Roadmapping Future E-Government Research

Government's role and responsibilities in the virtual world

Melanie Bicking
University of Koblenz-Landau, Institute for IS Research,
Research Group eGovernment
Universitaetsstr. 1, 56070 Koblenz, Germany
Tel: +49 261 287 2646, Fax: +49 261 287 100 2646
bicking@uni-koblenz.de
WWW home page: http://www.uni-koblenz.de/FB4/Institutes/IWVI/AGVInf

Abstract: Global electronic markets, virtual organisations, virtual identities, virtual products and services, and Internet-related crime are growing in prominence and importance. In a world that is increasingly non-physical and borderless, what are government's roles, responsibilities and limitations? The Internet plays a central role within the transformation process from traditional governments towards modern and innovative government that the requirements of an Information Society. Based on the findings of the eGovRTD2020 project, that aims at identifying key research challenges and at implementing a model for a holistic government with horizon 2020, this paper explains the necessity to investigate and understand the Internet and in particular government's role and responsibilities in it. Furthermore, the paper provides a research roadmap that details how to address certain issue related research questions.

1 Introduction

Many countries, as well as the European Union, ranked the development of an Information Society very high at their agenda. Scanning existing strategic documents and policies, international and national strategies focus often on research issues related to trust and security aspects, as well as user acceptance. At the moment

governments main interest in the virtual world is on how to deliver electronic public services secure through the Internet. Analysis of several strategic documents indicate a common awareness across Europe that people and business will only use online services if data transfer and transactions are secured and protected. Hence European governments fund research and development on security issues, e.g. Digital Rights Management (DRM). But the virtual world offers much more opportunities and threats than discovered by now. The Internet is a paradise not only for information search and customising but also for all kinds of criminals 00. Global electronic markets, virtual organisations, virtual identities, and virtual products and services are increasingly prominent. Governments all over the world have to face this growing new world. First problems and challenges appeared through increasing movie and music piracy via peer-to-peer systems established in the Internet. Existing legal frameworks, as well as law enforcement methods and tools were very high ranked in agendas of several governments. Following questions came up and needs still to be answered: How to regulate the Internet? What are government's role, responsibilities and limitations in a world that is increasingly non-physical and borderless?
Within the foci of the 6th Framework Programme of Information Society Technology (IST) that address "ICT research for innovative Government" and "Strengthening the Integration of the ICT research effort in an Enlarged Europe"0 the EC funded the project eGovRTD2020. This project is a specific support action in order to develop a research roadmap for eGovernment in 2020. It aims at identifying key research challenges and at implementing a model for a holistic government with horizon 2020. Key findings from the eGovRTD2020 project leads to insight that government's role and responsibilities in the virtual world are still unclear but it will be necessary for governments to become more proactive in the Internet. The following chapters introduce the methodology of eGovRTD2020 and point out those research themes and activities, as well as actors needed in order to investigate and define government's role and responsibilities in the virtual world.

2 Overall methodology to develop an eGovernment research roadmap

This chapter is about the underlying holistic reference framework of eGovRTD2020 (see Fig. 7). It introduces the overall methodology of the eGovRTD2020 project that is applied to develop research roadmap for eGovernment 2020.

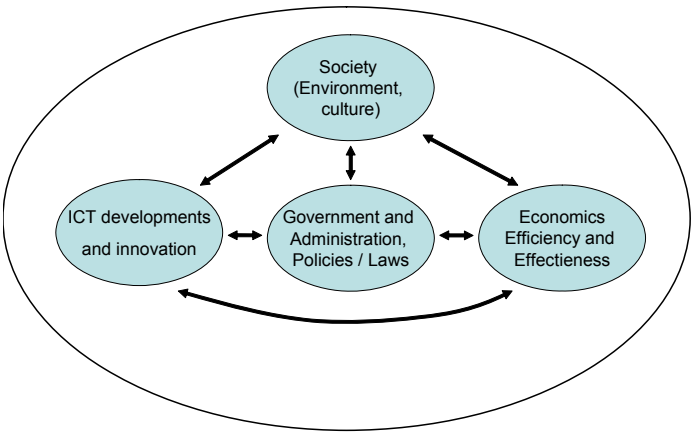

Fig. 7, Holistic reference framework of eGovRTD2020 0

According to the EC 00 "eGovernment is the use of information and communication technologies (ICT) in public administrations - combined with organisational change and new skills - to improve public services and democratic processes and to strengthen support to public policies." Besides, the United Nations (UN) 0 defines eGovernment as "a government that applies ICT to transform its internal and external relationships". Each of above mentioned definitions underscore the growing awareness that eGovernment should be based on considerations from technology, social, organisational, economic and legal areas that guided the investigations of the overall project methodology that is divided in four successive steps (see

2).

