloud services specifically or are applicable to cloud as well as similar activities.

IETF, ISO, ITU and a number of other organizations, forums and consortia are involved in standardization work concerning cloud computing. ITU, for example, has a Focus Group on Cloud Computing.

There are a number of working groups on cloud computing, such as The Open Group Cloud Computing Work Group, which includes some of the industry's leading cloud providers and end-user organisations; and the Cloud Computing Strategy Working Group of the European Telecommunications Standards Institute (ETSI).

Cloud computing is addressed from various policy perspectives: critical information infrastructure (availability of cloud services), data protection (securing data stored in the cloud), encryption (protection of data in communication among cloud servers), privacy, and consumer protection in providing services from cloud servers.

Areas of ambiguity, unresolved issues and possible gaps in dealing with cloud computing

The expansion of cloud computing has raised concerns about security, data protection and privacy. While the importance of protecting data in a cloud environment is broadly accepted, jurisdictions addressing it in different countries diverge significantly. While there is not necessarily a need to develop laws and regulations which are specific to cloud computing, legal reforms would be important in areas which are relevant to cloud computing such as privacy, data protection, information security and cybercrime. [19]

Cloud computing is a relatively new phenomenon where there may be a need for more research, data and awareness raising. On the policy level there is a need for more intersectoral analysis of the interplay between cloud computing and other related Internet public policy issues such as the above mentioned data protection and privacy, technical infrastructure, e-commerce, and security, among others. An international response could also include consideration of what constitutes a base-line regulation on these issues and how to make national regulations more interoperable.

---

[18] UNCTAD, *Information Economy Report 2013: The Cloud Economy and Developing Countries* (New York and Geneva, United Nations publication), p. 18.

[19] Ibid. p. 88.

2.9 Convergence

From a technical point of view, convergence refers to the ability of diverse networks and devices to carry and deliver a variety of services, each of which was previously carried or delivered separately. As a result, among other things, companies can offer consumers a variety of services such as cable television, Internet and mobile access in one bundled package. The Internet has blurred the boundaries between telecommunications, media and the management of information, leading to convergence of different policy fields.

Convergence challenges relate to technology (a common platform for delivery data, voice and multimedia), services (variety of digital services delivered via the same medium), and regulation (the need for more integrated regulation of previously separate areas of telecommunication, information, broadcasting, etc.).

Status of mechanisms for convergence

The policies which are relevant to convergence are mainly defined and implemented at national level. At international level, governance mechanisms are mainly used for the exchange of best practices and experiences. The ITU's Telecommunication Development Sector (ITU-D) has a study group on the converging environment. The Council of Europe has a Steering Committee on Media and Information Society (CDMSI) which brings together government experts from 47 member states. The CDMSI is responsible for elaborating policies and standards on freedom of expression, media and the Internet. These policies cover one aspect of convergence, namely the interplay between traditional and new digital media.

Convergence is most directly related to net neutrality, the Internet of Things, the role of intermediaries, e-commerce, consumer protection, and taxation.

Areas of ambiguity, unresolved issues and possible gaps in dealing with convergence

While technical convergence has progressed rapidly, its legal aspects need some time to evolve. For example, while technological development creates convergence of services for telephony, Internet access, and television, these three areas are still in many countries regulated by different legal rules. Eventually, legal solution should address technological convergence properly.

The mechanisms analysed appear to indicate a knowledge gap of data, research, and awareness of the impact of convergence on Internet public policy issues.

2.10. The Internet of Things

The Internet of Things (IoT) refers to the imminent emergence of wide range of Internet-connected devices, including new generation of devices ranging from fridges that communicate directly with a smartphone, and watches that can detect and monitor health.

The IoT's core functionality depends on collecting and on networks capable of processing high volumes of data in real time.

Status of mechanisms concerning the Internet of Things

The governance of the IoT is at relatively an early stage. The IETF and the IEEE have developed standards of relevance to the IoT. ITU hosts the Internet of Things Global Standards Initiative and its Study Group 13 (Future networks including cloud computing, mobile and next generation networks) covers issues related to IoT. At regional level, the EU has a Task Force on the Internet of Things. At the Internet Governance Forum, it is addressed by the IGF Dynamic Coalition of the Internet of Things.

Areas of ambiguity, unresolved issues and possible gaps in dealing with the Internet of Things

The digitalisation and automation of devices, as well as the sheer volume of data to be managed, creates new challenges for regulation. Confidence in and acceptance of the IoT depends on the creation of a regulatory environment that provides protection for users' rights. Concerns over privacy, data protection and security are the most frequently mentioned.

The development of the IoT will depend on the existence of a reliable and effective system for handling data. Integration of the IoT in very large numbers of devices raises new challenges concerning user consent. The IoT will also depend on the development of technical standards to facilitate effective communication among different devices with different operating systems.

The mechanisms analysed appear to indicate that there is a knowledge gap concerning the impact of the development of the IoT on human rights, consumer protection, competition policy, and other relevant public policy issues.

3. Security cluster

The public policy issues in the security cluster aim to ensure functional and reliable use of the Internet. The security cluster highlights cyber security as its main umbrella issue, and includes other more specific Internet policy issues.

3.1 Cybersecurity

There is no universally agreed definition of cybersecurity. The ITU has defined its meaning as "the collection of tools, policies, security concepts 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."[20]

Cyber security is an umbrella concept covering several areas including cybercrime, critical information infrastructure protection (CIIP), and cyber conflicts. Most online threats come about as a result of software and hardware vulnerabilities exploited by organised and expanding global cybercrime communities. The international community still lacks a systematic and decisive approach to combating global cybercrime.

Status of governance mechanisms concerning cybersecurity

At national level, a growing volume of legislation and jurisprudence deals with cyber security, with a focus on combating cybercrime and, increasingly, protecting the critical information infrastructure from sabotage and attacks. At regional levels, an increasing number of organisations are realising the importance of cybersecurity and are working on strategies, recommendations, and conventions concerned with it. These include the Council of Europe Convention on Cybercrime, the Asia-Pacific Economic Cooperation (APEC) Strategy on Secure Online Space, the Cybersecurity Strategy of the European Union, the OSCE Decision No. 1106[21], and the African Convention on Cybersecurity and Data Protection.

At the international level, there have been annual reports of the United Nations Secretary-General and the United Nations General Assembly has adopted several resolutions on *Developments in the field of information and telecommunications in the context of international security* on a yearly basis. In addition there have been three Groups of Governmental Experts (GGE) that have examined the existing and potential threats from the cyber-sphere and possible cooperative measures to address them. [22]

In WSIS, the Action Line C5 on Building Confidence and security in the use of ICTs is primarily concerned with cyber security. Its implementation is facilitated by the ITU. Under its Global Cybersecurity Agenda (GCA), ITU fosters initiatives such as Child Online Protection and the ITU-IMPACT Partnership. In addition to activities related to facilitation of the Action Line, the ITU has produced resolutions as well as standards and recommendations concerned with cybersecurity.

---

[20] ITU Recommendation ITU-T X.1205, available at https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items (accessed 9 April 2015).

[21] OSCE, 2013, *Initial Set of OSCE Confidence Building Measures to reduce the risk of conflict stemming from the use of Information and Communication Technologies* (PC.DEC/1106).

[22] More information on the outcomes of the United Nations General Assembly in this area is available at http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/69/28 (accessed 9 April 2015).

The OECD adopted *Guidelines for the Security of Information Systems and Networks* in 2002. It also prepared a study of national cybersecurity strategies[23] that was released in 2012.

The Forum of Incident Response and Security Teams (FIRST) is an international technical network which coordinates the activities of national and regional Computer Emergency Response Teams (CERTs). For the network security, a key existing mechanism is the Security and Stability Advisory Committee (SSAC) under ICANN.

A series of Conferences on Cyberspace has been held in London (2011), Budapest (2012), Seoul (2013), and The Hague (2015).

Cybersecurity has also been widely discussed in the context of the Internet Governance Forum.

Areas of ambiguity, unresolved issues and possible gaps in dealing with cyber security

The transborder nature of Internet as well as the speed and the sheer volume of communications pose several challenges to cybersecurity such as those related to the identification, investigation, jurisdiction, criminalisation and prosecution of those who commit security breaches.

There has been much debate about the desirability of a new international legal instrument on cyber security but there is no consensus on this issue.

There have also been calls for more multilateral and multi-stakeholder cooperation and coordination on cyber security issues. More could be done to address cyber security issues in an intersectoral way by involving different professional groups, including: the telecom sector, diplomatic communities, security communities, corporate sector associations, hacker communities and civil society.

In addition, there is a need for more research on the impact of cyber security, including assessment of impact of cyber security breaches on society.

3.2 Cybercrime

Cybercrime is part of a broader cyber security approach aimed at ensuring Internet safety and security. Cybercrime encompasses harmful acts that are committed from or against a computer or a network. It includes existing criminal offences conducted online (*e.g.* fraud), crimes that take new forms due to the Internet (*e.g.* child abuse), and new crimes that have emerged with the Internet (*e.g.* unauthorised access, damage to computer data, pay-per-click

[23] OECD, 2012, *Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy* (OECD publication), available at http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf (accessed 13 April 2015).

frauds). These three aspects are often referred to in the context of cybercrime. However, there is no internationally accepted definition of the term.

International cooperation in fighting cybercrime is vital for two reasons: (i) offenders are often in different jurisdictions, exploiting transborder aspects of the Internet; (ii) effective responses to cybercrime require fast action (*e.g.* preserving evidence, investigation).

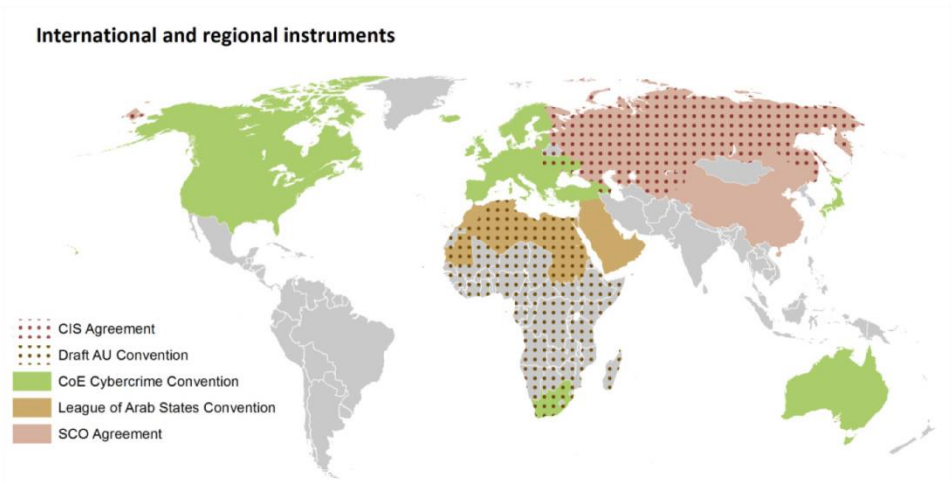
Status of mechanisms concerning cybercrime

Combatting cybercrime involves diverse and elaborate mechanisms. As of November 2014, 117 countries (of which 82 developing and transition economies) had enacted cybercrime legislation, and another 27 countries had draft legislation underway.[24]

The Council of Europe Convention on Cybercrime (the so-called Budapest Convention, 2001) is the oldest cybercrime legal instrument, and has inspired a number of other regional and national regulations. Other regional instruments include: the League of Arab States Convention on Combating IT Offences (2010), the Shanghai Cooperation Organisation Agreement on Cooperation in the Field of International Information Security, and the African Union Convention on the Confidence and Security in Cyberspace (2014).

