European principles and guidelines for Internet resilience and stability

- Version of March 2011 -

PREAMBLE

On 30 March 2009, the Commission announced, via Communication COM(2009) 149, the launch of an action plan on Critical Information Infrastructure Protection. The main goal of the action plan – running from 2009 until 2011 – is to focus on a number of urgent activities which, according to the Commission, are necessary in order to strengthen the security and resilience of vital ICT infrastructures. The action plan was broadly supported by the Council of the European Union in December 2009.

The CIIP action plan is part of a more extensive strategy of the European Commission to strengthen network and information security in the information society. It follows and complements Communication COM(2006) 251 on a Strategy for a Secure Information Society, the legislative and non-legislative initiatives to fight cyber-crime and ensure online safety, and feeds into the "trust and security" objectives of the Digital Agenda or Europe, one of the flagship initiatives of the Europe 2020 strategy of the European Commission (COM(2010) 2020).

In the context of the CIIP action plan, the Commission proposed to work with Member States to identify European principles and guidelines for the resilience and stability of the Internet, with the intent – among others – to strengthen a common European approach to the matter. Furthermore, these principles and guidelines should be used as a basis for international discussion and cooperation with other States, with International organisations and, where appropriate, with global private-sector organisations – by using existing *fora* and processes, such as those related to Internet Governance, where relevant – with the objective to agree on a global set of principles for the resilience and stability of a truly globally interoperable Internet at the global level.

This document is the result of several months of discussion, debate and reflections with the national experts participating in the European Forum for Member States (another one of the initiatives launched via the CIIP action plan). The principles and guidelines proposed here are without prejudice, and should on the contrary be interpreted and implement in light of, the relevant *acquis* of the European Union, as transposed in its Member States.

This document should also serve as a tool for all stakeholders to frame their activities, as they relate to the stability and resilience of the Internet. Such activities should be based on a good understanding by all stakeholders of the issues under their control that impact on the stability and resilience of the Internet; on the responsibility by all stakeholders to take appropriate actions, based on risk assessment, to prevent damages to the Internet and its users; and on an open and transparent approach to policy-making in the areas of concern to the stability and resilience of the Internet.

THE INTERNET

For the purposes of interpreting and applying the principles for Internet resilience and stability ("the Principles"), the Internet is to be understood as the global and public network of networks whose nodes communicate with one another using the Internet Official Protocol Standards and are identified by a globally unique address assigned via the relevant process (currently, the IANA function).

Explanatory note

The concept of Internet Official Protocol Standards should be interpreted with reference to the Request for Comments 5000 of the Internet Engineering Task Force.[1] It is without prejudice to future political, legal or technological developments concerning one or more of the elements of the definition provided above.

The concept of "resilience" is generally understood as "[t]he ability of a system [in this case the Internet, as defined above] to provide and maintain an acceptable level of service, in face of faults (unintentional, intentional, or naturally caused) affecting normal operation".[2]

The concept of "stability" can be understood as "the ability of a system [in this case the Internet, as described above] to remain in a constant state unless affected by disturbance and to return to that constant state when disturbance is removed". The property of stability must be complemented by a certain degree of elasticity, lest the system (the Internet) becomes completely inflexible to potentially useful changes.[3]

Although the concepts of "resilience" and "stability" refer to slightly different properties of a system (the Internet) they cannot be totally dissociated from one another: just to make one example, providing an acceptable level of service in the face of faults – i.e. being "resilient" – is normally dependent on the ability of a system to regain its original state after a specific amount of time.

Furthermore, the following principles (as well as their concrete implementation, whatever form it may take) should be based on the understanding that the Internet, as an open, global and distributed network of networks with limited points of central control/failure, has become an essential element of the daily life of European citizens, businesses and public authorities. The dependence of our society on this basic ICT infrastructure, as well as on many of the services that could not exist without it, calls for a real and inclusive engagement of all Internet stakeholders – all those stakeholders which have a legitimate interest in the well-functioning of the Internet – having due regard to their respective roles and responsibilities, in order to ensure the stability and resilience of the Internet.

