Our society is heavily dependent on distributed systems and services in which networked computers play a central role in controlling communications, databases and infrastructures.

There are several drivers for research over the next few years:

- **Network Architecture:** Peering forward into the future, two key challenges present themselves. The first is satisfying the demand for pervasive connectivity and seamless roaming ("Internet as infrastructure") between competing technologies and markets. The second challenge is to convert today's data networks into "human networks" with a focus on user services. Promising directions here may leverage peer-to-peer and network overlay techniques.

- **Operating Systems:** One key future direction is, as often the case in systems research, a revisitation of a hot-topic of the past: virtual machine monitors. Research projects in the United States (e.g. Denali at the University of Washington) and within Europe (e.g. the XenoServers project at the University of Cambridge) are reapplying VMM techniques to modern architectures with a view to supporting micro-services: components of Internet-scale applications which require only a small fraction of the resources of a server. Other intriguing avenues for future operating systems research include building tiny embedded systems for sensor network (or other extremely network systems), and support for 'ad hoc supercomputing' in the GRID.

- **Real-time Operating Systems:** In the near future, networked systems and operating systems will become even more important. Therefore, composability will be a central property of future real-time networks and systems (both large systems and small devices). Clearly, composability is only achievable if the necessary operating system and middleware support is provided. To facilitate this, appropriate specifications of composable real-time interfaces are needed.

- **Dependable Systems:** On Fault Prevention, the formal definition of security policies in order to prevent the introduction of vulnerabilities and the human factors issues in critical "socio-technical" systems. On Fault Tolerance, especially in embedded systems, state-of-the-art fault tolerance techniques cannot ignore that most faults experienced in real systems are transient faults. Other drivers concern fault-tolerance in large, complex distributed applications, the improvement of the robustness of COTS components, reflective technologies to allow introspection and intercession and the extensions to address security issues through the notion of intrusion-tolerance.
On Fault Removal, the development of statistical testing and robustness testing, and on Fault Forecasting, the establishment of a faithful and tractable model of the system's behavior, the analysis procedures that allow the (possibly very large) model to be processed and the use of fault injection techniques to build dependability benchmarks for comparing competing systems/solutions on an equitable basis.

- The World Wide Web. The development of dependable distributed systems based on the Web Services Architecture is an active area of research that is still in its infancy. A number of research challenges are thus yet to be addressed to actually enable the dependable composition of Web Services. Issues include the thorough specification of individual Web Services and of their composition, so as to ensure the dependability of the resulting systems as well as to allow the dynamic integration and deployment of composed services. Also, associated dependability mechanisms should be devised to enable full exploitation of the dependability properties enforced by individual Web Services and also to deal with the specifics of the Web. Another issue relates to allowing the deployment of Web Services on various platforms, ranging from resource-constrained devices to servers.

- Distributed Event-based Systems: A heartbeat infrastructure is needed to cope with the distributed system characteristics of service and network failure. Work on federated systems must continue and allow communication between domains and event system within those domains. Access control (visibility or scoping) also must be addressed. A further interesting direction is the wide-scale deployment of event systems over multicast (IP or overlay) to investigate the properties and problems of high-volume, wide-area, event notification.

- Mobile Computing: While in the past a significant research effort has been invested in relatively lower-level protocols and services, such as for instance, network access, routing-protocols, QoS preservation, or power consumption, in the future, it is expected that the emphasis will shift to the upper layers, covering issues such as middleware, security, human-interfaces, applications, etc. Research should address: a) virtual cellular networks and ad hoc networks, b) networking and routing protocols, c) middleware for ad hoc networks, d) power management, e) security and identity management issues and f) human interfaces and QoS.

- Network Storage Services: We can expect to see the commoditization of storage, and more precisely the integration of storage services into the network model. Some initial work here focuses on logistical networking, that is, considering storage and communication as tightly coupled problems and designing solutions accordingly. Other challenges for the future include building effective personal storage networks, enhancing data availability in times of network outage or partition, increasing information security, and raising the semantic level of access interfaces.

This is not a comprehensive list of topics and drivers for future research. We are aware that research on Architectures implies several other technological fields like Object and Agent technologies, Platforms technologies, System Configuration and Management and that using such architectures for “Ambient Dependability” implies the integration of many other aspects related to societal issues, which are outside the scope of this note. In any case we consider that advance in the previous fields will be very relevant for an Information Society which can be trusted.