



COUNCIL  
OF EUROPE

CONSEIL  
DE L'EUROPE

H/Inf (2010) 10

# International and multi-stakeholder co-operation on cross-border Internet

*Interim report of the Ad-hoc Advisory Group on Cross-border Internet  
to the Steering Committee on the Media and New Communication Services  
incorporating analysis of proposals for international and multi-stakeholder  
co-operation on cross-border Internet*



# **International and multi-stakeholder co-operation on cross-border Internet**

**Interim report of the Ad-hoc Advisory Group on Cross-border Internet  
to the Steering Committee on the Media and New Communication Services  
incorporating analysis of proposals for international and multi-stakeholder  
co-operation on cross-border Internet**

*The members of the Ad Hoc Advisory Group on Cross-border Internet are:  
Mr Bertrand de la Chapelle, Mr Wolfgang Kleinwächter, Mr Christian Singer,  
Mr Rolf H. Weber, Mr Michael V. Yakushev*

Directorate General of Human Rights and Legal Affairs  
Council of Europe  
F-67075 Strasbourg Cedex

© Council of Europe 2010  
Printed at the Council of Europe

## Contents

|  |    |
|--|----|
| <b>I. Introduction</b> .....   | 5  |
| <b>II. Challenges affecting the Internet – threats to fundamental rights and freedoms</b> .....  | 7  |
| <b>III. General principles of Internet governance</b> .....  | 8  |
| 1. Protection of and respect for fundamental rights and freedoms .....   | 9  |
| 2. Multistakeholderism .....   | 9  |
| 3. Universality of the Internet .....  | 10 |
| 4. Stability, robustness and resilience of the Internet .....  | 11 |
| 5. Empowerment of Internet users .....   | 11 |
| 6. Architectural principles of the Internet ...  | 12 |
| 7. Inclusive participation .....   | 13 |
| 8. Cultural and linguistic diversity .....   | 13 |
| 9. Decentralised management responsibility   | 14 |
| 10. Responsibilities of states for Internet-related public policy .....  | 14 |
| <b>IV. Rights, responsibilities and duties of states in respect of resources that are critical for the functioning of the Internet in a cross-border context</b> ..... | 15 |
| <b>A. General principles of international co-operation</b> .....   | 15 |
| A.1. Multistakeholder participation .....  | 15 |
| A.2. Prevention and management of and response to Internet disruptions and interferences .....   | 16 |
| A.3. Co-operation .....  | 18 |
| A.4. Implementation .....  | 18 |
| A.5. Responsibility .....  | 19 |
| <b>B. Standards, information exchange and co-ordinated action</b> .....  | 20 |
| B.1. Standards and best practices .....  | 20 |
| B.2. Information sharing and notification ...  | 21 |
| B.3. Co-ordinated management and response .....  | 22 |
| B.4. Mutual assistance .....   | 22 |
| <b>C. Transnational management of resources that are critical for functioning of the Internet.</b>   | 23 |
| <b>V. Protection of cross-border flow of Internet traffic</b> .....  | 24 |
| <b>VI. Conclusions and recommendations</b> .....   | 24 |



## I. Introduction

1. The Ad-hoc Advisory Group on Cross-border Internet (MC-S-CI) was set up following the 11th meeting of the Steering Committee on the Media and New Communication Service (CDMC), which took place from 20 to 23 October 2009. Its Terms of Reference were approved by the Steering Committee on the Media and New Communication Services (CDMC) on 27 May 2009 and adopted by the Committee of Ministers on 8 July 2009 and revised on 9 November 2009. The Ministers' Deputies decided at their 1099th meeting on 23 November 2010 to renew the Terms of Reference of the MC-S-CI for 2011.<sup>1</sup>

2. The Group is instructed under its Terms of Reference to:

i. continue to examine the shared or mutual responsibilities of states in ensuring that critical Internet resources are managed in the public interest and as a public asset, ensuring delivery of the public service value to which all persons under their jurisdiction are entitled. Make proposals, in particular, relating to the prevention and management of events, including malicious acts, falling within member states' jurisdictions or territories, which could block or significantly impede Internet access to or within fellow members of the international community with the objective of guaranteeing the ongoing functioning and universal nature and integrity of the Internet;

ii. explore the feasibility of drafting an instrument designed to preserve or reinforce the protection of cross-border flow of Internet traffic openness and neutrality.”

3. The Group has taken note of the decision of the Ministers' Deputies, at their 1068th meeting, on 20 and 21 October 2009,<sup>2</sup> in which they “invited, in particular, the CDMC to seek to ensure multistakeholder participation in the implementation of relevant parts of its terms of reference and to give priority attention in that work to

the elaboration of legal instruments designed (i) to preserve or reinforce the protection of the cross-border flow of Internet traffic and (ii) to protect resources which are critical for the ongoing functioning and borderless nature and integrity of the Internet (i.e. critical internet resources).”

4. The MC-S-CI started consideration of issues pertinent to its Terms of Reference and of working methods at two telephone conferences in January 2010. It had its first formal meeting on 1 and 2 March 2010 in Paris where it decided to prepare a paper for the European Dialogue on Internet Governance (EuroDIG, 29 and 30 April 2010, Madrid) and agreed on the elaboration of draft Committee of Ministers declarations on (i) member states' active participation in the Governmental Advisory Committee (GAC) of ICANN and (ii) the management of IP address resources in the public interest.<sup>3</sup>

5. The draft Declaration of the Committee of Ministers on enhanced participation of member states in Internet governance matters – Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) and the draft Declaration of the Committee of Ministers on the management of Internet protocol address resources in the public interest were elaborated and finalised by the MC-S-CI and the CDMC through online communication. They were subsequently adopted by the Committee of Ministers.<sup>4</sup>

6. At the EuroDIG meeting (Madrid, 29 and 30 April 2010) the MC-S-CI organised a workshop where it presented and discussed with participants its discussion paper “A conceptual approach for setting a standard of care for cross-border Internet”<sup>5</sup> This was based on input papers which were elaborated by the members of the Group. The Group had a first informal meeting on the margins of EuroDIG where it agreed to structure its analysis in two major parts, respectively Internet governance

---

1. See Terms of Reference at [http://www.coe.int/t/dghl/standardsetting/media/MC-S-CI/MC-S-CI\(2009\)Rev\\_mandat\\_en.asp](http://www.coe.int/t/dghl/standardsetting/media/MC-S-CI/MC-S-CI(2009)Rev_mandat_en.asp).

2. See CM/Del/Dec (2009) 1068/4.4E, 23 October 2009, available at [https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Del/Dec\(2009\)1068/4.4](https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Del/Dec(2009)1068/4.4).

3. See MC-S-CI (2010) 005, available at <http://www.coe.int/t/dghl/standardsetting/media/MC-S-CI/MC-S-CI%282010%29005%20Report%201st%20meeting.asp>.

4. The Declaration on enhanced participation of member states in Internet governance matters – Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) was adopted by the Committee of Ministers on 26 May 2010 at the 1085th meeting of the Ministers' Deputies and is available at <https://wcd.coe.int/ViewDoc.jsp?id=1627399>; the Declaration on the management of Internet protocol address resources in the public interest was adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies and is available at <https://wcd.coe.int/ViewDoc.jsp?id=1678299>.

5. The discussion paper is available at [http://www.guarder.net/eurodig/2010/WS6%20Discussion%20Paper%20CoE%20\\_MC-S-CI.pdf](http://www.guarder.net/eurodig/2010/WS6%20Discussion%20Paper%20CoE%20_MC-S-CI.pdf).

principles (Part I) and responsibilities of states (Part II). It also agreed to update the discussion paper accordingly and to submit to discussion of the Internet Governance Forum (IGF) in Vilnius (14-17 September 2010). In addition, the Group decided to elaborate elements for a possible draft declaration of the Committee of Ministers in connection with the Granada Ministerial Declaration. The draft Declaration of the Committee of Ministers on the Digital Agenda for Europe was elaborated and finalised by the Group through online communication. The draft was subsequently endorsed by the CDMC and adopted by the Committee of Ministers.<sup>6</sup> During this time, one of the members of the MC-S-CI, Mr Mark Kelly, had resigned.

7. Some of the members of the Group met on the margins of the 38th meeting of the Internet Corporation for Names and Numbers (ICANN), which took place in Brussels from 20 to 25 June 2010. There was discussion of preparations for participation in the IGF and an exchange of views with external experts. In Vilnius the MC-S-CI organised a workshop where representatives from European and non-European governments, private sector organisations, lawyers, academics, technologists and other stakeholder groups participated.<sup>7</sup> The MC-S-CI submitted a discussion paper “Draft Elements for a Framework of General Principles of Internet Governance and Duties of States with Respect to the Protection of Critical Internet Resources in a Cross-border Context”. On 15 September 2010 the Group had a second informal meeting where it agreed to elaborate explanatory notes to its proposals which are largely reflected in the analysis included in this report. The Group has exchanged views with external experts on a number of occasions including formal and informal meetings as well as events in the framework of the EuroDIG and IGF.<sup>8</sup>

8. At its second formal meeting, which took place on 8 and 9 November 2010 in Strasbourg, the MC-S-CI members and other participants took stock of findings and conclusions reached at its meetings (formal and informal) as well as of feedback received during and after discussions with participants in EuroDIG and IGF. The Group explored prospects and options for future standard-setting action in relation to its Terms of Reference and decided:

- to submit to the CDMC a report on the work and activities carried out during 2010 which incorporates its analysis of legal aspects of cross-border Internet as well as proposals for standard-setting action;

- in respect of item (i) of its Terms of Reference, to invite the CDMC to consider further action aimed at drawing up new international legal instruments on cross-border Internet, in the first place, by instructing the Group to prepare a draft Committee of Ministers’ Declaration on the general principles of Internet governance and a draft Committee of Ministers’ Recommendation on international co-operation in respect of resources that are critical for the functioning of the Internet, on the basis of the analysis included respectively in Parts III and IV of this report, also by taking into account the multi-stakeholder nature of the governance of the Internet and the need for innovative approaches for the development of policy regulatory frameworks;
- in respect of item (ii) of its Terms of Reference, to invite the CMDC to consider a decision to instruct the Group to continue the examination of the feasibility of drafting instruments designed to preserve or reinforce the protection of cross-border flow of Internet traffic openness and neutrality;
- to recommend to the CMDC to organise a dedicated event to discuss with stakeholders the feasibility of international law responses to issues related to international co-operation in respect of resources that are critical for the functioning of the Internet.