The Principles constitute an attempt to build the basis of proper governance of the technological, social, economic, legal and political challenges to achieve this goal and of the best ways to tackle them.

[1] See http://datatracker.ietf.org/doc/rfc5000/.

[2] See http://www.enisa.europa.eu/act/res/files/glossary.

[3] As might be the case, for example, when routing paths from one end-point to the other need to change because intermediate nodes or network paths have failed.

Coherence with Core European Values and Interests

Activities of all EU stakeholders, and in particular the activities of public authorities, concerning the stability and resilience of the Internet shall be guided by the overarching goal of promoting the core values and interests of the European Union.

Explanatory note

These values include peace and the well-being of the people of the EU, as well as the respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.[4]

In particular, all activities aimed at enhancing the stability and resilience of the Internet must do so in accordance with the Charter of Fundamental Rights of the European Union of 7 December 2000, as adopted at Strasbourg, on 12 December 2007,[5] as well as with all other relevant National, European and International instruments for the protection of human rights, fundamental freedoms and civil liberties. This entails full respect for, *inter alia*, the rights to privacy and the protection of personal data, the right to receive and impart information and the right to a due process.

Care must be taken to choose technological, legal and/or organisational solutions that will allow most effectively safeguarding the stability and resilience of the Internet while at the same time respecting these core values. While certain solutions may theoretically result in increased stability and resilience of the Internet (e.g. massive monitoring and surveillance of Internet activities, aggressive profiling of Internet users, filtering and blocking of Internet connections and communications), their implications for these core values, in particular for individual autonomy and freedom and for democratic transparency, as well as the actual proportionality of these measures to the intended goals, must be carefully assessed *ex ante*.

[4] See art. 2 and art. 3 of the Treaty of the European Union (TEU).

[5] See art. 6 of the Treaty of the European Union (TEU).

THE GLOBAL CONTEXT

The Principles shall take into the utmost account existing principles, guidelines, regulations and other instruments at the global level.

Explanatory note

A number of global principles, guidelines, regulations and other instruments have been devised in the past years. Although some of them are not immediately applicable to the Internet and/or fully coherent with, and conducive to, European values and interests, it is nonetheless important to keep in mind that the Principles being discussed here do not live in a vacuum, but must strive to achieve coherency with this global context.

INTERNATIONAL COOPERATION

The Principles should be used as a basis for international discussion and cooperation with other States, with International organisations and, where appropriate, with global private-sector organisations, with the objective to agree on a global set of principles for the resilience and stability of a truly globally interoperable Internet. International cooperation on resilience and stability of the Internet should be promoted by all relevant stakeholders, as the Internet is a truly global infrastructure.

Explanatory note

The Internet is a global infrastructure. Threats to its resilience and stability cannot be properly addressed at the national or even at the European level, alone. At the same time, it is essential to avoid that legitimate concerns for the security of States and the wellbeing of citizens be used as a justification to fragment the Internet. The principles for Internet resilience and stability, which Member States of the European Union will agree to, should be used as a basis for international discussion and cooperation with other States, with International organisations and, where appropriate, with global private-sector organisations, with the overarching objective to agree on a global set of principles for the resilience and stability of a truly globally interoperable Internet. Clear principles at the global level would ensure that National choices will be guided by a better understanding of the potential effects outside of National borders.

I. A MATTER OF PUBLIC POLICY

ROLE OF PUBLIC AUTHORITIES

The fundamental importance of the Internet for society calls on public authorities to cooperate with relevant stakeholders and be actively involved in the key decision-making processes that underlie the development and functioning of the Internet, including with regards to its resilience and stability, having due regard to the cross-border and global nature of this distributed and shared resource.

Explanatory note

Public authorities have both the right and the duty to create the conditions to ensure that the opportunities opened by the Internet can be truly exploited by all citizens, including by ensuring an appropriate level of preparedness in the face of potential threats to the stability and resilience of the Internet, including by implementing appropriate controls and safeguards.

