

EUROPEAN UNIVERSITY INSTITUTE
Department of Political and Social Sciences

**The Digital Challenge:
National Governments and the Control of the Internet**

By
Giampiero Giacomello

Thesis submitted for assessment with a
view to obtaining the Degree of Doctor of the
European University Institute

Florence, September 2001

B/C →

European University Institute



3 0001 0034 6465 0

EUROPEAN UNIVERSITY INSTITUTE
Department of Political and Social Sciences

6
R0280



**The Digital Challenge:
National Governments and the Control of the Internet**

By

Giampiero Giacomello

Thesis submitted for assessment with a
view to obtaining the Degree of Doctor of the
European University Institute

Examining Jury:

Prof. Richard Breen (EUI – co-supervisor)
Prof. Gary Chapman (University of Texas, Austin)
Prof. Giorgio Natalicchi (Università di Firenze)
Prof. Thomas Risse (EUI – supervisor)

Florence, September 2001

784.3

Vertical line on the left side of the page.

Vertical line on the right side of the page.

*This dissertation is dedicated
to the memory of my father,
a true visionary of electronic commerce.*

DISSERTATION ABSTRACT
The Digital Challenge

Only a few years ago, the Internet was still the domain of scientists and computer geeks. Today, scholars, businessmen, criminals and millions of ordinary people access "the Net" for the most diverse reasons. Its increasing social and economic importance has prompted governments into undertaking actions to regulate access and, sometimes, to control the Internet's contents. Because international cooperation has largely failed, governments have embarked on the technically costly and difficult operation of setting up national controlling mechanisms.

The dissertation explains why national governments attempt to control the Internet, using a liberal/domestic politics theoretical approach, and comparing it with another international relations mainstream theory, i.e. realism. Based on these theories, five competing hypotheses have been devised to explain my research question: 1) national security, 2) individualism level, 3) democratic structure, 4) degree of privatization/liberalization in the telecom sector, and 5) economic freedom/trade openness.

These hypotheses are first tested in Part I, through quantitative techniques (using proxies to represent the hypotheses and variations of the level of control, and with data freely available on the Net). In this part, the most significant result has been the intersection between the effects of de-regulation/liberalization in the telecommunications and the need for more control required by the logic of "national security" in the sampled countries. These circumstances have thus promoted an "accidental alliance" between pro-liberties NGOs, users' and consumers' groups and the private sector on the one side, and the national security communities on the other.

In Part II, in order to further clarify Internet control, three case studies (the United States, Germany and Italy) have been selected to further test my arguments. All the cases confirmed the findings of Part I, as well as the importance of that "accidental alliance" in the three democracies to stem efforts by governments to increase Internet control. Clearly, issues about letting the Internet spread, finding ways for it benefit the economy and society, or policing cybercrime or unwanted contents among users are challenges that national governments will continue to face.

Vertical line on the left side of the page.

Vertical line on the right side of the page.

TABLE OF CONTENTS

| | |
|---|------------|
| ABSTRACT | iii |
| LIST OF ABBREVIATIONS | ix |
| ACKNOWLEDGMENTS | xv |
| | |
| 1. CHAPTER ONE – INTRODUCTION | 1 |
| 1.1 “On the Internet Nobody Knows You Are a Dog!” | 1 |
| 1.2 The Research Question (Where It Comes From and Why It Is Important) | 6 |
| 1.3 Specifying the Dependent Variable | 9 |
| 1.3.1 Freedom of Expression and Censorship | 9 |
| 1.3.2 Privacy and Data Protection | 11 |
| 1.3.3 Cryptography | 16 |
| 1.3.4 The Domain Names System Electronic Business and the New Economy | 19 |
| 1.4 The Competing Hypotheses | 22 |
| 1.5 Your Meter or My Scale? Measuring the Level of Internet Control | 28 |
| 1.6 A Summary of Conclusions | 31 |
| 1.7 The Singular Nature of the Internet | 39 |
| 1.8 The Internet and the Study of International Relations | 43 |
| 1.9 The Dissertation’s Structure | 47 |
| | |
| 2. CHAPTER TWO - A BRIEF HISTORY OF THE INTERNET | 49 |
| 2.1 Introduction: “The Accidental Superhighway” | 49 |
| 2.2 Making Internet History | 51 |
| 2.3 A History of the Future | 59 |
| 2.4 Some Concluding Remarks about the Future of the Internet | 67 |
| | |
| Part I | |
| | |
| CHAPTER THREE - THE QUANTITATIVE ANALYSIS OF INTERNET CONTROL | 71 |
| 3.1 Introduction | 71 |
| 3.2 The Methodology | 72 |
| 3.2.1 Working Hypotheses and Indicators for Variables | 72 |
| 3.2.2 Internet Levels of Control (LOC): Dependent Variables | 75 |
| 3.2.3 Control Variables | 77 |
| 3.2.4 The Step by Step Procedure | 79 |
| 3.2.5 The Sample and Data-Related Problems | 80 |
| 3.3 Test Results | 86 |
| 3.3.1 Multivariate Regression Results | 88 |

| | |
|--------------------------|----|
| 3.3.2 Multicollinearity | 94 |
| 3.3.3 Heteroskedasticity | 95 |
| 3.4 Conclusions | 96 |

Part II

| | |
|--|-----------|
| INTRODUCTION - THE QUALITATIVE ANALYSIS (Methods and the Selection of Case Studies) | 99 |
|--|-----------|

| | |
|---|-----|
| II.1 Case Study Methodology | 99 |
| II.2 The Countries: Why Are They All Democracies? | 101 |
| II.3 Some Final Remarks on Sources for the Case Studies | 104 |

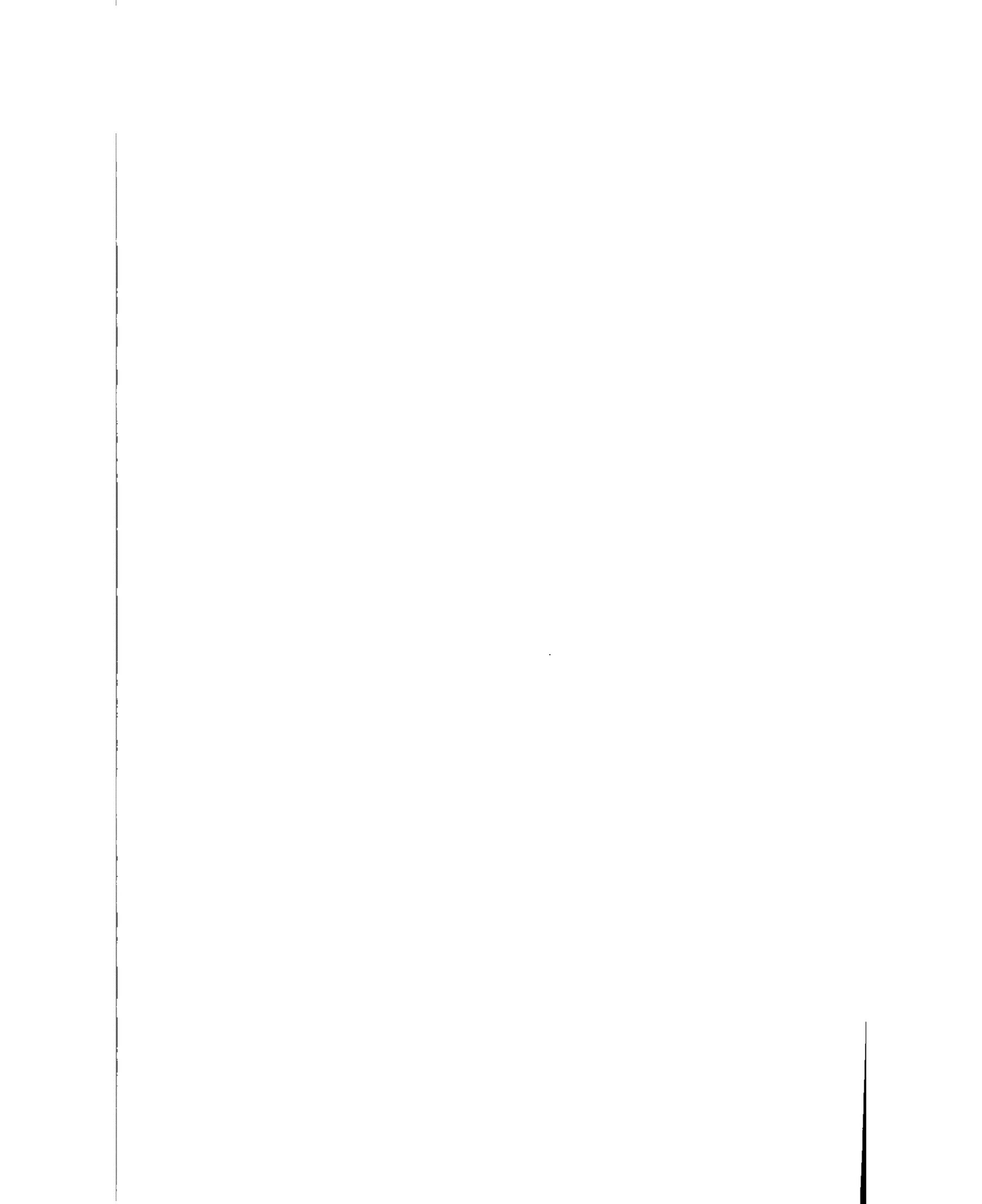
| | |
|--|------------|
| CHAPTER FOUR - THE UNITED STATES: THE SOLE INFORMATION SUPERPOWER | 109 |
|--|------------|

| | |
|--|-----|
| 4.1 Introduction | 109 |
| 4.2 The Complexity of the American Decision-Making Machinery | 112 |
| 4.3 The Chronology of the Debate | 115 |
| 4.4 The Main Players of the Internet Debate | 120 |
| 4.4.1 The Government | 121 |
| 4.4.2 Congress and Judiciary | 130 |
| 4.4.3 The Industry | 133 |
| 4.4.4 NGOs and Private Groups | 136 |
| 4.5 Current Issues of the Debate | 139 |
| 4.5.1 Freedom of Speech | 142 |
| 4.5.2 Privacy | 144 |
| 4.5.3 Free Use of Cryptography | 147 |
| 4.5.4 The National Information Infrastructure (NII) | 152 |
| 4.5.5 Domain Name System (DNS) | 159 |
| 4.5.6 The "e"-economy | 163 |
| 4.6 Conclusions | 166 |

| | |
|--|------------|
| CHAPTER FIVE - GERMANY: "DAS NETZ ÜBER ALLES" | 171 |
|--|------------|

| | |
|--|-----|
| 5.1 Introduction | 171 |
| 5.2 Historical Background | 172 |
| 5.3 The Main Actors | 180 |
| 5.3.1 The Government | 180 |
| 5.3.2 The Private Sector, Consumers' Organisations and Users' Groups | 188 |
| 5.4 The Issues | 190 |
| 5.4.1 Freedom of Speech and Neo-Nazi Propaganda | 191 |
| 5.4.2 Privacy | 194 |

| | |
|---|------------|
| 5.4.3 Encryption and Digital Signature | 197 |
| 5.4.4 New Economy, e-commerce and ICANN | 199 |
| 5.5 Conclusions | 202 |
| CHAPTER SIX - ITALY: THE ELUSIVE INFORMATION SOCIETY | 205 |
| 6.1 Introduction | 205 |
| 6.2 Historical Background | 207 |
| 6.3 The Main Actors | 217 |
| 6.3.1 The Government | 217 |
| 6.3.2 Public Administration and Independent Authorities | 221 |
| 6.3.3 Law Enforcement | 224 |
| 6.3.4 Political Parties and NGOs | 226 |
| 6.3.5 The Industry and Private Sector | 228 |
| 6.4 The Issues | 231 |
| 6.4.1 Italy's Top-Level Domain | 232 |
| 6.4.2 The New Economy and e-commerce | 234 |
| 6.4.3 Privacy, Cryptography, Digital Signature and the e-government | 237 |
| 6.5 Conclusions | 240 |
| CHAPTER SEVEN - CONCLUSIONS: DIGITAL WINNERS, VIRTUAL LOSERS | 245 |
| 7.1 Now, Where Do We Stand? | 245 |
| 7.2 Explaining the Cases | 246 |
| 7.2.1 Democracies and Autocracies | 251 |
| 7.2.2 The False Promise of the Internet Threat to National Security | 253 |
| 7.2.3 Any International Regime, Anytime Soon? | 254 |
| 7.3 <i>Internet</i> -ional Relations? | 256 |
| 7.4 A Slightly Normative Ending (Or What the Internet Can or Cannot Do) | 258 |
| 7.5 Finally, Where Do We Go from Here? | 261 |
| GENERAL BIBLIOGRAPHY | 265 |
| APPENDIX (A): LIST OF INTERVIEWS | 281 |
| APPENDIX (B): THE CODE BOOK AND DATASET | 283 |



LIST OF ABBREVIATIONS

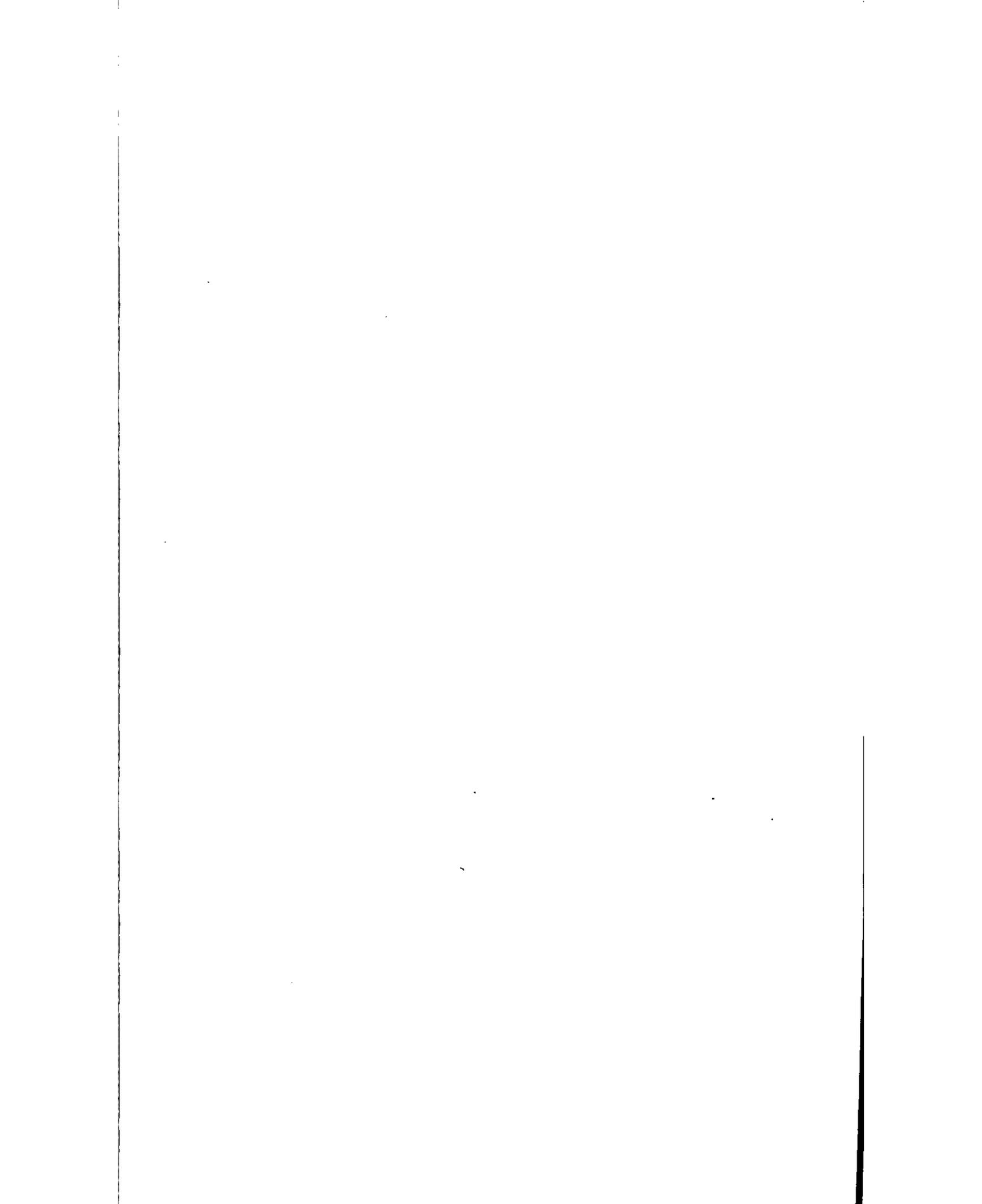
| | |
|---------|--|
| ABI | Associazione Bancaria Italiana |
| ACLU | American Civil Liberties Union |
| AGCOM | Autorita' Garante per le Comunicazioni |
| AIPA | Autorita' per l'Informatizzazione della Pubblica Amministrazione |
| ALCEI | Associazione per la Libera Comunicazione Elettronica |
| ARP | Address Resolution Protocol |
| ARPA | Advance Research Project Agency |
| ARPANET | ARPA Network |
| ATM | Asynchronous Transmission Mode |
| BBN | Bolt, Beranek and Newman |
| BDA | Bundesvereinigung der Deutschen Arbeitgeberverbände |
| BDSG | Bundesdatenschutzgesetz |
| BfV | Bundesamt für Verfassungsschutz |
| BKA | Bundeskartellamt |
| BMI | Bundesministerium des Innern |
| BMBF | Bundesministerium für Bildung und Forschung |
| BMWi | Bundesministerium für Wirtschaft und Technologie |
| BND | Bundesnachrichtendienst |
| BSA | Bundeskriminalamt |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BXA | Bureau of Export Administration |
| CALEA | Communications Assistance to Law Enforcement Act |
| CCC | Chaos Computer Club |

| | |
|--------|--|
| ccTLD | Country Code Top-Level Domain |
| CDA | Children Decency Act |
| CDT | Center for Democracy and Technology |
| CDU | Chirstliche Demokratische Union |
| CERT | Computer Emergency Response Team |
| CESA | Cyberspace Electronic Security Act |
| CIAO | Critical Infrastructures Assurance Office |
| CNR | Consiglio Nazionale delle Ricerche |
| COESIN | Comitato Esperti Internet |
| COPA | Children On-line Protection Act |
| COPPA | Children On-line Privacy Protection Act |
| CPSR | Computer Professionals for Social Responsibility |
| CSA | Computer Security Act |
| CSNET | Computer Science Network |
| D21 | Deutschland 21 st Century Initiative |
| DARPA | See ARPA |
| DES | Data Encryption Standard |
| DNS | Domain Name System |
| DOC | Department of Commerce |
| DOD | Department of Defense |
| DOE | Department of Energy |
| DOJ | Department of Justice |
| DOS | Denial of Service Attacks |
| DTAG | Deutsche Telekom |
| EFF | Electronic Freedom Foundation |

| | |
|---------|---|
| EGP | Exterior Gateway Protocol |
| EPIC | Electronic Privacy Information Center |
| EUROPOL | European Police |
| FBI | Federal Bureau of Investigation |
| FCC | Federal Communication Commission |
| FIDNET | Federal Intrusion Detection Network |
| FNC | Federal Networking Council |
| FSI | Forum sulla Societa' dell'Informazione |
| FTC | Federal Trade Commission |
| GARR | Gruppo Armonizzazioni Reti di Ricerca |
| GdF | Guardia di Finanza |
| GII | Global Information Infrastructure |
| GILC | Global Internet Liberties Campaign |
| GUUG | German Unix Users Group |
| HTML | Hypertext Mark-up Language |
| HTTP | Hypertext Transfer Protocol |
| HUMINT | Human Intelligence |
| IAB | Internet Architecture Board |
| IANA | Internet Assigned Names Authority |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| ICT | Information and Communication Technologies |
| IETF | Internet Engineering Task Force |
| IMG | Inter-ministerial Group |
| ISOC | Internet Society |
| ISP | Internet Service Provider |

| | |
|--------|---|
| IT | Information Technologies |
| IT2 | Internet Two |
| ITIC | Information Technology Industry Council |
| ITU | International Telecommunication Union |
| IuKDG | Informations-und Kommunikationsdienste-Gesetz |
| IVBV | Bonn-Berlin Federal Network |
| IW | Information Warfare |
| NA | Naming Authority |
| NGI | New Generation Internet |
| NGO | Non-Governmental Organizations |
| NII | National Information Infrastructure |
| NIPC | National Infrastructure Protection Center |
| NIST | National Institute of Standards and Technology |
| NPD | Nationale Partei Deutschland |
| NSA | National Security Agency |
| NSI | Network Solution Inc. |
| NSF | National Science Foundation |
| NSFNET | National Science Foundation Network |
| NSTL | National Security Threat List |
| NTIA | National Telecommunication and Information Administration |
| OECD | Organization for Economic Cooperation and Development |
| OSI | Open Standard Interconnection |
| PA | Public Administration |
| PCCIP | Presidential Commission on Critical Infrastructure Protection |
| PDD | Presidential Decision Directive |

| | |
|----------------|--|
| PECSENC | President's Export Council Subcommittee on Encryption |
| PGP | Pretty Good Privacy |
| PKC | Public Key Cryptography |
| RA | Registration Authority |
| RMA | Revolution in Military Affairs |
| RegTP | Regielurungsbehörde für Telekommunikation und Post |
| RFC | Request for Comments |
| SAFE | Security and Freedom through Encryption Act |
| SigG | Digitale Signatur Gesetz |
| SIGINT | Signal Intelligence |
| SME | Small and Medium-size Enterprises |
| SPD | Sozialdemokratische Partei Deutschlands |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TKG | Telekommunikation Gesetz |
| TIA | Telecommunication Industry Association |
| TIM | Telecom Italia Mobile |
| TIN | Telecom Italia Network |
| TLC | Telecommunications |
| TLD | Top-Level-Domain |
| UMTS | Universal Mobile Telecommunication System |
| WIPO | World Intellectual Property Organization |
| WTO | World Trade Organization |
| W3C | World Wide Web Consortium |



ACKNOWLEDGMENTS

I have always liked computers. When I was a teen-ager, I used to read science-fiction books, and computers were there. I used to watch movies like *2001: A Space Odeissy* or *WarGames*, and computers were there too. To me, it has always looked logical, almost “natural”, that computers would communicate with each other, as well as with human beings. Thus, when I was preparing the research proposal for my dissertation for the European University Institute (EUI), I knew that I wanted it to include computers. The Internet made an ideal topic for a dissertation in International Relations. Ultimately, I have presented the findings and conclusions of this dissertation on several occasions and conferences. The response and feedback have been consistently positive, making me think that the choice has been the right one for me.

I have been lucky enough to encounter academic advisors and teachers intellectually open to appreciate such (admittedly) “off-mainstream” ideas. Within the EUI, first and foremost, I want to thank Thomas Risse and Richard Breen for their remarkable and highly stimulant supervision, as well as for their undiminished willingness to talk about my many doubts and perplexities. Both of them were always to the point, challenging, demanding (particularly on those parts that I would have preferred to skip), and direct, (Thomas knew I “could take it”).

Academically, I have a considerable debt of gratitude with Gary Chapman of the University of Texas, Austin, and Giorgio Natalicchi of the University of Florence, with whom I have engagingly discussed my ideas on several occasions, and have enthusiastically accepted to join the defense committee for my dissertation. Last, but not least, I also want to thank R. Craig Nation with the U.S. Army War College, who has always been willing to listen to my complains and grievances on the topic I had chosen, and to give sound and friendly advice, although this topic was quite removed from his immediate field of expertise.

After four years at the European University Institute, and countless hours and days spent discussing dissertations’ topics, methodology and academic life in general, the fellow Ph.D. researchers I owe something to are just too many to name all of them here. Hence, I will cite only a handful of them, representing (ideally) all the others, and apologizing for such a short selection. I want to thank Pieter Bowen, Martin Dahl, Dirk de Bievre, Hazelzet Hadewych, Craig Robertson, and Chiara Strozzi (for all the statistics and tables!). Moreover, I would like to thank Maureen Lechleitner and Marie-Ange Catotti of the

Department of Social and Political Sciences of the EUI for their unredeemed willingness to help with the Department's rules and "traditions". A special mention here goes to my friend and colleague Benita C. Blessing, visiting student at the EUI from the University of Wisconsin, since she has read, commented and edited this dissertation more than once. Clearly, all the errors still in the dissertation are exclusively my fault.

Outside the Institute, I have debts of gratitude also with Andrea Brandani, who has spent several hours searching the Internet for data and figures, Harald and Ulli Müller, and Claudia Hermes for their help with the German interviews. Many thanks to all of the interviewees who gladly put their time and expertise at my disposal (the complete list is included in the Appendix, but a special mention for Andrea Monti, Lucio Picci and the staff at EPIC). Frank Schimmelfennig of the Darmstadt University of Technology was a rigorous and encouraging discussant when I presented my early research design at the EUI International Relations Working Group Workshop, November 20-22, 1998.

Needless to say, my greatest "thank you" goes to Lee M. Miller and Emma Michela. Not only Lee and Emma had to put up with a husband and a father that was (more often than not) away and busy. They have also done their best to support me in this endeavor. The fact that Emma was not with us at the very beginning of this project, but "joined" later has only made this path all the more worthwhile.

CHAPTER ONE - INTRODUCTION: IS IT THE END OF THE WORLD AS WE KNOW IT?

*"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."
(Universal Declaration of Human Rights, Article 19,
Adopted by UN General Assembly Resolution 217A
(III) of 10 December 1948)¹*

*"The Internet is for everyone, - but it won't be if Governments restrict access to it, so we must dedicate ourselves to keeping the network unrestricted, unfettered and unregulated. We must have the freedom to speak and the freedom to hear."
(Vint Cerf, Co-Founder, Internet Society, and Co-inventor of
TCP/IP, April 7, 1999)²*

1.1 "On the Net, Nobody Knows You Are a Dog!"

In the mid-1990s, a popular cartoon pictured a dog describing the *Internet* or, more familiarly, "the Net", to a fellow dog with this wry but appropriate punch-line. It was an early attempt to lighten up a stodgy, though brand new, piece of technology: the "network of computer networks". The joke summarized well one of the features of the Net that many users already treasured at that early date: on the Internet, one's identity can be concealed, or altered, or falsified at will. This important feature, however, like many aspects of the Net, had not been an explicit part of the Net's original concept.

The birth and expansion of the Internet have been riddled with such contradictions and surprises. Originally a communication network designed to connect the many different machines of the U.S. Department of Defense (DOD), the Net was conceived in the midst of the Cold War, and DOD planners and engineers thought it might further be useful in a nuclear war.³ Almost by accident, the Internet was then developed to disseminate knowledge among universities. It now carries news, data, and impressive sex-related

¹ <http://www.hrw.org/hrw/universal.html> (last visited on April 4, 2001). "Visited on" will be henceforth abbreviated in "v."

² <http://www.isoc.org/isoc/media/speeches/forevervone.shtml> (v. October 10, 2000).

³ The first to write about "distributed communications" and its implications for the military was a RAND engineer, Paul Baran, in 1964 (<http://www.rand.org/publications/RM/RM3420/> v. November 8, 2000). For the historical background of the Internet see chapter two.

material, and will, ultimately and again by coincidence, revolutionize the way private companies do business.

In this way, as it expands in both size and scope, the Net can simultaneously be, a threat to, a tool for, or the object of statutory control (Mulgan, 1995:5). As *The Economist* (March 7, 1998:18) noted,

Governments are schizophrenic about the Internet. Most are genuinely excited by its phenomenal growth and the opportunities it offers to business and education. They also sense that any country attempting to hold it back risks looking foolish and technophobic. On the other hand, they find the Internet's libertarian culture and contempt for national borders subversive and frankly terrifying.

This observation makes one wonder how national governments have intended to control what has been thought uncontrollable, i.e. the Internet, and, further, why they have wanted to do so at all. This dilemma is the primary theme of this dissertation.

In the first phases of development and adoption of new technologies, national governments tend to act conservatively, trying to guess what changes may result from the assimilation of innovation.⁴ In this period of time, before the technical novelties become more "established", governments are more inclined to listen to what the national security/law enforcement community has to say, before equally influential interests' combinations, usually economic growth, consumers' health protection, or the like, emerge as a counterbalance.

At that point, national governments are faced with three potentially contradictory goals: (a) to exploit the economic potentialities of the new technology, (b) to protect citizens' privacy, freedom and health, and (c) to preserve national security (with regards to internal and external threats).⁵ The same pattern is apparent in governments' responses to the Internet. Once a powerful alliance of business and pro-civil liberties/pro-consumer rights NGOS emerged, it offset the interests of the national security community, represented

⁴ This is true also for the United States. Even though the Internet has been developed with government funds, the early 1990s idea that the U.S. government had of the "information highways" was different (and it was never clear). The Internet simply "was there", and it fulfilled the role amazingly. The American government reacted positively, but nonetheless has paid too much attention to what the national security community has said about the Net for a long time, somewhat reducing the community's influence only recently, when another powerful alliance of private businesses and pro-freedom groups demanded to restrain the "security experts".

⁵ National security is an extensive, all-embracing, and, for that matter, undefined concept that states use at their pleasure to justify controlling or repressing an equally broad variety of social behaviors, from human rights to organized crime or terrorism.

by law enforcement/intelligence (in all countries) and defense (mostly in the U.S., less so in other countries) agencies.⁶

From the brief account given here, it is easy to appreciate how this scheme applies more to democracies than to non-democracies. Democratic countries are more open, and thus willing to be more receptive to innovations, than autocracies. Interests aggregations, whether of entrepreneurs, consumers, civil libertarians, human rights activists, environmentalists, etc., are the norm in democracies. Vice versa, non-democratic governments have more tools at their disposal to detach their societies from the effects of those interests' representation. Furthermore, the national security community in those countries can be challenged by almost no one, and has a powerful voice with the government's leaders. Finally, many democracies, which are also the world's most advanced economies, are at the forefront of the Internet phenomenon. Many non-democracies are far behind. Democracies thus have a unique chance to greatly shape the future of the Net. Hence an analysis of democracies' Internet policies may provide reliable evidence for predicting the future of Internet control.

One of the features of the Internet that has worried governments the most is the near impossibility of knowing for certain that a precise action has been carried out by a specific user. It is clearly possible to trace the IP address of a given machine on the Net, but there is no guarantee of the individual's identity behind the computer. These circumstances, as states have inferred, may have serious consequences for the cohesion of their societies. As Reiss (1984:27) has observed, modern societies are based on trust, and certainty about the members' identities is essential to maintain that trust relationship. The prospect of Internet users (or Netizens⁷ as they call themselves) hiding their identities has undoubtedly unnerved several governments, whose mission is to defend (from cybercrime or human rights activists, for that matter) themselves, their states, and the interests they represent.

This state of affairs—coupled with the lack of accountable authorities for the Internet—represents a fundamental challenge for all states. An “old” pattern is at play here: at the outset, some media (particularly radio and television) have been used by national leaders and their constituencies as strategic tools to foster nationality and the legitimacy of

⁶ With reference to the U.S. case, this thesis has recently been espoused (and popularized) also by Steven Levy in his book *Crypto: How the Code Rebel Beat the Government-Saving Privacy in the Digital Age*, (2001).

⁷ The term “Netizen” has been coined and used in the United States. American Internet activists know the term and its meaning, but its use does not appear to be particularly widespread. The situation is probably even worse in Europe. Conveniently, the term is used descriptively in this dissertation to indicate “independent activists interested in Internet-related issues”. For more extensive definitions see http://whatis.techtarget.com/definition/0..sid9_gci212636.00.html (v. July 11, 2001).

governments. Over time, however, as other non-state actors (e.g. independent news agencies, NGOs, large corporations) have gained access to and have learned to use the same media, as well as other channels of communications (e.g. fax machines), the states' quasi-monopoly on information has begun to erode. This process has not stopped since. More to the point, state bureaucracies ignored the Internet for a long period of time.⁸

This fact has permitted the Net to attract an even larger coterie of would-be communicators otherwise excluded from access to the media circle. Netizens (with their groups and NGOs) thus had time to improve their Internet skills, while the national security community (law enforcement, intelligence and defense agencies) had not been given a mandate "to familiarize" itself with the network and did not have specific powers to intercept Internet communications. Law enforcement and intelligence agencies in several countries have therefore complained that they have "to run after" instead of being ahead of Internet developments and changes.⁹

The most efficient way to manage, and control, the Net would be through an international regime, which at the moment seems difficult to create. On-line countries would be under pressure to achieve consensus on which issues should be legally prohibited on the Net. A revealing example is offered by the ASEAN (Association of South East Asian Nations), which includes multi-party democracies (Thailand and the Philippines) as well as one-party autocracies (Myanmar and Laos). In the September 1996 meeting, ASEAN members "...agreed in theory to police the Internet and block sites that run counter to Asian values...[but could] not reach an agreement on what to block, or how".¹⁰

Between 1997 and 1998, the EU Commission—at the behest of Commissioners Bangemann and Brittain—launched a proposal for an "international charter" for international cooperation and greater consistency of rules in the area of the on-line

⁸ There are two main reasons to clarify this circumstance: (a) at least at the beginning, it developed slowly, and it seemed to many that it was "the right thing, at the right time", (b) the diffusion of the Internet (a network for scientists and academics) has taken almost everybody by surprise and was thus mostly overlooked at, and (c) with few exceptions in the United States, political leaders in most national governments and parliaments have little direct familiarity with computer networks (a generational problem) which contributed to the previous problem.

⁹ It should be noted that, for a long time (perhaps as early as 1947, and constantly modernized since) the United States, Great Britain, and other English-speaking countries have had in activity global electronic communications surveillance system (Echelon) with highly sophisticated intercepting capabilities. Nevertheless, if Echelon is as good as it is believed, one cannot help but wonder why, for instance, the FBI is constantly asking the federal government and Congress for more snooping powers, claiming that they risk being outsmarted by criminals with advanced encryption software.

¹⁰ <http://www.CataLaw.com/doom/threat.shtml> (v. November 27, 2000). ASEAN countries, however, have tried to move ahead on the road to technological modernity. In November 2000, they signed a free-trade pact aiming to eliminate duties on information technology goods and services by 2010. The pact also urged the members to pass legislature to make digital signature legally binding

economy.¹¹ International organizations, Internet non-profit groups as well as national governments would have roles in this international charter.¹² The United States—which has never seen favorably the ingress of international institutions into a matter that it considers primarily the competence of the private sector’s self-governance—never supported the initiative, which died out.

The United States, on the other hand, supports the Council of Europe Convention on Cybercrime of December 2000,¹³ and will seek to have non-member countries (including Canada, Australia, and Japan) sign the convention. Moreover, experts consider the Convention a valuable document, but believe that it will also be hard to implement nationally.¹⁴ Nevertheless, as has occurred recently, new versions of the draft are consistently received with almost overt hostility by the Internet business community,¹⁵ and, as I will argue in this dissertation, as long as these conditions persist and users’ NGOs and consumers’ organizations cooperate with the private sector, national governments efforts to increase Internet control will be thwarted.

Lack of cooperation at the international level will not stop governments from trying to pursue control at the national level. Noam (1990:vii)—summarizing the thoughts of de Sola Pool—has noted that “...governments, fearful of a loss of control over sovereignty and culture, will continue to resist opening new communication channels [including the Internet], despite centuries of experience with the self-defeating results of such

(http://dailynews.yahoo.com/h/ap/20001122/bs/ascan_summit_1.html v. November 28, 2000).

¹¹ The document was called “Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on Globalization and the Information Society: The Need for Strengthened International Coordination (COM(98) 50final, 4/2/98) at <http://europa.eu.int/ISPO/eif/policy/councilad hoc.html> (v. November 27, 2000). The EU Commission proposed “...to hold a major international conference, bringing together private sector and governments in early 1999 (most likely in February or March 1999)”.

¹² The World Trade Organization (WTO), the International telecommunication Union (ITU), the World Intellectual Property Organization (WIPO), the Internet Society (ISOC), the World Wide Web Consortium (W3C), and many others would have participated.

¹³ The most recent draft of the convention is at <http://conventions.coe.int/treaty/EN/projets/cybercrime24.htm> (v. December 5, 2000).

¹⁴ Robin Urry, visiting scientist, EU Joint Research Center at Ispra (Italy), personal communication, European University Institute, November 24, 2000. Civil liberties and human rights organizations have extensively criticized the convention (for instance <http://www.gilc.org/privacy/coe-letter-1000.html> or <http://www.securityfocus.com/commentary/98> v. December 5, 2000). These circumstances are further exacerbated by the mismatch between technological innovation and the condition of laws on cybercrime in several countries. In December 2000, a Washington-based consulting company, McConnell International, published a study on the status of cybercrime laws in 52 countries. Only nine of the countries surveyed “...amended their laws to cover more than half of the kinds of crimes that need to be addressed” (<http://www.mcconnellinternational.com/services/CyberCrime.htm> v. December 12, 2000).

¹⁵ Draft n.25 (the most recent) has been no exception (<http://www.wired.com/news/politics/0,1283,42228,00.html> and <http://news.cnet.com/news/0-1007-200-5043832.html> v. April 4, 2001).

restrictiveness”.¹⁶ Accordingly, Mayer-Schönberger and Foster (1997:243) have remarked that

...national legislatures might continue to enact regulations, but their regulatory endeavors are unlikely to be as effectively enforceable as they desire. To circumvent the limitations of national regulatory attempts, one might advocate for an international regulatory measure to restrict the content of Internet communications...[States, however,]...differ dramatically in the kinds of content they prefer to regulate”

Conflicting views are even present within countries. In the United States, the most influential country for the future of the Internet, the prevailing attitude has been “let’s see what develops” (Kahin and Nesson, 1997:viii) or “hands-off” (*The Economist*, July 5, 1997:13). At the same time, civil liberties and pro-family advocates lobby Congress with opposing views on how to and what to regulate on the Net, with varying degrees of success. These anomalies in the behavior of states regarding the Internet inevitably lead one to the thought-provoking puzzle of understanding what is behind governments’ attempts at controlling the Net.

1.2 The Research Question (Where It Comes from and Why It Is Important)

This work is a causal enquiry into the reasons why national governments want to control the Internet. My units of analysis are those institutional actors belonging to the category of “governments”.¹⁷ Although I agree with the many scholars who criticize the traditional depiction of the “state as unitary actor”—with the government’s actions representing the state’s actions—as a strong simplification of reality, it is also true that pitching the analysis at the government level sheds light on the behavior of several countries. Since I am interested in explaining states’ efforts at controlling the Internet, other important variables—such as the impact of national identities or cultural patterns—will require future research to complete the depiction of reality.

Currently, many national governments seem to disregard the shared conviction among many observers that “...governmental controls are ineffective today and in danger of becoming irrelevant tomorrow” (Barth and Smith, 1997:295). On the contrary, repeatedly, governments seek to respond to the Internet challenge with national reactions. For instance, after a number of attempts to limit access to Internet contents had been criticized by

¹⁶ See also de Sola Pool (1990:66, 113, and 210).

¹⁷ In this dissertation, for ease of comprehension, I have used the terms “government”, “state”, and “country” interchangeably.

computer experts and civil liberties groups and failed,¹⁸ as late as November 2000, a French court still ordered the U.S. company Yahoo! "...to block French users from accessing Nazi memorabilia on its US sites".¹⁹ *The Economist* (November 25, 2000:101) did not miss the opportunity to remark that the French initiative might set an "...uncomfortable precedent for the ways in which national governments might try to impose their laws in an online world...".²⁰

What are then the reasons of these stubborn attempts by governments—democratic and non-democratic—to control the Net? I have articulated my research question in two parts. The first part focuses on the reasons for statutory control of the Internet; the second on what tools are used by governments to control the Net, and whether there are differences between democracies and non-democracies. More precisely:

1. *Why do national governments want to exercise control over the Internet?*
2. *Are there substantial differences between democracies and non-democracies in their efforts, and in the tools they use, to control the Net?*

The scheme in which I address these two questions includes both quantitative as well as qualitative analysis. I have first (a) built a database, and (b) treated it through quantitative analysis (i.e. the first part of this dissertation). The results of this part were further tested through three case studies, selected among all the observations (that is, countries) present in the database.

Scholars of international communication systems have studied the power distribution among actors on the information flows through the typologies of information

¹⁸ In July 2000, CNN on-line reported that "Germany, which has some of the world's toughest laws banning race hate propaganda, has conceded defeat to the cross-border reach of the Internet and given up trying to bar access to international neo-Nazi sites" at <http://europe.cnn.com/2000/TECH/computing/07/25/germany.internet.reut/index.html> (v. November 21, 2000).

¹⁹

<http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT3JGPOTSFC&live=true&tagid=IXLBOPYY8CC>, <http://europe.cnn.com/2000/TECH/computing/11/06/france.yahoo/index.html>, and http://news.bbc.co.uk/hi/english/world/europe/newsid_1032000/1032815.stm and http://news.bbc.co.uk/hi/english/talking_point/newsid_1033000/1033752.stm (all v. November 21, 2000). An executive of the international league against racism and anti-semitism that brought the case against Yahoo!, was quoted in the *Financial Times* as saying: "We feel that Yahoo! was ready to accept the host government's political demands in setting up its operations in China. This judgment simply makes it clear that local jurisdictions and the customs of particular countries have to be respected in cyberspace" (at <http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT3JGPOTSFC&live=true&tagid=IXLBOPYY8CC> v. November 21, 2000).

²⁰ *The Economist* did not fail to remind its readers about the "chilling effect" the pretension to apply every national regulation in every area of the world would have.

control (Mowlana, 1997), of which Internet control is the most recent evolution.²¹ Mowlana (1997:34) has classified four types of "control": (a) *internal* (i.e. within the members of the communication system) and *actual* (i.e. with concrete measures); (b) *external and actual*; (c) *internal and perceived*; and finally (d) *external and perceived*.²² In the case of the Internet, statutory control is definitively *actual*; it is *external*, because it is imposed by governments; but also *internal*, because governments are active members of the Internet community, and, in several instances, willing providers of abundant official information.

Statutory control over the Internet can be exercised, essentially, in two ways, notably (a) limitation and discrimination of access to the Net (e.g. through licensing procedures based on political or social affiliation or restricting access to trusted users), and/or (b) censorship of contents exchanged on-line. In turn, the latter can be performed through (b1) actively monitoring the behavior of local Internet Service Providers (ISPs), and/or (b2) screening the various on-line procedures (e-mail, newsgroups, Web sites, etc.) utilized by private individuals to exchange information over the Net. Originally, I had intended *statutory control* as the actions (including national regulations) by governments to limit individuals' access to the Net, as well as to search and monitor preferences and choices of Internet users.

Investigating how states can put limits on Internet access in their territories, however, was more complex than anticipated. Most of those limits, in fact, are indirect and they are difficult to identify and measure. Limits imposed on certain groups or individuals to access the Net are seldom explicit. For instance, rarely, if ever, are there legal provisions that formally bar a specific group or a single user from the Net. More likely, limits are on the basis of census (i.e. resources to buy hardware or pay phone calls), or affiliation.²³ It is thus quite hard to identify viable indicators that capture such circumstances. In the end, I decided to focus on more detectable indicators of statutory control in the areas of censorship and content monitoring.²⁴

²¹ Actually, some authors (e.g. Mulgan, 1991:8) have argued that studying "control" is to a post-industrial world what studying "power" was to an industrial (mechanical) world. That is, control, more than power, "...is a concept more appropriate to a world aware of the importance of information" (Mulgan, 1991:8).