9. This report presents the state of examination and analysis of the MC-S-CI of items (i) and (ii) of its Terms of Reference as of the end of the second meeting of the MC-S-CI and as submitted to the CDMC at its 13th meeting (Strasbourg, 16-19 November 2010). It also includes changes made to prepare the report for sharing with a wider group of readers as well as up-to date information further to the CDMC meeting. The CDMC took note of the ongoing work of the MC-S-CI and supported its proposals for standard-setting action as well the organisation of a conference with government representatives, including states which are not members of the Council of Europe, key industry actors and relevant academics the content of those proposals and explore possible further action to be taken on the subject. It also agreed to appoint Mr Bertrand de La Chapelle Program Director at the International Diplomatic Academy as member of the Group. Part II of the report provides an assessment of the need for international and multi-stakeholder co-operation on cross-border Internet issues. Parts III and IV provide a frame of reference for the standard-setting action proposed by the MC-S-CI to the CDMC.

6. The declaration was adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers’ Deputies and is available at <https://wcd.coe.int/ViewDoc.jsp?id=1678251>.

7. Information about this workshop is available at the IGF website, <http://www.intgovforum.org/cms/component/chronocontact/?chronoformname=WSProposals2010View&wspid=60>.

8. In particular, the Group has benefited from exchanges of views with Mr Chris Buckridge (RIPE NCC Community) Mr Bertrand de La Chapelle (formerly Thematic Ambassador and Special Envoy for the Information Society in the French Foreign and European Affairs Ministry, presently Program Director at the International Diplomatic Academy), Ms Maeve Dion (University of Stockholm), Mr William Drake (Graduate Institute of International and Development Studies in Geneva), Ms Athina Fragkouli (RIPE NCC Community), Mr Everton Lucero (Foreign Ministry of Brazil), Ms Joanna Kulesza (University of Lodz), Mr Massimiliano Minisci (ICANN staff), Ms Yuliya Morenets (TAC Strasbourg), Mr Milton Mueller (Syracuse University), Mr Michael Rotert (EuroISPA), Mr George Sadowsky (Technologist and ICANN Board member), Mr Thomas Schneider (Federal Office of Communications, Switzerland), Mr Henrik Spang-Hanssen (Senior Researcher on Internet-related policy), Ms Shane Tews (Vice President, Global Public Policy and Government Relations VeriSign), Ms Hong Xue (Institute for the Internet Policy and Law at Beijing Normal University).



## **II. Challenges affecting the Internet – threats to fundamental rights and freedoms**

10. Internet's openness and accessibility have become preconditions for the enjoyment of fundamental rights, notably the right to freedom of expression and access to information which in accordance with Article 10 should be guaranteed "regardless of frontiers". There are examples of access to broadband Internet connection being recognised as a legal right in some European countries such as Finland and Switzerland. Universal broadband access is also a formally adopted policy, albeit not articulated as an enforceable right, in other countries such as Iceland.

11. Because of the cross-border interconnectedness and interdependencies of the Internet infrastructure, restrictions placed on different types of information, content, services and applications on the Internet may affect the free flow of information across borders. The stability and resilience of the Internet depend on critical resources which are distributed in different jurisdictions and are managed by various entities, without a common governance approach.

12. Users' capacity to access the Internet is exposed to risks of disruptions of the stable and continuous functioning of the network and is vulnerable to technical failure or other acts of interference with the infrastructure of the Internet.

13. Decisions made in the framework of the technical co-ordination and management of critical Internet resources, such as the IP addresses resources and the domain name space, may have a direct bearing on access to information and respect for privacy. A noteworthy example is a recent decision of the French Constitutional Council which acknowledged that freedom of expression can be at stake in the context of management of the French domain name system and that the relevant regulatory framework should include safeguards on freedom of expression.<sup>9</sup>

14. The principle of global public interest in the management of the Internet and the importance of sustaining its stability, robustness and resilience can be derived from the affirmation of the Tunis Agenda for the Information Society which emerged from the second phase of the World Summit on the Information Society (hereinafter the Tunis Agenda) that the Internet has developed into "a global facility available to the public".<sup>10</sup> Critical infrastructure located within specific jurisdictions should be regarded as part of this global facility and its uses should take full account of the common interest. Similarly, the

use of critical resources which are managed beyond the boundaries of national jurisdictions should be open to every nation and every user. Critical Internet resources should be regarded as global commons under the stewardship of the international Internet community as a whole. Their management must be done in full respect for international law, including human rights law.<sup>11</sup>

15. The borderless nature of the Internet infrastructure raises the need to address the challenges to its stability and robustness on a multilateral basis and through international co-operation. The threats affecting the Internet and the integral threats to freedom of expression and access to information can be addressed by internationally co-ordinated preventive, management and response policies.

16. Against this background, it is necessary that there be a common understanding of the fundamental principles and best practices for the stability, robustness and resilience of the Internet by all stakeholders. States can play a key role in structuring action to achieve this goal by promoting and facilitating the development and implementation of common practices, rules and standards of resilience, regular cross-border exchange of knowledge and expertise, experience and technology sharing, exchange of personnel, consultation, participation in joint exercises and mutual assistance in case of need.

17. There are examples of international co-ordination and co-operation in the area of Internet stability and resilience. Mention can be made of the Forum of Incident Response and Security Teams, an international confederation of computer emergency teams which co-operatively deal with cyber security incidents and promote incident prevention programmes.<sup>12</sup> Also, the European Network and Information Security Agency (ENISA) of the European Union (EU) functions on the basis of a model of co-operation amongst national computer emergency teams which builds confidence in its system of technical advice by virtue of its independence, quality of advice and transparency of procedures.<sup>13</sup>

18. However, these interactions are based on technical and operational trust rather than on legal commitments. Their sustainability should be guaranteed by means of a higher level of commitment. International law lacks a basic framework for preventive, management and response action in situations of disruptions of or interferences with the Internet's ongoing functioning, one that includes requirements on timely and effective exchange

9. Decision No. 2010-45 QPC of 06 October 2010, available at <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/cc-201045qpc.pdf>.

10. WSIS-05/TUNIS/DOC/6(Rev.1)-E 18 November 2005, available at <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>, see paragraphs 29, 30 and 31.

11. Resolution on Internet governance and critical Internet resources adopted at the 1st Council of Europe conference of ministers responsible for media and new communication services (Reykjavik, 28-29 May 2009), available at [http://www.coe.int/t/dghl/standardsetting/media/MCM\(2009\)011\\_en\\_final\\_web.pdf](http://www.coe.int/t/dghl/standardsetting/media/MCM(2009)011_en_final_web.pdf), see page 9.

12. See website of the Forum of Incident Response and Security Teams at <http://www.first.org/>.

13. See ENISA's website at <http://www.enisa.europa.eu/>.

of information, disclosure of transboundary risks to critical Internet resources, co-ordination of incident response measures and aid in cases of technical failure or interference with the network.

19. The MC-S-CI considers that a framework of commitments for international and multi-stakeholder co-operation is needed in order to preserve and reinforce the protection of cross-border flow of Internet traffic and the stability and ongoing functioning of the Internet as a means to safeguard freedom of expression and information regardless of frontiers. General principles of Internet governance, on the one hand, and shared responsibilities of states with respect to the preservation of critical Internet resources and the cross-border flow of Internet traffic, on the other hand, should be the two main pillars of such commitments.

### **III. General principles of Internet governance**

21. This part contains the frame of reference for developing a Committee of Ministers' draft Declaration on general principles of Internet governance as proposed in paragraph 8 of this report.

22. The heads of states and government participating in the second phase of the World Summit on the Information Society adopted the following definition of Internet governance as part of the Tunis Agenda:

"[...] Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."<sup>14</sup>

23. The relationship between, on the one hand, local Internet-related policies and Internet management action and the global Internet, on the other hand, should be guided by a set of governance principles that are accepted globally. In the Tunis Agenda the governments commit to "the development of globally-applicable principles on

20. The topic of protection of critical Internet resources is complex due to its inherent features of decentralised management, interconnectedness, interdependencies and control by multiple actors (mainly private) and encompasses diverse types of arrangements. The complexity of an exercise leading to setting legal standards that bring together all actors calls for some caution at this stage in the normative realm. The MC-S-CI has analysed a variety of issues and has developed a frame of reference for the proposals it is expected to make to the CDMC under its Terms of Reference. Although the content of these proposals needs further elaboration, the basic elements and the legal analysis that supports them, have been identified and are explained below. The desirability of reinforcing standard-setting action in relation to cross-border Internet should be considered in due course.

public policy issues associated with the co-ordination and management of critical Internet resources" and "[i]n this regard, [...] call[s] upon the organizations responsible for essential tasks associated with the Internet to contribute to creating an environment that facilitates this development of public policy principles."<sup>15</sup>

24. The principles formulated below set out the general context in which the topic of prevention and management of and response to Internet interferences and disruptions is elaborated. They draw from those which are generally recognised by the Internet community. Initiatives in different parts of the world have advanced a common understanding of the Internet governance principles. For example, the Brazilian Internet Steering Committee has developed a set of Principles for the Governance and Use of the Internet.<sup>16</sup> The European Union promotes a set of Internet governance principles which it considers as enablers of the success of the Internet.<sup>17</sup>

---

14. See above, page 7, footnote 10, paragraph 34.

15. *Id.* paragraph 70.

16. Resolution CGI.br/RES/2009/003/P, available at <http://www.cgi.br/english/regulations/resolution2009-003.htm>.

17. Communication from the Commission to the European Parliament and the Council, Internet governance: next steps, COM (2009) 277 final, at page 6, available at [http://ec.europa.eu/information\\_society/policy/internet\\_gov/docs/communication/comm2009\\_277\\_fin\\_en.pdf](http://ec.europa.eu/information_society/policy/internet_gov/docs/communication/comm2009_277_fin_en.pdf).

## 1. Protection of and respect for fundamental rights and freedoms

**Human rights and fundamental freedoms, which are guaranteed in international law, are non-derogable and core values of Internet governance. They apply equally to offline and online activities and regardless of frontiers. The right to security of persons, privacy, the right to freedom of thought and religion, the right to freedom of expression and access to information, the right to freedom of assembly, the right to the protection of property, the right to education as well as respect for human dignity must be guaranteed in all Internet governance processes. All stakeholders should be aware of developments leading to enhancement of fundamental rights and freedoms and fully participate in efforts aimed at recognising new emerging rights.**

25. This principle draws inspiration from key instruments of international human rights law such as the Universal Declaration on Human Rights and the European Convention on Human Rights. The Council of Europe member states have affirmed that “[f]undamental rights and Council of Europe standards and values apply to online information and communication services as much as they do to the offline world. This stems, *inter alia*, from Article 1 of the European Convention on Human Rights which lays out the obligation of the contracting parties to “secure to everyone within their jurisdiction” the rights and freedoms protected by the Convention (without the online/offline distinction). This approach has been affirmed by the Committee of Ministers of the Council of Europe.”<sup>18</sup>

26. The Council of Europe’s Committee of Ministers has acknowledged that the Internet and other ICT services have high public service value in that they serve to promote the exercise and enjoyment of human rights and fundamental freedoms for all who use them, and that their protection should be a priority with regard to the

governance of the Internet.<sup>19</sup> Every citizen should benefit from the public service value of the Internet. The Committee of Ministers has recommended that member states adopt and develop policies to preserve and, whenever possible, enhance the protection of human rights and respect for rule of law in the information society.

