I

(Resolutions, recommendations, guidelines and opinions)

RESOLUTIONS

COUNCIL

COUNCIL RESOLUTION

of 22 March 2007

on a Strategy for a Secure Information Society in Europe

(2007/C 68/01)

THE COUNCIL OF THE EUROPEAN UNION,

HEREBY ADOPTS THIS RESOLUTION AND

WELCOMES

The 31 May 2006 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions — A Strategy for a Secure Information Society — 'Dialogue, Partnership and Empowerment';

NOTES

The 15 November 2006 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Fighting spam, spyware and malicious software;

RECALLS

1. The 28 January 2002 Council Resolution on a Common Approach and Specific Actions in the area of Network and Information Security ([1]);

2. The 18 February 2003 Council Resolution on a European Approach towards a culture of Network and Information Security ([2]);

3. The 8/9 March 2004 Council Conclusions on Unsolicited communications for direct marketing purposes or 'spam' and the 9/10 December 2004 Council Conclusions on Fight against spam;

4. The March 2005 European Council Conclusions re-launching the Lisbon strategy and the European Council March 2006 Conclusions calling on the Commission and the Member States to implement the new i2010 Strategy vigorously;

5. The EU Regulatory Framework for Electronic Communications ([3]), and, in particular, the provisions relating to communication security, privacy and confidentiality, which have contributed to ensuring a high level of personal data and privacy protection and the integrity and security of public communications networks;

6. The 10 March 2004 Regulation (EC) No 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency (ENISA) ([4]);

7. The Tunis Agenda and the Tunis Commitment of the World Summit on the Information Society (WSIS) highlighting the need to continue the fight against cyber-crime and spam while ensuring the protection of privacy and freedom of expression, and to further promote, develop and implement, in cooperation with all stakeholders, a global cyber-security culture;

8. The Presidency Conclusions of the Annual European Information Society Conference (27-28 September 2006) 'i2010 — Towards a Ubiquitous European Information Society', in Espoo, Finland;

([1]) OJ C 43, 16.2.2002, p. 2.
([2]) OJ C 48, 28.2.2003, p. 1.
([3]) Directives 2002/58/EC (Directive on privacy and electronic communications), 2002/20/EC (Authorisation Directive), 2002/22/EC (Universal Service Directive) (OJ L 201, 31.7.2002, p. 37, OJ L 108, 24.4.2002, p. 21 and OJ L 108, 24.4.2002, p. 51, respectively).
([4]) OJ L 77, 13.3.2004, p. 1.

ACCORDINGLY STRESSES THAT:

1. Our societies are rapidly moving into a new phase of development, towards a ubiquitous information society, where more and more of the everyday activities of the citizens are based on the use of Information and Communications Technologies (ICT) as well as electronic communications networks; network and information security should be considered as a key enabler for this development and for its success;

2. Trust is a vital element in the success of the new Information Society; trust also relates to the experiences of the end-users and to the need to respect their privacy; therefore, network and information security should not be merely considered as a technical issue;

3. Network and information security is an essential part in the creation of a European Information Space as part of the i2010 Initiative, thus contributing to the success of the renewed Lisbon Strategy; ICT is also a critical component of innovation, economic growth and jobs throughout the economy;

4. New technologies that will lead us to the ubiquitous information society are already under development; the advent of ground-breaking technologies (such as, high-speed wireless networks, Radio Frequency Identification (RFID) Devices, sensor networks) and innovative, content-rich services (such as, Internet Protocol Television (IPTV), Voice over Internet Protocol (VoIP), mobile-TV and other mobile services) require adequate levels of network and information security from the very beginning of the development phase, in order to reach real commercial value; the early adoption of the new promising innovations is very important for the development of the information society and the competitiveness of Europe; governmental bodies and enterprises should adopt as soon as practicable secure, emerging new technologies and services in order to speed up their widespread adoption;