²² Mulgan (1991) has also classified control as *exogenous* (external) or *endogenous* (internal).

²³ In Saudi Arabia, for instance, only members of the royal family can afford, and are permitted, Internet access.

²⁴ This point is discussed further in section 4.

1.3 Specifying the Dependent Variable

This section will address the “hottest” issues that make up the debate on Internet control (i.e. my dependent variable, DV). The topics presented here (starting with those that are most sensitive for the pro-liberties and consumers NGOs, then moving on to those crucial to the business community) help specify the DV, particularly for the qualitative analysis. While for the quantitative analysis I have used only the Cryptography Index (see 1.3.3), the qualitative analysis of the three cases (the United States, Germany and Italy) has required the inclusion of other elements that did not emerge at first in the quantitative analysis but that were equally decisive to understand my DV.

This section may thus be seen as a close examination of a hypothetical “manifesto” of the unusual alliance between civil liberties, consumers, and users’ associations and the ICT industry. I begin with freedom of speech (a priority for civil libertarians) and privacy (about which consumers’ organizations are increasingly worried), then move to cryptography (encryption software is crucial for users’ freedom and privacy, as well as for business applications), and conclude with the New Economy (here the problem of domain names is probably the most critical).

1.3.1 *Freedom of Expression and Censorship*

Article 19 of the 1948 Universal Declaration of Human Rights clearly states that everyone has the right to freedom of opinion and expression. In addition, in all “real”²⁵ democracies, this right is either explicitly asserted in their constitutions, or, if not so, it is corroborated *ex post* by the prevalent jurisprudence as if, albeit implicitly, it were actually included in the constitution. Consequently, most individuals in democratic countries take this right for granted. Lessig (1999:164) has remarked that freedom of speech (or of expression) in the United States is constitutionally protected in a “complex, and at times convoluted, way”, and that this protection is intended to counterbalance government control. Writing on the American experience, Haiman (1978:xi [1976]) commented that

[o]f all the rights Americans take for granted, the freedom to speak one’s mind seems the most secure. A person may be poor or jobless, may be the victim of racial, ethnic or sexual discrimination, but at least that individual can talk freely, can protest, and can advocate causes no matter how unpopular or radical they may be. At least so goes the mythology of our democracy.

²⁵ “Real” as opposed to “phony” democracies, which are “a more sinister phenomenon”—even worse than partial democracies—because their appearance deceives (*The Economist*, June 24, 2000:17/18).

With specific reference to the Internet, in the landmark 1997 decision (ACLU vs. Reno),²⁶ the U.S. Supreme Court ruled that "...the Internet is a unique medium entitled to the highest protection under the free speech protections of the First Amendment to the US Constitution".²⁷ This interpretation could hardly not have an impact on other democracies, which have gradually included it in their national jurisprudence. Defining what free expression really is, however, is a demanding task, since "freedom of speech" is culture dependent. Mayer-Schönberger and Foster (1997:246) were thus correct in noting that "[r]egulating the content of speech on the Net is still thought of as a national issue". Traditionally, the United States has defined free speech more broadly than has Europe. In the U.S., hatred, racist or neo-Nazi publication—which are a criminal offense in Germany for instance—is protected by the First Amendment, and civil liberties organizations support this view. To further complicate this matter, "[h]ate mongers were among the first to realize the tremendous power of the Internet to spread their hateful messages and recruit members to their hateful causes" (Mock, 2000:141).²⁸ Paradoxically, this circumstance has launched "...a battle between free speech advocates and human rights advocates" (Mock, 2000:147).²⁹

Curbing freedom of expression and imposing censorship are state instruments to control the information exchange,³⁰ and are among the most unequivocal examples of resistance by governments to the Internet's role in enabling individuals' communications. Governments "...know that unfettered speech can shape and transform individuals' expectations, giving them a renewed sense of the possible" (Shapiro, 1999:65). Simultaneously, states aiming to control the exchange of information are fully aware that such an outcome is effectively attainable only by seriously infringing upon individual rights, such as the right to privacy and freedom of expression—the true hallmarks of democracies (Steeves, 2000:188).

²⁶ This was the decision on the 1996 Children Decency Act (CDA or, also ACLU vs. Reno).

²⁷ <http://www.cdt.org/speech/cda/> (v. November 17, 2000).

²⁸ Two of the best "hate-watch" Web sites are the Hate Watch at <http://www.hatewatch.org/frames.html> (v. November 17, 2000) and the Simon Wiesenthal Center at <http://www.wiesenthal.com/watch/index.html> (v. November 17, 2000).

²⁹ Mock (2000:151) recommends education for users as the key solution to this problem. This is precisely the goal of organizations such as Hate Watch or the Wiesenthal Center.

³⁰ Focusing on free press, which can only function if freedom of expression is guaranteed, Freedom House publishes a Press Freedom Survey. In 2000, Freedom House found that Internet Censorship was the newest threat to freedom of speech. In particular, the report on the comprehensive survey of print and electronic news media discovered that

"...nearly two-thirds of countries, accounting for 80 percent of the world's population, restrict press freedom.... 69 countries (37 percent), representing all continents, as having a free press. Partly free news media are found in 51 countries (27 percent). In another 66 countries (36 percent), print and broadcast systems are considered not free" (at <http://www.freedomhouse.org/news/pr041700.html> v. November 17, 2000). The on-line full report is available at <http://www.freedomhouse.org/pfs2000/> (v. November 17, 2000).

One of the frequent justifications used to restrain freedom of expression—and privacy, or secrecy of communications for that matter—is the violation of national interests, including national security (Cox, 1981:6). Democratic and non-democratic countries alike may use this explanation; however, the former have a much lower record of citing “national security” or “national interest” to curtail basic freedoms than the latter.³¹ Even in democracies, however, the definition of certain issues as “national security matters” poses considerable obstacles to Netizens, civil liberties and human rights activists alike. Since it is national governments that decide what is to be included in the classification of “national security”, individuals who may XXX to challenge the state’s exclusion of certain topics from public discussion are *de facto* deprived of a considerable portion of legal ground for actions against their governments. At the time of writing, the only certainty is that the legal and political battles will continue, until public opinion, in those communities and cases in which it plays a role, will decide that one aspect is more important than the other.

To conclude, it must also briefly be recalled that threats to freedom of expression and imposition of censorship may also come from the private sector. As Shapiro (1998:67) has pointed out, “[s]ometimes, the driving concern of the state seems to be that someone needs to rein the Net—if not government, then private actors”. In September 2000, the Global Internet Liberties Campaign (GILC) pointed its finger at the Internet Content Rating Association, a global consortium of corporations, which includes, among others, AOL, Microsoft, IBM, British Telecom, and Bertelsmann, aiming for a world-wide policy of self-rating.³² Content rating, complained the GILC, could threaten the freedom of expression, diversity of views, and accessibility that the Internet currently offers.³³ Scholars will also have to address these aspects of the problem of Internet control.

1.3.2 Privacy and Data Protection

it is possible that today’s struggle over the Net between national governments and the “unholy” alliance of private businesses and civil liberties activists, may in the near

³¹ Cox (1981:6 [1980]) has identified only one major post-World War II case in the United States—the “Pentagon Papers”—of conflict between first amendment freedoms and national security. China, for instance, gives a rather different interpretation of the reach of “national security” and of “state secrets”. See for example, http://news.bbc.co.uk/1/hi/english/world/asia-pacific/newsid_1010000/1010708.stm (v. November 17, 2000).

³² <http://news.cnet.com/news/0-1005-200-346750.html?tag=> (v. November 17, 2000).

³³ <http://www.gilc.org/speech/ratings/> (v. November 17, 2000). The conduct of some major Internet companies for the November 2000 decision on the new Internet domain names in the Internet Corporation for Assigned Names and Numbers (ICANN), i.e. the organization managing the system for the Internet, has added evidence to these fears. See further the section on domain names.

future also extend to battle between former allies, i.e. with businesses and NGOs and Netizens on opposite sides of the barricade. For the time being, however, as long as the shadow of government meddling with the Internet is particularly menacing, the alliance holds. Two issues may lead to breaking the alliance and future antagonism: one is privacy, and the other is the Domain Name System (DNS). I address the former in this section and the latter in section 1.6.4.

Privacy is popularly defined as “the right to be left alone”. Indeed, privacy is a fundamental—but not absolute—right recognized in article 12 of the 1948 Universal Declaration of Human Rights,³⁴ and it is constitutionally guaranteed in many countries (EPIC, 1999b).³⁵ Still

[a]uthors have now given up trying to define privacy, and there is no generally accepted definition....For virtually every commentator, however, the fundamental issue has been the loss of human dignity, autonomy and respect that results from loss of control over personal information (Bennett, 1992:26).

All the most important international organizations, including the United Nations, the OECD, and the EU have stressed the significance of protecting privacy and personal data.³⁶ Privacy, however, is also frequently violated by governments—it often stands in the way of law enforcement, national security (Diffie and Landau, 1998), and companies’ business practices alike. Furthermore, not all states offer the same degree of protection to their citizens. For instance, the treatment of personal data in Europe is more strictly regulated and enforced than in the United States,³⁷ which prefers to rely on “self-governance” for businesses. Europeans argue that self-governance alone cannot protect consumers sufficiently. EU directive 95/46EC entered into effect in October 1998, and initiated a hot debate between the EU and the United States on the export of data of European citizens treated outside the EU, to the point that transatlantic trade relations could be seriously

³⁴ “No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honor or reputation. Everyone has the right to the protection of law against such interference or attacks”.

³⁵ There is also an interpretation of individual “privacy” that is seen as detrimental for democracy. This point is well explained, for instance, in Ruiz (1997:particularly 9/10).

³⁶ *Guidelines Concerning Computerized Personal Data Files*, adopted by the U.N. General Assembly on December 14, 1990, the *Guidelines on the Protection of Privacy and Trans-border Data Flows*, published by the OECD (1990), and the *EU Directive 95/46EC of October 24, 1995*.

³⁷ For an overview on these differences in telecommunications see Ruiz (1997). The fact that privacy is more regulated in Europe does not mean that Americans are not fond of it. On the contrary, the “right to be left alone” is more strongly felt in a country the size of the United States than in many crowded countries of Europe.

hampered.³⁸ The United States even threatened to challenge the directive in the World Trade Organization (WTO) if it were used against American companies (Jonquieres and Kehoe, October 8, 1998:14).

Computers,³⁹ the digitalization of electronic signals,⁴⁰ and the Internet itself have accentuated the problem of protecting individuals' privacy. A survey by the Pew Internet and American Life Project in August 2000 showed that "[p]rivacy has emerged as a central policy concern about the Internet as more Americans go online every day...".⁴¹ Another survey among Internet users in the United States in September 2000 by Gallup confirmed that a strong majority of them were concerned about threats to their privacy.⁴² The busting of DoubleClick, an on-line advertising and marketing company, is one more example of this occurrence. DoubleClik gathered information on preferences of anonymous Internet users. When the company announced that it wanted to "give a name and address" to those anonymous users, strong protests ensued. Its stocks collapsed and the Federal Trade Commission began an investigation (*The Economist*, November 11, 2000:104).

As Bennett (1992:17) has observed, "[i]nstantaneous access to vast quantities of information from multiple and remote locations has changed the character of the modern organization and of the society in which it is embedded". Many early Internet users thought the original anonymity of the Net would indefinitely remain as such; companies as well as governments, however, quickly realized that faceless users could mean the failure of marketing strategies and an encouragement to unaccountable behavior on-line.⁴³ In addition,

³⁸ As one observer noted, "Europeans are concerned with protecting people from companies,...America's priority is to protect them from government" (quoted in Jonquieres and Kehoe, October 8, 1998:14). The press release on the directive entering into force is at http://europa.eu.int/comm/internal_market/en/media/dataprot/news/925.htm (v. November 10, 2000).

³⁹ Computers, more than other technologies in the past, have elicited impulsive fears in the larger public since their appearance (Bennett, 1992:121). It is the very idea of the *deus ex machina*, the machine that can search for and collect information on people's lives. In this respect, this image has fostered the demand for more regulations on privacy protection, at least in industrialized democracies.

⁴⁰ The effects of digitalization of the Net can be also seen, for instance, in the spreading of digital cameras for surveillance. In Britain alone there are an estimated 300,000 cameras covering shopping areas, housing estates, car parks and public facilities in great many towns and cities

(<http://www.privacy.org/pi/issues/cctv/index.html> v. November 14, 2000). As Lessig (1999:152) has remarked, in this constantly taped world, the burden of proof is on "the monitored", to first establish his/her innocence.

⁴¹ <http://pewinternet.org/reports/reports.asp?Report=19&Section=ReportLevel1&Field=Level1ID&ID=44> (v. November 30, 2000). The groups most concerned with privacy were women, African-Americans and elderly users. The whole report is available for download at

http://63.210.24.35/reports/pdfs/PIP_Trust_Privacy_Report.pdf (v. November 30, 2000).

⁴² Among the surveyed, the image of a "large on-line database" with telephone numbers, property tax information, and legal information was the most startling, at

http://www.gallup.com/poll/indicators/indputer_net.asp (v. November 21, 2000).

⁴³ An excellent overview on markets and privacy is hosted by the U.S. Department of Commerce at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm> (v. November 15, 2000).

surfing the Net and other activities inside computer networks leave clear and easily followed tracks. At the same time, cheaper and cheaper computing power has allowed even small companies or governments in less developed countries to run large relational databases that permit efficient cross-referencing which only large corporations or rich states could afford in the past. All these actors have developed both techniques and software to track those paths, and possibly ascertain the identity of previously anonymous users.⁴⁴

Violation of privacy can occur at different levels, personal communication is just one of these. More precisely, in telecommunications, the gathering of information about individuals can be done in any of the three layers normally making up the telecom system:⁴⁵

1. *layer one* is the basic infrastructure, carrying undifferentiated digital data,⁴⁶ which is reserved only to network providers (i.e. telecom companies). In this layer it is not possible to screen what information sender and receiver are exchanging. For this reason, privacy laws do not apply here, as is the case for Europe. This level, however, is where *traffic analysis* takes place: it can provide useful information on the locations of the sender and receiver, how long they communicate, who else they contact etc. All this is extremely valuable information that law enforcement officials may obtain from a telecom carrier by a simple request, without a judge's warrant;
2. *layer two* is where service providers operate, for instance offering Internet access to businesses and individuals (that is, the ISPs) or storage space.⁴⁷ In this layer, data are roughly divided into general information about the *identity* of the senders and receivers, and the contents of their messages. Data protection acts usually apply at this level, since here it is possible to pinpoint who is communicating with whom. A judge's warrant is usually required by the service providers to disclose this information to legally authorized personnel;

⁴⁴ With regards to the importance of anonymity on-line, Marc Rotenberg, EPIC's executive director, has testified before the U.S. Senate Commerce Committee that "[w]hile anonymity does create some risk, the loss of anonymity in the on-line world could significantly undermine any legislative effort to safeguard privacy. We have noticed a disturbing trend in the last year with more and more web sites requiring registration and making use of new tracking techniques to profile Internet users. Legislative safeguards will help limit the worst of the abuses, but formal recognition of a right to be anonymous in the online world may be the most robust form of privacy protection in the years ahead" (http://www.epic.org/privacy/internet/testimony_1000.html v. November 15, 2000).

⁴⁵ I am grateful to Professor Hansjürgen Garstka, Data Protection and Information Access Commissioner of the State of Berlin, for his thorough explanation of this point (Berlin June 27, 2000).

⁴⁶ There is no distinction among bytes representing the names, numbers or address of callers and the contents of their messages.

⁴⁷ A storage service provider (SSP) is a company that provides computer storage space and related management to other companies (http://www.whatis.com/WhatIs_Definition_Page/0,4152,345131,00.html v. November 10, 2000). There are ISPs that make available the same service to individual users (e.g. X-Drive, at <http://www.xdrive.com/>).

3. finally, *layer three* is the platform on which content providers, such as hosts of Web pages, function.⁴⁸ At this level it is possible for the provider to gather plenty of information about the *preferences* and tastes of users and hence “profile” them, which is what many Web sites do.⁴⁹ Data protection laws clearly apply to this layer as well, and correct Internet behavior would require providers to explicitly state their privacy policy.⁵⁰

In the end, with the advent of the Internet, reasons of image—appearing more “advanced”—as well as the aim of reducing costs have increasingly encouraged political leaders in several industrialized countries to enthusiastically embrace “e-government”.⁵¹ Undoubtedly, the more “electronic” governments and companies become—and many circumstances point in this direction—the more efficient and less expensive their services should be. Nonetheless, although the number of citizens familiar with the Internet will increase—thus reducing the “fear” of it so common in certain sectors of the population—it is also likely that the same Internet-savvy citizens will be more aware of the risks to their privacy. Therefore, these individuals are all too likely to loudly demand more protection for the details of their personal lives. “1984” may only remain the work of a visionary, but Netizens and ordinary citizens alike will always have to remember that

...vastly more efficient governments will also know vastly more about each and every one of their citizens. The exponential increase in the ability of e-governments to gather, store and mine data about people will raise well-founded worries about privacy and civil liberties. The price of happy e-citizenship will be eternal vigilance. (Symonds, June 24, 2000:26).

In the end, the best protection for users/consumers’ privacy will be for them to send a clear signal to the whole on-line industry, namely “no privacy, no business”. Signs of this

⁴⁸ Some ISPs such as America On Line (AOL) are also content providers, that is they provide access and contents.

⁴⁹ A content provider of a Web page can—mostly thanks to “cookies” (small text files placed on the user’s computer) but not exclusively—not only know the IP address of users accessing that Web page, but also how many times the same user has accessed that page and what other pages s/he has visited before. Cookies can generally be read only by the server that has placed them. However, “third-party-cookies” could be placed on the user’s computer (without his/her knowledge if the browser does not alert him/her) by other Web servers than the one the user has visited.

⁵⁰ For instance, in September 2000, the U.S. General Accounting Office (GAO) published a report (http://www.epic.org/privacy/internet/armey_gao_study.pdf v. November 10, 2000) indicating that 85% of the 65 government Web sites surveyed posted a privacy policy as recommended by the Federal Trade Commission. However, 14% of the notices stated that the Web site allowed cookies to be placed by third-parties. Furthermore, private companies are known to be compliant even with federal guidelines on privacy policies http://www.epic.org/privacy/internet/armey_gao_study.pdf v. November 10, 2000, particularly pg.4 and 11).

⁵¹ Generally speaking, most of the services offered so far, with some exceptions, concern consulting on-line documents. The United States has an excellent portal for this purpose at <http://www.firstgov.gov/> (v. November 15, 2000).

attitude have already appeared: Forrest Research, a Massachusetts-based technology consultancy, has reckoned that over Christmas 1999 privacy concerns stopped consumers from completing more than \$12 billion of on-line purchase (*The Economist Technology Quarterly*, December 9, 2000:4/5). This request for privacy will impact hard upon many of the current on-line retailers, which have made the trade of personal information their main business. However, as more “traditional” (i.e. less dependent on information-gathering for profits) stores go on-line, providing such guarantees should not be a problem, and it can also become a mark of quality of service.

1.3.3 Cryptography

Cryptography⁵² and encryption software are clearly interrelated with privacy⁵³(Levy, 2001) and computer networks’ security. In addition, the legal use of cryptography in private communications is essential to protect freedom of speech. As Denning (1997:176) states, “encryption can protect communications and stored information from unauthorized access and disclosure”. Barth and Smith, (1997:291) have also observed that “[g]overnmental controls on encryption technology often interfere with legitimate private sector needs for strong encryption”. Finally,

[g]overnmental regulation of cryptographic security technology endangers personal privacy. Encryption ensures the confidentiality of personal records, such as medical information, personal financial data, and electronic mail. In a networked environment, such information is increasingly at risk of being stolen or misused” (EPIC, 1999:2/3).

The small and highly specialized mathematical field of cryptography has a new celebrity status, Until recently, the techniques for encrypting and decrypting messages were the domain of mathematicians, the military and diplomats. Individuals used to consider their communications through letters or phone calls not important enough to require the expensive and tiresome procedure that encryption entails just to say “I love you” to their dear ones—and many Netizens still think that way. The law enforcement and military intelligence communities could hence concentrate all their energies and skills on controlling their enemies’—who are almost exclusively states—encrypted communications.

⁵² *Cryptography* is the art of creating and using cryptosystems. A cryptosystem or cipher system is a method of disguising messages so that only certain people can see through the disguise. Cryptanalysis is the art of breaking cryptosystems—seeing through the disguise even when you’re not supposed to be able to. Cryptology is the study of both cryptography and cryptanalysis (excerpt from <http://www.faqs.org/faqs/cryptography-faq/part03/> v. November 18, 2000). Encryption software simply enables computer to perform fast and efficiently the mathematical processes (algorithms) to encrypt messages.

⁵³ In its guidelines to protect personal privacy, the Electronic Frontier Foundation (EFF, see chapter 4) unmistakably recommend to “use encryption!” (n.12 at

Three changes have made this depiction obsolete: the Internet, cheap computing power, and Public Key Cryptography (PKC) (Levy, 2001). The Net has brought about electronic mail, the most popular communication medium since the telephone. Cheap computing power has made the management of increasingly complex mathematical operations (indispensable for strong cryptography) available on the desk of the average PC user. PKC has put in the hand of Internet users a powerful instrument to hide their messages from unwanted interception. Diffie⁵⁴ and Landau (1998:36) have described PKC as follows:

[I]n public key cryptosystem, every message is operated on by two keys, one used to encipher the message, and the other to decipher....The keys are inverses in that anything encrypted by one can be decrypted by the other. However, given access to one of these keys, it is computationally infeasible to discover the other. This makes possible the practice that gives public-key cryptography its name: one of the two keys can be made public without endangering the security of the other.

As a consequence of these new circumstances, national law enforcement and intelligence organizations have witnessed an unanticipated but steady increase of Internet users hiding their communications, which were previously transmitted "in clear". To continue the monitoring of this startling number of encrypted messages, those government organizations have seen their interception and deciphering resources stretched to the limits.⁵⁵ The solution envisaged by governments—first and foremost by the United States—and advised by the above mentioned organizations was to render the acquisition of encryption software more difficult through its regulation. Barth and Smith (1997:283) have remarked how, "[s]ince its advent, government encryption regulation has been driven by two distinct interests: (1) a foreign intelligence interest in collecting all information implicated in national security; and (2) a law enforcement interest in collecting evidence of criminal activity". Furthermore,

[g]overnments face a dilemma since two contradictory political objectives are at play. Indeed, sophisticated cryptography is a necessity in a networked environment for protecting the privacy of personal information and the secrecy of confidential business information. However, the use of cryptography may impair the ability of law enforcement agencies to combat crime and protect national security (Szafran, 1998:45).

http://www.eff.org/pub/Privacy/eff_privacy_top_12.html v. November 15, 2000).

⁵⁴ Withfield Diffie and Martin Hellman were the first inventors of PKC.

⁵⁵ Large government organizations, particularly in industrialized countries, have certainly the resources to monitor, encipher, and decipher (i.e. computing power) large quantities of messages. However, if it takes, for instance, one day to read ten encrypted messages, with the same computing power 1000 messages will require ten days of work, and 100,000 messages 100 days. With 10 million encrypted messages, the same organizations with the same computing power will be saturated—since it takes proportionally much more computing power to decipher than to encrypt messages.

Since cryptographic freedom would allow everyone, including criminals, drug dealers and terrorists to be confident that their e-mails are secure, this state of affairs has obliged governments to face the fundamental question of whether or not they should legislate against cryptography (Singh, 1999:302). Denning (1997:176) has also stressed this point, warning that the widespread availability of unbreakable encryption software, coupled with anonymous re-mailing services could well lead to "...a situation where practically all communications are immune from lawful interception (wire-taps) and documents from law search and seizure".

This situation is well known to U.S. government agencies such as the FBI and the National Security Agency (NSA), which consider the selling of the latest encryption software to non-Americans as a possible "threat to their national security". These agencies are increasingly concerned about organized crime and terrorist groups using stronger and stronger encryption software for their communications. They are thus pressuring Congress to enact more restrictive legislation on the export of cryptography software (which is already a federal offense), and allow them to have access to individual users' cryptographic keys. Civil liberties pressure groups fully oppose such a possibility.⁵⁶ The U.S. authorities appear extremely concerned about the terrorism issue on the Internet. U.S. intelligence agencies have therefore stepped up their efforts to control the flow of information over the Internet, "...counterattacking an unholy alliance of civil libertarians and business chiefs who back the introduction of secure encryption technologies to protect personal privacy and commercial data on-line".⁵⁷ Thus, the battle about regulating the use of encryption software simply pinpoints a larger "conflict", between the national security community and private business (in particular telecom and e-commerce companies), which "connect" with civil liberties groups on this matter.

Last, but not least, encryption software is also crucial to defending human rights activists. In fact, "[m]any human rights groups currently use encryption to protect their files and communications from seizure and interception by the governments they monitor for abuses" (EPIC, 1999:3). Therefore, if the United States and other countries with advanced software industries make it more difficult for human rights groups to acquire strong

⁵⁶ See for instance for the year 1997 <http://www.techweb.com/wire/news/1997/09/0925unclesam.html> and for the year 1998 <http://www.techweb.com/wire/storv/TWB19980210S0007> (both v. November 30, 2000).

⁵⁷ Duncan Campbell (1997) quoted in http://www.infowar.com/hacker/hack_091897b.html-ssi v. November 18, 2000).

encryption software by regulating the export and availability of that software, they will also have to consider that they are probably indirectly favoring undemocratic governments.

Most of these fears about the consequences of the unrestricted availability of encryption software appear to be unfounded. Actually, governments that praise freedom of speech—that is, “real” democracies—should not be concerned if Netizens exchange their communications in clear or encrypted. It is part of the job of intelligence and law enforcement officials to pin down criminals among law-abiding citizens while respecting the latter’s liberties. The claim that organized crime could take advantage of such a situation remains only speculative. Organized crime could use *ad hoc* encryption software—which is much harder to break—instead of publicly available software (such as Pretty Good Privacy, PGP) that most Netizens utilize. Ultimately, the degree of freedom in legally employing, selling and buying encryption software for private communications is an excellent indicator of countries’ attitudes about Internet control.⁵⁸

1.3.4 The Domain Names System (DNS), Electronic Business and the New Economy

Along with privacy violations, disputes within the Domain Name System are the most significant sources of tension within the informal alliance of business/pro-freedom NGOs and Netizens, which, in the future may lead to a break up of that alliance. Similarly, DNS quarrels are generating severe strain among businesses themselves. But why is the DNS so important for business people and Netizens alike, as well as the future of the whole Net?

Basically, the DNS determines on-line identities, or, in other words, who can be called what. Clearly, the DNS is vital for the private sector, where brands and trademarks are the key to business success. Companies want their names to be recognized worldwide—including the World Wide Web—and do not want unknown individuals to illegally exploit or meddle with their reputation. But the freedom of choosing whatever name one pleases has implications for free expression on-line and for who that person or organization can be on the Internet. Furthermore, if names on the Internet are strictly regulated and/or monitored, on-line anonymity, which has already been lessened, will further be trimmed down. Many Netizens and pro-freedom NGOS are openly distressed by such a prospect. In this respect, privacy and DNS concerns noticeably overlap. Finally, incidentally, the DNS

⁵⁸ The Cryptography Index (derived from the “1998 Cryptography and Liberty. An International Survey of Encryption Policy” of the Global Internet Liberties Campaign, GILC) is the main indicator for my dependent variable (level of Internet control). See Chapter three.

(through the IP hosts count) is also one of the few available indicators that can give a rough estimate of the size of Internet. Thus, analyzing the developments within the current DNS dispute is essential for the goals of this work.

A domain name locates an organization or other entity on the Internet,⁵⁹ while the DNS “translates” the name, which is easier for users to remember, into an Internet Protocol (IP) address.⁶⁰ The most important names are those at the “top” of the DNS hierarchy, that is the country code top-level domains (ccTLD), for instance, *.it .de .us*, etc.), and the generic top-level domains (gTLD), such as *.int .net .org* or *.com, .gov*, and *.mil*. The latter two are reserved only to the to the U.S. federal administration.

The DNS was invented by one of Internet’s fathers, Jon Postel, who in 1994 drafted the principal document (Request for Comments, RFC, 1591).⁶¹ The DNS was not intended as a standard and Postel did not expect other TLD to be created.⁶² The ccTLD were assigned to regional networking organizations called “registries”, while the gTLD were managed by the Internet Assigned Numbers Authority (IANA) in coordination with the U.S. Department of Commerce (DOC). IANA later passed the management of gTLD to a private company. In Postel’s view, in the original spirit of the Net, the DNS was a technical solution. Nobody expected the tremendous success of the Internet, nor the rush of private businesses to cyberspace. Soon, names and trademarks became as precious on-line as they were off-line, and they became a primary target of patent and copyright lawyers.⁶³ The commercial values of domains skyrocketed, and so did the complexity of their management.

In October 1998, a new organization, the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit, private sector corporation formed by a broad coalition of the Internet’s business, technical, academic, and user communities was born. ICANN was “...recognized by the U.S. Government as the global consensus entity to coordinate the technical management of the Internet’s domain name system, the allocation of IP address

⁵⁹ http://www.whatis.com/WhatIs_Definition_Page/0,4152,211988,00.html (v. November 19, 2000).

⁶⁰ http://www.whatis.com/WhatIs_Definition_Page/0,4152,213908,00.html (v. November 19, 2000).

⁶¹ <http://www.isi.edu/in-notes/rfc1591.txt> (v. November 19, 2000).

⁶² “It is extremely unlikely that any other TLDs will be created”—Postel quoted in <http://www.isi.edu/in-notes/rfc1591.txt> (v. November 19, 2000).

⁶³ In the early phases of the DNS, a few individuals registered famous names, such as *microsoft.com* or *mcdonald.com*. Once the trademark companies decided that it was time to have a Web site, they found their names already owned. The only solution, at that time, was to “buy back” the name at a considerable price. This phenomenon was called “domain-grabbing” or “cybersquatting”, and it is no longer possible now under the new ICANN rules on names registration.

space, the server system”.⁶⁴ ICANN has since become the closest thing that there is to an “Internet government” (*The Economist*, June 10, 2000:99/101).⁶⁵ The private sector’s sudden discovery and breathtaking dash into the Net—first as electronic commerce and then as e-business—have made it possible for ICANN to attain a pivotal position in the Internet’s recent architecture.

Electronic commerce is defined as “...the buying and selling of goods and services on the Internet, especially the World Wide Web”.⁶⁶ E-commerce was born in the mid-1990s, when a handful of companies that had no physical infrastructures, such as Amazon.com, discovered that it was possible to sell some products (books or music CDs) on the Internet. The expectations that this new form of commerce generated in the private sector took everybody, including national governments, by surprise. In 1998, before “the New Economy”, the *Financial Times* summarized the original stance on e-commerce of many governments as follows:

Many governments accept, at least in principle, that e-commerce must retain market-led and free from burdensome structural and bureaucratic barriers. But such liberal precepts jostle awkwardly with defensive anxieties that, once the full power of the internet is unleashed on the world, it will *challenge* national laws and may eventually elude *government control* altogether (Jonquieres and Kehoe, October 8, 1998:14).⁶⁷

E-commerce then became e-business in 1997, when IBM launched the term, adding servicing customers and collaborating with business partners to the buying and selling—thus including banking and financial services on the Net.⁶⁸ When business analysts included revenues and jobs from the Information and Communication Technologies (ICT) to the (anticipated) returns from e-business, they started to talk about a “New Economy”, characterized by speed and innovation.⁶⁹ This situation has had a considerable impact on the

⁶⁴ <http://www.icann.org/general/fact-sheet.htm> (v. November 19, 2000). Presumably, the rest of the world had no option but to accept the U.S. government’s recognition of ICANN as the principal organization for the managing of the DNS.

⁶⁵ Two other “quasi-governmental” bodies on the Internet are the World Wide Web Consortium (W3C) and the Internet Engineers Task Force (IETF). Both organizations, as well as ICANN are based in the United States.

⁶⁶ http://www.whatis.com/WhatIs_Definition_Page/0,4152,212029,00.html (v. November 19, 2000).

⁶⁷ My emphasis.

⁶⁸ http://www.whatis.com/WhatIs_Definition_Page/0,4152,212026,00.html (v. November 19, 2000). The two terms, however, are often used interchangeably.

⁶⁹ The New Economy is also called Internet Economy. For correct and in-depth definitions see <http://www.InternetIndicators.com/indicators.html#layers> (v. November 19, 2000), and a remarkable study by the University of Texas, Austin, at http://cism.bus.utexas.edu/works/articles/internet_economy.pdf (v. November 19, 2000). To sum up, in the Internet Economy (this term is less common but more correct), (1) a few months are comparable to several years of “normal (human) time”, (2) not all the goods can have the same odds of success, (3) services must be really valuable to have users pay for them—“free” is a key word on the Net.

struggle for control over the Internet.⁷⁰ In fact, secure communications are critical for fostering the New Economy, and encryption software is indispensable for secure communications. Thus an alliance between users and civil liberties activists with private businesses has ensued.

As Barth and Smith (1997:297) have stated, “[m]arket realities based on continued rapid advances in technology make it likely that strong encryption will be an essential component of the international structure of electronic commerce”. Two telling examples of these changes in governments’ attitudes are the United States and France. In the cryptography survey of 1998 (GILC, 1998),⁷¹ both countries were reported as having restrictions on the use and export of encryption software. In 1999 and 2000, both eased their limits on that software because of industry pressure (EPIC, 1999).⁷² The promise of benefits in the New Economy is simply too persuasive for many governments to resist. This condition will make it harder for them to implement overly restrictive and obtrusive measures of Internet control, at least as long as those expectations are not shown to be unfounded.⁷³

1.4 The Competing Hypotheses

Most, if not all, national governments envisage a specific role for the Internet in their own agendas for political enhancement and economic development. In pursuing their plans, they thus have “good” reasons why they want the Net to perform in certain ways and not others. What are those reasons?

Generally speaking, two main theories⁷⁴ are useful to explain states’—and governments’—behavior: realism (with all its variants) and liberalism (with all its

⁷⁰ Clearly, if governments are pleased with the estimated gains from e-business, they will also have to face other challenges. For instance they will have to find new, effective ways to collect taxes from businesses online (Bishop, January 29, 2000).

⁷¹ The first version of the survey was done under the name of Global Internet Liberties Campaign (GILC) by investigators of the Electronic Privacy Information Center. In 1999 and 2000, Electronic Privacy Information Center took the report under its sole name.

⁷² The most recent version of the survey is available yearly at the Electronic Privacy Information Center (EPIC) at <http://www.epic.org/> (v. several times between November 1997 and January 2001). For the United States official trade policy on encryption see <http://www.bxa.doc.gov/Encryption/> (v. November 19, 2000).

⁷³ Non-democratic governments such as China’s are facing the dilemma of fostering the Net while increasing the level of control. The two policies will inevitably collide sooner rather than later.

⁷⁴ Clearly, this viewpoint on International Relations (IR) theory is greatly reductive, and the description of these ideas is necessarily over-simplified (although, even the original concepts are not always precise). Other eminent theories such as Globalism, Critical Theory and Social Constructivism have enriched the field of IR, and have provided scholars with remarkable tools to conduct their inquiries. Moreover, authors such as Amid Mowlana (1997) argue that Global Communications should be a field on its own, requiring a distinct theoretical framework.

variants).⁷⁵ The former theory emphasizes states' security concerns, power distribution, and the anarchic nature of the international system (and an *Hobbesian* worldview). The latter stresses international cooperation and interdependence among state actors, and the significance of domestic structures and interest configuration in the making of international politics (a *Lockean* worldview). Realism basically asserts that when a country's security is at stake, all other matters—including a country's economic well-being—should be of secondary importance for national governments.

Liberalism argues that democracies should not feel threatened by other democracies (since democracies do not fight each other), and that economic interdependence and international trade would reduce the risks of war and make the world a safer place. Finally, while realists tend to view states as unitary actors and study their interactions on this premis, liberals consider states (and governments) complex and fragmented organizations, which function as a conglomeration of diverse interests.⁷⁶ Indeed, some of the most convincing and innovative work done in liberal theory by scholars has rightly focused on the interaction between domestic politics and international relations.⁷⁷ Moreover, Milner's work (1997) has at last called attention to the importance of information distribution among political actors in accomplishing their goals. This factor has had a profound impact on the debate about and the implementation of Internet control. In a rare event, the pro-control party (the national security community) has thus been confronted by the anti-control party (private business, and users' and consumers' NGOs) that was equally (and sometimes even better) informed about technical and legal matters.

Heise (1975:23) has correctly pointed out that, especially in the social sciences, "...few phenomena of interest depend on just a single cause and effect". Social science phenomena usually involve many different kinds of events, determined by a number of different things, each affecting a number of other things". To explain my research questions I originally devised five working hypotheses, which have all been tested in chapter three, namely:

⁷⁵ For convenience, in this short summary, I have used the term "liberalism" to stand for both institutionalism and liberal/domestic politics approach. In this dissertation, however, I have applied only the latter as a tool of investigation.

⁷⁶ The number of books covering these two theories is impressive. In fact, these theories still provide a substantial contribution to the field of IR. For a comprehensive (pre-and post-Cold War) overview of these two competing views see Keohane (1986) and Baldwin (1993).

⁷⁷ In this respect, one of the most convincing models has been the Two-Level game developed by Robert Putnam (1988). The model has been further convincingly applied by, among others, Moravcsik (1995) and Milner (1997).

1. the *requirements of national security*, that is, “the more a state is determined to protect its national security, the more it will seek to control access by its citizens to the Internet”;
2. the *individualist/collectivist structures* of on-line societies or, “the more the state considered is concerned with individuals’ liberties (including personal communications), the more free Internet access will be”;
3. the *democratic status* of on-line countries, or “the more democratic a state, the greater the access to the Internet its citizens will have”;
4. the *regulatory propensity* of on-line countries, i.e. “the stronger the historical tradition of regulatory behavior, the stronger the regulatory propensity of states considered, and the more controlled Internet access will be”;
5. finally, the *free trade/economic openness* of the countries considered: “the higher the free trade propensity and the more open the economy of a state, the freer the Internet”.

Hypothesis number one inevitably relates to the realist position. If one accepts this hypothesis as an explanation, the other four hypotheses should then be rejected as irrelevant. The focus in this hypothesis is on protecting the security of the country against aggressions via the Internet. On-line assaults can be launched by foreign as well as domestic foes with the goal of undermining the state or reducing its ability to act independently.⁷⁸ Business interests can also be acknowledged by the government, but their demands (especially on the availability of encryption software or protecting personal information) should be thoroughly evaluated.

Consistent with a more articulated view of what states are and how they act than realism, the other competing hypotheses are variants of liberalism. These assumptions stress the explanatory potential of cultural-political and economic factors, and clearly abandon the characterization of states as unitary actors concerned with protecting themselves from cyberthreats. More precisely, hypothesis number two investigates individualistic versus collectivist cultures. Since the Net still has a strong independent/individualist image, individualistic societies should be less inclined towards Internet control. Hypothesis number three examines the relevance of a democratic or non-democratic political system.

⁷⁸ The fact that there is almost no distinction between domestic or foreign foes is an important condition. Such differentiation has been slowly losing its significance, and it is even less suitable for the Internet. This unified approach allows, for instance, the United States to confront domestic terrorists in the same way they do foreign (whether state-sponsored or not) terrorists (e.g. Lake, 2000). However, it also permits China to treat its domestic dissidents as “enemies of the state”. Other threats, such as malicious hackers or cybercrime, have increasingly become “internationalized”, with local groups setting up with similar actors for technical assistance and exchange of information. In more sophisticated instances, different groups may decide to launch coordinated attacks from faraway locations.

Democracies “can take more information” (Keohane and Nye, 1998), thus they should be more restrained regarding controlling the Net. Hypotheses number four and five try to represent the economic returns that states hope to collect from the diffusion of the Internet. Since these expectations are fairly difficult to define and assess (they are, after all, “hopes”), I opted for two hypotheses with the idea that at least one of them would satisfactorily capture the variations of states’ behavior in this respect. Number four, thus, puts the accent on the process of liberalization/privatization of the telecom sector (and the Internet is an integral part of this sector) in most countries, while number five focuses on the economic freedom. The argument here is that countries with high liberalization in telecoms or high economic freedom should be readier than other countries to meet the demands of the business community and to accept a lower level of statutory control on the Net.

After completing my quantitative analysis, as illustrated in chapter three, I had to revise the five competing hypotheses accordingly, before proceeding with the qualitative study. Hypothesis number one remained unaltered. Hypothesis number two did not produce any relevant outcome, while, at the same time, hypothesis number five did not supply useful clues about economic expectations. Hence, I had to abandon number two altogether, while number five was basically merged with hypothesis number four (telecom liberalization/privatization). This assumption showed remarkably clear signs of an inverse (negative) correlation with hypothesis number one.

Finally, the democracy assumption (number three) has turned out to be an important intervening variable. The sample contained both autocratic and democratic countries, the (negative) correlation of national security/telecom liberalization has held true for a large number of them. In democratic countries, the room for maneuver granted to business, consumers’, and civil rights’ organizations to represent their own interests and to contest the national security’s viewpoint is greater than in non-democracies. At the same time, in democracies, this representation of interests is also highly complex and articulated, and sometime even contradictory. Thus, as Risse-Kappen (1995b:188) has correctly observed, since “[i]deas do not float freely...[d]ecision makers are always exposed to several often contradictory policy concepts”. Overall, the insertion of the democracy variable increases the complexity of the models, thus requiring further investigation that was not possible with the available database, but required extensive qualitative research.

The three case-studies presented in this work have fundamentally confirmed the outcomes of the quantitative analysis: national security (both internal and external) is a

primary reason why states want to control the Net. Under the pressure of the pro-civil liberties NGOS/private business unofficial “alliances”, governments have also begun to pay more attention to the economic returns of the Internet, and what the best ways are to maximize them. Consequently, faced with another powerful and technically competent player (the above mentioned alliance), and millions of individual users, the national security community has had to make concessions. Hence, users, companies and NGOS in democracies have enjoyed thus far a relatively low degree of control.

The three case can be summarized as follows. First, one must consider the United States (the “high security” case), where the stalemate is more apparent than actual. Even in that country, where the national security community is largest, most vociferous, and most able to advocate its arguments with other government branches as well as Congress, the other alliance (pro-freedom/consumers’ organizations and the private sector) is winning the day. For instance, if one takes into account the free availability of encryption software, or the awareness about users’ privacy as indicators of Internet control, in the United States the predisposition of the government and the general public is toward favoring the accidental alliance, at the expense of the national security party. If it is true, as the realist argument goes, that when security is at stake, all other matters must take a backseat, the skeptical public reaction to the arguments of the national security community needs to be explained. It may be either because (a) there is no “real” threat to national security, therefore no need to increase control on the Net, or (b) the threat is real, but not grave enough to justify curbing liberties and privacy on the Net, and can be dealt with well enough by improving efficiency standards of internal security personnel (law enforcement). Either way, the validity of the national security group’s standpoint is put into question.

