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

Discussion paper of the

Council of Europe
Ad-hoc Advisory Group on Cross-border Internet
(MC-S-CI)[*]

for

Workshop no. 60 A proposal for setting a standard of care in international law for cross-border Internet

Internet Governance Forum
14-17 September 2010
Vilnius

[*] The members of the Ad Hoc Advisory Group on Cross-border Internet are: Wolfgang Kleinwächter (Chair), Professor at the University of Aarhus, International Association for Media and Communication Research; Christian Singer, Director at the Department III/PT2 Telecommunications Law, Federal Ministry of Transport, Innovation and Technology of Austria; Rolf H. Weber, Professor, Faculty of Law, University of Zurich, GIGA net and Michael V. Yakushev (Vice-Chair), Chairman of Board, Coordination Center for the ccTLD '.ru'.

Introduction

The ministers responsible for media and new communication services participating in the Reykjavik Conference in May 2009 adopted a Resolution on Internet governance and critical Internet resources which recalls the obligation and commitment of member states to secure to everyone within their jurisdiction their fundamental rights and freedoms contained in the European Convention on Human Rights (ECHR).

In this context, they underlined the importance of freedom of expression and information regardless of frontiers while at the same time stressing that access to the Internet is an important means by which large numbers of users are able to fully exercise and benefit from this right. They added that acts or events which could block or significantly impede Internet access to or within fellow members of the international community may have significant implications under Article 10 of the ECHR, which guarantees the right to freedom of expression and information.

The Resolution refers to a shared responsibility of Council of Europe member states to take reasonable measures through multi-lateral cooperation to ensure the ongoing functioning of the Internet and, in consequence, the delivery of the public service to which all persons under their jurisdiction are entitled. On this basis, the participating ministers called on all state and non-state actors to explore ways to ensure that critical Internet resources are managed in the public interest, and as a public asset, in full respect of international law, including human rights law. This could include, if appropriate, international supervision and accountability of the management of those resources.

In response to these proposals, the Committee of Ministers of the Council of Europe invited the competent intergovernmental cooperation body, the Steering Committee on the Media and New Communication Services (CDMC), to give priority attention 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).

In this connection, an Ad-hoc Advisory Group on Cross-border Internet (MC-S-CI) was established reporting to the CDMC. This group is made up of selected Internet governance experts, including government, industry, civil society and academia and has been mandated to consider and make proposals on these matters.

Having examined the issues falling under its mandate, the MC-S-CI considers that disruption of and interference with Internet infrastructure and resources within one jurisdiction can have an impact on the stability, security and resilience of Internet across borders and ultimately affect negatively the effective enjoyment of fundamental rights and freedoms. Moreover, processes and decisions on the management of critical Internet resources, which are taken by private sector entities, may have a direct bearing on the exercise of fundamental rights and freedoms.

Because of the transboundary nature as well as complex interdependencies of the network, the challenges to the protection of critical Internet resources can be handled effectively only on a multilateral basis and through international co-operation. The development and implementation of common practices, rules and standards, regular cross-border exchange of knowledge and expertise, experience and technology sharing, exchange of personnel, consultation and participation in joint exercises can significantly enhance the national capabilities for dealing with network vulnerabilities and incidents.

National agencies whose mission is to address emergencies related to the protection of critical infrastructure, such as computer emergency teams, do currently engage in patterns of co-ordination and co-operation similar to those mentioned above[1]. However, these interactions are based on technical and operational trust rather than on legal obligations. International law lacks a framework of commitments for effective and timely exchange of information, including timely disclosure of vulnerabilities of and risks to the critical Internet resources, aid in cases of technical failure, co-ordination of incident response policies and measures or maintenance of minimum incident response capabilities.

The concept of state responsibility for preventing significant transboundary harm, under a due diligence standard of conduct, is well established in international law.[2] Moreover, international law provides a wealth of legal concepts and models that are useful in crafting a functioning legal regime for the protection of critical Internet resources.[3]

In light of these considerations, the MC-S-CI proposes to develop a legal framework for inter-state co-operation to preserve and reinforce the protection of critical Internet resources. Such legal framework should build on the principles developed in the framework of the World Summit on the Information Society, operate within the boundaries set out by the principles of Internet governance which are generally recognised by the Internet community and enable the continuous functioning of the Internet. The political conditions for creating a legal mechanism for post-incident liability may not be met yet. Nonetheless, states can, at this stage, undertake to engage in consultation with a view to develop international law on responsibility and liability for the mitigation of and compensation for damage and the settlement of related disputes.

[1] Examples of such interaction are those taking place in the framework 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. Also, the European Network and Information Security Agency of the European Union functions on the basis of a model of co-operation amongst national computer emergency teams which builds confidence in its system of technical advise by virtue of its independence, quality of advice and transparency of procedures.

[2] See the International Law Commission (ILC) Articles on Prevention of Transboundary Harm from Hazardous Activities adopted in 2001, U.N. Doc. A/56/10 Supp. No. 10 (2001) and the ILC Articles on State Responsibility annexed to the UN General Assembly Resolution Responsibility of States for Internationally Wrongful Acts, GA. Res. 56/83, U.N.Doc. A/RES/56/83 (12 December 2001.