The United Nations Office on Drugs and Crime (UNODC) is the leading organisation at a global level, with a set of international instruments to combat cybercrime. It addresses cybercrime through multiple channels, including through the United Nations Convention against Transnational Organized Crime. It has mapped different international and regional cybercrime instruments as follows.

Figure 3: Geographic coverage of the international and regional cybercrime instruments.



Source: *UNODC Comprehensive Study on Cybercrime – 2013*

[24] UNCTAD *Information Economy Report 2015: Unlocking the Potential of E-commerce for Developing Countries*, p. 73.

Interpol facilitates a global network of 190 national police organisations, which plays a crucial role in the cross-border investigation of cybercrime. Interpol's Global Complex for Innovation (IGCI) is a research and development facility for the identification of crimes and criminals, innovative training, operational support and partnerships.

The G8 has been addressing cybercrime since 1997 when it established a Subcommittee on High-tech Crimes. One of the committee's main achievements was the establishment of an international 24/7 network of contacts for dealing with cybercrime issues.

FIRST is a forum in the technical community for addressing cyber security and cybercrime issues, which functions as a network of CERTs, the main bodies for addressing cyber security issues at national level.

The Anti-Phising Working group (APWG) acts as a worldwide coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors.

Cybercrime is most directly related to the following Internet policy issues: technical standards, cyber security, child safety, encryption, freedom of expression, privacy and data protection, jurisdiction, intermediary responsibility, e-commerce, e-money, access, cloud computing, and content policy.

Areas of ambiguity, unresolved issues and possible gaps in dealing with cybercrime

The ambiguity concerning cybercrime is caused by the predominantly transborder nature of Internet which poses particular challenges for the detection of online crimes as well as for law enforcement.

The main knowledge gap is related to a shortage of reliable statistics and data on cybercrime that should trigger, inform, and shape cybercrime policy and responses. Policy gaps include the lack of a common or widely accepted definition of cybercrime. In addition, it is difficult to create a mechanism to ensure that policy against cybercrime stays abreast of technological developments.

Implementation gaps include the insufficient use of international instruments in criminal matters (mutual assistance agreements, regional, and global arrangements). Harmonisation of national cybercrime legislation could be enhanced in order to facilitate cooperation in cybercrime investigation. However, it should be noted that there is no consensus on creating a new international instrument on cybercrime.

Institutional and individual capacities in cybercrime (juridical, law enforcement) are needed in order to reduce the number of "safe havens" for cybercrime attacks, as is an intersectoral approach for cybercrime activities, including human rights (privacy protection, freedom of expression), and economic aspects (trustworthy environment for e-commerce).

3.3 Internet as part of critical information infrastructure

There are several definitions of critical information infrastructure (CII). According to one definition, it is "systems that are so vital to a nation that their incapacity or destruction would have a debilitating effect on national security, the economy, or public health and safety."[25]

The Internet provides an important part of critical information infrastructure today. First, the Internet is a communication, economic, and information platform for all almost three billion Internet users. Second, it provides communication supports for vital systems of modern society. Therefore, the Internet must be accessible, secure, and reliable.

Status of mechanisms concerning Internet as part of critical information infrastructure

The CII is commonly addressed in the context of its protection which is primarily addressed at national level. A systematic approach includes also enhanced regional and international cooperation and effective public-private partnerships.

CII is increasingly addressed by various regional organisations (OSCE, ASEAN, Shanghai Cooperation Organisation, OAS, APEC). In 2008, the OECD adopted a *Recommendation of the Council on the Protection of Critical Information Infrastructures* that sets forth a policy framework for governments to implement the *OECD Security Guidelines* in relation to the protection of CII. CERTs are also important governance mechanisms.

Built around annual conferences, the Meridian Process is a global platform which seeks to exchange experiences and to initiate actions for the cooperation of governmental bodies on Critical Information Infrastructure Protection (CIIP).

Technical infrastructure and cloud servers are essential for the functioning of the Internet as part of the CII.

Areas of ambiguity, unresolved issues and possible gaps in dealing with Internet as part of critical information infrastructure

One submission to this review suggested that there is a need for careful consideration of how the CII has evolved to date and how it may support future security needs and requirements. In general, the mechanisms analysed appear to indicate a knowledge gap due to insufficient research and lack of awareness of the CII's importance in many countries.

Some submissions to the WGEC/CG also indicated lack of policy mechanisms for addressing CII issues at regional and international levels, including a forum for exchange of security awareness and related information for organizations tasked with protection of CII globally.

---

[25] See IETF *Internet Security Glossary (Version 2) RFC 4949*, available at https://datatracker.ietf.org/doc/rfc4949/ (accessed 9 April 2015).

3.4 Cyber conflict

There is no universally accepted definition of cyber conflict. According to one definition, it is "actions taken by parties to a conflict to gain advantage over their adversaries in cyberspace by using various technological tools and people-based technics." Cyber conflict can be carried out by damaging, destroying, disabling, or usurping an adversary's computer systems (cyber attack) or by seeking information that the adversary would prefer to keep secret (cyber espionage, or cyber exploitation).[26] If applied in the context of international humanitarian law, use of the term cyber conflict should be restricted to contexts of armed conflict or related to armed conflict.

Cyber conflict covers three main fields: the conduct of cyber conflict, weapons and disarmament, and humanitarian aspects of cyber conflict.

Status of mechanisms concerning cyber conflict

Several international initiatives do research and map the field of cyber conflict. The United Nations Institute for Disarmament Research (UNIDIR) has developed a Cyber Index which provides survey of cybersecurity activities on national, regional and international levels.

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* provides – so far – the most comprehensive analysis of the interplay between existing international legal instruments and various aspects of cyberconflict.

Areas of ambiguity, unresolved issues and possible gaps in dealing with cyber conflict

The ambiguity relate to the applicability of the International Law in cyber conflict. The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security has noted that International Law, in particular the Charter of United Nations, is applicable on the ICT environment. In its report, the group made a number of recommendations, including a further study to promote a common understanding on how norms that are derived from International Law apply to State behaviour and the use of ICTs by States.[27]

The most challenging questions with regard to the conduct of cyber conflict and to humanitarian aspects of it are concerned with the application of the international law (e.g. The Hague Conventions) to cyberspace. For weapons and disarmament, the main governance mechanisms are likely to emerge through adjustments to existing disarmament mechanisms.

---

[26] Herbert Lin, *Cyber conflict and international humanitarian law*, International Review of the Red Cross (Volume 94, number 886, Summer 2012), p. 515. Available at https://www.icrc.org/eng/assets/files/review/2012/irrc-886-lin.pdf (accessed 9 April 2015)

[27] United Nations General Assembly, 2013, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98), available at http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 (accessed 9 April 2015).

Issues concerning humanitarian law rules relate to the applicability of the Geneva conventions to cyber conflict.

The analysis of existing mechanisms indicates a knowledge gap related to insufficient data and research on the nature of cyber conflicts and their impact on international Internet public policy issues. On the policy level, there is a lack of common and widely accepted definitions of key concepts in the field of cyber conflicts.

There are wide differences of opinion of the need for international legal instruments on cyber conflict.

3.5 Child safety online

Many issues related to safe Internet behaviour are primarily concerned with protecting young people, especially minors from online threats and empowering them on their rights and responsibilities and on what constitutes safe online behaviour.

This section discusses protecting children and minors from threats which include, among others, cyber-bullying, abuse, and sexual exploitation, including the distribution of child sex abuse images. There is a need to educate children and young people on risks and responsibility they may encounter when using the Internet. Close cooperation among key actors – parents, educators, and the community – is essential for developing capacity building and other initiatives to safeguard children and to empower them to recognize and avoid dangers in computer-mediated environments.

Status of mechanisms for child safety online

At national level, in many countries there is a policy focus on child safety with many regulatory, training, and awareness-building initiatives. Child safety online is addressed in the IGF within the Dynamic Coalition on Child Online Safety. UNICEF has research, policy development and awareness-building activities on child safety and digital citizenship. The ITU has launched a Child Online Protection initiative. The European programs INSAFE and INHOPE are regional mechanisms whose scope reaches beyond Europe.

NGOs such as the International Centre for Missing and Exploited Children, ECPAT International, Save the Children, and the Child Exploitation and Online Protection Centre play an important role, both maintaining strong networks focused on awareness, education, monitoring, information sharing, and alerts (call centres), and through lobbying to establish governance mechanisms in this field.

Interpol and Europol are developing implementation mechanisms for the protection of children online.

The OECD Council adopted a *Recommendation on the Protection of Children Online* in 2012. It built on OECD's earlier report *The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them*.

Areas of ambiguity, unresolved issues and possible gaps in dealing with child safety online

Protecting children and young people and educating them on risks and responsibilities on using the Internet is a global task. A holistic approach empowers children and young people to recognize and avoid dangers, while equipping them with online literacy and awareness of their own rights and responsibilities on the Internet, and addressing the potential for their voices to become more widely heard.

The mechanisms analysed appear to indicate the existence of a policy gap in the coordination of various policy initiatives and activities. There is also insufficient inclusion of concerned actors in international policy activities (*e.g.* international organisations, Internet industry, NGOs, youth and children associations). The review also indicates a policy gap in intersectoral coordination in dealing with child safety online (e.g. security, human rights, education).

3.6 Encryption

Encryption refers to the scrambling of electronic documents and communication into an unreadable format which can be read only through the use of encryption software. To read encrypted file, one must have access to a secret key or password.

Encryption is the most commonly used method to achieve data security on the Internet. Protection of credit card and personal information through encryption constitute key to electronic commerce.

Status of mechanisms concerning encryption

The only international instrument that regulates the sharing of encryption technologies is the Wassenaar Arrangement, through which 41 countries restrict the export of conventional weapons and "dual use" technologies to countries at war or to other countries indicated by the Wassenaar member States. In 1997, the OECD adopted *Guidelines on Cryptography Policy*, to promote the use of cost-effective, interoperable, portable and mobile cryptography systems without unduly jeopardizing public safety, law enforcement, and national security.

Encryption is most directly related to the following Internet policy issues: cloud computing (encryption of data exchanged among servers in cloud – particularly important for Internet companies to ensure protection of users' data), technical standards, the Internet of Things, cybercrime, privacy, data protection, jurisdiction, intermediaries, e-commerce, e-payment, consumer protection, access, and content policy.

Areas of ambiguity, unresolved issues and possible gaps in dealing with encryption

Governments balance between the respect for the privacy of online communications and the need to monitor some communication of relevance to national security. The emergence of new encrypted products has raised a policy debate on whether governments should have access to decrypted messages and if so, under what conditions.

The certification of security measures including encryption has been also under debate. There is no consensus on who should issue such certificates and how they should be issued.

The mechanisms analysed appear to indicate the existence of a policy gap in ensuring human rights considerations (freedom of expression, protection of privacy) in the encryption standardisation process.

3.7 Spam

Spam is usually defined as unsolicited e-mail sent to a wide number of Internet users. It is mainly used for commercial purposes. However, spam is also used as a tool for pfishing, distibution of malware and other illegal activities.