Second, turning one’s attention to Germany and Italy (the “low security” cases), claims that in Germany and Italy the business community has prevailed—as demonstrated here—because these countries are under no or little threat are incorrect. In fact, the more advanced an economy is, the more computer dependent it is; and the more it is computer-dependent, the more vulnerable it is to malicious hackers, cyberthieves or cyberterrorists. In this respect, as developed economies, Germany and Italy are only slightly less vulnerable than the U.S.. Furthermore, among the various “cyberthreats”, cybercrime (organized crime and other technically-savvy criminals) is currently considered by many—including law enforcement officials in the U.S. and the EU—the most probable menace. If cybercrime were to become significant enough to constitute a clear and present “national security” crisis, then Germany and Italy, as computer-dependent, advanced economies should worry

as well. The reason they have not done so thus far is because they do not think that cybercrime—or information warfare for that matter—is a believable threat to the security of their territories or their economies.

Given these circumstances, realist objections can be anticipated. First and foremost, the United States information infrastructure can become a target for domestic and foreign enemies, and the United States has been openly identified as the main foe by several countries. Neither Germany nor Italy exhibit comparable conditions. At the same time, the U.S. federal government cannot ignore the demands of the business community: a stalemate ensues. Furthermore, unlike the United States, Germany and Italy do not have national security concerns because they are not seriously under “threat”, and their governments can thus easily accommodate the requests of the private sector. If they indeed were in the same situation as the United States government, the status and the debate on Internet control in Germany and Italy would be substantially similar to those on the other side of the Atlantic.

Realist explanations fall short not because Italy and Germany can disregard cyberthreats, and hence can back the demands of the pro-freedom/business alliance (while the U.S. government has to take seriously menaces to its national security), but because both Italy and Germany do not regard the Internet as a source of additional risk—including potentially the most credible one, i.e. cybercrime—or a national security emergency. Even the United States government tends to be better disposed toward meeting the demands of the ICT industry, and therefore of the pro-freedom/pro-consumers/business alliance, than listening to the “Cassandras” from the national security community. Overall, analyses of domestic structural differences and the idea of interests’ representation (i.e. the liberal argument) do a better job of explaining variations of my DV (Internet control).

In her important work, *Interests, Institutions and Information*, Helen Milner (1997) has introduced the specific element of “information”, which has previously been overlooked in *Two-Level Games* (Putnam, 1988).⁷⁹ Several books (e.g. Jervis, 1976) have indeed dealt with the problem of asymmetric distribution of information among states, but not within states. Moreover, Milner has argued that while groups within states have different policy preferences (which is common knowledge in liberal theory), the effects of information distribution among them has been have not been studied. Finally, Milner (1997:21) has pointed out that in many cases political executives possess information advantages over other domestic actors, and this is particularly true as regards foreign policy matters.

⁷⁹ Although Putnam did relax the perfect information assumption to allow for uncertainty in the game.

In the case of the Internet, however—which is also a foreign policy area—the information is scattered among the different actors in interesting ways. Governments, law enforcement and intelligence agencies have access to large collections of information on security flaws, social engineering skills,⁸⁰ fraudulent techniques, privacy breaks, encryption software keys, and the like. The most conspicuous feature of the allocation of information about the Internet is that private businesses, consumer organizations, pro-liberties NGOS, and ordinary users have access to the same—and in some instances even better—information than governments' agencies themselves. Thus, it is harder for the national security community to make the same case as they could for nuclear policy that they had made in the United States, and to some extent in Germany and Italy, in front of parliaments (especially Congress) and the public opinion. In that instance, the general public had little or no opportunity to critically evaluate what governments said about national security, since all the relevant information was classified by the government itself.

1.5 Your Meter or My Scale? Measuring the Level of Internet Control

Assessing government control on the Internet has proven to be problematic. The main obstacles have been to find viable ways to measure variations, and the lack of reference and field work on this topic. To overcome these obstacles, I have applied triangulation in this study. Triangulation is the application of two distinct methods (e.g. statistical analysis and in-depth case studies) to assess the plausibility of the same arguments. If my hypotheses “survived” this double test, the probability that they were correct would be greatly increased. In fact, my assumptions have passed this trial, and provided good explanations for my research questions. More specifically, I employed “between methods” triangulation, that is, using two diverse techniques of inquiry—as opposed to “within methods”, which implies replication of results. Many scholars (Smith, 1975, Jick, 1983, and King et al., 1994) have praised the advantages of triangulation in general as a sound strategy of investigation.

Another fundamental tactic of my research has been to combine the two most important domestic politics forms of explanation in the literature, namely (a) the one

⁸⁰ Social engineering is a technique that allows the person/s performing it to acquire, exploiting the common willingness of most people to be helpful, critical information by posing as a legitimate recipient of that information. Such pieces of information are then used to penetrate computer systems.

focusing on domestic structures (Katzstein, 1996 and Risse-Kappen, 1995a and 1995b) and (b) the other privileging domestic interest configurations (Putnam, 1988, Evans et al., 1993, Moravcsik, 1993 Introduction in Evans pp.3/42 and Milner, 1997). With respect to this dissertation, Milner has also been important for her work on the value of information distribution and asymmetries in domestic politics. She has observed that the distribution of information domestically is an essential factor, since it confers (or denies) political advantage to specific political actors. Such findings have helped me in the analysis of the simultaneous international/domestic dimension of the Internet by providing a basis for a more precise conceptualization of the problem of Internet control, especially in the qualitative analysis.

Clearly, information asymmetries are also decisive for maintaining social control, and thus the societal cohesion (which is one of the many tasks of government). Pound (1997:25), for instance, has remarked that social control is primarily a function of the state and is exercised through law. This is obviously a narrow notion of social control, which is, in turn, exercised by all kinds of societal institutions, which can produce, modify, alter or hide crucial pieces of information. National laws, and official government documents (decrees, reports, position papers, etc.), are useful objects of observation to appreciate a state's policies towards the Internet. These records, however, capture only a fraction of reality; studying the distribution of information among the different social actors (governments, interests groups, political parties, NGOs, private businesses, civil society, etc.) is also fundamental to addressing my research question. This level of analysis can be achieved only via qualitative interviews with representatives of all those groups, and by outlining the interests' representation, as I did in the three qualitative chapters.

I have earlier defined political control as national rules and regulations adopted by governments to limit individuals' access to the Net and to censor contents exchanged by Netizens. Such control can be specifically exercised through limitation and discrimination of licensing procedures (based, for instance, on political or social affiliation) and/or through monitoring the activity of local Internet Service Providers (ISPs) and users. While no efficient statutory control of the Internet is possible without seriously violating individuals' rights, at the same time, governments do not want to jeopardize their chances to harvest the benefits of e-business and the New Economy. Last but not least, in some respects, many democratic governments talk about controlling the Net in ways which non-democracies might be expected of.

Given this framework, I decided that I would need (a) a “snapshot”, as general as possible, of the global situation, and (b) to select a few significant cases that would allow me to investigate the phenomenon. With these goals in mind, the best path to follow was to undertake a quantitative analysis first, and then pick three cases for in-depth examination. I have thus developed proxies for the independent, control and dependent variables (see chapter three), assembled a sample of countries as large as possible (65),⁸¹ and tested all the working hypotheses by statistical methods. Among the cases in the sample, I then chose the United States, Germany and Italy as crucial examples.

The three countries are members of the OECD “club”. In fact, between 80 and 90% of all Internet traffic is among OECD countries, which also host the same percentages of Web pages and secure servers.⁸² They are also all democracies: as explained in the Introduction to Part II, studies done by Reporters Without Frontiers and Human Rights Watch have demonstrated how autocratic countries control the Internet no less than other media. Autocracies try to control all communications “by default”, and analyzing only the Internet (the subject of this work), detached from other media, would be nearly impossible. This is not the case with democracies where few would argue that an un-restricted television or un-censored press is a “threat to national security”, or that too much control of the radio may endanger the expected returns of a new economic paradigm. Moreover, if someone did support those views, plenty of civil liberties groups, consumers’ organizations, political parties and opposition leaders would stand up and argue against them. These circumstances have all materialized with regards to the Internet in democratic countries, where the arguments in favor of and against statutory control on the Net be an on-going fight that will continue long into the future.

Overall, studying the behavior of democracies and their enduring dilemmas about Internet control presents a far more interesting prospect for social scientists than do autocracies. The latter, however, cannot hope to escape facing the same predicaments, sooner or later. As the Internet spreads to more countries, more governments will see it as a tremendous economic opportunity as well as a tool for greater sophistication of their societies. But, at that point, those states will face an even greater dilemma as to how much entrepreneurial freedom and individual initiative to allow.

More specifically, within the OECD democratic club, the United States and Germany stand out as “crucial” cases. The U.S. is the “only information superpower”, since

⁸¹ It is a “non-probability” sample, that is, observations are included whenever they are available.

⁸² Secure servers are indispensable for e-commerce.

its supremacy in the Internet is unmatched. For a considerable future yet, how the United States acts with regards to controlling the Net will inevitably have global repercussions. On the other hand, for a number of users, hosts and Web pages, as well as investment in telecoms and the New Economy, Germany has shown clear signs of wanting to be the leading Internet country in Europe—battling with Britain for that position. Germany's Internet example cannot be easily ignored by its fellow Europeans. Italy, finally, can be considered as a "control" case. Despite being part of the OECD and being an advanced industrial democracy, Italy has suffered from institutionally "weak" governments—unlike Germany's and the United States' "strong" executives. Assessing how a "weak" government may reconcile regulating the Net, investing in the New Economy and creating the Information Society has shed further light on states' motivations for controlling the Net, and thus makes Italy a suitable in-depth study for this work.⁸³

1.6 A Summary of Conclusions

This work is firmly in the tradition of rational choice analysis. All actors presented are assumed to be rational: political leaders (whether in governments or parliaments) want to secure economic growth and protect public order to increase their chances to be reelected; interest groups have their own goals (whether to protect privacy or intellectual property for instance); consumers want cheaper prices and better services. To different extents all these actors are, at the same time, users and content providers on the Internet, and they want to shape the Net the way they think it should develop.

Rational choice theory is a useful tool for inquiry in the social sciences: it is not, however, "a miracle cure" (Milner, 1997:248). Inevitably, rational choice models such as this one simplify the more complex and often contradictory reality. Internet-related dilemmas come from technology (computers are error-prone, and computer networks even more so), jurisdictions (which are still mostly based on national boundaries), and politics (which is almost an all-inclusive class, where anything goes). Moreover, all these areas overlap, and at the same time affect and alter one another. A simpler model, however, can say a lot in IR, particularly in areas that have been so far ignored, such as the information distribution, by mainstream research.⁸⁴ Several IR scholars may maintain that capabilities

⁸³ Italy is nonetheless among the fastest growing countries on-line. See <http://www.isc.org/ds/WWW-200007/dist-bynum.html> or <http://www.nctSizer.com/> (both v. December 4, 2000).

⁸⁴ Exceptions are Evans et al. (1993) and Milner (1997).

distribution will remain central in this field, but the study of information asymmetries will progressively gain ground. Within this framework, presumably, more models of the Internet will be needed in the IR field in the future.

The quantitative analysis has helped to discard one hypothesis (H2)—because of clear negative results—and to redefine the others. The latter achievement, however, is less straightforward. While the level of *individualism* (H2) has been irrelevant, *national security* (H1) has appeared as the main cause for concern for states to control the Internet. However, the requirements of national security clearly collide with a tendency in several countries towards increasing *deregulation* of the telecom industry (H4), and, thus, more or less directly, also of the Internet. This conflict inevitably ends up curbing the demand for more control. These effects failed to surface when testing H5, i.e. the *open economy/ free trade* hypothesis, but only because of the lack of reliable indicators and data that measure the overall size of electronic business. Most of the figures currently available on the topic are projections.

Despite the unsatisfactory results of H5, in the end, during the qualitative investigation, it seemed appropriate to “merge” H4 and H5, and consider gains from e-business and hopes for the benefits of the New Economy as a major explanatory factor that has counterbalanced national security. Deregulation and privatization of telecoms are, after all, prerequisites for the diffusion of the Internet, which, in turn, is a precondition for the take-off of e-business. In fact, these findings were further confirmed in the qualitative part by the recurring eagerness for the “New Economy” in all the three countries considered. Precisely on this point, Mulgan (1991:137) has argued that

[in] the past, the control of communications networks was primarily determined by considerations of security, nation-building or social equity. By the late 1980s and early 1990s the needs of the economy for productivity growth and competitiveness far outweighed other considerations. Paradoxically, deregulations coincided with an ever more active role for governments and state agencies in creating what they believed to be the best climate for the communications economy. What was happening was not the end of state control,...but rather a change in its forms, a change that can best be understood as one from control within a closed system to control within an open one.

In the same manner, even though the data utilized in the quantitative analysis have not produced a clear and conclusive outcome, the relevance of the *democratic level* (H3) also emerged from the case studies, as a crucial intervening variable. Both democratic and non-democratic governments, in some instances, have used national security as a catalyst for justifying Internet control. However, there are considerable differences in what democracies perceive to be the acceptable level of Internet control.

The three case studies have confirmed the previous findings, and, by exposing more details, have shed more light on the intricacies and obstacles that states face as regards questions of Internet regulation. The specific positions of the United States, Germany and Italy are summarized hereafter. Points n.1 and 2 are the most significant, while n.3 is relevant but, at the same time, less crucial.

1. *Democracies and Autocracies.* Whereas several national governments want to control the Internet, there are still considerable variations among them on how far-reaching and intrusive this statutory control should be. This point is the essence of the “digital challenge”: governments—democracies and non-democracies alike—have to decide what level of control they can impose on the Internet without damping its diffusion in schools and universities or putting a brake on the growth of e-business.⁸⁵ Inadequate statutory control could foster an increase in “illegal” activities, whether by child-pornographers, malicious hackers, or human rights activists—depending on viewpoints. All in all, despite some common problems, democracies face a harder digital challenge than non-democracies. At the same time, the former have to expand e-business, protect their citizens’ privacy and civil liberties and assure infrastructures’ security (externally and internally)—these goals often require conflicting solutions. The latter have only to spread out e-business and protect national security.

These objectives can also imply difficult choices but, once the thorny (and never settled) issue of safeguarding the state while respecting individual liberties is removed, finding convergent answers that can simultaneously satisfy the business and national security communities becomes simpler. Finally, in the near future, only a handful of non-democracies, e.g. like Singapore and China, will have to address the challenge, whereas the majority will continue to heavily limit access to the most loyal and forbid external contacts.

Predictably, democracies have a lower level of Internet control, the average level of which has tended, thus far, to remain quite stable.⁸⁶ Most democracies are also highly industrialized (all OECD members are, albeit to different degrees, democratic). In these countries, the business community is vocal, and represents a noteworthy competitor for the

⁸⁵ For instance, the Internet has already forced “wrenching change” on financial services (Long, May 20, 2000), and threatens to change forever the way governments collect taxes (Bishop, January 29, 2000).

⁸⁶ Using the *Cryptography Index*, it is possible to notice a fair balance between the number of democratic countries that relatively increase their control, and the number of those reducing control. Between 1998 and 1999 for instance, of the 100 countries surveyed by EPIC (1999:108), nine increased their controls on encryption software (including all the Scandinavian democracies), while 16 decreased it (including Kirghizia, one of the Internet’s enemies according to *Rapporteurs Sans Frontiers*, “the Enemies of the Internet” at <http://www.rsf.fr/uk/home.html> v. November 27, 2000). The variation between the 1998 and 1999 surveys is also noticeable on the summary data set included in the Appendix B.

national security and law enforcement agencies when it comes to drawing the attention of parliaments or lobby political leaders to the development of the Internet. Normally, in democracies, companies know that showing consideration for personal privacy, attention to consumers' demands, environmental conscience, and, in general, respect for individuals is good business practice encouraging customer loyalty. If another vocal, technically and legally adept actor like civil liberties/consumers'/users' NGOs joins the already influential business community, the result is a persuasive, albeit unofficial, coalition that can seriously compete with the law enforcement/national security faction.

All three countries selected for the qualitative analysis are democracies, albeit with different political specificity. The United States, a society-dominated structure, is the "high security" state of the three cases, has potent interest groups, and is truly the Internet's only information superpower. Access to the executive, Congress and the bureaucracy for organized groups is fairly effortless and structured. Information is widely available (e.g. many official government documents can be obtained through the Freedom of Information Act, FOIA), and transparency is high and valued.

Germany is a corporatist democracy, functioning mostly through consensus among the main institutional actors (federal and local governments, trade unions, industrialists' associations, etc.). The process of building consensus is obviously time-consuming, but once agreement is reached, the necessary policies are adopted, implemented and followed. Access to federal and local governments and legislatures for institutional actors is unrestricted. Transparency is good, although not as high as in the United States, because Germany is willing to accept more limits to freedom of speech to ban neo-Nazi material, and protects privacy more broadly than the United States. A "low security" case like Italy, Germany is also the "no.1" Internet country in Europe.

Italy is another case with distinctive features. Despite the instability and frequent changes of its governments, heavy state intervention in the economy has been a characteristic of the Italian Republic since its origins. Policies (and the formation of governments, for that matter) are mostly the results of extensive bargaining and negotiations among countless political parties, which, for visibility and prestige, in the end must all be allocated some advantage. Although specific policies are often reversed or changed, some general, long-term policies (such as state intervention in the economy at all levels) remain remarkably constant. Other institutional actors are listened to, but for the most part have a "supporting role", while access to national and local governments and legislatures is

thoroughly controlled by middle-men and intermediaries.⁸⁷ Although transparency has improved recently, for an advanced democracy, it is still unsatisfactory, and few Italians are used to checking independent sources of information—of which there are plenty.

It is possible to envision conditions, however, under which even democracies may ultimately be obliged to accept greater control on the Internet. Those conditions are most likely to occur with some international agreements that even democracies, without timely counter-arguments by pro-freedom NGOs and users' groups, may be prompted by less democratic partners into signing.⁸⁸ If, after all, "...the most promising approach from the governments' point of view is coordinated action to gain some control over the online world" (*The Economist*, January 13, 2001:20), this scenario is not out of reach. It should be thus possible in democracies to have a broader public debate on which international regimes would be desirable to join, and which would not be.

2. *The false promise of the Internet threat to national security.* Few other acts are more representative of states' authority than deciding what national security consists of. This adaptive tool allows states' leaders to identify, sometimes rather subjectively, what can endanger national security, whether another superpower, malicious hackers or unarmed human rights activists. All individuals working in defense departments, intelligence and counterintelligence agencies, as well as law enforcement officials belong to the "national security community". National security implies the survival of the state. Therefore, realist scholars claim, it should be taken extremely seriously and prevail over any other considerations. Kozak and Keagle (1988:258), however, have pointed out that "[a]s with any bureaucracy...the national security community is penetrated by outside group and interests". Indeed, the key factor in setting the agenda for national security and defense is what political leaders *perceive*, in a specific moment, to be a threat. In this respect, national security and defense are just part of "politics".

The justification for Internet control based on "national security" conditions has presented Internet liberties NGOs, ordinary users and also private business with considerable complications, since, in many countries, national security cannot even be argued against.⁸⁹ Autocracies such as China and Singapore, for instance, are in such a

⁸⁷ Paradoxically, the United States is "weaker state" model compared with Italy's, because the number of actors that can actually influence policies there is greater and more efficient, whereas bottom-up approaches in Italy have only little impact on high politics.

⁸⁸ Admittedly, for the time being, there are still few autocratic states (e.g. Singapore, China and few others) that have enough weight on the Internet to exercise such influence.

⁸⁹ Among national governmental agencies, it is usually the intelligence services—because of their traditional mission—that are better equipped and trained to cope with cybercrime, than proper law enforcement officials.

situation, but also “high security” democratic states such as France or the United States can be problematic. In the latter, however, the “unofficial” coalitions of competent pro-liberties and consumers’ NGOs and of private business have provided such technically and legally competent cases against widespread or excessive control that those governments have been reluctant to accept the requests of their national security/defense agencies.

In chapter four the United States case has been explored in detail. The Internet was invented and developed thanks to the U.S. federal government (more precisely the U.S. Department of Defense, DOD). Even today, most Americans see the Internet as an American product.⁹⁰ All the most important organizations for Internet standards are based in the U.S., and so are the majority of host computers and Web pages. ICANN—an international non-profit body—operates under Californian law, and if the Department of Commerce (DOC) should not be satisfied with agreements reached within ICANN, it could always withdraw its support, rendering the management of domain names impossible. The United States is the country most dependent on computer networks, and thus the most vulnerable to cyberattacks, but it is also the country that, if it so decided, could still “turn off” the Internet.⁹¹

Despite this unparalleled hegemony and vulnerability, overall, the U.S. government has seen the world-wide diffusion of the Net as a positive outcome,⁹² and has thus far stalled requests for increasing Net control by its defense/intelligence and law enforcement personnel. This outcome is mostly the result of the accidental but highly effective alliance of pro-freedom, consumers’ and users’ NGOs and of the ICT industry. The stalemate that

This development is certainly worrying for civil liberties activists (and many individuals as well), because (even, if to a lesser extent, in democracies) intelligence services are usually most accountable only to the executive (Robin Urry, visiting scientist, EU Joint Research Center, Ispra (Italy), personal communication, November 24, 2000).

⁹⁰ Most American e-commerce companies assert that they are too busy in the home market to contemplate Europe’s. However, it could also be that “...geeks are convinced that government in Europe, which they believe regulates anything that moves, poses an even greater danger to the infant [e-commerce] than in America” (Peet, February 26, 2000:36).

⁹¹ To have an idea of the overlapping and cross-fertilization of private industry, national security and technical and policy consulting that sometimes occur in a country like the United States, one should consider the case of the Internet Policy Institute (IPI). IPI is a Washington-based Internet think tank with the mission of providing “...objective, high-quality analysis and outreach on the key issues affecting the global development and use of the Internet” (including “briefing” the US. president) at <http://www.internetpolicy.org/about/index.html> (v. November 23, 2000). Sitting on its board of directors are some prominent figures in the history of the Net—like Vint Cerf and Robert Kahn, inventors of TCP/IP. But an even more revealing profile is that of Michael A. Daniels, who is senior vice president of Science Application International Corporation (SAIC)—a long-time DOD contractor—, chairman of Network Solution Inc (NSI)—the private company that has a quasi-monopoly for awarding the .com, .net, and .org domains—and served as an advisor in the National Security Council. All this information is publicly available at <http://www.internetpolicy.org/board/index.html#daniels> (v. November 23, 2000).

⁹² Obviously, the more the Internet grows outside the U.S., the more the U.S. hegemony will be challenged.

has followed has safeguarded the current *status quo*, which, with some improvements in personal privacy and infrastructures' security, the NGOs, users and the industry would like to maintain. Indeed, the existence of such an "unofficial" alliance and the Internet control stalemate are the two most important findings of the case-study on the United States.

As explained earlier, neither Germany nor Italy have put particular emphasis on the Internet as a threat to national security, the most notable exception being a certain attention to cybercrime—which is also a great concern for e-business. The realist explanation for this variation is that these two countries do not share the "high risk" position of the United States, therefore they can afford to overlook national security. This explanation is unconvincing. Germany and Italy are advanced economies, and would be vulnerable to attacks to their infrastructures. Both countries have taken seriously the only instance of the Internet dangers that has proved to be at least credible, i.e. cybercrime. On the other hand, they have disregarded the Internet as an "external" menace or a matter for defense ministries or national security agencies, because there is almost no evidence that such a threat is convincing and probable.

The Italian case has added specific value to such an explanation. Since Italy was a late-comer to the Internet, the delay in setting up the proper legislative framework (still quite underdeveloped) and the postponement of political and social recognition that users' and consumers' NGOs had to endure, could have meant that law enforcement/intelligence/defense agencies gained upper hand in controlling the Net.⁹³ This event did not occur. On the contrary, Italy has developed a similar profile to Germany, which had "embraced" the Net earlier and faster, and the Italian national security community does not seem too impressed by Internet threats.

3. *No international regimes.* The last pertinent finding of the case studies is that national governments have not yet been able to find common legal ground for international treaties to regulate the Internet, and that the "accidental coalitions" in all three countries (and other democracies as well) would cooperate to oppose intergovernmental treaties. Because they are concerned with the Net, which is "naturally" international, these coalitions have by default international links that can be activated if necessary.⁹⁴ Indeed, the record of international agreements on the Internet has been rather insignificant thus far. Questions

⁹³ National governments are usually rather unadventurous and conservative when dealing with unforeseen and unplanned occurrences such as the Internet explosion, and sending out security personnel on "scouting" missions is not an atypical response.

⁹⁴ A possible exception is the Council of Europe Convention on Cybercrime, (still at the draft stage). The coalitions have already begun to coordinate their effort in several countries to oppose it.

like intellectual property rights, cybercrime, domain names, and several others can only be effectively addressed via international settlements. Political, cultural and legal differences among the states have, however, made it difficult to find enough common ground for needed international agreements.

The central conclusion in the case of international agreements on the Internet is that as long as national governments insist upon an intergovernmental approach, forcing aside pro-liberties NGOs and users' groups, they will have take into account that these actors will likely put up a very "knowledgeable" resistance. In fact, the most noteworthy aspect of these pro-liberties, users' and consumers' NGOs is their impressive display of technical and legal information, as well as their ability to use access to legislature and government to effectively oppose (and sometimes even nullify) the position of national security agencies. If these groups manage to secure support for their views from the private sector, governments' efforts are likely to fail most of the time, or succeed only at a high price. Including the active participation of these actors may guarantee better chances for comprehensive regimes on regulating Internet. Given these circumstances, and if "[i]n general, asymmetries of information domestically work in favor of the executive" (Milner, 1997:21), some governments may decide that the only appropriate response to the digital challenge is to go "national".

Several governments in less or non-democratic countries will continue to use the Internet threat to justify their levels of control, although the hard, unquestioned evidence of serious dangers from, or through, the Net has yet to emerge. If the same forces that have been active in the United States, Germany, Italy and other democracies were able to act, the same results would follow. If, however, these accidental alliances were to break up, with private businesses siding with national governments, the outcomes would indeed be quite different.⁹⁵ In the January 13, 2001 issue, *The Economist* noted that

[I]n the Internet, the struggle between freedom and state control will range for sometime. But if recent trends in online regulation prove anything, it is that technology is being used by both sides in this battle and that freedom is by no means certain to win. The Internet could become the most liberating technology since the printer press—but only if governments let it (.p23).

Civil liberties NGOs and user's groups had best remember that information distribution and "unusual" alliances will be even more valuable, if freedom is to win this challenge.

⁹⁵ Not an unlikely event, as the digital certificates, wanted by governments companies alike, seem to demonstrate (*The Economist*, January 13, 2001:19/23).

1.7 The Singular Nature of the Internet (Or, Where Do These Questions Come From?)

The Internet Society, one of the oldest on-line activist organizations, defines the Internet as "...a global network of networks enabling computers of all kinds to directly and transparently communicate and share services throughout much of the world".⁹⁶ There is no official "authority" to regulate the Internet. The three organizations that resemble a system of governance of the Net—the World Wide Web Consortium (W3C), founded by Tim Berners-Lee, inventor of the Web; the Internet Corporation for Assigned Names and Numbers, ICANN; and the Internet Engineers Task Force (ITEF)—are all based in the United States and operate on consensus (*The Economist*, June 10, 2000:18/19 and 99/101). These organizations derive their legitimacy from "having being there first". They began to work on Internet development spontaneously and on a volunteer basis—ICANN is something of an exception, having received from the U.S. Department of Commerce the job of managing the domain name system (DNS).

For a long time in human societies, it has been the extended family/collectivity that has mediated between the source of information and the single individual. This filtering action by the community has had the goal of maintaining the social cohesion of the group, occasionally at detriment to the individual's freedom of choice. It is only fair to say that the Internet is a communication medium that empowers individuals who, in many instances, can now access unfiltered information, often remotely located with respect to the local community. At least in the "connected world"⁹⁷, the information and telecommunication revolution, in which the Internet plays a leading role, is endowing the average Netizen with considerable communication capabilities.

The link between controlling information flows, exercising social control, and the manifestation of national sovereignty has always been greatly appreciated by states, and consequently by political scientists. Saurin (1995:256) has remarked that "[t]he concept of sovereign statehood [has been] intimately bound up with the control of clearly marked territory...the ability to enforce the boundaries [has been] central to the security of both the concept and practice of sovereignty". Anderson (1996:2) has also noted that,

...the policies and practices of governments are constrained by the degree of *de facto* control which they have over the state frontiers. The claim of the modern state to be 'the sole, exclusive font of all powers and prerogatives of rule' could only be realized if its frontiers were made impermeable to unwanted external influences. The incapacity of governments in

⁹⁶ <http://www.isoc.org/internet/> (v. November 8, 2000).

⁹⁷ Provided, of course, that, even in the "connected world", the ordinary citizen would have access to telephone lines, modems and ISPs.

the contemporary world to control much of the traffic of persons, goods and information across their frontiers is changing the nature of states.

On this point, Krasner (1995:268) has argued that

all the states...even the smallest and the poorest, possess one sometimes critical prerogative: the right to grant legitimate access,...[however,] broadcasting is an example of a situation in which the most important resource available to all states, the right to grant territorial access, could not be effectively exercised.

Focusing on the critical role of governments and the specificity of the telecommunication sector, Stone (1997:14) has confirmed that

[i]nnovation and entrepreneurship in telecommunications differ from those in many other industries in a crucial way that shapes the politics of that sector. In many other industries, a firm may enter without the necessity of obtaining the approval of governmental authority. Telecommunications has traditionally been characterized by entry controls.

Finally, Agnew and Corbrige (1995:179) have pointed out that

[f]rom the point of view of international relations...the development of micro-computers has probably been less significant than the coupling of micro technologies to the new systems of telecommunications...[t]he emergence and rapid deployment of these linked technologies is leading both to an extraordinary escalation in the number of international connections of the traditional kind and to wholly new means of interfacing at-a-distance.

The development and availability of communication means has not been without ambiguity. In the past, national one-to-many communication systems (radio, and television) have allowed national governments and their agencies to spread nationalistic rhetoric to the entire citizenry (Camilleri and Falk, 1992:56). Soon, however, professional media organizations (such as the BBC or the CNN), human rights NGOs, and individuals have all learned to take advantage of the same systems to distribute non-governmental information, counter-claims, independent reports etc. This international flow of messages, images and money is still growing at an extraordinarily rapid rate. More importantly, this traffic flows through increasingly integrated world communication systems which are no longer dominated by national bodies (Camilleri and Falk, 1992). If, at first glance, the Internet may be subsumed under the same category as the radio or the television—traditional subjects for the social sciences—the Net actually displays some rather unique features. These features render it different from all the other media, and make it the fastest growing communication medium ever (Woodall, September 28, 1996:4).

Communication means can be divided into three categories, according to their communication modes. Whereas (a) the telephone is a *one-to-one* (from one source to one receiver) and (b) the television a one-to-many (from one source to many receivers) means of

communication, (c) the Internet is a *many-to-many* (from many sources to many receivers) means of communication (Kedzie, 1997:24/27). The Net is, first and foremost, an interactive medium. Unlike radios and televisions, the applications used over the Net to communicate (i.e. e-mail, mailing lists, newsgroups, the Internet Relay Chat, and the World Wide Web itself) have been created to facilitate the exchange of information between senders and receivers and vice versa on a large scale. The awareness of being part of the transmission of news or creation of ideas is highly motivational for users, who act more as protagonists than mere passive spectators. The interactivity of the Net allows it to function simultaneously as a medium for publishing and communication, unlike other traditional media.

Second, the birth and early growth of the Net have been largely “anarchic”, i.e. lacking effective control by a superior authority, despite the origin of the Internet (the ARPANET was financed by the U.S. Government). Additionally, the continuous growth of the Internet has been made possible by grants from the U.S. National Science Foundation (NSFNET) and the spontaneous participation of American universities.⁹⁸ These conditions have prevented the emergence of a hierarchical structure, with no specific center managing the Net. The popular transmission technology (TCP/IP) and the distributed network structure have thus made the Internet a well-liked communication system, but at the cost of having no central authority.

A significant example of this case is the utter failure to substitute the TCP/IP (i.e. the *lingua franca* of the Net), created by researchers working on connecting networks, with the OSI protocol (Open Standard Interface) by the International Standard Organization. OSI came to be regarded by Internet “free-thinking” users and scientists as a top-down imposition by an intergovernmental institution that had no part in creating the network. It may happen that, in the future, some portions of today's Internet will be precluded to the general public, because they will become the basis for a more secure business-oriented network, or that faster networks, such as the Internet 2 (IT2) or the New Generation Internet (NGI) will be introduced to connect universities, government institutions, and the business community, leaving the slower, present-day Internet available for its current users.

Third, until now, Internet access has been reasonably cheap, permitting a growing share of people in industrialized countries to log on (*The Economist*, April 5, 1997:88 and October 19, 1996:21/24). Individuals and groups normally excluded from more traditional

⁹⁸ For the political battle within the federal administration and Congress for the development of the Internet in the United States in the 1990s see Hundt (2000) and Stone (1997).

media have been offered an “amplifier” to voice their opinions, disagreement and anger at very affordable prices, and are now coexisting on-line along with government and private business sites. These conditions, however, are unlikely to remain unchanged for long, as the increasing demand for fast transmission of video and voice on-line will raise costs of connection, and may marginalize some of the poorest users (Crawford, 1997). Admittedly, this low cost access has yet to benefit more than a fraction of the world’s population (Moisy, 1996).

The reasons presented above make the Internet truly unique among the media and telecommunication systems. National authorities have been slow to recognize that the Internet has a higher potential to cross borders and reach domestic users than other media currently have.⁹⁹ Consequently, control exercised by many national governments over the contents of information exchanged over the Net has often been contradictory and questionable. As telephone companies cannot be held responsible for the contents of calls, likewise Internet Service Providers (ISPs) cannot be penalized if their users connect to sites in another country and download a Web page containing information which is considered illegal in their country (but not so in the country where the bytes have been digitally produced). Where is the illegal act committed? In country A, where the information is temporarily downloaded (in the buffer memory of the computer)? In country B, where the information has been created? In country C, where an ISP server has been temporarily accessed from A to reach B? In all the other countries that the packets (the transportation cells containing the information) have crossed (Johnson and Post, 1997)?

As early as the 1970s, the new information technologies were thought to be likely to increase states’ vulnerability. A report to the Swedish government, the Tengelin Report (Tengelin, 1981) emphasized the main risks of a networked society (including dependence on foreign vendors and the threat of hackers’ raids). Once national governments realized the actual extension of the Internet and the potential reach of individual users, they started to consider increasing control over the contents exchanged on the Net. After all, controls over inflows and outflows of people, goods and information have been vital for states to assert their authority, and thus their sovereignty. As Anderson (1996:189) has noted, “[t]he general purpose of frontiers in the sovereign state was to establish absolute physical control

⁹⁹ The television and the radio at their beginnings were seen as powerful means to foster national views by governments, and thus became parts of the national arrays of “weapons” of many countries. Over time, however, other actors (such as human right and environmental activists) as well as independent news agencies have become skilled at using the same systems. The crucial difference between the Net is that control of television and radio was, from the beginning, in the hands of governments, not universities or individuals.

over a finite area and to exercise exclusive legal, administrative and social control over its inhabitants. But...frontiers are losing their hard-edged clarity”.

To different extents, national governments in connected countries are aware that the Net can introduce information into their territories—as some states have already experienced with radio broadcasting—over which they have inadequate or no control. This information may affect the attitude of their citizenry *vis-à-vis* the political and economic structures of their countries. Indeed, information asymmetries have often been instrumental for governments to achieve their objectives. Under these conditions, the set of reactions from national authorities has ranged from mild concern to suspicious alert to outright severing of connections, often depending on which government branch is in charge of Internet control.

Given the obstacles posed by establishing an international regime of regulation over the Net, and the increasing accessibility of the Net, governments have embarked on the technically more costly and difficult operation of setting up national regulations. These projected or actual national dispositions, however, are greatly divergent in terms of the extension and intrusiveness of control and of the topics covered by them. How can the field of political science/international relations help better understand these states' actions and qualitative variations?

1.8 The Internet and the Study of International Relations

Despite its origins in the late 1960s as a U.S. government-sponsored project, the Internet became known to the larger public only in the first half of the 1990s.¹⁰⁰ After being just a communication network of U.S. academics and bureaucrats, in the 1990s, the Internet was discovered by individuals, companies, and the media. Since then, and quite accidentally, it has developed into being the closest thing to the “information superhighway”, and has been praised and demonized by the media. As a brand new communication medium, the Internet has started to influence the habits of people and the functioning of societies in the industrialized part of the world, and, inevitably, it has also become a new topic of study for academics, as well as one of the favorite subject of futurologists.¹⁰¹

¹⁰⁰ A brief history of the Internet is in chapter two. By far, the best single account on the origins and early development of the Internet is Hafner and Lyon (1996). The Internet Society Web site has a considerable listing of “Internet histories” (<http://www.isoc.org/internet/history/> v. December 4, 2000).

¹⁰¹ See, for instance, Cairncross (1997), Omahe (1995), Negroponte (1995) and Naisbitt (1994).

The first scholars to realize the serious implications of the Internet for society were law students. Constitutional rights (freedom of speech, privacy and data protection), property rights (copyright), state jurisdiction, the imposition of taxes, and the validity of electronic documents and signatures are but a few of the legal realms affected by the growing access to the Internet world wide (Lessig, 1999, Kahin and Nesson, 1997 and Gewirtz, 1997). Moreover, legal scholars have been needed to address the challenge of establishing what laws should be applicable to the Internet, a task complicated by the difficulty of finding viable examples of legal frameworks that could be adapted to the case of the Internet.¹⁰²

Second to arrive on the scene were sociologists, including scholars in the more traditional discipline of mass communication and cultural studies.¹⁰³ Sociologists and communication researchers have been particularly attracted by (a) the ease with which “virtual communities” (that could be open or closed, but all share the same “feeling of belonging”) are formed on the Net, (b) the fascination that masking identities has for many users (“nobody knows you’re a dog!”), and (c) the variety and composition of “alternative” groups accessing the Internet.¹⁰⁴ Last, but not least, mass communications sociologists have addressed the problems of control in communications (Mulgan, 1995), including individuals’ “cyberpower” (Jordan, 1999).¹⁰⁵ Almost at the same time (but not much before political scientists), economists began to focus on the Internet as a topic for research. Economists have especially concentrated on the pricing of the new telecommunication system, the problem of taxation, the promises of electronic commerce (e-commerce), and the emergence of markets with imperfect but abundant information.¹⁰⁶

Finally came political scientists. There has been a long tradition in Political Science of studying the effects of telecommunication and global media on politics, both domestic and international. The field of global communication, in fact, is considered to be at the intersection of various disciplines, such as sociology, psychology, anthropology, international relations and political science (Frederick, 1993). Mowlana (1997:11) has identified information flow as “...the essential ingredient in the evolution of international

¹⁰² Cargo shipping law has been proposed by Robert (1995) as “the closest equivalent”.

¹⁰³ See, for instance, Castells (1997), Newhagen and Rafaeli (1996), December (1996), and Morris and Ogan (1996).

¹⁰⁴ See for instance Loader (1998), Parks and Floyd (1996), and Mayers (1994)..

¹⁰⁵ A major drawback with cultural and mass communication studies is the methodological approach that does not provide political scientists with easily available categories for analysis.

¹⁰⁶ See, for instance, McKnight and Bailey (1997), and Scharzt (1997). See also the several high-quality surveys of *The Economist*, i.e. Long (May 20, 2000), Peet (February 26, 2000), Bishop (January 29, 2000), Symonds (June 26, 1999), Anderson (May 10, 1997) and Woodall (September 28, 1996).

political economy...”, in addition to its “traditional” role in international political communication (i.e. diplomacy and propaganda). Political activists and political actors were also been among the early enthusiastic supporters of on-line politics (Mann, 1995) and continue to be (Hundt, 2000). Studying political activism on-line, Hill and Hughes (1998) have actually concluded that politics and society will change the Net more than the Internet will shape politics, as differences between current Netizens and real population fade away. Notwithstanding this long tradition, *ad hoc* studies on the Internet have still been extremely scarce.

One major drawback of studying the Internet from the point of view of the international relations/political science field is that (a) it is problematical to properly define and frame the issue, and (b) it is arduous to find the link between the former and the latter. Everard's *Virtual States* (2000) is archetypal in this respect. While challenging “the idea that the nation-state is dead”, it explores the systemic inequalities brought about by globalization, covering *en passim* issues such as war, censorship and the philosophical implications of hypertext, with hardly any causal logic.¹⁰⁷

Karl Deutsch (1966) was the first political scientist to provide a theoretical framework for the impact of communications on governments. Basing his analysis on cybernetics—i.e. the study of communication and control in organizations—Deutsch (1966:80) highlighted the value of feedback and of the learning process (“the learning net”), for governments' functioning and actions. Deutsch (1968) explored further the impact of communications in international relations theory, thus firmly establishing the investigation of communications and information in the field of political science/international relations.¹⁰⁸ Deutsch (1988:54) observed that “international politics generally involves groups and states...individuals usually act effectively through groups, through other groups on whom they may exert some influence from the outside or through influencing some governments”. According to Deutsch, the Internet is then an instrument of international politics.

One of the first scholars to understand and appreciate the value of freedom of speech for new communication technologies—including computer networks—was de Sola Pool. Correctly identifying the problem in the early 1980s, de Sola Pool argued that

¹⁰⁷ This occurrence may still be explained by the lack of a coherent body of literature on the topic and the obvious “rush” to fill the gap while the Internet is a “hot” topic for publishers.

¹⁰⁸ Other scholars have followed this direction of study, e.g. Cioffi-Revilla, et al. (1987), Krasner (1990), and Frederick (1993).

[f]reedom is fostered when the means of communications are dispersed, decentralized and easily available, as are printing presses and microcomputers. Central control is more likely when the means of communications are concentrated, monopolized, and scarce, as are great [telecommunication] networks (1983:5).

In a subsequent work, de Sola Pool (1990) was among the first scholars to expose the ambiguous attitude of national governments toward communication flows that they cannot control, but that, simultaneously, they need for their economies to prosper. It remains a dilemma that all governments face.

Jervis published his study on the role of (mis)perceptions and the images of other countries in international politics in 1976. Since then psychology has been applied inconsistently to the field of international relations, but the significance of perceptions and images in international politics and their implications for national security have not been lost.¹⁰⁹ Not coincidentally, the United States currently considers “perception management” one of the essential components of information warfare.¹¹⁰ In perception management operations, a country should be able to monitor the incidence and dissemination of slanderous information—old-fashioned propaganda or psychological warfare—and adopt appropriate solutions to counter it.

As the country most reliant on computer networks, the United States has been highly concerned about the problem of on-line threats, and, almost uniquely in the world, its defense agencies have developed an impressive collection of studies and publications on the topic.¹¹¹ Moreover, the United States also has required that superiority in information technologies is an inestimable strategic asset, indispensable to preserving American primacy in the world in the next century. Influential publications such as *Foreign Affairs* and *Foreign Policy*—which often reflect the mainstream thinking of U.S. elites—have been early and well-informed supporters of this standpoint, providing it with authoritative analyses.¹¹² Increasing roles for national security and intelligence agencies and growing enthusiasm for the issue in other countries have been among the side effects of the search for “information superiority”. This occurrence has inevitably yielded (a) greater attention on

¹⁰⁹Frederick (1993:190/191) has called attention once more to the consequences of spreading stereotypes and images of other countries (or ethnic groups) in international politics, as well as to the significance of studying this issue for the international relations discipline.