[3] For example, the notion of equitable and reasonable use of critical resources is widely accepted in international environmental law. Conventional and customary law elaborate international preventive obligations relating to the protection of the environment and corresponding duties of states, which include cooperation in scientific research, exchange of information, notification of risks, environmental impact assessment, consultation, risk assessment, warning and emergency assistance, emergency preparedness and mutual assistance.

The main elements of the MC-S-CI's proposal are outlined below in two parts. Part I sets out the general principles of Internet governance with which the exercise of the shared responsibilities of states should be balanced. Part II elaborates on the duties of states which are essential for balancing the interests of all actors concerned (states and other stakeholders) by giving them the opportunity to take preventive, preparedness and incident response measures.

Part I

General principles of Internet Governance

1. Protection of fundamental rights and freedoms

Human rights and fundamental freedoms, which are guaranteed by 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 should be guaranteed in all Internet governance processes. The availability, integrity and ongoing functioning of the network and the unimpeded access to Internet content, services and applications are conditions for the enjoyment and full exercise of fundamental rights and freedoms on the Internet.

2. Multistakeholderism

Internet governance needs the involvement 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 governmental and non-governmental organisations participate in a collaborative way. Each single Internet issue needs its special multistakeholder Internet governance mechanisms; there is no "one size fits all" governance model for all Internet related issues.

3. Universality of the Internet

The Internet has developed into a space of freedom for the Internet community worldwide and has become one of the driving forces for economic growth 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, each state has the responsibility to ensure that activities within its jurisdiction do not cause damage to the use of Internet resources beyond its boundaries.

4. Stability and security

As citizens' and economic activities rely significantly on the Internet, its stability, security and resilience have become crucial objectives. The vulnerabilities of the Internet infrastructure and the criticality of its resources have come to the forefront of concerns of the private sector and states which should be able to respond to Internet users' legitimate expectation that Internet policy will reflect the public interest and that critical Internet resources will be managed as a public asset for the Internet community as a whole. In order to preserve the stability of the infrastructure and the functioning of the network as well as users' trust on the Internet, it is necessary to promote international and multistakeholder co-operation as well as technological measures and education of Internet users.

5. Empowerment of Internet users

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. Core societal values such as the free exercise and effective enjoyment of human rights and fundamental freedoms, the protection of human dignity, free and autonomous development of identity, rule of law, democracy and protection of cultural heritage should be preserved in the context of development of new services and technologies. Citizens should be empowered to interact with new technologies.

6. Openness and interoperability of the Internet

Global, open and non-proprietary core Internet standards and protocols are key features of the Internet architecture. They allow for the independent development of applications, content and technological innovations. Protocols and standards should continue to be developed in a framework of pluralistic, transparent collaborative processes and with multiple stakeholders according to the principle of subsidiarity. The fundamental functions and the core principles of the Internet must be preserved in all layers of the Internet architecture with a view to guaranteeing the interoperability of networks in terms of infrastructures, services and contents. They should be guiding principles for international policy making.

7. Network Neutrality (end-to-end principle)

The Internet network provides basic and unrestricted data transport while leaving choice of content, applications and other forms of user-specific information processing to the devices attached to the endpoints of the network. This principle 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 as well as the dissemination of knowledge. The end-to-end principle should be protected globally.

8. Decentralised management responsibility

Internet infrastructure, software and services are owned and administered by autonomous entities, which in turn leads to decentralised network operation and policies. The private sector has contributed to promote the universality of the Internet, to ensure the robustness and resilience of its infrastructure and networks and to unleash economic potential and develop democratic processes. The private sector should retain its leading role in the technical and operational matters while being accountable to the Internet community for its actions that have an impact on public policy.

9. Development and bridging the digital divide

Internet-related public policies and decisions should ensure full participation of developing countries. International co-operation opportunities should be explored further with the aim of bridging the digital divide, reducing differences in national Internet resilience capabilities and achieving a coherent approach to network stability and security at a global level.

10. Cultural and linguistic diversity

Internet should be a space for expression, exchange and interaction of all cultures and languages. 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.

11. Responsibilities of states

States have the responsibility to ensure that human rights and fundamental freedoms of their citizens are guaranteed both in offline and online activities and regardless of frontiers in accordance with international human rights law. 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. As guarantors of human rights, they should also ensure accountability of private entities; this is also relevant as regards citizens' legitimate expectation that Internet services be accessible and affordable, secure, reliable and ongoing (public service value of the Internet) and its corollary expectation that Internet policy will reflect the public interest and the critical Internet resources will be managed as a public asset for the Internet community as a whole.

12. International co-operation

Being a transnational communication network, the challenges to the protection of fundamental rights and freedoms, universality, security, stability and openness of the Internet can be effectively addressed only on a multilateral basis and through common responses, notably through co-ordination and co-operation in the prevention of,

preparation for and provision of responses to disruptions of and interferences with critical Internet resources. International co-operation should build on the existing mechanisms or arrangements on Internet governance in a spirit of complementarity and co-operation.