Spam invades the recipient's privacy. It may also represent consumer fraud and/or include content which is harmful for minors.

Spam elevates business costs, lowers productivity and represents a challenge to the development of the Information Society as a whole.

Status of mechanisms for addressing spam

The OECD has undertaken series of activities in fight against spam. In addition to its 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce* which recommend protection against spam, the OECD has established a task force on spam. In 2006, it adopted an anti-spam toolkit. At the regional level, the EU established the Network of Anti-Spam Enforcement Agencies, and APEC prepared a set of *Voluntary Online Consumer Protection Guidelines* in 2012. A provision regarding spam was included in the ITU's *International Telecommunication Regulations* (ITRs), revised in 2012.

The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) brings the messaging industry together to work collaboratively and to successfully address the various forms of messaging abuse. The Anti-Spam Technical Alliance gathers leading Internet companies that host e-mail accounts. The London Action Plan includes representatives from the government regulatory and enforcement community and industry, and provides a platform for information sharing about anti-spam regulation and enforcement initiatives. Organizations such as the Internet Society (ISOC) conduct projects to assist developing

countries in combating spam. The Internet Governance Forum also provided a number of best practices on combating spam within its Best Practices Forum in 2014.

Spam relates most directly to the following Internet policy issues: technical standards, net neutrality, cybercrime, child safety, digital signatures, freedom of expression, privacy, jurisdiction, intermediaries, e-commerce, consumer protection, access, the digital divide, and content policy.

Areas of ambiguity, unresolved issues and possible gaps in dealing with spam

Spam continues to be a problem in many countries. According to one statistics, 66 per cent of email traffic in 2013 was spam[28]. Spammers are increasingly exploiting the cross-border nature of the Internet. There is no one single solution that would tackle the problem. Appropriate legislation, its effective enforcement and stronger cooperation and partnerships across borders is needed to effectively combat it.

Failures to combat spam may be due to insufficient capacity and technical tools. The mechanisms analysed appear to indicate the existence of a gap on the availability of information on spam related issues. Although there are initiatives to evaluate the impact of spam, there is insufficient reliable information concerning spam, its costs and its consequences.

3.8 Digital signatures

Digital signatures are a method of authentication for individuals on the Internet, in particular in e-commerce transactions. Digital signatures are often discussed in the broader context of authentication, including the questions of anonymity and attribution of activities on the Internet. They are particularly important in building trust on the Internet.

Status of mechanisms for digital signatures

In 2001, UNCITRAL adopted the Model Law on Electronic Signatures, which grants the same status to digital signatures as to handwritten ones, providing some requirements are met. In 2005, the United Nations adopted the UNCITRAL Convention on the use of Electronic Communications in International Contracts. It builds upon earlier instruments drafted by the UNCITRAL: the aforementioned Model Law on Electronic Signatures and the Model Law on Electronic Commerce.

[28] Symantec, 2013 Trends, Volume 19, *Internet Security Threat Report 2014* (published April 2014). p. 14, available at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf (accessed 9 April 2015).

The International Chamber of Commerce (ICC) issued a *General Usage for International Digitally Ensured Commerce* (GUIDEC), which provides a survey of the best practices, regulations, and certification issues.

Digital signatures are most directly related to the following Internet policy issues: technical standards, the Internet of Things, cybercrime, encryption, privacy, data protection, jurisdiction, intermediaries, e-commerce, e-payment, consumer protection, cloud computing, access, and content policy.

Areas of ambiguity, unresolved issues and possible gaps in dealing with digital signatures

E-transactions laws vary from country to country and provide different standards for what constitutes an electronic signature. The main challenge in this area is how to increase global compatibility and interoperability among different domestic electronic signatures laws in order to enable cross-border recognition of e-signatures on a technology-neutral basis and therefore to facilitate faster development of e-commerce.

4. Human rights cluster

"The same rights that people have offline must also be protected online" is the underlying principle for human rights on the Internet. [29] The principle of human rights should apply to all aspects of the Internet. The review takes into consideration relevant human rights legal instruments and United Nations General Assembly resolutions.

In WSIS, the *Geneva Declaration of Principles* refers to Article 19 of the Universal Declaration of Human Rights (UDHR) as the foundation of the Information Society. The said article affirms that "everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[30]

The *Geneva Declaration of Principles* also reaffirms the commitment to Article 29 of the UDHR which notes that "everyone has duties to the community in which alone the free and full development of their personality is possible", and that, "in the exercise of their rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others

[29] This principle was affirmed by the United Nations Human Rights Council in its resolutions concerning *Information and Communication Technologies for Development* (Resolution A/RES/68/198) and by the United Nations General Assembly in its resolutions on *The Right to Privacy in the Digital Age* (A/RES/69/166 and A/RES/68/127) following consideration by the United Nations Human Rights Council in 2013.

[30] See *Geneva Declaration of Principles*, para 4. WSIS outcomes are published in ITU, 2005, WSIS Outcome Documents: Geneva 2003-Tunis 2005 (Geneva, United Nations publication).

and of meeting the just requirements of morality, public order and the general welfare in a democratic society."[31]

Human rights issues are cross-cutting and interdependent. Therefore, it is also important to consider the interdependencies and inter-relationships between different human rights in the context of the Internet. For example, freedom of expression and information is related to access to the Internet and net neutrality. Protection of minority rights is influenced by multilingualism and promotion of cultural diversity. Ensuring protection of privacy is important in dealing with cybersecurity. Human rights include various other rights that are relevant but have not been discussed here, such as freedom of association.

4.1 Freedom of expression

Freedom of expression includes that "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[32] Any limitations to freedom of expression should be the exception rather than the norm.

With the growing relevance of the Internet, the policy debate on freedom of expression has gained online relevance.

Status of mechanisms concerning freedom of expression

Freedom of expression is protected by the Universal Declaration of Human Rights (UDHR) (Article 19, see above) and the International Covenant on Civil and Political Rights (Article 19 as well). Any limitation on freedom of information should comply with Article 29 of the UDHR (see above) and Article 19(3) of the International Covenant on Civil and Political Rights.

Regional instruments concerned with freedom of expression include the European Convention on Human Rights (Article 10) and the American Convention of Human Rights (Article 13). The mechanisms that are concerned with freedom of expression apply also to Internet. The United Nations Human Rights Council's Resolution concerning *The promotion, protection, and enjoyment of human rights on the Internet* affirms "that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance

[31] Ibid., para 5.

[32] United Nations, *International Covenant on Civil and Political Rights*, Article 19.

with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."[33]

UNESCO is mandated to promote freedom of expression and associated rights online and offline. UNESCO has examined dimensions of online rights in two major publications – *Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet* (2011) and a *Global Survey on Internet Privacy and Freedom of Expression* (2012).

Non-governmental organizations such as Human Rights Watch, Amnesty International and Freedom House have developed numerous mechanisms for monitoring and discussing freedom of expression on the Internet.

Areas of ambiguity, unresolved issues and possible gaps in dealing with freedom of expression

The main open issue is how to establish the right interplay (or balance) between Article 19 of the International Covenant on Civil and Political Rights, which defines freedom of expression, and also sets out the limits of freedom of expression to protect the rights or reputations of others or to protect national security public order, public health or morals.

While censorship in general is considered as a violation of freedom of expression, it may be legitimate, in some cases, to block certain content, such as material that incites violence. This brings about questions as to what to block, for how long, in what proportion, and with what transparency and redress mechanisms.[34]

The mechanisms analysed appear to indicate the existence of a knowledge gap with regards to data and research on the ways how the Internet technical architecture impacts freedom of expression. For example, freedom of expression is influenced by the degree of anonymity on the Internet, which in turn could be shaped by technical solutions that facilitate access to the Internet.

4.2 Privacy and data protection

Privacy can be defined as the right of citizens to control personal information and to decide whether, to whom, and under what circumstances it may be known to and/or used by others. Privacy and data protection are interrelated public policy issues of relevance to the Internet.

---

[33] United Nations Human Rights Council, 2014, *The Promotion, Protection, and enjoyment of human rights on the Internet* (Resolution A/HRC/RES/26/13).

[34] UNESCO, 2015, *Keystones to foster inclusive Knowledge Societies: Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet, Draft study* (Paris, UNESCO publication), p. 36.

Data protection is a legal mechanism that establishes rules governing the privacy of digital information.

Status of mechanisms concerning privacy and data protection

The International Covenant on Civil and Political Rights (ICCPR) includes the provision according to which "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[35] United Nations Specialized Agencies also include privacy and data protection matters in their basic instruments. UNESCO is working on the right to privacy. It has published a *Global Survey on Internet Privacy and Freedom of Expression.*

The OECD *Guidelines on Protection of Privacy and Transborder Flows of Personal Data* (1980) have inspired other national and regional online privacy regulations. They were updated in 2013, with revisions focused on the practical implementation of privacy protection through an approach grounded in risk management, and on recognition of the need for greater efforts to address the global dimension of privacy through improved interoperability.

On the regional level, in Europe the main instruments are the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) and the European Union's Data Protection Directive. In Asia, APEC has introduced a regional *Privacy Framework.*

In December 2013, the UN General Assembly (UNGA) adopted a resolution on *The right to privacy in the digital age* in which it requested the United Nations High Commissioner for Human Rights to prepare a report to the United Nations General Assembly in 2014 on online privacy and the impacts of surveillance[36].The report *The right to privacy in the digital age* was presented to the United Nations Human Rights Council at its 27th session in September 2014 and to the United Nations General Assembly at its 69th session. In December, the General Assembly approved a further resolution on the *Right to privacy in the digital age*.

At the regional level, The European Court of Justice's judgement on the right to be forgotten has introduced a controversial new mechanism in dealing with privacy and data protection.

Privacy and data protection are very important for the future growth of the Internet of Things, cloud computing, and e-commerce.

Following table lists international documents that include provisions concerning data protection.

---

[35] United Nations, *International Covenant on Civil and Political Rights*, Article 17.

[36] General Assembly, 2013, *The right to privacy in the digital age* (Resolution A/RES/68/167).

Table 1: Data protection principles in international documents

Data Protection Principles	Council of Europe Convention	OECD Guidelines	EU Directive on Data Protection	APEC Privacy Framework
Fair and lawful means of collecting data	✓	✓	✓	✓
Specified and legitimate purposes of collection	✓	✓	✓	✓
Relevance of data to the purpose of collection	✓	✓	✓	✓
Accuracy of data	✓	✓	✓	✓
Limitation in time of data storage to The purpose of collection	✓	-	✓	-
Special treatment of 'sensitive data'	✓	-	✓	-
Security of data processing and storage	✓	✓	✓	✓
Information of data subject about data processing	✓	✓	✓	✓
Access to and intervention of data subject on personal data	✓	✓	✓	✓
Accountability for data processing	✓	✓	✓	✓

Source: Tan, 2008.

Areas of ambiguity, unresolved issues and possible gaps in dealing with privacy and data protection

Freedom of expression and the right to privacy are related human rights. The right to privacy underpins other rights and freedoms, including freedom of expression, association and belief. Challenges arise in applying these rights in the context of the Internet's transnational diffusion, the opportunities and functionality of new media, and disparate national legal frameworks.