¹¹⁰ In this framework, scholars consider “netwar” more appropriate. For the differences see for instance <http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html> or <http://www.rand.org/publications/RRR/RRR.fall95.cyber/cyberwar.html> (v. November 29, 2000).

¹¹¹ See for instance <http://carlisle-www.army.mil/library/bibs/infowar.htm> updated to February 1998, or <http://www.psycom.net/iwar.1.html> (v. November 29, 2000).

¹¹² See for instance Nye and Owens (1996), Burton (1996), and Keohane and Nye (1998).

the side of civil liberties activists as well as (b) a long awaited consideration on the side of few political scientists for the study of statutory control on the Internet. Wright (2000) has been among the first scholars to consider political control on the Internet in the wider context of changes in policing and intelligence—which are increasingly based on communications intelligence more than human intelligence.

Other significant branches for analysis of the Internet in political science/international relations are the effects of the Net on human rights and democracy-building. On these themes, the early works of Metzler (1996) on the advantages of Internet use for human rights activists and of Kedzie (1996) on the correlation between democracy and the use of e-mail should be mentioned. More recently, Hick et al. (2000) have further explored the consequences of the Internet on human rights, including the influence of on-line hatred (Mock, 2000). Finally, research on Internet and comparative political activism are likely to grow, and the quality of its methodology should also improve as the full scope of the Internet is better understood (Hill and Hughes 1998).

Van Evera (1997:100) has argued that research questions usually arise from scholarly literature or real-world events. Given the relative scarcity of individual scholarly work on the Internet in political science/international relations, my questions have arisen from observations of real-world events. In other words, while this work would be consistent in general terms with the tradition described earlier, it would also explore a topic that is still unusual for political science students. As Bennett (1992:2) has observed, “one way to break away from the confines of sectorization is to study a completely new policy problem, one not subject to either established wisdom within the political science literature or to a long and institutionalized legacy of political development”. With that, Bennett meant that new, innovative policy problems can contribute to expanding the field of study of the political science discipline, and injecting originality in it. This can be an appropriate reading also for the case of the Internet in international relations.

1.9 The Dissertation's Structure

Having outlined my framework, chapter two presents a brief history of the Internet. Although more and more readers are familiar with the Net, this chapter puts the Internet in a chronological perspective. Chapter three focuses on the quantitative analysis of my sample. The indices of the competing hypotheses are explained as well as the data used for the analysis. The data set containing all the details is included as an appendix.

Part II consists of the in-depth case studies. I have enclosed a qualitative introduction to Part II, explaining what the criteria for my selection of countries were, in particular why these countries belong to the OECD's democratic "club". It also provides details about the techniques used for the interviews—i.e. the main source of information (along with the Internet itself) in this part. The list of interviews is also included at the end. Chapter four analyses the United States, the IT "heavy-weight". The United States is one of the countries where the struggle is most evident between the groups and individuals that support self-governance, and self-rule and those government agencies that warns about the risks of an uncontrolled Net.

Chapter five examines Germany as an example of one of the most active countries in Europe to develop the Information Society and the New Economy. Germany has welcomed the Net, and the German government intends not to miss out on the economic benefits that many expect from Internet diffusion. Chapter six presents Italy, the Internet late-comer case, which also has considerable hopes for the advantages that the Internet may offer, particularly in the South. Unlike Germany and the United States, however, Italy has rarely enjoyed stable governments. Hence, this chapter investigates how a "weak" government plans to spread the Internet in the society. Chapter seven, finally, summarizes the main conclusions of this research, outlining its significance for the field of International Relations and offering some clues about what the directions of future research on this topic may be.

To conclude, a few words of caution are necessary. Investigating national legislation and governments' actions can demonstrate the attitude of governments towards the Internet, but does not prove their actual ability to enforce rules and regulations about Internet control. Studying the efficacy of statutory control on the Internet, however, goes beyond the scope of this dissertation. Indeed, studying the comparative efficiency of laws is a daunting and often unsuccessful task due to "horrendous investigative problems" (Gibbs, 1982:104). The decision to limit the analysis to national governments' actions regarding the Internet was thus paramount for a workable research project, although further research in this direction will prove indispensable.

CHAPTER TWO - "THE ACCIDENTAL SUPERHIGHWAY": A BRIEF HISTORY OF THE INTERNET

"The Internet is chaos"
(Reid, 1997:xv)

"The Internet changes everything"
(Silicon Valley saying, circa end of 1990s)

2.1 Introduction: "The Accidental Superhighway"

This chapter provides a brief historical introduction to the Internet. It highlights the vision of those American scientists who worked to create the Net, and the hopes of the U.S. government—originally of the Department of Defense—in supporting that vision. The United States has enjoyed the "first mover advantage", allowing it to considerably shape the Net to its own needs and interests. This privileged position has slowly been eroded since the early 1990s, as an increasing number of countries with sufficient technical knowledge has gone on-line.

In the early 1990s, people outside the military and academic world in the United States started discovering the Internet—a brand-new communications medium, able to influence the habits of people and the functioning of societies in the industrialized part of the world, and a new topic of study for futurologists. It also provided several journalists with a lead story: the claim that the Internet had been developed to withstand a nuclear exchange. "Nuclear survivability" was perhaps a feature of the Net, but it was only one of principles that led to its development.¹

If the ultimate goal had been to create a communications network for military applications, the Internet would have not been born lacking the security and control mechanisms that are included in all fabrications destined for military use. Nevertheless, it would be impossible to ignore the "roots of the Internet in the darkness of the Cold War" (Rosenzweig, 1998:1533). Or downplay the fact that "...the Defense Department would never have committed funds to projects like ARPANET without the beliefs that they would ultimately serve specific military objectives and larger Cold War goals" (Rosenzweig,

¹ The confusion was a consequence of the simultaneity of several scientists working on the same idea of communication networks based on "packets" of bytes in different locations.

1998:1541). The creation, testing and development of the Net has been a combination of innovative thinking, government funding, chance, and independent brainstorming by various research centers, especially in the first stages of its development. Thanks to this uncoordinated approach, and although planned for the Cold War, the Internet has had the unplanned consequence of growing into the closest thing to an “information superhighway”, or, rather “the *accidental* superhighway” as *The Economist* correctly labeled it (Anderson, 1995).

Through the second half of the 1990s, as the number of Netizens rose, national governments in on-line countries became aware that the Net might introduce information into their territories over which they have limited or no control, and which could bias the attitude of their citizenry *vis-à-vis* political and economic structures. This situation resembles past experiences with radio and television broadcasting, which have been instrumental for several governments to reach foreign audiences (Camilleri and Frank, 1992).²

Given the near impossibility of establishing an international regime of regulation either over the Net or to its increasing accessibility, several governments have embarked upon the technically costly and difficult operation of setting up national mechanisms of control. Under these conditions, the kinds of actions taken by national authorities have ranged from concerned discussions to cautious alerts to outright severing of connections, depending on which government branch is responsible for controlling the Net.

Governments and public opinions alike are now conscious (at least in the connected world) that the Internet can endow individuals with increasing communication power which, until recently, had been exclusively reserved to national authorities. This consciousness aroused competition as well as cooperation among the various actors to influence the Internet path of evolution. As Agnew and Corbrige (1995) have noted, the blending of computer technologies with the new systems of telecommunications is leading towards extraordinary changes from the point of view of international relations. This short chapter will outline the most significant stages in the genesis of the “accidental superhighway”, and stress those unique features of the Net that are still pertinent today.

² Serbia during the Bosnia war and during the NATO airstrikes in Kosovo in the late 1990s is one such example (although more mildly, NATO also applied perceptions management techniques to support the bombing). Other examples could include Radio Free Europe/Radio Liberty that broadcast to Eastern Europe during the Cold War, or, the still active Voice of America (<http://www.voa.gov/> v. April 4, 2001).

2.2 Making Internet History

The 1960s: ARPANET and packet switching

When in 1957 the Soviet Union successfully launched the first artificial earth satellite, the American reaction was fear of losing the technology race to the Soviets. The following year, within the Department of Defense (DoD), the United States established the Advanced Research Projects Agency (ARPA), "to lead in science and technology".³ ARPA will become the breeding ground of the Internet. The true vision at the foundation of the Internet can be traced back to a series of memos by J.C.R. Licklider of MIT in August 1962. Therein, Licklider—later first head of the computer program at the ARPA—envisioned the "Galactic Network" concepts, i.e. a globally interconnected set of computers through which data and programs could be accessed by anyone from any site, much like the Internet today.⁴ In those years, the Defense Department was the largest buyer of computers in the world, all of which had completely different operating systems and *ad hoc* software (Hafner and Lyon, 1996:42). Thus, the Pentagon was greatly interested in finding solutions to make its computers communicate together.

The other fundamental discovery at the origins of the Net was the development of packet-switching theory, based on the work by Kleirock (also at MIT) between 1961 and 1964, which was tested by connecting a computer in Massachusetts and one in California via a low speed dial-up telephone in 1965. Ordinary voice communications are carried through telephone networks as analog electronic signals. By connecting one circuit to another, the circuit-switching process enables the signals to travel from the caller to the receiver, within the same block as well as between two continents. In circuit-switching communications, however, the line connecting the caller and the receiver is occupied for the whole time, even though one or both users are not talking, excluding any other transmission on that line.

The packet-switching technology converts data (including voice, sounds, videos, etc.) into bytes which are then "grouped" together in packets. In other words, the digitalized

³ <http://www.isoc.org/guest/zakon/Internet/History/HIT.html> (v. March 18, 1999 and December 20, 2000).

⁴ The Web site of the Internet Society holds a substantial collection of "brief histories" of the Internet and the World Wide Web by different authors and in various languages (<http://www.isoc.org/internet/history/> v. March 10, 1999). I have mostly used the work "A Brief History of the Internet" by Leiner et al. (at <http://www.isoc.org/internet/history/brief.html>) because it included several of the "fathers" of the Internet among its authors. The most exhaustive, and most frequently updated timeline is the Hobbes' Internet Timeline by Robert Zakon (<http://www.isoc.org/guest/zakon/Internet/History/HIT.html> v. March 10, 1999 and December 12, 2000).

message is broken into “smaller messages” that can travel on telephone lines independently. Packets generated by different messages can line up and travel together, allowing a more efficient use of the same telephone line. In the same years, Paul Baran and his group at RAND studied the survivability of communications systems to nuclear attacks, thereby elaborating the concept of “distributed network”. To test the necessary “redundancy level” (i.e. the degree of connectivity between nodes in the network), Baran ran numerous

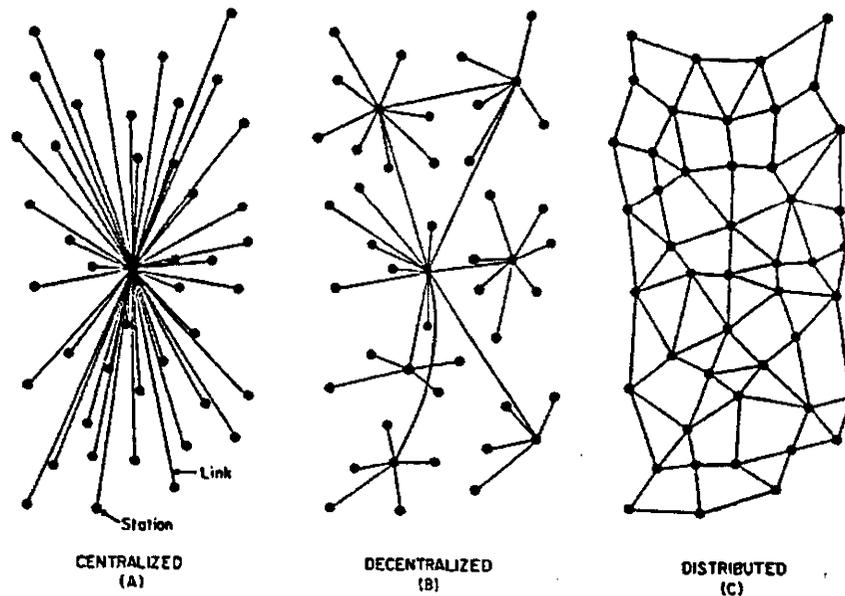


FIG. 1 – Centralized, Decentralized and Distributed Networks

simulations to determine the probability of distributed network survival under a variety of attack scenarios. He concluded that a redundancy level as low as 3 or 4—each node connecting three or four other nodes—would provide an exceptionally high level of ruggedness and reliability” (Hafner and Lyon, 1996:59). For the Defense Department the combination of survivability of communications systems and the ability of different computers to communicate with each other was too vital an opportunity to miss, and hence, began to invest growing resources in computer networks research. The sketches above are Baran’s three typologies of networks from his work “On Distributed Communications” (August 1964) (Courtesy of Cybergeography).⁵

It is worth noting that during the same time that the essential concepts of networking were being developed, computers were still highly centralized localized machines, and

⁵ <http://www.cybergeography.org/atlas/historical.html> (v. December 12, 2000). Baran’s original work is available at <http://www.rand.org/publications/RM/RM3420/> (v. March 18, 1999 and December 12, 2000).

computer technologies were hardly perceived as instruments of decentralization and diffusion. On the contrary,

...college students in the 1960s saw computers as impersonal tools used by the Establishment to keep control over the masses. But as the cost and the size of electronics continued to decline, the uses (and perceptions) of computers changed radically" (Resnick, 1998:11).

In 1967, the paper outlining the "ARPANET" was published by L. Roberts, while in 1968, a group from Bolt, Beranek and Newman (BBN), headed by Frank Heart and including Robert Kahn, won the DOD contract to build the first batch of the ARPANET. In April 1969, the first "Request For Comments" (RFC)⁶ discussing the basic "handshake", with which two computers start exchanging data was sent out to all the participants in the project (Hafner and Lyon, 1996). In September 1969, BBN installed the first host computer at the University of California (Los Angeles) which was soon connected to the Stanford Research Institute. A month later the University of California (Santa Barbara) and the University of Utah joined the network. Thus, by the end of 1969, through the mostly independent work of the MIT, RAND and ARPA—and the technical implementation by BBN—"...four host computers were connected together into the initial ARPANET, and the budding Internet was off the ground".⁷

The 1970s: The Internet Protocol (TCP/IP) and E-mail

In the 1970s, the idea of the Internet as a collection of independent networks began to mature, based on the key technical innovation called *open architecture networking*. "In the open-architecture network, the individual networks may be separately designed and developed and each may have its own unique interface which may be offered to users and/or other providers... Each network can be designed in accordance with the specific environment and user requirements of the network".⁸ Significantly, the types of networks, their scope or geographic location have been intentionally excluded by Internet creators from its origins. Indeed, as early as 1973, the first international connections of the ARPANET with the United Kingdom and Norway were established.

⁶ From then on, all the documents related to the Internet began using the same denomination and numeration.

⁷ <http://www.isoc.org/internet/history/brief.html> (v. March 20, 1999). Two British researches, Davies and Scantlebury, were also working on packet-switching in the U.K. at the same time.

⁸ <http://www.isoc.org/internet/history/brief.html> (v. March 20, 1999).

Two people were chiefly responsible for the TCP/IP protocol, namely the *lingua franca* set of instructions that allow otherwise incompatible systems to communicate together as a unique network, Robert Kahn (at DARPA) and Vint Cerf (at Stanford). Kahn and Cerf began to work together in 1973, thanks to their knowledge of NCP (Network Control Protocol)—the communication standard at the time—with the aim of shifting ARPANET and other networks from NCP to the more flexible TCP/IP. With the help of many other contributors, it still would take Kahn and Cerf ten years to work through the diffusion of LANs (Local Area Networks), personal computers (PCs) and workstations to achieve that goal.

The most important communication application of the 1970s, however, was electronic mail, familiarly called e-mail.⁹ E-mail was the brainchild of Robert Tomlison (at BBN), who in 1972 wrote the basic message send-and-read software, and chose the emblematic icon of all today's electronic communications (and to some extent of the Internet itself), the "@", as the symbol to separate the user's name from the host computer name.

Although "the ARPANET was not intended as a message system" but was only meant for resource-sharing (Hafner and Lyon, 1996:189), Tomlinson was "...motivated by the need of the ARPANET developers for an easy coordination mechanism".¹⁰ To this day, e-mail is still the most common application over the Internet.¹¹

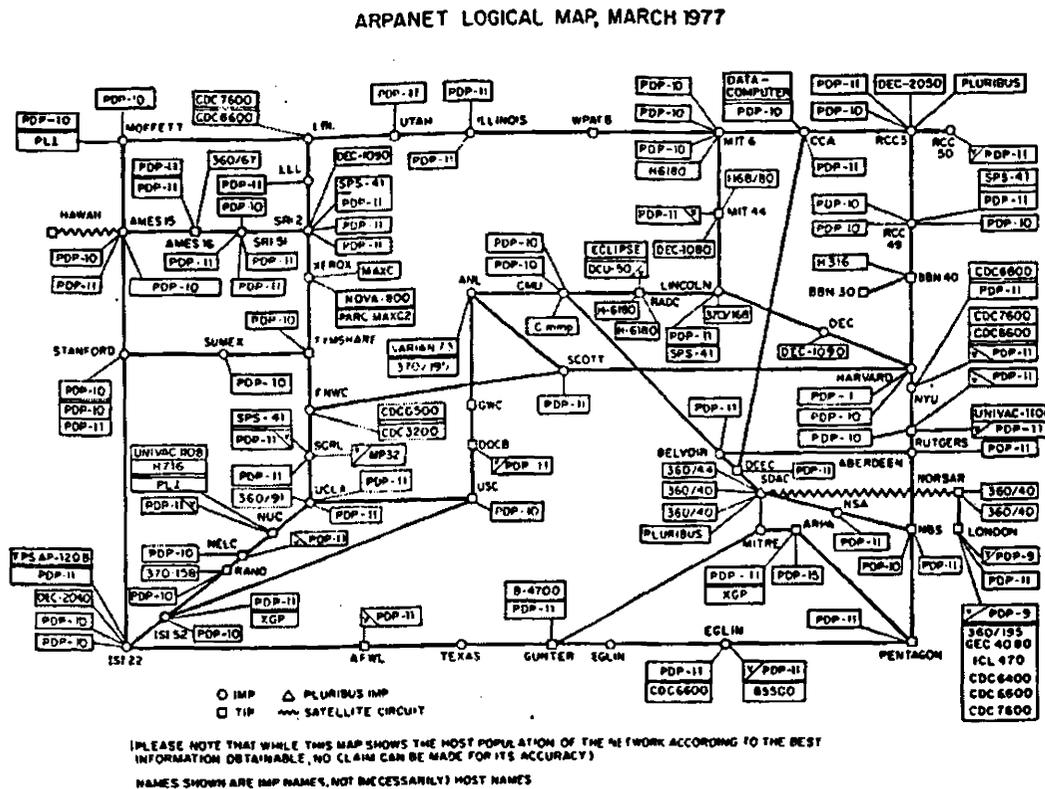
In the 1970s, time-sharing, networking and above all e-mail allowed more and more people to access and use computer power. Indeed, "[t]he more that people used the ARPANET for e-mail, the more relaxed they became about what they said. There were antiwar messages and, [during the Watergate crisis] a student advocated Nixon's impeachment" (Hafner and Lyon, 1996:205). As a consequence, as early as the 1970s, the new information technologies began to be seen as likely to increase the vulnerability of states. In a report to the Swedish government, the Tengelin Report, the main risks of a networked society were already highly emphasized, including dependence on foreign vendors and the threat of hackers' raids (Tengelin, 1981).

⁹ The comment by Postel (another of the Internet founding fathers) when he received the RFC describing e-mail was: "Now, that's a nice hack" (quoted in Hafner and Lyon, 1996:192).

¹⁰ <http://www.isoc.org/internet/history/bricf.html> (v. March 21, 1999).

¹¹ Vittal (a "hacker's hacker" according to Hafner and Lyon) marked another fundamental contribution to e-mail by inventing the "answer" (today's "reply") command which has made far easier to send messages without having to retype the e-mail address of the sender.

At the end of the 1970s, the debate on free speech was considered of vital importance within the networking community. In the words of Hafner and Lyon (1996:218), “by the 1980 the Net was far more than a collection of computers and leased lines. It was a place to share work and build friendships and more open methods of communication”. This graph represents a topology of the ARPANET in March 1977 (Courtesy of Cybergeography)¹²



The 1980s: NSFNET and the Domain Name System (DNS)

As mentioned earlier, it took a decade from the first studies of Kahn and Cerf to complete the transition of the ARPANET and other networks to TCP/IP. TCP/IP was adopted as a defense standard in 1980. On January 1, 1983, almost all the hosts converted simultaneously from NCP to the new protocol. The name "Internet" was chosen from the "Internetwork Protocol" section of the TCP/IP.

Between the end of the 1970s and the 1980s, access to the Internet for users at U.S. universities computer science departments became a discriminating condition for new students in deciding where to apply. Universities with ARPANET access had more and better candidates and more funds to carry out research in the new field. In order to compete

¹² <http://www.cybergeography.org/atlas/historical.html> (v. December 12, 2000).

with this trend, other networks without ARPANET connections began to grow: the CSNET (Computer Science Network, 1981), Bitnet ("because It's Time" Network, 1981), EUnet (European Unix Network, 1982) and so on. The most important was CSNET, created with funds from the National Science Foundation (NSF).

The NSF actually financed a high-speed (for that time) backbone (56Kbytes per second) which linked five super-computing centers, providing computing power for virtually every university in the United States. Thus, through its grants, the expanding participation of American universities, and the linking of ARPANET and CSNET in 1983 and later of the other networks (through Exterior Gateways Protocols, EPG), the U.S. National Science Foundation slowly became *de facto* the unofficial "administrator" of the Net for over a decade. A representative of the U.S. scientific community, the NSF, however, was never perceived by the community of users as a regulating, or let alone a controlling, authority. The strong belief that no hierarchical structure could be suitable for a distributed network was reinforced by the NSF management. The transmission technology (TCP/IP) and the distributed network structure thus indeed made the Internet a communication system that would be highly resistant to a nuclear attack, since there is no central "soft belly" that could be destroyed. This near invulnerability, however, was achieved at the price of not having a single authority center and centralized control mechanisms.

Notably, attempts to substitute the TCP/IP confederation approach (Gillet and Kapor, 1997), created by researchers working on connecting networks with other protocols, such as the OSI protocol (Open Standard Interconnection) by the International Standard Organization, have been met by reluctant or even hostile users. Despite its technical proficiency, the OSI has been regarded by Internet engineers and users alike as an imposition of an intergovernmental institution, which goes against the spirit of community and horizontal cooperation of the Net. According to Hafner and Lyon (1996:247/251),

on the OSI side stood entrenched bureaucracy, with a strong we-know best attitude, patronizing and occasionally contemptuous...[but] what the TCP/IP had it to recommend was the fact that it was unerringly 'open'. Its entire design was an open process...¹³

One of the essential innovations of the 1980s that also made possible the development of the World Wide Web (www or W3) was the Domain Name System (DNS). The DNS was first outlined in 1981/82 by Jon Postel and others. It has become more

¹³ The TCP/IP modularity and flexibility allow other protocols such as ISO's OSI to be used on the Net.

and more important since.¹⁴ The DNS (through the Address Resolution Protocol, ARP, and the Reverse-ARP) has enormously facilitated the learning of hosts IP addresses. Netizens, have no longer be compelled to remember the unfriendly decimal numeration of IP addresses (e.g. 149.139.6.101, i.e. www.iue.it). Host computers can then be given "names" (such as *whitehouse.gov*, *microsoft.com* or *iue.it*), so even casual or non-technical users can remember their email or their favorite Web page address.

As the first domains, *.com*, *.edu*, and *.gov* were registered at the Internet Assigned Number Authority (IANA), the DNS slowly evolved as one of the most sensitive and strategic issues about the Internet. Johnson and Post (1997:11) have observed that "although the net creators designed this system as a convenience, it rapidly developed commercial value because it allow[ed] customers to learn and remember the location of particular Web pages or e-mail addresses". IP addresses and domain names appear to be the same thing to non-technical users: however, unlike telephone numbers, IP addresses, once associated with domain names, are no longer "just numbers", but become as "personal" as an e-mail account or a trademark (e.g. www.cnn.com or www.mcdonalds.com), with considerable legal and commercial consequences (Shaw, 1997 and Oppedahl, 1997).

IP addresses and domain names are managed in slightly different fashions. Until recently, the most important institution was IANA, headed by the late Jon Postel, based at the University of Southern California and funded by the U.S. government. IANA allocated both domain names and IP addresses. The difference is evident at the lower level: IP addresses were distributed by the Regional Internet Registries (RIRs) for Europe, Asia-Pacific and the rest of the world, while country-specific Top Level Domains (ccTLDs), e.g. *.it* *.jp* *.uk* or *.za*, were issued to national organizations (such as a university or a telecom company), which acted as national registries and set their own policies (Gillet and Kalpor, 1997). Generic TLDs (gTLDs) such as *.com* *.edu* *.net* and *.org* were administered by InterNIC, operated by SAIC Network Solutions, a private company. InterNIC was also funded by the U.S. government and collected fees for the *.com* domain. IANA was then reformed in 1997.

¹⁴ Among the many RFCs on the DNS, worth mentioning here are n. 805 (February 1982 by Postel, [ftp://ftp.is.co.za/rfc/rfc805.txt](http://ftp.is.co.za/rfc/rfc805.txt)), n.819 (August 1982 by Postel, [ftp://ftp.is.co.za/rfc/rfc819.txt](http://ftp.is.co.za/rfc/rfc819.txt)), n.820 (October 1984 by Postel, [ftp://ftp.is.co.za/rfc/rfc920.txt](http://ftp.is.co.za/rfc/rfc920.txt)), n.1304 and 1305 (November 1987, by Paul Mockapetris, [ftp://ftp.is.co.za/rfc/rfc1034.txt](http://ftp.is.co.za/rfc/rfc1034.txt) and <http://www.dns.net/dnsrd/rfc/rfc1035/rfc1035.html>), and n.1591 (March 1994, the last by Postel, [ftp://ftp.is.co.za/rfc/rfc1591.txt](http://ftp.is.co.za/rfc/rfc1591.txt)). The complete list of RFC is available at <http://www.dns.net/dnsrd/rfc/>. All these RFC were visited on March 22 and 23, 1999 and January 8, 2001).

The 1990s: the Web, Mosaic, and the new (multi)media

Writing about the on-line world in the early 1990s, Reid noted that “[f]or all of its technological wonder, the Internet was an obscure scientific endeavor” (1997:xxiii). Even if, at the end of the 1980s, thousands of people were already using the Internet daily, the vast majority of them were scientists, researchers, and university students. Outside the research community few people knew about the Internet. Many of those scientists—quite logically and following the Internet tradition—made their research results and other documents available on-line. Search mechanisms able to find information and data, such as Archie, or user interface such as Gopher were already available to users. None of these mechanisms, however, could later compete with the popularity of the World Wide Web, WWW or simply, the Web.

The Web—the first “*killer application*” (Horak 1997:385)—was developed by Tim Berners-Lee at Geneva’s CERN, the European Laboratory for Particle Physics in 1989. “Tired of the hunt-and-peck process of locating and obtaining information...” (Reid 1997:xxiii), Berners-Lee developed software and networking protocol—the now ubiquitous HyperText Transport Protocol, HTTP—to support multimedia applications on a Graphic User Interface (GUI).¹⁵ In Berner-Lee’s words, “[t]he dream behind the Web [was] of a common information space in which we communicate by sharing information”.¹⁶ The Web was the first hypertext-based application to sort information by subjects. A multimedia hypertext mechanism allows an unknown word to be linked to its explanation which, in turn, could be linked to other documents as texts, images, graphics or sounds.

Berners-Lee and the CERN made two browsers (one text-based and the other for X/Windows, the MIT GUI for UNIX computers) and most of the codes for the Web available on the Internet. Borrowing from these sources, in 1992, as the Web was slowly attaining consideration and praise among the Netizens, Dan Thompson, John Hardin, Marc Andreessen, and Eric Bina of the National Center for Supercomputer Applications (NCSA) of the University of Illinois began working on the idea of a graphic browser which was later called Mosaic (Wallace, 1997). Later Adreessen left NCSA and, with John Clark, founded Mosaic Communications, which in October 1994 posted Netscape 1.0 freely downloadable on the Internet.

¹⁵ HTTP is the principal protocol for Web applications. Berners-Lee also developed the HyperText Markup Language (HTML).

¹⁶ <http://www.w3.org/People/Berners-Lee/ShortHistory> (v. December 20, 2000).

Netscape Navigator quickly became the favored browser of an increasing number of users. Thus, between 1994 and 1995, the graphic refinement of the new browsers and the multimedia capability of the Web became the ultimate ingredients that truly allowed the Internet to grow from a scientists' instrument to a mass culture phenomenon. Indeed, the possibility to send images, and more recently music and videos, over the Internet has changed considerably and forever the nature and appeal of the medium, particularly for businesses. Shapiro and Varian (1999:6) have noted that "the computer scientists that designed the protocols for the Internet and the World Wide Web were surprised by the huge traffic in images". The widespread talks and interests of the international business community for the Net can thus be explained by the fact that "image is everything in the information biz, because it's the image that carries the brand name and the reputation" (Shapiro and Varian, 1999:6).

In 1995 NSFNET reverted back to a pure research network. The majority of Internet traffic was then carried through interconnected networks providers, both public and private (ISPs). With its "privatization", the Internet came of age into its present form.

2.3 A History of the Future

As in the past, the dilemmas facing the future of the Internet can be grouped together into two sets, namely technical and ethical/political problems which have often "competed" in the past to steer the evolution of Net in one way or another. It is not accidental that, currently, the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB) and the Internet Society (ISOC) are among the most prominent, non-governmental "Net-institutions" for the future of the Net. With the progressive commercialization of the Internet, their influence could be challenged probably only by another Net-institution, namely ICANN, the authority for the DNS.

Among others, the Net future challenges will include technical problems due to the growing demands of the business community for faster and more reliable services, such as videoconferencing, as well as ethical/political issues including privacy, free speech and harmful contents. A major breakthrough in the evolution of the Net is already identifiable: i.e. the birth of faster, newer "Nets", connected to the old, public Internet, but without many of its current users. As Hallgren and Mc Adams (1997:470) have observed,

the Internet of today could face the same fate as did the ARPANET of old...The performance of the ARPANET became increasingly degraded (its service was depleted more and more) while access became more and more widespread (it remained non-excludable). This proved to be the worst of all world.

Indeed, the old Internet version 4 (IPv4) is markedly inadequate for the requirements of so many users, including private businesses, or those of advanced research. As *The Economist* (October 19, 1996:15) has noted,

...companies are increasingly building private Internets either to connect their internal users, or to ensure fast communications with other firms. These private networks will solve other Internet problems: they offer quality-of-service guarantees, and better security against hackers. Geeks will grumble that they risk causing the balkanization of the Net. Customers will be delighted by absence of delays.

The new Internet—based on the IPv6 protocol, the Asynchronous Transmission Mode (ATM) or other protocols, or a combination of them—will be designed and equipped with security and control mechanisms incorporated from the beginning, an added feature that was not available with the old version of the Net. In the second generation Internet, the adoption of more efficient, top-down standards and regulations will probably be facilitated and accepted by users who will favor effectiveness, reliability, and stability at the cost of greater structuralization and accountability, rather than openness and accessibility. Ultimately, the Net may become dominated by user-friendly networks such as AOL (America On Line)-Time Warner, or MSN (Microsoft Network) and portals like Yahoo!, which offer safe-for-children contents and simplicity of use.

With so many private and public subjects offering Internet access, logging on the Internet has become increasingly “commoditized”, while industry players have been forced to adjust their pricing strategies in order to cope with fierce competition. As a consequence, prices to access the Internet have decreased, although differences between countries and major providers remain enormous. Pricing, quality of service and priority traffic (such as video) will press private businesses and telcom carriers towards “...parallel global internets of their own on which customers, for a premium payment, will be guarantee more reliable service than the public Internet can now offer” (*The Economist* October 19, 1996:24).

The tradition of time-sharing and efficient use of computing power has remained embodied in today's Internet. The simultaneous use of computers in temporary idle status spread over the entire Net to solve complicated mathematical problems is one of the contemporary symbols of that tradition.¹⁷ This technique, called parallel computing, has also

¹⁷ The SETI (Search for Extra Terrestrial Intelligence) project is one the most famous.

made it possible to routinely break the DES (Data Encryption Standard) code, i.e. the algorithm used to make secure all the U.S. government communications. In 1998, Distributed.Nets—a worldwide coalition of computer enthusiasts—along with the Electronic Frontier Foundation's (EFF) *Deep Crack*, a specially designed supercomputer, teamed up a network of nearly 100,000 PCs on the Internet. Together, they won a competition to crack information coded with the United States government's DES in a record-breaking 22 hours and 15 minutes.¹⁸

The open community spirit has also been discernible in the competition between open and proprietary source software. Operating systems (OS) like Linux, browser like Netscape and languages like Java are all based on open source software. With open source software, the “inner core” (the algorithm) of the application/system is made available to anyone to be modified, adapted or otherwise changed. Usually, the original creators of the software retain some sort of “veto” (the so-called “benevolent dictator”), but the possibilities for variations are endless. In so doing, software products take advantage of the enthusiasm and dedication of thousands of software developers. While “the Internet makes it possible to distribute the results of their labor anywhere at almost no cost...open source software is the fruit of creative anarchy” (*The Economist*, February, 20, 1999:73). In this respect, open source is still in harmony with the original nature of the Net, and the attitudes of countless Netizens.¹⁹

On the contrary, proprietary source software such as the Windows operating system and Windows applications is known only to Microsoft engineers, and improvements and changes could only be done “in house”. Open and proprietary source codes have been compared, respectively, to “The Bazaar and the Cathedral” (*The Economist*, February 20, 1999:74). If one thinks of the some 40 million lines of code of Windows 2000, the image of a towering software cathedral does not appear to be inaccurate.

Microsoft began to be interested in the Internet only in 1995 when the multimedia Web and Netscape were rendering the Net more attractive and accessible for non-technical users and, above all, businesses. Despite that the open nature of the distributed network was incompatible with the proprietary software policy of Microsoft (Wallace, 1997), Microsoft devoted considerable resources in contesting Netscape supremacy by developing its own

¹⁸ The Global Internet Liberty Campaign (GILC), News Alert, January 25, 1999 at <http://www.gilc.org/alert/> and also <http://www.pcworld.com/cgi-bin/pcwtoday?ID=9413> (v. March 18, 1999).

¹⁹ In fact, within “...the loose fraternity of volunteers...tampering with the file that lists the contributors to a program amounts to a high crime” (*The Economist*, February 20, 1999:74).

browser Explorer, and making it freely available with Windows 95. Microsoft soon conquered a near monopolist position in the browser business as well (Reid, 1997 and Wallace, 1997).

This outcome led to an anti-trust trial recently in the late 1990s unfair business practice of Microsoft's, which saw the unusual coalition of the U.S. Justice Department and Internet libertarians. Many users have indeed interpreted Microsoft's attention to the Net as an attempt by the software monopolist to impose its will also upon the "anarchic" on-line community (Wallace, 1997). Currently, Netizens and Internet liberties groups are afraid that soon national governments will be replaced by large corporation in the struggle to control the Net, and that the case with Microsoft was only a foretaste of things to come.

Another example of the on-going struggle described above is the battle over free use of encryption software by individual users. While computer networks enormously facilitate communications among distant people and on-line services such as electronic commerce, they can also provide vast collection of personal data and preferences of users. Cryptography is thus the more important as a means to protect personal identities and data, which for many human rights activists becomes a matter of survival. At the same time, cryptography is indispensable to on-line commercial transactions. These circumstances have stimulated the alliance between Netizens, civil liberties, and human rights NGOs and the private business sector, which now have a common view on the free use of encryption software. This outcome is all the more important since on other human rights issues, the two sides frequently clash.

The countries producing most of the encryption software are all members of the Wassenaar Arrangement: i.e. an international agreement signed by 33 countries in July 1996 about, among other items, cryptography.²⁰ Following fundamentally the U.S. position ("because of terrorism fears"), the 33 members countries of the Wassenaar have agreed that the distribution and export of cryptography software with keys over 64 bits²¹ in length should be regulated through international controls, (Nua Survey, 1998). However, as

²⁰ Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, Slovakia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and the United States (<http://www.wassenaar.org/docs/talkpts.html#States> v. March 20, 1999). Most of the members of the Wassenaar Agreement (<http://www.wassenaar.org/> v. March 20, 1999) were also members of the COCOM committee which regulated dual-technology exports during the Cold War.

cryptography experts still see 64 bit software as insufficient to ensure secure and private transactions, other countries, such as Canada and Finland, have taken a more liberal approach, in order to promote e-commerce by ensuring greater security.

The Waassenar Agreement has not been an expression of unanimous opinions. The European Union and the United States have rather divergent views about allowing Netizens to strongly encrypt their communications so that it would prevent government agencies from intercepting them. According to the "Cryptography and Liberty" survey by the Global Internet Liberty Campaign in 1998, with the exception of France, all EU member states have a "relaxed attitude" toward free use of cryptography for individual communications. Recently, even France has become more moderate in that regard (EPIC, 1999a).

In January 1999, with the stated goal of increasing the confidence of the French consumers in the security of on-line transactions, the French government announced that it would allow the use of 128-bit²² encryption technology. The decision to liberalize was a consequence of long-term lobbying by French private business and was opposed by the French Army (Alberganti, 1999). Until then, France's traditional policy on the use of encryption was to permit only 40-bit technology, and to require that any use of encryption be authorized by the government which should also be provided with a key. The conditions for freer use of encryption software have also changed in the United States as well (Levy, 2001; see also chapter four).

The different attitude in the EU and the United States with regard to the collection of personal data and privacy protection is worth stressing too, as the European Union has adopted a more interventionist stance than the United States, approving the Directive 95/46 setting common rules for the trade and use of those data.²³ Article 25 of the Directive—which went into force on October 25, 1998—has caused considerable concern among US businesses trading or residing in Europe. Actually, the article stipulates that information should pass freely between member states who embrace the directive, but not to countries where there is inadequate privacy protection.²⁴ The Directive triggered considerable

²¹ A 64 bytes encryption key (i.e. 2⁶⁴ possible combinations) can be broken in months or years by the only intelligence organization with enough computing power, i.e. the U. S. National Security Agency (Campbell, 1999)

²² 2¹²⁸ possible permutations.

²³ http://europa.eu.int/eur-lex/en/lif/da/1995/en_395L0046.html (v. March 30, 1999).

²⁴ The United States has actually fares rather low in the classification used in the quantitative analysis section of this work. In a scale from 0 to 7.5, the United States scores 2.5 (see chapter three).

discontent among US businesses (*Financial Times*, 1998), and the possible threat of a trade war about personal data cannot be entirely excluded (*The Economist*, January 19, 1999)

The treatment of personal data and encryption software are not the only issues that may put the United States and the EU on a collision course. The struggle to control the DNS allocation and power distribution within ICANN are also likely to raise tensions. Controlling the allocation of domain names and influencing ICANN's activity have tremendous effects on the success or failure of on-line business, as well as on the freedom of users to choose the names they prefer. Examining the DNS dispute will also be important since it will shed some light on the in-coming struggle between users and large corporation, once their struggle against governments' control will be over.

Managing the DNS has always been complicated, if not worse. As Shaw (1997:108) has observed, "...what began as essentially a U.S. mess [has turned] into a global one". Generic TLDs have always had a particular appeal for businesses and Netizens alike. Although a national domain name for the U.S. does exist (.us), the United States has retained exclusive jurisdiction on .gov .mil .edu TLDs. Thus only .org .net .int and, above all, .com are truly international. Indeed, because of the growing commercialization of the Net, .com has become *the* essential domain for companies, thus generating considerable pressure on its allocation. Moreover, the collection of fees and the management policies to distribute that TLD by an American company has provoked considerable discontent in many other countries.

In July 1997, the U.S. administration decided to privatize the management of the DNS. In 1998, the U.S. Department of Commerce, Internet NGOs—including ISOC and IETF—and a few private companies founded the Internet Corporation for Assigned Names and Numbers (ICANN).²⁵ ICANN, a not-for-profit organization, will manage generic TLDs and IP addresses much as IANA, but it will not depend on the U.S. government for funds and should be completely sustaining.

On the surface, ICANN would appear to be less subject to influence from the U.S. government. In practice, the role and authority of American actors within the ICANN is immense, and the whole process of creation of ICANN has induced significant unease in many European participants, including the EU. It is only probable that with the increasing commercialization of the Internet there will be more and more occasions for management policy conflicts between the United States and Europe over TLD assignment.

The final point worth mentioning with regards to the future of the Net is that of freedom of speech. Hafner and Lyon (1996:211), in summarizing the disposition of the original developers of the Internet with reference to freedom of speech, have observed that “in a realm where, in a sense, personal identity is defined entirely by the words people choose, free speech seemed second only to the concern about the survival of the realm itself”. For many Netizens, freedom of speech is still the foremost peculiarity of the network.

Nowadays, freedom of speech on the Net is defended by many non-governmental “Net-institutions”, such as the Internet Society and the Electronic Frontier Foundation, which are the oldest and most important; the Center for Democracy and Technology, the Electronic Privacy Internet Center, and several others. They are all coordinated by the Global Internet Liberty Campaign. The defense of freedom of speech on-line was seriously hindered though because, until recently, these organizations were almost exclusively concerned with events in the United States; most of them now have national branches in other countries (particularly in OECD countries) and try to coordinate the protection of free speech and other civil liberties policies in the on-line world.

Despite the multinational reach of the Internet, it would be wrong to assume that the effects of U.S. domestic policy decisions on what constitutes free speech—or privacy, for that matter—are now less powerful in relation to the future evolution of the Internet. On the contrary, it seems that there has been a sort of “internationalization” of the First Amendment as the standard to assess freedom of speech in countries with access to the Net is further strengthened by article 19 of the Universal Declaration of Human Rights on the free flow of information principle.²⁶

Shapiro and Varian (1999:2) have remarked that interconnection battles have arisen regularly in the past century, from telephone, to airlines, to the computer industry. The Internet cannot avoid being the current bone of contention. While it is too early to identify the winning parties among the various actors (governments, private business, civil liberties NGOs, etc.) competing to influence the future evolution of the Internet, two generalizations emerge from this “history of the future”. First, the unusual alliance between private

²⁵<http://ntiantl.ntia.doc.gov/ntiahome/domainname/agreements/92899sccpr.htm> (v. March 30, 1999).

²⁶ Art.19 state the “freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers”. Notwithstanding the First Amendment (and its “internationalization”), American pro-family groups will continue their attempts to activate legislation to impose restrictions and filters on Internet content (see chapter four).

businesses and civil liberties NGOs is winning the day against the law enforcement/national security community on the common ground of protecting the Net from further intrusion by governments. Second, the next struggle about Internet control will be between users and pro-freedom NGOs against large corporations (Microsoft and the like).

