Intersessional Panel of the Commission on Science and Technology for Development

Geneva, Switzerland
26-28 November

The mapping of international Internet public policy issues

ADVANCED VERSION

Prepared by the CSTD Secretariat 21 November 2014

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 in response to the recommendation of the United Nations Economic and Social Council[1]. The work was carried out in August–November 2014, and has been supported by independent expert advice and comments from peer reviewers[2].

The review builds on earlier work initiated by the CSTD Working Group on Enhanced Cooperation (WGEC). It further continues the work towards creating 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. This information has been included in a database created for this purpose. The report draws from the findings of the database, reviewing each of the international public policy issues in the same order as they are presented in the database.

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 UN 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, through seeking, compiling and reviewing inputs from all Member States and all other stakeholders, and to make recommendations on how to fully implement this mandate. The group was composed of 22 Member States and 20 invitees from all other stakeholders, namely, 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 start a mapping exercise. 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,*

[1] E/RES/2014/27 from 16 July, 2014.

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

(c) Identify the status of mechanisms, if any, whether they are addressing the issues,

(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 on 30 April-2 May 2014. In this meeting, the work of the CG was presented in the spreadsheet. The WGEC took note of the presentation of the CG's work and suggested that the spreadsheet should be considered as a living document.

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´*.[4] 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.

In consequence, in its resolution E/RES/2014/27, from 16 July 2014 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, whether they are addressing the issue 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 progress made in the implementation of the outcomes of the World Summit, to be prepared for the consideration by the Commission at its eighteenth session.´

This report present the work that was carried out to continue the work initiated in WGEC, in compliance with the ECOSOC resolution E/RES/2014/27.

---

[3]Chairman's summary of the second meeting of the WGEC. Available at http://unctad.org/meetings/en/SessionalDocuments/WGEC_2013_Chairmans_summary_en.pdf

[4] Chairman' s summary, E/CN.16/2014/CRP. Available at http://unctad.org/meetings/en/SessionalDocuments/ecn162014crp3_en.pdf

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.

The data that was initially gathered through the CG was reviewed and reorganised. Adjustments were made in the listing of issues to allow more detailed information on the relevant mechanisms.[5] 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
- sociocultural

It should be noted, however, that this classification in seven broad clusters is only indicative. Its objective is to assist readers in their understanding of the complex field of Internet public policy. Most of the issues are intersectoral, and consequently, they could also be classified in other clusters, depending on the context.

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

As part of the review, the mechanisms identified by the CG have been examined: the mechanisms that were retained from the CG's work are marked as OLD in the database; NEW mechanisms were added, where appropriate; some general mechanisms identified by WGEC (e.g. mentioning the name of the organisation) were supplemented by more specific mechanisms describing the activities of the organisations mentioned (e.g. consultation mechanisms, conventions, events); some mechanisms were dropped because they did not fulfill the criterion of being 'international'.

Altogether, the database has 643 mechanisms, classified in 40 issues, in 7 clusters. These consist of organisations, policy processes, and policy instruments, among others. Several mechanisms, such as the Internet Governance Forum (IGF), appear under more than one issue. The list of mechanisms is not exhaustive, given the breadth and constant evolution of the field of Internet public policy.

[5] 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)6
   - 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. For example, the IGF falls into this category.
   - 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 are the possibilities 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 (submit 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 such as human rights, trade, standardisation, security? The following criteria are used:
   - Exclusive coverage in, or mandate for, one policy community (e.g. technical, legal, economic).
   - Ad hoc intersectoral coordination.

[6] These are referred to as ´Instruments´ in the database.

- Structured coordination across policy sectors (e.g. coordination groups).
- Full intersectoral coverage of IG 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 those issues that have been identified. The initial gaps identified by the CG are listed briefly in the database along with their originators. Other possible gaps were identified while the work continued. They are summarised in the database. This report gives a brief account of some of the possible gaps identified in the database.

Through a few iterations of analysis, the review identified four major groups of gaps, named as knowledge gaps (insufficient data and 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 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 discussed. Consequently, following this introduction, Chapters 2–8 present the main findings of the review. Each chapter presents the analysis of the issue included in the respective cluster, the key findings on the mechanisms addressing the issue, and the status of those mechanisms. An attempt is also made to identify potential gaps in those mechanisms. Chapter 9 presents the main conclusions, describes the main challenges encountered in the course of the work, and discusses potential areas for continuation.

2. Infrastructure and standardisation cluster

The infrastructure and standardisation cluster includes three types of issues that ensure the core functionality of the Internet. First is the telecommunication infrastructure that facilitates digital communication. Second are 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. The third group of issues such as net neutrality, cloud computing, and the Internet of Things deal with the policy aspects that may shape and determine future Internet developments.

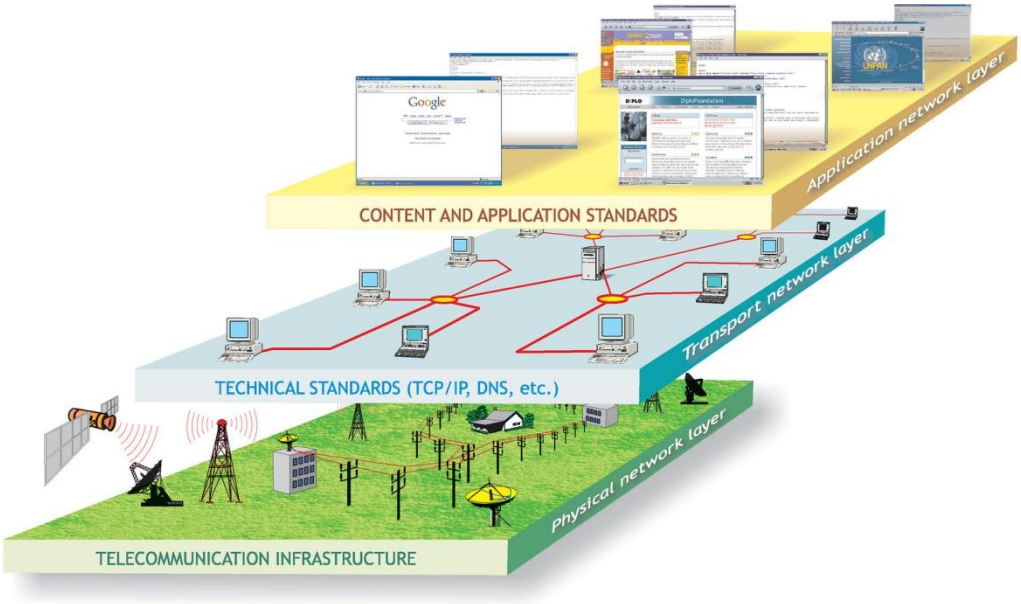

Figure 1. This illustration summarises the three main layers of relevance for the infrastructure and standardisation cluster (Source: DiploFoundation graphic library).

2.1 Telecommunication infrastructure

The telecommunication infrastructure includes telephone wires, fibre-optic cables, satellites, microwaves, and wireless links. Fibre-optic cables, with 95 per cent of the international Internet traffic, are the core segment of the telecommunication infrastructure. Technological development and innovation are likely to introduce new telecommunication solutions, such as telecom drones and balloons. The governance of the telecommunication infrastructure has an important impact on how the Internet is developed and used.