While there are existing legal instruments on privacy protection, a few submissions indicated the view that there is a lack of international mechanisms to address online aspect of privacy protection.

Some submissions stated that another gap is a lack of mechanisms to address mass surveillance. There is ongoing discussion concerning ways to protect personal data in

accordance with the laws applicable to individuals' countries of domicile. However there is no consensus on this.

The mechanisms analysed indicate the existence of policy gaps due to insufficient intersectoral approaches to privacy and data protection at both regional and global levels.

4.3 Rights of people with disabilities and the Internet

The Internet provides new opportunities for the social inclusion of people with disabilities, but at the same time offers challenges for accessibility. The lack of accessibility arises from the gap between the abilities required to use hardware, software, and content, and the functional capacities resulting from some disabilities. An appropriate policy solution can help in maximising use of the Internet by people with disabilities. Policy actions are moving in two directions:

- including accessibility standards in the requirements for the design and development of equipment, software, and content; and
- fostering the availability of hardware and software accessories that increase or substitute for functional capabilities.

Status of mechanisms concerning rights of people with disabilities on the Internet

The Convention on the Rights of Persons with Disabilities (2006) provides the general legal context for the rights of people with disabilities on the Internet. This policy issue is also addressed by the IGF Dynamic Coalition on Accessibility and Disability, by initiatives such as the Internet Society Disability and Special Needs Chapter, and by the International Center for Disability Resources on the Internet. International standards in web accessibility are developed by W3C within its Web Accessibility Initiative.

Areas of ambiguity, unresolved issues and possible gaps in dealing with rights of people with disabilities

Many web applications do not comply with accessibility standards due to a lack of awareness on the part of their designers, or the perception that compliance involves complexity and high costs.

The mechanisms analysed indicate the existence of a knowledge gap concerning data and research on the relationship between the Internet and the accessibility needs of people with disabilities. In spite of major efforts, there are still policy gaps of the structured coverage of accessibility in the development of Internet technical and web standards.

4.4 Women's rights online

The main focus of women's rights online is in respect to discrimination in the exercise of rights, such as the right to hold office, the right to equal pay, and the right to educational and economic opportunities. With the increasing shift of professional and social life activities to the Internet, the full achievement of women's rights online will depend on different policies related to both online and offline contexts.

Status of mechanisms concerning women's rights online

Established in 2010, UN Women focuses on gender equality and the empowerment of women with strong involvement in the implementation and follow-up to the WSIS process.

The UN Human Rights Council has also an important role to play, with active work on various aspects of women's rights overall. The United Nations secretariat and the United Nations Funds, Programmes and Specialized Agencies address gender equality and women's empowerment on the Internet from their own work area. For instance,

The Internet Governance Forum has an active Dynamic Coalition on Gender Rights.

Areas of ambiguity, unresolved issues and possible gaps in dealing with women's rights online

There appears to be a significant digital divide in ICT access and use between women and men, in particular as far as developing countries are concerned.

The mechanisms analysed appear to indicate the existence of a policy gap in mainstreaming online aspect of activities of existing international bodies and processes dealing with women's rights. In addition, it is indicated that there is a lack in policy coordination among various international initiatives dealing with women's rights online. The capacity gap exists with regard to insufficient capacity of organisations dealing with women's rights to address the online aspect of these rights.

5. Legal cluster

Legal Internet public policy issues are cross-cutting, affecting most of the other policy clusters. Most issues are already legally regulated for the offline environment (jurisdiction, copyright, trademark, labour law). The main challenge in this cluster is the application of existing legal mechanisms to Internet transactions, particularly in view of the transborder nature and the speed of Internet activities.

5.1 Jurisdiction

Jurisdiction concerns the authority of the court and state organs to decide on legal cases. Each state has the sovereign right to exercise jurisdiction over its territory. With the high level of transborder exchange, the Internet poses challenges to the traditional concept of jurisdiction. For example, e-commerce transactions often involve numerous jurisdictions. In cybercrime, similarly, it is often difficult to establish jurisdiction. The effectiveness of international Internet regulations will depend substantially on addressing the question of jurisdiction.

Status of mechanisms concerning jurisdiction

There is a wide range of rules and practices addressing the question of jurisdiction for specific public policy issues, including contract law and law concerning data protection, defamation, intellectual property and taxation.

The regulation of jurisdiction impacts on the following Internet public policy issues: cybercrime, freedom of expression, privacy, copyright, arbitration, intermediaries, e-commerce, consumer protection, taxation, and content policy, among others.

Areas of ambiguity, unresolved issues and possible gaps in dealing with jurisdiction

An implementation gap exists in the lack of mechanisms that will ensure efficient and cost-effective approaches to jurisdictional aspects of Internet public policy issues, especially since addressing jurisdictional aspects in traditional juridical procedures typically takes a long time and requires considerable human and financial resources. This implementation gap could particularly affect individuals and institutions that do not have the financial and human resources needed for long and expensive litigation processes. The fact that the Internet is cross-border in nature, while jurisdictions are mostly national, produces tensions which indicate a policy gap. However, this does not necessarily imply a need for full harmonization of legislation.

A capacity gap exists in the insufficient institutional and expert capacity of national court and judicial systems to deal with the jurisdiction aspects of Internet public policy issues.

5.2 Arbitration and other forms of dispute resolution

Arbitration is an important dispute resolution mechanism. Typically, it is established by a private contract with parties agreeing to settle any future disputes through arbitration. In comparison with traditional courts, arbitration offers the following advantages: higher flexibility, lower expenses, faster resolution of disputes, and the easier enforcement of arbitration awards. There is a longstanding tradition of international arbitration within the business sector.

Status of mechanisms concerning arbitration and other forms of dispute resolution

The main international instrument is the United Nations Commission on International Trade Law (UNCITRAL) Model Law on International Commercial Arbitration (1985, with amendments as adopted in 2006). The enforcement of arbitration awards is regulated by the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards. The most substantial example of the dispute resolution mechanism in online matters is the Universal Domain-Name Dispute-Resolution Policy (UDRP), which is accredited by ICANN as the primary dispute resolution procedure. The WIPO Arbitration and Mediation Center provides services for UDRP. Since the introduction of the UDRP in 1999, the Center has handled 22,500 cases. In addition, there are four other UDRP service providers, The Asian Domain Name Dispute Resolution Centre, the National Arbitration Forum of the United States, the Czech Arbitration Court Arbitration Center for Internet Disputes for the European Union, and the Arab Center for Domain Name Dispute Resolution.

Self-regulatory models complement traditional forms of arbitration. For instance, the Better Business Bureau's BBBonline is an example of an online consumer complaint management system.

Areas of ambiguity, unresolved issues and possible gaps in dealing with arbitration

There is a knowledge gap in research concerning the applicability of arbitration and other dispute resolution mechanisms to Internet public policy issues. It would be useful to explore the applicability of successful features of UDRP to other fields of online disputes (e.g. defamation).

5.3 Copyright

Copyright protects the expression of an idea when it is materialised in various forms, such as a book, CD, or computer file. Copyright is based on two main elements: the protection of authors' rights and protection of the public interest. Striking the right balance between these two elements is one of the main challenges for copyright both on the Internet and in more traditional contexts.

Status of mechanisms concerning copyright

The principal governance approach to copyright online consists of the application of existing measures for the protection and enforcement of copyright, with adjustments geared toward addressing the challenges and opportunities raised by the digital environment. This approach has been followed in the main international instruments, including the WTO's Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS), and the WIPO Conventions, including the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, negotiated to address new and emerging copyright issues in the digital environment.

Areas of ambiguity, unresolved issues and possible gaps in dealing with copyright

Mechanisms for ensuring an appropriate balance between the protection of authors' rights and protection of the public interest are needed.

Some commentators/ submissions to the WGEC correspondence group have called for the consideration of non-IPR issues as part of copyright policy (*e.g.* risk of infringement of other human rights while protecting copyright including privacy and freedom of expression).

5.4 Trademark

The most significant issue concerning trademarks on the Internet concerns the registration of domain names. In the early phase of Internet development, the registration of domain names was done on a first come, first served basis. This led to cybersquatting, the practice of registering names of companies and selling them later at a higher price. Trademark holders reacted by introducing mechanisms for stricter protection of trademark through ICANN's policy development processes, in the form of the Uniform Domain Name Dispute Resolution Policy (UDRP), which was approved in 2000. The New gTLD Program included a fundamental policy recommendation that the introduction of new gTLDs had to be done in a way that protects the rights of others, and additional mechanisms have been developed for trademark protection as it relates to domain names.

Status of governance mechanisms for trademark

WIPO's Madrid and Paris Conventions provide the basis for trademark protection on the Internet. In 2001, WIPO adopted *Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet.*

The Uniform Dispute Resolution Procedures (UDRP) is the primary dispute resolution procedure. The UDRP is stipulated in advance as a dispute resolution mechanism in all contracts involving the registration of gTLDs (e.g. .com, .edu, .org, .net) and for some ccTLDs. Its unique aspect is that arbitration awards are applied directly through changes in the DNS without resorting to enforcement of trademark protection through national courts.

ICANN has the following mechanisms concerning trademark disputes: The Trademark Clearing House under ICANN's new gTLD program authenticates information from rights holders and provides this information to registries and registrars. The Uniform Rapid System (URS) mechanism allows trademark holders to combat clear-cut cases of abuse. The Post-Delegation Dispute Resolution Procedure (PDDRP) allows rights holders to assert rights against registry operators where a registry's operation or use of a domain leads to or supports trademark infringement.

Areas of ambiguity, unresolved issues and possible gaps in dealing with trademark

One submission to the WGEC/correspondence group indicated a potential policy gap in dealing with competing claims for protection of trademarks and other internationally important names (e.g. the example of '.amazon' as a new gTLD).

The question of protection of names of international organisations remains unresolved.

5.5 Labour law

The Internet has changed the way in which many people work. It has facilitated teleworking as well as a higher level of temporary and short-term workers. The Internet has provided a technical infrastructure for the outsourcing of ICT and other services such as call centres and data processing units. These developments pose a new challenge for traditional labour policies and regulations.

Status of governance mechanisms for labour law

Policy processes in this field are at an early stage. The most applicable convention for the use of temporary agency workers in the Internet sector is International Labour Organization' s ILO Convention 181 on Private Recruitment Agencies (1997), together with Supplementary Recommendation 188. In 2001, ILO produced the report *Life at Work in the Information Economy*.

Labour law is most directly related to the following Internet policy issues: the Internet of Things, child safety, privacy, disability rights, jurisdiction, intermediaries, access, the digital divide, education, and multilingualism.

Areas of ambiguity, unresolved issues and possible gaps in dealing with labour law

There is a knowledge gap in available data and research on the impact of the Internet on labour-related public policy issues.

5.6 Intermediaries

Intermediaries play a vital role in ensuring Internet functionality. ISPs are the critical online intermediaries who connect end-users to the Internet. Their role often provides the most direct mechanism for governments to enforce legal rules concerning the Internet. This is why many governments have concentrated their law enforcement efforts on ISPs. The increasing influence and role of intermediaries has led to debates about their liability and about related juridical challenges in the cross-border Internet environment. One of the main issues in this context concerns whether there should be intermediary liability for content created or transmitted by those who make use of an intermediary's services.