From the problems outlined in this section, it is only reasonable to conclude that, in the absence of a multilateral international agreement, the United States, the European Union and other countries will continue to argue over many of these issues. The effects of these quarrels—given also the political, economic, and technical supremacy of the United States in this respect—will profoundly influence the evolution of the Net and its receptions by new users as new countries come on-line. Some key issues, however, are most likely to stimulate the most computer-dependent countries (notably all OECD members) to make extra efforts to enhance cooperation and establish international regimes. Of these issues, the most significant is cybercrime.

The Council of Europe (COE)'s Draft Convention on Cybercrime can be regarded as a relatively successful example of a "limited" international regime on the Internet, since it has seen the participation of several concerned countries.²⁷ Originally, the forty-some members²⁸ of the Council, the United States, Japan and others were scheduled to sign it in December 2000, and then in June 2001.²⁹ However, it will be extremely complicated to enact the same provisions in such different penal systems.³⁰ Furthermore, the convention will exclude several Asian, African and South American countries. While these countries still produce little Internet traffic, they may oppose the treaty as being imposed by the industrialized, networked North. They may prefer a U.N.-based treaty, which would take even longer to be drafted and then signed—and, clearly, be even more generic.³¹

²⁷ <http://conventions.coe.int/treaty/EN/cadreprojets.htm> (v. November 23, 2000 and March 14, 2001).

²⁸ [http://www.coe.int/portal.asp?strScreenType=100&L=E&M=\\$t/1-1-1//portal.asp?L=E&M=\\$t/001-00-00-2/02/EMB.1.0.0.2.Map.stm](http://www.coe.int/portal.asp?strScreenType=100&L=E&M=$t/1-1-1//portal.asp?L=E&M=$t/001-00-00-2/02/EMB.1.0.0.2.Map.stm) (v. November 23, 2000). All the European countries, including Russia, Ukraine, and Turkey, minus Bosnia, Yugoslavia, and Bielorussia.

²⁹ As of March 2001, the number 25th draft is in its 5th version (probably it was thought that having a draft no.30 would be too many) (<http://conventions.coe.int/treaty/EN/cadreprojets.htm> v. March 14, 2001).

³⁰ The implementation should be easier for EU countries, which can rely on the "third pillar" (justice and home affairs) of the Maastricht Treaty. Nonetheless, EU member states' penal codes are still considerably dissimilar. Discrepancies also exist within countries (<http://www.mcconnellinternational.com/services/CyberCrime.htm> v. December 12, 2000).

³¹ Here as elsewhere, with regards to the Internet, time is a critical factor. Normally, international treaties take considerable times between their drafting and their reception by national legislatures (extensive negotiations are the norm in international diplomatic law). Given the pace of technical changes, however, on the Internet, a year or even a few months are considered to be significant intervals of time by computer experts, and, as demonstrated by the MCDonnell International's report, it will take considerable time and effort to update laws to new technological levels in the majority of countries

A most remarkable aspect of the cybercrime draft, however, has been that, after version no.18 of the draft was produced by the COE's Committee of Experts on Cybercrime, it was decided to make the drafts public, and put them on the Web.³² Once the drafts had become public, pro-liberties NGOs in Europe and the United States started harshly criticizing the proposal of the convention. In December 2000, the Global Internet Liberty Campaign (GILC), an umbrella organization for several Internet NGOs, sent an open letter to the COE Secretariat opposing the draft,³³ while many NGOs assured that they would counter the signature of the convention in their national legislatures. The domestic constraints of a national COE delegation have obliged governments to make the convention public. Once the information was available, it was passed around by NGOs and concerned users, who have organized their resistance. For unclear reasons, the actual signing keeps being delayed.

2.4 Some Concluding Remarks on the Future of the Internet

The brief historical review has shown how the Internet is truly unique among the media and telecommunication systems, with a frontier penetration capability that other means do not have. Many (if not all) national governments have been slow to recognize this fact. Gradually, the most diverse political or social groups have learned how to exploit the Net to voice their interests. The Internet has also created its own community, i.e. "a group of human beings with complimentary habits of communication" broadly defined (Deutsch, 1988:75). What used to be a small, compact community, however, will become a polarized mass in the near future: those who are willing to accept more control in exchange for faster and more dependable performance of the Net and those who are not.

In the future the Internet will probably be split into two networks: the faster Internet 2 (or whatever it will be called), to connect universities, government institutions, and the business community, and the slower, older but cheaper Internet on IPv4. The cost/quality ratio, the bandwidth consumption, and the multiplicity of information and other service sources will be cardinal for today's users to decide which network they will use. For the time being, the majority of users seem still to value multiplicity of contents as much as

(<http://www.mcconnellinternational.com/services/CyberCrime.htm> v. December 12, 2000).

³² Although it has not been confirmed, it seems that the Swedish delegation to the COE insisted that if the drafts were not made public by the COE, Sweden would then publish them.

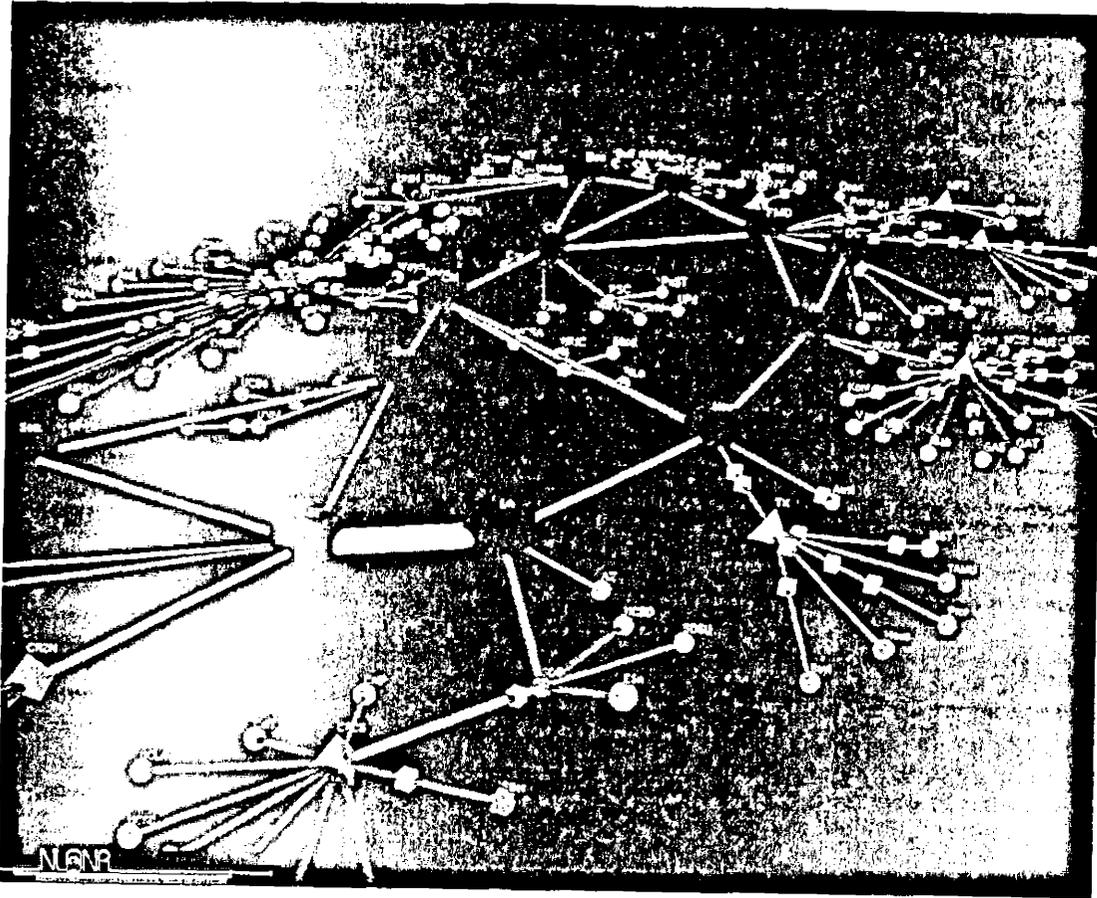
³³ <http://www.gilc.org/privacy/coe-letter-1200.html> (March 14, 2001).

connection speed. A “cheap” Internet will continue to exist and a growing share of people in non-industrialized countries will be able to log in.

As it keeps expanding, after surviving its privatization, commercialization and much expected collapses, it is only likely that it will continue to do so in the future. The burden of controlling the Net will then shift from governments to private enterprises.³⁴ At least in democracies, the most striking aspect of this evolution will be that while governments (admittedly, to different degrees) are accountable to parliaments and voters, private business area accountable only to their shareholders. The latter can be pressured by the market, but civil liberties organizations, as well as Netizens, will have to learn the skills of this new trade, and understand that companies do not react to the same stimuli as national governments. In 2001, even a pro-market magazine such as the *The Economist* (Siegele, April 14, 2001)—noting that the future of the Net could not be left to a “handful of firms”—went as far as demanding that governments shifted funds from government regulating agencies to informal, but well-established and well-recognized groups such as the Internet Engineering Task Force (IETF). Such non-profit, quasi-academic groups come very close to the idea of scientific communities that would operate for the welfare of the Internet as public good.

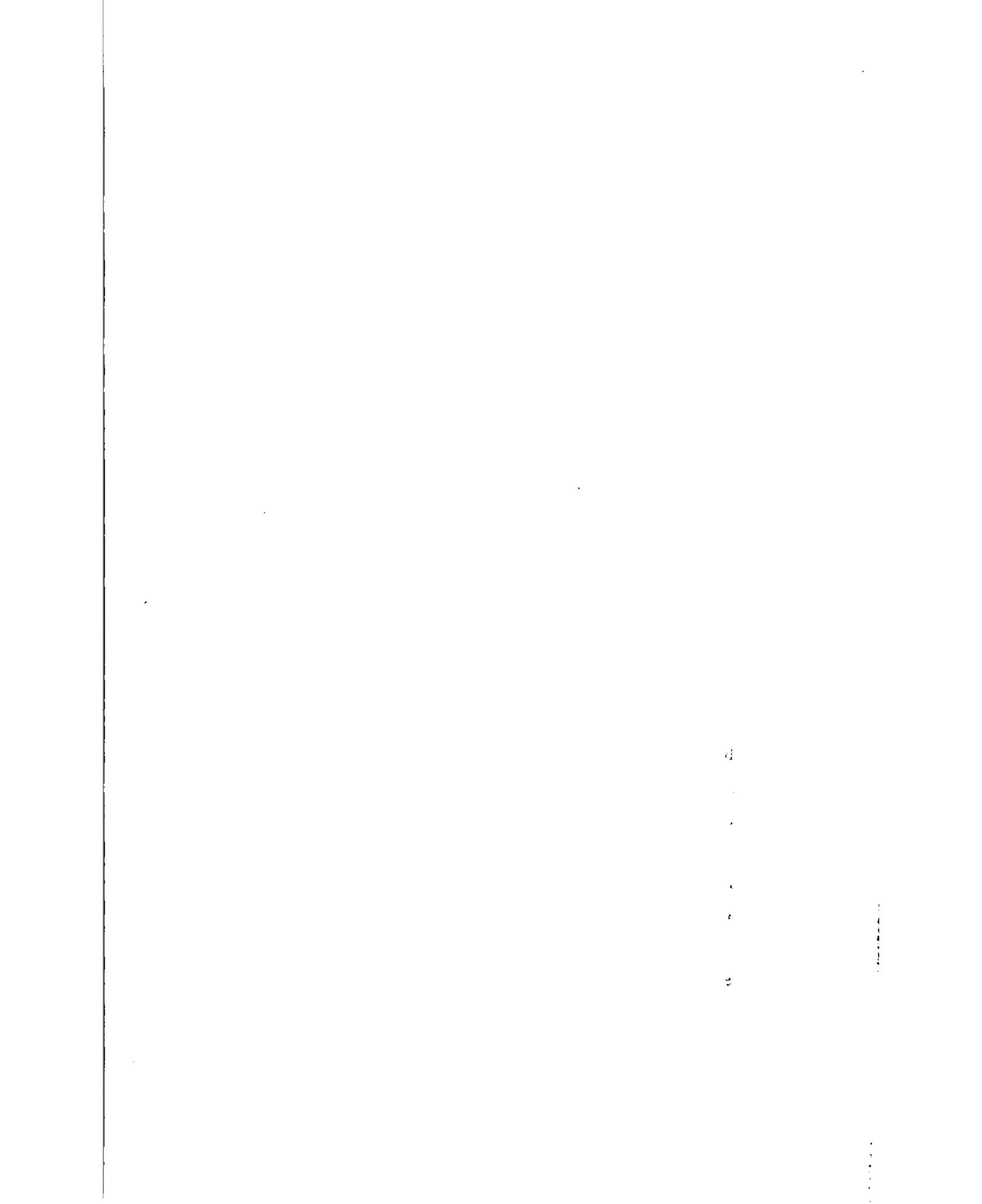
As Rosenzweig (1998:1552) has noted, “[t]he future remains uncertain. But it is clear that any history of the Internet will have to locate this story within its multiple social, political, and cultural contexts”. To overcome the problem of connecting different machines—and despite its Cold War origins—the Internet has been built with goals of openness and general access for any users. The notion that one day data and information should need to be protected or excluded from users was hardly present in the minds of the original developers of the Net (although it was probably well present in the minds of the DOD’s planners). Today’s requirements for corporate data or public administration information impose different priorities for which today’s Internet is not always truly compliant. The Internet of tomorrow will thus be the sum of more articulated networks with differentiated access for users and various degrees of control, constantly in balance between centralizing tendencies and its open, distributed, and ultimately *chaotic* structure.

³⁴ For instance, at the end of 2000, the Computer and Communication Industry Association (an American industry group) published a report that “[t]he private sector [was] handling the e-commerce craze just fine, thank you, and the government should just butt out”...”, at <http://www.techweb.com/wirc/story/TWB20001013S0008> (v. December 20, 2000 and January 10, 2001).



A topological, 3D map of the Internet in 2000, with the different colored blocks representing communication nodes (Courtesy of Cybergeography).³⁵ The “picture” only shows U.S. nodes (which, as of 2001, are still the most numerous), but gives a fairly accurate indication of what the Internet worldwide is now like.

³⁵ <http://www.cybergeography.org/atlas/topology.html> (v. December 12, 2000).



CHAPTER THREE: THE QUANTITATIVE ANALYSIS OF INTERNET CONTROL

3.1 Introduction

The goal of this chapter is to present the quantitative methods I have applied in my research, along with the cross-tab matrices containing the data currently available, and the final results of the computation. I first used quantitative analysis techniques to investigate my hypotheses. The basic "bits" of data for my observations have been national laws and regulations, information on income, education or defense spending, as well as results from surveys. This procedure for quantitative inquiry is similar to that used by Quinn (1997) to measure changes in international financial transactions.

Quantitative analysis is a powerful instrument to explore causal inference, even for non-experimental research, as is often the case for social sciences (e.g. Blalock, 1970). However, many problems could be encountered in undertaking such investigations: data are missing or of poor quality, the sample may not be entirely representative, etc. etc. These conditions are particularly true when the units of analysis are countries.

A casual glance at the draft SPSS and Excel printouts enclosed in the appendix confirms such pitfalls: a considerable portion of observations lack data for one or more of the 11 variables. Furthermore, research on the political implications of the Internet has only recently been undertaken by political science scholars,¹ and attempts to assess the levels of national control on the Internet (LOC) have been nonexistent. In addition to the scarce literature on the issue, there is more significantly no accepted unit of measure. The sample for my research includes 65 countries. Despite the complications mentioned above, even if ten or more observations were excluded at each computation, there would be still enough observations to be within the limits of the "rule of thumb" of the Social Sciences that $N > 30$ (Lewis-Beck, 1995:33) to justify the choice to perform quantitative analysis.

Even when information is of good quality, establishing causality often requires supporting the findings of quantitative techniques with other methodologies, such as case-studies, which, incidentally, is the path that I intend to pursue in my investigation. Indeed Blalock (1960:337) has pointed out that "...correlation analysis cannot be directly used to

¹ For instance see Kedzie (1996) on the impact of e-mail and Internet communication on the development of democracy.

establish causality because of the fact that correlations merely measure covariation or the degree to which several variables vary together". King et al. (1994:69) have suggested that the practice of combining the insights of case studies with large-*n* techniques should be followed more often in contemporary social science.

As Lewis-Beck (1995:1) points out, judgment must ultimately be exercised in properly interpreting any statistical result, especially when it comes from non-experimental social research like this project. Given the scarcity of sources and information on this issue, applying these techniques have offered an additional, indeed invaluable, perspective in my research work and the completion of this dissertation.

3.2 The Methodology

Here, the five working hypotheses are presented and described as they originally were conceived of before I started my quantitative analysis. Clearly, at the end, the results obtained have made revising the hypotheses inevitable. One was rejected (H2), and the others modified, before proceeding with the second part of the research (the qualitative analysis).

3.2.1 Working Hypotheses and Indicators for Variables

In this section, the five competing hypotheses (H1 to H5) are summarized, along with the indicators to represent them. In the next section, the indicators for the dependent variable, i.e. the level of control (LOC) over the Internet will be illustrated. Details about the data and their sources are given in the section 3.2.5 further ahead, as well as in the Summary Table in the last pages of this dissertation. The five working hypotheses are:

1. the exigency of national security (H1 or X1); I have generalized the national security hypothesis as follows: *the more a state is determined to protect its national security, the more it will seek to control access by its citizens to the Internet.* Indeed, many governments tend to keep their level of control over the Net from public discussion because of "national security reasons". As Supperstone (1981:270) observes, "once the government controls the definition of 'national security', there is no limit to what information it may decide to fall into that category". This attitude seems quite common, although currently, only a minority

of all the countries currently on-line truly run the risk of becoming targets of information warfare-related attacks. The variable for H1 is called **defense** in the data matrices.

2. the individualist/collectivist structures of on-line societies (H2 or X2). Often used in social psychology, this differentiation has been applied, for instance, by A. Horowitz (1980, p.13 in particular) in his study on social control. This hypothesis can thus be summarized as, *the more that the state under consideration is concerned with individuals' liberties (including personal communications), the freer the Internet will be; and vice versa the more concerned with social cohesion the state is, the more controlled the Internet.* Pro-individual societies would pressure their governments to grant the most open and free access to the Internet, accepting just a minimal level of regulation (such as self-regulation, for instance). The indicator is the Individualism Index developed by Geert Hofstede in 1984 (and re-used in 1991), which measures the level of individualism in the sample of 40 countries. The variable for H2 is labeled **individ**.

3. the democracy level of on-line countries (H3 or X3). The third working hypothesis can be outlined as *the more democratic a state, the freer the access to Internet for its citizens, and vice versa the more authoritarian a state, the more controlled the Internet access.* The qualification of countries as democracies and non-democracies is the subject of many and diverse research approaches. For this hypothesis, I rely on the Polity III data set for the categorizing of countries as democracies and non-democracies. The variable for H3 is named **democracy**.

4. the regulatory propensity of the sample countries (H4 or X4). To cope with the problem of controlling Internet access and use in their territories, in all likelihood, states will fall back on their regulatory propensity towards other media and telecom services.² As a matter of fact, several governments could argue that, despite its peculiarities, the Internet does not need a special code since it is already covered by existing laws on telecommunications and media (press and broadcasting). Working hypothesis number 4 can be epitomized as *the stronger the regulatory propensity of states considered, the more controlled the Internet access will be.* The regulatory propensity can be assessed by looking at how the process of

² For the relevance of government's role in telecommunications, compared with other industrial sectors, see Stone (1997).

liberalization and privatization of the economy are. Observations for this hypothesis have focused on the telecommunication sector; 11 types of telecom services have been categorized by the International Telecommunication Union (ITU) as fully competitive (C), partially competitive (PC) or monopoly (M). The higher the number of services which are either in full or partial competition, the lower the propensity toward regulating telecoms and media services. The variable for H4 is called **telcomp** (telecom competition).

5. finally, the **free trade/economic openness** of the countries considered (H5 or X5), or in other words, *the higher the free trade propensity and the more open the economy of a state, the freer the Internet*. For this hypothesis, the type of economic approach will be paramount for the classification of countries. States with open market economies and favorable to international trade will tend to assure fair conditions to everybody wishing to enter the market for e-business, whereas states with more controlled economies may adopt regulations about on-line business that would protect specific sectors of the economy, both in industry and finance, or certain social groups or economic elites. These states will privilege the cohesion of their societies to the possibility of expanding trade and financial services with other countries via the Internet.

H5 was originally tested with two indicators, **tradepro** and **ecofree**. The former has been chosen to indicate the *international trade propensity*, the latter the level of *economic freedom* in selected countries. Countries with higher international trade propensity should have a positive attitude and hence higher expectations about e-commerce as an instrument to foster their commercial proficiency. Countries with higher levels of economic freedom/openness should also have a positive stance about e-business (they would see it as an additional opportunity to expand their economies), and thus should not control/regulate the net. Clearly, some countries with large or dynamic domestic markets may also be highly interested in e-business—and thus have high expectations—regardless of their propensity toward international trade. Other countries with less open economies may equally see the Internet as an opportunity to look more “modern” or even more open.

These problems, as others similar to them, are associated with the quality of data. Unfortunately, although I have surveyed other studies, proper indicators for e-business are still under development.³ This is the main reason why I have tried two indicators for H5.

³ For instance, a 1999 study by the University of Texas (“Measuring the Internet Economy”, at

Expectations for the benefits of e-business and the New Economy play a fundamental role in limiting the level of governments' control on the Internet. Technically and legally, Internet control can represent a severe hindrance to e-business. Thus, national governments that have high economic expectations about the Net will seek to limit control to what is absolutely necessary. Assessing these expectations, however, is extremely problematic, since there are no universally accepted indicators. Consequently, in addition to H5, I have decided to consider H4 also as a measure of such anticipations.

3.2.2 Internet Levels of Control (LOC): The Dependent Variables

The variation of the intensity of control (expressed through higher or lower levels) adopted by different governments is my dependent variable (DV). Indeed, the objective of my research is to comprehend the causes that determine different levels of political control (LOC) on the Internet across countries. As the dependent variable, the LOC is neither easily measurable nor promptly available in the existing literature. Hence, the LOC can be studied only through the observation of proxy indicators.

Political control over the Internet can be exercised, essentially, in two ways, notably (a) *limitation and discrimination of access* to the Net (e.g. through licensing procedures based on political or social affiliation or restricting access to trusted users), and/or (b) *censorship on contents* exchanged on-line. In turn, the latter can be performed through (b1) pro-actively *monitoring* the behavior of local Internet Service Providers (ISPs), and/or (b2) passively *screening* the various on-line procedures (e-mail, newsgroups, Web sites, etc.) utilized by private individuals to exchange information over the Net. This latter action includes, most notably, checking whether or not users encrypt their communications.⁴

In this work, I have defined *statutory control* as national rules and regulations adopted by governments to limit or select individuals' access to the Net; to search and monitor on-line users' preferences and choices; as well as the prohibition, as criminal acts, of accessing specific Web pages or newsgroups; or diffusing, through Web pages,

http://cism.bus.utexas.edu/works/articles/internet_economy.pdf v. October 27, 1999 and March 26, 2001, and also mirrored at <http://www.internetindicators.com/internetindic.html>), or the OECD Internet and Electronic Commerce Indicators (<http://www.oecd.org/dsti/sti/it/cm/stats/newindicators.htm> v. October 27, 1999, October 13 and 15, 2000, and March 26, 2001). Both these studies, however, did not offer data that I could manipulate to test my hypotheses. Finally, several market research companies have their own data, but they are mostly reserved for their clients.

⁴ Such an act, in fact, would indicate that the user has something that he/she does not want others to know. In several countries this could be at least highly suspicious, if not outright forbidden.

newsgroups, or e-mail information or data considered illegal by the users' law enforcement authorities. Measuring the effectiveness and efficiency of these measures, however, are beyond the scope of this dissertation. My data can provide clues on how firm the attempts at controlling the Net are by states, not the actual results. For all practical purposes, to evaluate the success of Internet control by governments, other indicators would be needed. Furthermore, the findings in this respect would not help to answer my research question.

Originally, I thought a reliable cross-national indicator of LOC would be the number of laws (from national to local) referring to or regulating the Internet. This choice, however, was soon discarded, given the difficulty in collecting sufficient and trustworthy information on such pieces of national legislation. Moreover, several governments have claimed that the Internet does not need special legislation any more than other media. The numbers and typologies of "laws" (e.g. national and local acts, government's decrees, administrative regulations, etc.), however, is a reliable measure of how active a state is (not successful though) about a certain issue.

I have opted for the following proxies to represent the LOC. The first two (namely, the Cryptography and the Privacy Indexes) have indeed been estimated on the numbers and typologies of "laws" related to the free use of encryption software and of privacy protection: (1) the conditions/attitudes for the **free use of cryptography in private communication** (Y1). As Denning (1997, p.172) has noted, "encryption can protect communications and stored information from unauthorized access and disclosure". Denning also warns that "the widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception (wire-taps) and documents from lawful search and seizure".

In the United States, for instance, government agencies such as the FBI and the National Security Agency (NSA) consider exporting some of the strong key encryption software as a possible "threat to their national security". They are pressuring Congress to enact more restrictive legislation on the use and sale of cryptography software, while civil liberties NGOs, users' groups and the private sector oppose such restrictions. Actually, governments that praise freedom of speech should not be worried if Internet users on their territory exchange communication in clear or encrypted. In the data set, this indicator is called **crypto**.

(2) the **degree of protection of privacy and personal data** (Y2). Indeed, privacy is a fundamental right recognized in all major international treaties on human rights, and is

constitutionally guaranteed in many countries. All the most important international organizations, namely the U.N. General Assembly (Guidelines concerning computerized personal data files, adopted on December 14, 1990), the OECD (Guidelines on the protection of privacy and transborder data flows), and the EU (Directive 95/46 EC of October 24, 1995) have stressed the significance of protecting privacy and personal data.

Despite these legal safeguards, privacy is frequently violated by governments (and businesses) which, routinely, cross-reference data from different sources. Given the substantial trail of information that the average Net user leaves behind, it is fundamental that individuals' right to privacy is utterly protected in on-line countries to prevent governmental and ISP abuses. Clearly, privacy laws protect personal information "at large"; that is, they include communications but also information collected through databases or other media. In this respect, privacy laws do "capture" more than just the Internet. In the end, such circumstances can make using this indicator for my dependent variable problematic. The degree of privacy protection is designated as **privacy** in the data-set.

(3) finally, one of the few available indicators to estimate the size of Internet diffusion and the approximate amount of users is the **number of IP hosts**.⁵ (i.e. the Internet number behind the www.iue.it) (Y3). The type of Internet access can vary considerably from country to country, from simple e-mail to the full World Wide Web. The counting of IP hosts can nonetheless give a reasonably estimate of the number of computers connected to the Internet in a given country. An attempt to cover this aspect of my DV should thus be made, even if it does not produce a successful outcome.

As a general criterion, great numbers of IP hosts in a country could indicate that Internet users should not be monitored by their governments, and that access is relatively open to individuals. It is crucial to bear in mind that such a criterion is susceptible to many exceptions. Nonetheless, it could still be a reliable proxy for the level of control over the Net at the national level, once it is controlled for variables such as income distribution, education and telecom infrastructures. The proxy for the level of IP hosts is named **iphosts**.

3.2.3 Control Variables

Control variables are at all effects independent variables which are used to standardize data from diverse observations. That is, to guarantee that the different values of

⁵ Hosts are computers that allow users to access the Internet. They all have a "32-bit network address that uniquely locates a host or a network within its internetwork" (Loshin, 1997:400).

the dependent variables are the factual consequences of changes in the independent variables and not undesired effects due the analytic incomparability of available observations, a certain degree of homogeneity across units is necessary. Usually, large-*n* studies may not require the unit homogeneity assumption if they are based on random selection. The sample used in this study, however, was assembled through judgmental and not random selection (Black and Champion, 1976:304/307).⁶ Thus, as King et al (1994:95) recommend, I “...resort to some version of the unity homogeneity assumption in order to make valid causal inference”.

As the subjects of this study are countries and their governments which differ considerably in size, wealth, and infrastructures, the need for standardization is simply more compelling. Weighted comparisons (i.e. balancing the structural variances across countries) are valuable in this respect, and control variables are used to this end. In this study, I have selected three control variables, namely, average national income, the national level of education and the conditions of infrastructures necessary to access the Net:

(1) **National income (C1)** is often chosen as a control variable. Differences in per capita wealth across countries can be a powerful constraint to the desire of an individual to access and use the Net. In many countries, personal computers, modems and telephone lines are beyond the reach of the majority of the population simply because they are too expensive. To exclude the possibility that the scarce use of the Internet is only due to poverty and not to government restrictions, controlling for personal income becomes essential. In the data-set this variable is called **income**.

(2) **The level of education (C2)** is another common control variable. Indeed, despite their presumed “user-friendliness”, computers and networks still require an above average level of education which is merely unrealistic to expect from a large portion of the population in several countries. As in the previous case, weighting the impact of the level of education across units is also indispensable. The variable for the level of education is labeled **educ**.

(3) My last control variable is the **size of telecom and computer infrastructures (C3)**. This may be considered a more controversial controlling criterion. The indicator in the data set is

⁶ A judgmental (or purposive) sampling is one where the researcher picks up the observations (i.e. the investigator exercise his/her judgment). There are advantages in this non-random sampling (less costly, more accessible to the researcher etc.), as well as disadvantages. The most critical one is that inferential statistics are based on randomness (i.e. each case in the population has a known probability of being selected into the sample). Zeller and Carmines (1978), and Trochim (1999) call this technique “haphazard sampling”. In this specific case, I have simply included all the available observations, being aware of the limits of this type of selection.

named *mulmedia* and its values are the results of aggregating into a single number the percentage of telephone lines and personal computers per 100 people in the sampled countries. *Educ* and *Income* alone could not capture the technological disposition that some countries have while others lack. Even in industrialized countries, the spread of computer and telecom technology—particularly among non-business, private users—is far from uniform.⁷ Hence the different stages of penetration of these technologies had to be considered to attest that limited use of the Internet is the result of government action rather than of discontinued diffusion of personal computers and telecommunication lines.

3.2.4 *The Step-by-Step Procedure and Problems*

The technique I have used in this chapter is a cross-sectional analysis of a database containing 65 observations (countries). Data have been collected (depending on availability) from various years, from 1995 to 1999. Each observation has one data point for each variable (IV, DV and CV). Details (sources, dates, significance of the indicators, etc.) about the data are presented in the next section (3.2.5, Data Sources). The whole *codebook* is included in the Appendix, before the Summary Table, containing all the figures for all the variables (notes to the Summary Table are reported at the end, after the table).

Bivariate Correlations

Correlation coefficients are the most immediate signs of a relationship between two variables, because they indicate that the two phenomena vary together. Indeed, when operating with several variables and indicators, calculating the correlation coefficients is an essential operation because it helps the researcher to separate the data that are significantly linked together from those that are weakly connected. I have used correlation coefficients in the early phases of my research to stress the most immediate links among all the variables. The regression results are reported in section 3.3.

Partial Correlations

Correlation coefficients are mostly helpful in research where the units of observation are structurally similar (e.g. individuals) or when the effects are clearly the consequence of a single cause. Indeed, the complexity of social reality manifests itself in a variety of ways, and most social phenomena are affected by a multiplicity of factors. Hence, social

⁷ The same case applies rather often to business users.

researchers must try to disentangle these factors so that they can be evaluated as to their relative and separate importance. In correlation and regression this is accomplished by using partial correlation coefficient (Zeller and Carmines 1978:155).

In the more advanced phases of this work I have favored partial correlation coefficients, since they yield a single measure summarizing the degree of relationship between two variables, controlling for a third (Blalock 1960:332), and facilitating, at the same time, the comparison across dissimilar countries.

Multiple Regressions

The overall limit of correlation or partial correlation coefficients is that they are *non-directional*, i.e. once calculated they do not indicate which of the hypothesized variables influence the other(s) (Lewis-Beck, 1995). Indeed, correlation coefficients simply denote that two or more variables covariate together. However, it would be arduous to argue that there is a causal relationship between the two variables because the percentages of cars and telephones vary across countries.

To complete the search for causal explanations of my hypotheses, the calculation of regression coefficients has been the necessary and conclusive step. As it appeared evident from the first runs of computation, simple regression operations had to be discarded in favor of *multiple regression*. Indeed, identifying the causes of government control over the Internet has required a more complex and articulated model than what could be suggested by the early working hypotheses.

Selecting which results to present in a chapter is a painstaking process. As Achen (1982:67/68) has observed, "...the selection of a suitable regression to summarize a data-set is an art not a science" and "...any choice among competing regressions is to some extents arbitrary". Thus, only a selection of regression coefficients is presented in section 3.3, and it is inevitably discretionary. The full data set is included in the Appendix.

3.2.5 The Sample and Data-related Problems

Empirical observations in the real world, whether of human behavior or social events, however, are rather messy and confused, as the objects of study are often entangled in a "noisy" cloud of contradictory signals and discordant results. Moreover, lack or inaccessibility of reliable data, coding errors, various biases, and plain misinformation by unchecked sources are the recurrent anxieties that accompany quantitative researchers—and

to large extent also the qualitative ones—in all their undertakings, and my work offers no exception. This section is intended to pinpoint the principal problems I have encountered during the investigation. The Listwise Deletion of Missing Data option of SPSS was selected as default option during calculations, thus excluding a higher number of observations with missing values from the computation.

Overall, samples can be of two types, probabilistic and non-probabilistic. The main distinction is that in the former “[e]ach element has a known, non-zero chance of being included in the sample. Consequently, selection biases are avoided, and statistical theory can be used to derive properties of the survey estimators” (Kalton 1983:7). Hence this method should be the preferred one when possible. Again, especially when working with countries, this practice is not always possible: more data are available on some countries than on others. Moreover, countries as units are so intrinsically different that the researcher must intervene in the sampling procedure in order to guarantee that all these differences are represented. The cost of such an intervention is greater subjectivity which, in turn, requires greater care and attention in the generalization process. Nonetheless, I had no choice but to revert to non-probability sampling (Kalton 1983), and more precisely to haphazard (Zeller and Carmines, 1978, Trochim, 1999), or judgmental (Black and Champion, 1976) sampling, which selects observations based on availability, as all the relevant data I could find are now in the sample.

The second problem to be addressed was that, given the newness of this field of research, I had to elaborate an operational definition of the level of control (LOC) over the Internet. I have defined the LOC as composed of (a) censorship on contents and (b) limits to access to the Net, hence I should use two or more indicators. I have selected as trustworthy proxies for the LOC information national legislation on (1) the use of cryptography, (2) the protection of privacy and (3) the number of IP hosts (for details on sources, see the Appendix).

Originally, I intended to combine these three indicators into a single scale that could allow me to measure different LOCs. To test the viability of this option, i.e. to corroborate the assumption that they do measure the same phenomenon, I have correlated the three indicators and compared their coefficients. The results for the Pearson's r test are the following in table n.1:

Correlations

| | | Cryptography Score 1998 | Privacy Score | Number of IP Hosts per 10.000 people |
|---|---------------------|----------------------------|---------------|---|
| Cryptography Score 1998 | Pearson Correlation | 1.000 | .410** | .204 |
| | Sig. (2-tailed) | . | .005 | .113 |
| | N | 62 | 46 | 62 |
| Privacy Score | Pearson Correlation | .410** | 1.000 | .329* |
| | Sig. (2-tailed) | .005 | . | .022 |
| | N | 46 | 48 | 48 |
| Number of IP Hosts per 10.000 people | Pearson Correlation | .204 | .329* | 1.000 |
| | Sig. (2-tailed) | .113 | .022 | . |
| | N | 62 | 48 | 65 |

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

Table 1

The results show that the relationship among the indicators was more complex than anticipated, and they cannot be unified into a single measure for the LOC because to do so would require higher coefficients. I have considered various possible alternative explanations of why the three indicators are only halfway correlated; after all, they do represent three of the most crucial and much discussed features of the Internet.

An articulated explanation of why the relationships among the indicators appear to be rather mild is now necessary. First of all, privacy is a fundamental issue in the struggle for control over the Net, but the Privacy Index was based on the 1998 Global Internet Liberties Campaign survey which encompassed all the aspects of privacy and personal data protection. Thus the index represents the overall conditions of privacy in the observed countries. Privacy protection is equally as important for the Internet as it is for the use of personal information in other media or for the treatment of individuals' health data in hospitals or in the public administration. It is then difficult to pinpoint within the privacy realm how much change is due to government control over the Internet and how much to other contingencies. A noteworthy result, albeit not enough to consent the merge of the two indicators, is the reasonable correlation between *Privacy* and *Crypto*. Such an outcome confirms that a relationship exists between the two. Of the two, however, I have selected *Crypto* as an indicator for the DV, since it captures less "background noise" than *Privacy*, as explained above.⁸

⁸ I have also correlated *Privacy* and *Crypto*, controlling for income (C1), level of education (C2), multimedia level (C3), defense expenditures (X1) and democracy level (X3), so as to ensure that all the relationship

The utilization of cryptography in personal communications, in fact, does have repercussions in terms of protection of privacy. Unlike the Privacy Index, however, the Cryptography Index (also based on a GILC survey) may portray the conditions of Internet control more precisely. Indeed, before the diffusion of the Internet, outside military and intelligence circles, the use of cryptography to protect personal communications was an occurrence totally unheard of; people would make phone calls or write letters knowing that the chances of their communications being read were almost nil. Many Netizens today know that reading e-mail or collecting personal information on the Net is possible for any knowledgeable user—let alone national secret services.

It is hence correct to conclude that the status of cryptography in the sampled countries can provide the researcher with a specific and more accurate indicator to measure the level of Internet control than the *Privacy* or *IPHosts* indexes. Actually, the state of *IPHosts* seems to depend more on the level of technical proficiency and economic development of the single countries in the sample than on any other factors considered here. But this case can be set momentarily aside and will be discussed in details along with the other results presented in section 3.3 (Test Results).

The last problem to tackle was the dissimilarity of data to be compared, as some variables are ordinal whereas others are continuous. Even if the tables and print-out indicate only numbers, in reality some of those numbers represent categories, such as the conditions of legislation on cryptography or the arbitrary scoring of privacy protection (see the appendix for details). To overcome this difficulty, I have operated in two phases: first, all the indicators have been considered as continuous and correlated through Pearson's r ; second, the ordinal variables have been compared through γ and τ - c non-parametric tests.

However, this solution is not without consequences: different measures of association produce rather different coefficients. Blalock's scale of test reliability (1972:424), i.e. $\gamma > \tau$ - $b > \tau$ - a , is not always applicable, particularly to matrix tables that are not squared as in many cases in my research.⁹ For instance, a cross-table for the comparison of the democracy/cryptography variables would match three classes for X to

between the two indicators for the DV was only due to the common influence of C1, C2 and C3. The correlation coefficient, although not high (.274), it highlights that, to some extent, *Privacy* and *Crypto* also pick up other influences.

⁹ In some cases, "squaring" matrices should be possible (i.e. reducing or increasing the number of classes), but this is not applicable as a general solution.

five for Y, clearly incompatible with the square rule. Ultimately, despite further analysis and discussion on the most correct procedure, the outcomes of non-parametric tests were so poor and insignificant that I had to abandon this alternative altogether.¹⁰

Data Sources

Data sources are treated here only for summarizing purposes since the complete details are reported in the notes of the Summary Table at the end. Almost the entire set of data used for the quantitative analysis has been found on and downloaded from the Internet, particularly the World Wide Web. The URLs (Uniform Resources Locators) are reported here and in the Appendix:

1. **Hypothesis 1 (X1): *defense*.** X1 is represented by the percentage of GDP in USD devoted to defense expenditures by each countries, (SIPRI 1998).¹¹ Higher percentage means greater military expenditures, and thus higher propensity toward national security.
2. **Hypothesis 2 (X2): *individ*.** X2 is operationalized via the Individualism Index created by Hofstede (1984:158 and 1991). Higher scores mean a higher level of individualism.
3. **Hypothesis 3 (X3): *democry*.** X3 is indexed by the Democracy Scores (0-10)¹² of the Polity III database by Ted Gurr, downloaded by the ICPSR Web site.¹³ The higher marks, the more democratic the country.
4. **Hypothesis 4 (X4): *telecomp*.** X4 is the level of privatization/liberalization in the telecommunications and broadcasting sectors, (ITU World Telecommunication Development Report 1995, and 1997). The higher the numbers, the more liberalized the telecom sector is.
5. **Hypothesis 5 (X5): *tradepro* and *econfree*.** X5 was tested with two indicators: the former is the countries' trade % of PPP GDP (Table 6.1, World Bank Development Indicators 1998); the higher the percentage, the greater the trade propensity.¹⁴ The latter

¹⁰ I must admit that using ordinal variables in regression analysis is not consistent with traditional regression assumptions (Lewis-Beck, 1980 and 1995), which requires that all variables are continuous. However, as I mentioned in the text, non-parametric test yielded such poor results that they could not give me any reliable indications or directions for my research. As other authors in the same situation have reverted to regression techniques (e.g. Kedzie, 1996), I feel comfortable using the same techniques in my work.

¹¹ Hofstede used two surveys conducted among the employees of a large multinational (IBM) in subsidiaries in 40 countries in the early 1970s. Unfortunately Hofstede's Individualism Index has been the only such study (i.e. portraying perceptions of individualism) in a large number of countries.

¹² 0=no democracy at all, 10=maximum level of democracy. An Autocracy Score was also available but not used here.

¹³ <ftp://isere.colorado.edu/pub/datasets/polity3/politymay96.data> (v. various days, November and December 1998).

¹⁴ <http://www.worldbank.org/> (v. various days, November, and December 1998, and January 1999).

- is the Index of Economic Freedom, by the Heritage Foundation/The Wall Street Journal (1998), and again the higher the score, the greater the economic freedom of the country considered.¹⁵
6. The **first indicator** for my dependent variable (Y1) is *crypto*. Y1 is given by national legal conditions to use encryption software for private communications. The first survey was conducted by the Global Internet Liberties Campaign (GILC/EPIC,1998).¹⁶
 7. The **second indicator** (Y2): *privacy*. Y2 is the level of legal protection that personal privacy is granted in diverse countries. This survey as well has been conducted by GILC/EPIC (GILC/EPIC, 1998), and higher numbers mean a greater degree of protection for personal privacy¹⁷
 8. The **third indicator** (Y3): *iphosts*. Y3 is the ratio between the number of Internet hosts (IP-Hosts) and the population of a given country (Table 5.11, World Development Indicators, World Bank, 1998). The higher figures indicate large numbers of IP host computers, and hence easier access to the Net, and few or no obstacles to set up a host.
 9. The **first control variable** (C1): *income*. C1 is represented by the 1997 GNP per capita in PPP by the World Development Indicators (World Bank, 1998).
 10. The **second control variable** (C2): *educ*. C2 is the level of education as % of the relevant population enrolled in secondary school (Table 2.10 of the World Development Indicators, World Bank, 1998). The higher the number, the more educated (more school-years) the population.
 11. The **third control variable** (C3): *multimedia*. C3 is the 1995 index of access to multimedia (as calculated in Table 2 of the World Telecommunication Development Report, (International Telecommunication Union, 1995:4). The greater the score, the more “wired” the country is.

