| ROADMAP | | | |
|---|---|---|---|
| TITLE OF THE INITIATIVE | **Proposal on a European Strategy for Internet Security** | | |
| TYPE OF INITIATIVE | x CWP • Non-CWP • Implementing act/Delegated act | | |
| LEAD DG – RESPONSIBLE UNIT | INFSO A3 | | |
| EXPECTED DATE OF ADOPTION | Month/Year: Q3 2012 | | |
| VERSION OF ROADMAP | No: 4 | Last modification: | Month/Year: November 2011 |

This indicative roadmap is provided for information purposes only and is subject to change.
It does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content and structure.

## A. Context, problem definition

(i) What is the political context of the initiative?
(ii) How does it relate to past and possible future initiatives, and to other EU policies?
(iii) What ex-post analysis of the existing policy has been carried out and what results are relevant for this initiative?

The Internet has undergone a historical change in the last decade – it evolved from being yet "another" emerging infrastructure to become the nervous system of our economy and society as a whole. The digital ecosystem supports the creation of better conditions for more high-quality jobs, smarter and sustainable growth and increases the level of productivity in the economy. The World Bank estimates that with 10% percent increase in high speed Internet connections, economic growth increases by 1.3%. The Internet is also one of the largest and most successful platforms for cultural expression and access to knowledge ever known. Last, not least, it can also be a powerful tool for democratisation and the exercise of fundamental rights, such as freedom of expression.

At the same time, we are witnessing that the threat landscape is constantly expanding and the number and seriousness of attacks is increasing Internet's vulnerability. We are witnessing an alarming trend towards using Information and Communication networks for exploitation purposes (e.g. GhostNet[1], ETS[2], recent attacks against government systems and EU Institutions); disruption purposes (e.g. Conficker[3], StuxNet[4] , submarine cable breaks); or destruction purposes. Not only have networks become targets, but also individual companies have suffered attacks. Moreover, threats can now originate from anywhere in the world and, due to global interconnectedness, impact any other part of the world. According to the World Economic Forum there is a 10% likelihood of a major Critical information infrastructure breakdown with potential economic damages of over $ 250 billion.

Securing the smooth functioning of this vital infrastructure is therefore essential to our economic stability and growth. Failure to do so, would pose an enormous risk to the proper functioning of the single market in terms of lost growth, jobs and prosperity, and to reaching our goal of achieving a true digital single market by 2015. The increasing sophistication of threats and the global interconnectedness call for a much tighter cooperation and collaboration between Governments, as well as between public and private sectors.

The time has come for **a step change** in the way Europe addresses Internet security issues, considering that the Internet is increasingly becoming the backbone of our economy and the consequent increasing level of threats and potential damages that incidents and disruptions could inflict on the EU and Member States. It is therefore crucial that the EU recognises the need for an effective European Strategy for Internet Security to avert and/or minimise the risk of a major attack or technical failure of its information and communication infrastructures.

A new Strategy for Internet Security will be based on previous results and achievements.

In 2006, a strategy for a secure information society (COM(2006)251) was adopted in response to the urgent need to coordinate efforts for building up trust and confidence of stakeholders in electronic communications and services. The main elements of this strategy were endorsed in a Council Resolution (2007/068/01). This strategy also strengthened the role of the European Network and Information Security Agency (ENISA), established in 2004 with a view to contribute to the goals of ensuring a high and effective level of NIS within the Union and to develop a culture of NIS for the benefit of EU citizens, consumers, enterprises and administrators.

[1] A large-scale cyber spying operation discovered in March 2009
[2] Emissions Trading Scheme
[3] A computer worm targeting the Microsoft Windows operating system that was first detected in November 2008
[4] A computer worm discovered in July 2010. It targets Siemens industrial software and equipment running on Microsoft Windows.

On 30 March 2009, the Commission adopted a Communication (COM(2009) 149) on Critical Information Infrastructure protection (CIIP) focusing on the protection of Europe from cyber attacks and cyber disruptions by enhancing preparedness, security and resilience. The Communication launched an action plan with five pillars of actions: preparedness and prevention; detection and response; mitigation and recovery; international cooperation; criteria for the ICT sector.

The Action plan was endorsed in the Presidency Conclusions of the Ministerial conference on CIIP in Tallinn in 2009. These commitments were further advanced by the Council Resolution on "A collaborative European approach to network and information security" adopted on 18 December 2009.

Security and resilience issues are notably addressed under the Trust and Security chapter of the Digital Agenda for Europe (COM(2010) 245), one of the flagship initiative of the EU 2020 Strategy. In particular, its Key action 6 calls for measures aimed at a reinforced and high level Network and Information Security policy.

The Digital Agenda for Europe is complementary to other initiatives such as the Stockholm Programme for Freedom, Security and Justice and the Internal Security Strategy in action (COM(2010)673).