Status of governance mechanisms for the telecommunication infrastructure

The governance mechanisms for telecommunication infrastructure are managed by a wide variety of public and private organisations. The main international organisation involved in

the international facilitation of telecommunication is the International Telecommunication Union (ITU), which provides a global framework for the coordination of national telecommunication systems. The ITU also plays an important role in the allocation of the radio spectrum, which is relevant to wireless Internet communication. The World Trade Organization (WTO) has been the key player in the liberalisation of telecommunication markets worldwide. The most prominent professional and technical actors include the Institute of Electrical and Electronic Engineers (IEEE), which develops standards such as the WiFi standard (IEEE 802.11b), and the Groupe Speciale Mobile Association (GSMA) which develops standards for mobile networks.

With a growing demand to develop local content and keep Internet traffic closer to users (e.g. Internet Exchange Points), the question of global interconnection among a wide range of networks will be important for the future growth of the Internet. Governance of the telecommunication infrastructure is closely related to net neutrality, in particular when it comes to the prioritisation of Internet traffic. A reliable telecommunication infrastructure, in particular fibre-optic cables, facilitates wider access to the Internet in developing countries.

How the telecommunication infrastructure is governed has implications for other Internet policy issues including: technical standards, the Internet of Things, cybersecurity, data protection, jurisdiction, cloud computing, and intermediary liability.

Possible gaps in dealing with the telecommunication infrastructure

The mechanisms analysed appear to indicate the existence of a gap in terms of the implementation of existing policies and rules. This possible gap is related to insufficient guidelines, practices and capacity building aimed at reducing ambiguity in the regulatory border zone between telecommunication and Internet public policy rules.

For example, when Internet service providers (ISPs) filter traffic in order to detect spam and viruses, they could interfere with the content on the Internet. Should such a practice be considered as a telecommunication issue, or is it an Internet public policy issue?

2.2 Technical standards

The Internet's architecture is based on a set of technical standards. These standards influence – among others – 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). The most important technical standard is TCP/IP (Transmission Control Protocol/Internet Protocol), which is in the basis of the Internet infrastructure.

Status of governance mechanisms for technical standards

The Internet Architecture Board (IAB) oversees the technical and engineering development of the Internet. Most Internet technical standards are set by the Internet Engineering Task Force (IETF) in the form of Request for Comments (RFC). Both the IAB and the IETF have their institutional home within the Internet Society (ISOC).

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.'[7] The IETF makes decisions through an open and consensus-based process which is often described as 'rough consensus and running code'.

As the basis of the Internet infrastructure, Internet technical standards have an impact on other Internet public policy issues.

For example, RFC 6409 sets a standard separating mail submission from the message relay. This standard has direct relevance for all operators of e-mail systems, including intermediaries who have, for example, flexibility to set their own rules in handling the security of e-mail communication.

Internet technical standards on e-mail authentication can influence the level of anonymity on the Internet with a direct impact on cybersecurity and cybercrime (anonymity increases the complexity of identifying perpetuators of cyber attacks), freedom of expression (in some cases anonymity can ensure 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.

Possible gaps in dealing with technical standards

A possible policy gap relates to insufficient coverage of non-technical aspects (e.g. human rights, competition policy, and security) in the process of developing technical standards.

There appears to be a gap as far as participation in the development of standards is concerned. Even though participation is open to all stakeholders, some submissions to the WGEC/correspondence group have noted the need for more involvement from the part of governments and for example from consumer representatives.

[7] Available at https://www.ietf.org/rfc/rfc2026.txt

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 growth of the 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).

Status of governance mechanisms for web standards

Web standards are set by the World Wide Web Consortium (W3C), headed by the inventor of HTML, Tim Berners-Lee. They are developed through the elaborate process which aims to reach consensus, and they are published in the format of W3C Recommendations.

W3C standards have high economic relevance, which triggered the active participation of Internet industry and software developers in the development of the W3C standards. They can have direct impact on many policy areas on the Internet, including multilingual content on the Internet, access for people with disabilities, and e-commerce.

Possible gaps in dealing with web standards

As with the Internet technical standards, the possible gap in the development of web standards is related to the coverage of non-technical aspects (e.g. human rights, competition policy, and security). Web standards have an even stronger impact on non-technical aspects since, more so than technical standards, they shape the way the Internet is accessed and used.

2.4 Internet protocol numbers

IP numbers are unique numeric addresses that are used by all computers and other devices connected to the Internet. Two computers connected to the Internet cannot have the same IP number. This makes IP numbers a potentially scarce resource. The depletion of IP numbers (under IP version 4) accelerated with the fast growth of Internet-enabled devices (such as mobile phones, personal organisers, home appliances). IP version 6 (IPv6) was introduced in order to overcome the limited pool of IP numbers. The transition to IPv6 has been progressing slower than necessary to effectively address the shortage of IP numbers within the IPv4 arrangement.

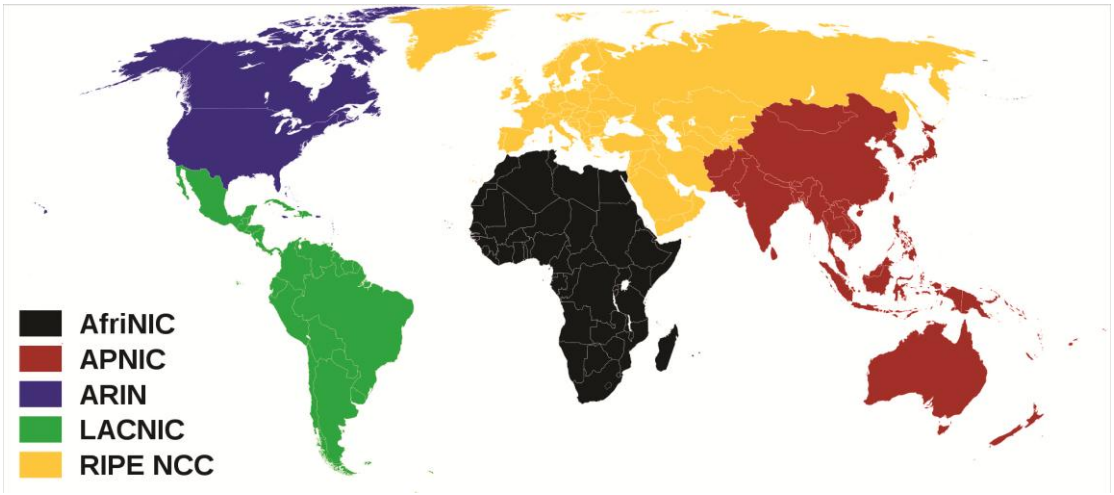

Figure 2. Geographic coverage of the five regional Internet registries (Source: Wikimedia)

Status of governance mechanisms for IP numbers

The governance of IP numbers is coordinated by IANA (the Internet Assigned Numbers Authority – a subsidiary of ICANN, the Internet Corporation for Assigned Names and Numbers). IANA distributes blocks of IP numbers to the five regional Internet registries (RIRs). RIRs distribute IP numbers to local Internet registries (LIRs) and national Internet registries, which in turn distribute IP numbers to smaller ISPs, companies, and individuals further down the ladder. The Number Resource Organisation (NRO) coordinates the work of the five RIRs. The Address Supporting Organisation (ASO) reviews and develops recommendations on 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.