27. There are discussions in academic and other fora on new emerging rights such as the right to anonymity, the right to be forgotten, the right to virtual identity. The Charter of Human Rights and Principles for the Internet that is being drafted by the Rights and Principles Dynamic Coalition, a group of stakeholders’ representatives which was created within the framework of IGF, states that everyone has a right to digital identity and that the virtual personality of human persons needs to be respected.<sup>20</sup> Although there is no world-wide recognition of these rights in international law yet, the general principles of Internet governance should be looking forward to the future and call on all stakeholders to participate in the development of new emerging rights.

## 2. Multistakeholderism

**Internet governance needs the participation of governments, the private sector and civil society, in their respective roles, for the development and application of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the Internet. Internet Governance is a multi-layer and multi-player mechanism in which a broad range of entities participate in a collaborative way.**

28. This principle reflects the understanding of the “Declaration of Principles: Building the Information Society: a global challenge in the new Millennium” adopted at the first phase of the World Summit on the Information Society, which took place in Geneva from 10 to 12 December 2003 (hereinafter the Geneva Declaration of Principles) underlining the need to ensure a multi-stakeholder

approach in Internet governance processes. The “[i]nternational management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations.”<sup>21</sup> It also builds on the working definition of Internet Governance which is included in the Tunis Agenda (see above, paragraph 22, page 8).

18. See above, page 5, footnote 4, and page 6, footnote 6.

19. Recommendation CM/Rec (2007) 16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, adopted by the Committee of Ministers on 7 November 2007 at the 1010th meeting of the Ministers’ Deputies, available at <https://wcd.coe.int/ViewDoc.jsp?id=1207291>.

20. Draft 1.0 of the Charter of Human Rights and Principles for the Internet, September 2010 is available at <http://internetrighsandprinciples.org/node/367>, see section 9 (b) (c).

21. WSIS-03/GENEVA/DOC/4-E, 12 December 2003, available at <http://www.itu.int/wsis/docs/geneva/official/dop.html>, see paragraph 48. See also above, page 7, footnote 10, paragraph 29.

29. A similar reflection can be found in the EU context. The European Commission has stated that “[t]he multi-stakeholder process on Internet governance continues to provide an inclusive and effective mechanism for promoting global co-operation and needs to be further encouraged.”<sup>22</sup>

30. It should be noted that the Working Group on Internet Governance (WGIG), a group of stakeholders’ representatives has analysed in certain details the principle of multistakeholderism. The WGIG “came to the conclusion that from an operational point of view, the WSIS

criteria of multilateralism, transparency, democracy and full involvement of all stakeholder groups have somewhat different meanings, possibilities, and limits in relation to different types of governance mechanisms. They may therefore be regarded as having different shades of meaning in different contexts. For example, the WGIG recognised that “full involvement of all stakeholders” would not necessarily mean that every stakeholder group should have the same role in the development of policies, the preparation of decisions, the actual decisions and then the implementation of decisions.”<sup>23</sup>

### **3. Universality of the Internet**

**The Internet has developed into a global space of freedom for the Internet community worldwide and has become one of the driving forces for economic growth and innovation in our societies as well as a key promoter of education, culture and dissemination of knowledge. The Internet network is part of every nation’s most crucial infrastructures as well as of the transnational communication network. In this regard, without prejudice to the protection of human rights and fundamental freedoms in full respect of international human rights law, all stakeholders have the responsibility to ensure that Internet related policies are developed in a manner that recognises the universal nature of the Internet.**

31. This principle is the basic premise for global free flow of information over the Internet. Several countries have recognised that the free flow of information is essential to democracy, freedom and economic growth. While acknowledging the public service value of the Internet, the Committee of Ministers called on its member states to “affirm freedom of expression and the free circulation of information on the Internet, balancing them, where necessary, with other legitimate rights and interests, in accordance with Article 10, paragraph 2, of the European Convention on Human Rights as interpreted by the European Court of Human Rights [*inter alia*] by promoting freedom of communication and creation on the Internet, regardless of frontiers.”<sup>24</sup>

32. The Seoul Declaration on the Future of the Internet Economy adopted at the OECD Ministerial Meeting on the Future of the Internet Economy, 17 and 18 June 2008 incorporates a commitment of the 39 signatory states and the European Community to “[f]oster creativ-

ity in the development, use and application of the Internet, through policies that, inter alia, maintain an open environment that supports the free flow of information, research, innovation, entrepreneurship and business transformation.”<sup>25</sup> Also, The EU has also acknowledged that the Internet is part of the critical information infrastructure.<sup>26</sup>

33. The topic of universality of the Internet is related to discussions on the topic of state jurisdiction on the Internet. International private law provides basic principles that offer guidance on the exercise of jurisdiction.<sup>27</sup> The principle of universality as proposed to be stated in a declaration of the Committee of Ministers should not be interpreted as attempting to construct a jurisdictional regime or as an effort to answer questions of jurisdiction in cyberspace. Moreover, it is understood that the concept of sovereignty in cyberspace is currently being reviewed in modern literature.<sup>28</sup>

22. See above, page 8, footnote 17, at page 6.

23. The WGIG members were designated by the UN Secretary General “to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005” and to present the result of its work in a report “for consideration and appropriate action for the second phase of the WSIS in Tunis 2005”. The WGIG Background Report of June 2005 is available at <http://www.wgig.org/docs/BackgroundReport.doc>, see paragraph 20.

24. See above, page 9, footnote 19, part III.

25. The Seoul Declaration on the Future of Economy, 18 June 2008 is available at <http://www.oecd.org/dataoecd/49/28/40839436.pdf>.

26. COM (2009) 149 final 30 March 2009, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>.

27. Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (1968), the United Nations Convention on Contracts for the International Sale of Goods (1980).

28. See Rolf H. Weber, “New Sovereignty Concepts in the Age of Internet”, *Journal of Internet Law*, August 2010, at page 12.

#### 4. Stability, robustness and resilience of the Internet

**Internet's stability, robustness and resilience are pre-conditions for the full enjoyment of fundamental rights and freedoms and key objectives of Internet governance. In order to preserve the integrity and ongoing functioning of the Internet's infrastructure as well as users' trust and reliance on the Internet, it is necessary to promote international and multi-stakeholder co-operation.**

34. The Tunis Agenda “recognize[d] that all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet” as well as “the need for development of public policy by governments in consultation with all stakeholders.”<sup>29</sup>

35. One of the main considerations included in the EU's statement of Internet governance principles is that “[t]he Commission believes in maintaining a strong emphasis on the need for security and stability of the global Internet, the respect for human rights, freedom of expression, privacy, protection of personal data and the promotion of cultural and linguistic diversity.”<sup>30</sup> The European Commission has also emphasised the need to

identify principles and guidelines for Internet resilience and stability (at a European level) and to promote them at a global level.<sup>31</sup>

36. As mentioned above, the Committee of Ministers of the Council of Europe has recognised the public service value of the Internet. People rely on the Internet for their every day activities and have a legitimate expectation that Internet services should be accessible and affordable, secure, reliable and ongoing.<sup>32</sup> States have a key role to play in preserving peoples' trust and reliance on the Internet stability and ongoing functioning and have a duty to live up to their legitimate expectation that Internet policy will reflect the public interest.

#### 5. Empowerment of Internet users

**Users should be fully empowered to exercise their freedom of expression and access to information, design their privacy, make their political, commercial or other decisions and participate in online environments, including through the development of user-centred governance mechanisms, according to their own values and preferences and in full respect of fundamental rights and freedoms. Awareness raising and empowerment of Internet users is integral to a free and open Internet and promotes innovation.**

37. Internet users' trust on the Internet relies on the stability of the network, the security of online activities, in the way personal information is processed by state authorities and private entities and on the availability of content in diverse languages and formats. The Geneva Declaration of Principles underlined that “[s]trengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.”

38. Users should have the information necessary to make informed decisions and the tools and knowledge to participate in the online environment as well as to interact with new technologies. These tools and methods should give them the possibility not only to find the information they wish but also to block contents they do not wish to have access to and to disconnect from the online world. Enhancement of users' capabilities such as compu-

ter and information literacy and the development and promotion of technologies of user empowerment should be key objectives of Internet-related policies.

39. Everyone is entitled to take advantage of the public service value of the Internet. The Council of Europe's Committee of Ministers has recommended to member states to develop, in co-operation with the private sector and civil society, strategies which promote the integration of ICTs into education, media and information literacy and training in formal and non-formal education sectors for children and adults in order to empower them to use media technologies, to encourage them to exercise their democratic rights and civic responsibilities effectively and to encourage them to make informed choices when using the Internet and other ICTs.<sup>33</sup> In addition, the Council of Europe has developed a number of standards on media literacy, ongoing and life-long education as well as on the protection and empowerment of children in online environments.<sup>34</sup>

29. See above, page 7, footnote 10, paragraph 68.

30. See above, page 8, footnote 17, at page 6.

31. See above, page 10, footnote 25, at page 11.

32. See above, page 9, footnote 19.

33. Id.



## 6. Architectural principles of the Internet

**Openness, interoperability, the end-to-end nature of the Internet as well as the principle of network neutrality, understood as non-discriminatory and universal access to Internet resources and choice of content, applications and services by the end users, should be normative guides to international policy-making on the Internet.**

40. The Internet is based on a stable, secure and efficient operation of its core architecture. Sustaining its integrity and performance and ensuring interoperability of the Internet with the support of all members of the Internet community is an important normative goal. The inter-networking layer which enables global connectivity over diverse hardware is best exploited by preserving the end-to-end nature that characterises the Internet's architecture. The end-to-end nature of the Internet is described as a function of the network in which the intelligence is at the endpoints rather than hidden in the network.<sup>35</sup>

41. Global, open and non-proprietary core Internet standards and protocols are fundamental features of the Internet design. They allow for the development of applications, content and technological innovations independently. The Internet community shares ownership over the core architecture of the Internet.<sup>36</sup> Protocols and standards should continue to be developed in the framework of pluralistic, transparent and co-ordinated collaborative processes as well as with multiple public and private stakeholders according to the principle of subsidiarity, which calls for decisions to be made at the most appropriate and efficient level with efficient co-ordination. Open standards should apply to all layers of the Internet architecture to guarantee the interoperability of networks in terms of infrastructures, services and contents.