More recently, two key policy components have been completing this picture, from the network and information security angle:

- The activity of the European Network and Information Security Agency (ENISA), for which a proposal to modernise the mandate is under discussion in the Council and the European Parliament (COM(2010) 521);
- The Commission second Communication on CIIP of March 2011 (COM(2011) 163) ('Achievements and next steps: towards global cyber-security') which takes stock of the results achieved since the adoption of the CIIP action plan in 2009 and describes the next priorities planned under each action at both European and international level. Council Conclusions on CIIP were adopted on 27 May 2011.

The revised regulatory framework for electronic communications also sets new security provisions including security breaches notifications (Art. 13 a and b), to be transposed at national level by 25 May 2011.

Discussions are also ongoing as regards relevant proposals on a Directive on attacks against information systems and on a Directive on combating sexual abuse, sexual exploitation of children and child pornography.

At the international level, since the 2010 EU-US summit, a joint EU-US Working Group on Cyber-security and Cybercrime has been established.

Most of the 2009 Action Plan measures are planned to be completed by 2012 (at the latest by 2013), and there are already visible results in a number of areas, e.g. strengthened cooperation via the European forum for Member States, and European Public-private Partnership for resilience, the establishment of National/governmental CERTs in 20 Member States, etc .

It is necessary to develop a vision for the years beyond 2012, building on the up-to-now achievements but looking ahead and providing a more comprehensive, consistent and structured EU approach to Internet security.

What are the main problems which this initiative will address?

Since 2006, the threat landscape has changed fundamentally.

Not only have the Internet and digital technologies become even more central to our economies and societies, but their vulnerability has increased and the number and seriousness of attacks magnified (attacks on Estonia, on the French Finance Ministry prior to the G20 summit, on the EU Emissions Trading System and most recently on the European External Action Service and the Commission are cases in point).

Not only have networks become targets, also individual companies have suffered attacks. Destruction of networks or production processes cannot be ruled out. Moreover, threats can now originate from anywhere in the world and, due to global interconnectedness, impact any other part of the world. The threats are also moving to new technological platforms, notably the smartphones and tomorrow possibly the connected devices of the "internet of things". They are also cross-sector – in particular as regards critical infrastructures (e.g. energy grids, transport networks).

Despite achievements made, the cyber-security capabilities within the EU are still not at the level which is necessary in order to ensure a high and efficient protection within the EU. Furthermore, most of the actions are carried out on a voluntary basis also considering that security is considered mainly to be a national prerogative. This can result in a lack of clear commitment by the Member States and stakeholders to deliver on those actions.

Who will be affected by it?

Public authorities (at the European and national level), the private sector (both the information security industry, the ICT industry which relies on appropriate levels of trust and security in ICT throughout society, and in general all sectors of the industry which rely on Information and Communication Technologies for their activities), citizens.

(i) Is EU action justified on grounds of subsidiarity?
(ii) Why can Member States not achieve the objectives of the proposed action sufficiently by themselves? (Necessity Test)
(iii) Can the EU achieve the objectives better? (Test of EU Value Added)

The interdependencies between networks and information systems, and in particular the Internet, make it extremely difficult, if not impossible, for individual actors to correctly judge the global economic and societal impact of their (lack of) measures taken to protect against cyber incidents and disruptions. Furthermore, entities (public and private, including citizens) that are completely unrelated are impacting each other. Increasing globally the ability of network and information systems to resist threats therefore requires public intervention at the European level. Uneven national policies and practices are a clear disruption of the internal market, due to the negative externalities resulting from cyber security incidents (inadequate policies impacting markets in other Member States), but also due to the positive externalities of good NIS practices (good practices in one Member State positively impact cyber security as a whole, thus creating a clear societal good). In cases where such externalities exist across Member States, European policy intervention may be justified as it provides a real added value to the functioning of the internal market.

Progress has been fostered by the 2009 Critical Information Infrastructure Protection Action Plan and implementation of the specific actions of the Digital Agenda for Europe. Unfortunately, the importance of Internet security is not yet recognised at the appropriate level in all Member States. It is both urgent and important for the EU to recognise the need for an effective European Strategy for Internet Security to avert and/or minimise the risk of a major attack or technical failure of its information and communication infrastructures.

National responses alone are no longer effective. As our economies and networks (e.g. energy, transport, payment systems) have become more and more integrated, the need for EU co-operation and common approaches has only increased. A major disruption of the Internet resulting from a malicious attack (or a technical problem) in one or more Member States will have immediate implications for all others and for the proper functioning of the single market – in terms of lost growth, jobs and prosperity. Internet security is therefore an important part of **the Europe 2020 strategy**.

## B. Objectives of the initiative

What are the main policy objectives?

The goal of the initiative is to propose a comprehensive Internet Security Strategy for Europe. It will foresee one or more legal instruments, thereby making an important step-up from the current voluntary towards a binding approach.