Possible gaps in dealing with IP numbers

The mechanisms analysed appear to indicate the existence of a knowledge gap related to awareness, data, and research on transition to IPv6. In addition, some submissions to the WGEC/correspondence group point to a possible policy gap in mechanisms for coordination and faster facilitation of the transition from IPv4 to IPv6.

2.5 Domain name system

The DNS is often defined as the Internet 'address book', which provides mapping of the host name to its IP address. It takes language-based Internet addresses and converts them to the numeric IP addresses. Internet-connected devices use IP numbers to communicate with one

another. The DNS is hierarchically organised with the top level consisting of root servers and top-level domain (TLD) servers, and under these a large number of DNS servers located around the world which. The DNS ensures that accurate information may be found about any address at any time, from anywhere, with confidence as to its veracity.

The DNS includes three types of TLDs: generic (gTLD), country code (ccTLD), and sponsored (sTLD). gTLDs include domains that can be obtained by anyone (.com, .info, .net, and .org). Since 2014 many other gTLDs have been added like .pub, .بازار (bazaar), .rentals, .ngo, or .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 governance mechanisms for the DNS

The organization and management of DNS is based on the Internet standards and recommendations (Requests for Comments adopted by the IETF). For country domains, the most relevant is the ISO 3166 standard, 'Codes for the representation of names of countries and their subdivisions'. ICANN provides overall coordination of the DNS by establishing agreements and accrediting registries and registrars. For each gTLD there is one **registry** that maintains an address list. For example, the .com gTLD is managed by Verisign. Final users purchase specific 'second level' domain names (the part in front of the dot in each TLD) from **registrars**. ICANN also decides on the introduction of new gTLDs (such as .city, .wine, .christianity).

The policy development function for the DNS is within the Country Code Names Supporting Organisation (CNSO) and the Generic Names Supporting Organization (GNSO) and their councils. The main dispute resolution mechanism for the DNS is the Uniform Domain-Name Dispute-Resolution Policy (UDRP). Since the introduction of the UDRP in 1999, the World Intellectual Property Organization (WIPO) Arbitration and Mediation Center has handled 22 500 cases. In addition to the WIPO Arbitration and Mediation Center, there are four other regional UDRP service providers.

The high policy relevance of the DNS came into sharper public focus with the introduction of the new gTLDs. For example, it opened the policy debate on the right to register the domain '.amazon' with claims from the company Amazon that owns the trademark and from countries in Amazon basin. Another debate has been conducted on the 'closed generic' gTLDs – dictionary words not available for public use; for example, Amazon's application for .book. Some new domains such as '.doctor' or '.lawyer' could run the risk of misleading Internet users should individuals who – for example – do not have necessary medical and/or legal qualifications register under these domains.

Possible gaps in dealing with the DNS

Some submissions to WGEC/correspondence group have suggested that the main policy gap derives from the way coordination of the DNS is designed. The process of changing this was initiated by an announcement made by the US Department of Commerce's National Telecommunications and Information Administration (NTIA) on 14 March 2014 of its intent to transition key internet domain name functions to the global multistakeholder community[8].

Another policy gap that has been referred to in some of the submissions to WGEC/correspondence group has been the status of governments in the current decision-making structure of ICANN. However, there is no consensus on this issue. Whereas some view governments' role through the Government Advisory Council (GAC) insufficient and point out that formally speaking, the role is only advisory, others are of the opinion that in practice, governments play an important role and there are formal procedures in place for cases 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). It ensures the functional integrity of the Internet. It consists of 13 root servers (10 in the USA and one each in Sweden, the Netherlands, and Japan). In addition, there are some 200 copies of the root zone servers around the world (called 'anycast' servers).

Status of governance mechanisms for 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 USA's historical role in the supervision of the root zone and ICANN. On 14 March 2014, the US government announced that it would pass its supervisory function of the root zone to a multistakeholder global entity. The process of transition, including public consultations, is underway.

Possible gaps in dealing with the root zone

Some inputs to WGEC have highlighted the oversight of the IANA function as one of the main policy gaps in the current arrangement for the root zone. However, there is no global consensus on this issue.

[8]http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

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 reality, however, the Internet providers conduct some form of appropriate traffic management (i.e., reasonable differentiation) aimed at avoiding congestion, and delivering a reliable quality of service.

Discussions mainly revolve around defining (in)appropriate and (un)reasonable management and discrimination practices, especially those that are conducted for commercial (e.g. anti-competitive behaviour) or political reasons (e.g. censorship).

Net neutrality is a complex issue which requires careful balancing in order to avoid the implementation of 'solutions' which then turn into problems. Net neutrality has three important aspects: technical (impact on Internet infrastructure), economic (influence on Internet business models), and human rights (possible discrimination in the use of the Internet).

Status of governance mechanisms for net neutrality

Net neutrality features prominently in Internet policy debates at national level in many countries. At regional level, the European Union is leaving the enforcement power concerning net neutrality to the national regulatory authorities and their European association, BEREC (Body of European Regulators of Electronic Communications). The Council of Europe emphasises the human rights perspectives of the issue, and the Committee of Ministers has adopted the Declaration of the Committee of Ministers on Network Neutrality (2010). The OECD approaches the issue from an economic perspective, through hearings related to competition and consumer protection issues.

At international level, net neutrality is mainly discussed at the IGF, especially within its Dynamic Coalition on net neutrality. UNESCO's Internet Universality approach doesn't address net neutrality directly, although it refers to the 'freedom to seek and receive information and ideas through media regardless of frontiers'.[9] A number of Internet principles initiatives by global NGOs, such as the Internet Rights and Principles Coalition, include net neutrality among their fundamental principles (either directly or through a non-discriminatory principle).

Possible gaps in dealing with net neutrality

The analysis of the mechanisms show a knowledge gap related to the lack of data and research on traffic management practices and their effects on quality of service, competition, innovation, investments, and protection of human rights.

---

[9] Available at http://www.un.org/en/documents/udhr/

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

Some submissions to the WGEC/Correspondence Group indicated a lack of a global forum where net neutrality issues can be addressed.

2.8 Cloud computing

Cloud computing has emerged with the major shift of data from personal computers and local servers to servers in the clouds (i.e., huge server farms). The first wave of cloud computing started with the use of online mail servers (Gmail, Yahoo!), social media applications (Facebook, Twitter), and 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 main groups: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The main players in cloud computing are Google, Microsoft, Apple, Amazon, and Facebook, who either already have or plan to develop big server farms.

Status of governance mechanisms for cloud computing

The governance framework for cloud computing can be divided into two parts. On the one hand, laws and regulations adopted by governments, public administrations, and independent regulatory authorities; on the other hand, the contractual agreements entered into between the various providers of the cloud ecosystem and the end users of their services.[10]

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 by 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), and consumer protection in providing services from cloud servers.

Possible gaps in dealing with cloud computing

The analysis of mechanisms shows a knowledge gap related to the lack of data and awareness of the impact of cloud computing on Internet public policy issues. On the policy level there is insufficient intersectoral analysis of the interplay between cloud computing and other related

[10] UNCTAD Information Economy Report 2013, The cloud economy and developing countries, p. 68.

Internet public policy issues: technical infrastructure, data protection, e-commerce, and security, among other policy areas.

2.9 Convergence

The Internet has blurred the difference between telecommunication, broadcasting, information management, and media. Convergence is related 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 governance mechanisms for convergence

Convergence is mainly addressed 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, covering one aspect of convergence: the interplay between traditional and new digital media. Convergence is most directly related to net neutrality, the IoT, the role of intermediaries, e-commerce, consumer protection, and taxation.