Status of governance mechanisms for intermediaries

The role of intermediaries is mainly regulated at national level. However, there are a few international mechanisms. The OECD includes the role of intermediaries among its 14 principles for Internet policy-making. In 2011, the OECD Council adopted *Recommendation of the Council on Principles for Internet Policy Making*, which asserts that appropriate limitations of liability for Internet intermediaries "play an important role in promoting innovation and creativity, the free flow of information, and in providing incentives for co-operation among stakeholders."[37] There are regional Internet service provider associations around the world. The European Court of Justice focuses on the role of intermediaries in the Court Case of Delfi vs Estonia (10 October 2013).

UNESCO has launched a research on Internet intermediaries' role in fostering freedom online which examines how their actions may either protect or jeopardize end user rights to free expression and privacy, in line with the *UN Guiding Principles on Business and Human Rights*. Intermediary reliability is also often discussed at the Internet Governance Forum.

Areas of ambiguity, unresolved issues and possible gaps in dealing with intermediaries

There is a knowledge gap in data and research on the role of intermediaries in dealing with international Internet public policy issues. Some submissions to the WGEC/correspondence group indicated a potential policy gap in the lack of legal and other mechanisms for addressing role of intermediaries in the cross-border Internet transactions.

6. Economic cluster

Economic activities have been among the main engines of Internet growth, and contribute to overall economic and social development. This cluster includes e-commerce, which is a longstanding issue on the Internet, alongside new issues such as virtual currency that have emerged more recently.

6.1 E-commerce

There are various definitions of e-commerce. According to the WTO, e-commerce is: "the production, distribution, marketing, sale, or delivery of goods and services by electronic

[37] OECD, 2014, *Recommendation of the Council on Principles for Internet Policy Making*, See Annex *Communique on Principles for Internet Policy Making.*

means".[38] The one adopted by OECD and the Partnership on Measuring ICT for Development deviates from that used by the WTO, stating that e-commerce is "the sale or purchase of goods or services conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders; payment and delivery are not considered." [39]

There are different types of e-commerce depending on the parties involved; business-to-business (B2B), business-to-consumer (B2C), consumer-to-consumer (C2C) and business-to-government (B2G). The object of the transaction may be a physical good as well as intangible product or service.

As UNCTAD foresaw in 1999, e-commerce has become a major engine for trade and development on a global scale. For enterprises, it offers potential benefits in the form of enhanced participation in international value chains, increased market access and reach, and improved internal and market efficiency, as well as lower transaction costs. For consumers, it often means greater consumer choice and lower prices.[40]

E-commerce has also been one of the main engines promoting the growth of the Internet over the past fifteen years.

Status of mechanisms concerning e-commerce

E-commerce is covered by the WTO General Agreement on Trade in Services (GATS). The WTO Work Programme on Electronic Commerce is also undertaken through the Councils on Trade-related Aspects of Intellectual Property Rights, Trade in Goods and Trade in Services, as well as through the Trade and Development Committee. More specifically, the WTO established the Work Programme for Electronic Commerce in 1998, though activity in this area has been limited; the main achievement has been a moratorium on taxes levied on international "electronic transmissions" which has been renewed at every subsequent WTO Ministerial Meeting since 1998. The analysis of existing mechanisms also indicates a shift of policy focus from global (WTO) to regional level, with many regional trade agreements also addressing e-commerce.

UNCTAD acts as lead facilitator, together with International Trade Center (ITC) and Universal Postal Union (UPU) of the WSIS Action Line on e-business.[41] It provides capacity

---

[38] WTO, 1998, *Work Programme on electronic commerce*, available at https://www.wto.org/english/tratop_e/ecom_e/wkprog_e.ht (accessed 9 April 2015).

[39] *OECD Science, Technology and Industry Scoreboard 2013 Innovation for Growth* (OECD publication), p. 226.

[40] UNCTAD, *Information Economy Report 2015: Unlocking the Potential of E-Commerce for Developing Countries*, p.2.

[41] E-business is a broader term than e-commerce. It includes e-commerce but also covers other processes such as inventory management, product development, risk management, finance, knowledge management and human

building in the area of ICTs and Law Reform and advisory services to governments to review their national ICT policies. Its Information Economy Reports monitor global trends in ICTs as they affect the economic development of developing countries. The *Information Economy Report 2015: Unlocking the Potential of E-commerce for Developing Countries* includes an initiative to map cyber legislation related to e-transactions, consumer protection, data protection and privacy, and cybercrime. E-commerce is also addressed in the OECD's 1999 *Guidelines on Consumer Protection in the Context of Electronic Commerce*, which are currently being revised.

Many national cyberlaws have been influenced by the legislative standards prepared by the United Nations Commission on International Trade Law (UNCITRAL). Its Model Law on Electronic Commerce (1996) has been enacted in more than 60 jurisdictions. Twenty-nine jurisdictions have based their legislation on the UNCITRAL's Model Law on Electronic Signature (2001). The United Nations Convention on the Use of Electronic Communications in International Contracts (ECC, 2005) has been signed by 18 States and acceded to or ratified by six.

Following table illustrates the share of economies which have adopted legislation which is of relevance to e-commerce.

Table 2: Share of economies with e-commerce laws, 2014, by region.

	Countries (number)	E-transaction laws (%)	Consumer protection laws (%)	Privacy and data protection laws (%)	Cybercrime laws (%)
Developed economies	42	97.6	85.7	97.6	83.3
Africa	54	46.3	33.3	38.9	40.7
Asia and Oceania	48	72.9	37.5	29.2	56.3
Latin America and the Caribbean	33	81.8	54.5	48.5	63.6
Transition economies	17	100.0	11.8	88.2	70.6
All economies	194	74.7	47.4	55.2	60.3

Source: *UNCTAD, 2015.*

resources as well as production of ICT goods and services. The adoption of e-business practices has also grown rapidly over the past ten years.

Areas of ambiguity, unresolved issues and possible gaps in dealing with e-commerce

Many consumers and enterprises hesitate to engage in e-commerce because of a lack of trust in online transactions. Concerns may be related to losing payments, having personal data compromised or misused, or to the risk of the goods or services purchased not meeting the quality expected. Lack of trust and poor legal frameworks are significant barriers to online shopping. Security and trust are therefore crucial to creating an environment conducive to e-commerce. In order to address these issues, national governments need to adopt relevant laws in areas such as e-signature, consumer protection, data protection and privacy, and cybercrime.

The extent to which countries have adopted national cyberlaws and have enacted them to facilitate security and trust in online transactions varies considerably. There are significant gaps in international compatibility and interoperability of legislation in this area. Harmonization of laws and the need to align them with international legal instruments is important to facilitate cross-border e-commerce.[42]

6.2 E-money and virtual currencies

A legal definition of electronic money is included in Article 1 of European Parliament and Council Directive 2000/46/EC. The definition states that "electronic money shall mean monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; (iii) accepted as means of payment by undertakings other than the issuer."[43] E-money is usually associated with so-called smart cards issued by companies such as Mondex and Visa Cash or stored in the servers of specific providers. E-money is integrated in the existing banking and monetary system.

Unlike e-money, virtual currencies are not directly linked to the traditional financial system. The issuance of decentralised virtual currencies is akin to printing money without the control of a central banking institution. Bitcoin is the best known decentralised virtual currency.

---

[42] Ibid.

[43] Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0046&from=EN (accessed 9 April 2015).

.

Status of mechanisms concerning e-money and virtual currencies

Decentralised virtual currencies are at an early stage of both national and international policy developments. At international level, one potential venue for addressing decentralised virtual currencies and e-money issues is the Committee on Payments and Market Infrastructures (CPMI) of the Bank for International Settlements (BIS). E-money and virtual currencies are also considered in a number of international networks that deal with money laundering, such as the Financial Action Task Force (FATF).

Areas of ambiguity, unresolved issues and possible gaps in dealing with e-money and virtual currencies

There is a knowledge gap in the research and understanding of the impact virtual currencies on Internet public policy issues related to e-commerce, taxation, and consumer protection among others. The review also indicates a lack of international coordination of policy approaches to e-money and virtual currencies.

6.3 Consumer protection

Consumer protection has evolved since the emergence of the Internet from a primarily national to an increasingly international as well as national public policy issue. In the past, consumers rarely needed international protection. They bought locally and therefore needed local consumer protection. With e-commerce, an increasing number of transactions take place across international borders. Consumer protection is essential in ensuring trust as one of the main preconditions for the successful development of e-commerce.

Status of mechanisms concerning consumer protection

The OECD has adopted three important mechanisms for consumer protection on the Internet: the 1999 *Guidelines for Consumer Protection in the Context of Electronic commerce*, the 2003 *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders*, and the 2007 *Recommendation on Consumer Dispute Resolution and Redress*. The main principles in these instruments have served as the basis for OECD members and some non-member countries to adapt existing consumer protection or adopt new and specific e-commerce frameworks. The principles have also been adopted by business associations, including the International Chamber of Commerce (ICC) and the Council of Better Business Bureaus. Work is ongoing in the OECD to update the guidelines on Consumer Protection in the context of Electronic Commerce, to address new and ongoing consumer challenges in e-commerce.

A number of private associations and NGOs also address consumer e-commerce protection, including Consumers International, the International Consumer Protection and Enforcement Network, and Consumer Reports WebWatch.

Consumer protection is most directly related to the following Internet policy issues: the Internet of Things, cybersecurity, digital signatures, cybercrime, data protection, jurisdiction, intermediaries, access, cloud computing (*i.e.*, consumer protection is related to ensuring trust of consumers in cloud computing services), content policy, copyright, and multilingualism.

Areas of ambiguity, unresolved issues and possible gaps in dealing with consumer protection

Consumer protection has been raised in connection with the possible misuse of domain names such as .lawyer and .doctor. If registration for these domains is not regulated (*e.g.* if it does not require a law or medical degree), it could be misused, to the detriment of Internet users and consumers. ICANN is currently addressing advice that it has received from its Governmental Advisory Committee on the establishment of safeguards for strings such as these. In addition, ICANN's New gTLD Program has a Public Interest Commitment requirement, with a dispute resolution process available if a registry fails to meet its public interest commitments.

Some delegations have raised consumer protection issues under the WTO E-commerce Work Programme. However, the mechanisms analysed appear to indicate that consumer interests could be introduced and discussed more systematically in international bodies dealing with relevant aspects of Internet policy issues (*e.g*. ICANN, WTO). This capacity gap is particularly noticeable in the case of consumers from developing countries.

Consumer protection laws vary between countries. At global level, there seems to be a gap in the harmonisation of relevant legislation.

On the policy level, there is insufficient coordination among various policy initiatives and processes in addressing online aspects of consumer protection.

6.4 Taxation

The question of taxation on the Internet has become particularly relevant since the financial crisis in 2008. For many governments, the growing volume of economic activity on the Internet raises concerns about the potential loss of tax revenue. Others see opportunities for increased fiscal revenue.

Status of governance mechanisms concerning taxation

In 1998, the OECD adopted the *Ottawa Taxation Framework Conditions*, which specify that the same principles that governments apply to taxation of conventional commerce should equally apply to e-commerce.[44] The Ottawa conclusions remain the main governance

[44] OECD, 2001, *Taxation and Electronic Commerce; Implementing the Ottawa Taxation Framework Conditions* (Paris, OECD Publication).

mechanism in the field of taxation on the Internet. They introduced a "destination" principle that specifies that taxes should be collected on the consumer side of transactions. In 2012, the OECD began to address taxation issues related to the digital economy.