It will aim to:

- describe some of the main risks and challenges as well as the economic and geopolitical opportunities, thereby linking the efforts in the area of cyber security with the broader Commission agenda (Europe 2020, MFF, CSF, Cohesion policy)

- examine and assess the risks associated with a lack of efficient cooperation and coordination at EU-level

- compare with "preparedness" or political attention given to the topic in other third countries (US, Canada, China, India, Japan, etc.)

- describe the major issues at stake or problems to be addressed both in the area of governance, security, trust & confidence and in the political, economic and social areas

- assess the on-going or planned actions where and when they exist, but also highlight the areas where more EU action, coordination or competences are required,

- propose actions in other areas where so far there is no or little EU action.

The policy initiative would focus, *inter alia*, on:

- Every Member State will be expected to nominate an agency/competent body responsible for cyber security and ensure it has the necessary cyber security capabilities. We need to make sure that there are no weak links in the chain;

- National/Governmental CERTs to become part of an effective network in which information is exchanged according to the necessary *confidentiality standards.* Protection of confidentiality will need to be given legal force to ensure effective sharing of information, as is the case in other sectors where sensitive information is exchanged (e.g. banking supervisors).
- Confidence-building measures will need to be foreseen, for example, strengthening the "European Forum of Regulators". Measures will also have to be defined to foster a culture of network and information security and risk management, in particular by putting in place mechanisms for peer evaluation and assistance and for exchange of good practices which will support better cooperation and foster trust among Member States.
- Protocols to be agreed in case of cyber disruptions or attacks involving several Member States;
- Incentives (technical, legal or regulatory) will need to be put in place to ensure adequate investments and adoption of good practices and take-up by the private sector in network and information security and to foster a risk management culture. In this regard, we can capitalise on activities of the European Public Private Partnership for Resilience (in particular those of its working group on Baseline requirements for security and resilience of electronic communications). Private sector efforts to improve security in products and services could be stimulated by introducing security breach notification obligations, e.g. extending the provisions in Art. 13a of the Regulatory Framework Directive of e-communications to other sectors beyond the telecom one (e.g. financial services, energy, transport). In these sectors, and in co-operation with the competent regulators, the relevant authorisation procedures can also be strengthened with regard to network security safeguards. This could in turn be combined with mandatory security audits (failing which the authorisation could be suspended). In other sectors, measures can be taken to promote notifications to CERTs of disruptions and attacks, for example by ensuring confidentiality, as currently companies are reluctant to inform authorities. This could help the responsible CERT to alert other companies of risks and how to address them.
- To be successful, these policy measures need to be complemented by the adoption of state-of-the-art technologies, processes and methods. Europe needs to develop and apply the best solutions for cyber security and online privacy, by generating innovative technology (R&D effort) and putting it at work (innovation strand).

Besides these binding provisions, the Strategy would cover other key aspects such as:

Ø stimulating private sector efforts to improve security in products and services through the development of appropriate (legal, regulatory and economic) incentives. Reducing vulnerabilities in products, applications and web services to make the ICT infrastructure more resilient to malware would be a priority. Codes of conduct could also be drawn up in specific industry sectors.

Ø reinforcing and better coordinating R&D activities by developing and deploying appropriate technologies for proactive, real-time and automatic solutions (rather than on-demand, manual ones) which respond both to present and future security challenges. Actions, based on existing initiatives, to promote innovation should be implemented too. Additionally, Horizon 2020 will offer a good opportunity for a comprehensive approach to technological and socio-economic research and innovation on the topic.

Ø assessing how procurement of innovative solutions can be promoted to tackle the slow market take up of available technologies. Such promotion initiatives should build on and reinforce national initiatives and policies and be implemented in close cooperation with national authorities and industry. The creation of partnerships will be essential in the piloting, procurement and deployment of solutions. Security solutions should become an integral part of the provision of e-services, mandatory for governmental e-services, and recommended for the private sector, with audit seals provided.

Ø raising consumers' awareness by promoting appropriate mechanisms to engage intermediaries in providing tailored programs and messages on risks, security and safe online behaviour.

Ø encouraging Member States to build up their security capacities – in an interconnected way - with the support of structural funds (notably as part of their future national digital growth plans) and other funding of the future Connecting Europe Facility (CEF). The CEF is also intended to support deployment of service infrastructures such as e-authentication which offer more secure services.

Ø The strategy would also encompass, as appropriate, specific initiatives in the area of fighting cybercrime to ensure an integrated and coherent approach to tackling wider cyber-security challenges. Consistent links must be made with Mrs Malmström's Internal Security Strategy and with international debates on the subject with key partners, notably the US. There is indeed an important external dimension to be considered.