To this end, public authorities shall provide a clear, stable and long-term framework for the activities of all stakeholders (see the principles on the "Importance of a multi-stakeholder approach" and on "Responsibility and accountability") that relate to the resilience and stability of the Internet, so that every stakeholder can develop reasonable expectations concerning their rights and obligations and adjust their plans accordingly.

Given the distributed nature of the Internet, both from the purely technological and from the administrative and organisational points of view, public authorities should carefully consider in which situations bottom-up, distributed approaches to ensuring the stability and resilience of the Internet would be possible and preferable to top-down, centralised approaches.

Furthermore, given the cross-border and global nature of the Internet, public authorities must ensure that such framework is coherent at the EU level as well as at the global level (see principle on "International Cooperation"). The achievement of National interests, which is obviously a perfectly legitimate objective for States, may not always be the best way to ensure the resilience and stability of a global infrastructure such as the Internet – which is not a private garden, but rather a complex ecosystem in which every participant must work together (see the principles on "Tools and Instruments" and "International Cooperation") to ensure that their shared interests are fulfilled, including by making recourse to supranational decision-making processes, as appropriate.

IMPORTANCE OF A MULTI-STAKEHOLDER APPROACH

It is recognised that all Internet stakeholders have an important role to play in ensuring the stability and resilience of the Internet*[6]*. That's why public authorities should work with private sector, civil society and international organisations in order to pursue the objective of ensuring the stability and resilience of the Internet

Explanatory note

Private-sector leadership in the development and day-to-day management of the Internet, including for what concerns its resilience and stability, has proven to be a successful model and should be preserved. In particular, a continuous dialogue with the technical community involved in the research and development of protocols and specifications related to the stability and resilience of the Internet (including the Internet Engineering Task Force) must be sought.

Furthermore, the role of civil society (including non-commercial, non-governmental organisations) in enhancing the stability and the resilience of the Internet and in contributing to the understanding of the complex interplay and the necessary balance between the core values touched upon by these processes should be fully recognised and encouraged.

Each stakeholder must be aware of his/her own responsibility and be accountable for his/her own actions and for the effects that such actions have on the stability and resilience of the Internet as a whole.

[6] In line with the conclusions of the World Summit on the Information Society, it is understood that the management of the Internet, including for what concerns its stability and resilience, should be multilateral, transparent and democratic, with the full involvement of, and effective cooperation among, public authorities, the private sector, civil society and international organisations, according to their different roles and responsibilities and leveraging on their expertise.

IMPORTANCE OF INCENTIVES

Given the extremely dynamic nature of the Internet, public authorities should resort to regulation only when strictly necessary to pursue the objective of ensuring the stability and resilience of the Internet, taking into account its cross-border and global nature, too. The application of appropriate social and economic incentives that could achieve the same goal should be considered, as appropriate. Coordination at the EU level will avoid fragmentation of the internal market.

Explanatory note

This principle is without prejudice to the freedom of Member States to use the tools they find most appropriate in order to achieve the goal of ensuring the stability and resilience of the Internet; rather, it is highlighted that in several cases other forms of intervention, such as the use of social and economic incentives (e.g. public procurement policies with adequate security requirements, limited exemptions from liability for organisations which put in place minimum security standards, etc) might be more appropriate and effective and could in any case be complementary to regulation.

II. A NECESSARY WELL-FUNCTIONING MARKET

STRENGTHENING THE EUROPEAN ICT SECURITY INDUSTRY

The resilience and stability of the Internet can significantly benefit from a strong European ICT security industry. A well-functioning market, based on appropriate levels of transparency and proper information to users, is a fundamental precondition for the development of such industry.

Explanatory note

Nowadays, a significant part of hardware and software that is used on the Internet is produced outside Europe. This is especially true for central network components which form the basis for a resilient and stable Internet. From a security perspective, Europe (as any other large region of the world) should have its own highly productive and competitive industry. This will become even more important as operators of Critical Infrastructures start using the Internet as a communication infrastructure on which critical processes depend on.

