



www.ddsi.org

National Dependability Policy Environments

FRANCE

Report Version: Final
Report Preparation Date: 1 November 2002
Classification: Public
Preparation led by: RAND Europe (NL)

Contract Start Date: 1 June 2001 Duration: 18 months
Project Co-ordinator: RAND Europe (NL)

Partner: RAND Europe (NL, Project Coordinator); King's College London (UK);
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);
Ernst Basler + Partner (CH), Isdefe (E)



IST-2000-29202

Project funded by the European Community
under the "Information Society Technology"
Programme (1998-2002)

Table of Contents

Overview of the Country’s Information Infrastructure 3

Main ICT Regulatory and Legal Developments 4

Assessment of Phenomena Undermining Dependability 5

Government Initiatives Aimed at Tackling Cyber-Security 6

Industry and Other Non-Government Activities Related to Dependability 7

Public-Private Partnerships 9

Research and Development 9

Overview of the Country's Information Infrastructure

France is one of Europe's most advanced ICT countries, although significant improvement is still necessary. In 1999, the revenues generated by ICT services totalled 54 billion EUROS. The share of ICT services represented 40% of the total ICT revenues and 50% of total ICT employees. Meanwhile, the telecommunications sector represented 57% of total ICT services revenues. In terms of employment, software services counted for just over half of all ICT employees in services.¹

Between 1992 and 1997, ICT intensity in France had an annual growth rate of 2%. This is significantly less than in Portugal, for example, where a growth of more than 10% was registered for the same period. In 1997, ICT intensity by component in France amounted to over 6% - less than the OCED average of almost 7%, although more than the average for the European Union.

In France, investment in 'knowledge' (R&D, software and public spending on education²) is high. In 1995, such investment represented 9-10% of the GDP, in contrast to the OECD average of 8%. In the same year, investment in physical equipment, as a percentage of French GDP, was close to 20% - just under the EU average.

Notwithstanding the positive trends indicated in the previous statistics, ICT penetration in households in France is relatively low. Only 35% of homes in France had access to PCs in early 1999, compared with 75% in Iceland and 65% in the Netherlands. Similarly, whilst in Iceland, USA and Sweden 42% of households had access to the Internet, in France this figure lagged behind at just 15%. The situation is, however, improving. In recent years there has been a rapid increase in household ICT penetration in France. In May 2001, one in five French people were connected at home, in contrast to one in twelve in November 1999. In December 2001, three quarters of white-collar workers were registered as computer-equipped both at work and home.³

The computer presence in business is also on the rise in France – increasing from 50 % in 1998 to 59.6 % in 2000. In large-sized enterprises, this percentage is higher, with 88 % in 1997 and 98 % in 1999. Greater still has been the increase in Internet presence, growing from 28% in 1997 to 60% in 1999. Again this figure is higher in large-sized enterprises, with 75% in 1997 and 98% in 1999. Software spending in business amounted to 36.3 Billion EUROS in 1997.⁴ In relation to other countries, however, France does not fair so well. The percentage of employees using e-commerce-enabling technologies in 1999 was close to 40% in France compared with 65 % in USA and Canada and 62 % in the UK.⁵

¹ Ministère de l'Economie, des Finances et de l'Industrie, L'industrie française des technologies de l'information et de la communication, (Paris, Les chiffres, édition 2001). pp.6-7.

² OECD definition, Information Technology Outlook, 2000.

³ Sessi, L'internet : les français se hâtent lentement, available at <http://www.premier-ministre.gouv.fr/francais/chiffcles/france.htm> (visited on 21 March 2002)

⁴ Secrétariat à l'industrie, Technologies et société de l'information, édition 1999 et Premier Ministre, La France dans la société de l'information, 1999.

⁵ OCED data.