Ø The implementation of the strategy should be supported by targeted R&D efforts and measures (e.g. standardisation, public procurement, tax incentives) to promote greater innovation and competitiveness of the European network security industry. Funding, in particular the structural funds in the case of

cohesion countries, could come in support of Member States needing assistance to build up the required administrative capacity.

By bringing its own house in order, Europe would be better placed to co-operate with its global partners and to influence global Internet governance too (ranging from the architecture of the future Internet to the management of Internet domain names). Additionally, it will be important to consider the ways in which the EU could contribute to ensuring an open and transparent development of a secure and resilient global Information Society, including by engagement in the development of 'responsible State norm-based-behaviour'.

Do the objectives imply developing EU policy in new areas?

The initiative would not replace existing or planned actions but will put them in a global political framework and will prepare the agenda for further work.

The initiative will review and develop further the European Strategy for a Secure Information Society by taking into account the progress made since 2006 when the last Strategy for a Secure Information Society (COM(2006)251) was adopted. It will build on the achievements of other related policy initiatives in this area, i.e. the Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009)149); the Communication on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" (COM(2011)163).

## C. Options

(i) What are the policy options being considered?
(ii) What legislative or 'soft law' instruments could be considered?
(iii) How do the options respect the proportionality principle?

The proposed initiative will be a strategy which will outline the direction in which specific initiatives will be developed. Policy options will be examined for each of these specific initiatives as appropriate.

## D. Initial assessment of impacts

What are the benefits and costs of each of the policy options?

See above.

Could any or all of the options have significant impacts on (i) simplification, (ii) administrative burden and (iii) on relations with other countries, (iv) implementation arrangements? And (v) could any be difficult to transpose for certain Member States?

To be examined, as appropriate, for each of the specific initiatives which will follow from the strategy.

(i) Will an IA be carried out for this initiative and/or possible follow-up initiatives? (ii) When will the IA work start? (iii) When will you set up the IA Steering Group and how often will it meet? (iv) What DGs will be invited?

(i) An impact assessment will be carried out for the individual specific initiatives stemming from the strategy

(ii) January 2012

(iii) Q1 2012. The IA Steering Group s expected to meet at least 3 times.

(iv) The list of possible DGs and services to be involved includes: COMP, DIGIT, ENTR, ENV, HOME, HR, JUST, JRC, MARKT, RTD, SANCO, SG, SJ and the EEAS

(i) Is any of options likely to have impacts on the EU budget above €5m?

(ii) If so, will this IA serve also as an ex-ante evaluation, as required by the Financial regulation? If not, provide Information about the timing of the ex-ante evaluation.

No

## E. Evidence base, planning of further work and consultation

(i) What information and data are already available? Will existing impact assessment and evaluation work be used?

(ii) What further information needs to be gathered, how will this be done *(e.g. internally or by an external contractor)*, and by when?

(iii) What is the timing for the procurement process & the contract for any external contracts that you are planning (e.g. for analytical studies, information gathering, etc.)?

(iv) Is any particular communication or information activity foreseen? If so, what, and by when?

(i) The initiative will build on the information gathered so far via:

- previous impact assessments on related initiatives, e.g. the IA accompanying the Communication on Critical Information Infrastructure Protection (SEC(2009)399 and SEC(2009)400) and the IA accompanying the proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA) (SEC(2010)1126 and SEC(2010)1127);
- the views and ideas gathered via the European Forum for Member States and the European Public-Private Partnership for Resilience;
- Work done by ENISA;
- etc.

Which stakeholders & experts have been or will be consulted, how, and at what stage?

Stakeholders:

- Member States bodies, involved in the field of network and information security and other relevant areas;
- National Regulatory Authorities in the field of electronic communications networks and services;
- Telecommunications operators and Internet Service Providers as well as other Information Society Service Providers and related sector associations;
- Manufacturers of hardware and software components for electronic communications networks and services and related associations;
- Public bodies involved in the field of NIS such as national competent authorities, Computer Emergency Response Teams (CERTs);
- Academics and research communities;
- Major corporate users of information infrastructures from the financial, energy and transport sector, etc.

Events and forums:

- Meetings of the European Forum for the Member States (EFMS). The forum meets regularly (3/4 times per year);
- Meetings of the European Public-Private Partnership for Resilience (EP3R) – the EP3R meets regularly (3/4 times per year) and has launched since 17 November 2010, three Working Groups on respectively: (WG1): Key assets, resources and functions for the continuous and secure provisioning of electronic communications across countries. (WG2): Baseline requirements for the security and resilience of electronic communications. (WG3): Coordination and cooperation needs and mechanisms to prepare for and respond to large scale disruptions affecting electronic communications;
- Meetings of the Inter-service Group on cybercrime and cyber-security led jointly by DG INFSO, DG HOME and the EEAS;
- Roundtables on Internet security at the European Parliament;
- Discussions at Council level;
- Ad hoc events