42. Internet architecture and its governance evolve as technological innovation continues to emerge, the number of mobile Internet uses increases, more diverse terminals are connected and the peer-to-peer system develops. The development of knowledge of these technologies should be promoted in order to allow for the

progress of Internet uses in society. Innovation should be a key objective of Internet-related public policy.

43. Network neutrality has generated value for society as it has been the driving force behind technological innovations, network growth and market competition, and has encouraged the diversification of information available online by means of lowering the thresholds for the dissemination of knowledge.

44. The Committee of Ministers' Declaration on network neutrality states that "users should have the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice."<sup>37</sup> Such a general principle, commonly referred to as network neutrality, should apply irrespective of the infrastructure or the network used for Internet connectivity. Access to infrastructure is a prerequisite for the realisation of this objective."

The Declaration adds that "traffic management should not be seen as a departure from the principle of network neutrality. However, exceptions to this principle should be considered with great circumspection and need to be justified by overriding public interests. In this context, member states should pay due attention to the provisions of Article 10 of the European Convention on Human Rights and the related case-law of the European Court of Human Rights."

45. The Brazilian Principles for the Governance and Use of the Internet give the following formulation in respect of the principle of neutrality of the network "[f]iltering or traffic privileges must meet ethical and technical criteria only, excluding any political, commercial, religious and cultural factors or any other form of

34. Recommendation CM/Rec (2009) 5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment, adopted by the Committee of Ministers on 8 July 2009 at the 1063rd meeting of the Ministers' Deputies, available at [https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec\(2009\)5](https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2009)5); Recommendation Rec (2006) 12 of the Committee of Ministers to member states on empowering children in the new information and communications environment, adopted by the Committee of Ministers on 27 September 2006 at the 974th meeting of the Ministers' Deputies, available at [https://wcd.coe.int/ViewDoc.jsp?Ref=Rec\(2006\)12](https://wcd.coe.int/ViewDoc.jsp?Ref=Rec(2006)12); Declaration on protecting the dignity, security and privacy of children on the Internet, adopted by the Committee of Ministers on 20 February 2008 at the 1018th meeting of the Ministers' Deputies, available at [https://wcd.coe.int/ViewDoc.jsp?Ref=Decl\(20.02.2008\)](https://wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)); Recommendation 1836 (2008) of the Parliamentary Assembly, Realising the full potential of e-learning for education and training, adopted by the Standing Committee acting on behalf of the Assembly on 29 May 2008, available at <http://assembly.coe.int/documents/AdoptedText/ta08/EREC1836.htm>; Recommendation 1466 (2000) of the Parliamentary Assembly on media education, adopted by the Assembly on 27 June 2000 (19th Sitting), available at <http://assembly.coe.int/documents/adoptedtext/ta00/erec1466.htm>; Recommendation 1111 (1989) of the Parliamentary Assembly on the European dimension of education, adopted by the Assembly on 22 September 1989 (12th Sitting), available at <http://assembly.coe.int/documents/adoptedtext/ta89/erec1111.htm>; Recommendation 1110 (1989) of the Parliamentary Assembly on distance teaching, adopted by the Standing Committee, acting on behalf of the Assembly, on 6 July 1989, available at <http://assembly.coe.int/documents/adoptedtext/ta89/erec1110.htm>.

35. RFC 1958 of the Internet Engineering Task Force, Internet Architecture Board, June 1996, available at <http://www.ietf.org/rfc/rfc1958.txt>, see section 2.1.

36. *Id.* section 2.4.

37. The Declaration on network neutrality was adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies and is available at <https://wcd.coe.int/com.instranet.InstraServlet?Index=no&command=com.instranet.CmdBlobGet&InstranetImage=1647862&SecMode=1&DocId=1631194&Usage=2>.

discrimination or preferential treatment. A related principle, namely unaccountability of the network is formulated as “[a]ll action taken against illicit activity on the network must be aimed at those directly responsible for

such activities, no at the means of access and transport, always upholding the fundamental principles of freedom, privacy and the respect for human rights.<sup>38</sup>

## 7. Inclusive participation

**International Internet-related public policies and Internet governance arrangements should ensure full and equal participation of all countries.**

46. The Tunis Agenda “recognize[d] as fundamental elements to bridge the digital divide in developing countries, in a sustainable way, poverty reduction, enhanced national capacity building and the promotion of national technological development.”<sup>39</sup> It also committed governments “to review and follow up progress in bridging the digital divide, taking into account the different levels of development among nations, so as to achieve the internationally agreed development goals and objectives, including the Millennium Development Goals, assessing the effectiveness of investment and international co-operation efforts in building the Information Society, identifying gaps as well as deficits in investment and devising strategies to address them.”<sup>40</sup>

47. The Council of Europe Committee of Ministers has recommended to member states to develop, in co-operation with the private sector and civil society, strategies which promote affordable access to the Internet for individuals, irrespective of their age, gender, ethnic or social origin, including persons and groups of persons on low incomes, those in rural and geographically remote areas and those with special needs (for example, disabled persons) bearing in mind the importance of design and application, affordability, the need to raise awareness among these persons and groups, the appropriateness and attractiveness of Internet access and services as well as their adaptability and compatibility.<sup>41</sup>

## 8. Cultural and linguistic diversity

**Cultural and linguistic diversity and the development of local content, regardless of language or script, should be key objectives of Internet related policy, international co-operation and development of new technologies.**

48. The protection of cultural heritage as well as intercultural dialogue is part of Council of Europe conventional standards such as the European Cultural Convention (ETS No. 018) and the Framework Convention on the Value of Cultural Heritage for Society (ETS No. 199).<sup>42</sup> The European Charter for Regional or Minority Languages (ETS No. 148), the Framework Convention for the Protection of National Minorities (ETS No. 157), the European Outline Convention on Transfrontier Co-operation between Territorial Communities or Authorities (ETS No. 106) and the Convention on the Participation of Foreigners in Public Life at Local Level (ETS No. 144) promote and protect diversity in a spirit of tolerance.<sup>43</sup> The Committee of Ministers and the Parliamentary Assembly have also adopted a panoply of recommendations on different aspect of intercultural dialogue.

Notably, in the 1999 Declaration on a European policy for new information technologies, the Committee of Ministers urged member states to promote the full use by all, including minorities, of the opportunities for exchange of opinion and self-expression offered by the new information technologies as well as to encourage the provision of cultural, educational and other products and services in an appropriate variety of languages.<sup>44</sup>

49. The utilisation of a website by users in their own language is an important element of access to the Internet and of user empowerment. Multilingualism in cyberspace is a key concept to ensure cultural diversity and participation of all linguistic groups in the information society. The Internet has developed into a space for expression, exchange and interaction of all cultures and languages. The introduction of the first four internationalised

38. See above, page 8, footnote 16, principles 6 and 7.

39. See above, page 7, footnote 10, paragraph 87.

40. *Id.* paragraph 119.

41. See above, page 9, footnote 19, part II, a, b and c.

42. ETS No. 018 is available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=018&CM=8&DF=13/11/2010&CL=ENG>; ETS No. 199 is available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=199&CM=8&CL=ENG>.

43. ETS No. 148 is available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=148&CM=8&DF=13/11/2010&CL=ENG>; ETS No. 157 is available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=157&CM=8&DF=13/11/2010&CL=ENG>; ETS No. 106 is available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=106&CM=8&DF=13/11/2010&CL=ENG>; ETS No. 144 is available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=144&CM=8&DF=13/11/2010&CL=ENG>.

44. The Declaration was adopted by the Committee of Ministers on 7 May 1999, at its 104th Session, available at <https://wcd.coe.int/ViewDoc.jsp?id=448133>.

domain names (IDNs) in the domain name system by ICANN in May 2010 has enabled the creation of spaces for local language content and contributed to the global nature of the Internet. Meanwhile 13 more IDNs country code Top Level Domains (ccTLDs) have passed the process of string evaluation in ICANN.

50. The UNESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions of

20 October 2005<sup>45</sup> provides guidance on the protection of multilingualism and cultural diversity. The promotion and preservation of diverse cultural identities and languages should be a key objective of international Internet related policy, which should provide instruments to enable support for capacity building for the production of local language content and availability of translation technology in order to promote knowledge diversity.

## **9. Decentralised management responsibility**

**The decentralised nature of the responsibility for the management of the Internet should be preserved. The private sector should retain its leading role in the technical and operational matters while ensuring transparency and being accountable to the Internet community for its actions that have an impact on public policy.**

51. Internet infrastructure, software and services are owned and administered by private entities, which in turn leads to decentralised network operation and policies. The private sector has contributed to promote the universality of the Internet, unleash economic potential and develop democratic processes and is on the front lines of action aimed at, ensuring the robustness and resilience of Internet's infrastructure.

52. The EU promotes a similar principle which states that “[p]rivate-sector leadership of day-to-day Internet management needs to be maintained but private bodies responsible for the co-ordination of global Internet resources need to be accountable to the international community for their actions. The role of governments should

be mainly focused on principle issues of public policy, excluding any involvement in the day-to-day operations.”<sup>46</sup>

53. Transparency is a central feature of many of the affirmations of the Tunis Agenda. It is described as a basic premise of the governance of the Internet in general<sup>47</sup> and is embodied in a number of other affirmations on specific topics and issues such as the development of strategies for global connectivity and equitable access,<sup>48</sup> multilingualisation<sup>49</sup> and development of regulatory frameworks.<sup>50</sup> Transparency enables verification of whether the management decisions guarantee the protection of the public interest in an adequate manner. Hence, the need for accountability for private sector actions and decisions that have an impact on public policy.