The number of Internet users in France has increased from 1.1 million in 1997 to between 7 and 10 million in 2001, depending on the source of information.⁶ There were 6 million registered users in June 2001 versus 4.2 million a year earlier.⁷ One in five is a weekly user.⁸ However, the number of secure web servers per million habitants in France was less than 20 in 1999, compared with more than 120 in the USA. The number of Internet hosts is also relatively low. In July 1999, it stood at 25 per 1000 inhabitants, the EU average being 35 per 1000. By 2000, France had made little progress whilst other countries like the USA represented 230 per 1000, followed by Finland with more than 150 per 1000. The EU average remained at 35 per 1000. Mobile telephone presence in medium and large-sized enterprises represented 89% in 1999 and 98 % in large-sized enterprises.⁹

In terms of wireless penetration, in April 2001, France accounted for the highest share in Europe of wireless connections (including cable, satellite, ADSL/DSL and T1/specialised links) with 6% of all households connected. This was twice the level recorded in the UK and Spain.¹⁰

The e-commerce take up in France is also improving. Combined with Minitel, electronic commerce in France now amounts to around 2.2 billion EUROS.¹¹

Main ICT Regulatory and Legal Developments

On 25 August 1997 the Prime Minister made France's entry into the information and communication society a priority for Government action. Beyond its "technical dimension," he declared, "the emergence of an information society represents a political challenge and constitutes, in this respect, a primary preoccupation [for the Government]". Refusing to allow the "digital divide," he "decided to make up for France's lost time in the information technology domain, which could rapidly have grave consequences for competitiveness and employment."¹²

After much consultation, the PAGSI (Government Action Programme for the Information Society) was set up¹³ and adopted during the meeting of the Inter-ministerial Committee for Information Society (CISI) on 16 January 1998. The PAGSI listed the overall priorities to be tackled through six projects.

⁶ Chiffres clés, *L'internet en France*, available at <http://www.premier-ministre.gouv.fr/francais/chiffcles/france.htm> (visited on 21 March 2002)

⁷ Association des fournisseurs d'accès à Internet (AFA), available at <http://www.premier-ministre.gouv.fr/francais/chiffcles/france.htm> (visited on 21 March 2002)

⁸ Sessi, *L'internet: les français se hâtent lentement*, available at <http://www.premier-ministre.gouv.fr/francais/chiffcles/france.htm> (visited on 21 March 2002)

⁹ Secrétariat à l'industrie, *Technologies et société de l'information*, édition 1999 et Premier Ministre, *La France dans la société de l'information*, 1999.

¹⁰ NetValue figures quoted in *L'internet en France*, available at <http://www.premier-ministre.gouv.fr/francais/chiffcles/france.htm>

¹¹ Secrétariat à l'industrie, *Technologies et société de l'information*, édition 1999 et Premier Ministre, *La France dans la société de l'information*, 1999.

¹² Prime Minister quotation, available on <http://www.internet.gouv.fr/francais>, (visited on 21 March 2002)

¹³ Chantiers gouvernementaux, *Société de l'information*, PAGSI, available on <http://www.premier-ministre.gouv.fr>

First was education, for which a support fund of 79 million EUROS was allocated to connect secondary schools. Second was culture. Support mechanisms were set up for projects relating to the French language for example, and ninety-eight “Multimedia Culture Centres” were created. Third was the modernisation of government, in particular the systematic use of Internet standards, training for civil servants and the improvement of general public service.

The fourth project was electronic commerce. This initiative included new measures to assist companies in adopting ICT services and products. The fifth was research and innovation, which aimed to encourage start up companies through capital risk finance. In this context, a 137 million EURO fund was established. Under this project an information society programme was also granted 45.7 million EUROS for research. Lastly, the project concentrated on devising the appropriate regulations, such as the adaptation of French law for safer use of information technologies and networks and the liberalisation of encryption.

Since 2000, whilst the role of the PAGSI has been reinforced in some fields such as the security of information system, there has been a lack of significant progress on the legislative side (the Information Society Law). This seems to indicate a slowdown of the dynamism previously noted. In June 2001, the project Information Law¹⁴ was launched to both promote on-line confidence and contribute to a more democratic use of the Internet. The project, in particular, wants to promote access of digital information to citizens, establish a legal framework for electronic commerce, foster the development of digital networks and counter cyber-crime.