Part II

Duties of States with respect to the protection of critical Internet resources in a cross-border context

A – General principles

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

2. 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 to protect critical Internet resources and cross-border flow of Internet traffic.

3. 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, including the establishment of suitable monitoring mechanisms, to implement these provisions.

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

B – International co-operation

(i) Protection of critical Internet resources

1. States should co-operate with a view to support the development and implementation of common standards, rules or practices[4] and the establishment of co-operation and

[4] Examples could include facilitating and participating in the development of common standards (i.e. good practices) for information sharing, incident reporting and promoting their implementation in the public and private sector; supporting and facilitating the development and implementation, in conjunction with private sector, of harmonised resilience measurement methodologies or techniques; promoting, facilitating and participating in the development of common standards or practices for deploying Internet design principles (principles on end-to-end resilience) and technologies that improve the security and resilience of the Internet network (e.g. DNSSEC or resilient routing technologies); and providing market incentives for wide take-up of security technologies as well as promoting research in this context.

dialogue platforms[5] designed to preserve and strengthen the stability, security and resilience of the Internet.

2. States should, in co-operation with relevant stakeholders, take all reasonable measures to ascertain whether activities involving risk of causing significant transboundary disruption to the stability, security and resilience of network resources are taking place within their jurisdiction, assess the possible adverse effects or consequences that such activities may have and provide prior and timely notification and relevant information to potentially affected states[6].

3. States should co-ordinate their emergency and incident response policies[7], exchange relevant information and engage in consultations with a view to achieving mutually acceptable solutions regarding measures to be adopted to respond to technical failures or significant transboundary disruption of the stability, security and resilience of Internet. States should, in good faith, offer their assistance to mitigate the adverse effects or consequences of these events.

(ii) Transnational management of critical Internet resources in the public interest

States should take all appropriate measures to ensure that the development and application of standards, policies, procedures or practices in the framework of the management of the domain name space and Internet protocol address space incorporate protections for human rights and fundamental freedoms of Internet users in compliance with the standards recognised in international human rights law[8].

(iii) Prevention of and response to cyber attacks

1. 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

[5] Examples could include promoting and facilitating co-operation platforms or mechanisms on awareness raising, information sharing, incident management and reporting capabilities, international exercises; setting up public-private co-operation platforms. With respect to root-servers, states should take all reasonable measures to ensure that the public interest of the global Internet community is preserved in the operation of root servers located within their respective jurisdiction as well as in activities related to the co-ordination of the root zone file. States should facilitate the development of confidence building measures in the root server management system, in particular by promoting enhanced interaction and co-operation among stakeholders, through formal and informal meetings, exchange of information, consultations and other forms of co-operation.

[6] Examples of reasonable measures could include risk management preparedness measures, for example developing and implementing national strategies for proactive management of risks pertinent to information infrastructures and risks inherent in technology, applications and their use. This may include the establishing of private-public partnerships tasked with 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 co-ordination activities..

[7] Examples could include facilitating and participating in the development of common standards (e.g. good practices) on emergency preparedness and recovery, promoting their implementation by relevant stakeholders, promoting and facilitating multistakeholder dialogue on co-operation, information sharing and mutual assistance during incidents.

[8] States should promote the principle that policymaking in relation to the allocation and management of critical Internet resources 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.

transboundary consequences for the stability, security and resilience of network resources as well as freedoms of Internet users in other states[9].

2. States should take all reasonable measures to prevent cyber attacks which use resources located in their respective territories[10]. In particular, states should ascertain whether activities involving risk of causing significant transboundary interference with Internet resources are taking place within their jurisdictions, assess the adverse effects or consequences that such activities may have and provide prior and timely notification and relevant information to potentially affected states.

3. States should exchange relevant information and enter into consultations with a view to achieving mutually acceptable solutions regarding measures to be adopted to prevent or respond to cyber attacks or other activities which may cause significant transboundary interference with Internet resources, or at any event to minimise the risk thereof.

4. As appropriate and with due regard to their capabilities, states should co-ordinate their incident response efforts and offer their assistance to other affected states with a view to mitigate the adverse effects or consequences of cyber attacks.

(iv) Protection of cross-border flow of the Internet traffic

1. States should take all appropriate measures to ensure that activities taking place within their 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 applicable, should be granted effective remedies.

[9] Examples could include accession to other relevant international law instruments (such as to the Budapest or Cybercrime Convention) or participation in the development and implementation of Internet user education and public awareness programmes, promotion and facilitation of dialogue with stakeholders.

[10] See also footnote 7. States should co-operate with a view to enhancing their capacity to prevent and respond to cyber-attacks, including through exchange of information and best practices, consultation, co-ordination of risk assessment, network stability and recovery strategies, co-ordination and co-operation in the framework of international cyber response forces, organisation of joint exercises with the participation of all actors and other measures of a preventive and emergency preparedness character.