## **10. Responsibilities of states for Internet-related public policy**

**States have rights and responsibilities for developing and implementing international Internet-related public policy and, in this regard, they should ensure full participation of the private sector and civil society. They have legitimate expectations *vis-à-vis* fellow members of the international community and mutual responsibilities to take reasonable measures to ensure the ongoing functioning, stability and universality of the Internet. International co-operation and new relationships should build on existing mechanisms or arrangements on Internet governance in a spirit of complementarity and co-operation.**

54. Council of Europe member states have recognised that fundamental rights and freedoms apply equally to offline and online activities. As bearers of the duty to guarantee the protection of fundamental rights and freedoms, states should ensure that international Internet-related policy incorporates adequate safeguards for fundamental rights and freedoms. Citizens' legitimate expectation that Internet services be accessible and af-

fordable, secure, reliable and ongoing (public service value of the Internet)<sup>51</sup> and the corollary expectation that Internet-related policy and governance arrangements reflect the public interest of the Internet community as a whole, raise the need for effective public policies as well as private sector accountability. The Council of Europe ministers responsible for media and new communication services have affirmed that “Council of Europe member

45. The text of this convention is available at [http://portal.unesco.org/en/ev.php-URL\\_ID=31038&URL\\_DO=DO\\_TOPIC&URL\\_SECTION=201.html](http://portal.unesco.org/en/ev.php-URL_ID=31038&URL_DO=DO_TOPIC&URL_SECTION=201.html).

46. See above, page 8, footnote 17, at page 6.

47. See above, page 7, footnote 10, paragraph 29: “[t]he international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations”.

48. *Id.* paragraph 50 (b).

49. *Id.* paragraph 53.

50. *Id.* paragraphs 19, 90(b) and 96.

51. See footnote 19 above.



states share the responsibility to take reasonable measures to ensure the ongoing functioning of the Internet and, in consequence, of the delivery of the public service value to which all persons under their jurisdiction are entitled. Interstate co-operation and solidarity is of paramount importance to the proper functioning, stability and universality of the Internet.”<sup>52</sup>

55. The Tunis Agenda recognised that “[p]olicy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues. Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related

public policy issues.”<sup>53</sup> It also recognised “the need for development of public policy by governments in consultation with all stakeholders.”<sup>54</sup> The EU promotes the principle that “[g]overnments need to fully interact with [...] multi-stakeholder processes, with stakeholders accepting that it is governments alone who are ultimately responsible for the definition and implementation of public policies.”<sup>55</sup>

56. This principle should be read together with Part IV in which the MC-S-CI elaborates more on the rights, responsibilities and duties of states in respect of critical Internet resources in a cross-border context as well as on different ways to construct international and multistakeholder co-operation.

## **IV. Rights, responsibilities and duties of states in respect of resources that are critical for the functioning of the Internet in a cross-border context**

57. This part provides the frame of reference for the MC-S-CI proposal to the CDMC in respect of developing

a Committee of Ministers’ draft Recommendation (see above, paragraph 8, page 6).

### **A. General principles of international co-operation**

#### **A.1. Multistakeholder participation**

**States acknowledge and are guided by the general principles of Internet governance in processes of developing public policy on the Internet. In particular, states acknowledge the role and the efforts of the private sector to address risks and vulnerabilities of the Internet infrastructure as well as the fundamental role of civil society in developing and monitoring policies and arrangements in relation to the preservation of the stability, robustness and resilience of the Internet. States should create an enabling and collaborative environment for the private sector and civil society to play their roles and should forge partnerships among all actors.**

58. This principle affirms the general principles of Internet governance as normative guides for policy making on the Internet, with a special emphasis on the principle of multistakeholderism. It acknowledges that the private sector, as administrator of Internet’s infrastructure, is on the front lines of action taken to address vulnerabilities and risks of the infrastructure, in different ways, such as by taking precautions, adopting recovery measures and developing market solutions. States also affirm the watchdog role of civil society on public policy on the Internet.

59. As bearers of the duty to ensure respect for the public interest, states should undertake a commitment to create an enabling environment for all stakeholders to play their roles. States can facilitate dialogue, information and knowledge sharing, co-ordinated action and co-operative activities among private sector actors. They can act as conveners of meetings or promoters of structured dialogue among stakeholders including the industry, the civil society and governmental agencies. They can help institutionalise these partnerships by creating or facilitating the operation of institutional collaborative and transparent arrangements.

52. See footnote 11 above.

53. See above, page 7, footnote 10, paragraph 35.

54. *Id.* paragraph 68.

55. See above, page 8, footnote 17, at page 6.

## A.2. Prevention and management of and response to Internet disruptions and interferences

**States should, in co-operation with each other and with all relevant stakeholders, take all reasonable measures to prevent, manage and respond to significant transboundary disruption of and interference with the stability, robustness, resilience and openness of the Internet, or at any event minimise the risk and consequences thereof.**

60. This principle is based on the principle of prevention of the International Law Commission's Draft Articles on Prevention of Transboundary Harm from Hazardous Activities which reads:

"The State of origin shall take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof."<sup>56</sup>

61. In customary international law, the principle of prevention has been derived from the application of general principles of law such as the principle *sic utere tuo ut alienum non laedas*, affirming that "one should use his own property in such a manner as not to injure that of another". The duty of a state to ensure that activities within its territory or under its jurisdiction do not cause damage to other states has been affirmed in the 1938 Trail Smelter Arbitration (*United States v. Canada*);<sup>57</sup> in the 1949 Corfu Channel case (*United Kingdom v. Albania*),<sup>58</sup> in which the International Court of Justice stated the obligation of a state not to knowingly allow its territory to be used contrary to the rights of other states; as well as in the 1957 Lac Lanoux Arbitration (*France v. Spain*)<sup>59</sup> which stated the obligation of a state to take all necessary measures to prevent transboundary damage.<sup>60</sup>

62. The principle of prevention served as the basis for the development of the no-harm rule that was integrated in international law. The most notable example is Principle 21 of the 1972 Declaration of the United Nations Conference on Human Environment (Stockholm 5-16 June 1972) which affirms, on the one hand, states' sovereign rights relating to the exploitation of resources pursuant to their national environmental policies and, on the other hand, the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction.<sup>61</sup> Principle 2 of the Rio Declaration on Environment and Development affirms that "[s]tates have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to exploit their own resources pursu-

ant to their own environmental and developmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction."<sup>62</sup>

63. The principle of prevention has been adopted in international treaty law concerning the protection of the environment (the United Nations Convention on the Law of the Sea;<sup>63</sup> the Convention on the Prevention of Marine Pollution by Dumping of Wastes and Other Matter;<sup>64</sup> the Vienna Convention for the Protection of the Ozone Layer;<sup>65</sup> the Convention on Environmental Impact Assessment in a Transboundary Context<sup>66</sup>), concerning international watercourses (the Convention on the Protection and Use of Transboundary Watercourses and International Lakes<sup>67</sup>), as well as nuclear accidents (the Convention on Long-Range Transboundary Air Pollution<sup>68</sup>).

64. Principle A.2, together with principle A.3 on co-operation, is intended to provide the basic foundation for the other proposed commitments of states in respect of the preservation of the ongoing functioning of the Internet and the protection of cross-border flow of the Internet traffic. A.2 is a statement of principle. The phrase "all appropriate measures" refers to all those specific actions and steps that are identified in the subsequent proposed commitments of states (Section B including exchange of information, consultation and mutual assistance). The reason for the formulation of principle A.2 is to underline the primary nature of the proposed commitments of a state to prevent, manage and respond to significant transboundary disruption of or interference with the stability, robustness, resilience and openness of the Internet. Only in case this is not fully possible a state should exert its best efforts to minimise the risk or consequences thereof.

65. The proposed commitments of prevention and management of disruptions of and interferences with the Internet apply to policies and measures adopted by states to deal with situations which involve a risk of causing or

56. ILC Articles on Prevention of Transboundary Harm from Hazardous Activities adopted in 2001, UN Doc. A/56/10 Supp. No. 10 (2001), Article 3.

57. UNRIAA, vol. III (Sales No. 1949.V.2), p. 1905 (1938, 1941).

58. ICJ Reports 1949, p. 4, at p. 23.

59. UNRIAA, vol. XII (Sales No. 63.V.3), p. 281.

60. See also above, page 5, footnote 5.

61. UN Doc. A/Conf.48/14/Rev. 1 (1973); 11 ILM 1416 (1972) available at <http://www.unep.org/Documents.Multilingual/Default.Print.asp?documentid=97&articleid=1503>.

62. UN Doc A/CONF.151/26 (1992), available at <http://www.un.org/documents/ga/conf151/aconf15126-1annex1.htm>.

63. 1833 UNTS 3, see article 194.

64. 1046 UNTS, see article 1.

65. 1513 UNTS 293, see article 2.

66. 1989 UNTLS 309, see article 2 (1).

67. 1936 UNTS 269, see article 2 (1).

68. 1302 UNTS 217, see article 2.

as a consequence of which there is significant transboundary disruption of or interference with the stability, robustness, resilience and openness of the Internet. Different situations could be envisaged under this category such as technical failures or malicious activities on the Internet. Such events happened in the case of the submarine cable system failure in the Mediterranean Sea on 30 January 2008 which affected 70% of Egypt's online traffic and half of the India's Internet capacity or in the case of the most noteworthy European hacking attack through distributed denial of service attacks on Estonia in April/May 2007.

66. Suggestions have been made at different stages of discussion of the MC-S-CI analysis and proposals to specify the instances which involve risk of causing or as a consequence of which there is significant disruption of or interference with the Internet's stability, robustness and resilience. Also, it has been suggested to give consideration to cases when the Internet does not necessarily suffer disruption or there is no interference with the Internet itself but instead the Internet infrastructure is used as a "vector" for interference with other critical infrastructure.

67. In respect of the latter suggestion, the understanding of the Group is that these cases do not fall within the scope of examination that is expected under its Terms of Reference.<sup>69</sup> The current examination of issues related to the protection of the integrity, ongoing functioning and openness of the Internet in a cross-border context is justified by the fact that the protection of freedom of expression and right to access to information is dependant on a stable, robust and resilient Internet. The Group recalls that the Council of Europe ministers responsible for media and new communication services stated in their Resolution on Internet governance and critical Internet resources that "Article 10 of the European Convention on Human Rights [freedom of expression] is especially relevant in [...] respect [of cross-border nature of the Internet] given that the rights and freedoms protected therein are guaranteed "regardless of frontiers".<sup>70</sup>

68. Against this background, it is understood that risks of disruption or interference with the stability, robustness and resilience of the Internet should have the potential to have a major impact on a significant number of users' ability to access information, services and applications available online across borders. A specification of a list of cases or activities that would fall under this category does not seem to be essential in terms of making the primary commitments on prevention, management and response operational. Any such list is likely to become quickly obsolete in the light of fast evolving technology. Also, the risks of disruption or interference which flow from a certain activity are primarily related to specific contexts and a matter of technical operation. Furthermore, a generic list could not capture all these factors. It

may be further noted that states have the possibility to provide guidance in respect of specific activities coming within the scope of the primary commitments in the context of measures taken to implement them.