Taxation is most directly related to the following Internet policy issues: the Internet of Things, arbitration, jurisdiction, intermediaries, e-commerce, e-payment, access, cloud computing, and content policy.

Areas of ambiguity, unresolved issues and possible gaps in dealing with taxation

The analysis of existing mechanisms points to a knowledge gap on data and research about taxation on the Internet. One submission to the WGEC/correspondence group indicated a lack of international bodies where best practices could be shared and necessary coordination ensured. Another submission indicated a lack of both global treaties and soft law regarding the taxation issues related to the digital economy. However, there is no consensus on this issue.

7. Development cluster

Development considerations are cross-cutting. They affect all other clusters, ranging from telecommunications infrastructure in developing countries, through capacity-building for cybersecurity protection, to questions of multilingualism as a way to broaden use of the Internet in the developing world. Development issues concerning the Internet are contextualised within an ecosystem which includes technical development, human development and the development of governance.

The development aspects of the Internet became prominent in the United Nations at the World Summit on the Information Society (WSIS), held in two phases in Geneva in December 2003 and in Tunis in November 2005. The commitments made in the four WSIS outcomes documents - *the Geneva Declaration of Principles, Geneva Plan of Action, Tunis Commitment* and *Tunis Agenda for the Information Society* - set out a path for the international community to bridge the digital divide and to leverage greater developmental value of the ICTs. The potential of the Internet in social and economic development has been well demonstrated in the implementation of and follow-up to the WSIS outcomes.

This cluster highlights three topics that are concerned with Internet in the context of development; access, the digital divide, and capacity development. The Internet is also having fast-changing impacts on ICT applications in development, but these fall outside the remit of this report.

7.1 Access

Access to the Internet and through it, to information and knowledge, is widely considered vital for the economic and social development in the modern societies. For developing countries, access involves a wide range of technical, financial, institutional, policy and capability issues. Improved Internet access in developing countries contributes to bridging the digital divide, but other factors such as enabling legal and regulatory environment, the availability and affordability of applications and services and adequate capacity to use them are also important in achieving this.

The vast majority of access finance comes from the private sector. The roll-out of mobile broadband technology and the maximizing of local traffic through independent Internet Exchange Points (IXPs) have become priorities in terms of improving access to infrastructure, reducing local connectivity costs and enhancing the quality and affordability of Internet services. They have also contributed towards developing the expertise and capacity of local technical communities.

Status of mechanisms concerning access

Access issues are addressed in international mechanisms such as those arising from the WSIS, the work of the World Bank and other international agencies, the Broadband Commission for Digital Development, the ITU's Telecommunication Department Sector and its relevant Study Groups, and elsewhere. Access has also been the most prominent issue in IGF deliberations. In the Internet Governance Forum, it has been addressed from different angles including technical infrastructure, disabilities, and capacity development.

Access is most directly related to the following Internet policy issues: telecommunication, infrastructure, technical standards, net neutrality, cybersecurity, freedom of expression, disability rights, women's rights online, copyright, intermediaries, consumer protection, labour law, capacity development, the digital divide, education, cultural diversity, multilingualism, and global public good.

Areas of ambiguity, unresolved issues and possible gaps in dealing with access

While there have been considerable improvements in global connectivity and access to the Internet in the past decade, more than half the world's population remains unconnected to the Internet. There is a substantial gap both between and within countries in terms of quality of connectivity as measured by speed, bandwidth and costs. There is also a gap in terms of users' capacity to take advantage of what networks and services can offer.

In addition, there are weaknesses in the monitoring and measurement of access. In particular, this applies to the measurements of the impacts that the Internet has on social and economic

development. Strengthening the statistical measurement and monitoring mechanisms would be vital to better understand the developments in access.

On a policy level, there is a lack of coordination among various international organisations and networks dealing with the access issue. In addition, there is lack of intersectoral approach from technical, legal, economic, educational and other relevant public policy perspectives.

According to one comment to this report, there is a lack of consensus regarding the steps to take to reduce the costs of international connectivity for developing countries.

7.2 The digital divide

The digital divide can be defined as a gap between those who, for technical, political, social, or economic reasons, have access and capabilities to use ICT/Internet, and those who do not. Various views have been put forward about the size and relevance of the digital divide. Digital divide(s) exist at different levels: within countries and between countries, between rural and urban populations, between the old and the young, as well as between women and men.

Status of mechanisms concerning digital divide

The WSIS was driven by the objective to bridge the digital divide. The outcomes of its first phase (2003) were particularly concerned with this issue. Since WSIS, the reports of the United Nations Secretary-General on *progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels,* and the subsequent Economic and Social Council and General Assembly resolutions, have discussed the various aspects of digital divides in the context of the implementation of WSIS outcomes. The digital divide is also monitored by the ITU's ICT Development Index and WEF's Networked Readiness Index.

The digital divide is most directly related to the following Internet policy issues: telecommunication infrastructure, freedom of expression, disability rights, women's rights online, copyright, intermediaries, e-commerce, capacity development, access, cloud computing, education, multilingualism, and global public good.

Areas of ambiguity, unresolved issues and possible gaps in dealing with the digital divide

While the digital divide in terms of access to basic Internet services has been considerably reduced in recent ten years, other divides, for example in terms of network capabilities and quality may have widened. For instance, despite improvements in infrastructure, there is a growing gap in the quality of connectivity if measured by speed and bandwidth. This poses challenges to policy makers.

Data concerning the statistical measurement of Internet are of variable quality. Weaknesses in statistical measurement are accentuated by the rapid changes taking place in ICT technology and markets. This implementation gap leads to a knowledge gap on the impact of various policy actions and mechanisms on the nature and level of digital divide.

On the policy level, the digital divide was not included in the form of measurable targets in the *Millennium Development Goals*, though quantitative targets were agreed at WSIS. Also, to date, the digital divide has not been fully integrated in the reflections on the new post-2015 development agenda.

One submission to the report stated that there is a lack of sufficient funding to deal adequately with the issue of digital divide.

7.3 Capacity development

Capacity development is essential for the faster growth of the Internet in developing countries and the reduction of digital divides. It includes development of both institutional capacities (an enabling environment for Internet growth, policy-making, implementation), and individual competencies (*e.g.* literacy, ICT skills, cybersecurity culture).

Support for capacity building includes ensuring that citizens, especially young people, have access to and acquire media and information literacy (MIL) competencies, including through the school curriculum. These competencies enable understanding of the context of ICTs, Internet and digital-related matters as well as technical skills. Ensuring access to MIL can inform and empower citizens to become more critical users of the Internet, and better equipped to take full advantage of the economic, social and other opportunities offered by the Internet.

Status of mechanisms concerning capacity development

Capacity development features prominently in the WSIS final documents and subsequent policy developments. It has been undertaken by a wide range of organisations including UNESCO, the ITU, the Internet Society, DiploFoundation, and the Association for Progressive Communications, the European Summer School on Internet Governance, the South School in Latin America and the African School on Internet Governance. Also ICANN and other Internet organizations such as RIRs provide capacity development.

UNESCO, in particular, works on the capacity development in the area of media and information literacy.

Capacity development is most directly related to the following Internet policy issues: telecommunication infrastructure, technical standards, cybersecurity, spam, freedom of

expression, disability rights, women's rights online, intermediaries, e-commerce, labour law, access, education, and global public good.

Areas of ambiguity, unresolved issues and possible gaps in dealing with capacity development

The mechanisms analysed appear to indicate the existence of gaps in terms of the lack of the focus on institutional capacity development. Most programmes are related to individual training and skill improvement of individual experts. There is a need for more comprehensive and sustainable capacity development at institutional level. The review also indicated an implementation gap mainly related to the lack of available funds and other resources for ensuring sustainable capacity development initiatives.

8. Sociocultural cluster

Internet public policy issues in the sociocultural cluster reflect the broad impact of the Internet on the social and cultural life of modern society. The cluster includes a wide range of issues, from content, promotion of cultural diversity, and multilingualism to online education and the status of the Internet as a global public good.

8.1 Content policy

The Internet has represented an historical advance in the development and dissemination of content. It has not only enabled much faster and more efficient dissemination of content, but also expanded the range of content, including content relevant to local needs, and opened up the opportunity for users of the Internet to become content creators.

There have been significant improvements in access to basic infrastructure in the range of content available and in the linguistic diversity of that content. However, there remain challenges concerning the availability of locally relevant content and content in minority languages.

Policies that are relevant to content are largely defined, adopted and implemented at national level. Therefore, they are bound to a certain cultural context. Content policy is often seen through the prism of rights, including access to information and freedom of expression. Content policy is also related to discussions concerning net neutrality and the possibility that traffic management could provide a mechanism for *de facto* content policy (by slowing access to particular websites). In the field of child protection, web standards have been used to help parents filter access to inappropriate content for their children.

Status of mechanisms concerning content policy

Content policy is an intersectoral issue. The question of jurisdiction is often raised in deciding which court or national authority has the right to address specific issues of content policy. One of a few international instruments that address content is the Council of Europe's Additional Protocol to the Convention on Cybercrime. It defines racist and xenophobic material as "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors."[45]

Courts are becoming more active in this field. The European Court of Justice ruling on the right to be forgotten (May, 2014) affects content policy by requesting Google to filter certain types of content for users in EU countries.

Freedom of expression, access to information and copyright are often related to content policy, including issues such as filtering. Other Internet policy issues that are related to content policy include data protection, e-commerce, access, cloud computing, education, cultural diversity, and multilingualism.

Areas of ambiguity, unresolved issues and possible gaps in dealing with content policy

The definition of online content which breaches the boundaries of acceptability is one of the most complex and contentious issues in Internet policy. The issue requires interpretation of the limitations to freedom of expression set out in Article 19(3) of the International Covenant on Civil and Political Rights. Problems also arise from the relationship between local cultural and religious specificities of content policy and the principle of ubiquitous access to any content on the Internet.

The tension between national regulation and the cross-border nature of the Internet has led to many different challenges. A case in France in 2001, for example, concerned problems arising from the availability of Nazi-related materials on the Yahoo.com auction website. While exhibition and sale of these materials was prohibited in French law, their display and sale were not illegal in the United States where the website was hosted. The French court judgement required Yahoo! to identify and block access from France using geo-location software.

---

[45] Council of Europe, 2003, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Article 2.

8.2 Cultural diversity

Cultural diversity is promoted as one of the key principles of global cooperation. The Internet has been perceived both as a means for reinforcing global cultural diversity, and as a means for undermining it, with the risk of cultural homogenisation.

Status of mechanisms concerning cultural diversity

The main instruments in this field are adopted by UNESCO: the Universal Declaration on Cultural Diversity (2001), the Charter of the Preservation of Digital Heritage (2003), and the Convention on the Protection and promotion of the Diversity of Cultural Expressions.

Cultural diversity is most directly related to the following Internet policy issues: web standards, net neutrality, child safety, freedom of expression, disability rights, women's rights online, copyright, intermediaries, consumer protection, access, the digital divide, education, content policy, and multilingualism.