Assessment of Phenomena Undermining Dependability

According to the Central Direction of Security of Information Systems (DCSSI), the number of on-line criminal activities has been increasing exponentially. In 1999, over 90% of on-line criminal activities involved credit or debit card frauds. The remaining malicious activities related to paedophilia, racial and hate-motivated threats and provocations. In total, over 2500 cases were registered in 1999 causing around one million EUROS worth of damage.¹⁵

The Markess International-Synthec Croissance survey found that in 50% of the cases involving intrusions and breaches, there was a loss of confidential data. The remaining 50% involved the violations of internal networks and the spread of viruses.¹⁶ Moreover, according to Evidian, 56% of the breaches originated from inside the network perimeter, and are considered to be internal to the enterprise, versus 44 % which are external.¹⁷ More importantly, it has been noted that over 65% of the breaches are caused by errors by authorised users. Meanwhile, the other 35% are the result of deliberate actions.¹⁸

It has been argued that intrusions and viruses undermine users’ perceptions of safety and security. In France, safety fears are highest among transactors (53%) compared with information seekers (32%) and particularly compared with non e-Government users (7%). This would indicate that the need for safety is

¹⁴ The project on Information Law, available on <http://www.internet.gouv.fr/francais/textesref/pagsi2/lasi.htm> (visited on 21 March 2002)

¹⁵ DCSSI, *Augmenter la confiance*, available at <http://www.ssi.gouv.fr/fr/confiancefiches/fiche9.html>, (visited on 21 March 2002)

¹⁶ Markess International, Cercle Synthec Croissance, *Sécurité sur Internet chez les prestataires de services e-business*, septembre 2001, pp. 1-5.

¹⁷ Evidian, research paper, *A study into the diversity of e-security across Europe*, 2001, pp. 1-17.

¹⁸ Ibid.

paramount. However, security concerns relating to the provision of personal information over the Internet do not always prevent people from interacting on-line with government institutions. Only 47% of those who have made on-line transactions considered it unsafe to provide the Government with personal information.¹⁹

Government Initiatives Aimed at Tackling Cyber-Security

Security of Information Systems (SSI) and the fight against cyber-security are two of the priorities of the PAGSI action plan. France favours the legal and internal affairs issues proposed by the eEurope Action Plan. The French Government is also promoting international co-operation in the field with strong support to the Council of Europe cyber-crime convention²⁰.

Since the beginning of 2000, the means of Government action in the area of dependability have been reinforced. In May 2000, the Central Office for the Fight Against Hi-Tech Crime was launched²¹. It is linked to the French Ministry of Interior and co-operates with Interpol.²² Similarly, in 2000, a new Central Direction for Security of Information Systems (DCSSI) was created, linked to the General Secretary of National Defence (SGDN).²³ In structuring these initiatives, it does not seem that a full appreciation of the Y2K experience has been taken into consideration.

In 1998, France's Ministry of Economics, Finance and Industry had started an information communication campaign in order to raise awareness about the Millennium Bug risks particularly among SMEs. This campaign involved the creation of an ad-hoc website, free toll-free numbers and many targeted publications. The results of this communication strategy was very positive. According to a SOFRES survey, 91% of the French population heard of it and 80% of people interviewed found the campaign useful. Another pivotal benefit brought forward by these activities was the renewal of IT hardware and software inside many public and private organizations, as well as more general training on the risks associated with dependency with information and network infrastructures. Finally, it is important to indicate that a special fiscal regime related to Y2K was put in place and extended in 2000.

The strategy of the Security of Information Systems (SSI) involves two levels. First, the DCSSI contributes to the SSI Inter-Ministerial Committee and provides expertise to the public and private sector.²⁴ It also has a training centre dedicated to administration staff. Secondly, it co-ordinates activities among the different government administrations.²⁵

¹⁹ TNS consultants, Government Online, a national perspective, 2001 Benchmarking Research Study, Taylor Nelson Sofres, November 2001, pp.1-16.

²⁰ DCSSI, Augmenter la confiance, available at <http://www.ssi.gouv.fr/fr/confiancefiches/fiche1.html> (visited on 21 March 2002)

²¹ Ibid.