¹⁵ The survey on economic freedom has been performed by the Heritage Foundation since 1995. I have used the 1998 figures. The data from the years are available on line at <http://www.heritage.org/index/> (v. various times, in September, October and November 1998, and April 1, 2001). I have reversed the order of the scores (in the original, the lower the score, the greater the freedom).

¹⁶ The survey ranked countries from *green* (value 5 in my database, most free and uncontrolled) to *red* (1, most restricted and controlled). <http://www.gilc.org/crypto/cryptosurvey.html> (v. various days, October, November, December 1998 and January 1999). The GILC is a transnational, umbrella organization that includes several pro-liberties NGOs. The survey was actually organized and run by the civil liberties NGO, EPIC in 1998, on behalf of GILC. In 1999 and 2000, EPIC conducted two more surveys, but this time under its own name.

¹⁷ <http://www.gilc.org/privacy/survey.html> (v. various days, October, November, December 1998) and <http://www.privacyexchange.org/iss/surveys/codesum.html> sample of countries (v. various days, October and November 1998).

3.3 Test Results

Measuring social phenomena is a difficult and not always successful undertaking, particularly when studying issues such as the level of control over the Internet. Yet, the pitfalls and complexity of the subject at hand also make more challenging research. From exploratory studies such as this, other scholars may produce more accurate research, and perhaps more accurate indicators to measure LOC could be devised.

I am fully aware that the existence of national laws limiting the use of cryptography on-line or restraining access to the Internet does not immediately translate into highly efficient on-line control. It does mean, however, that states are concerned about the possible consequences of open access to the Net in their territories. Actually, many national authorities think that "all that is not specifically permitted, is forbidden" with regard to the freedom of choice of their constituencies, and thus may want to prevent possible effects of unrestricted access to the Internet by massively regulating various on-line issues, ultimately hoping that they will be able to enforce those rules and persecute law-breakers. Therefore, the results of the cross-national matrix should, at least, yield a crude trace about attitudes of countries regarding the control of the Internet.

After collecting and coding the data, and preparing the sample, I have compared correlation and regression coefficients. As a consequence, on the basis of negative test results, some indicators have been definitively abandoned as extraneous or irrelevant. As indicated by Sarin and Stronkhorst (1984), the working hypotheses have been revised and corrected to yield a more solid model (presented below) for the explanation of national differences in controlling the Internet.

Whereas negative results can reject hypotheses, positive results are more ambiguous to interpret, and causality is more difficult to infer without recurring to more advanced statistical methods or in-depth qualitative investigation. The model resulting from the quantitative investigation will be further tested through the qualitative analysis of three case studies selected out of the countries in the sample..

To conclude this section, a few words on significance testing are necessary. Needless to say, using different measures of associations increases the complexity of implementing this testing. For instance, ordinal measures such as *tau* do not assume bivariate normal population, which is the case for Pearson's *r*. As the overall goal of using quantitative techniques in this research was that of identifying a viable model to explain government behaviors with regard to controlling the Net, in the end, I have decided to elect Adjusted R

square coefficients as the discriminating factor for designing the model that will guide the qualitative analysis.

Achen (1982:44) has observed that "...how large an effect must be before it matters is not a statistical question". As already mentioned, the testing and checking of alternative explanations for my research questions is made possible by the inclusion of tables in the appendix, including all the correlation coefficients. Here, the partial correlation coefficients are reported in table 2:

Partial Correlation Coefficients for Independent and Dependent Variables¹⁸

| | DEFENSE | INDIVID | DEMOCRACY | TELECOM | TRADEPRO | ECONFREE |
|---------|-------------------|-----------------|------------------|------------------|-----------------|-------------------|
| Crypto | -.577** (.001) | .059 (.753) | .046 (.808) | .471** (.009) | -.006 (.971) | -.245 (.191) |
| Privacy | -.196 (.299) | -.011 (.951) | .429** (.018) | .142 (.454) | -.050 (.752) | -.428** (.018) |
| IPHosts | -.147 (.437) | .217 (.249) | -.066 (.729) | .207 (.272) | -.045 (.804) | .015 (.934) |

Table 2 (N>30; ** = 0.01 2-tailed significance; in parentheses the probability)

Given the reciprocal influence that these factors exercise on one another—which is, incidentally, also the “core business” of most social sciences—as it should be expected, indications of degrees of relationship are visible for most of the indicators. The most conspicuous results are the negative correlation coefficients of *Defense* and *Crypto*, *Econfree* and *Privacy*, and the positive ones between *Telecomp* and *Crypto*, and *Democracy* and *Privacy*. As preliminary assessments, higher levels of defense expenditure correspond to lower scores in the free use of cryptography, i.e. the individual use of encryption software is more restricted, and vice versa, higher levels of competition in telecommunications coincide with the freer utilization of cryptography. Moreover, higher democracy levels correspond to greater protection for and care of people’s privacy, while the reverse is true for higher scores of economic freedom. These results have determined the subsequent runs of multivariate regressions whose outcomes are summarized in Table 3.

The low coefficients for *IPHosts* led me to the first important conclusion of my quantitative analysis, i.e. a low number of host computers in a given country is *not* related to government attempts to limit or discourage access to the Internet in that country. Indeed, in developing the *IPHosts* indicator, I assumed that low numbers of host computers could be

the artificial consequence of national authorities trying to control the Net by imposing harsh licensing procedures and high costs to would-be ISPs. Few and expensive ISPs would then dishearten many would-be users, and perhaps limit access to favored elites who may be more loyal to and supportive of the national government.

This assumption had to be rejected. Moreover, in the ensuing rounds of multiple regressions, the most significant t-statistics have consistently corresponded to the *Mulmedia* indicator. This has led me to conclude that the number of IP hosts is mainly a function of the level of *Mulmedia*¹⁹ that is determined by the conditions of the technical infrastructures in a country. Those technical infrastructures are, in turn, a consequence of overall national economic conditions. Finally, one indicators for H5 (*Econfree*) has substantial *negative* correlation coefficients with *Privacy*. This negative correlation between *Econfree* and *Privacy* is significant: several nations with the highest *Econfree* score, also had low *Privacy* marks.²⁰ These circumstances can be explained by the fact that privacy protection is not considered relevant and/or indispensable for successful private business.

These data mostly depict the situation in the off-line world of business and commerce, since specific data on e-business are still in short supply. However, businesses on the Internet will have to offer better protection for customers' personal data as a value-added service, since more and more users in Europe and the United States (still the most numerous on-line customers) have been demanding privacy more and more. Investigating this conclusion is beyond the scope of this dissertation—and, most likely, the data I have used are far from appropriate to clarify such relationships. Nonetheless, these figures point toward another worthwhile area of research.

3.3.1 Multivariate Regression Results

The next three tables (n.3,4,5) display the results for the three models. Model 1 tests the DV *Crypto*, model 2 *Privacy* and model 3 *Iphosts*.²¹ All the models presented here have

¹⁸ Controlling for education level (Educ), national income (Income), and telephone and computer infrastructures (Multimedia).

¹⁹ Number of telephone lines and computers per 100 people in the observed countries.

²⁰ For instance, countries such as Mexico, Malaysia or Singapore (most open economies are Asian countries that have not scored high on privacy) .have great trade propensity and often greater openness then European counties, but their privacy protection records were far from satisfactory.

²¹ The numbers in the tables indicate (a) the beta coefficients, (b) the standard error (in parenthesis), at the bottom there are (c) the R-squared and the number of cases. The three control variables (income, education and multimedia) appear in every column (while the independent variables do not) because they are included in every regression.

been controlled for national income (*Income*), education level (*Educ*), and telephone and computer infrastructures (*Mulmedia*). The most important results are summarized after each tables, and commented on further ahead in this section.

Model 1: DV Crypto

| INDEPENDENT VARIABLES | | | | | |
|-----------------------|----------------------|--------------------|--------------------|------------------------|---------------------|
| Defense | -.454** (.100) | | | | |
| Individ | | 1.51E-03 (.013) | | | |
| Democry | | | .138 (.079) | | |
| Telcomp | | | | 1.180** (.375) | |
| Econfree | | | | | .577 (.506) |
| Income | -1.2E-04** (.000) | -9.6E-05 (.000) | -8.1E-05 (.000) | -1.360E-02** (.000) | -1.4E-04* (.000) |
| Educ | -6.3E-04** (.008) | 1.66E-02 (.011) | 5.28E-03 (.009) | -4.941E-04** (.008) | 7.54E-03 (.009) |
| Mulmedia | 4.03E-02** (.015) | 1.87E-02 (.021) | 1.93E-02 (.018) | 3.280E-02** (.016) | 2.95E-02 (.018) |
| R ² | .413 | .210 | .182 | .289 | .155 |
| N. of cases | 47 | 35 | 48 | 49 | 49 |

Table 3 (N>30, **=0.01, 2-tailed significance, *=0.05, 2-tailed significance)

Defense and *Telecom* and their opposite signs are the most substantial results. *Income*, *Educ* and *Mulmedia* are obviously noteworthy (for *Defense* and *Telcomp*), since the presence of multimedia appliances, the necessary income to afford them, and the technical proficiency to use them justify the diffusion of encryption software.

Model 2: DV Privacy

| INDEPENDENT VARIABLES | | | | | |
|-----------------------|-----------------|----------------------|------------------|--|--|
| Defense | -.180 (.129) | | | | |
| Individ | | -3.942E-03 (.013) | | | |
| Democry | | | .320** (.104) | | |

| | | | | | |
|----------------|-----------------------|-----------------------|----------------------|----------------------|----------------------|
| Telcomp | | | | .560 (.425) | |
| Econfree | | | | | -278 (.516) |
| Income | -2.797E-05 (.000) | -2.204E-05 (.000) | 1.19E-05 (.000) | -3.8E-05 (.000) | -5.7E-06 (.000) |
| Educ | 3.271E-02** (.010) | 3.667E-02** (.011) | 2.58E-02** (.010) | 2.91E-02** (.011) | 3.46E-02** (.010) |
| Mulmedia | 1.808E-02 (.017) | 1.578E-02 (.021) | 3.16E-03 (.016) | 1.69E-02 (.017) | 1.44E-02 (.017) |
| R ² | .502 | .539 | .579 | .496 | .478 |
| N. of cases | 43 | 35 | 43 | 44 | 44 |

Table 4 (N>30, **=0.01, 2-tailed significance, *=0.05, 2-tailed significance)

In Tab.4, the notable outcomes are the correlation of *Democry* (and *Educ*) with privacy (the relevance of cultural factors is evident here), whereas *Mulmedia* and *Income* have little impact.

Model 3a: DV Iphosts

| | | | | | |
|-----------------------|--------------------|--------------------|--------------------|--------------------|--------------------|
| INDEPENDENT VARIABLES | | | | | |
| Defense | -5.566 (8.431) | | | | |
| Individ | | 1.217 (1.022) | | | |
| Democry | | | -2.307 (5.582) | | |
| Telcomp | | | | 46.901 (26.714) | |
| Econfree | | | | | 5.891 (34.227) |
| Income | -4.8E-03 (.004) | -9.2E-03 (.006) | -4.8E-03 (.004) | -6.4E-03 (.004) | -5.5E-03 (.005) |
| Educ | -.450 (.659) | -.703 (.876) | -.334 (.651) | -.552 (629) | -.239 (.631) |
| Mulmedia | 4.471** (1.240) | 4.900** (1.644) | 4.494** (1.263) | 4.471** (1.176) | 4.410** (1.221) |
| R ² | .549 | .540 | .550 | .571 | .543 |
| N. of cases | 49 | 37 | 50 | 51 | 51 |

Table 5 (N>30, **=0.01, 2-tailed significance, *=0.05, 2-tailed significance)

As explained earlier, due to the great impact that e-business is expected to have on the whole of the Net, in addition to *Econfree*, H5 (economic openness/trade freedom) was

also tested with another indicator, *Tradefree* to measure the propensity to free trade. The results are reported in the table n. 6 below.

Model 3b: all DVs

| | CRYPTO | PRIVACY | IPHOSTS |
|----------------|---------------------|----------------------|--------------------|
| Tradefree | 3.33E-04 (.004) | -1.3E-03 (.004) | -.240 (.278) |
| Income | -1.3E-04* (.000) | -1.2E-05 (.000) | -3.3E-03 (.004) |
| Educ | 3.28E-03 (.010) | 3.49E-02** (.011) | -.284 (.696) |
| Mulmedia | 3.69E-02 (.019) | 1.35E-02 (.019) | 4.154** (1.290) |
| R ² | .139 | .466 | .552 |
| N. of cases | 48 | 43 | 50 |

Table 6 (N>30, **=0.01, 2-tailed significance, *=0.05, 2-tailed significance)

Just like *Econfree*, this indicator for H5 failed to produce significant results, and thus I had to discard it. Indeed, from the point of view of liberalism, one would expect less statutory control on the Net, the more open (domestically and internationally) an economy is, and these proxies measured the trade propensity and openness of economies. The regression results of *Econfree* and *Tradepro*, however, were inconclusive as regards my research question. The most likely explanation of such circumstances is that, much like in the case of the DV indicator *Privacy*, *Econfree* and *Tradepro* encapsulate considerable “background noise”, which have nothing or little to do with the Internet and e-business.

Overall, it seems that the degree of liberalization/state intervention in the telecom sector (the IV for H4, conveyed by *Telcomp*) captures more closely the effects, actual or perceived, of the Net on a country’s economy. Actually, in section two, commenting about the correlation coefficients of the dependent variable indicators, I concluded that at least two of them, *Privacy* and *IPHosts*, may flag some effects of government control on the Internet. However, these effects are “disturbed” by the presence of some macro-factors which influence not only the developments of the Net but also—and more importantly—the whole “social habitat” of many countries.

These conclusions have been confirmed by the multiple regression analysis. In the numerous calculation runs performed with different variables, the t-ratios of *Democracy* (democracy level) and *Educ* (education level) have consistently been the most significant in

explaining changes in the level of privacy protection (*Privacy*). On the other hand, the same variables seem to have only negligible influence in accounting for the number of host computers (*IPHosts*) that are active in the countries observed. Actually, the measures of *IPHosts* seem to be strongly correlated with the multimedia index (Pearson's $r=.724$) and, to a lesser extent, to *Income* ($r=.604$), as reported in Tab. n.7 below. These correlation coefficients are confirmed by t-ratios in multiple regressions.

Correlations

| | | Number of IP Hosts per 10.000 people | Degree of Telecoms Competition | National Average Income in PPP | Multimedia Index | Economic Freedom Positive |
|--------------------------------------|---|--------------------------------------|--------------------------------|--------------------------------|----------------------|---------------------------|
| Number of IP Hosts per 10.000 people | Pearson Correlation Sig. (2-tailed) N | | | | | |
| Degree of Telecoms Competition | Pearson Correlation Sig. (2-tailed) N | .386** .002 63 | | | | |
| National Average Income in PPP | Pearson Correlation Sig. (2-tailed) N | .604** .000 58 | .483** .000 58 | | | |
| Multimedia Index | Pearson Correlation Sig. (2-tailed) N | .724** .000 64 | .426** .001 63 | .894** .000 58 | | |
| Economic Freedom Positive | Pearson Correlation Sig. (2-tailed) N | .468** .000 62 | .370** .003 61 | .791** .000 57 | .697** .000 62 | |

** Correlation is significant at the 0.01 level (2-tailed).

Table 7

The most significant regression coefficients have been those between *Crypto* and *Defense*, *Crypto* and *Telecomp*, and *Privacy* and *Democry*.²² Hence the resulting model can be finally represented as $Y1 = -X1 + X4 + C1 + C2 + C3$.²³ The relationships between *Defense*, *Telecomp* and *Crypto* have been helpful to enhance my working hypotheses, which was the goal of my quantitative analysis, before proceeding with the case-studies. The opposite signs of the two correlations appear to suggest that the two independent variables have competing effects on variations of *Crypto*. The explanation can be straightforward: cryptography is essential for secure telecommunications—the fastest growing industry in the world—particularly on the Net, but, at the same time, extensive reliance on strong encryption software by individual users could put communications among criminals out of the reach of

²² As an additional check, I have also added *Iphosts* as IV to the final model, and run the regression.

The regression coefficient, however, did not seem to further contribute to the explanation.

²³ $Crypto = -Defense + Telecomp + Income + Educ + Mulmedia$. Defense has negative sign.

law enforcement agencies. Hence, various national business communities lobby for freer use (and also export liberalization in the United States) of encryption software, while national security and law enforcement agencies and personnel pressure central governments to restrict individuals' access to that software.

Based on my data-set, four cases can be devised:

1. **Country A** has high sensitivity to national security issues (hence, high defense expenditures) but the telecom sector is not or barely liberalized (the attitude towards regulating is high); no conflict arises as national security prevails and cryptography is restricted/controlled;
2. **Country B** has low defense expenditure but the telecom sector is highly liberalized (regulations are low) and no conflict arises here either as the business logic succeeds and individual use of cryptography is free;
3. **Country C** has low defense expenditure and no or little liberalization in telecoms which are highly regulated, here the conflict is irrelevant as there are no competing exigencies and the free/not free use of cryptography is a non-issue;
4. **Country D** has high defense expenditures and strong liberalization in telecoms. Here, the conflict is mostly active as the opposite pressures of the national security and business communities compete to convince the national government that cryptography should be free or not free. A recent example of this struggle is France, which at the start of this research had very restrictive laws on cryptography (*Crypto* score=2), but has recently relaxed those laws to meet the requests of French entrepreneurs (Alberganti, 1999).

Tab.8 Variable Values for the Selected Cases

| | United States | Germany | Italy |
|----|---------------|---------|-------|
| Y1 | 2 | 5 | 4 |
| Y2 | 2.5 | 7.0 | 6.0 |
| Y3 | 379.39 | 84.46 | 25.76 |
| X1 | 3.6 | 1.7 | 1.6 |
| X2 | 91 | 67 | 76 |
| X3 | 10 | 10 | 10 |
| X4 | 2.81 | 3.00 | 3.00 |
| X5 | 4.10 | 3.70 | 3.50 |

Given these typologies, the countries selected for the qualitative analysis are the United States (D type), Germany (B type), and Italy (B type). Their values for Ys and Xs are presented in the table above. Both Germany and Italy are peculiar B type countries, because some valuable characteristic of my DV have not clearly emerged in the quantitative analysis, thus making the qualitative investigation all the more necessary. Germany, for instance, scores high for privacy protection, but, at the same time, its freedom of speech (no measure quantitatively here) is certainly more curbed than in the United States.²⁴ This is an interesting contradiction, which makes it a worthwhile qualitative investigation of the country.

Italy is also a different B type. Italy has had a long history of heavy state intervention in the economy, and has been a late-comer to the Internet and to liberalizing telecommunications. Moreover, having lacked a proper legal framework on the Internet (and social appreciation for the Net) for a long time (until late 1990s), Italy could also present a valuable case for qualitative investigation. Thanks to these circumstances, in fact, law enforcement and the intelligence agency may have jumped into a window of opportunity and extended their preventive controlling power to the Net before it became widely popular, and indispensable for companies.

Finally, the relationship between *Democracy* and *Privacy*, albeit quite intuitive, has also been an important finding. It further underlined the importance of privacy in democracies, an issue which I then analyzed in the investigation of the case studies. In the last part of this chapter, some observations about the most common violations of regression assumptions—in particular the problem of multicollinearity and that of heteroskedasticity—are discussed.

3.3.2 *Multicollinearity*

As Lewis-Beck (1995:62) has suggested, “the independent variables in a non-experimental regression analysis of sample observations are invariably *collinear*...Because collinearity is inevitable, a little is not a problem but a lot can be”.²⁵ The coefficient of multiple determination (R^2) should be .8 or higher to speak of multicollinearity (Lewis-Beck 1980). The test for multicollinearity is done by regressing each independent variable of the

²⁴ In Germany any references or publications denying the Holocaust or supporting nazism are forbidden.

²⁵ Emphasis in the original.

model against all the others (including controlling variables). The goodness of fit measures for multicollinearity are reported in Table 9.

Multicollinearity Test Results

| | DEFENSE | TELECOMP | INCOME | EDUC | MULMEDIA |
|----------------|--------------------|--------------------|------------------------|--------------------|----------------------|
| Defense | | -.129** (.038) | 64.601 (350.279) | -1.246 (2.113) | .999 (1.129) |
| Telecomp | -1.614** (.468) | | 1701.323 (1211.324) | 7.504 (7.408) | .701 (4.021) |
| Income | 1.17E-05 (.000) | 2.47E-05 (.000) | | -1.5E-03 (.001) | 2.76E-03** (.000) |
| Educ | -6.2E-03 (.010) | 2.97E-03 (.003) | -40.320 (23.880) | | .287** (.068) |
| Mulmedia | 1.71E-02 (.019) | 9.62E-04 (.006) | 261.058** (24.267) | .996** (.235) | |
| R ² | .235 | .477 | .860 | .583 | .892 |
| N. of cases | 49 | 49 | 49 | 49 | 49 |

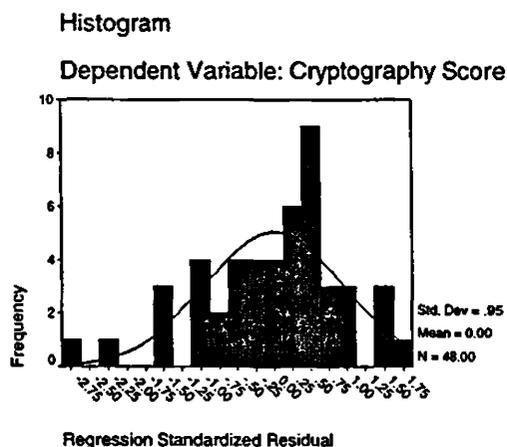
Table 8 (-N>30, **=0.01, 2-tailed significance, *=0.05, 2-tailed significance)

There is certainly some collinearity between *Defense* and *Telecom* according to their coefficients, but it is still safely under the limits. *Income* and *Mulmedia*, on the other hand, have high multicollinearity. These measures suggest that it would be difficult to exclude reciprocal influence effects in all the variables. However, the results of the control variables could be comfortably set aside, as they are not the focus of my research, and both *Telecomp* and *Defense* pass the multicollinearity test.

3.3.3 Heteroskedasticity

The problem of heteroskedasticity arises particularly in cross-sectional data when "...the variability in the residual error terms is not constant for all values of the independent variable" (Schroeder et al. 1986), or, in other words, when measurement errors are systematic and do not cancel each other out. The textbook method for testing for heteroskedasticity is to study the residuals. I have saved the standardized residuals²⁶ as a new variable and plotted them against my explanatory variables. The resulting scatterplots and histograms appear to exclude the case for heteroskedasticity.

²⁶ Residuals are expressed in standard deviation units above or below the mean.



The histogram for *Crypto* shows a good normal distribution for errors, whereas the scatterplot is more or less straightforward, and, somehow, more undetermined. The scatterplots and histograms of *Privacy* and *IPHosts* have been omitted here because, ultimately, only *Crypto* has been used as indicator for the dependent variable.

3.4 Conclusions

In discussing the methods for causal inference based on non-experimental observations, John Stuart Mill, Blalock (1961:14) has noted that those methods could, at best, "...be used only to enable one to eliminate inadequate causal arguments...[as]...there seems to be no systematic ways of knowing whether or not one has located all of the relevant variables". Nonetheless, locating all the relevant variables was precisely the goal when I decided to employ quantitative techniques in this work. Despite a few structural problems, such as the sample size and selection, measurement errors etc., and the inevitable prudence that should always accompany generalizations in the social sciences—regardless of the method used—the quantitative analysis has fulfilled my expectations.

As indicated above, two indicators of my dependent variable, namely *Privacy* and *IPHosts*, do show some effects of variations of levels of control on the Net (LOC), but, at the same, time, they also capture the disturbing reverberations caused by other social phenomena which have little or no relevance for my study. Through all this social "noise", it is rather arduous to establish to what degree the two models that were devised to account for changes in those two indicators can also explain variations in the levels of Internet control. Nonetheless, given the relevant relationship of democracy and privacy that has emerged here, I have kept in mind these two important variables in the investigation for the case

studies. The model correlating the rival effects of telecoms competition and national security with variations in the free use of cryptography for individual communications appears to be the most viable in understanding the causes of Internet control. After all, “if the message gets through with all this noise, it means that there *is* something there, in the real world”²⁷

This chapter has just been the conclusion of the first part of my research. Of the other independent variables not included in the principal model, individualism, democracy, and economic freedom, the former has been entirely discarded. The propensity of a society toward individualism (H2) does not contribute to explaining my research question. The democracy level, in the inquiry for the case studies, has emerged as an essential intervening variable, differentiating the attitude on Internet control of democracies versus autocracies.

The quantitative analysis of economic freedom/trade openness (H5) have failed to produce useful results. In fact, the economic relevance of the Internet seems captured more closely by the liberalization/privatization of the telecom sector. In the case of H5, the proxy and the available data did not work properly. Thus, to explain Internet control, hypothesis H5 appears to be quite irrelevant in that respect. Does this outcome contradict the most important conclusion of the principal model, namely that market forces—specifically represented here by the telecoms sector—compete with national security requirements in the contest for Internet control?

The answer to that question is straightforwardly negative, for the very simple reason that e-business is too new an occurrence in the on-line world (itself a recent invention) to produce viable indicators and data to study its impact on national economies. Statistical offices in industrialized countries are still in the process of evaluating how to measure e-commerce (OECD, 1997), and it will take a few years before the first data sets will be available to scholars.²⁸

Furthermore, preliminary solutions for other problems of the Internet will be necessary before firms and consumers actually embrace the Net as a viable and secure channel to conduct their business. Large use of powerful encryption software and a

²⁷ Thanks to professor Richard Breen for this point.

²⁸ This was personally confirmed during an informal talk by Alessandra Colecchia, (an economist with the Statistical Office of OECD) Milan March 24, 1999. One of the most notable examples of attempts to study e-business and the New Economy, “Measuring the Internet economy” has been conducted in 1999 by the University of Texas, Austin (http://cism.bus.utexas.edu/works/articles/internet_economy.pdf v. various times November, December 1999, January and February 2000, and April 1, 2001).

widespread appreciation for protection of personal data are hence among the necessary prerequisites to fully establish e-business. Other improvements, such as better telecom infrastructures or more extensive utilization of credit cards, are simply consequences of other, much needed social imperatives, such as more solid economic conditions and better education. Some of these effects have been visible in the telecom sector (and highlighted in H4), which has been thoroughly restructured and liberalized in several countries to reap the full economic benefits of the expansion of the sector in the 1990s.

Since the decision about how to answer these questions ultimately rests with the individual scholar, the only proper behavior in these situations is to adhere to one of the “golden rules” of scientific research; that is, to be as open and transparent as possible about the methods used and the findings obtained. The model resulting from my quantitative analysis does adhere to this logic. Despite some indeterminate results, which I have obviously discarded, the model presented here does highlight those factors that help to understand why countries want to control the Internet. The original working hypotheses had to be revised and modified, but that was precisely goal of this part of my research. In the end, the findings and interviews of the second part (the three case studies) have thoroughly confirmed the accuracy of the decisions made in this first part.

PART II - THE QUALITATIVE ANALYSIS: JUSTIFICATION AND CASES SELECTION CRITERIA

II.1 Case Studies Methodology

In this introductory section I intend to outline (a) the justification to undertake the qualitative analysis and (b) the criteria that have led the selection of my cases. Many of the objections to rely only on quantitative analysis have been mentioned both in the previous chapter as well as in the introduction, namely the quality of data, discrete dependent and independent variables etc.. In order to judge among competing hypothesis which one could better explain my research question, applying quantitative methods—albeit imperfect—was a necessity, but it covered only the first part of my investigation. In fact, “...large-*n* methods tell us more about whether hypotheses hold than why they hold. Case studies say more about why they hold” (Van Evera, 1997:55).¹ Hence a selection of case studies from the sample of countries has been indispensable. In section two of this introduction I will explain why all the countries selected are OECD democracies. In section three, I will summarize characteristics of each case.

In a pattern all too familiar to social scientists, making generalizations only on the basis of the outcome of my quantitative analysis would expose my work to serious criticisms. A possible solution to such problem is to use different methods to test the same hypotheses. If those hypotheses are then confirmed, then one may claim that he/she has some basis for the theory. Moreover, as Trochim has observed (1999:157)², “...there is so much value in mixing qualitative research with quantitative. Quantitative research excels at summarizing large amounts of data and reaching generalizations based on statistical projections. Qualitative research excels at ‘telling the story’ from the participant’s viewpoint, providing the rich descriptive detail that sets quantitative results in their human context”.

The literature about case studies is vast, to say the least. Being the preferred method of analysis—and often the only one available—of many social scientists, this circumstance

¹ There is a terminological ambiguity that it is worth clarifying here. Some authors (e.g. Van Evera, 1997) speaks of *case studies* intending specific observations that are to be compared. Others (e.g. King et al., 1994, Eckstein, 1975 and Lijphart, 1971) distinguish between *comparative method* (many observations to compare) and *case study* or one definite event that is examined in its individuality. In this context, I use case studies (as by Van Evera) intending the observations selected to be investigated with comparative methodology.

² <http://trochim.human.cornell.edu/kb/index.htm#Top> (v. October 3, 2000).

is hardly surprising. It is an established method and, if well used, it provides the scholar with a favorable cost/benefit ratio in conducting his/her research. Research resources for a dissertation do not allow for years of extensive investigation, thus the number of selected cases is necessary small, giving way to problems such as too few observations for causal inference.

First and foremost, the cases presented here are coherent with Mill's "method of difference", i.e. all the three countries are democratic, industrialized, technically well-educated, but their political configurations, and economic structures are different. Although all of them have acknowledged their expectations for the New Economy, they have diverse views on how to achieve that goal, as well as dissimilar stories of privatizing their telecom providers, not to mention their attitudes towards military spending (as an indicator of national security).³ For research such as this one, the scholar should also look for Lijphart's theory-confirming cases (1971) or Eckstein's crucial cases (1975). The two categories actually define the same type of cases, as George (1979:66) has indicated. With reference to the Internet, the United States (as explained below) is definitively a crucial case, while Germany's role in Europe makes it another decisive actor.⁴ Italy, as I explain in section three is important in this analysis to investigate the behavior of an Internet late-comer.

Selecting countries for the in-depth analysis can turn out for the investigator to be rather tricky. In this circumstance, the soundest rule would be to adopt randomness, which is the normal procedure in statistics. Given that there are 65 countries in my sample, I could have use that rule. However, as I explained in chapter three, it is a non-probability sample, and thus, its representativeness of the population may be far from perfect. Moreover, also King et al. (1994) admit that with random selection there is the risk of missing important

³ I must admit, however, that the dissimilarities are stronger between the United States and the two European countries, than between Italy and Germany themselves.

⁴ The last reference for choosing the United States, Germany and Italy as my cases, however, is Van Evera's data-rich cases selection (1997). As Van Evera (1997:79) has written, "[d]ata richness can take several forms. Abundant archival data may be available. Participants in the case may be alive and available for interviews". These conditions applied very well to my cases. Data, particularly on-line, in forms of official government documents and reports, in-depth studies by research institutes, and news articles have been abundantly available. Moreover, I could have access to well informed persons in academia, non-governmental organizations, as well as in the public administrations in all three countries. Finally, Eicksten (1975:132) has argued that case studies should not be selected for theoretically trivial reasons such as, among other, the knowledge of the language. While I agree that selection based only on the knowledge of the language or the congeniality with specific cultures would be rather poor criteria, at the same time, all too often the knowledge of a language is not considered among the methodological skills normally required to conduct sound research. If scholars are serious about raising the quality level of most research in the social sciences, then they should start regarding good command of a language as one of the factors that would facilitate the fulfillment of that goal.



cases. In the next section I will present the reasons why all the case studies are industrialized democracies.

II.2 The Countries: Why Are They All Western Democracies?

The focus of my dissertation has been on why national governments around the world, regardless to their geographical location, try to activate statutory control on the Internet. Indeed—despite the difficulties in finding comparable statistical data for my sample for certain countries that have somehow skewed it towards a greater presence of advanced industrialized economies—I have tried to construct a sample with states from different geographical areas. Yet, one may argue, the cases selected for in-depth research are all OECD, Western democracies. What is the rationale of such decision? The answer is twofold: (1) OECD countries produce the bulk of Internet traffic,⁵ (2) all the non-democracies of the world do control the Internet by default.

OECD Countries and Internet Traffic

The most industrialized and technologically advanced countries in the world are all members of the OECD,⁶ and hence, they clearly send and receive the bulk of Internet traffic and are home of the majority of Web sites.⁷ In fact, OECD countries are home to over 35,473,000 of host computers, compared with over 1,265,000 for the rest of the world (OECD, 1999:86). Moreover, in 1998 there were 468 host computers and 311.2 personal computers per 10,000 people in the high income countries (all in the OECD), compared with 3.1 and 15.7 in developing countries.⁸ Furthermore, by April 2000 there were more than 74 000 secure servers in the OECD area representing 95 per cent of the global total. In just one year (from April 1999 to April 2000) the OECD total grew by 95 per cent.⁹ In the same period (April 2000), the US had 193 secure servers per million inhabitants compared to

⁵ See "Top Indicators" at <http://www.worldbank.org/data/databytopic/databytopic.html#INFORMATICS> (v. October 3, 2000).

⁶ All EU countries are members.

⁷ The members are required to share "...the principles of the market economy, pluralist democracy and respect for human rights" (<http://www.oecd.org/about/general/member-countries.htm> v. October 24, 2000).

⁸ This comparison has been made by selecting "INFORMATICS/Top Indicators in the World Bank database and then select "High Income" countries which are, by default, compared with developing countries. See <http://devdata.worldbank.org/external/dgcomp.asp?rmdk=110&smdk=500005&w=0> (v. October 24, 2000).

⁹ <http://www.oecd.org/dsti/sti/it/cm/stats/newindicators.htm#servers> (v. October 24, 2000).

Canada (101), UK (59), Germany (37), France (19), Japan (17), and Italy (12).¹⁰ According to another OECD study, among the 29 members, the United States belongs to the “High Intensity” ICT group, Italy to the “Medium intensity” and Germany, quite interestingly, to the “Low Intensity” (OECD, 2000:30/31).¹¹

Finally, all OECD countries with the exception of Mexico are part of the Wassenaar on the export of dual-use technologies which also include instructions on where, when and with whom to trade in such sensitive sectors as telecommunications, computers and information security—including encryption software.¹² Given these circumstances and for the time being, the choice of the United States, Germany and Italy is quite representative of the “OECD club”.¹³

Non-Democracies and the Internet

Two studies have been considered for this part, namely Reporters Without Frontiers’s (*Rapporteurs Sans Frontiers*, RSF) “The Enemies of the Internet” (1999),¹⁴ and Human Rights Watch’s (HRW) “Freedom of Expression on the Internet” (1998, 1999, and 2000).¹⁵ RSF has noted that “[45] countries restrict their citizens’ access to the internet—usually by forcing them to subscribe to a state-run Internet Service Provider (ISP). Twenty of these countries may be described as real enemies of this new means of communication”.¹⁶ As often mentioned in this dissertation, economic expectations exercise a powerful influence on many governments that, in order not to spoil their chances, have become more careful in imposing control on the Net. Given the Internet impact on economic growth, it is small surprise then, among the 45 countries that restrict their citizens Internet access, that “[t]he economic argument seems to be winning the day in countries such as Malaysia and Singapore...”.¹⁷ Governments there (as well as in the rest of South-East Asia) “...were quick

¹⁰ <http://www.oecd.org/dsti/sti/it/cm/stats/newindicators.htm#servers> (v. October 24, 2000). The OECD also regularly publish guidelines for its members on, among other things, e-commerce, protection of personal data, and cryptography. Although these guidelines are not binding, they are usually followed by OECD members.

¹¹ The report is also available at http://www.oecd.org/dsti/sti/it/prod/measuring_ict.pdf (v. October 24, 2000).

¹² <http://www.wassenaar.org/list/Table%20of%20Contents%20-%2099web.html> (v. October 24, 2000). The Wassenaar is the “heir” of the Cold War CoCom list which included items that could not be traded with the Soviet Bloc. As in the old CoCom, the United States is rather influential in the Wassenaar (and in many instances in the OECD too).

¹³ Needless to say the three countries are also members of the G7/G8.

¹⁴ <http://www.rsf.fr/uk/home.html> (v. August 25, 1999 and July 31, 2000).

¹⁵ <http://www.hrw.org/hrw/advocacy/internet/fe-wr98.htm> (v. August 25, 1999 and July 31, 2000), <http://www.hrw.org/worldreport99/special/internet.html> (v. September 5, 1999 and July 31, 2000), and <http://www.hrw.org/wr2k/Issues-04.htm> (v. July 31, 2000).

¹⁶ <http://www.rsf.fr/uk/home.html> (v. July 31, 2000) (“The Enemies (sic.) of the Internet”).

¹⁷ <http://www.rsf.fr/uk/home.html> (v. July 31, 2000).

to spot the opportunity of the Internet, but also the threat" (*The Economist*, November 14, 1998:8).¹⁸ Within this large group, there are 20 countries that RSF "...regards as enemies of the Internet because they control access totally or partially, have censored Web sites or taken action against users".¹⁹

The Internet real enemies, according to RSF, are thus: Azerbaijan, Belarus, Burma, China, Cuba, Iran, Iraq Kazakhstan, Kirghizia, Libya, North Korea, Saudi Arabia, Sierra Leone, Sudan, Syria, Tajikistan, Tunisia, Turkmenistan and Uzbekistan, and Vietnam. All these countries are known non-democracies, ranging from totalitarian regimes to autocracies.²⁰ Free media and freedom of expression are nonexistent there, and it would be surprisingly that the Internet did not attract the authorities' attention. Actually, HRW has identified several attempts to control various aspects of the Net, from access to ISP responsibility for contents exchanged from democracies and autocracies alike. However, the most severe attempts at controlling the Net come, among others, from states such as China, Saudi Arabia,²¹ Iran, or Vietnam, etc.—once more not surprisingly.²²

Among these most keenest controllers, China is a noteworthy example of a non-democratic government that has embraced the Net for its expected economic returns, struggling, at the same time, to retain a strict control through any means on what Chinese Internet users are allowed to know. As *The Economist* (November 14, 1998:76) has put it, "[a]s much as any nation, China stands to benefit by applying the technology of the Internet to commerce, finance, science, entertainment, and education. More than most, however, it also has reason to fear the Internet's freewheeling ways with uncensored and unapproved news".²³

¹⁸ Possible explanations for increasing easiness in granting widespread access to the Net in Malaysia and Singapore, and the rest of South-East Asia are based on cultural attitudes ("...young and talented workers...listen to their leaders...", *The Economist*, February 5, 2000:72) or on specific corporatist structures, binding together bureaucrats, public and private administrators (Rodan, 1998) that would guarantee those governments that some degree of control on the Net would be tolerated by users.

¹⁹ <http://www.rsf.fr/uk/home.html> (v. July 31, 2000).

²⁰ After the death of Syrian President Hafez al-Assad in August 2000, Syria may change its attitude toward the Internet—at least this is what Bashar al-Assad seems to favor (<http://www.wired.com/news/print/0,1294,35882,00.html> v. October 11, 2000).

²¹ Recently, Saudi Arabia has once again conveyed its intention of controlling Net surfers, and similar behavior is still common in most of the Middle East (<http://www.mercurycenter.com/svtech/news/breaking/merc/docs/056237.htm> v. October 3, 2000).

²² <http://www.hrw.org/wr2k/Issues-04.htm> (v. July 31, 2000), and <http://www.hrw.org/worldreport99/special/internet.html> (v. July 31, 2000).

²³ See also Zambardino (September 11, 1996), Pisu (December 31, 1997), and Poole (December 13, 1998). More precisely, "[a]ccording to China's laws, operators of Internet bars must install a "software manager" which can tell the government who is using the computers and for what purpose. Customers must also show

Given these circumstances, choosing a country like China, Singapore (one of the most wired places), Iran or even Tunisia would simply confirm what (a) is already common knowledge, i.e. that non democratic countries control the Net *by default*, since they do not permit individuals' expression, and (b) has been adeptly already demonstrated by RSF and HRW studies. If one evaluates the "Enemies" on the indicator for my dependent variable—the Cryptography Index—however, it appears that Internet control is not limited to these countries. China, Tunisia, Belarus, Vietnam have all scored "red" (highest restrictions on cryptography), but even some more democratic states have scored "red" or "yellow-red".²⁴ It is thus undoubtedly more valuable for my research as an original contribution to the field to consider and explain why democracies, founded on civil rights and personal liberty, do attempt to control the Internet.

The importance of these countries with regards to the future development of the Internet has been clearly summarized by the HRW Report "Silencing the Net. The Threat to Freedom of Expression On Line" already in 1996.²⁵ In the Report, it was noted that "[a]uthoritarian regimes are attempting to reconcile their eagerness to reap the economic benefits of Internet access with maintaining control over the flow of information inside their borders. *Censorship efforts in the U.S. and Germany lend support to those in China, Singapore and Iran, where censors target not only sexually explicit material and hate speech but also pro-democracy discussion and human rights education*".²⁶

II.3 Some Final Remarks on Sources for the Case Studies

The United States, with its society-dominated structure, is the "national security" case as well as "the only information superpower", so dominant is its position in steering the future structural development of the Net.²⁷ Interest groups have full access to federal and local governments, legislatures and bureaucracy. These organizations are able to reasonably influence policies, at least in the short term. Coalitions are quickly formed on specific issue-

identity cards when using Internet cafes so they can be tracked down if they break the rules" (<http://www.insidechina.com/news.php?id=203567> v. October 3, 2000).

²⁴ For instance, in the first survey in 1998, the United States, France and Israel, all democracies, belonged to that group. In 1999, both the United States and France improved their score (see the table in the Appendix).

²⁵ <http://www.cwrl.utexas.edu/~monitors/1.1/hrw/summary.html> (v. July 31, 2000).

²⁶ <http://www.cwrl.utexas.edu/~monitors/1.1/hrw/summary.html> (v. July 31, 2000), emphasis added.

²⁷ The case with domain names is most telling in this respect. An American company, Network Solution Inc.(NSI), manages the most important generic TLDs, thanks to an informal agreement with the U.S.

areas, but they equally fast change. Independent sources of information abound, and its circulation is unrestricted and highly valued by Americans.

The United States is also *primus inter pares* among democracies and its attitude toward controlling the Internet (e.g. by limiting freedom of speech on-line) is likely to influence the behaviors of other countries, which would have an excellent justification to increase their on-line control. Finally, the degree of dependence of the United States' economy and infrastructures on the Net is unmatched in the world. It is hardly surprising that the United States' has been the first government to consider threats to and on the Internet as threats to the country's national security and own survival. In these respects, the United States is a crucial case to assess the governments' complicated relationship with the Net and its possible future.