Possible gaps in dealing with convergence

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 (IoT)

The IoT refers to the ubiquitous use of Internet-enabled devices ranging from wearables to fridges that communicate directly with a smartphone, and watches that can detect and monitor health. The IoT is also essential for the development of smart cities. The core functionality of the IoT relies on collecting and processing high volume of data in real time.

Status of governance mechanisms for the IoT

The governance of the IoT is at an early stage. However, for instance, the EU has a Task Force on the Internet of Things and it has also been dealt in the IGF Dynamic Coalition of the Internet on 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 will also depend on the creation of a regulatory environment that provides protection for users' rights, including privacy. The first regulatory challenge for the IoT will be how data is

collected and managed. The development of the IoT will depend on the existence of a reliable and effective system for handling data. With the IoT integrated in numerous devices, it is not realistic to have user consent for the use of data whenever this data is provided. The IoT will also depend on the development of technical standards which will facilitate effective communication among different devices.

Possible gaps in dealing with the IoT

The mechanisms analysed appear to indicate that there is a knowledge gap on the impact of the development of the IoT on human rights, 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 cybersecurity as its main umbrella issue, and includes other more specific Internet policy issues.

3.1 Cybersecurity

There is no agreed definition of what cybersecurity is. The broad understanding is that it includes issues related to technical security of networks, national security and security for the general public. It is an umbrella concept covering several areas: cybercrime, critical information infrastructure protection (CIIP), and cyberconflicts. 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 these global cybercrime groups.

Status of governance mechanisms for cybersecurity

At national level, a growing volume of legislation and jurisprudence deals with cybersecurity, with a focus on combating cybercrime and, increasingly, protecting the critical information infrastructure from sabotage and attacks as a result of conflicts and terrorist attacks. At regional levels, more and more organisations are realising the importance of cybersecurity and are working on strategies, recommendations, and conventions, such as the Council of Europe Convention on Cybercrime, the Asia-Pacific Economic Cooperation (APEC) Strategy on Secure Online Space, the EU Cybersecurity Strategy, the OSCE Decision on Confidence-Building measures, and the African Cybersecurity Convention.

At the international level, the UN General Assembly has passed several resolutions on a yearly basis on ‘developments in the field of information and telecommunications in the context of international security’. The ITU has produced a large number of security standards and recommendations. A security on provision was included in the 2012 International Telecommunication Regulations (ITRs). One of the main G8 developments in cybersecurity was establishing 24/7 communication between the cybersecurity centres of member states. 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) and Seoul (2013).

Possible gaps in dealing with cybersecurity

The mechanisms analysed appear to indicate the existence of policy gap in coordination of various cybersecurity initiatives and policy processes. It starts with lack of widely acceptable definition and terminology. The review also shows that there are not many mechanisms for addressing cybersecurity issues in an intersectoral way by involving different professional groups, including: the telecom sector, diplomatic communities, security communities, corporate sector associations, hacker communities (e.g. 'white hats'), and civil society.

3.2 Cybercrime

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

These three aspects of cybercrime exist in various definitions of cybercrime. However, there is no internationally accepted definition of cybercrime.

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

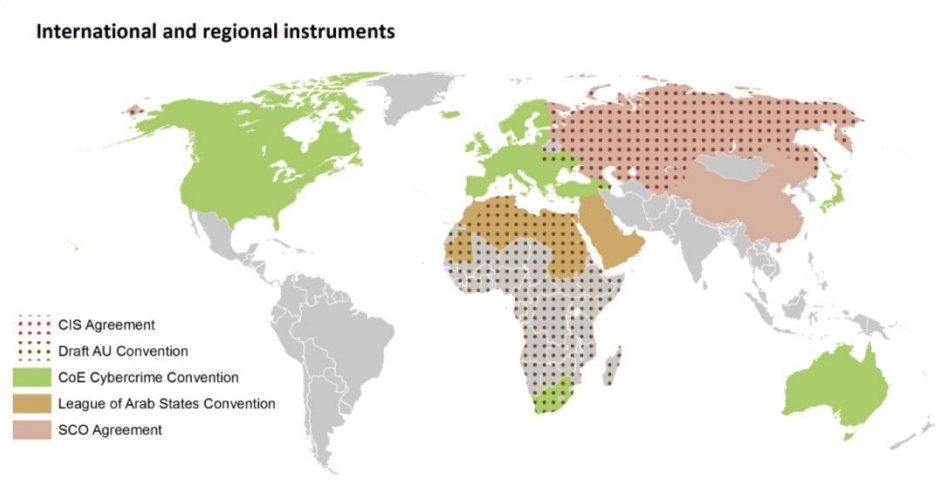

Figure 3: Geographic coverage of the international and regional cybercrime instruments (Source: UNODC Comprehensive Study on Cybercrime – 2013)

Status of governance mechanisms for cybercrime

Combatting cybercrime involves diverse and elaborate mechanisms. According to the UNODC Report *Comprehensive Study on Cybercrime*, 82 countries have signed and/or ratified legally binding cybercrime conventions (Figure 3). The Council of Europe's Budapest Cybercrime Convention (2001) is the oldest cybercrime legal instrument, and it has inspired many other regional and national regulations on cybercrime worldwide. Other regional legal 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).

On the global level, the UNODC is the leading organisation, with a set of international instruments to fight cybercrime. Since cybercrime often involves an organised approach, the UNODC's Convention against Transnational Organised Crime could be used in the fight against cybercrime. Interpol facilitates a global network of 190 national police organisations, which plays a key role in the cross-border investigation of cybercrime. The ITU hosts the World Summit on the Information Society (WSIS) implementation process in cybersecurity, labelled the *ITU Global Security Agenda*.

The Group of Eight (G8) has been addressing cybercrime since 1997 when it established the 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 coordinates network of CERTs. FIRST is the main forum in the technical community for addressing cybersecurity and cybercrime issues. It functions as a network of CERTs, the main bodies for addressing cybersecurity issues at national level.

Many regions have been developing programmes against cybercrime: Asia (Asia-Pacific Economic cooperation), Africa (African Union and UN Economic Commission for Africa), Americas (Organisation of American States), Asia (Shanghai Cooperation Organisation), *etc.*

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, cybersecurity, child safety, encryption, freedom of expression, privacy and data protection, jurisdiction, intermediary responsibility, e-commerce, e-money, access, cloud computing, and content policy.

Possible gaps in dealing with cybercrime

Most gaps are caused by the predominantly transborder nature of cybercrime and the limited international mechanisms available to fight it.

The main knowledge gap is related to a shortage of reliable statistics and data on cybercrime that should trigger, inform, and shape cybercrime policy actions. Policy gaps start with the lack of common or widely accepted definition of cybercrime. In addition, there are no sustainable and effective mechanisms to ensure that policy response to cybercrime follows technological development effectively.

Implementation gaps include the insufficient use of international instruments in criminal matters (mutual assistance agreements, regional, and global arrangements) in cyber matters. Regional and global harmonisation of national cybercrime legislations is lacking as effective mechanisms for cooperation in cybercrime investigation (electronic evidence and cyber forensic).

Institutional and individual capacities in cybercrime field (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 the following aspects: human rights (privacy protection, freedom of expression), and economic (trustworthy environment for e-commerce).