²² OCLCTIC, available at <http://www.interieur.gouv.fr/police/oclctic/index.htm> (visited on 21 March 2002)

²³ DCSSI, Augmenter la confiance, available at <http://www.ssi.gouv.fr/fr/confiancefiches/fiche1.html> (visited on 21 March 2002)

²⁴ DCSSI, Directive n°4201/SG, available at <http://www.ssi.gouv.fr/fr/reglementation/4201/index.html> (visited on 21 March 2002)

²⁵ DCSSI, Direction centrale de la sécurité des systèmes d'information, documentation, available at <http://www.ssi.gouv.fr/fr/dcssi/decretcdcscicissi.html> (visited on 21 March 2002)

Cyber-crime prevention, nevertheless, has been retained as one of the most efficient ways to foster on-line trust and security.²⁶ In addition to the necessary technical and management controls and processes, it also requires an exchange of data about vulnerabilities and threats, possibly through CERTs. In France, at present there are three types of CERTs²⁷. CERT-RENATER²⁸ is dedicated to the community of members of GIP RENATER (National Network of Telecommunications for Technology, Education and Research). The Renater network was the first network and was created in 1993. It gathers information and shares it among the network. Created in January 1999 and hosted at DCSSI, CERT-A is dedicated to the French administration sector²⁹.

In addition to these activities, France has started to devise the necessary Internet-friendly legal framework. Firstly, there has been a substantial relaxation of the French legislation in terms of cryptology, following the decree of 17 March 1999.³⁰ The Government decided to allow complete freedom to use encryption methods in France while, at the same time, adapting the means to combat the use of encoding methods for illicit purposes. Electronic signatures have also been recognised according to the terms of the EU directive.³¹ Finally, France is also committed to data privacy. The activities in this domain are in the hands of the National Commission for Computing and Liberty (CNIL), an independent administrative organisation established in 1978.³²

Industry and Other Non-Government Activities Related to Dependability

In France, industry and other non-Government activities related to dependability generally come under two major types of initiatives. Firstly, there is the creation of CERTs under a common international agenda. These initiatives have been examined in previous paragraphs. Secondly, there is the development of groups and associations focusing on dependability issues, dedicated to private businesses.

Both CERT-IST and CERT-intexxia aim to serve France's private sector as a contact point for security incident response.³³ These private CERTs interact with the French national security organisations, Secretariat General de la Defense Nationale (SGDN) and Central Direction for Security of Information Systems (DCSSI), in conjunction with CERT-RENATER and CERT-A. Both private organisations are also active at the international level since both are members of FIRST (Forum for Incident Response and Security Teams).³⁴

²⁶ DCSSI, Augmenter la confiance, available at <http://www.ssi.gouv.fr/fr/confiancefiches/fiche1.html> (visited on 21 March 2002)

²⁷ Qu'est-ce qu'un CERT?, available at <http://www.certa.ssi.gouv.fr/certa/cert.htm> (visited on 21 March 2002)

²⁸ CERT RENATER, available at <http://www.renater.fr> (visited on 21 March 2002)

²⁹ CERT-A, available at <http://www.certa.ssi.gouv.fr> (visited on 21 March 2002)

³⁰ DCSSI, Augmenter la confiance, available at <http://www.ssi.gouv.fr/fr/confiancefiches/fiche1.html> (visited on 21 March 2002)

³¹ Law of 13 March 2000 and decree of 30 March 2001, available at <http://www.legifrance.gouv.fr/citoyen/jorf> (visited on 21 March 2002)

³² CNIL, available on <http://www.cnil.fr/textes/text02.htm> (visited on 21 March 2002)

³³ CERT-IST, available at <http://www.cert-ist.com> (visited on 21 March 2002)

³⁴ FIRST, available at <http://www.certa.ssi.gouv.fr/certa/first.htm> (visited on 21 March 2002)

CERT-IST was launched with France Télécom and TotalFinaElf in January 1999.³⁵ Two French industry leaders, Alcatel and CNES, initiated its creation following a 1998 study on the weakness in information security. In January 2000, Sanofi Synthelabo also joined the network. CERT-IST benefits from the expertise of the Alcatel CIT Security Department, which provides operation and logistical support.³⁶ Moreover, it has been selected as a Project of Public Interest by the Ministry of Interior.³⁷

The CERT-Intexxia is part of Intexxia³⁸, a consultancy company specialising in risk analysis and security provision, which started its activities in September 1999. The department dedicated to the CERT was created in 2001. Intexxia clients primarily include financial as well as non-profit and governmental institutions. The company is an active member of CLUSIF and the AFNOR, the French Agency for Standardisation. CERT-Intexxia has been part of the TF CSIRT since 2001.