The EU Experience. On the other side of the Atlantic, European Union has enthusiastically embraced the Internet mostly for its perceived economic benefits (lower administrative costs, new jobs, e-commerce, etc.), albeit with a different attitude than the United States. The EU Commission has launched several programs related to the Internet and the Information Society. The Commission's main initiative, however, came on December 8, 1999 with the adoption of the Communication "e-Europe – An Information Society for all". Recognizing that "[t]he application of digital technologies has become a vital factor for growth and employment in the 'new economy', mainly driven by the Internet....The initiative aims at accelerating the uptake of digital technologies across Europe and ensuring that all Europeans have the necessary skills to use them".²⁸ Despite admitting that, notwithstanding "...Europe's lead in certain digital technologies, e.g. mobile communications and digital TV, the uptake of the Internet in Europe remains comparatively low...", in endorsing the e-Europe plan, EU member governments have avoided to indicate how they intend to contest America's supremacy on the Net (*The Economist*, April 1, 2000).²⁹ To give an idea of how far is reality from hope in the EU strategy towards implementing the Information Society and the new Economy, one has just to look at the situation of the mainstay of Europe's economy, i.e. small and medium enterprises (SMEs).
EU governments

Department of Commerce (DOC). The informal agreement expired in September 2000, but it is unlikely that, after that, NSI would act in ways that may profoundly upset the DOC.

²⁸ http://europa.eu.int/comm/information_society/eeurope/background/index_en.htm (v. October 23, 2000).

²⁹ By reading the documents, one has the impression that EU governments seem to refrain from acknowledging the situation. However, the EU is the only other major economic actor—the other being Japan—that might seriously compete with the United States about which future the Internet should have.

...have actively attempted to promote innovation by SMEs through funding science parks, technology transfer and regional innovation networks, and by involving technology-based SMEs in R&D”)...[and yet] small firms tend to rank the new technologies below other ‘critical success factors’ in explaining their performance...[and they] do not believe that information is a source of market competitiveness” (Hepworth and Ryan, 2000:76, 82 and 91).

Among the leading European countries, I have discarded Great Britain. British influence on EU core policies often appears to be relative, but Britain has always had a remarkable weight in EU telecoms policy and is now at the forefront of Internet diffusion. Nonetheless, Britain’s pattern towards the New Economy has very strong resemblance with the United States’.³⁰ Hence, the exploration of the British case would have been only marginally innovative. I have also excluded France, which is still struggling to abandon its ill-conceive attempt with Minitel that has delayed Internet penetration in that country.³¹ The other two major EU countries, Germany and Italy, have been included in this study.

Germany is a corporatist model of democracy. Institutional actors (business associations, trade unions, consumers’ organizations, some NGOs etc.) have excellent access to the federal and local governments and legislatures. All these elements are involved in the consensus-building process, which always take considerable time. However, once consensus is reached, it lasts. Thus policies resulting from this process are likely to be maintained for a lengthy period of time. The spreading of information is of high-quality mostly among the institutional actors, but individuals and less-institutionalized groups (such as hackers’ for instance) can benefit from a profusion of independent sources. The Internet issues that mostly concern the German public are freedom of speech (because of racist propaganda) and the protection of privacy.

Germany competes with Britain as the leading Internet country of Europe.³² In fact, the German governments has made the development of Net a strategic goal. Recently, Germany’s federal government, as the United States’, has made more and more information through its Web sites. Newspapers and other media have done the same, thus qualifying Germany as a “data-rich” instance for a research. The most critical factor in choosing Germany is that it would be impossible to envision a European plan for Internet’s future

³⁰ That is, strong support for private businesses but also a higher reliance on designating a higher proportion of Internet issues (such as the export of encryption software or wire-tapping) as “national security” concerns.

³¹ To some extents, France has adopted the same attitude as Britain’s with reference to national security, although the situation is slowly changing and now France is more aligned with the other EU partners.

³² For instance, *Deutsche Telekom*’s ISP is the world second largest and the domain *.de* is the second most common on the Web after *.com*.

without strong involvement of Germany's government and business.³³ These circumstances make Germany Europe's "crucial case".

While the United States and Germany—along with other "typical" Internet countries such as China, and Singapore³⁴—have normally been included in other studies such as Kizza (1998), Italy, on the other hand, is an "underdog" among industrial countries for Internet diffusion. For this reason, thus far, extremely few comparative studies have been conducted of the Italian situation by Italian as well as foreign scholars.

Italy is the "volatile government" model, with a long tradition of intervention in the economy. Because of Italy's political system, the government can hardly enjoy unquestionable confidence from the coalition parties supporting it in Parliament. At periodical intervals, the government's head has to devote time and resources to negotiate with all the majority parties about how to move—a far cry from the mandate that the U.S. President and the German Chancellor can expect from their electorates. Under such conditions, the Italian government is definitively an "unstable" government. Parties dominate politics and access to local and national governments, legislatures and bureaucracy for actors is heavily filtered by middle-men and intermediaries with links to those parties. Policies are the result of exchange of favors and promises among the parties, and thus they are often subject to turnaround and reconsideration.

Last, but not least, Italy is a late-comer to the Net. This occurrence means that, since a proper legal framework has lacked for a long time (it is still being developed), national security/law enforcement agencies could have seized the occasion to consolidate their presence on and control of the Net. Hence, despite being a "low security" state much like Germany, Italy presented a noteworthy variation with respect to Germany which justified its inclusion in this study.

The main sources for this qualitative part were (a) original government documents (or their summaries) from official government Web sites, (b) other on-line reports, statements or position papers, like those used in this section and (c) personal interviews. As

³³ The fact that, for the 2000 elections of the quasi "Internet government"—i.e. the board of directors of the domain name organization ICANN—Germany mustered (a) more registered voters than the U.S. (where the organization is based) or any other European country, and (b) the all top four candidates. Unsurprisingly, one of them became the director for Europe (http://members.icann.org/pubstats_unverified.html and <http://www.election.com/us/icann/region2.html> v. October 24, 2000).

³⁴ China is often quoted on media because of its clear and stated attempts at controlling what its users do on-line, and Singapore because does the same but with a higher success rate, and without (apparently) obstructing the spreading of the Net among its citizens and companies (Rodan, 1998).

I did in the first part of this dissertation, I have entered all the URL (Uniform Resources Locators, i.e. the “address” of Web pages) in footnotes with the dates of my visits. When necessary, I have added further instructions in the footnotes to access the information I have reported in the body of text.

Along with these available data, personal interviews have been the other principal source of information for the qualitative analysis of this dissertation. The interviews were “qualitative research interviews”, which are mostly appropriated when “...a quantitative study has been carried out, and qualitative data are required to validate particular measures or to clarify and illustrate the meaning of the findings” (King, 1994:16). Or as Trochim has written, “[t]he purpose of the interview is to probe the ideas of interviewees about the phenomenon of interest” (1999:163). In fact, if the interview is used as an adjunct to other methods of data collection—the statistical analysis and references in this work—it is a common practice in the social sciences (Black and Champion, 1976:375). The interviews to political figures, government officials and academics—the full list is included in the Appendix—lasted circa an hour each, and I have kept extensive notes on them in file. I opted for unstructured interviews, because “...the interviewer is less prone to impose one or another bias that would slant the course of the conversation and restrict the flow of data” (Black and Champion, 1976:365).³⁵

³⁵ A risk to be aware in using structured qualitative interviews as sources of information is that, when doing theory-testing/theory-confirming dissertation such as this one (Van Evera, 1997:90), the interviewer, consciously or not, may try to push his/her interviewees in the direction of confirming his/her conclusions. However, unstructured interviews have other significant limits such as questionable comparability of data, risk of time waste, etc. (Black and Champion, 1976:365). Hence the interviewer must be aware of these limits as well.

CHAPTER FOUR - THE UNITED STATES: THE SOLE INFORMATION SUPERPOWER

*"Nobody really understands the United States—
neither foreigners, nor its own people."
Karl Deutsch (1980:231)*

*"The U.S. economy and society are ever more
dependent on information systems"
Martin C. Libicki (1997:11)*

*"Because so many key components of
our society are operated by the private
sector, we must create a genuine
public/private partnership to protect
America in the 21st century."
President William J. Clinton¹*

4. 1 Introduction

The first case-study is the United States, because it scored high in two indicators for my independent variables, that is, economic freedom/telecom freedom and national security. This profile² is one of the most interesting, since it gives me the possibility of observing the two variables in action. Thus far, in the United States, the private business/civil liberties informal alliance, which backs economic/telecom freedom, has gained the upper hand (Levy, 2001). In my field research trip, I interviewed government officials, NGOs activists and academics. All of them, with varying emphasis and to different extents, confirmed the main results that arose in chapter three about the U.S. government's attitude towards controlling the Internet. The "information economy"—prominently represented in this work by the liberalization/privatization of the telecom sectors—and the exigency of national security are on diverging paths. The plain fact, however, is that the U.S. national security complex has had to yield.

In addition, it would be impossible to write a study on government control of the Internet without investigating the United States. Historically, structurally and content-wise, the overall position of the United States is so vital for the future of the Internet that analyzing the American political debate on this issue corresponds closely to examining *the*

¹ <http://www.fbi.gov/nipc/nipc.htm> (v. October 1, 1999).

² It was indicated as "Country D" type in the chapter three.

core debate on the Internet. This circumstance is accurately described by the International Telecommunication Union (ITU) as “US-centric: [w]hether measured by the location of Internet users, websites or direction of traffic flows, the United States takes the lion’s share of the Internet. This is reflected too in the policy-making process in which all major decisions have been, until now, effectively set in the United States” (ITU, 1999:1). Simon Singh (1999:304) writing about the cryptography problem and the Internet has also confirmed that “...whatever policy is adopted in America will ultimately have an effect on policies around the globe.” This state of affairs is explained by historical (the Internet was born in the U.S.), technical (principal backbones are in the U.S.)³ and cultural (English is the dominant language of the Net) factors (ITU 1999).

The United States is the “information society”: it is actually the only “information superpower”. In 1998, a report published by the National Telecommunication and Information Administration (NTIA) at the request of Vice President Gore found that “...Americans have increasingly embraced the Information Age through electronic access in their homes”.⁴ Nation-wide penetration rates were 93.8% for telephones, 36.65% for personal computers, 26.3% for modems, and 18.6% for on-line access.⁵ Between 1994 (the year of the first survey) and 1997, PC ownership has increased by 51.9%, modem ownership 139.1% and e-mail access by 379.1%

Despite this considerable increase, disparities among the different racial groups and households incomes are still considerable. Indeed, the digital divide between racial groups has increased since 1994. For instance, White households are twice as likely to own a computer than Black or Hispanic households. Education also plays a great role in the development of the information society, since those with a college education are almost *ten times* as likely to own a computer as those with high school (63.2% vs. 6.8%).⁶

As Risse-Kappen (1995:208) has correctly pointed out, the United States represents a society-dominated structure, with a strong organization of interest groups, in which societal demands can be mobilized easily and quickly. Access to federal and state governments, legislatures and bureaucracies is ample and structured. Interest groups are greatly institutionalized, and very efficient. Transparency, at all levels, is highly valued by

³ In 1999, during the NATO bombing in Kosovo, out of curiosity, with a colleague I tried to “trace-route” (follow the route of a packet) to a server at the University in Belgrade. Not surprisingly, from Italy, the trace-route packet reached Belgrade going through two major backbones in the United States.

⁴ “Falling Through the Net”, <http://www.ntia.doc.gov/ntiahome/net2/failling.htm> (v. September 29, 1999)

⁵ <http://www.ntia.doc.gov/ntiahome/net2/failling.htm> (v. September 29, 1999)

⁶ <http://www.ntia.doc.gov/ntiahome/net2/failling.htm> (v. September 29, 1999) (emphasis in the text).

the public opinion.⁷ The availability of independent sources of information is remarkable, and the American public appreciates the diversity and autonomy of media. Much like transnational alliances, domestic, intrasectoral alliances can as well influence specific policies in the short run, since they can straightforwardly access decision makers.

Not only are the Federal government and the whole political system highly decentralized with different actors (including the President) competing for influence and obliged to search for compromise—thus making the identification of lines of decisions complicated and laborious. But also, as explained in chapter two, many of the fundamental solutions pertaining to the development of the Internet have been informally⁸ generated by individuals or groups who were highly preoccupied with the efficiency and functioning of those solutions. Those same people would not bother finding out who was officially designated or held the executive power to authorize those solutions to be implemented: technical and management problems were simply tackled by those confronted with them.

Needless to say, this method has offered the Internet an effective practice to deal with unavoidable technical bottlenecks, but meanwhile renders the attribution of executive responsibilities hard to ascertain. For instance, the whole crucial dispute on the domain names system (DNS) traces its origins in several documents (RFCs) that have been written by several scientists since the early 1980s. In one of those documents describing the .gov TLD, (for federal government offices in the United States), Jon Postel wrote that "...a decision was taken to register only agencies of the U.S. Federal government in this domain".⁹ He did not specify who made the decision, or why. Thus, one of the most important documents about one of the most important Internet issues is lacking a noteworthy piece of evidence.

In the first parts of this chapter, I will outline the principal actors in the Internet debate in the United States. I will then illustrate the main issue-areas of the current status of Internet debate. Finally, in the last section, I will offer some preliminary conclusions as well as speculations on how, if the accidental alliance of pro-liberties NGOs and users groups with the private business were to split, the contest between the national security and ICT business communities might evolve and influence the future development of the Net.

⁷ According to the "Opacity Index", developed by economists at the consulting firm *PricewaterhouseCoopers*, the United States has a very low score (on a 1-100 ranking, the U. S. scores 36), indicating a high degree of transparency (the index is available at http://www.opacityindex.com/ind_theindex.html v. March 20, 2001).

⁸ As explained earlier, all the "strategic" decisions have been published under the unceremonious and casual title of "Request For Comments" (RFC).

⁹ Postel RFC 1591, March 1994, at <http://www.isi.edu/in-notes/rfc1591> (v. October 1, 1999).

4.2. The Complexity of the American Decision-Making Machinery (and Why Americans Like It the Way It is)

Karl Deutsch's opening remark that cited at the beginning of this chapter plainly summarizes the principal complication that students of U.S. politics must always face. Dahl (1994:13) has shared Deutsch's conclusions, noting that "Americans must now cope with a political system that works in opaque and mysterious ways that probably no one adequately understands". This section examines the complexity of the American political system. The fragmented nature of this system in fact is an intervening variable that, in the case of the United States, contributes to explain why the federal government cannot afford to ignore any of the several actors concerned with the struggle of setting the level of control on the Internet. Law enforcement and intelligence agencies, pro-family groups, ICT associations, private companies, and civil liberties organizations through multiple (and sometimes overlapping) channels promote their own agendas with policy-makers in the government and in Congress. Compromised agreements and watered down initiatives are inevitable, while the federal government is torn in the attempt of accommodating as many actors as possible.

The complications of understanding the American political system originate from a multiplicity of factors: a patchy political system, resting on a societal mosaic and contained by a "uncertain" federal state.¹⁰ "Such a degree of fragmentation and lack of integration is unmatched in other advanced democracies, especially those with a strong tradition of a state" (Chamorel, 1994:63)—namely Japan or most European countries (Dahl, 1994, Bowles, 1993, and Deutsch, 1980).¹¹ It is noteworthy that, on the one hand, "[t]he American federal system has never been a neat system of distinct governmental activities and functions" (Lees, 1970:49). On the other hand, "[t]he Tenth Amendment to the Constitution¹² reflects an American antipathy to government in general, to a unitary state in particular..." (Bowles, 1993:259). Consequently, since "...the people are sovereign [...] ... the powers of government are limited" (Saye et al., 1966: 87).

The main and most direct consequence of the "separation of powers" constitutional principle is that pluralism, rivalry, and competition creep into the very center of government. It also elicits "...the representation in the executive and legislative branches of

¹⁰ The attribution of being "uncertain" to the federal government is justified if the government is compared with other institutional actors such as the states, Congress, the judiciary, local legislatures, etc. Abroad, however, the U.S. government is usually perceived as "strong" and effective.

¹¹ Indeed, Chamorel has observed that "...with the possible exception of Canada, the United States probably has the most decentralized political system among the major industrialized democracies" (1994:77).

differing and possibly divergent interests, and...the strong likelihood that the president and Congress will press for conflicting policies" (Dahl, 1994:5). Finally, Bowles (1993:233) has noted that "separation of powers, combined with Federalism renders bureaucracy complicated, dispersed, decentralized, and its accountability to representative politicians problematic". Not accidentally, the process of identifying the lines of authority in the country is more perplexing and complex, since even presidents are constantly obliged to negotiate and compromise with other politicians who, in turn, have their own agendas and constituencies (Bowles, 1993:90).

Another peculiar feature of the American political landscape contributes to the complexities of analyzing the decision-making process in the federal republic, namely the "interest industry" (Bowles, 1993). As Dahl (1994:8) has observed, "in recent decades... both the number and variety of interest groups with significant influence over policy-making have greatly increased". The occurrence of such a large number of interest groups in American politics is an aftereffect of the First Amendment to the Constitution, which states the right of the people "to petition the government for a re-address of grievances". Consequently, "...modern American government is deeply penetrated by private groups, its process of policy-making the product of particularistic patterns of interaction between groups and public officials" (Bowles, 1993:211).

However, attributing the responsibility for this impractical fragmentation only to the constitutional system—hardly modified since its inception—would be misleading. Indeed, this state of affairs seems rather in accordance with the prevailing mood of the American public. Yergin and Stanislaw (1998) have noted that while distrust in and skepticism for government is part of the American culture, the role of the Federal government has steadily increased in the life of the country. The answer, argue Yergin and Stanislaw quoting W. Scheider, is "pragmatism"—a cornerstone of the American culture.¹³

¹² "Powers not delegated to the United States by the Constitution...are reserved to the States, or the people".

¹³ Pragmatism as a philosophy for the unity of theory and practice was developed entirely by American philosophers, namely Charles Pierce (1839-1914), his follower William James (1842-1910) and John Dewey (1859-1952) and more recently Richard Rorty. According to James Kloppenberg (in Wightman Fox and Kloppenberg editors, 1995:537), pragmatism is currently undergoing a revival. Along with "individualism", "...an almost sacred concept signifying the primacy of personal interests and self-determination" (Gillian Brown in Wightman Fox and Kloppenberg editors, 1995:337), these are the distinct cultural attributes normally associated with the "American society" by both Americans and non-Americans alike. See Wightman Fox R. and J. Kloppenberg (editors) (1995), *A Companion to American Thought*, Oxford, UK and Cambridge, USA: Blackwell, and Bothamely J. (editor) (1993), *Dictionary of Theories*, London et al.: Gale Research International Ltd.

This viewpoint was confirmed by Tamar Frankel of the Boston University Law School.¹⁴ During my interview, professor Frankel pointed out a distinct feature of the American character, namely an aversion towards “concentration of power”. She based her discovery upon her study of the organization of the law enforcement system in the United States. The proliferation of law enforcement agencies and of levels of competence of various actors (i.e. federal, state, county, local, private etc. etc.) create enormous problems of coordination and duplication, without increasing efficiency.¹⁵

Clearly, “[b]y promoting competition between branches of a weak central state, fragmentation of Federal government begets weakness of central authority, corresponding penetration of governments by groups, and relative openness of policy process” (Bowles, 1993:209). The self-evident solution to such a problem would be to concentrate the investigative and repressive competence of law enforcement agencies in one or two police institutions. However, such a solution would imply a tremendous concentration of power—which could and would be abused. Thus, professor Frankel concluded, although Americans will not stop complaining about rising crime, pragmatically they are willing to accept less efficiency to avoid power concentration. Interestingly, Chamorel (1994:57) has also observed that although in Europe “.., efficiency was considered a virtue of the political system and required, it was believed, a certain degree of order in society as well as in government structures”, the “weak” American state was not built around concepts of rationality and efficiency. The ensuing system reflected the profound mistrust that Americans almost instinctively feel towards any concentration of power.

The complexity of many public interests—ranging from health care to taxation, immigration or economic growth—in a modern democracy has brought about the proliferation of interest groups as well as an expanded role of the government in these matters. Having to administer such articulated issues requires reconciling a variety of interests and endowments as well as the dependence of the federal government on specialized sources of information that are often monopolized by the same interest groups. Consequently, the many segments of the federal government (the president, department secretaries, and federal agencies) can be more easily approached and influenced by professional lobbyists. Ultimately, the orderly structure described in this chapter is an

¹⁴ Tamar Frankl, professor, Boston Law School, Boston University, personal interview Boston, MA, July 13, 1999.

¹⁵ Morgan and Connor (1971) have also noted the same problem of many law enforcement agencies any laws.

attempt at emphasizing the prime actors and crucial nodes of the political system, more than the actual representation of America's way of doing politics.

4.3 The Chronology of the Debate

For a country like the United States, telecommunications have always had strategic importance. The size of the country coupled with government and business requirements have obliged Americans to pay particular attention to this domain. The oldest piece of legislation on telecommunications in the United States is the 1934 Telecommunications Act—i.e. the “...basic law governing the regulation of communications by wire or radio within the United States and between the United States and overseas points” (ITU, 1998:121). The 1934 Act also established the government authority for radio and wireless communications, namely the Federal Communication Commission (FCC) (see section 4.4.1).

The first major modernization of that piece of legislation was the 1996 Telecommunication Act signed by President Clinton on February 8, 1996. The 1996 Act “...open[ed] up intrastate and local (intra-city) telecommunications services to competition and [set] rules under which the incumbent providers of local and intrastate service [could] begin to offer intrastate and local service” (ITU, 1998:121). In other words, the 1996 Act laid “...the ground rules for competition and regulation in virtually all sectors of the communications industry, from local and long-distance telephone services to cable television, broadcasting and equipment manufacturing...”.¹⁶

If the performance and reliability of the telecom sectors have enjoyed long-standing consideration by American legislators and public officials, neither is the U. S. government's attention to computer security a radically new phenomenon that has arisen with the diffusion of the Internet. On the contrary, computer security conditions have deteriorated with the advent of the Internet. Until 1984, responsibility for computer security standards in the civilian realm was assigned to the National Bureau of Standards (NBS) within the Department of Commerce (DOC). Indeed, “during the 1970s, NBS became a pivotal player in the development of computer security standards, particularly the Data Encryption Standard (DES)” (EPIC, 1998:5), which was then adopted to protect non-military

¹⁶ http://www.tiaonline.org/government/telecom_act/ (v. October 2 and 3, 1999). The 1996 Act contained also provisions for illegal transmissions via computer of obscene and indecent material to minors, which would constitute the basis for the passing of the 1996 Communication Decency Act (CDA)

government communications.¹⁷ Military communications security and foreign eavesdropping—namely encrypting and code-breaking—were the exclusive competence of the National Security Agency (NSA)

In 1984, the NSA succeeded in convincing President Reagan to sign the National Security Decision Directive 145 (NSDD-145) which “...authorized the NAS to develop means to protect ‘unclassified sensitive’ information...[and] to curb the use of public cryptography...”(EPIC, 1998:5). Hence, the NSA overtook the NBS in establishing security standards for civilian communications and data which also meant, incidentally, that the NSA had the power to question private companies about their security procedures or customer relations. As a consequence, in 1987, Congress passed the Computer Security Act (CSA), noting that the NSDD-145 had “raised considerable concern within the private sector and the Congress”.¹⁸ However, in 1989, a memorandum of understanding between the NBS (then renamed National Institute of Standards and Technology, or NITS) returned many of the competence restricted by the CSA to the NSA, particularly in the realm of cryptography.¹⁹

The notoriety commanded in both the U.S. and foreign media by two incidents involving electronic intrusion between the late 1980s and the early 1990s contributed to a new international dimension to the threat perceptions of the national security and law enforcement communities, mostly conveyed by the NSA and the FBI. In the former case, West German hackers presented their intruding “services” to the KGB, while in the latter case, Dutch hackers offered military information stolen by 34 U.S. Department of Defense (DOD) sites to the Iraqis, during operation Desert Storm.²⁰

With specific regards to the Internet, the majority of the “historical” decisions that have transformed a sophisticated research tool into an international communication network have been made in the United States by American scientists, and more or less openly endorsed by the U.S. government. The decision by the National Science Foundation (a U.S. government agency) to cease its operational management of the Net backbone (the NSFNET) in 1995 and the growing economic expectations for electronic business has

(http://www.ntia.doc.gov/otiahome/tiiap/newsletter/telcom_act.htm#SUMMARY) (v. October 2 and 3, 1999).

¹⁷ DES works with algorithms based on 56 bites (i.e. 2^{56} possible permutations).

¹⁸ Quoted in EPIC (1998:11).

¹⁹ The cryptography issue will be examined in more details in section 4.

²⁰ In both incidents, it was more a case of appearance than substance. The first event was popularized by Cliff Stoll, the actual “chaser” of the West German intruders, in his book *The Cuckoo's Egg* (London: Pocket Books, 2000), and by Katie Hafner, co-author (with J. Markoff) of *Cyberpunk* (1991), New York: Touchstone, where she convincingly presents the episode by the intruders' side. The second episode was never extensively investigated, but it appears that the Iraqis turned down the offer, thinking it was a “hoax”.

meant that the U.S. government has progressively been flanked by other substantial stakeholders on the Net future: the EU and its governments, the World Trade Organization (WTO), the World Intellectual Property Organization (WIPO), telecommunication and software companies, and the like.

This resolve by the U.S. government has certainly made it easier for millions of non-American users to access the Net at reasonable conditions and costs.²¹ At the same time, however, alerted by the intelligence community, the executive became aware of the increasing risks to the national infrastructures system that such a decision might entail. Through uncontrolled Internet access points, foreign nationals, either government-sponsored or terrorists, could reach and exploit the security vulnerabilities of critical infrastructures, thus compromising America's national security. Given the manifest reliance of the United States on computer-assisted operations to manage energy, financial, transportation, and communication networks, it is not surprising that the Clinton Administration took the alert seriously.

Ever since entering office in the early 1990s, the Clinton Administration has tried to be accredited with the establishment of the "information highway," with Vice President Al Gore as a leading figure in this respect.²² Indeed Al Gore introduced the U.S. vision for the Global Information Infrastructure (GII) at the ITU World Telecommunication Development Conference held in Buenos Aires in March 1994. Among the principles declared at the conference were to encourage private sector investment and to promote competition, as well as to provide open access and ensuring universal service.²³ These principles were then incorporated into the ITU's *Buenos Aires Declaration on Global Telecommunication Development for the 21st Century*. At the same time, however, the Internet was becoming the GII, or the "accidental highway" (Anderson, 1995).

The unexpected Internet explosion took the government quite by surprise, but the strategic vision of the "information society" has not changed. Thus, in 1997, President Clinton declared that world governments should adopt a "hands-off" policy approach to the Internet, eliminating taxes and unnecessary regulations that could hinder the development of the new medium. Indeed, this standpoint was later elucidated in the government plan for e-

²¹ This decision was unquestionably concordant with the guiding principles of the Clinton Doctrine as outlined in the 1994 National Security document (A Strategy for Engagement and Enlargement) which called for the promotion of free market democracy abroad.

²² 2000 Presidential candidate (and current U.S. President) George Bush actually called Presidential candidate Al Gore as "the man who thought he invented the Internet" (<http://www.cnn.com/2000/ALLPOLITICS/stories/10/04/campaign.wrap/index.html> v. December 19, 2000 and January 10, 2001).

commerce that, in December 1997, was promoted through an *ad hoc* Web site maintained by the Secretariat for Electronic Commerce, U.S. Department of Commerce.²⁴

The framework program for e-commerce has stated that "...governments should refrain from imposing new and unnecessary regulations, bureaucratic procedures, or taxes and tariffs on commercial activities that take place via the Internet."²⁵ To fully realize the potential of e-commerce, therefore, "...governments must adopt a non-regulatory, market-oriented approach to electronic commerce, one that facilitates the emergence of a transparent and predictable legal environment to support global business and commerce".²⁶ Furthermore, in 1999, the report *The Emerging Digital Economy II* by the DOC noted that "electronic commerce (business transactions on the Web) and the information technology (IT) industries that make 'e-commerce' possible are growing and changing at breathtaking speed, fundamentally altering the way Americans produce, consume, communicate, and play."²⁷

From these occurrences, it can be concluded that, well before the Net became a mass phenomenon in 1994/95, some key actors within the federal government were greatly disturbed by the inherent frailty and openness of software and computer networks. The United States has since grown more and more dependent upon these software and networks, certainly more than any other industrialized countries.²⁸ Hence, as Chapman has noted, in the 1990s, "...the Internet has increasingly been regarded by national security officials as a new playing field for international conflict, a new medium in which national security will take on new forms, and one in which the U.S. government agencies responsible for national security have a growing stake" (1998:2).

By demanding greater control and restrictions in computer security matters, these actors were certainly convinced that they were acting in the interest of their country; that is, a disposition that cannot be dismissed or ignored. At the same time, they were also acting in the interest of their own institution or agency which would increase its relative prestige—and, thereby, predominance—within the structure of the U.S. federal government. Since

²³ <http://www.iitf.nist.gov/documents/docs/gii/giiagend.html>. (October 4, 1999)

²⁴ <http://www.ecommerce.gov/> (v. October 5, 1999).

²⁵ <http://www.ecommerce.gov/framework.htm> (v. October 5, 1999).

²⁶ <http://www.ecommerce.gov/framework.htm> (v. October 4 and 5, 1999).

²⁷ <http://www.ecommerce.gov/ede/summary.html> (v. October 4 and 5, 1999).

²⁸ Possible exceptions may include Japan, which, however, is hardly perceived as a credible "threat" by other nations, and the Scandinavian countries, where the telecommunication industries are so crucial for those countries' economies that serious disruptions in those industries would severely compromise their national security. Personal interview with Colonel Robert Ghent, U.S. Army War College, personal interview, Carlisle, PA, July 20, 1999.

there is no dominant center of power in the United States federal government, and no sense of a 'State' (Bowles, 1993:233), alterations in the relative distribution of influence among government actors have recurrently induced reactions by other government bodies, but also by the legislative and judiciary branches, to reestablish the balance. The popularization of the Internet, with its open protocols and evident lack of hierarchical control by any authority, directly amplified the known problem of the protection of America's growing reliance on computer-managed networks. Indeed, even if, for a long period of its existence, the Internet has had a divergent path from "national security", its path is now converging, "...but in a way that makes the Internet problematic and even threatening to national security" (Chapman, 1998:4).

Unlike other, more distinctive matters of national security, in which law enforcement/intelligence/defense personnel have most of the time enjoyed a quasi-monopoly of information (the most noticeable case was nuclear warfare), the impact of Internet on national security has triggered an unexpected situation. Because of its origins and development, the Internet has always prized the maximum distribution and availability of technical information. Plenty of on and off line sources display and explain drawbacks, defects, "bugs", patches and upgrades for the Net. All this information is normally available to any moderately knowledgeable user. Pro-liberties NGOs, users' groups and consumers' organizations have seized this mass of information, "boosted" it with competent legal expertise, and with the more or less open support by the ICT industry, which has traditionally been skeptical about government intrusion,²⁹ and have engaged the national security/law enforcement community on its ground to fight off Internet control.

Until the early 1990s the main concern of the "controllers" was how to limit the number of young pranksters accessing non-public computers. Now, how controlled the Net will be will rest on the outcomes of the current controversies on (1) the free use of cryptography, (2) the protection on critical infrastructures, (3) free speech, and (4) the domain name system. How these issue will be addressed will affect the privacy of users—i.e. how much about them the controlling parties may or may not know—their ability to communicate, and ultimately the future nature of the Net. Because the United States is a democracy, in this struggle, the public's support is sought by all the actors, i.e. the federal

²⁹ A report of an ICT industry association in 2000 confirmed this long-standing attitude of American businesses, noting that "[t]he private sector is handling the e-commerce craze just fine, thank you, and the government should just butt out..." (<http://www.techweb.com/wire/story/TWB20001013S0008>, v. March 20, 2001).

government, private industry, and the civil liberties organizations.³⁰ At the time of writing, public support was mostly in favor of the “unusual” alliance, which has at least stalled the drive of the national security community for greater government control on the Net.

4.4. The Main Players of the Internet Debate

For the sake of clarity, the primary actors taking part in decisions about Internet control have been sorted into four wide groups: the federal government, the Congress and Judiciary, the private sector, and Non-Government Organizations (NGOs) acting on fields such a privacy and consumers’ protection and civil rights as well as users’ groups. However, the subjects in these neatly defined groups overlap and duplicate many of their actions, and cooperate as well as disagree to considerable extents.

For instance, speaking of one political “alliance” active in the debate, Wayne Madsen, senior researcher at the Electronic Privacy Information Center (EPIC), referred to it as the “red-brown” coalition.³¹ He recognized that as the accidental partnership of extreme left and right sympathizers, born to oppose the federal government intrusions in individuals’ privacy.³² Normally these activists hold opposite political views, but their common perception of the government as “Big Brother” threatening to curtail the privacy of U.S. citizens has coerced them into becoming temporary, albeit awkward, bedfellows.

In addition to that, fig.1 reports just some of the principal bodies of the federal government that are currently taking part in shaping the Net. As mentioned in the introductory section of this chapter, although formally parts of the same institution—i.e. the federal government—many of these actors often do not coordinate their actions and sometimes even pursue conflicting interests. Or, they are part of the government, but respond to Congress. The most noticeable of these conflicting interests is the attempt by the intelligence community (led by the NSA and FBI) to restrain the use of cryptography for individual use, while the Department of Commerce (DOC) is trying to ease the rules for exporting strong encryption software produced by American companies.

³⁰ Personal interview with Ari Schwartz, Policy Analyst, Center for Democracy and Technology (CDT), Washington, D.C., July 12, 1999.

³¹ The color brown is a reference to the “brown shirts” of the Nazi party.

³² Wayne Madsen, Senior Researcher, (and Marc Rotenberg, Executive Director), EPIC, personal interview Washington, D.C., July 16, 1999.

4.4.1. The Government

| NAME | ACRONYM | RESPONSIBLE ORGANIZ. |
|--|---------|----------------------------|
| President's Commission on Critical Infrastructure Protection | CCIP | White House |
| Critical Infrastructure Assurance Office | CIAO | White House |
| Department of Commerce | DOC | |
| Federal Trade Commission | FTC | DOC |
| Federal Communications Commission | FCC | Congress |
| Federal Networking Council | FNC | |
| National Telecommunications and Information Administration | NTIA | DOC |
| Institute for Telecommunication Sciences | ITS | DOC |
| National Institute of Standards and Technology | NIST | DOC |
| Telecommunications and Information Infrastructure Assistance Program | TIIAP | |
| U.S. Navy's EC/EDI Program Office | | DOD |
| Defense Advanced Research Projects Agency | DARPA | DOD |
| Department of Energy's (DOE) Computer Incident Advisory Capability | | DOE |
| National Coordination Office for Computing, Information and Communications | NCO/CIC | |
| National Science Foundation | NSF | |
| National Security Agency | NSA | DOD |
| Office of Information Technology | | Government Services Agency |

Fig.1 The Federal Government³³

The term "government" can be used to indicate both the elected officials—such as, in the U.S. case, the President and even Congress—as well as the bureaucracy which is designated to implement the decisions made by those officials. For practical purposes, most of the time, the majority of citizens connect with "the government" through the

³³ <http://www.cybertelecom.org/links.htm> (v. October 11 and 12, 1999).

bureaucracy, not the elected officials. Thus, they often identify civil servants with "the government".

In the United States, the bureaucracy is more than just a mere appendix of the federal government. More correctly, Bowles (1993) has called it the "Fourth Branch", thus attributing it with independent decision-making powers from the other traditional branches. Again, the federalist interpretation of the form of the state and the American affinity in distrusting concentrations of power have conspicuously preserved this status quo. Moreover, Bowles has noted that, "the Federal bureaucracy is highly decentralized both within Washington and throughout the country. Its key organizational units are usually not Departments but the semi-autonomous agencies or bureaus within them" (1993:233). Within this framework, in analyzing the activities of the executive branch with regard to the Internet, the scholar has to examine the acts and performance of both the President and its staff and cabinet as well as those of the permanent bureaucracy. Consequently, these two sides of the "Administration" are considered jointly in this section.

The Department of Commerce (DOC) is the branch of the Administration that oversees trade, both domestically and internationally. Concerned that "[b]y 2006, almost half of the U. S. workforce will be employed by industries that are either major producers or intensive users of information technology products and services",³⁴ in recent years, the DOC has steadily increased its appreciation for information technology and the Internet. The most important branch of the DOC with regard to the Net and telecommunications in general is the National Telecommunications and Information Administration (NTIA).³⁵ NTIA is the Executive Branch's principal voice on domestic and international telecommunications and information technology issues,³⁶ as well as serving as the President's principal advisor on telecommunications and information policy matters.³⁷

The DOC influence on future Internet developments is substantial, even superior to that of the DOD and certainly more essential than the DOJ or any other federal department. This influence is evident in two critical areas: (a) the DOC has the prime responsibility for authorizing the export of over 40-bit encryption software (via the Bureau of Export Administration, see section 4.4)³⁸ and (b) the DOC operates closely with the non-profit

³⁴ <http://www.ccommerce.gov/cde/summary.html> (v. October 11 and 12, 1999).

³⁵ <http://www.ntia.gov/> (v. October 14 and 15, 1999).

³⁶ <http://www.ntia.doc.gov/ntiahome/ntiafact050698.htm/> (v. October 14 and 15, 1999).

³⁷ NTIA has its own research body on telecoms, the Institute for Telecommunication Sciences (ITS).

³⁸ Since 1998, the DOC has granted blanket exceptions for certain countries and uses (e.g. banking and financial services). Only a handful of countries on a "black" list are completely banned from the export of strong key encryption software (being "sponsors of terrorism." i.e., Iran, Iraq, Libya, North Korea, Sudan,

Internet Corporation for Assigned Names and Numbers (ICANN) for the management of the domain names system (DNS). Both these factors are indispensable for electronic commerce and the implementation of the e-economy (see sections 4.2 and 4.6).

With reference to the future developments of the Net and statutory control by the U.S. government, the role of the “devil’s advocate” is played by the law enforcement/national security communities symbolized by the National Security Agency (NSA) and the FBI that are parts of the Departments of Defense (DOD) and Justice (DOJ). Although the Department of Defense (DOD) is greatly concerned with Information Warfare and the protection of the National Information Infrastructure (NII), the DOD’s overall orientation is rather in the direction of foreign threats. The “domestic battle” is somehow shouldered more specifically by the NSA on the issue of free use of encryption software. In addition to the FBI’s activities to protect the federal communications, the DOJ is also responsible for telecommunications matters that raise possible antitrust issues.³⁹ Finally, the Department of State is responsible for formulation and coordination of foreign policy related to international communications and information policy, while the Department of Energy (DOE) is assigned with the mission of protecting the energy distribution systems, parts of the NII.

All of these main players have been required to nominate two members to the first crucial body earmarked for the protection of the NII, namely the President’s Commission on Critical Infrastructure Protection (PCCIP), created with Executive Order 13010 in July 1996. More specifically the members of the PCCIP are the (1) Department of the Treasury, (2) Department of Justice, (3) Department of Defense, (4) Department of Commerce, (5) Department of Transportation, (6) Department of Energy, (7) Central Intelligence Agency, (8) Federal Emergency Management Agency, (9) Federal Bureau of Investigation, and (10) National Security Agency.

The Clinton Administration’s Policy on Critical Infrastructure protection was further specified in 1998 with the Presidential Decision Directive 63 (PDD-63) that stated that “[e]very department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems”.⁴⁰ Moreover

Syria and Cuba).

³⁹ The DOJ was the counterpart to Microsoft in the 1999 antitrust case against the software giant, thus siding, in this case, with civil liberties NGOs.

⁴⁰ http://www.ciao.ncr.gov/CIAO_Document_Library/paper598.html/ (v. October 17 and 18, 1999).

the PDD-63 established the CIAO, Critical Infrastructure Assurance Office, to oversee the implementation of PDD-63 in each department.⁴¹

The Federal Communications Commission (FCC)

The Federal Communications Commission (FCC) is an independent government agency, directly responsible to Congress (5 Commissioners, appointed by the President and confirmed by the Senate). The FCC— whose jurisdiction covers the 50 states, the District of Columbia, and U.S. possessions—was established by the Communications Act of 1934 and “is charged with regulating interstate and international communications by radio, television, wire, satellite and cable”.⁴² The FCC’s Bureaus “...are responsible for developing and implementing regulatory programs, processing applications for licenses or other filings, analyzing complaints, conducting investigations, and taking part in FCC hearings.”⁴³

Since “[t]he Internet Economy...is rapidly changing the way America does business”, the FCC see its mission as the following: as market forces have driven the Internet’s growth, the FCC has had a role to play in creating a deregulatory environment in which the Internet could flourish.⁴⁴ Hence, the FCC aims at ensuring “...near universal availability... giving rise to the unregulated growth of the Internet... [backing] availability of inexpensive dial-up Internet access... deregulating the telecommunications equipment market...[and] implementing flexible spectrum licensing policies...”.⁴⁵ The official position of the FCC regarding the future of Internet-based traffic may be summarized as “resisting government intervention”,⁴⁶ while guaranteeing fair competition and open access to the Net (e.g. the Broadband Internet Access project⁴⁷) to users and companies alike. In fact, a document released by the FCC clearly states that “...the growth and continued success of the Internet, and the ability of market forces to sustain and encourage that growth, can be attributed to one basic attribute: the openness of both the Internet and the underlying telecommunications infrastructure”.⁴⁸

⁴¹ <http://www.ciao.ncr.gov/default.htm> (v. October 17 and 18, 1999). The overall problem of the NII protection is analyzed in greater details in section 4.4.

⁴² <http://www.fcc.gov/aboutus.html/> (v. October 19 and 20, 1999)..

⁴³ <http://www.fcc.gov/aboutus.html/> (v. October 19 and 20, 1999)

⁴⁴ http://www.fcc.gov/Bureaus/OPP/News_Releases/1999/nrop9004.html/ (v. October 22 and 23, 1999).

⁴⁵ http://www.fcc.gov/Bureaus/OPP/News_Releases/1999/nrop9004.html/ (v. October 22 and 23, 1999).

⁴⁶ http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp31.txt/ (v. October 22 and 23, 1999)

⁴⁷ The Broad Band Access project aims to provide American households with fast Internet access at very affordable prices. With large band access, contingencies such as video-on-demand or music broadcasting would become easier and more common. See also <http://www.fcc.gov/broadband/>.

⁴⁸ “The FCC and the Un-regulation of the Internet”, at

http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp31.txt/ (v. October 23, 1999)..

One should not think, however, that, on the basis of the statements reported here, the FCC has embraced a “self-governing” Net or that it indiscriminately advocates the cause of civil liberties NGOs. For instance, in 1999, the FCC adopted rules that require new TV sets to be equipped with the “V-Chip”, a technology that allows parents to block certain TV programs.⁴⁹ The initiative has been criticized by civil liberty NGOs because it can set an example for the Internet and help champion web-page rating initiatives. The FCC disposition toward more or less statutory control on the Net in the United States will ultimately be influenced by the President’s and Congress’ close scrutiny.