3.3 Critical information infrastructure

The Internet is a critical information infrastructure (CII) in two main aspects. First, the Internet is a communication, economic, and information platform for almost 3 billion Internet users. Second, it provides communication supports for vital systems of modern society, including energy network, water supply, and financial systems, among others. The IETF defines a CII as '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.' As a CII, the Internet must be accessible, secure, and reliable.

Status of governance mechanisms for critical information infrastructure

The CII requires a systematic national approach with enhanced regional and international cooperation networks for information sharing. Its governance involves a wide range of private and public organisations. With more than 80% of the CII owned and/or operated by the private sector, effective governance mechanisms should inter alia involve public-private partnerships. Among international organisations, the ITU has many initiatives related to the CII. This issue is increasingly addressed by various regional organisations (OSCE, ASEAN, Shanghai Cooperation Organisation, OAS, APEC). CERTs are also important governance mechanisms.

Technical infrastructure and cloud servers are essential for the functioning of the Internet as a CII. For example, many businesses and individual users depend on the services provided from the cloud servers, including Facebook and Twitter.

Possible gaps in dealing with the critical information infrastructure

The mechanisms analysed appear to indicate the existence of a knowledge gap in this issue due to insufficient research and lack of awareness of the CII's importance in many countries, starting from the strategic level in the governments. Some submissions to the WGEC/correspondence group also indicated lack of policy mechanisms for addressing CII issues at regional and international levels.

3.4 Cyberconflict

Cyberconflict, often labelled cyberwar, covers three main fields: the conduct of cyberconflict, weapons and disarmament, and the humanitarian aspects of cyberconflict.

Status of governance mechanisms for cyberconflict

With regard to the conduct of cyberconflict, the main question is how to apply the law of war (*e.g.* The Hague Conventions) to cyberspace. For weapons and disarmament, the main governance mechanisms are likely to emerge through adjusting existing disarmament mechanisms. Lastly, humanitarian law rules are related to the applicability of the Geneva conventions to cyberconflict. Several international initiatives are mapping the field of cyberconflict. UNIDIR has provided a classification of cyberconflict, warfare, and weapons. 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.

Possible gaps in dealing with cyberconflict

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

3.5 Child safety online

Most of the issues related to Internet safety are primarily concerned with youth, especially minors. These issues include cyber-bullying, abuse, and sexual exploitation. Close cooperation among key actors – parents, educators, and the community – is essential for developing initiatives to safeguard children in computer-mediated environments.

Status of governance 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 important regional mechanisms which scope reaches beyond Europe. NGOs 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. Particularly active NGOs are the Internet Watch Foundation, the International Centre for Missing and Exploited Children, ECPAT International, Save the Children, and the Child Exploitation and Online Protection Centre. Interpol and Europol are developing implementation mechanisms for the protection of children online.

Possible gaps in dealing with child safety online

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. In recent two years, the question of encryption has come into sharper focus for the global public.

Status of governance mechanisms for encryption

The main international instrument that deals with the encryption is the Wassenaar Agreement, adopted by 41 countries to restrict the export of conventional weapons and 'dual use' technologies to countries at war or considered to be 'pariah states'.

The main question is how to find the right balance between the need to respect the privacy of online communication and the need for governments to monitor some types of communication of relevance for 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.

Possible gaps in dealing with encryption

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.

The encryption standardisation process is limited in term of ensuring the right balance between security and human rights considerations (freedom of expression, protection of privacy).

3.7 Spam

Spam is usually defined as unsolicited e-mail sent to a wide number of Internet users. Spam is mainly used for commercial promotion. Its other uses include social activism, political campaigning, and the distribution of pornographic materials.

Status of governance mechanisms for spam

The most proactive international actor dealing with spam is the OECD, which has established a task force on spam and prepared an anti-spam toolkit. At the regional level, the EU established the Network of Anti-Spam Enforcement Agencies, and APEC prepared a set of consumer guidelines.

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 IGF 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.

Possible gaps in dealing with spam

Spam continues to be a problem in many countries. This may be due to insufficient capacity and technical tools to combat it. The mechanisms analysed appear to also indicate the existence of a gap on the availability of information on spam related issues. There is not enough reliable evidence and data on spam and its cost and 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 governance 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 technical requirements are met. The International Chamber of Commerce (ICC) issued a General Usage in 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.

Possible gaps in dealing with digital signatures

The mechanisms analysed appear to indicate the existence of a policy gap due to a lack of widely accepted standards on digital signatures that will ensure global compatibility, reduce transaction complexity, and 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. Human rights issues are cross-cutting, affecting other Internet public policy areas. For example, freedom of expression and information is directly 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 is a fundamental human right. With the growing relevance of the Internet, the policy debate on freedom of expression has gained online relevance. The main open issue is how to establish the right interplay (or balance) between Article 19 of the Universal Declaration of Human Rights, which grants freedom of expression, and Article 29, which states the limits of freedom of expression for the sake of morality, public order, and general welfare.

Status of governance mechanisms for freedom of expression

Freedom of expression is protected by global instruments, such as the Universal Declaration of Human Rights (Article 29) and the International Covenant on Civil and Political Rights (Article 19), and regional instrument such as the European Convention on Human Rights (Article 10) and the American Convention of Human Rights (Article 13). The main governance mechanism for addressing online freedom of expression is the UN Human Rights Council Resolution on Protection of Freedom of Expression on the Internet (2012). NGOs such as Human Rights Watch, Amnesty International and Freedom House have developed numerous mechanisms for discussing and implementing freedom of expression on the Internet.

Possible gaps in dealing with freedom of expression

The mechanisms analysed appear to indicate the existence of a knowledge gap with regards to data and research on the impact of the technical architecture of the Internet on freedom of expression. For example, freedom of expression is influenced by the degree of anonymity, which in turn depends upon technical features (or solutions). In this context, there may be a policy gap related to the consideration of freedom of expression aspects in the development of technical and web standards.

4.2 Privacy and data protection

Privacy is usually 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 two interrelated public policy issues of relevance for the Internet. Data protection is a legal mechanism that ensures privacy.

Status of governance mechanisms for privacy and data protection

The International Covenant on Civil and Political Rights (ICCPR) is the main international instrument in the privacy protection field. The OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data (1980) is one of the first policy documents in this field which inspired other national and regional online privacy regulations. 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 EU Directive on Data Protection. In Asia, APEC introduced a regional Privacy Framework. In 2013, the UN General Assembly (UNGA) resolved that the UN High Commissioner for Human Rights should deliver a report to the UNGA in 2014 on online privacy and the impacts of surveillance. The UN Human Rights Council discussed that report on online privacy during its September 2014 meeting and it is to be considered by the UNGA in late 2014. The European Court of Justice's judgement on the right to be forgotten introduced a new juridical 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.

Table 1. Data protection principles in international documents (Tan, 2008).[11]

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	✓	✓	✓	✓

11 Tan J (2008) A comparative study of the APEC privacy framework: A new voice in the data protection dialogue? Asian Journal of Comparative Law, 3(1).

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	✓	✓	✓	✓

Possible gaps in dealing with privacy and data protection

A few submissions to the WGEC indicated the lack of international mechanisms to address online aspect of privacy protection.

The mechanisms analysed appear to indicate the existence of policy gaps in insufficient intersectoral approach to privacy and data protection on both regional and global levels.