69. The most important element that would determine whether certain situations would fall within the scope of the proposed commitments is the transboundary effect on the Internet's stability, robustness and resilience to which preventive and response measures and policies should be applicable. Activities leading to such situations would be carried out or would take place within the jurisdiction or territory of a state and would involve the risk of having or would actually have negative consequences in another jurisdiction.

70. The proposed commitments to prevent, manage and respond to the risks mentioned above are intended to allow a state likely to be affected or actually affected by significant transboundary disruption of or interference with Internet to demand from the state, within the jurisdiction of which activities leading to this situation take place, compliance with the latter's commitments. These are concerned with the management of risk and consequences of Internet disruptions or interferences and emphasise the duty of co-operation among the states concerned.

71. A commitment to prevent Internet disruptions and interferences would naturally include reasonable measures to prevent cyber attacks which use resources located in a specific territory or jurisdiction as well as to combat cybercrime. In this context, states should take appropriate measures to prevent Internet users' involvement in cyber-attacks and other forms of malicious use of the Internet which may have significant transboundary consequences for the stability, robustness and resilience of network resources as well as the freedom of Internet users in other states. Examples could include accession to relevant international law instruments such as the Budapest Convention,<sup>71</sup> and participation in their follow up arrangements including the Convention's Committee (T-CY), the Octopus conference which brings together representatives from different countries who are professionally involved in cybercrime matters and the 22/7 network which facilitates international co-operation on investigations or proceedings concerning cybercrime. States should also participate in the development and implementation of Internet user education and public awareness programmes, promotion and facilitation of dialogue with stakeholders as well as other appropriate measures.

72. The commitment of a state in respect of taking measures to prevent, manage and respond to transboundary disruptions or interferences would be one of due diligence. It is the conduct of the state in question that would determine whether it has complied with its duty of due diligence. This duty is the standard in inter-

69. See above, page 5, footnote 1.

70. See above, page 7, footnote 11, paragraph 2.

71. ETS No. 185, available at <http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=1/19/2007&CL=ENG>.

national treaty law in respect of the protection of the environment (see above paragraph 61, page 16). Acting with due care imposes on a state a duty to do all it can, or in other words, to take all appropriate measures at its disposal to prevent and minimise foreseeable significant transboundary harm.

73. In the context of the Internet stability, robustness and resilience, due diligence would be manifested in reasonable efforts by a state to inform itself of factual and legal components that relate to transboundary disruptions or interferences with the Internet infrastructure and to take appropriate measures in a timely fashion to address them. Such measures would include firstly, formulating policies designed to prevent and respond to disruptions or interferences, or to minimise risk or consequences thereof and secondly implementing these policies.

74. The required degree of care should be proportional to the degree of risks involved or consequences incurred. The disruption and interference should be foreseeable and the state concerned must know or should have known under the circumstances that the given activity involved a risk of significant consequences. A state should not bear the risk of unforeseeable consequences to states likely to be affected by activities taking place within its jurisdiction. However, the commitment “to take all reasonable measures” to prevent and respond to disruptions or interference, or to minimise risks and consequences thereof, would be of a continuous nature. An efficient observance of a due diligence commitment is understood as the implementation of those measures which would be commensurate with the overall capabilities of the country concerned to address the risks.

### **A.3. Co-operation**

**States should co-operate mutually, in good faith and in consultation with each other and with concerned stakeholders at all stages of designing and implementing policies in relation to the Internet.**

75. This principle sets forth a general requirement of co-operation among states and stakeholders at all stages of policy design and implementation. The modalities of co-operation are stated more specifically in the subsequent principles under section B. They envisage participation of states within whose jurisdiction disruptions or interferences with the Internet stability, robustness and resilience may originate, and states likely to be affected or actually affected, in action aimed at prevention of, preparedness for and response to risks and threats to critical Internet resources. A multi-stakeholder approach is crucial in the success of such action. States concerned would be required to co-operate in good faith. The prin-

ciple of co-operation is generally accepted in international law. The Vienna Convention on the Law of Treaties, 23 May 1969, declares that the principle of good faith is universally recognised and affirms its central importance in respect of the observance, application and interpretation of the treaties.<sup>72</sup>

76. In particular, states should co-operate in the creation of public awareness about the risks and opportunities of cross border Internet traffic and the development of educational tools to enable citizens to share responsibilities for a safer Internet.

### **A.4. Implementation**

**States should develop, within the limits of non-involvement in the operational issues and ordinary administration of Internet activities, reasonable legislative, administrative or other measures as appropriate, including the establishment of suitable monitoring mechanisms, to implement their commitments.**

77. This principle describes some of the modalities according to which a state within whose jurisdiction disruptions of or interference with the Internet originate could discharge its due diligence commitments of prevention, management and response. These may include legislative, administrative or other action necessary to implement these commitments. It is understood that this action should be subject to the capabilities of the state concerned. At first sight, it may seem that this paragraph is redundant as it states in general terms the specific requirements contained in the subsequent principles, namely that states should take necessary implementation

measures. It is felt, however, that a statement of the requirement of implementation is necessary in order to stress the continuous character of the commitment which requires action to prevent and respond to disruptions of or interferences with the Internet.

78. This principle should not be interpreted as an assertion of exclusive competence by state authorities in respect of the stability, robustness and resilience of the Internet. The reasonable and appropriate measures referred to in this principle should be understood in the context of public-private partnerships. The principle of subsidiarity or non-involvement of states in the ordinary

72. 1155 UNTS 331, see the preamble and articles 26 and 31 (1).



administration of the network or operational issues sets the limit of such measures (see principles 9 and 10 in Part III). It should be applicable to the extent that the state is not the actual operator or manager of critical Internet resources. It builds on the Tunis Agenda which affirms that the private sector takes the lead in the day-to-day operations of the Internet<sup>73</sup> and “recognise[s] the need for enhanced co-operation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues.”<sup>74</sup>

79. Legislative action may be necessary in order to overcome barriers to international co-operation which

may arise as a consequence of differences in legal environments, levels of organisational, political or financial support for computer emergency teams or in operational standards and practices.<sup>75</sup> Other measures may involve other positive action such as developing and implementing national strategies for proactive management of risks pertinent to or inherent in Internet infrastructure.

80. Although it is not the purpose of the proposed commitment of co-operation states may establish mechanisms that are suitable for monitoring the implementation of their preparedness and prevention commitments in respect of disruptions and interference with the infrastructure of the Internet. The role of the private sector and that of the civil society would be of great importance in this connection.

### A.5. Responsibility

**With the objective of ensuring accountability in respect of adverse consequences on the stability, robustness and resilience of the Internet, states should engage in dialogue and co-operate to the further development of international law relating to the responsibility and liability for the assessment of and compensation for damage as well as the settlement of related disputes.**

81. This principle is inspired by and modelled after the United Nations Convention on the Law of the Sea of 10 December 1982 which in article 235 on Responsibility and Liability states:

“With the objective of assuring prompt and adequate compensation in respect of all damage caused by pollution of the marine environment, States shall co-operate in the implementation of existing international law and the further development of international law relating to responsibility and liability for the assessment of and compensation for damage and the settlement of related disputes, as well as, where appropriate, development of criteria and procedures for payment of adequate compensation, such as compulsory insurance or compensation funds.”<sup>76</sup>

82. Principle A.5 affirms that the set of international commitments proposed by the MC-S-CI does not address the issues of legal consequences for failure to deliver on the commitments of co-operation contained in A.2 and A.3 and more specifically those under section B. It does not attempt to establish a legal regime of liability and reparation in respect of adverse consequences or damages on the stability, security and resilience of the Internet or to address the issue of settlement of disputes arising from the interpretation or application of the commitments on international co-operation.

83. The Group’s endeavour is to define viable legal structures, which in the context of preservation of the stability, robustness and resilience of the Internet, support specific commitments and therefore may be considered as primary in nature. The proposed approach is not concerned with determining the legal consequences for failure to fulfil any of these primary commitments or any other existing obligations in international law. In particular, this approach is not concerned with determining whether activities which involve disruption or interference with the Internet’s infrastructure constitute breaches of obligations recognised in international law, particularly those in respect of the maintenance of peace which are set forth in the United Nations Charter. It is also understood, that commitments on prevention, management and response to Internet disruptions or interferences should not have any bearing upon international co-operation to fight cybercrime in accordance with the Budapest Convention.

84. According to the International Law Commission the protection against risks or threats associated with activities that are not prohibited by international law is quite a distinct topic from that of state responsibility for failure to fulfil international obligations (internationally wrongful acts).<sup>77</sup> The presence of conduct (action or omission) attributable to a state under international law and the fact that such conduct constitutes a breach of

73. See above, page 7, footnote 10, paragraph 55.

74. *Id.* paragraph 69.

75. ENISA report CERT co-operation and its further facilitation by relevant stakeholders, 17 June 2009, available at <http://www.enisa.europa.eu/act/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders>, see section 7.3.

76. See above, page 16, footnote 66.

77. The International Law Commission has clarified this distinction in the commentaries to the Articles on State Responsibility annexed to the UN General Assembly Resolution “Responsibility of States for Internationally Wrongful Acts”, GA Res. 56/83, UN Doc. A/RES/56/83 (12 December 2001), see *Yearbook of the International Law Commission*, 1973, vol. II, general comments at page 169.

international obligations are essential conditions to establish the existence of internationally wrongful acts and to give rise to state responsibility. Article 3 of the draft articles on state responsibility as elaborated by the International Law Commission states:

“There is an internationally wrongful act of a State when:

- a. Conduct consisting of an action or omission is attributable to the State under international law; and
- b. That conduct constitutes a breach of an international obligation.”

85. The MC-S-CI examination focuses on the determination of international commitments which would help create a system of prevention, management and response to disruption and interference with Internet’s infrastructure through international co-operation. The Group considers that it is necessary to maintain a strict distinction between this task and any endeavour to determine the rules that govern the responsibility for non-fulfilment of these commitments. Thus, it is understood that commitments to prevent and manage cross-border disruptions of or interferences with the Internet, which would be primary in nature, are different from existing international law rules governing responsibility for internationally wrongful acts.

