

**Enhancing Survivability of Europe's Information Infrastructures:  
Current Activities for a Safer European Future Online**

**By**

Lorenzo Valeri

Dr Andrew Rathmell

Associated Research Fellows

Strand Bridge House, King's College London

WC2R 2LS London, United Kingdom

Email: (lorenzo.valeri; andrew.rathmell)@kcl.ac.uk

*Submitted for ISW 2001-Vancouver 15-17 October 2001*

**Abstract**

Dependability and survivability are becoming public policy issues in Europe. This paper examines two initiatives aimed at supporting the European Commission in addressing these topics: Dependability Development Support Initiative (DDSI) and European Warning Information System (EWIS). It briefly highlights the contents and programmes of this initiatives. Particular emphasis is directed to underline the strong commitment of all European stakeholders to tackle these issues so that Europe can become better equipped to exploit the full economic and social potential brought by the Internet and other information and network systems.

**Introduction**

There has been growing concern in Europe's technical and business communities for a number of years about the increasing interdependency and vulnerability of information infrastructures. However, it has only been in the past two years that the issue has gained strong political prominence and made rapid European policy action imperative.<sup>1</sup> After several scoping meetings and workshops, in 2000 and 2001 EU member states have given the European Commission backing for establishing for more comprehensive policy approaches to tackle various issues related to this increasing societal dependability on complex information infrastructures. This support is exemplified by the eEurope programme, an overarching initiative unveiled during the European Council held in Lisbon, Portugal in March 2000. The ambitious goal was to turn Europe into the world's most competitive and dynamic economy area.<sup>2</sup> In a subsequent meeting, the heads of state and governments of the fifteen EU member states have then presented a more detailed and comprehensive eEurope Action Plan 2002, which highlighted, inter alia, the importance of network security and dependability of information infrastructures to foster Europe's information society. In particular, it was noted that: "Information and communication infrastructures have become a critical part of our economies. Unfortunately, these infrastructures have their own vulnerabilities and offer new opportunities for criminal conduct ... there is little doubt that these offences constitute a threat to industry investment and assets, and to safety and confidence in the information society."<sup>3</sup>

These activities have been paralleled by other Community initiatives aimed at countering cybercrime and other Internet-based criminal activities. In January 2001, the European Commission released a Communication [Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime.](#)<sup>4</sup> Here, the Brussels-based European body

detailed its thinking in relation to the substantial and procedural criminal aspects of cybercrime and indicated the necessary non-legal actions. The goal is to guard Europe's information infrastructures and enhance overall trust and confidence towards these new information and communication instruments. The latter has been discussed in great detail in another communication released on 6 June 2001. Here, the Commission emphasised that "Concerns about security of electronic networks and information systems have been growing along with the rapid increase in the number of network users and the value of their transactions. Security has now reached a critical point where it represents a prerequisite for the growth of electronic businesses and the functioning of the whole economy."<sup>5</sup> Notwithstanding some of the national prerogatives of each EU member-states, the Commission suggested several European-level public policy initiatives aimed at working towards a common understanding of the underlying security issues and the specific measures to be taken. Particular attention has been devoted to issues related to public-private partnerships, early warning, technological support, market-oriented standardization, certification and the need for specific legal framework and international co-operation.

It is in this European policy context that the Dependability Development Support Initiative (DDSI) and forthcoming workshop on issues related to an early warning information system (EWIS), have been recently launched.

### **Dependability Development Support Initiative**

Europe's commitment to an open policy making process that engages all stakeholders was reflected at the launch of the Dependability Development Support Initiative (DDSI) in June 2001. DDSI is a consortium of European research centres and companies aiming at assisting the Commission in mapping the technical and socio-political requirements of dependability policy. Funded by the EU Information Society Technology (IST) programme, DDSI aims to contribute to a better understanding of dependability policy issues by bringing information and expertise together from all over the world onto one platform. From the outset, DDSI will have a primary and a wider focus. The former is on the dependability of the infrastructures and services underpinning Europe's information society (i.e. telecommunications and Internet infrastructures and supporting critical infrastructures, such as power distribution). The latter is on the wider set of critical infrastructures that support post-industrial societies and which are increasingly dependent on networked information systems. These sectors include energy generation, transport, water sewage, food production and distribution and core government services.

Notwithstanding the overarching nature of the DDSI initiative, it has also some limitations in respect of the wide range of potential vulnerabilities and threats that might undermine Europe's information society. In this case, too, DDSI has a primary objective and a wider focus. The primary objective is to assist in the development of policies addressing threats and vulnerabilities that are susceptible to short and medium term solutions. They include, for instance, detection and prevention of malicious attacks in the form of Denial of Service or malicious software over the Internet. Wider issues to be examined are problems related to the increasing reliance on Commercial Off The Shelf (COTS) technologies and vulnerabilities to market forces of global supply and value chains on which European industries are increasingly reliant.