4.3 Rights of people with disabilities and the Internet

The Internet provides new possibilities 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 of a person with a disability. 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.
- Fostering the availability of hardware and software accessories that increase or substitute the functional capabilities of the person.

Many web applications do not comply with accessibility standards due to a lack of awareness, or the perception that compliance involves complexity and high costs (which is far from today's reality).

Status of governance mechanisms for 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. More specifically, this policy issue is addressed by the IGF Dynamic Coalition on Accessibility and Disability, and other initiatives such as the Internet Society Disability and Special Needs Chapter, and the International Center for Disability Resources on the Internet. International standards in web accessibility are developed by W3C within its Web Accessibility Initiative.

Possible gaps in dealing with rights of people with disabilities

The mechanisms analysed appear to indicate the existence of knowledge gap in data and research on an impact of international Internet public policy issues on the accessibility needs of people with disabilities. In spite of major efforts, there are still policy gaps of the structured coverage of accessibility needs in 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 against bias 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 the online world.

Status of governance mechanisms for women's rights online

The IGF has an active Dynamic Coalition on Gender Rights. However, a significant challenge remains to mainstream the online facets of activities of existing women's rights bodies established in the context of the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW). The UN's Human Rights Council has an important role to play, with active work on various aspects of women's rights overall, as does UN Women as the multilateral women's issues agency.

Possible gaps in dealing with women's rights online

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 aspects of these rights.

5. Legal cluster

Legal Internet public policy issues are cross-cutting, affecting most of the other policy clusters. Most legal issues are already 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 transborder aspects and the speed of Internet activities.

5.1 Jurisdiction

Jurisdiction is 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 as the attribution of online activities could be both difficult to establish and to link to a specific jurisdiction. The effectiveness of international Internet regulations will depend substantially on addressing the question of jurisdiction.

Status of governance mechanisms for jurisdiction

International aspects of jurisdiction are regulated by private international law (referred to as conflict of laws, in the Anglo-Saxon legal system).

There is a wide range of rules and practices addressing the question of jurisdiction for specific public policy issues, such as contract law, data protection, defamation, intellectual property, and taxation. The jurisdiction regulation impacts the following Internet public policy issues: cybercrime, freedom of expression, privacy, copyright, arbitration, intermediaries, e-commerce, consumer protection, taxation, and content policy, among others.

Possible gaps in dealing with jurisdiction

An implementation gap exists in the lack of mechanisms that will ensure efficient and cost-effective dealing with jurisdictional aspects of Internet public policy issues since addressing jurisdictional aspects in traditional juridical procedures typically takes a long time and considerable human/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 and jurisdictions mostly national produces tensions which indicate a policy gap. However, this does not necessarily imply a need for full harmonization of legislation.

The capacity gap exists in insufficient institutional and expert capacity of national court and juridical system to deal with the jurisdiction aspects of Internet public policy issues.

5.2 Arbitration

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

Status of governance mechanisms for arbitration

The main international instrument is the United Nations Commission on International Trade Law (UNCITRAL) 1985 Model Law on International Commercial Arbitration. The enforcement of arbitration awards is regulated by the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards. The most successful example of the use of arbitration 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. 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 EU, and the Arab Center for Domain Name Dispute Resolution.

Possible gaps in dealing with arbitration

There is a knowledge gap in the research on applicability of arbitration mechanisms to Internet public policy issues as well as in sharing experience regarding the relevance 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 remains one of the main challenges for copyright on the Internet.

Status of governance mechanisms for copyright

The main governance approach is that existing copyright regulations could be applied to the Internet with minor adjustments mainly related to 'dematerialising' copyright. This approach

has been followed in the main international instruments, including the WIPO conventions and the WTO's agreement on trade-related aspects of intellectual property rights (TRIPS).

Possible gaps in dealing with copyright

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

There may be too little coverage of non-IPR aspects in the protection of copyright (*e.g.* risk of infringement of other human rights while protecting copyright – *e.g.* privacy and freedom of expression).

5.4 Trademark

The main relevance of trademark on the Internet is the question of 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 stricter protection of trademark in the ICANN governance regime. The recent introduction of the new gTLDs reinvigorated the relevance of trademark for domain names, ICANN, and overall IG.

Status of governance mechanisms for trademark

WIPO's Madrid and Paris conventions provide the basis for trademark protection on the Internet. Another WIPO instrument, the Nairobi Treaty on the Protection of the Olympic Symbol, was in focus during the debate on the special protection of the Olympic name in the registration of new gTLDs.

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 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 as well. 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.

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. cases of '.amazon' as new gTLD).

5.5 Labour law

The Internet has been changing the way in which we work. It has facilitated teleworking as well as a higher level of temporary and short-term workers. The Internet has been 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

The policy processes in this field are in an early stage. The International Labour Organization (ILO) produced the report: *Life at Work in the Information Economy* (2001). Given the major problem of the use of temporary agency workers in the Internet sector, the most applicable convention is ILO Convention 181 on Private Recruitment Agencies (1997) and Supplementary Recommendation 188.

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.

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 key online intermediaries who connect end-users to the Internet. They are often the most direct way for governments to enforce legal rules on the Internet. This is why many states have started concentrating their law enforcement efforts on ISPs. The increasing influence and role of the intermediaries has led to debates about their liability and about related juridical challenges in the cross-border Internet environment. One of the main issues is intermediary liability for content created or transmitted by users or customers using 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. Intermediary reliability is often discussed at the IGF. The OECD includes the role of intermediaries among its 14 principles for Internet policy-making. 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).

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 one of the main engines of Internet growth. They also contribute to the overall economic and social growth of modern society. This cluster includes e-commerce, which is an old issue in terms of Internet history, and some new issues such as virtual currency that started emerging recently.

6.1 E-commerce

There are various definitions of e-commerce.[12] According to the WTO, e-commerce is: 'the production, distribution, marketing, sale, or delivery of goods and services by electronic means'.[13] E-commerce has been one of the main engines promoting the growth of the Internet over the past 15 years.

Status of governance mechanisms for e-commerce

E-commerce is covered by the general WTO treaties, in particular the General Agreement on Trade in Services (GATS), and the Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS). More specifically, the WTO established the Work Programme for Electronic Commerce in 1998, though activity in this area has been limited; the main achievement is a moratorium on taxes levied on international 'electronic transmissions' which is renewed every two years. The WTO's dispute resolution mechanism had USA/Antigua Online Gambling case which is of relevance for e-commerce. Recently, the OECD has started to deal with taxation issues related to the digital economy.

Many consumers and enterprises hesitate to engage in e-commerce due to 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 key barriers to shopping online. Security and trust are thus fundamental for 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. Harmonization of laws is important to facilitate cross-border e-commerce.

---

[12] The OECD and the Partnership on Measuring ICT for Development use a more narrow definition, emphasizing that the placing or receipt of the order needs to be made electronically, but the delivery and payment may be made offline. OECD (2011). *OECD Guide to Measuring the Information Society 2011*. Org. for Economic Cooperation & Development. Paris.

[13] WTO (1998) Work programme on electronic commerce. Available at http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm [accessed 17 February 2014].

Table 2: Potentially applicable bodies of international economic law; adapted from Joel P. Trachtman 'International Economic Law in the Cyber Arena'.