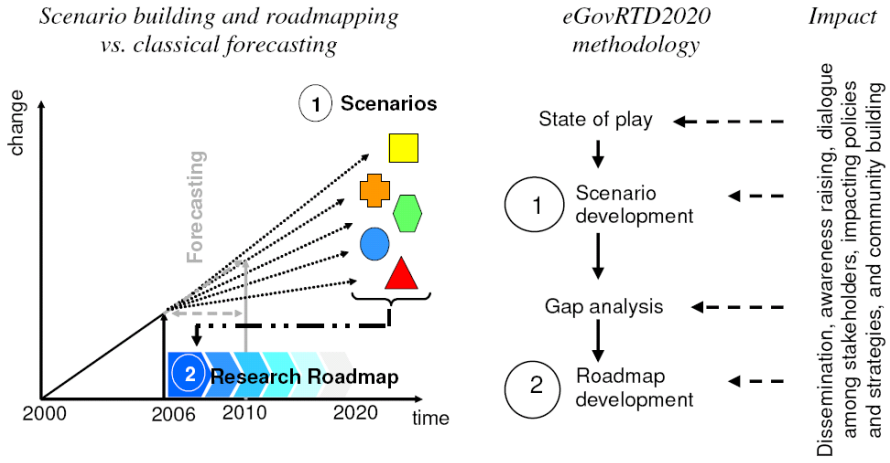

Fig. 2, eGovRTD2020 overall methodology to develop an eGovernment research roadmap for innovative Governments in 2020 0

The holistic framework of eGovRTD2020, depicted in Fig 1, bases on the above named definition of the EC. A key function within the project was to take the EC definition and breaks the broad definition down into a framework in order to make it easier to process the single aspects in the following steps.

In step 1 current status of eGovernment research and eGovernment strategies is given in order to outline trends related to design the current eGovernment transformation process through research (cf. 0). For instance, several strategies and research programmes focus on security issues. All eGovernment services are or will be delivered through the Internet face security issues, e.g. data protection. Consequently, many eGovernment strategies focus on research and development in order to develop a secure communication infrastructure. In this context the following topics of interest are mentioned several times, for example data protection, identity management, authentication, secure data and information transfer.

In step 2 different visions of the future were built up during a series of regional workshops in Europe, the USA and Australia. Experts from those regions develop scenarios about governments interacting with society and market through innovative ICT and thereby creating a certain public value (cf. 0). In the end 29 scenarios were carried out in seven workshops. In order to condense the scenario results and to provide a reasonable and manageable amount of input for the roadmapping workshops, the scenario analysis aims at identifying a minimal set of three key dimensions (contextual environment, trust in government and scope of government service provision) to classify the 29 scenarios and derive a final set of eight consolidated scenarios. The scenarios draw pictures of future eGovernment in which ICT penetrates every part of every day life. In this context ICT networking and convergences of ICT are often mentioned. Besides, expectations that governments all over the world will cooperate and collaborate through ICT networks and the Internet, in several scenarios internet crime and the loss of data privacy through the internet is pointed out. It follows from this that many experts are concerned about developments in the Internet.