Areas of ambiguity, unresolved issues and possible gaps in dealing with cultural diversity

There are differing views concerning whether the Internet contributes to cultural diversification and encourages homogenisation. This is difficult to measure. There has been research on what is sometimes called the "filter bubble", in other words, the tendency of Internet users to stay within the comfort zone of content that they think of interest to them, encouraged by companies which tailor services to our personal tastes.

The mechanisms analysed indicate a possible policy gap in bringing Internet policy into the mainstream of existing international mechanisms dealing with cultural diversity. In addition, there is a knowledge gap on the ways and means of protecting online artifacts as part of our global cultural heritage.

8.3 Multilingualism

Multilingualism is an important aspect of the promotion and development of cultural diversity on the Internet. If the Internet is to be used by all within society, content needs to be accessible in more languages.

Status of mechanisms concerning multilingualism

UNESCO, the lead international organization on this issue, supports the inclusion of new languages in the digital world, the creation and dissemination of content in local languages on the Internet and mass communication channels, and encourages multilingual access to digital resources in cyberspace. It adopted a *Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace in 2003*.

UNESCO is also the lead facilitator of the WSIS Action Line C8 on Cultural diversity and identity, linguistic diversity and local content.

One of the early initiatives related to the multilingual use of computers was undertaken by the Unicode Consortium – a non-profit institution that develops standards to facilitate the use of character sets for different languages.

As far as technical development to promote multilingualism on the Internet is concerned, IETF and ICANN have taken steps to enable the use of Internationalised Domain Names (IDNs) by developing the underlying protocols and enabling country code and generic IDN top level domains (TLDs) in the root zone respectively. IDNs facilitate the use of domain names written in Chinese, Arabic, and other non-Latin scripts.

Multilingualism is most directly related to the following Internet policy issues: web standards, the DNS, digital signatures, freedom of expression, copyright, trademark, consumer protection, access, the digital divide, education, cultural diversity, and content policy.

Areas of ambiguity, unresolved issues and possible gaps in dealing with multilingualism

In spite of efforts to create technical possibilities and to encourage the development of multilingual content, many languages are still not yet at all or widely present on the Internet. Quantitative measurement of the availability of content in different languages and on the access and usage of that content is very challenging, and therefore statistical data on content creation and publication is still weak. One may conclude an implementation gap in this regard.[46]

Apart from the considerable progress made in developing a multilingual Internet, the analysis indicates the need to have the multilingual aspect more structurally integrated in the process of developing future Internet standards and technical solutions.

8.4 Online education

The Internet has enabled new possibilities for education. Numerous e-learning, online learning, and distance learning initiatives have been introduced, using the Internet as a medium for the delivery of courses.

[46] See Partnership on Measuring ICT for Development, 2014, *Final WSIS Targets Review: Achievements, Challenges and the Way Forward* (Geneva, ITU Publication), p. 271-314.

Status of mechanisms concerning online education

Traditionally, education policy has been developed by national institutions. The accreditation of educational institutions, the recognition of qualifications, and quality assurance are all governed at national level. However, cross-border online education requires the development of new governance approaches. Many international initiatives aim at filling the governance gap, especially in areas such as quality assurance and the recognition of academic degrees.

As the main international organisation dealing with education, UNESCO facilitates the implementation of WSIS commitments on e-learning under the WSIS Action line C7, ICT Applications. It has, among others carried out work on Open Educational Resources (OER) and on the use of ICTs in education management information systems (EMIS) and created an *ICT Competency Framework for Teachers*.

National and Regional Research and Education Networks (NRENs and RENs) support the needs of research and education communities, including improving the e-learning, within countries and regions.

At the WTO, in the context of the GATS process, there was a policy debate on whether education should be expected to form a global trade regulation as a government-provided service. The EU has developed a regulatory framework with the European Credit Transfer and Accumulation System (ECTS). The Asia-Pacific region has introduced its own regional model for the exchange of students and a related credit system – the University Mobility in Asia and the Pacific (UMAP) programme.

Online education is most directly related to the following Internet policy issues: access, web standards, freedom of expression, data protection, intermediaries, content policy, and global public good.

Areas of ambiguity, unresolved issues and possible gaps in dealing with online education

The mechanisms analysed suggest the existence of a knowledge gap in understanding how online learning will affect international aspects of educational policy (accreditation, standardisation, quality control).

There are also insufficient international mechanisms for exchanging best practices and coordination among institutions dealing with policy aspects of online education.

8.5 Internet as global public good

The Internet has been often referred to as a "global public good". The validity of this term depends on the application and understanding of the concept of “global public goods” and the context in which it is used.

In any event, it is clear that the Internet provides many valuable services to the global public. It is considered to be a global resource that many people believe should be governed in the global public interest.

Many aspects of the Internet are related to the idea of the Internet as a global public good, including: access to the Internet infrastructure, protection of knowledge developed through Internet interaction, protection of public and open technical standards, and access to online education and educational material online.

Status of mechanisms concerning the Internet as a global public good

There are no major international initiatives focusing on the Internet as a global public good.

The view that the Internet is a global resource that should be governed in the global public interest has been put forward at a regional level in the Council of Europe's Committee of Ministers' *recommendation to member states on the protection and promotion of the universality, integrity and openness of the Internet* (2011). The Council of Europe's expert report on *ICANN's procedures and policies in the light of human rights, fundamental freedoms, and democratic values* suggests the following public interest objectives: respect for human rights, fundamental freedoms and democratic values; linguistic and cultural diversity; and care for vulnerable persons and groups. ICANN itself may only address the issue of human rights as bounded by its mission.

The concept of the Internet as a global public good is most directly related to the following Internet policy issues: web standards, net neutrality, cybersecurity, freedom of expression, disability rights, copyright, labour law, capacity development, access, cloud computing, education, cultural diversity, and multilingualism.

Areas of ambiguity, unresolved issues and possible gaps in dealing with global public good

The mechanisms analysed appear to indicate the existence of a knowledge gap in research and data on the global public good aspects of the Internet developments, including sharing of experience from other policy fields such as environmental protection.

8.6 Internet and ethics

The pervasiveness of the Internet and its ability to bring together people from different backgrounds, cultures and societies has raised a variety of ethical considerations. Content that may be considered obscene or inappropriate in one culture may be perfectly acceptable in another. Ethical considerations apply to all areas of Internet governance from the research and development of technical infrastructure, software and applications, to their manufacturing, commerce and distribution, from the development and execution of policies and practises to the responsibility of users themselves for their online behaviour.

Ethics should be considered in an inter-disciplinary manner together with possible principles or objectives to be reached. According to UNESCO, the Internet should help advance respect for and realization of human rights and universal values. Possible discrepancies between this vision and real-world situations raise issues for ethical considerations, which include human rights, peace, equity, and justice.

Status of governance mechanisms concerning Internet and ethics

The WSIS outcome documents raised the issue area of ethics in the context of the Information Society. Facilitation of the WSIS Action Line on Ethical dimensions of the Information Society (C8) was entrusted to UNESCO which works on this topic through it Management of Social Transformations (MOST) programme, Information for All Programme (IFAP) and World Commission on the Ethics of Science, Technology and Knowledge (COMEST). Ethics are considered one of the four *Key Stones to foster inclusive Knowledge Societies* in a UNESCO draft study bearing the title published in 2015.

The ethics of the Information Society have been discussed in a number of non-binding documents, declarations and recommendations developed through the work of Intergovernmental agencies and others. For example, the *NETmundial Multistakeholder Statement* of the Global Multistakeholder Meeting on Future of Internet Governance, held in São Paulo, Brazil, in April 2014, set recommendations for common principles and shared values in the area of Internet governance. Discussions have taken place in the Internet Governance Forum concerning the ethical dimensions of the Internet governance and the potential for soft regulation relating to these.

Organizations and private entities involved in Internet governance have their own codes of ethics. A number of professional codes of practice also provide voluntary standards and guidelines.

Areas of ambiguity, unresolved issues and possible gaps in dealing with Internet and ethics

The rapid progress of technology and the emergency of innovations such as big data and Internet of Things have raised new ethical challenges which need to be considered in a comprehensive manner.

There is a need for greater awareness of the ethical implications of the Internet, its use and its impacts on individuals and societies. In parallel, there is a need to build national capacity to support stakeholders at all levels. The exchange of information concerning regional practices, lessons and insights and the broadening of the international debate in this field are also important goals. Finally, research is needed in a number of areas including emerging technologies and the ethical implications around the values and choices they provide, and the relationship between technology and socio-cultural value systems.

9. Concluding remarks

The review identified 41 international public policy issues pertaining to the Internet, which have been organized in seven broad clusters. The first cluster – infrastructure and standardisation – deals with technical issues related to the proper functioning of the Internet (*e.g.* the domain name system, the root zone, and net neutrality). The other six clusters concern broader policy issues which are relevant in both offline and online environments.

Thanks to the pervasiveness of Internet and its impact in almost every aspect of society, any attempt to list or categorize the issues pertaining to it must be indicative rather than comprehensive. The issues have complex interrelationships, and their relevance varies depending on different contexts and perspectives. Several issues can be regarded as primarily cross-cutting. Nor are these issues static. The rapid pace of technological change on and around the Internet, and its impact on the way the Internet is perceived, deployed and addressed in wider societal contexts means that any attempt to list and review the issues around it will be a product of its time. A mapping of Internet public policy issues can, at best, provide only a snapshot of current reality.

The pervasiveness of the Internet is also reflected in the abundance of mechanisms which address Internet public policy issues. The review followed the approach adopted in the earlier phase of work (by the Correspondence Group), according to which any type of entity, agreement or non-binding document, process or programme that was relevant to the Internet could be counted as a mechanism. All of those mechanisms that were included therefore address one or more of the issues that have been identified in the report. As with issues, the list of mechanisms is non-exhaustive and could be updated over time as old mechanisms seize to exist and new mechanisms appear.

The mandate for the work in this report included assessment of the mechanisms and how effectively they are addressing the issues with which they are concerned. Criteria were identified to conduct a rudimentary assessment, covering the type of mechanism concerned, its function, participation arrangements, and the extent to which the mechanism uses an intersectoral approach in its activities or in relation to a given topic. These criteria yielded information on the mechanism, but it would be too simplistic to make value judgements on that basis alone. It was noted that assessing the extent to which the mechanisms are capable of addressing the issues effectively, of solving imminent problems or of producing significant outcomes is difficult against criteria that could be applied to all mechanisms with sufficient similarity. Opportunities for participation, for example, may be determined by several factors, including the rules and regulations of an organization, security measures, physical limitations, the nature and the scope of the topic under consideration, awareness and capacity to participate.

Overall, the review demonstrated considerable diversity of ways in which the mechanisms identified are governed, depending on their nature and the ways in which they have been

established and evolved. Most of the mechanisms identified within the infrastructure and standardisation cluster have developed incrementally through a process of collaborative endeavour often described as "rough consensus and running code". From a technical standpoint, the most elaborate group of mechanisms includes those concerned with managing critical Internet resources (Internet protocol numbers, the domain name system and the root zone) and related technical and web standards. Most of these mechanisms have emerged as practical solutions to specific problems (*e.g.* how to manage domain names).

The assessment of possible gaps in the mechanisms identified is naturally subject to interpretation, depending on the perception of what constitutes "a gap" in the first place. The international debate on Internet governance demonstrates divergent views, in this respect. Some regard the ability of governments to participate on an equal footing and/or to make sovereign decisions as the criteria against which all mechanisms should be assessed, and conclude that in this respect crucial gaps exist, in particular, in the management of critical resources (domain name system and root zone). Others do not consider these criteria necessarily applicable for assessing gaps, believing that current arrangements have functioned in practice and enabled the Internet to evolve.