		Potentially Applicable Bodies of International Economic Law				
		Trade in Goods Law	**Government Procurement Law**	**Trade in Services Law**	**Foreign Investment Law**	**Intellectual Property Law**
Means of delivery	**Network**	Inapplicable	Applicable	Applicable	Inapplicable	Possibly applicable
	Movement of equipment	Applicable	Applicable	Inapplicable	Inapplicable	Inapplicable
	Human activity *in situ*	Inapplicable	Applicable	Applicable	Applicable	Possibly applicable

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). Meanwhile, 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. Work is furthermore ongoing in both the OECD and the United Nations to update their guidelines on consumer protection, including with a view to better reflect e-commerce.

Possible gaps in dealing with e-commerce

The analysis of existing mechanisms indicates a shift of policy dynamism from global level (WTO) to regional level with many regional trade agreements also addressing electronic commerce. With regard to the adoption of e-commerce laws at national level, there are still significant gaps in the extent to which key issues are addressed in different countries. Thus, diverse regional and national regulatory responses have started creating a global compatibility gap as far as legislation in the e-commerce field is concerned.[14]

6.2 E-money and virtual currencies

E-money is defined by the Bank for International Settlements (BIS) as 'stored value or prepaid payment mechanisms for executing payments via point-of-sale terminals, direct transfers between two devices, or over open computer networks such as the Internet'. E-money is usually associated with so-called smart cards issued by companies such as Mondex

[14] See UNCTAD (forthcoming), *Information Economy Report 2015: Unlocking the Potential of E-Commerce for Developing Countries* (New York and Geneva: United Nations).

and Visa Cash. E-money is anchored in the existing banking and monetary system (financial legal tender).

Unlike e-money, virtual currencies are not part of a national financial system. Issuing virtual currencies would be akin to printing money without the control of a central banking institution. Bitcoin is the best known virtual currency.

Status of governance mechanisms for e-money and virtual currencies

E-money and virtual currencies are at an early stage of both national and international policy developments. At international level, one potential venue for addressing e-money is the Basel Committee E-Banking Group. E-money and virtual currencies are also in focus for various international networks that deal with money laundering such as the Financial Action Task Force (FATF)

Possible gaps in dealing with e-money and virtual currencies

There is a knowledge gap in the research and understanding of the impact of e-money and 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 been transformed with the Internet from a mainly national to an increasingly international 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 governance mechanisms for consumer protection

The OECD adopted two important mechanisms for consumer protection on the Internet: the 1999 Guidelines for Consumer Protection in the Context of E-commerce and the 2003 Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders. The main principles established by the OECD have been adopted by business associations, including the ICC and the Council of Better Business Bureaus.

ICANN's At large Advisory Committee (ALAC) protects, inter alia, consumer and user of domain names. A number of private associations and NGOs also focus on consumer e-commerce protection, including Consumers International, the International Consumer Protection and Enforcement Network, and Consumer Reports WebWatch.

More specifically, consumer protection was raised in relation to the possible misuse of domain names such as '.lawyer' and '.doctor'. If the registration for these domains is not regulated (*i.e.* if it does not require a law or medical degree), registration under these domains could be misused, which could ultimately harm Internet users and consumers.

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, and multilingualism.

Possible gaps in dealing with consumer protection

The mechanisms analysed appear to indicate the existence of a capacity gap for the representation of consumer interests in international bodies dealing with relevant aspects of Internet policy issues (e.g. ICANN, WTO). This capacity gap is particularly noticeable for consumers from developing countries.

Consumer protection laws vary by country. At global level, there seems to be a gap in the harmonisation of legislation in this domain.

On the policy level, there is insufficient coordination among various policy initiatives and processes in addressing the online aspects of consumer protection. Work is ongoing in both the OECD and the United Nations to update their guidelines on consumer protection, with a view to better reflect e-commerce.

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 activities of the Internet is the first place where they can increase fiscal income.

Status of governance mechanisms for taxation

The OECD has adopted the Ottawa Principles that specify that e-commerce should not have special taxation treatment. E-commerce should be taxed like any other commercial transaction. The Ottawa Principles introduced a 'destination' principle that specifies that taxes should be collected on the consumer's side of transactions. The OECD's Ottawa Principles remain the main governance mechanism in the field of taxation on the Internet.

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.

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.

7. Development cluster

Development considerations are cross-cutting. They affect all other clusters, ranging from telecommunication infrastructure in developing countries for Internet access, via strengthening capacity in developing countries for cybersecurity protection, to questions of multilingualism as a way to broaden use of the Internet in the developing world, to name just a few. The development aspect has been a pillar of the main policy developments in this field, including the World Summit on the Information Society (2003-2005). This cluster highlights three main development issues: access, digital divide, and capacity development.

7.1 Access

Access to the Internet is the key development issue. For developing countries, access involves a wide range of technical, financial, institutional, policy, and skill issues. Improved Internet access in developing countries will reduce the digital divide.

Status of governance mechanisms for access

Access issues are treated in a range of international mechanisms such as WSIS outcomes, the UN Broadband Commission for Digital Development, the ITU's Telecommunication Department Sector and relevant Study Groups, and others. Access has also been the most prominent issue in IGF deliberations. 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.

Possible gaps in dealing with access

The mechanisms analysed appear to indicate the existence of a implementation gap. Monitoring mechanisms are needed for evaluating developments in the field of 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.

7.2 Digital divide

The digital divide can be defined as a rift 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 men and women. In IG, the main focus is on the digital divide between developed and developing countries.

Status of governance mechanisms for the digital divide

The World Summit of the Information Society (WSIS) was driven by the objective to bridge the digital divide. The WSIS outcomes, in particular the Declaration of Principles and the Plan of Action of the Geneva phase of WSIS, talk extensively on the digital divide. Since WSIS, the UN Secretary-General report on WSIS implementation and follow-up and the subsequent ECOSOC resolutions discuss the various aspects of digital divides annually as they review progress made in the implementation of WSIS outcomes. The digital divide (or divides) is also addressed in the context of the other development issues (UN Millennium Development Goals). It is also monitored by the UNDP's Human Development Report and WEF's Networked Readiness Index.

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

Possible gaps in dealing with the digital divide

There is knowledge gap related to the lack of data and research on the impact of various policy actions and mechanisms on the nature and level of digital divide. On the policy level, there is insufficient mainstreaming of digital divide issues in the Millennium Development Goals. Also, to date, the digital divide has not been fully integrated in the reflections on the new post-2015 Development Agenda.

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).

Status of governance mechanisms for capacity development

Capacity development features prominently in the WSIS final documents and subsequent policy developments. It has been performed by wide range of organisations including the ITU, ISOC, DiploFoundation, APC, the European Summer School on Internet Governance, the South School in Latin America and the African School on Internet Governance. Also ICANN provides capacity development.

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.

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. 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

How to define acceptable online content is one the most complex and contentious issues in Internet policy. The problems are based in the gap between, on one hand, the local cultural and religious specificities of content policy and, on the other hand, ubiquitous access to any content on the Internet. This gap has triggered a wide range of reactions. The 2001 Yahoo! case in France addressed the gap between the prohibition under French law to exhibit and sell Nazi-related objects and the possibility for French citizens to access Nazi-related materials at the Yahoo.com auction website, hosted in the USA where the display of such materials is not illegal. The court judgement required Yahoo! to identify and block access from France using geo-location software.