There are two main associations in France that address dependability-related issues. They are ISDF and CLUSIF.

Established in 1989 under the name Institute for Risk Management, the French Dependability Institute (ISDF) is strongly supported by the Department of Industry. The founding members were MFQ, AFIM and AFAV. This organisation is also supported by automotive, military and space industries and by professional organisations. The institute aims to develop connections with all the other national associations working in the dependability field and to become the official representative of France in international organisations. It also works towards the establishment of strong connections with industry and the fostering of information exchange.

CLUSIF is a non-profit organisation of over 300 members.³⁹ Since its establishment six years ago, it has been documenting and analysing threats, offering sources of news, establishing a list of new risks, completing analysis reports and providing references on the subject of security of information systems.

Another dependability-related organisation is CIGREF. It involves over 100 companies, excluding IT suppliers and providers.⁴⁰ The members include banking and finance (13 %), energy (4 %), industry (25 %), insurance (14 %), research (4 %), retail (7 %), services (20 %), social and health services (7 %) and transport (5%). They include all major French companies. One of CIGREF's strengths is its role in fostering exchange of information and best-practices, including information security.

Other clubs like the SEE (Society of Electricity, Electronic and TIC)⁴¹ have developed specific working groups on dependability or, as in the case of Groupement des Cartes Bancaires⁴², have created e-commerce working groups that deal with information security.

³⁵ CERT-IST, available at <http://www.cert-ist.com> (visited on 21 March 2002)

³⁶ From 1994 to December 2000, this department was part of Alcatel TITN Answare.

³⁷ CERT-IST, available at <http://www.cert-ist.com> (visited on 21 March 2002)

³⁸ CERT-Intexxia, available at <http://www.intexxia.com> (visited on 21 March 2002)

³⁹ Clusif, available at <http://www.clusif.asso.fr> (visited on 21 March 2002)

⁴⁰ Cigref, available at <http://www.cigref.fr> (visited on 21 March 2002)

⁴¹ SEE, available at <http://www.see.asso.fr> (visited on 21 March 2002)

⁴² Groupement des cartes bancaires, available on <http://www.gie-cartes-bancaires.fr> and www.cartes-bancaires.com (visited on 21 March 2002)

Public-Private Partnerships

The information sharing initiatives among private, public and individual actors are still limited in France. These kind of initiatives have traditionally been handled by the Ministry of Finance, Economics and Industry and by the Ministry of Research. The emphasis on PPP is particularly strong in the research field. The French administration, nevertheless, has developed a volunteer policy aimed at extending innovation and research to market development. In addition, a Strategic Council of Information Technologies (CSTI)⁴³, linked to the Prime Minister, was launched in April 2001. Its aims are to ensure a better co-ordination between public-private actors in research; to create a dialogue with enterprises so as to bridge the gap between fundamental research and development; and to direct exchanges between researchers, industrialists and the French administration.

That said, the only private-public partnership involves the Project Oppidum⁴⁴, which was initiated by the Ministry of Industry to promote information security related R&D. The Oppidum project has distributed a total of 6 million EUROS to date.⁴⁵

Research and Development

In 2001, Technologies of Information and Communication (NTIC) research represented the second priority of the Government and of the Inter-ministerial Committee for Scientific and Technology Research (CIRST)⁴⁶. There were four major axes in the policy, of which two are directly relevant to dependability: the National Network of Telecommunication for Technology, Education and Research (RENATER); and the RNRT (National Network of Telecommunications Research) and the RNTL (National Network for Software Technologies)

RENATER was created in 1993 and among its founders there are the National Centre of Scientific Research (CNRS), the National Institute of Automatic and Software Research (INRIA), the Commissariat in Atomic Energy (CEA), the National Ministry of Research and Technology (MNRT), the National Centre of Spatial Studies (CNES) and Electricité de France (EDF)⁴⁷. Its activities were refreshed in 1999. RENATER has a CERT co-ordination body of four people that interact with 700 correspondents scattered around 75 universities and 150 engineering schools. This team is composed of four people and financed by the Ministry of Research.