A strong European ICT industry may also enhance the diversity of supply chains, reduce the dependence on technological monocultures and raise the number of skilled experts in the field.

GOOD RISK MANAGEMENT

Good risk management by both the public and private sector is critical to internet resilience. All stakeholders have a role to play in ensuring that risks are understood, measured and mitigated against appropriately. Good risk management includes, but is not limited to, being aware of societal dependencies on the Internet; ensuring responsibility and accountability of each stakeholder for the effects of its action on the stability and resilience of the Internet; putting in place reasonable and proper contingency and fall-back strategies; striving for an appropriate diversity of sources in the supply chain of the technologies used on the Internet.

Explanatory note

All stakeholders have their own unique set of risks to manage and should adopt an all-hazard approach to risk-management. This is particularly true for operators of all the relevant networks that form the Internet, as well as for operators offering services which are essential for ensuring the stability and resilience of the Internet.

Good risk management includes, but is not limited to:

1) the identification of technological components which must be available for vital societal processes to continue – e.g. Internet Exchange Points, the Domain Name System, the routing infrastructure of the Internet and others as appropriate. The cross-border nature of the Internet calls for a strong cooperation among public authorities in this identification activity.

2) The creation and strengthening, at all levels, of a "risk management culture", empowering all stakeholders to develop an appropriate level of preparedness and preventive/reactive capabilities against threats and disruptions to the stability and resilience of the Internet, whatever their nature is, in relation to the assessed risk.

3) A continuous fact-based assessment of the economic and social dimension of the resilience and stability of the Internet. The collection and sharing of trusted data, including on Internet threats, vulnerabilities and incidents thereof, is an essential element of this assessment.

4) The realisation that, due to its specific characteristics, using the Internet for certain critical functions and services may not always be the best possible choice. At the very least, those responsible for such critical functions and services should ensure a proper contingency strategy, including the use of alternative communication infrastructures, to cope with Internet failures.

5) Understanding that the availability of open standards, the diversity in the supply chain of technologies that implement such standards, the avoidance of one single technology and the recourse to multi-vendor solutions (especially for high-availability infrastructures) are essential to ensure, on the one hand, that States are in a condition to guarantee the stability and resilience of the part of the Internet for which they may claim (or be held to) some form of responsibility, and on the other hand that any national responsibility does not produce any form of fragmentation of the Internet. Notwithstanding the role of public authorities, the private sector should in any case be mindful about the reliability and potential vulnerabilities that may be present in particular products or services they rely on.

OPENNESS AND INTEROPERABILITY

All stakeholders, and in particular public authorities, must strive to preserve openness and interoperability in all their activities related to the stability and resilience of the Internet.

Explanatory note

The openness of the Internet and the interoperability of its constituting elements, i.e. the possibility, save for well-specified technical constraints and legal obligations, for any connected person or organisation to transmit and receive information and to use applications of their choice (thus allowing the creation and deployment of new applications, services and, in general, social activities by users) are both a challenge and an opportunity for the resilience and stability of the Internet.

While it cannot be denied that this openness may result in unwanted or harmful traffic, which may possibly result in threats to the resilience and stability of the Internet, it must be also recognised that the same openness allows extremely efficient and innovative responses to such threats to take place – for example, the usage of distributed "reputation lists" for blocking spam messages or the distributed monitoring of Internet route announcements, which, in the cases of involuntary errors or deliberate hijackings leading to Internet traffic being routed to the wrong recipient(s), allows remarkably quick countermeasures to be put in place.

It must also be recognised that the openness of the Internet, notwithstanding the potential problems it may create, serves a number of purposes – for example, the right to receive and impart information – which have equal, if not greater, value than preserving the stability and resilience of the Internet *per se*.

OPEN STANDARDS

All stakeholders, in particular public authorities, should recognise that the stability and resilience of the Internet depends crucially on the widespread availability and uptake of open standards, which should be designed with strong security and privacy requirements from the design phase.