Step 3, the gap analysis, extracts the major discontinuities, unknowns, and contrasts between the situation today and the alternative futures. The object of analysis might be classified as a problem 000 or as a gap 0. During analysis redundancies across the gap descriptions occurred and have lead to the insight that sometimes one or several gaps might be clustered or even merged. Hence the gap storylines were developed in order to show the interrelationships and interdependencies between the identified gaps. Gaps and gap storylines such as cyber wars and crimes, information access and transparency, crisis management, intellectual property, changing public values, virtual borders and citizenship, automatic monitoring and enforcement, competition among nations, rationalise the legal framework for eGovernment, standardisation of laws, regulations and taxes were identified in this step (cf. 0). They serve as foundation of the research theme "government's role in the virtual world" and of the corresponding roadmap (see Fig 3). Lastly on this basis, a research roadmap for the transformation process was developed within a second round of targeted workshops. The roadmapping effort was to examine the scenarios, gaps, and detailed underlying data from the

international workshops in order to review scenarios, prioritise gaps, and propose and phase research themes and actions. The final outcome comprises thirteen recurring themes that cut across the current state, the future scenarios, and the gaps in current practice and knowledge. The following chapter traces the line of argumentation through related aspects of government's role in the virtual included in the state-of-play and the future scenarios to the gap analysis. It concludes with the final research themes and actions that should be addressed in future.

3 Government's role and responsibilities in the virtual world

Within the last years Internet related crime became more and more popular in media since music and movie industry have suffered high losses when people started to swap songs and movies at Internet exchange meets. Currently main research and development efforts to actively counteract this kind of Internet related crime are undertaken by affected industries, consumer protection agencies and other private parties. Although governments expend efforts in setting up a proper regular framework for Internet related crimes in general, they are not really able to enforce these laws. What is the best regulatory framework good for, if there is no way to execute and enforce it? In the physical world governments know their role including obligations and restrictions with regard to crime prevention and prosecution. They have proved methods and means for law enforcement. Every Nation found its own way not only to deal with crime but also balance freedom and security. They set up policies and laws to protect both within its borders. These physical borders ground the variety of different nation depended individual rights. In the course of globalisation authorities of the different countries negotiated responsibilities in cases of international crime and consequently international law enforcement. But within the virtual world national borders disappeared and with it the enforcement of any national law becomes not only extraordinarily complex in general but also impossible in particular cases. Government's protection got lost in majority of cases. International cooperation 0 is often pointed out as crucial in regard to eGovernment in Europe. According to the Maastricht Treaty 0 the European Union bases on the following three main pillars:

1. European Community
2. Common Foreign and Security Policy
3. Police and Judicial Co-operation in Criminal Matters

The two last pillars are strongly related to government's role in the virtual world and substantiate previous argumentation for more cooperation in matters concerning the virtual world including Internet related crime.

However, several future scenarios mention that the trend of collecting more and more data is certain. But it is uncertain how these data will be used0. In addition several scenarios point out increasing competition between nations and global regions. In regard to government's role at regulating the Internet both leads to the question: What will happen if one or more governments extend efforts to strongly regulate the Internet? History is full of examples that changing balance of powers has been lead to strong reactions from affected people. Two fundamental principles of

western societies will be threatened by such developments. On the one hand there is freedom of opinion and on the other hand there is the right to privacy. The definition and therewith the protection of both variegates from country to country and within the borders of one country the protection of corresponding law is more or less guaranteed. But within the virtual world there are no explicit borders that would protect the individual against violations of unauthorised third parties, both individuals and organisation, as well as governments themselves. Consequently research question 1 arises: *How to translate national law into the Internet?*

There is a need to investigate what is realisable and what are restrictions? Is it possible to build up national borders in the Internet and do we really want virtual borders? A further solution might be the development of an international legal framework and enforcement. If national law solution is preferred for whatever reasons, then research question 2 is: *How to generate national borders in the virtual world?* If international law solution (see 0 ‘The new eWorld order‘) is favoured, then research question 2 is: *Who will then execute the law? Who will watch the watchers?*

However, the Internet is the first medium that supports individual and mass, synchronic and asynchronic, supply- and demand-oriented, moderated and unmoderated, personalised and anonymous, open and encrypted communication at the same time 0. The virtual world is world of imagination, re-imagination where people can have multiple identities and change identity if necessary. For instance, if one identity is regulated by government, people will create a new one. From this it follows the question: *What kind of virtual citizenship might appear*? Many people are living a second life within the Internet. For instance they are working and/or ‘living’ within the Internet. Virtual companies are making huge revenues because they are not paying taxes. At present there is a lack of taxation for virtual companies in the Internet. One approach to monitor and control Internet taxation might be the regulation of cash flows through physical banks. However, question still keeps how to apply and execute national tax systems in the Internet? For governments in general the question should be interesting, *what money governments might extract from the virtual world by e.g. taxation?*