Status of governance mechanisms for content policy

Typically, content policy is addressed at national level. One of a few international instruments that address content is the Council of Europe's Additional Protocol to the Convention on Cybercrime. The Additional Protocol defines hate speech 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'. 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.

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. Content policy is closely linked to discussions on net neutrality and the risk that traffic management could be the back door for *de facto* content policy (slowing down access to a specific website). In the field of child protection, web standards have been used to help parents filter access to inappropriate content for their children. Freedom of expression and access to information are often seen through the prism of content policy. In some cases, protection of copyright could be on the border zone with the filtering of content regardless of its copyright status. The other Internet policy issues that are related to content policy include data protection, e-commerce, access, cloud computing, education, cultural diversity, and multilingualism.

Possible gaps in dealing with content policy

The tension between national regulation and the cross-border nature of the Internet could trigger gaps also in dealing with content policy issues.

8.2 Cultural diversity

Cultural diversity is promoted as one of the key principles of global cooperation.

Status of governance mechanisms for 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.

Possible gaps in dealing with cultural diversity

The mechanisms analysed indicate a possible policy gap in mainstreaming the Internet policy aspects in 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

The multilingual Internet is a pre-condition for the promotion and further development of cultural diversity of the Internet. If the Internet is to be used by wider parts of society, content must be accessible in more languages.

Status of governance mechanisms for multilingualism

Multilingualism is a good example of public-private partnerships. UNESCO is the lead international organisation. 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. ICANN and the IETF took an important step in promoting Internationalised Domain Names (IDNs). IDNs facilitate the use of domain names written in Chinese, Arabic, and other non-Latin alphabets.

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.

Possible gaps in dealing with multilingualism

Apart from the considerable progress made in developing a multilingual Internet, the mechanism analysis indicates the insufficient existence of a structured approach to addressing the multilingual aspect in developing technical and web standards of relevance for the future Internet development.

8.4 Online education

The Internet has opened new possibilities for education. Numerous e-learning, online learning, and distance learning initiatives have been introduced; their main aim is to use the Internet as a medium for the delivery of courses. Traditionally, education has been governed 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.

Status of governance mechanisms for online education

As the main international organisation dealing with education, UNESCO has been also active in online education. 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: web standards, freedom of expression, data protection, intermediaries, content policy, and global public good.

Possible gaps in dealing with online education

The mechanisms analysed appear to indicate 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 Global public good

The Internet provides many valuable services to the global public. It is considered to be a global resource that should be governed in the global public interest. The Council of Europe's 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. 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 technical standards, and access to online education.

Status of governance mechanisms for global public good

There are no major international initiatives focusing on the Internet as a global public good. One of the non-profit initiatives is Creative Commons, aimed at promoting Internet content as a global public good.

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.

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 experience from other policy fields such as environmental protection.

9. Concluding remarks

The review identifies 40 international Internet public policy issues (Internet issues) organised in 7 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 contain traditional policy issues which have been affected to some degree by the Internet.

Table 3: Summary of identified mechanisms for international Internet public policy issues (version 20 November 2014)

Name of cluster	**Number**
Infrastructure and standardisation	142
Security	199
Human rights	99
Legal	75
Economic	42
Development	57
Sociocultural	25
Other	4
TOTAL Mechanisms	**643**

Most of the mechanisms identified within the infrastructure and standardisation cluster have developed incrementally through a process of collaborative endeavour often described as 'running code and rough consensus'. The most elaborate set of mechanisms manages critical Internet resources (IP numbers, the domain name system and the root zone) and related technical and web standards. For other issues, including net neutrality, cloud computing and the Internet of Things, the development of governance mechanisms is at an early stage. Most of the mechanisms for managing critical Internet resources have emerged as practical solutions for specific problems (*e.g.* how to manage domain names). The effective governance of the Internet infrastructure has facilitated the fast growth of the Internet, making it one of the most important inventions in modern history.

The very growth of the Internet – reaching towards three billion users – has posed new challenges. The more pronounced the societal impacts of the Internet technical solutions are, the more important becomes the need to introduce public policy considerations in making technical decisions, such as setting technical standards. The main challenge has become how to ensure a holistic approach aimed at protecting public interests, such as human rights, in both developing and managing Internet technical resources. The processes for addressing this challenge have already started in the activities of Internet organisations and the wider policy community.

For the other policy issues, organised in six clusters, the underlying principle is that the core rules for addressing these issues in the 'offline world' should be applied to the online world. This approach has been codified in the field of human rights by the UN Human Rights Council which stipulates that 'The same rights that people have offline must also be protected online'.[15]

While in many cases, traditional ('offline') legal principles and approaches remain relevant and applicable to Internet public policy issues, the main challenge is in their implementation to the specificities of the Internet world. The implementation gap is caused by differences between the transborder nature of the Internet and predominantly national regulation of traditional policy issues. For example, consumers used to buy mainly in the place where they lived, typically confined by national markets. Trademarks were protected within national territories. Most of the fight against crime took place on the national level. These and many other issues have gained an international dimension with the Internet transborder communication. Existing mechanisms for implementation of regulation have not been sufficient. In some areas such as cybercrime, this gap was filled relatively fast with the adoption of predominantly regional legal instruments (82 countries are parties to regional cybercrime conventions). In other areas, such as copyright and data protection, international cooperation is gradually taking shape. In other areas, such as consumer protection, the development of policy mechanisms for transborder online transactions is still in a very early stage. The policy response cannot follow fast Internet developments and may create a situation in which Internet public policy issues won't have the mechanisms and venue to be addressed on international level (so-called orphan issues).

The analysis indicates the following gaps appearing frequently in the review of mechanisms for addressing international Internet public policy issues:

- Insufficient institutional capacity and/or resources to address Internet aspects of traditional public issues (e.g. cybercrime, consumer protection, jurisdiction). This gap is particularly important in the enforcement and implementation of public policy given the specific nature of the Internet: the speed of Internet developments and the high level of transborder transactions.

- A lack of mechanisms for addressing Internet public policy issues in an intersectoral way. For example, there is a challenge on how to address online privacy and data protection from all relevant perspectives, including human rights, trade, standardisation, and security perspectives among others.

- A knowledge gap of data and research on international Internet public policy issues.

[15] UN Human Rights Council, Resolution: The promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13, adopted on 5 July 2012.

- A gap between the nominal possibility of participating in Internet policy mechanisms and the reality of participating in an effective and meaningful way, due to the lack of resources, expertise, and institutional capacity.

- A gap in the existence of comprehensive capacity building and information sharing mechanisms on Internet public policy issues. Other than the IGF and its regional and national initiatives, there are not many mechanisms which address Internet public policy issues in a comprehensive and holistic way, with the view of enhancing all stakeholders' capabilities and knowledge on these issues at the global level.

During the continuation of the work initiated by the Working group on Enhanced Cooperation and its correspondence group, a number of challenges were identified. For instance:

- There were substantive disparities in the level of mechanisms identified in the WGEC/correspondence group. This feature remains. The current review of mechanisms goes into detail in some aspects (*e.g.* specific coverage of IETF's Requests for Comments) while providing only a general mapping of other aspects.

- There should be reflection on the most appropriate criteria to assess the status of mechanisms, for instance with regards to transparency and accountability and to participation of various stakeholders.

- Difficulties were encountered in identifying the gaps in a way that is consistent and objective in the absence of clear set of criteria.

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)	Telecommunication 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
		Global public good	8.5