The RNRT⁴⁸ was created in 1998 for a period of five years. Its goal is to co-ordinate and promote public-private research projects dealing with the Internet, multimedia, mobile phones, satellite constellations and the like. This network involves, *inter alia*, France Telecom R&D, INRIA, CEA, CNRS. Financing comes from the Ministries of Economics, Finance and Industry. Up to this moment, over 166 projects has

⁴³ CSTI has dedicated web site <http://www/csti.gouv.fr> (visited on 21 March 2002)

⁴⁴ Appel à projet "Oppidum", available at http://www.telecom.gouv.fr/programmes/pna_oppidum.htm (visited on 21 March 2002)

⁴⁵ Interview with the Ministry of Industry

⁴⁶ CIRST, available at <http://www.recherche.gouv.fr/recherche/politic/cirst2.htm> (visited on 21 March 2002)

⁴⁷ CERT RENATER, available at http://www.renater.fr/securite/cert_renater.htm (visited on 21 March 2002)

⁴⁸ RNRT, available at <http://www.telecom.gouv.fr/rnrt> (visited on 21 March 2002)

received financing from the RNRT for about 334 million EUROS. More than 50% of the projects are connected with a small and medium sized enterprise.

The RNTL was founded in 1999 and aims to promote software-related R&D co-operation between public and private institutions. It participates in several EU funded projects and supports several national initiatives.

Levels of funding

The NTIC budget of the Ministry of Industry represents 182 million EUROS, of which 50% is devoted to support European projects.⁴⁹ The rest is dedicated to national networks including the RNRT and the RNTL. On a yearly basis, the ministries in charge of Research and Telecommunications assign 10 million EUROS to research projects and 30 million EUROS to industrial R&D⁵⁰. An additional 150 million EUROS will be directed to the national research budget in order to employ an additional 25% of researchers in this area.⁵¹

The NTIC budget of the R2IT (Networks of Technological Research and Innovation) and the National Centres of Technological Research (CNRT) is also set to grow by 50%. Meanwhile, the Group of Telecommunications Schools (GET) will benefit from an increase of 400 to 600 researchers in the coming five years.⁵² Finally, the National Centre of Software and Automatic Research at INRIA will have its research and administration budget increased over the next two years⁵³. Over 200 new positions will be created in 2001 and 2002.

Research centres

The LAAS (Laboratory for Analysis and Architecture of Systems)⁵⁴ is part of the CNRS and was created in 1967. The LAAS totals 454 employees with an average annual budget of 6 million EUROS. It has developed 30 co-operation agreements with 15 countries. It is one of the world's leading research institutions in the field of dependability. The CELAR (Electronic Centre of Armement)⁵⁵ employs over 700 researchers and has a dedicated technical defence centre for information warfare. It has developed national and international projects including issues such as security of information systems, technology of electronic components, electronic war and satellites, information systems and telecommunications.

⁴⁹ Interview with the Ministry of Industry

⁵⁰ Interview with the Ministry of Industry

⁵¹ Ministère de la recherche, <http://www.recherche.gouv.fr/recherche/politic/cisi/00.htm> (visited on 21 March 2002)

⁵² Ministère de la recherche, <http://www.recherche.gouv.fr/recherche/politic/cisi/00.htm>, (visited on 21 March 2002)

⁵³ Ministère de la recherche, <http://www.recherche.gouv.fr/recherche/politic/cisi/00.htm>, (visited on 21 March 2002)

⁵⁴ LAAS, available at <http://www.laas.fr>, (visited on 21 March 2002)

⁵⁵ For more information the CELAR, <http://www.rennes-atalante.fr/directory/celar.html>, (visited on 21 March 2002)