5. It is strategic for the EU that European industry is both a demanding user as well as a competitive supplier of network and of security products and services; diversity, openness and interoperability are integral components of security and should be promoted;

6. Network and information security knowledge and skills must also become integral part of everyday life of each individual and stakeholder in the society; a number of awareness raising campaigns have taken place both at national and EU-level, but there is still work to be done in this field, especially as concerns the end-users and small and medium-sized enterprises (SMEs); particular consideration should be given to users that have special needs or have low awareness of network and information security issues; all stakeholders should be aware that they are part of the global security chain and should be empowered to act as such; network and information security issues should be taken into account in all education and training relating to ICT;

7. The establishment of ENISA has been a major step forward in the EU's efforts to respond to the challenges relating to network and information security; the scope, objectives, tasks and duration of ENISA are defined by Regulation No 460/2004;

8. Resources directed to research and development (R&D) and innovation both at national and EU-level are one of the key elements in strengthening the level of information and network security of new systems, applications and services; efforts at the EU level should be reinforced in the fields of security-related research and innovation, in particular through the 7th Framework Programme (FP7) and the Framework Programme on Competitiveness and Innovation (CIP); efforts should also be directed towards measures to disseminate and encourage the commercial exploitation of the consequential results, including the evaluation of their usefulness for the wider community; this will enhance the ability of European suppliers to provide security solutions that will meet the specific needs of the European market;

9. The ubiquitous information society, while providing great benefits, also poses significant challenges, thus creating a new landscape of potential risks; threats to security and privacy, also through unlawful interception and exploitation of data, are becoming more and more serious, targeted and clearly aimed at economic benefit, new responses for the emerging and already existing threats should be created in an innovative manner and they should also cover issues arising from system complexity, mistakes, accidents or unclear guidelines; the creation and development of national computer emergency response bodies aimed at various actors and the cooperation between these bodies as well as with other relevant stakeholders should be encouraged and further promoted;

10. Standardisation and certification of products, services and management systems, in particular provided by existing institutions, deserve particular attention in the network and information security policy of the EU as a means to spread good practice and professionalism in the network and information security field; especially new emerging technologies like RFID and mobile-TV would benefit from timely adoption of possibly emerging open and interoperable standards; the functioning of the European standardisation bodies in this field should be encouraged;

11. As electronic networks and information systems play an increasingly central role in the overall operation of Critical Infrastructures, their availability and integrity becomes indispensable to administrations', businesses, citizens' safety and quality of life, as well as to overall functioning of societies;

12. Cooperation and practical approaches are needed more than ever; the various stakeholders should identify and recognise their respective roles, responsibilities and rights;

AND THEREFORE INVITES MEMBER STATES TO:

1. Support training programmes and raise general awareness of network and information security issues, by, for example, launching information campaigns about network and information security issues, targeting all citizens/users and sectors of the economy, especially SMEs and end-users with special needs or low awareness; by 2008, a common date could be selected as a European wide awareness raising day (e.g. 'Information and Network Security Day') to be conducted on an annual and voluntary basis in each Member State;

2. Strengthen the contribution to security-related R&D and to improve the usability and dissemination of the consequential results; encourage the development of innovative partnerships to boost the European ICT security industry growth and increase the early use of new network and information security technologies and services in order to give them a commercial boost;

3. Give due attention to the need to prevent and fight new and existing security threats on electronic communications networks, which also include unlawful interception and exploitation of data, recognise and deal with associated risks and to encourage, where appropriate in cooperation with ENISA, effective exchanges of information and cooperation between the relevant organisations and agencies at national level; to commit to fighting spam, spyware and malware, in particular through improved cooperation between competent authorities at national and international level;

4. Strengthen their mutual cooperation within the i2010 framework, in order to identify effective and innovative practices to improve network and information security and spread the knowledge of these practices throughout the EU on a voluntary basis;