In order to provide a detailed analysis of these issues and, thus, indicate concrete policy courses of action, DDSI involves different components. First, a vision and analysis paper detailing the major theoretical and technical issues surrounding dependability and policy making from a global perspective. This is presently

being drafted and will be made publicly available as soon as agreed among the DDSI research members. Afterwards, an inventory of current activities in this area carried out by individual EU member states and associate nations will be completed. The aims of this second work-package is to provide the Commission and other policy makers, as well as all stake-holders, with a clear understanding of dependability policies and research activities in Europe to avoid potential unnecessary policy and investment duplications. Afterwards, DDSI research members will concentrate in drafting detailed dependability-related roadmaps for concerted European actions in the areas of public policy, early warning, public-private co-operation and research and development. These roadmaps will be examined and tested through "light gaming exercises" involving both DDSI members and selected representatives from industry, public policy and scientific arena. The overall findings of DDSI will be presented during a final high-level conference to be held in Brussels in November 2002. As previously indicated, the entire DDSI research programme is run on the spirit of openness. All its findings and project deliverables will be freely available at <http://www.ddsi.org>. It is the intention of the DDSI research team to make this website one of the main information centres for issues related to dependability, information and network security and related public policy. More importantly, there is an unofficial commitment to continue to maintain and update the content of this website even beyond the official completion of DDSI in November 2002.

### **Towards a European Warning & Information System (EWIS)**

As part of its work-plan, DDSI is expected to examine the main issues related to both information sharing concerning malicious activities or general faults and the development of early warning capabilities aimed at protecting the overall dependability of Europe's information infrastructures. This research activity, nevertheless, parallels a similar need highlighted by the Commission in its recent communication on network security issues on 6 June 2001. In this document, the Commission clearly indicated that, at the present time, there is a limited cooperation among EU member-states in sharing signs of early warning of potential cyber-attacks or faults against European information infrastructures. Still, "cooperation is essential to ensure early-warning throughout the Union through the instantaneous exchange of information on the first signs of attack of one country".<sup>6</sup> In response to this pressing need, DDSI and the Institute for the Protection and Security of the Citizen of the EC Joint Research Centre (JRC) have joined forces to start the development of an initial roadmap to assist EU policy makers in assessing desired options for a European Warning and Information System (EWIS).

This cooperation presently involves the organisation of a major European workshop to be held in Brussels at the end of October 2001. This meeting is to be preceded by the preparation of a detailed study outlining the issues and options confronting a European Warning and Information System. Particular attention will be devoted to examining best practices by looking at the experiences of the Computer Emergency Response Teams-Coordination Centre and many other information sharing and threat assessment activities launched by private and public organisations. In parallel to these activities, the research team will start to discuss different scenarios for EU early warning systems from the perspectives of businesses and society at large, as well as the complexities and difficulties from a technical and organisational perspective. During the workshop, DDSI and JRC would like participants to examine the socio-political and economic aspects of EWIS, different business models, and privacy requirements. Particular attention will be devoted to examining legal issues such as liability and contractual issues and confidentiality requirements. The target audience for this pivotal workshop are representatives of national CERTs and commercial Information Sharing and Advisory Centres, as well as officials from end-users

organisations, information and communication companies, civil liberties and privacy actors and members of the research community. As with all of research activities of DDSI, the findings and results of these workshop will be openly available for comments and suggestions, as they will be posted at <http://ewis.jrc.it>.

## Conclusion & Next Steps

Building the dependable infrastructures upon which the European Information Society will rely poses a bewildering array of new problems to public policy makers and corporate leaders alike. Developing new forms of partnership and cooperation between sectors is one of the most pressing needs. Ensuring that information exchange takes place, especially in the form of warning, alerting and threat analysis, is a priority for private and public sectors alike both in Europe and further afield.

DDSI and EWIS provide an initial comprehensive baseline of the various problems and possible solutions. Nevertheless, these are just the first steps. There is now the opportunity to build on these national and European initiatives to ensure that coherent and interoperable warning and alerting architectures are developed at the global level. By trying to engage North American and Asian organisations, it will be possible to find joint solutions for enhancing the overall dependability of information and network systems. If successful, they will go a long way towards helping to build a safe and secure Information Society.

---

<sup>1</sup> An overview of several initial activities is available at the website of the European Dependability Initiative at <http://deppy.jrc.it> (visited on 20 August 2001)

<sup>2</sup> European Council, Presidency Conclusion, Lisbon European Council, Marc 23 -24 March 2000, available at [http://europa.eu.int/comm/off/index\\_en.htm](http://europa.eu.int/comm/off/index_en.htm) (visited 20 August 2001)

<sup>3</sup> European Commission, E-Europe: Information Society for All-Action Plan 2002 available at [http://europa.eu.int/information\\_society/eeurope/action\\_plan/actionplantext/index\\_en.htm](http://europa.eu.int/information_society/eeurope/action_plan/actionplantext/index_en.htm) (visited 20 August 2001)

<sup>4</sup> Document available at <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html> (visited 20 August 2001)

<sup>5</sup> European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Network and Information Security: Proposal for a European Policy Approach, 6 June 2001, p. 3, available at [http://europa.eu.int/information\\_society/eeurope/news\\_library/new\\_documents/index\\_en.htm](http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm) (visited on 20 August 2001)

<sup>6</sup> *ibid.*