Technological development has changed existing issues and introduced new ones – including net neutrality, convergence, cloud computing and the Internet of Things - while public policy considerations have been accentuated by the rapid expansion which has occurred in access to and use of the Internet. It is only natural that the development of appropriate mechanisms concerning emerging issues, including regulatory mechanisms, is at an early stage in many cases. There is often no global consensus concerning whether existing regulations are sufficient or a new international legal instrument is required to deal with a specific Internet public policy issue.

The tension between the transborder nature of the Internet, on the one hand, and predominantly national regulations that govern public policy issues pertaining to the Internet, on the other, results into challenges for the implementation of regulation. Making diverse legislation more interoperable and aligning national laws with existing international instruments helps in overcoming these challenges. At the international level, this calls for strengthened cooperation, capacity building and sharing of information and best practices.

Another challenge concerns how to ensure a holistic approach, aimed at protecting public interests in both regulatory and technical aspects of the Internet. The development of legal frameworks on online privacy and data protection, for example, must include, among others, human rights, trade, standardization and security perspectives. The more pronounced the societal impacts of Internet technical issues become, the more important also becomes the need to include public policy considerations in technical decision making such as standard setting. Ensuring a holistic approach requires that appropriate mechanisms are in place and that participation in these is sufficiently comprehensive and diverse. Attempts to address these challenges have begun in both Internet organizations and the wider policy community.

While "offline" legal principles and approaches remain relevant in the online world, their application to the specific cases in the "online world" is not always straightforward. This may be due to the lack of clear legal frameworks, institutional capacity, resources and/or expertise. Policy responses cannot always keep pace with technical developments, which may create situations where Internet public policy issues do not have established mechanisms through with they can be properly addressed. In cybercrime, this gap was filled relatively quickly through the adoption of predominantly regional legal instruments. In other areas, such as data protection and consumer protection, international cooperation is gradually taking shape.

In conclusion, the review illustrates that Internet governance is a broad and complex field, which includes a large number of different, often elaborate mechanisms that address the issues within their diverse mandates. However, gaps of several types are also apparent when it comes to addressing specific issues. They relate, among other things, to the legal frameworks and/or mechanisms to implement regulations in order to address a specific issue; intersectoral coverage of a specific issue; skills and competencies; capacity building and information sharing; opportunities to participate; and availability of data, research and awareness concerning a specific issue or set of issues. The review indicates that improvements could be made in respect of these gaps. At international level, strengthened coordination and collaboration across stakeholder groups will be critical in efforts to bridge them.

A number of different initiatives have been undertaken to map or frame public policy issues pertaining to the Internet, each addressing the issues from their specific standpoint.[47] Whatever the chosen methodology is, continuous updating and research are required to keep any map of such a diverse and dynamic sphere as the Internet up to date with new developments. Analysis of the interrelations between issues is particularly useful. Given the complex nature of Internet governance and the need to enhance public information and understanding, it is desirable that mapping efforts should continue and that there should be increased information sharing between them in order to enhance their substance and avoid overlaps. It may also be possible to bring some of these initiatives together to provide a holistic global monitoring and analysis framework, which would contribute to the objective of an Internet that serves the public interest of all.

[47] Some of these were discussed in a workshop No. 95 of the IGF 2014 meeting in Istanbul. The summary of the workshop is available at http://www.intgovforum.org/cms/wks2014/index.php/proposal/view_public/95 (accessed 9 April 2015).

Annex: Comparison between list of issues identified by the Correspondence Group and issues presented in database

N°	Correspondence Group	List of Issues from Database	N°
1	Technical standards	Technical standards	2.2
		Web standards	2.3
2	CIR management (including IP addresses, DNS and the root zone)	Communications Infrastructure	2.1
		Internet Protocol Numbers	2.4
		Domain Name System	2.5
		Root zone	2.6
		Critical information infrastructure	3.3
3	Fostering a sustainable and innovative Internet for future generations		
4	Internet and security	Cybersecurity	3.1
		Cyberconflict	3.4
		Spam	3.7
5	Cybercrime	Cybercrime	3.2
6	Child online protection	Child safety online	3.5
7	Privacy and data protection	Cloud computing	2.8
		Encryption	3.6
		Privacy and data protection	4.2
8	Human rights	Freedom of expression	4.1
		Rights of people with disabilities on the Internet	4.3
		Women's rights online	4.4
9	Competition policy, liberalization, privatization and regulations		
10	E-commerce and trade	Digital signature	3.8
		E-Commerce	6.1
		E-Money and virtual currency	6.2
		Taxation	6.4
11	Intermediary liability	Arbitration	5.2
12	Consumer rights	Consumer protection	6.3
13	Intellectual property rights (IPR)	Copyright	5.3
		Trademark	5.4
14	ICT4D		
15	Capacity building	Online Education	8.4
		Capacity development	7.3
16	Access, accessibility and affordability	Access	7.1
		Digital divide	7.2
17	Net Neutrality	Net neutrality	2.7

18	Multilingualism and cultural diversity on the internet	Content policy	8.1
		Cultural diversity	8.2
		Multilingualism	8.3
19	Legal & regulatory frameworks	Labour law	5.5
		Intermediaries	5.6
20	Applicable jurisdiction, cross border coordination	Jurisdiction	5.1
21	Media convergence	Convergence	2.9
22	Internet uses and applications		
23	Stakeholders and governance		
24	Emerging issues		
25	Other Issues		
		Internet of Things	2.1
		Internet as global public good	8.5
		Internet and ethics	8.6

Selective bibliography

Bradner, S. (1996), *The Internet Standards Process - Revision 3. Request for Comments: 2026*. IETF Network Working Group. Available at https://www.ietf.org/rfc/rfc2026.txt (accessed 4 April 2015).

Council of Europe (2010). *Declaration of the Committee of Ministers on network neutrality*. 29 September.

Economic and Social Council (2014), *Assessment of the progress made in the implementation of and follow-up to the outcomes of the Information Society*. Resolution E/2014/27. 16 July.

Economic and Social Council (2014), *CSTD working group to examine the mandate of WSIS regarding enhanced cooperation as contained in the Tunis Agenda (Working Group on Enhanced Cooperation, WGEC). Report of the Chair of the Working Group*. E/CN.16/2014/CRP.3. 8 May.

Global Multistakeholder Meeting on Future of Internet Governance (2014). *NETmundial Multistakeholder Statement*. Available at http://netmundial.br/netmundial-multistakeholder-statement/ (accessed 13 April 2015).

Shirey, R. (2007), IETF *Internet Security Glossary (Version 2. Request for Comments: 4949*. IETF Network Working Group. Available at https://datatracker.ietf.org/doc/rfc4949 (accessed 9 April 2015).

ILO (2001). *The World Employment Report 2001: Life at Work in the Information Economy*. United Nations publication. Geneva.

International Chamber of Commerce (2001). *GUIDEC -General Usage for International Digitally Ensured Commerce (version II)*. Paris.

ITU (2014). *Final WSIS Targets Review: Achievements, Challenges and the Way Forward*. United Nations publication. Geneva.

ITU (2012) International Telecommunication Regulations, Final Acts of the World Conference on International Telecommunications. Dubai.

ITU (2010). Definitions and terminology relating to building confidence and security in the use of information and communication technologies. Plenipotentiary Resolution 181, Guadalajara.

ITU (2005). *WSIS Outcome Documents: Geneva 2003-Tunis 2005*. United Nations publication. Geneva.

ITU (2005). *ITU Internet Reports 2005: The Internet of Things.* United Nations publication. Geneva.

ITU (2008). Recommendation ITU-T, X.1205, *Series X: Data Networks, Open System Communications and Security Telecommunication Security, Overview of cybersecurity*. United Nations publications. Geneva.

Lin, H. (2012). *Cyber conflict and international humanitarian law*, International Review of the Red Cross, Volume 94, number 886, Summer 2012, p. 515. Available at https://www.icrc.org/eng/assets/files/review/2012/irrc-886-lin.pdf (accessed 9 April 2015).

OECD (2014). Recommendation of the Council on Principles for Internet Policy Making. Paris.

OECD (2013).*OECD Science, Technology and Innovation Scoreboard 2013 Innovation for Growth.* OECD Publishing.

OECD (2012). *Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy.* OECD publication.

OECD (2011). *The Protection of Children Online: Risks Faced by Children Online and Policies to ProtectThem*. OECD Digital Economy Papers, No. 179. OECD Publishing.

OECD (2001). *Taxation and Electronic Commerce; Implementing the Ottawa Taxation Framework Condition*. OECD Publication, Paris.

OSCE (2013). *Initial Set of OSCE Confidence Building Measures to reduce the risk of conflict stemming from the use of Information and Communication Technologies* (PC.DEC/1106). 3 December.

Symantec (2014). 2013 Trends, Volume 19, *Internet Security Threat Report 2014*, available at http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_ v19_21291018.en-us.pdf (accessed 9 April 2015).

Tan, J. (2008). *A Comparative Study of the APEC Privacy Framework- A New Voice in the Data Protection Dialogue?* Asian Journal of Comparative Law. Volume 3, Issue 1, ISSN (Online) 1932-0205, Year: April 2008.

UNCTAD (2015). *Information Economy Report 2015 - Unlocking the Potential of E-commerce for Developing Countries.* United Nations. New York and Geneva.

UNCTAD (2013). *Information Economy Report 2013: The Cloud Economy and Developing Countries*. United Nations. New York and Geneva.

UNESCO (2015), *Keystones to foster inclusive Knowledge Societies, Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet.* Draft Study. Paris.

UNESCO (2003), *Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace*, available at http://portal.unesco.org/en/ev.php-URL_ID=17717&URL_DO=DO_TOPIC&URL_SECTION=201.html (accessed on 14 April 2015).

UNESCO (2012), *Global survey on Internet privacy and freedom of expression*. UNESCO Series on Internet Freedom. UNESCO. Paris.

UNESCO (2011). *Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*. Paris.

UNODC (2013). *Comprehensive Study on Cybercrime*. United Nations. New York, 2013.

United Nations General Assembly (2014). *The right to privacy in the digital age* (Resolution A/RES/69/166). 18 December.

United Nations General Assembly (2013). *The right to privacy in the digital age* (Resolution A/RES/68/167). 18 December.

United Nations General Assembly (2013), *Information and communications technologies for development* (Resolution A/RES/68/198). 20 December.

United Nations General Assembly (2013*). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98).* 24 June.

United Nations General Assembly (2012), *Information and communications technologies for development* (Resolution A/RES/67/195*)* 5 February.

United Nations Human Rights Council (2014). *The promotion, protection, and enjoyment of human rights on the Internet*. Resolution A/HRC/RES/26/13. 26 June.

WIPO and the Assembly of the Paris Union for the Protection of Industrial Property (2001). *Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet*. Thirty Sixth Series of Meetings of the Assemblies of the Member States of WIPO September 24 to October 3, 2001.

WTO (1998). *Work programme on electronic commerce.* Available at https://www.wto.org/english/tratop_e/ecom_e/wkprog_e.ht (accessed 9 April 2015).