At the moment the virtual world is faster than any regulating mechanism can react. Governments are always in the pursuit mode. Coherence and appearance is mentioned as requirement in order to regulate the Internet. Institutions are trapped in structural models. Acceleration of the regulation process has its own way on the grounds of democracy. Consequently regulation needs its time at the moment. But in future the adaptation of regulating mechanism needs accelerated modifications. There are two ways to approach the problem.

1. *Slow down Internet dynamics:* What are the conditions for sustainability in the virtual world?
2. *Accelerate legislative reforms:* What are the conditions for anticipation and flexibility in legislative?

Present approaches to change institutions towards new environmental needs and restrictions call for the challenge to jump the quantum for research. But participants claimed enthusiasm for smoother changing of institutions instead of fast revolution. Governments should not wait until the situation escalates. Because of capacity restrictions, changes should be carried out not so quick if something happens.

Decentralisation as far as possible, and with it anarchy, is one of the fundamental structural attributes of the Internet 00. Hence self-regulation within the Internet is the most popular kind of regulation because governmental regulation is very hard and maybe impossible to transform *properly*. Future research should identify what cases of Internet crime, e.g. protection of intellectual property, minors, etc. need to regulate by national or international law and governments, and what cases are better self-regulated 0. Within the virtual world things changing so fast that learning to adjust ourselves are also needed. However, only self-regulation might lead to anarchy within the Internet. In the case of data and privacy protection, individual concerns might lead to living in an Internet free zone.

If an Internet crime is discovered, prosecution will be required. But challenge is how to prosecute a crime in the Internet without coherence and appearance? Consequently governments need to know what the conditions for sustainability are in the virtual world.

In summary the following key research questions need to be addressed in future:

- What are government's roles, responsibilities and limitations in a world that is increasingly non-physical and borderless?
- Is a different legislation needed for the cyberspace? What is needed if national laws are to be translated into the Internet, e.g. to generate virtual national borders or to set up global international legal framework? If new international laws are needed, who will define and who will implement the laws?
- Who will monitor the legislators of international cyber laws? Who could be in possession of the sovereign power? What will happen if only a few governments undertake efforts to strongly regulate the Internet?
- What kind of virtual citizenship will appear?

summarises the research questions needs to be addressed in future and assigns them to the actors involved and needed for investigating the research questions.

Table 1. Phased actions for the research theme "Government's role in the virtual world"

No.	Description	Means	Actors	Timeline
1	Studies to investigate a proper understanding of the nature of the internet and where these characteristics challenge Governments to intervene in terms of action, reaction, prevention, and legislation, including the Identify current challenging trends in the Internet that require government action, intervention and regulation in order to prevent e.g. crimes Identify currently existing internet activity monitoring and crime prevention detection Linking trends with activities and actors, and assess the specific aspects that require government interaction (Privacy, data access, Intellectual property rights (IPR), criminal actions)	Risk and trend analysis, desk research, SWOT analyses, surveys, comparative studies, establishment of international expert groups	Research with key players from Governments, Politics and civic sector representatives	2007 -> 2009
2	Perform futures analysis on the basis of critical trends and evolutions identified, with specific focus on: Risks of cyber crime, cyber terrorism, spamming, spoofing, manipulation of the virtual world code of conduct, etc. Usage of the Internet as a crucial platform of communication in cases of catastrophes and near- What are the potential dangers and opportunities of internet, where government needs to clearly regulate the way and means as well as priorities of action in such scenarios	SWOT analysis, Scenario building, Trend analysis, risk analysis, analysis of critical interdependencies and hazardous situations	Researchers, legal experts, Governments and ICT industry	2008 –> 2010
3	Develop mechanisms and framework in order to monitor activities and trends in the virtual world; and to assess these activities and changes in terms of how far governments will be required to regulate imbalanced internet activities of stakeholders	Change analysis, Trend analysis, surveillance and monitoring conceptual design, internet laws	Research with key players from governments and consulting	2008 -> 2012
4	Put needs of regulations, mechanisms and framework into action and implementation How to properly adapt and enlarge a legal framework for eCrime Mechanisms and tools for crime prevention and prosecution with regard to balance freedom and security How to create sustainability in the internet? Examples of virtual regulation areas: taxation; IPR, customs; trade; information sharing, data privacy, violence; cyber crimes; education, eHealth issues, virtual citizenship, etc.	Legal drafting and implementation, reengineering of national laws, pilot projects; European directives	Governments, with support from research and consulting	2010 -> 2020
5	Training and education to prepare and empower people to handle the virtual world and make them aware of the challenges and implications of using the Internet Introduction of awareness and education in primary schools and continuing till higher Concepts for life-long learning, especially for newcomers in the Internet aera and parents which enable their kids unsupervised and unmonitored	Curricula updates, development of training and education modules, Seminars and workshops for new internet users, pilot projects	Research and education, Government, Consulting	2010 -> 2020
6	Implementation and monitoring of impact of regulations and training	EU directives	Governments, Consulting, ICT Industry, Academia, Civic Society and NGO	2010 -> 2020