Explanatory note

The development of different but interoperable implementations of such standards for the Internet, at all layers, will avoid a "technological monoculture" that constitutes a serious risk for the stability and resilience of the Internet.

It is recognised that the meaning of the term "open standard" is not universally shared and that different organisations may use different definitions. In this context, the term implies that the standard is defined and maintained using an open and transparent process.

Furthermore, the principle should be interpreted in light of its purposes: ensure wide interoperability of Internet technologies, thus stimulating competition and ultimately the quality of products and services using such standards; ensure that security and privacy concerns are embedded into standards-setting processes from the inception ("security by design" and "privacy by design").

III. COOPERATION

COOPERATION AND MUTUAL ASSISTANCE

Cooperation is an essential element in maintaining and strengthening the stability and resilience of the Internet. Sharing of good strategic and operational approaches would be beneficial for all involved stakeholders and is strongly encouraged. Furthermore, public authorities should put in place operational mutual assistance strategies with the most appropriate geographical scope, in order to ensure appropriate and coordinated recovery and continuity in the face of severe disruptions.

Explanatory note

Cooperation should take place both among the same category of stakeholders, e.g. between Member States, and among different categories of stakeholders. Without prejudice to the prerogatives of each stakeholder, in particular the division of competences between Member States and the European Union, and having due regard to the avoidance of duplication with other *fora*, mechanisms and/or processes, such cooperation should complement the work of national fora and be coordinated in a structured way at the European level. It should be based on trust between the different interlocutors. All appropriate technical and organisational measures, e.g. the use of the "traffic light protocol", should be taken in order to develop and maintain such trust.

TOOLS AND INSTRUMENTS

Besides sharing of information and good practices, more concrete efforts, including the development of appropriate measurement indicators, corresponding benchmarking activities, as well as the running of National, European and Global exercises should be pursued.

Explanatory note

In order for the principles for Internet resilience and stability to achieve concrete results, it is essential to develop or strengthen tools and instruments that would allow stakeholders to work together, efficiently and effectively.

These tools and instruments, as well as others that may be identified in due course, would also serve to better understand and identify societal, economic and political dependencies on the Internet, as well as the inter-dependencies between different sub-sectors therein. Furthermore, these tools and instruments would strengthen the preventive abilities of stakeholders, which in turn will help to avoid recourse to *ex post* or overly invasive security measures.

All these activities should be based on a strong cooperation among public authorities to allow access to the relevant technologies and expertise.

EDUCATION AND AWARENESS-RAISING

Public authorities, with the support of other stakeholders, as appropriate, should strive to educate and raise awareness on the risks associated with Internet-related activities.

Explanatory note

It is recognised that certain categories of stakeholders are not always in a position to properly understand the risks – both for themselves and for the stability and resilience of the Internet as a whole – associated with their Internet-related activities.

Without prejudice to the competences of Member States in the area of culture and education, and taking in the utmost account the principle of subsidiarity, a shared EU approach to such activities, with a view to achieve a global approach, should be sought.

The private sector has an important role to play in supporting public authorities and in providing clear information to all stakeholders, concerning the potential risks of their behaviours for the stability and resilience of the Internet, e.g. unwillingly propagating virus and other malware, having their computers enrolled in a Botnet, etc.

Strengthening education efforts in this area will also have the benefit of producing skilled experts in the needed ICT fields. Education and awareness-raising will also strengthen the preventive abilities of stakeholders, which in turn will help to avoid recourse to *ex post* or overly invasive security measures.

GUIDELINES

The following guidelines constitute an attempt to map the high-level principles, introduced above, into more concrete and operational activities. They are meant as a basis for enhancing coordination and, as such, the suggested actions are indicative and non-binding. In all suggested activities, full use of the European Network and Information Security Agency (ENISA), as well as of other relevant bodies such as the Joint Research Centre (JRC) of the European Commission should be made.

(1) Collect existing principles, guidelines, regulations and instruments at the global or regional level and map them on the principles and guidelines for Internet resilience and stability, in order to understand the compatibility and potential synergies between the two.