86. While the principle of liability and the related arrangements on reparation may have a deterrent effect on disruptions of or interferences with the stability, robustness and resilience of the Internet, it is considered that preventive and mitigating measures can have an even more direct and effective deterrent effect. Consequently the focus is on co-operation in the prevention of and response to disruptions of and interference with the Internet. This thinking is inspired by legal concepts contained in international law on the protection of the environment. Because of inherent limitations of compensatory liability regimes (mostly related to litigation and dispute settlement), international regulation on marine pollution, pollution of international rivers and lakes, atmospheric pollution and protection and conservation of fauna and flora places emphasis on preventive, management and mitigation measures rather than reparation.<sup>78</sup>

87. That said, states may already wish to undertake to engage in dialogue to develop further international law relating to the responsibility and liability for the assessment of and compensation for damage as well as the settlement of related disputes. This may be seen as a separate exercise which states may explore at a later stage.

## **B. Standards, information exchange and co-ordinated action**

### **B.1. Standards and best practices**

**States should co-operate with a view to support the development and implementation of common standards, rules or practices as well as the establishment of co-operation and dialogue platforms aimed at preserving and strengthening the stability, robustness and resilience of the Internet.**

88. This paragraph sets forth a commitment of co-operation with specific reference to the development of common rules and practices aimed at ensuring the stability robustness and resilience of the Internet infrastructure. These are considered as the first of a series of measures to preserve the ongoing functioning of the Internet.

89. Different forms of co-operation can give effect to this commitment. States can participate in and facilitate the development of common standards or good practices for information sharing and incident reporting as well as promote their implementation in the public and private sector. In conjunction with the private sector, states can promote and facilitate the development of common standards or practices for deploying Internet resilience technologies (e.g. Domain Name System Security Exten-

sions (DNSSEC) or resilient routing technologies). They should also provide market incentives for wide take-up of security technologies as well as promote research in this context.

90. States may fulfil this commitment in the context of promoting the creation and facilitating the operation of co-operation platforms, such as public-private co-operation platforms or other mechanisms on awareness-raising, information sharing, incident management and reporting and engaging in international exercises. Measures in respect of standardisation deserve nevertheless to be supported by a stand alone commitment rather than being implicit under a general requirement to promote co-operation platforms.

78. Francisco Orrego Vicuña, “State Responsibility, Liability, and Remedial Measures under International Law: New Criteria for Environmental Protection”, in *Environmental Change and International Law: New Challenges and Dimensions*, United Nations University Press 1992, available at <http://unu.edu/unupress/unupbooks/uu25ee/uu25ee0g.htm#11.%20the%20new%20law%20of%20stat>.

## B.2. Information sharing and notification

**States should create an environment that facilitates information sharing among stakeholders in respect of activities involving risk of causing significant transboundary disruption to or interferences with the stability and resilience of Internet resources. In particular states should take all reasonable measures to provide prior and timely notification and relevant information to states that may be potentially affected.**

91. This principle deals with information sharing as one in a series of anticipatory actions in respect of prevention of significant transboundary disruption of or interference with the stability, robustness or resilience of the Internet. It affirms the enabling role of states in respect of promoting and facilitating identification, assessment of vulnerabilities or risks originating within their jurisdiction as well as in respect of sharing of information among private sector actors. A major obstacle in creating resilient networks is the reluctance of certain operators to disclose and share data about vulnerabilities of information systems due to concerns on protection of reputation or competitive advantage reasons. As ENISA states “[t]here remains a lack of a clear framework for effective and timely exchange of information on critical infrastructure protection including responsible and timely disclosure of vulnerabilities.”<sup>79</sup>

92. There are different ways how states can exercise an enabling role in respect of information sharing. Examples of reasonable measures to perform this role may include positive action such as developing and implementing national strategies for proactive management of risks pertinent to information infrastructures and risks inherent in technology, applications and their use. It may also include participation, within the framework of private-public partnerships in the identification, collection and sharing of information on network vulnerabilities, risks to infrastructures or risks emerging from technologies and applications, identification of critical sectors benefiting from such infrastructures (e.g. energy, health, security), determination of risk management responsibilities for each stakeholder, development of good practices for risk assessments as well as other co-ordination activities.

93. The requirement of notification of transboundary risks and vulnerabilities is an indispensable part of any system of preparedness, prevention of and response to transboundary harm. Notification duties are embodied in

a number of international agreements, decision of international courts and tribunals, declarations and resolutions adopted by intergovernmental organisations (Convention on the Law of the Sea,<sup>80</sup> Convention on Environmental Impact Assessment in a Transboundary Context;<sup>81</sup> Convention on the Transboundary Effects of Industrial Accidents;<sup>82</sup> Rio Declaration,<sup>83</sup> OECD Council Recommendation of 14 November 1974 on “Some principles concerning transfrontier pollution”<sup>84</sup>).

94. It should be emphasised that reasonable measures to provide timely notification of risks of transboundary disruption or interference with the Internet’s infrastructure to potentially affected states are concerned with preparedness and management of risk or consequences and are aimed at co-operation and consultation among states concerned. The first principle proposed in the list of general principles of Internet governance, namely protection of fundamental rights and freedoms of Internet users as well as principle A.1 sets the limits for taking measures by states. This would be the response to concerns about surveillance measures expressed at different stage of discussions of the MC-S-CI analysis and proposals.

95. In addition, to identification of risks of causing significant transboundary disruption or interference with the Internet a requirement of notification of such risk should involve an assessment of the possible or actual adverse transboundary effects on the stability, robustness and resilience of the Internet’s infrastructure. This is considered necessary in order to enable a state to determine the nature of the risk or consequences involved and the type of prevention and response measures it should take. A requirement of assessment incorporates a precautionary approach. As it is foreseen to be discharged in the framework of public-private partnerships, it allows for participation the private sector and of the general public through their political representatives and civil society monitoring organisations and movements.

79. ENISA Work Programme 2010, available at <http://www.enisa.europa.eu/media/key-documents/enisa-work-programme-2010>, see page 14.

80. See above, page 16, footnote 66, articles 142, 198.

81. See above, page 17, footnote 70, article 3.

82. 2105 UNTS 457, see article 10.

83. See above, page 16, footnote 65, Principle 19.

84. C (74) 224, see Title E.

### B.3. Co-ordinated management and response

**States should co-ordinate their emergency and incident response policies, provide notification of an emergency and exchange relevant information without delay as well as engage in consultations with a view to achieving mutually acceptable solutions regarding measures to be adopted to respond to significant transboundary disruption of or interference with the stability, robustness and resilience of Internet.**

96. This principle aims at dealing with the management of a significant disruption of or interference with the stability, robustness and interference of the Internet through providing a set of steps which are essential to respond to events. It draws from article 28 of the United Nations Convention on the Law of the Non-navigational Uses of International Watercourses:

“When necessary, watercourse States shall jointly develop contingency plans for responding to emergencies, in co-operation where appropriate, with other potentially affected States and competent international organizations.”<sup>85</sup>

97. Nevertheless, a requirement of co-ordination of emergency and incident response policies would call for anticipatory rather than responsive action and is intended to enable a state to fulfil its due diligence commitment of prevention of transboundary disruption or interference with the Internet’s infrastructure. Although the primary responsibility for developing response policies lies with each state individually, it is felt that these policies and the ensuing response efforts will be more effective if they are developed in co-operation with other states. Emergency and incident response policies could include the establishment of early warning systems, development of common standards (e.g. good practices) on emergency preparedness and recovery as well as promoting their implementation by relevant stakeholders, exchange of knowledge and personnel.

98. The steps of notification and exchange of information and that of engaging in consultations regarding measures to be adopted to respond to technical failures, disruptions or other significant interferences pertain to

the action expected by a state in response to actual emergency situations. This action is justified by the significance or seriousness of adverse effects on the Internet’s normal functioning and is key to the commitment of prevention based on the concept of due diligence which is not a one-time effort but requires continuous efforts.

99. States would be expected to act “without delay” in providing notification of an emergency which means immediately upon a state becomes aware of the situation of emergency so that there will be sufficient time for the states concerned to consult on appropriate management measures and to take proper action. The word “relevant” is intended to emphasise the link between information and the situation and not any information. The information that is required to be exchanged is whatever would be useful for the purpose of management or prevention of the situation of significant disruption or interference with Internet’s infrastructure. States would be free to choose or construct in the spirit of co-operation the means of communication.

100. States would also be expected to enter into mutual consultation in order to agree on measures to manage or respond to situations of disruption or interference with Internet’s infrastructure. Such consultations are needed in order to maintain a balance of the legitimate interests of concerned states in respect of utilisation of critical Internet resources located in their jurisdictions. Their purpose is to enable the states concerned to achieve mutually acceptable solutions regarding management measures, which means those measures that are accepted by these states and based on an equitable balance of interests.

### B.4. Mutual assistance

**As appropriate and with due regard to their capabilities, states should in good faith, offer their assistance to other affected states with a view to mitigate the adverse effects or consequences of disruptions of or interferences with the stability, robustness and resilience of the Internet.**

101. The principle of aid which is aimed at mitigating adverse consequences on the stability, robustness and resilience of the Internet is set out here. Principles of prevention, management and mitigation work together in the international regulation of pollution or environmental harm. In the context of the Internet they are considered to be mutually reinforcing for the preservation of the stability, robustness and resilience of the Internet. The

principle of prevention aims to avoid harms to the Internet’s ongoing functioning e.g. interference with peoples’ access to the Internet or interference with legitimate uses of Internet resources. The principle of aid, on the other hand, aims to mitigate the occurrence of such harms.

102. The level or degree of care that is expected in providing aid to countries affected by disruptions of or interferences with Internet’s stability is proportional to and

85. Doc. A/51/869. C.N.353.2008.



commensurate with the mitigation capabilities of each country. The requirement of solidarity and good faith is an integral part of any international co-operation procedure.

### C. Transnational management of resources that are critical for functioning of the Internet

**States should take all appropriate measures to ensure that the development and application of standards, policies, procedures or practices in connection with the management of resources that are critical for the functioning of the Internet incorporate protections for human rights and fundamental freedoms of Internet users in compliance with the standards recognised in international human rights law. In particular, states should engage in a structured dialogue (methodology) with a view to identify appropriate responses to specific issues that may arise in respect of the management of resources that are critical for the functioning of the Internet.**

103. Freedom of speech on the Internet can be affected by decisions made in connection with the management of resources that are critical for the functioning of the Internet such as domain name addresses and Internet protocol addresses.