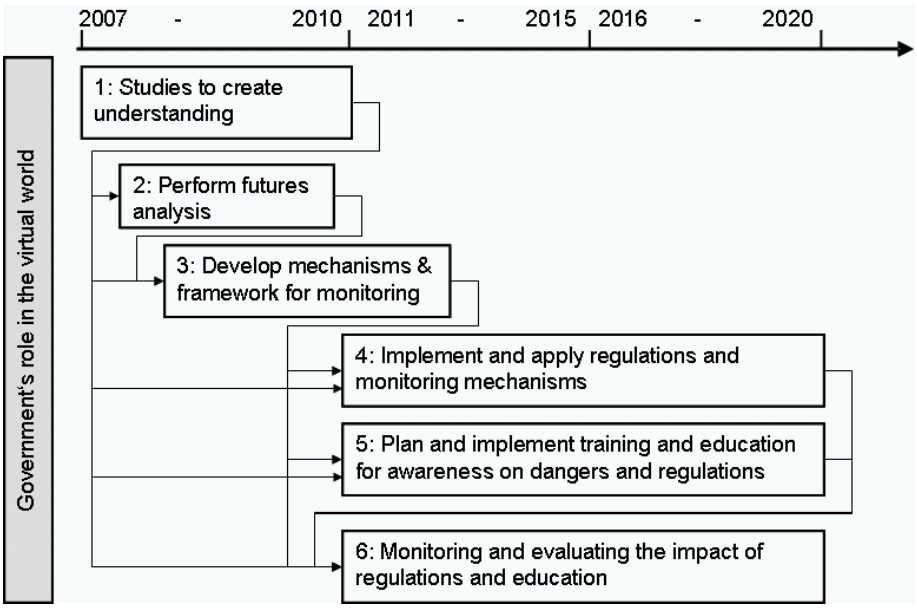

Fig 3, Phased actions for the research theme "Government's role in the virtual world"

In conclusion, although governments and private organisations already started to investigate the Internet, there is still a lack of effective laws, methods, measurements and technologies to enforce any law in the Internet. For instance the Centre for Socio-Legal Studies that is part of the Law Faculty of the University of Oxford discovered that existing laws, measurements and technologies are inappropriate to match the challenges of crime within the virtual world 0. However they pointed out that transparency of the Internet (e.g. standardisation of processes) is a key success factor for regulative interventions within the virtual world.

Concluding global electronic markets, virtual organisations, virtual identities, virtual products and services, and Internet-related crime are growing in prominence and importance. In a world that is increasingly non-physical and borderless, government's roles, responsibilities and limitations are currently not clear. Therefore research is absolutely necessary to discover the functional and structural basis of the Internet in general and to develop efficient and ethical correct laws and technologies to protect the individual, business and society. This task will be an essential part in order to create an information society. Participants of the Brussels workshop emphasised that doing nothing is the way to death. Now, the need for research about the virtual world is discovered, but governments still not react. Participants at the roadmapping workshops agreed that governments should not wait until the situation escalates. At this point more smooth changing of institutions is possible, instead of challenging institutions to jump the quantum for research towards a fast revolution later on. Governments need to identify their role in the new world. New power structures are coming up for younger people because they are growing up with the virtual world. In order to shape the future governments should understand what is next.