5. Encourage the continuous improvement of the national computer emergency response bodies;

6. Promote an environment, which encourages service providers and network operators to provide robust services to their customers and to ensure resilience as well as consumer choice in their security services and solutions; encourage or require where appropriate, network operators and service providers to ensure an adequate level of network and information security for their customers;

7. Continue a strategic discussion in the i2010 High Level Group, while taking into account ongoing development in the Information Society, and ensure a consistent approach between the dimensions of regulation, co-regulation, R&D and eGovernment together with communication and education;

8. In line with the i2010 eGovernment Action Plan, provide for the roll-out of seamless eGovernment services, promote interoperable identity management solutions and undertake all appropriate changes in the public sector organisation; governments and public administrations should serve as an example of best practice by promoting secure eGovernment services for all citizens;

WELCOMES THE INTENTION OF THE COMMISSION TO:

1. Continue the development of a comprehensive and dynamic EU-wide strategy for Network and Information Security. The holistic approach proposed by the Commission is of special importance;

2. Address network and information security as one of the objectives in the EU Regulatory Framework for Electronic Communications review;

3. Continue to play its role so as to achieve greater awareness about the need for general political commitment to fight spam, spyware and malware; reinforce the dialogue and cooperation with third countries, in particular through agreements with third countries including the issue of the fight against spam, spyware and malware;

4. Strengthen the involvement of ENISA in supporting the Strategy for a Secure Information Society in Europe, as set out in this Resolution, in line with the objectives and tasks set out in Regulation (EC) No 460/2004 as well as in closer cooperation and tighter working relations with Member States and stakeholders;

5. Develop, within the i2010 framework, in cooperation with Member States and all stakeholders, especially with statistical and Member States' information security experts, appropriate indicators for Community surveys on aspects related to security and trust;

6. Encourage the Member States to examine, via a multi-stakeholder dialogue, the economic, business and societal drivers with the aim of developing an ICT sector-specific policy to enhance the security and resilience of network and information systems, as a potential contribution to the planned European Programme on Critical Infrastructure Protection;

7. Continue its efforts, in coordination with Member States, to promote dialogue with relevant international partners and organisations to foster global cooperation on Network and Information Security, notably by implementing the WSIS Action lines and reporting to the Council on a regular basis;

AND CALLS UPON:

1. ENISA to continue working in close cooperation with the Member States, the Commission and other relevant stakeholders, in order to fulfil those tasks and objectives that are defined in Regulation (EC) No 460/2004 and to assist the Commission and the Member States in their efforts to meet the requirements of network and information security, thus contributing to the implementation and further development of the Strategy for a Secure Information Society in Europe, as set out in this Resolution;
2. All stakeholders to improve the security of software and the security and resilience of network and information systems in line with the Strategy for a Secure Information Society in Europe, as set out in this Resolution, as well as to engage in a structured multi-stakeholder debate on how best to utilise existing tools and regulatory instruments;
3. Enterprises to take a positive attitude towards information and network security in order to create more advanced and secure products and services, considering investments in such products and services as a competitive advantage;
4. Manufacturers and service providers to build, where appropriate, security, privacy and confidentiality requirements into their product- and service design and deployment of network infrastructure, applications and software, implement and monitor security solutions;
5. Stakeholders to cooperate and to launch experimental environments for testing and piloting new technologies and services in a secure manner; stakeholders to adopt in a timely manner the new secure technologies and services after they have been launched commercially;
6. All stakeholders to engage in further efforts to combat spam and other on-line malpractices and to actively cooperate with competent authorities at national and international level;
7. The service providers and the ICT industry to focus on enhancing security, privacy and usability in products, processes and services in order to have reliability, prevent and fight ID theft and other privacy-intrusive attacks;
8. Network operators, service providers and the private sector to share and implement good security practices and to foster a culture of risk analysis and management in organisations and business by supporting appropriate training programmes and developing contingency planning as well as make security solutions available to their customers as part of their services.