104. Domain name registration policies do not provide adequate protections for anonymous speech as anyone who wishes to register a domain name is required to disclose personal information.<sup>86</sup> Policies on resolving disputes between trademark owners and holders of domain names that convey political or cultural criticism of commercial activities involve consideration of nature and content of speech embodied in domain names and contained in websites and has therefore a bearing on the ability of Internet users to engage in critical speech. A recent academic analysis has shown that more than 6 000 domain name proceedings demonstrates that in cases where domain name holders used their domain names to criticise or comment upon certain trademarks or business, companies successfully invoked the Uniform Dispute Resolution Policy to respond to such criticism or commentary in a large number of cases.<sup>87</sup> The developing policy on new generic Top Level Domains, which involves, among others, evaluation of geographical, cultural and political sensitivities, is not constrained by specific protections or safeguards for freedom of expression (and the related freedom of association) or due process.

105. Similarly management policies over ccTLDs do not always include constraints stemming from considerations related to freedom of expression. This was exempli-

fied in a recent case before the French Constitutional Council found unconstitutional the relevant provisions of French law, considering that in the context of the French domain name system, a domain name attribution, renewal, transfer or cancellation process must not only respect intellectual property rights but also freedom of expression and freedom of entrepreneurship.<sup>88</sup>

106. Management and co-ordination of the Internet protocol addresses by private, non-profit and transnational governance entities, may, in respect of certain situations amount to “operational control over what is routed and (therefore what information is accessible) over the Internet”<sup>89</sup> As matters stand, management policies over IP addresses have no constraints stemming from considerations related to fundamental rights and freedoms. Private entities responsible for technical co-ordination have the potential to centralise power over the Internet which may affect freedom of expression of Internet users.<sup>90</sup> Although their policies are developed in bottom-up processes and by multi-stakeholder decision making structures such system of representation embodies the procedural democratic norm of political equality but does not impose checks on decision making that is adverse to fundamental rights. Their foundational documents fail to embody substantive democratic norms such as special protections for fundamental rights, notably freedom of expression.

107. It is, therefore, necessary that states promote the principle that policy-making in relation to the allocation and management of resources that are critical for the

86. Under some ICANN-Registrar Agreements second level domain name holders are required to disclose their names and addresses which is publicly accessible, see for instance section 3.3 of the Registrar Accreditation Agreement, available at <http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#3>.

87. Success by Default: A New Profile of Domain Name/Trademark Disputes under ICANN’s UDRP, a study prepared by Dr. Milton Mueller Syracuse University School of Information Studies, 24 June 2004, available at <http://dcc.syr.edu/PDF/marke-report-final.pdf>. See section 5, at page 26.

88. See above, page 7, footnote 9.

89. See *Building a new governance hierarchy; RPKI and the future of Internet routing and addressing*, 7 September 2010, available at <http://www.internetgovernance.org/pdf/RPKI-VilniusIGPfinal.pdf>. The authors, Milton Mueller, Brenden Kuerbis and Michel van Eeten, argue that Resource Public Key Infrastructure (RPKI), a routing security technology, which is currently implemented by three Regional Internet Registries links resources certificates to the institutions that control IP address resource allocation. This technology, could be used to give the latter institutions operational control over what is routed on the Internet. Arguably, technical co-ordination may attract influence by different political interests without well defined rules or constraints to protect basic human rights.

90. *Id.*

functioning of the Internet should articulate the public policy interest that it seeks to advance and formulate the policy in such a way that restrictions to fundamental rights and freedoms are made only in the public interest and in compliance with the principle of proportionality. In this connection, Article 4 of ICANN's Articles of Incorporation should be recalled which states that "The Corporation shall operate for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law and, to the extent appropriate and consistent with these Articles and its Bylaws, through open and transparent processes that enable competition and open entry in Internet-related markets. To this effect, the Corporation shall co-operate as appropriate with relevant international organizations."<sup>91</sup>

108. The proposed section C affirms also that not all issues that are pertinent to the preservation of the public interest in the context of the management of resources that are critical for the functioning of the Internet are addressed here. It is felt that, a framework of international co-operation in this area should have in-built flexibility for action in the future while constructing only a general commitment to co-operate at this stage. For example, one of the issues that may be mentioned in this context is the identification of appropriate confidence building measures in the root server system. While some of the general principles that were mentioned in the context of Internet disruptions could apply here (for instance, promoting enhanced interaction and co-operation among stakeholders, formal and informal meetings, exchange of information and consultation) other more appropriate measures may be identified as a result of a structured dialogue and co-operation.

## V. Protection of cross-border flow of Internet traffic

**States should take all appropriate measures to ensure that activities taking place within their effective jurisdiction do not interfere with the cross-border flow of Internet content, services and applications in other states. In this context, states should exchange information and engage in consultation and dialogue. In particular, states should co-operate with each other and with relevant stakeholders to ensure that Internet users receive information about restrictions to their access to Internet content, services and applications which may occur as a consequence of decisions taken in another jurisdiction and, where possible and applicable, should be granted effective remedies.**

109. This section is based on the premise that the free flow of information is crucial to the exercise of freedom of expression as well as to the promotion of democratic values regardless of frontiers. There are, however, restrictions imposed on the traffic flow in different jurisdictions. Such restrictions are based on different grounds varying from consumer protection to public safety. As a result access to certain types of information that may contain objectionable political or social content in one jurisdiction may be limited with spill over effects in other jurisdictions.

110. The content of this section is articulated in the form of a policy objective – national policies on access to information should be designed in a manner that recognises the global nature of the Internet and seek solutions that enable users' access to content, services and applications of their choice. This section does not yet identify the measures to implement the stated policy objective. This should be part of further examination of item (ii) of the Terms of Reference of the MC-S-CI as proposed in paragraph 8 of this report.

## VI. Conclusions and recommendations

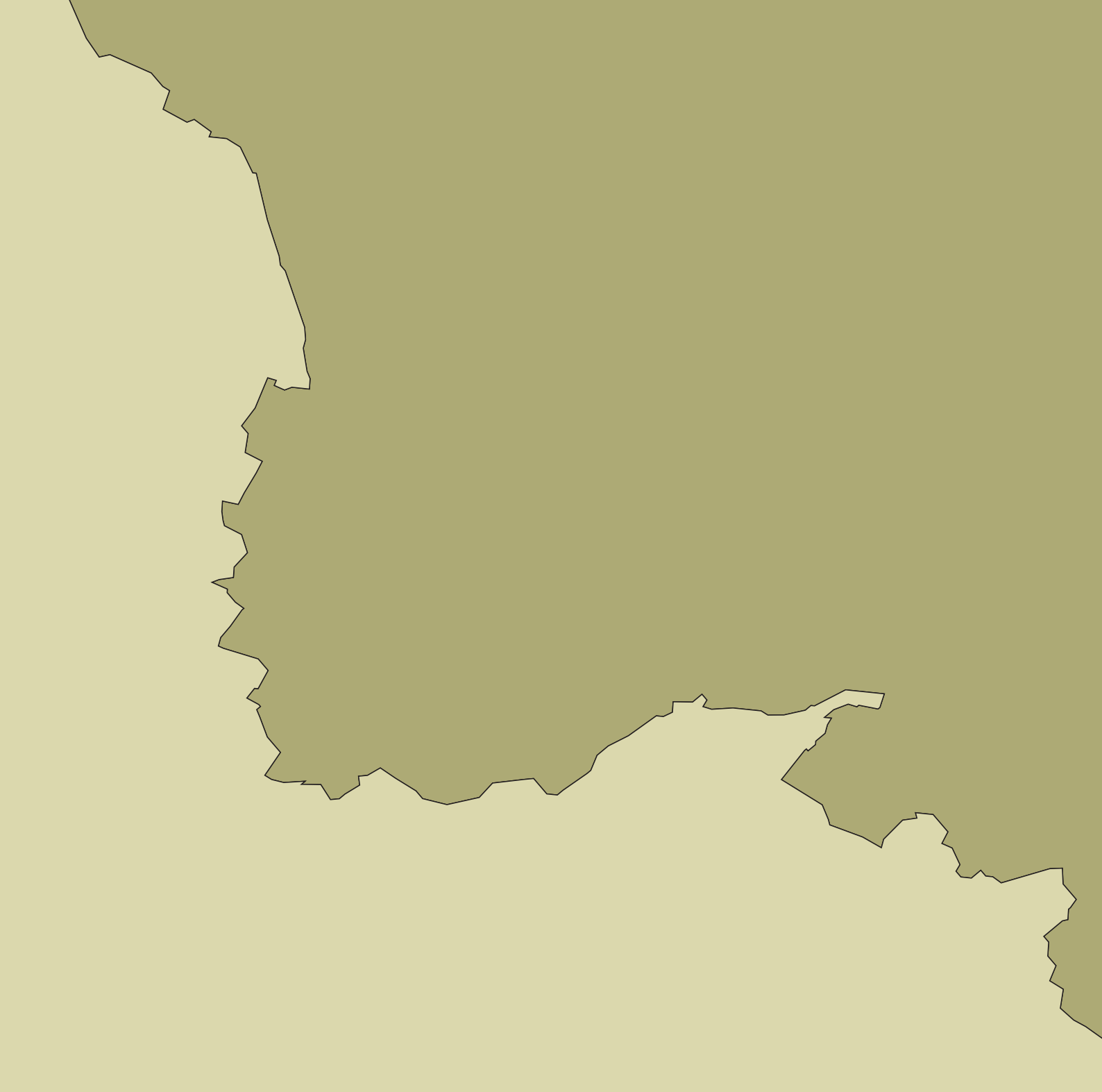
111. The MC-S-CI concludes that international and multi-stakeholder co-operation is needed in order to preserve and reinforce the protection of cross-border flow of Internet traffic and the stability and ongoing functioning of the Internet as a means to safeguard freedom of expression and information regardless of frontiers.

112. On that basis, the MC-S-CI recommends to the CDMC:

- to continue action aimed at drawing up new international legal instruments on cross-border Internet, which may include the development of mechanisms to identify issues where commitments or regulation are needed and for clarifying what the "respective role of governments" is in the development of such commitments and regulations;

91. The Articles of Incorporation as revised on 21 November 1998 are available at <http://www.icann.org/en/general/articles.htm>.

- to prepare, as a first step, a draft Committee of Ministers' Declaration on the general principles of Internet governance and a draft Committee of Ministers' Recommendation on international co-operation in respect of resources that are critical for the functioning of the Internet, on the basis of the analysis included respectively in Parts III and IV of this report;
- to continue the examination of the feasibility of drafting instruments designed to preserve or reinforce the protection of cross-border flow of Internet traffic, openness and neutrality;
- to organise a dedicated event to discuss with stakeholders the feasibility of international law responses to issues related to international co-operation in respect of resources that are critical for the functioning of the Internet.



**Directorate General  
of Human Rights and Legal Affairs  
Council of Europe  
F-67075 Strasbourg Cedex**

[www.coe.int/justice](http://www.coe.int/justice)