4 Conclusion

This paper shows that eGovernment, as a research discipline, is a complex and dynamic socio-technical system. Particularly, the question about government's role in the virtual world gives an idea about how complex and multifaceted eGovernment is. Also, the Internet itself is complex and dynamic system that serves for opportunities and threats whose extension we still not know. Chapter 3 depicts lacks of current eGovernment research regarding various Internet related issues concerning modern governments and in particular the Information Society. In future there is a particular need to focus research on the Internet and its impact related to governmental issues. At the moment governments main interest in the Internet is its deployment as a tool for service delivery but the eGovRTD2020 project finds out that the Internet's potential towards eGovernment is much more complex and extensive. Businesses both legal and criminal continue researching the potential of the Internet in order to find new fields of application useful for their business. From businesses findings about and business activities in the Internet, as well as from private activities a lot of areas of responsibility result for governments in the Internet. In future it will be absolutely necessary that government becomes more proactive in these relations. Laws, as well as law enforcement methods and tools are existing in the physical world do not meet the requirements of the virtual world.

However the chosen example, government's role and responsibilities in the virtual world, is just one research theme out of thirteen that is discovered by for 2020. The roadmapping methodology which is described in chapter 2 covers both transdisciplinary approach that resulted in broad field of investigation and a detailed analysis. Hence, the final roadmap comprises thirteen recurring themes that cut across the current state, the future scenarios, and the gaps in current practice and knowledge. Thereby each theme is the basis for a research roadmap. Chapter 2 introduces the research roadmap for government's role in the virtual world. But together with the twelve remaining research themes, the roadmaps cover the wide range of challenges needs to be addressed in future. Already years ago Alan Curtis Kay claimed that "the best way to predict the future is to invent it".

Acknowledgements

eGovRTD2020 (Roadmapping eGovernment research 2020, IST-2004-4-27139) is a specific support action co-funded by the European Commission under the 6th framework program of IST with the following partners: University of Koblenz-Landau (coordinator, DE), Delft University of Technology (NL), Center for Technology and Innovation Management (DE), Mykolas Romeris University (LT), University of Maribor (SI), European Institute of Public Administration (NL), Hautes Etudes Commerciales (FR), Australian National University, Center for applied philosophy (AU), Center for Technology in Government, University at Albany-SUNY (USA).

References

1. Bertelsmann Stiftung (2000) Selbstregulierung von Internet-Inhalten; http://www.bertelsmann-stiftung.de/cps/rde/xchg/SID-0A000F0A-C9914222/bst/hs.xsl/prj_8642_8650.htm

2. M. Bicking, M.A.Wimmer, *eGovernment research in Europe: findings from a recent state-of-play study.* In: Grönlund, A., Scholl, H.J., Andersen, K.V., Wimmer, M.A. (eds.). EGOV 2006 communications proceedings, Schriftenreihe Informatik # 18, Trauner Verlag, Linz, 2006, pp. 1-12

3. M. Bicking, M. Janssen, and M.A. Wimmer, *eGovernment 2020: Towards a Roadmap for future eGovernment research in Europe.* In: Cunningham, P., Cunningham, M. (eds.): Exploiting the knowledge Economy: Issues, Applications, Case Studies. Part 1, IOS Press, Amsterdam et al. (2006) 407-415

4. Capgemini (2005), Online Avaliability of Public Services: How is Europe Progressing? Web Based Survey on Electronic Public Services. Report of the Fifth Measurement Otober 2004. Online in the Internet; http://europa.eu.int/information_society/eeurope/2005/doc/all_about/egov_communication_de.pdf

5. Capgemini (2006), Online Avaliability of Public Services: How is Europe Progressing? Web Based Survey on Electronic Public Services. Report of the 6th Measurement June 2006. Online in the Internet; http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/online_availability_2006.pdf