WHO: European Union, Member States

(2) Promote core European values and interests via informed and conscious decisions on adoption of technologies, laws and policies, based on appropriate multi-stakeholder impact assessment, monitoring and *ex post* evaluation processes, possibly coordinated at the European level.

WHO: European Union, Member States

(3) Develop a coherent, long-term strategy of how public authorities would expect all European stakeholders to act in all matters related to the stability and resilience of the Internet, including by:

– developing and sharing good practices (coherent across the European Union) on the best approach to take when developing policy or taking action to ensure the stability and resilience of the Internet, having particular concern for the choice between top-down and bottom-up approaches

– communicating and promoting public policy priorities to other stakeholders

– actively participating in Internet Governance processes and fora that relate to the stability and resilience of the Internet

WHO: European Union, Member States.

(4) When discussing matters related to the resilience and stability of the Internet, identify and prioritise fora that guarantee inclusiveness and a significant multi-stakeholder participation. Encourage structured open consultations, at national and European level, on relevant public policy matters related to the stability and resilience of the Internet.

WHO: European Union, Member States

(5) Identify, at the National and European level, key physical and logical elements of the Internet infrastructure (e.g. naming, addressing and routing services), as well as societal dependencies on it. These processes should be informed by, and to the extent possible, be coherent to, international good practices in this area.

WHO: European Union, Member States, private sector

(6) Encourage participation in standardisation processes, striving to coordinate European efforts, in order to promote the adoption of open standards and ensure that security and

privacy requirements are included from the start. Leverage public procurement strategies to encourage openness and interoperability of Internet technologies, including via the adoption of open standards, in public procurement for ICT or ICT-related products and services.

WHO: European Union, Member States

(7) Discuss with stakeholders the feasibility of appropriate economic and social incentives, including:

- adequate security requirements in national public procurement standards, in a way compatible with relevant EU law.
- partial liability exemptions for companies which have demonstrably employed appropriate security technologies and procedures.
- where not already present in national law, liability for software and hardware producers for failure to guarantee appropriate levels of security.

In order to avoid fragmentations of the internal market, best practices on incentives should be exchanged at the European level.

WHO: European Union, Member States, private sector

(8) Ensure that all activities related to the resilience and stability of the Internet are developed in the context of a good risk management framework, including by:

- identifying the supply chains in the provision of essential elements of the Internet infrastructure and ensuring their diversity, possibly by coordinating, at the European level, the necessary industrial policies;
- developing measurement indicators, at the European level, to ensure a common understanding of the threats (and most effective counter-measures) to the stability and resilience of the Internet;
- perform peer-reviewed benchmarking activities on the basis of the above measurement indicators.
- collecting data on Internet threats, vulnerabilities and incidents;
- establishing a trusted platform for the exchange of such data at the European level;
- develop contingency strategies with the involvement of all relevant stakeholders;
- participate to pan-European and global exercises[7] on the resilience and stability of the Internet.

WHO: European Union, Member States, private sector

[7] The usefulness of which has been recognised by the Council of the EU in Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security (2009/C 321/01).

(9) Support the activities of the European Public-Private Partnership for Resilience (EP3R), including by ensuring an effective flow of information between it and national cooperation platforms. Support and participate to global Public-Private Partnership initiatives.

WHO: European Union, Member States, private sector

(10) At the National level, encourage public and private sector arrangements for mutual assistance, including by adopting and promoting the principles for Internet resilience and stability, propose guidelines, foster cooperation and agree on shared good practices. Assess the possibility to develop a pan-European mutual-assistance strategy.

WHO: Member States, private sector

(11) Develop curricula for secondary and tertiary education in fields relevant to the stability and resilience of the Internet, in order to empower young people. Launch national campaigns for awareness-raising on the importance of the stability and resilience of the Internet and on the appropriate measures that all stakeholders can take to enhance it. Exchange best practices on curricula and awareness-raising campaigns at the European level.

WHO: Member States, private sector