6. Centre for Socio-Legal Studies (2004), Self-Regulation of Digital Media Converging on the Internet: Industry Codes of Conduct in Sectoral Analysis; http://pcmlp.socleg.ox.ac.uk/text/execsummary.pdf

7. CERT (2007), International Coordination for Cyber Crime and Terrorism in the 21st Century; http://www.cert.org/reports/stanford_whitepaper-V6.pdf

8. P. Checkland, *Systems Thinking, Systems Practice,* John Wiley & Sons, Chichester (1999)

9. Computer Crime Research Center, Fraud in the Internet (2005); http://www.crime-research.org/articles/Internet_fraud_0405/2

10. K. Dahmann, Überwachung oder Selbstregulierung? (2004); http://www.dw-world.de/dw/article/0,,1311400,00.html?mpb=de

11. eGovRTD2020 consortium, Deliverable D 3.1 – Gap Analysis Report (2006); http://www.egovrtd2020.org

12. eGovRTD2020 consortium, Deliverable D1.1 – State of Play report, (2006); http://www.egovrtd2020.org/

13. eGovRTD2020 consortium, Deliverable D 2.1 - Scenarios report (including regional workshops report), (2006); http://www.egovrtd2020.org

14. European Commission, Better Public Services, (2003); http://europa.eu.int/information_society/soccul/egov/index_en.htm

15. European Union, Treaty on European Union, (1992); http://europa.eu/eur-lex/en/treaties/dat/EU_treaty.html

16. R. Heeks, Most eGovernment-for-Development Projects Fail, IDPM, (2003). International Content Rating Association (ICRA 2006); http://www.icra.org/

17. IST, Fith Framework Programme. List of “key” actions, (2002); http://www.cordis.lu/fp5/src/key.htm (9th May 2006)
18. IST, A thematic priority for research and development under the specific programme “Integrating and strengthening the European research area” in the Community sixth framework programme, (Commission Decision C (2005) 5588 of 14 December 2005); ftp://ftp.cordis.lu/pub/ist/docs/wp_4th_update_en.pdf
19. G. Lenart, U. Hribar,, *Technology support for soft problem solving, Informatics and management,* ISBN 3-631-51869-2, Florjančič, J., Pütz, K. (eds.),P. Lang, Frankfurt am Main (2004).
20. M. K. Lottor, RFC 1296 Internet Growth (1981-1991). Menlo Park, CA, (1992); ftp://ftp.cs.tu-berlin.de/pub/doc/rfc/rfc1296.gz
21. S. Možina, R. Rozman, M.I. Tavčar, D. Pučko, Š. Ivanko, B. Lipičnik, J. Gričar, M. Glas, J. Kralj, M. Tekavčič, V. Dimovski, B. Kovač, *MANAGEMENT: nova znanja za uspeh,* (2002).
22. OECD, Glossary of e-Government Terms, (2007); http://webdomino1.oecd.org/COMNET/PUM/egovproweb.nsf/viewHtml/index/$FILE/glossary.htm Definition dates back to the year 2005
23. S. Stecklow, Computer Users Battle High Tech Marketers Over Soul of Internet. *Wall Street Journal,* (16.9.1994)
24. B. Sterling, A Short History of the Internet. THE MAGAZINE OF FANTASY AND SCIENCE FICTION, (1993); gopher://gopher.eff.org/00/Publications/Bruce_Sterling/FSF_columns/fsf5
25. B. Sterling, The Hacker Crackdown. *Literary Freeware*, (1994).
26. M.A. Wimmer, Approaching secure and trustful e-government applications: technology won't make it alone! In P. Cunningham, M. Cunningham, P. Fatelnig (Eds.), Building the Knowledge Economy: Issues, Applications, Case Studies. Part 1, *IOS Press*, Amsterdam et al, pp. 626 – 632 (2003).
27. M.A. Wimmer, “Integrated service modeling for online one-stop Government. EM – Electronic Markets”, *special issue on e-Government*, Vol. 12, No. 3, pp. 1-8 (2002).
28. M. A. Wimmer, B. von Bredow, “Sicherheitskonzepte für e-Government. Technische versus ganzheitliche Ansätze”. *In Datenschutz und Datensicherheit*, Vol. 26, 9/2002, pp. 536 – 541, (2002).