Perhaps more important than the V-Chip is the fact that the FCC oversees the implementation of the Communications Assistance for Law Enforcement Act (CALEA)—which, according to civil liberty NGOs, if activated may seriously endanger individuals’ privacy in communications.⁵⁰ Despite strong opposition from industry and civil liberties organizations, Congress voted CALEA in the last session of 1994, after the government offered to pay telephone companies \$500,000,000 to make the proposed changes. CALEA’s main goal is to make the national telephone system more suited to wiretapping by law enforcers (mostly the FBI).⁵¹

More specifically, CALEA “...requires the telecommunications industry to design its systems in compliance with FBI technical specifications [however] ...over the last few years, the FBI and industry representatives were unable to agree upon those standards, resulting in the current proceeding before the Commission”.⁵² The contest between civil liberties organizations and telecom companies, and the FBI has been lingering since then, inasmuch as the private sector and the FBI have been unable to find common ground on the technical standards of CALEA. In fact, telecom operators have been afraid that granting the FBI and other law enforcers extensive wiretapping capabilities could result in excessive surveillance, thus seriously upsetting the public, and provoking severe financial losses—and Internet NGOs have duly emphasized this in particular.⁵³

⁴⁹ The provision for the V-Chip was contained in the 1996 Telecommunication Act

(http://www.ntia.doc.gov/otiahome/tiia/newsletter/telcom_act.htm#SUMMARY/ v. October 24, 1999).

⁵⁰For instance, EPIC opposed the enactment of CALEA in 1994 and has since participated as a party in the FCC proceeding, arguing that many of the FBI standards go beyond the scope of the legislation and threaten communications privacy. The full text of CALEA is available at <http://www.epic.org/privacy/wiretap/> (v. October 26 and 27, 1999).

⁵¹Since more and more telecom operators are relying on packet-switching traffic, which has been asked by the FBI to be included the deal, inevitably the developments of CALEA will have direct effects on the evolution of the Internet.

⁵² EPIC Alert, Volume 6.13 September 1, 1999 available at <http://www.epic.org/alert/> (v. October 26 and 27, 1999)

⁵³ Indeed, requests for interception by federal and State law enforcers went up by 12% and 24% respectively in

In August 1999, however, the Center for Democracy and Technology (CDT) observed that:

[w]hile claiming to respect privacy, the FCC ruled in favor of the government on virtually all issues of privacy concern, including ruling that wireless phone companies must be able to provide the cell site of their customers at the beginning and end of every call, effectively turning cell phones into tracking devices.⁵⁴

As EPIC has recognized, such a ruling could result in a significant increase in government interception of digital communications, since the Commission has directed that "packet-mode communications" should also be made available to law enforcement agencies no later than September 2001.⁵⁵

The U.S. Intelligence and Law Enforcement Communities: The FBI and the NSA

As demonstrated above, the list of special U.S. government agencies that are competent to monitor the Internet or protect the NII is rather long. In addition to the FCC, the NTIA, the CIAO—to mention but a few—there are the Federal Networking Council (FNC), the DOC's Information Infrastructure Task Force (IITF). However, the two principal subjects that are most under scrutiny by civil liberties associations, Netizens and scholars are, on the one hand, the Federal Bureau of Investigation—part of the Department of Justice—and, on the other, the National Security Agency (NSA)—part of the Department of Defense. To large extents, they personify the "true spirit" of the law enforcement and national security communities, as well as the progressive blurring into each other.

The Federal Bureau of Investigation (FBI)

The FBI's foreign counterintelligence mission is set out in a strategy known as the National Security Threat List (NSTL). The NSTL combines two elements: (a) national security threats, regardless of the country of origin: (b) a classified list of foreign powers that pose a strategic intelligence threat to U.S. security interests.⁵⁶ According to the NSTL, key threats most relevant for the National Information Infrastructure (NII) are: (a) terrorism

1998. At <http://www.epic.org/privacy/wiretap/stats/1998-report/default.html/> (v. October 26 and 27, 1999).

⁵⁴ http://www.cdt.org/digi_tele/ (v. October 29 and 30, 1999).

⁵⁵ <http://www.epic.org/alert/> (v. October 26 and 27, 1999). The FCC has specifically stipulated that "...for wire-line, cellular, and broadband Personal Communications Services (PCS) carriers, implementation of a packet-mode capability and six Department of Justice/Federal Bureau of Investigation "punch list" capabilities must be completed by September 30, 2001" (<http://www.fcc.gov/wtb/csinfo/calea.html> v. October 30 and November 1, 1999). On the other hand, at the end of 1999, CDT and the Cellular Communication Industry Association filed a lawsuit in federal court appealing the FCC's decision (http://www.cdt.org/digi_tele/ (v. October 30 and November 3, 1999).

⁵⁶ <http://www.fbi.gov/programs/ansir/ansir.htm/> (v. November 3,4 and 5, 1999).

(foreign power-sponsored or foreign power-coordinated activities), (b) espionage (foreign power-sponsored or foreign power-coordinated intelligence activity), (c) economic espionage, (d) targeting the NII, (e) targeting the U.S. Government, (f) perception management.⁵⁷

More specifically, (d) includes:

1. denial or disruption of computer, cable, satellite or telecommunications services;
2. unauthorized monitoring of computer, cable, satellite or telecommunications systems;
3. unauthorized disclosure of proprietary or classified information stored within or communicated through computer, cable, satellite or telecommunications systems;
4. unauthorized modification or destruction of computer programming codes, computer network databases, stored information or computer capabilities; or
5. manipulation of computer, cable, satellite or telecommunications services resulting in fraud, financial loss or other federal criminal violations.⁵⁸

The other major engagement of the FBI considering the future of the Internet comes from its central role in establishing the National Infrastructure Protection Center (NIPC). Located in the FBI's headquarters building in Washington, D.C., the NIPC includes representatives from the FBI, other U.S. government agencies, state and local governments, and the private sector "in a partnership to protect our nation's critical infrastructures".⁵⁹

Established in February 1998, the NIPC's mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against America's critical infrastructures. These infrastructures, which include telecommunications, energy, banking and finance, water systems, government operations, and emergency services, are the foundation upon which our industrialized society is based.

Because the FBI supports controversial initiatives such as CALEA, CDA, COPA, CESA, FIDINET and *Carnivore*,⁶⁰ civil liberties organizations and many Netizens alike have identified the federal law enforcers, along with the NSA, as the prime advocates of a

⁵⁷ <http://www.fbi.gov/programs/ansir/ansir.htm/>. (v. November 3, 4 and 5, 1999)

⁵⁸ http://www.fbi.gov/programs/ansir/ansir.htm (v. November 3, 4 and 5, 1999)

⁵⁹ <http://www.fbi.gov/nipc/welcome.htm/> (v. November 6 and 7, 1999)

⁶⁰ FIDINET is the federal intrusion detection network that should monitor federal networks for unauthorized or illegal access. In other words, a sort of "...'burglar alarm' which alerts the federal government to cyber attacks, provides recommended defenses, establishes information security readiness levels, and ensures the rapid implementation of system 'patches' for known software defects"

(http://www.ciao.ncr.gov/press_release/WhiteHouseFactSheet_Cyber_Security.html v. November 8 and 9, 1999). *Carnivore* is an FBI-developed software (basically a "sniffer") that, placed in specific routers would monitor Internet traffic in clear, searching for keywords, and copying suspect messages.

quasi-“Big Brother society”. This image has been eagerly consumed by the larger public, which commonly holds the conviction that the federal government is already too intrusive.

The National Security Agency (NSA)

Just to be consistent with the overall structure of the American political framework, the “intelligence community” is a euphemism identifying a large array of intelligence services whose activities often overlap or contradict each other. In addition to the CIA, the NSA, and other major agencies, each service branch has its own intelligence, as does the State department.⁶¹ In this respect, the most relevant actor for the analysis of Internet control in the United States is the NSA. The reason for such a choice is clear-cut: the task of “...making and breaking, communicating and intercepting secret messages...is the principal business of the National Security Agency, a huge governmental intelligence apparatus, larger and more expensive than the CIA” (Ransom, 1970:127). Thus, anything pertinent to what is defined as SIGINT (Signal Intelligence) or COMINT (Communication Intelligence) comes under the intense scrutiny of the NSA, including communications on the Internet.

Based at Fort Meade, Maryland, between Washington DC and Baltimore, the NSA has long been unknown to the American public⁶² —a considerable asset for an intelligence organization—to the point that its name was rarely “...even listed on the organizational chart of the United States government” (Ransom, 1970:128). More recently, however, as the importance of communications have steadily grown in the United States as well as in the rest of the world, inevitably, the NSA has found itself exposed to more and more notoriety.

The most serious challenge to the NSA capability to maintain its edge on intercepting other parties’ communications comes from the steady, irreversible diffusion of public-key encryption software (Levy, 2001) that, in turn, is made possible by the decreasing costs of computing power. As powerful computers become increasingly cheaper, encrypting one’s communication has turned into a routine action even for a run-of-the-mill user. With its calculating power resources, the NSA can probably still break most of the encrypted communications exchanged on the Net. However, two structural problems might considerably complicate the NSA activity, namely the increasing number of encrypted messages and the increased length of encryption keys.

⁶¹ In the movie *Sneakers* (1992), Robert Redford greeted two allegedly NSA officers with the remark: “Oh, so you are the guys that I hear breathing when I pick up the phone”. One of the two officers replied: “No, that’s the CIA. We are the good guys”. Redford played the role of a hunted CIA employee in the movie *The Three Days of the Condor* (1973).

⁶² The NSA has long been referred to as “No Such Agency”.

If a large portion of ordinary Internet traffic becomes encrypted with long encryption keys (128-bit, 256-bit or higher), and the time for breaking any message increases correspondingly, such an outcome could put a serious strain on the NSA's interception capability. If one considers the billions of messages that are exchanged every day on the Net in addition to the billions of faxes and phone calls—monitored by the NSA also partially through the Echelon system—it is not surprising that “the intelligence community is stretched thin”, as one knowledgeable observer put it.⁶³

It now appears that the NSA is engaged in a fight against the free use of cryptography for its own survival, and in the process it uses its most valuable asset, i.e. gathered information, to influence both Congress, the Administration and the private sector. In the past, the NSA demonstrated its ability to maintain its edge—or, rather, its quasi-monopoly—winning the battles with the private sector by imposing the 56-bit DES⁶⁴ and almost winning against academia on the question of independent research on cryptography (Bamford, 1983).

Preserving this quasi-monopoly, however, is turning out to be increasingly problematic for the NSA. The hasty and seemingly unstoppable expansion of e-mail, e-commerce, e-trade, e-banking and other “e” activities will pressure the private industry to release more secure encryption software (i.e. longer keys). Unlike the DES case, when relatively few people and institutions needed it, now the massive number of Net users and companies are likely to put up a fierce resistance to the NSA attempt to gain the upper hand. In this struggle, Netizens and users are likely to be actively supported by the software industry that is eager to capitalize on the growing need for secure communications and transactions. Furthermore, as the argument by the private sector goes, if American firms are not allowed to produce and export strong keys encryption software, European software companies less burdened by their national security communities are all likely to outsell American firms in the global market. Recent statements by the Clinton Administration seem to corroborate this point (see section 3.3, 4.2, and 4.6).

Even allowing for the legitimacy of the NSA institutional mission (helping to protect American national security), the evaluations of the agency in two books on the subject are equally discomfoting. Bamford has noted that “[l]ike an ever-widening sinkhole, NSA's

⁶³ I attended the lectures of the anonymous observer at the 20th ISODARCO Summer School, Rovereto, Italy, August 7-17, 1999.

⁶⁴ Bamford has reported, quoting code expert David Kahn (author of “The Codebreakers”), that the DES code should be “...weak enough for the NSA to solve it when used by foreign nations and companies” (1983:347).

surveillance technology will continue to expand, quietly pulling in more and more communications and gradually eliminating more and more privacy” (1982:378). The conclusion reached by Ransom (1970:133) is not different: “[t]he National Security Agency is a symbol of the pervasiveness of technology....[the] NSA is a huge, secret apparatus that bears watching, for it could become ‘Big Brother’s’ instrument for eavesdropping on the entire population if ‘1984’ were ever to come...”.

4.4.2. Congress and Judiciary

A list of the pieces of legislation affecting the Internet before the 106th (1999/2000) Congress includes, among others, the following topics: (1) domain name system; (2) e-commerce; (3) encryption; (4) First Amendment/free speech; (5) gambling; (6) intellectual property; (7) Internet2; (8) privacy (9) spam (Junk e-mail); (10) taxation.

The American public has begun to perceive the Judiciary, and more specifically the Supreme Court, as one of the crucial actors in the struggle over the future of the Internet after the Court’s rejection of the Communication Decency Act (CDA), ratified by Congress on Feb. 8, 1996. In the same year, the Telecommunications Act had been passed—which contained the legal prerequisite for the CDA. According to this law, individuals apprehended while disseminating “indecent” or “patently offensive” material could be fined up to \$250,000 and face two years in prison. The law was the result of a long campaign of pro-family advocate groups—such as the Family Research Council—concerned with the pornographic material widely available on the Net. A particular worry, it was argued, was the fact that the Internet was growing popular with children and teen-agers who might more easily become victims of pedophiles and pornographers.

The CDA was immediately targeted by the American Civil Liberties Union (ACLU). Within the ACLU, many NGOs associated with freedom of speech on-line, such as EPIC, EFF and CDT, were particularly active in emphasizing how the CDA constituted a dangerous precedent that could easily lead to more control on contents exchanged over the Net. Internet technology, it was argued, was “neither good nor bad” since it would ultimately be the individual’s choice, and educating children about actual risks was a parent’s responsibility. Moreover, given the ample availability and effectiveness of filtering software (e.g. Surf Watch),⁶⁵ there was no room to justify infringements of the First Amendment.

⁶⁵ Like any software program, Surf Watch can be rendered ineffective by clever children who often know their computers much better than their parents. Of course, the presence of filtering software does not diminish the

A three-judge court in Philadelphia, which challenged the CDA's compatibility with the First Amendment, had already blocked the application of the controversial law in 1996. After such an outcome, the Supreme Court had to be appealed for a constitutional decision. In June 1997, in "Reno vs. ACLU",⁶⁶ the Court expressed its opinion on the CDA—voting 7 against 2—arguing that some provisions of the federal law amounted to illegal government censorship. In the explanatory opinion of the judgment, Justice John Paul Stevens wrote that the CDA "...applies to a medium that, unlike radio, receives full First Amendment protection...[and] raise special First Amendment concerns because of its obvious chilling effect on free speech".⁶⁷ Thus, the Court's opinion concluded,

...in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproved benefit of censorship.⁶⁸

The Supreme Court ruling on the First Amendment and free speech principles to the Internet has had the far-reaching effect of blocking further similar initiatives in Congress—at least for the time being. The fighting strategy by pro-family advocates has thus become twofold: it has, on the one hand, moved from the Federal to the State level of legislation, since, currently, more than 20 states have fashioned their own laws to regulate Internet speech. On the other hand, these activist groups have tried to render future drafts for federal legislation in Congress more "court-proof".

Actually, the fight over Internet free speech was first resumed by these groups by aiming at public libraries and other public interest places. Indeed, in March 1998, U.S. Senate Commerce Committee approved the (a) "Internet School Filtering Act" (S. 1619), requiring schools and libraries receiving federal "e-rate" Internet subsidies to certify that they are using filtering software and the (b) S. 1482 bill, criminalizing "commercial" material that is "harmful to minors" on the Internet.⁶⁹

The "strategic" legal battle on Internet free speech resumed in February 1999 in Philadelphia where a lower court found that "...the new Internet censorship law would restrict free speech in the 'marketplace of ideas'."⁷⁰ The judge considered evidence that Children On-line Protection Act (COPA) passed by Congress in October 1998 imposed

case for responsible parenting.

⁶⁶ The name with which the case was discussed by the Court.

⁶⁷ http://www.ciec.org/SC_appeal/syllabus.shtml/ (v. November 14 and 15, 1999).

⁶⁸ http://www.ciec.org/SC_appeal/opinion.shtml/ (v. November 14 and 15, 1999).

⁶⁹ <http://rene.efa.org.au/liberty/debategl.html/> (v. November 16, 1999).

⁷⁰ EPIC Alert Volume 6.13 September 1, 1999, available at <http://www.epic.org/alert/> v. November 16 and 17,

technological and economic burdens on speakers, but concluded that ultimately the relevant inquiry is the “burden imposed on the protected speech, not the pressure placed on the pocketbooks or bottom lines of the plaintiffs.”⁷¹ The Justice Department filed the appeals against the court proceeding in April 1999, and this has been pending before the U.S. Court of Appeals for the Third Circuit since.⁷² (see the section on “free speech” for more details).

Moral issues such as whether or not schools and libraries should install filtering programs in their computers to protect children do spark intense debates in Congress, and if controversial bills are passed, the Supreme Court is likely to be called in. However, once drafts for federal legislation of telecommunications issues are submitted for voting in Congress, republicans and democrats tend to have similar voting patterns.⁷³ This phenomenon is further confirmed by the Congressional Internet Caucus Advisory Committee, “...a *bi-partisan* group of over 100 members of the House and Senate working to educate their colleagues about the promise and potential of the Internet”.⁷⁴ The Advisory Committee is also attentive to remind Congress members that “Internet users are voters”, by emphasizing that 78% of Netizens “almost always” vote in national and local elections, compared with 64% of non-users.⁷⁵

1999).

⁷¹ According to EPIC (see previous footnote), many Web sites that carry free information of for the public about fine art, news, gay and lesbian issues and sexual health for women and the disabled may be seriously hampered by the adoption of COPA. The entire text of which is available at http://www.epic.org/free_speech/copa/ (v. October 15 and 16, and November 16 and 17, 1999).

⁷² EPIC Alert, Volume 6.18 November 3, 1999, available at <http://www.epic.org/alert/> (v. November 17, 1999).

⁷³ The diagram presented below summarize the voting patterns of Democrats, Republicans, and Independents in the 106th Congress (House of Representatives).

Sample of Voting Patterns on the Internet and Telecoms-related Issues 1996/1999:

| Bills in Congress | Yes | Nos | Not Voted |
|---|-----------------------|--------------|---------------|
| Moratorium on E-commerce Tax, 1999 | 423 (218R, 204D, 1I) | 1(D) | 9 (3R, 6D) |
| Wireless Communication and Public Safety Act, 1999 | 424 (216R, 207D, 1I) | 2 (R) | 7 (3R, 4D) |
| Satellite Copyright and Consumer Protection Act 1999 | 422 (218R, 203D, 1I) | 1(D) | 9 (2R, 7D) |
| Wireless Privacy Enhancement Act 1999 | 403 (212R, 190D, 1I) | 3 (1R, 2D) | 28 (9R, 19D) |
| Electronic Freedom of Information Amendments Act 1996 | 402 (219R, 182 D, 1I) | | 31 (15R, 16D) |
| Telecommunications Reform Act 1996 | 414 (236R, 178D, | 16 (15D, 1I) | 4 (D) |

Fig.2 (R=Republicans, D=Democrats, I=Independents).

⁷⁴ <http://www.netcaucus.org/> (v. November 19, 20, 21, 22 and 23, 1999).

⁷⁵ <http://www.netcaucus.org/statistics/whovotes.jpg> (v. November 19, 20, 21, 22 and 23, 1999). Of course,

Such outcomes indicate that although Congress tries to meet the demands voiced by the various interests groups, the majority of Congress members are also fully aware of the importance of the Internet and of telecommunications in general to create the “information economy” as well as of Netizens’ political prowess. In fact, almost rivaling the multiplicity of government actors, more than one Senate and House Committees claim jurisdiction on various aspects of the Net; that is, Judiciary, Foreign Policy, National Security, and Commerce, to name a few. This attitude of Congress helps to explain why—despite the traditional attention and consideration that is usually attributed to issues concerning “national security” by Congress—thus far, the national security and law enforcement communities have failed to convince Congress to pass more restrictive federal legislation to control the use of the Internet.

4.4.3 *The Industry*

The U.S. ICT industry is another powerful player in the battle for Internet control, and its “battle cry” for the electronic marketplace is “thank you, we do just fine without too much government”.⁷⁶ This position has inevitably led to an “unofficial” (certainly accidental) alliance with the next player on the list, namely the collection of pro-liberties NGOs, users’ groups and consumers’ organizations. These two actors have come together, inadvertently, because of their overlapping concern in limiting government’s interference on the Net.⁷⁷ In doing so, they have formed a considerable obstacle for the national security community trying to insist on greater government power in controlling the Internet.

In the continuing struggle between governments and the private sector for the “commanding heights” of the economy (Yergin and Stanislaw, 1999), the swing is currently in favor privatization and government disengagement. This occurrence has contributed to fending off more determined efforts by the government to consider the Internet as a “strategic” utility, just as the telecoms or electricity at the start. Had the Internet emerged as a communication and information medium in the 1960s or ‘70s, the U.S. government—and

numbers pertaining to the Net should always be taken carefully. For a highlight on survey methods and related problems on and about the Net see for instance <http://www.wired.com/news/politics/0,1283.33800.00.html> (v. January 30, 2000).

⁷⁶ Given the traditional suspicion of the Republicans toward “too much government”, and several statements made by the republican presidential candidate before the 2000 elections, it is likely that the Bush Administration, overall, will encourage this attitude.

⁷⁷ Clearly different players give their primary attention to different agencies or government bodies. For instance, privacy NGOs are concerned with the FBI or the NSA, while private businesses can be more concerned with regulating authorities. All in all, however, all these players tend to view government intervention quite suspiciously, regardless of the area or issue in which the federal government intrudes.

many other governments worldwide—would have regarded the Net as one of those assets that only governments can efficiently own, manage, or, at least, supervise. The whole debate about controlling the Net, probably, would have not even happened.

In the last 30 years, the share of services contribution to GNP has constantly grown, now accounting for roughly 2/3 of it. Within this share, the telecommunication and computer industries—along with the entertainment industry that, incidentally, has increasing interests in the Internet development—have become predominant. Indeed, as a study of the University of Texas has shown, the size of the Internet Economy (over 301 billion USD in 1999) rivals that of century-old and more established industries such as automobiles (\$350 billion), telecommunications (\$270 billion) and energy (\$223 billion) (see section 4.6).⁷⁸ If the value of the telecom sector is added to that of the Internet Economy, the impressive sum of \$571 unmistakably marks them as the present “crown jewels” of the American economy.⁷⁹

Given the magnitude of wealth considered, it is not surprising that the professional associations representing information and communication technology (ICT) companies enjoy considerable credit with the federal government and Congress alike.⁸⁰ Three of the most prominent industrial associations, for instance, are the Information Technology Industry Council (ITIC)—whose members include Microsoft, America on Line (AOL), Cisco Systems, Sony, Apple, 3Com, Panasonic, IBM, etc.—, the Internet Alliance, and the Telecommunication Industry Association (TIA). Many companies have multiple membership: Microsoft, AOL and IBM are with the ITIC and the Internet Alliance at the same time, while Cisco and 3Com are with the ITIC and the TIA. TIA itself, for instance,—an organization with a membership of 1000 large and small information technology products—claims that the association's member companies manufacture or supply virtually all of the products used in global communication networks.⁸¹

As meaningful illustrations of the involvement of the private sector in the policy-making process, it is worth addressing the reports and statements prepared by these trade

⁷⁸ Center for Research in Electronic Commerce, University of Texas at Austin, “Measuring the Internet Economy”, (<http://cism.bus.utexas.edu/> v. December 2, 3 and 4, 1999). Thanks to a thoughtful and reliable methodology, this study appears to be among the first analyses that provide convincing evidence for these assertions.

⁷⁹ The number provided by the Telecommunication Industry Association is lower (517.6 billion USD) but still considerable (http://www.tiaonline.org/pubs/press_releases/1999/99-150.cfm v. December 9 and 10, 1999)

⁸⁰ E.g. the American Mobile Telecommunications Association (AMTA), the American Electronics Association (AEA), the Software and Information Industry Association (SIIA), etc.

⁸¹ <http://www.tiaonline.org/about/overview.cfm/> (v. December 9 and 10, 1999).

associations on various Internet issue-areas. On the crucial case of cryptography, for example, the position of TIA is that:

[t]elecommunications equipment manufacturers should be proactively represented and included in any effort to deregulate encryption technology...TIA should provide input to ensure that telecommunications equipment receives favorable treatment in any decision on encryption...[and] take a proactive, educational role in representing telecommunications manufacturers in encryption legislation and regulatory matters...[finally] Government regulation of encryption used for telecommunications purposes should be minimal...⁸²

The IA, on the other hand, "...will work to communicate to policymakers and consumers alike that encryption is fundamental for privacy in personal communications, privacy in shopping, and privacy for individual's health care needs".⁸³ Finally, ITIC has "...a direct interest in identifying and providing solutions, including a variety of technical solutions, to protect the privacy of all users and customers, both online and off".⁸⁴

Another issue commanding considerable agreement is industry self-regulation.

About this, TIA has remarked that:

[t]he setting of international standards is best left to the private sector. Most of the standards for the information superhighway or cyberspace have been set through the private standards setting process with little or no involvement by any level of government. These standards have been driven by marketplace considerations, such as the need to bring products to market or meet customer demands. The role of governments in successful standards setting mechanisms is diminishing and will probably continue to decline. Governments, hindered by their slower decision-making processes, cannot keep pace with the private sector international standards setting process in dealing with the ever escalating rapidity of technological change.⁸⁵

ITIC, on the other hand, "...is a strong advocate of private sector leadership in establishing a self-regulatory program for the protection of privacy, complemented by appropriate governmental enforcement of privacy-related laws."⁸⁶ Finally, the IA believes that:

...industry-led initiatives to protect consumers' privacy in the Internet online world is the most effective means to address privacy concerns. In the coming year, the IA will assert an industry lead on this issue by promoting industry self-regulation [and]...supporting the industry's efforts to self-regulate and to building the broadest possible coalitions to achieve this goal.⁸⁷

From these short excerpts it can be easily determined how substantial agreement exists among the main professional associations of the telecom and computer sectors;

⁸² <http://www.tiaonline.org/government/encryption/> (v. December 11 and 15, 1999).

⁸³ http://www.internetalliance.org/policy7_core_issues.html#consumer/ (v. December 17, 1999).

⁸⁴ http://www.itic.org/iss_pol/index.html/ (v. December 20, 1999)

⁸⁵ <http://www.tiaonline.org/government/encryption/> (v. December 11 and 15, 1999).

⁸⁶ http://www.itic.org/iss_pol/index.html (v. December 20 and 21, 1999).

⁸⁷ http://www.internetalliance.org/policy7_core_issues.html#consumer (v. December 17, 1999).

namely, backing for unrestricted use and export of encryption software for privacy and e-commerce, avoidance of content control, and resolute support for industry self-regulation. Common ground for understanding and cooperation with Internet NGOs is unequivocal, and has been instrumentally capitalized on by both parties for their functional goals.

4.4.4. *NGOs and Private Groups*

Given the Internet's nature and its historical development, it is not surprising that a considerable number of non-government organizations have flourished, tackling many important civil liberty issues related to the diffusion and use of the Net. Questions such as privacy, cryptography, security, and hackers' ethics are a few of the topics on which most of these organizations normally work. The most important ones are presented hereafter.

The American Civil Liberties Union (ACLU) is the oldest (1920) civil liberties NGO as well as "...the nation's foremost advocate of individual rights—litigating, legislating, and educating the public on a broad array of issues affecting individual freedom in the United States".⁸⁸ ACLU's main mission is "to defend" the Bill of Rights that includes, among others, freedom of speech and right to privacy. In this respect, ACLU has been active on these issues along with other Internet NGOs. However, ACLU activities are not limited to the Internet, but extend to other non-Internet related topics such as prisons, racial equality, workers' rights, etc.⁸⁹

The first Internet-specific organization has been the EFF, the Electronic Frontier Foundation, "...a non-profit, non-partisan organization working in the public interest to protect fundamental civil liberties, including privacy and freedom of expression, in the arena of computers and the Internet."⁹⁰ The EFF was founded in 1990, specifically "to encourage computer-based communications", "...to ensure that the principles embodied in the US Constitution and Bill of Rights (and the UN Universal Declaration of Human Rights) are protected as new communications technologies emerge", and to represent the interests of "Netizens" in general.⁹¹

Chronologically after EFF, the Internet Society (ISOC), founded in 1991—"...by a worldwide cross-section of individuals and organizations who recognized that the Society

⁸⁸ <http://www.aclu.org/library/pbp1.html> (v. January 4, 2000).

⁸⁹ To defend *the right* of people to free speech, ACLU has also made cases for the Ku Klux Klan and neo-Nazi groups.

⁹⁰ http://www.eff.org/EFFdocs/about_eff.html (v. January 7 and 8, 2000).

⁹¹ http://www.eff.org/EFFdocs/about_eff.html (v. January 7 and 8, 2000).

was a critical component necessary to evolve and globalize the Internet..."⁹² —has enjoyed a special place in the history of the Internet. In fact it was the result of the joint efforts of the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB), the two groups primarily responsible for the Net infrastructure—IETF and IAB included most of the scientists that had actually built the Net. ISOC now gathers more than 150 organizational and 6,000 individual members in over 100 countries, and has set as its primary mission to provide "...leadership in addressing issues that confront the future of the Internet..."⁹³

More recently, the Electronic Privacy Information Center—a public interest research center—was established in 1994, through the transformation of the Washington-based office of the Computer Professional for Social Responsibility (CPSR).⁹⁴ EPIC focuses public attention on emerging privacy issues such as the Clipper Chip, the Digital Telephony proposal, national ID cards, medical record privacy, and the collection and sale of personal information, as well as on cryptography policy and free speech.⁹⁵ EPIC is sponsored by the Fund for Constitutional Government—a non-profit organization established in 1974 to protect civil liberties and constitutional rights—and private donations. No corporate members are chartered.⁹⁶ Concrete actions by EPIC include the publication of the EPIC Alert newsletter, the pursuing of Freedom of Information Act litigation, and management of policy research.

Also based in Washington, DC, the Center for Democracy and Technology (CDT) "works to promote democratic values and constitutional liberties in the digital age...[and] is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media".⁹⁷ CDT's work concentrates on creating awareness in the public and Congress about free speech, data privacy, cryptography, and wiretapping, etc, and it publishes its own newsletter (CDT Policy Post). Financial support to CDT is provided

⁹² <http://www.isoc.org/isoc/general/> (v. January 10, 2000 and several other times). Among the founding members were Microsoft, MCI, IBM, Oracle, Compaq, 3Com, ATT, AOL, RAND and the DOD Defense Information Security Agency (DISA).

⁹³ <http://www.isoc.org/isoc/> (v. several times between 1999 and 2001)..

⁹⁴ The CPSR has been one of the first American NGOs concerned with the developments of growing reliance on computing power by the U.S. military. Since its inception (1981), CPSR has pursued this goal, becoming also more and more involved with the future of computer networks (<http://www.cpsr.org/> v. several times in January, February and April, 2000).

⁹⁵ EPIC surveys on cryptography and privacy have been used in my quantitative analysis as proxy indicators for the dependent variable, i.e. levels of control.

⁹⁶ EPIC proudly states that it has "no clients, no customers, and no shareholders" (<http://www.epic.org/#about> v. January 20, 2000).

⁹⁷ <http://www.cdt.org/mission/> (v. January 20 and 22, 2000).

by private as well as corporate donors—including, among others, AOL, ATT, Bell, Disney, IBM, Lotus, MCI, Microsoft, Netscape and Time Warner.

One of the principal organizations for consumers' protection is the National Consumers League (NCL), the oldest nonprofit consumer organization in the United States, which, in 1992, set up the National Fraud Information Center and, in 1996, the Internet Fraud Watch.⁹⁸ The Center's goal is "...for consumers to get advice about telephone solicitations and report possible telemarketing fraud to law enforcement agencies". The Internet Fraud Watch was created to offer consumers advice about promotions in cyberspace and route reports of suspected online and Internet fraud.⁹⁹ Other examples of consumers/users' groups and organizations are the Domain Name Right Coalition (to counter ICANN abuses),¹⁰⁰ the Digital Future Coalition,¹⁰¹ the Cypherpunks (hosted by the UC Berkeley),¹⁰² the Center for Media Education,¹⁰³ or the Open Source Initiative (which is also an international organization),¹⁰⁴ and many others.¹⁰⁵

With minor differences, all the NGOs and organizations described here are concerned with topics such as free speech, on-line privacy, free use of cryptography, consumers' protection and, in general, the government's presence on the Internet. These, along with two other critical issues, i.e. the e-economy and the National Information Infrastructure, constitute the main themes of the debate on the future of the Internet and are the subjects of the following section. The main goals of these organizations and groups are the gathering and dissemination of technical/legal information, and the building up of support in the public opinion for their activity. It is clear how the overlapping, vested interests of civil liberties and consumers' organizations, and users' groups and the ICT industry for a "government-free" Internet have triggered cooperation and joint action. Furthermore, several of these groups have international links. For instance, the complexity of Internet issues and the growing number of Netizens have prompted EFF, ISOC, EPIC,

⁹⁸ <http://www.fraud.org/info/aboutnfic.htm> (v. March 20, 2001).

⁹⁹ The NCL (<http://www.natconsumersleague.org/>) has also founded the Alliance Against Fraud in Telemarketing and Electronic Commerce (<http://www.fraud.org/aaft/aaftinfo.htm> v. March 20, 2001).

¹⁰⁰ <http://www.netpolicy.com/dmainindex.html> (v. March 20, 2001).

¹⁰¹ Which is "...committed to striking an appropriate balance in law and public policy between protecting intellectual property and affording public access to it" (http://www.dfc.org/dfc1/Learning_Center/about.html , v. March 20, 2001).

¹⁰² <ftp://ftp.csua.berkeley.edu/pub/cypherpunks/Home.html> (v. March 20, 2001).

¹⁰³ <http://www.cme.org/> (v. March 20, 2001).

¹⁰⁴ <http://www.opensource.org/index.html> (v. March 20, 2001).

¹⁰⁵ As Alexis de Tocqueville correctly noted, belonging to and founding associations is part of the American culture.

and CDT (and others) to create the Global Internet Liberty Campaign (GILC),¹⁰⁶ a transnational coalition to better coordinate their efforts. Thus, organizations such as these have become crucial actors in two-level games that governments have inevitably to play when tackling Internet control.

4.5 Current Issues of the Internet Debate

For a long time, the main coupling between national security and the Internet has been to prevent young pranksters—trying to imitate Matthew Broderick's character in the fiction movie *War Games* (1983)—from intruding into classified computers. This setting changed considerably with the popularization and internationalization of the Internet, opening up numerous areas of confrontation between “controllers” and “libertarians”. In this section, I will illustrate the current state of the controversies, the complexities of the U.S. case, and the representation of competing interests. Indeed, the topics debated here are “classical issue-areas;” that is, different actors/elites are involved depending upon the issue at stake, although the juxtaposition between the accidental alliance, and the national security/defense group can easily be identified throughout all these topics.

In the previous section I have described two of the most important players within the federal government, namely the FBI and the NSA that, to some extent, symbolize the “law enforcement” and the “national security” communities. Traditionally the two communities are supposed to operate separately - one inside, and the other outside the borders of the United States. However, as Diffie and Landau have noted (1998:121), “...at times...the distinction has been blurred”. Although most of the evidence is classified, thus inaccessible, it appears that the distinction is harder and harder to preserve.¹⁰⁷ For instance, according to Diffie and Landau, the Intelligence Authorization Act of 1997 while “[steering] clear of permitting [spying] on Americans directly, ...opens the way for unprecedented collaboration between the intelligence and law-enforcement communities” (1998:123).

Since the technical nature of the Net makes it rather problematic to distinguish between “domestic” and “foreign” flows of information, it is only logical to expect an overlapping of competencies and thus greater cooperation between the two communities. Actually, the other side as well, namely the “anti-government” alliance, has seen patterns of

¹⁰⁶ <http://www.gilc.org/> (v. January 23, 2000).

¹⁰⁷ It seems almost paradoxical that one of the chief agents responsible for such an outcome is the current Democratic Administration.

collaboration. In some cases, this has resulted in “strange bedfellows,” like, as mentioned earlier, civil liberties organizations and right wing movements (i.e. the “brown-red alliance”) and big corporations.

Despite these criticisms, however, the case presented by the NSA and the FBI has won remarkable ground in the Clinton Administration (e.g. CALEA, CDA, COPA, *Carnivore*, etc.), which, overlooking the first decade of the mass diffusion of the Internet, has had considerable influence on the future development of the Net. For instance, the August 1999 federal government initiative for the Cyberspace Electronic Security Act (CESA), if passed, could, according to EPIC,

...result in an unprecedented intrusion into the sanctity of private homes and businesses... [since it] would enable federal and local law enforcement agents to secretly break into private premises and alter computer equipment to collect e-mail messages and other electronic information.¹⁰⁸

Where encryption keys cannot be obtained by “recovery agents” (e.g. banks), law enforcers would be allowed to enact covert police entries into homes and offices to acquire the keys, while courts would be able to endorse such actions. More specifically, the CESA would

...ensure that law enforcement maintains its ability to access decryption information stored with third parties,...authorize \$80 million over four years for the FBI’s Technical Support Center,...protect sensitive investigative techniques and industry trade secrets from unnecessary disclosure in litigation or criminal trials involving encryption...¹⁰⁹

Finally, as if to confirm the main thesis of this work, in August 1999, at the same time the federal government was circulating the draft for CESA, the President’s Export Council Subcommittee on Encryption (PECSENC) (an advisory body) recommended that the Administration should substantially revise its restrictive stance on the export of encryption products. Notwithstanding the fact that PENSEC’s subcommittee chairman was William Crowell— a former Deputy Director for the National Security Agency—and that other members had links to the intelligence and security communities, “...the subcommittee cited a need for the U.S. government to ‘recognize market realities’ and reverse its course on encryption policy.”¹¹⁰

Among PENSEC recommendations were (a) “License-Free Zones” (i.e. a list of countries which do not pose any major terrorist threat, and allow encryption export without

¹⁰⁸ Epic Alert, Volume 6.13 September 1, 1999 available at <http://www.epic.org/alert/> (v. October 15, 16 and November 9, 1999)

¹⁰⁹ <http://www.bxa.doc.gov/Encryption/whpr99.htm/> (v. November 10, 1999).

¹¹⁰ Epic Alert, Volume 6.13 September 1, 1999 available at <http://www.epic.org/alert/> (v. October 15, 16 and

a license),¹¹¹ (b) “On-Line Merchants” such as banks and financial institutions based in other countries should be permitted to have access to strong encryption products from the United States, (c) “Mass-market hardware and software products” which utilize up to 128-bit key length triple DES should also enjoy a license exception, (d) the elimination of cumbersome reporting requirements for manufacturers of encryption products.

Since the Internet has the capability to dramatically transfer control to the user—and is already doing that today—this raises innumerable questions: e.g. who makes decisions? Is it always the user? What about children? When and how should they be allowed to make individual choices? At what age? Besides illegal content, which raises different questions, what information should be considered inappropriate for children? How can information be identified inappropriate? And how about a government role—given the global nature of the Internet, what courts and what standards will be involved in making decisions?¹¹²

Not all the issue-areas presented in this section have the same impact on ordinary users. In deciding the order of presentation of the different issues, for instance, it is no coincidence that the “free use of cryptography” comes right after “privacy”, since the latter is impossible in on-line communications without the former. The digitalization of communications has almost made “cryptography” a synonym for “privacy”, even though the results of the quantitative analysis of chapter three have shown that there is more to the concept of privacy than just communications. The correct use of information in databases is perhaps even more crucial for protecting privacy than whether or not some information is monitored during the communication process. However, many individuals have little control or influence on information legally stored in databases held by private companies or law enforcement agencies, or to whom a bank can transmit its borrowers’ credit rate or personal data.¹¹³

Finally, this state of affairs is likely to further deteriorate if, as Adrian Wooldridge of *The Economist* has written, “[mobile] phones and computers are about to converge, putting the Internet at your fingertips, anywhere” (1999:10). However, mobile phones “...are enemies of personal privacy” (Wooldridge, 1999:36), since they are so easy to tape. As the number of people who also use mobile phones for Internet applications increase, so

November 10 and 11, 1999)

¹¹¹ In this respect, the attitude of the EU—considerably reducing the limits to export—was considered by the committee as the criterion to follow.

¹¹² <http://www.netcaucus.org/issues/contentoverview.html> (v. January 27, 2000)..

¹¹³ Prof. Frankel emphatically remarked to me how “in the United States, borrowers have no rights” (Frankel personal interview).

will the chances of casual or illegal or unjustified wire-tapping, and so will the demand for stronger encryption software. In conclusion, “[d]igital technology has aided communications, but it has also given rise to the possibility of those communications being monitored” (Singh, 1999:297).

4.5.1. Freedom of Speech

Freedom of speech in the United States is directly protected by the First Amendment, hence, for a considerable time, threats to freedom of speech on the Net have never even been considered a problem. In fact, the community of engineers and scientists that contributed to building the Internet regarded the freedom to express divergent views and criticisms as one of its most valuable assets. Any attempts to raise profits from any product—as the University of Minnesota did in 1993 with its gopher—was seen as an act of treason in the academic and the Internet communities (Berners-Lee, 1999). Quite soon, this general attitude was turned upside down, as more and more private businesses discovered the Net’s commercial advantages.

Freedom of speech *per se* is not an indispensable ingredient of commercial activity—as demonstrated, for instance, by the flourishing of commercial transactions under authoritarian regimes. After the “privatization” of the Net in 1995,¹¹⁴ and the increasing presence of the private sector on the Internet, the risk of a growing irrelevance of on-line free speech has become evident to Netizens and scientists alike. However, this scenario has not unfolded in the United States. On the contrary, perhaps recognizing the special sensitivity of many users—and potential customers—to this issue, the American software and telecommunications industries have sided with civil liberties organizations in defending on-line freedom of speech and demanding less government interference on the Internet.

The battle over free speech on the Net resumed in 1999, after the backlash suffered by pro-family groups in 1997 when the CDA (ACLU vs. Reno) was judged unconstitutional under the First Amendment by the Supreme Court. The Child On-line Protection Act (COPA)¹¹⁵ was passed by Congress in October 1998, and challenged again in 1999, about COPA violation of the First Amendment. The legal dispute furthermore became known as

¹¹⁴ When the National Science Foundation stopped the funding of NSFNET, heir of ARPANET, and then the main backbone of the Internet.

¹¹⁵ In the same budget bill, Congress also approved the Child On-line Privacy Protection Act (COPPA, not to be confused with COPA) that requires parental consent to collect information on the Web about children less than 12 years old.

CDA II or ACLU vs. Reno II, thus linking the two acts together as major threats to on-line freedom of speech.

As one of the judges embroiled in the COPA dispute said,

[t]wo diametric interests—the constitutional right of freedom of speech and the interest of Congress, and indeed society, in protecting children from harmful materials—are in tension in this lawsuit....However, the Court is acutely cognizant of its charge under the law of this country not to protect the majoritarian will at the expense of stifling the rights embodied in the Constitution.... Indeed, perhaps we do the minors of this country harm if First Amendment protections, which they will with age inherit fully, are chipped away in the name of their protection.¹¹⁶

In the opinion of the lower court, COPA has been declared likely to be found unconstitutional if challenged before the Supreme Court; therefore is not being enforced. As with the CDA, this is a temporary interval, certainly not the end of the struggle over freedom of speech on the Net. In fact, several bills have already been introduced in Congress mandating the use of filtering software in schools and libraries receiving federal funding, such as the Juvenile Justice Bill (HR 1501).¹¹⁷ Along the same lines, other bills that require public schools and libraries that receive federal funds to install software to protect children from obscenity were introduced before the 106th session of Congress.¹¹⁸ The only one that was approved in December 2000 was the Children's Internet Protection Act (CIPA),¹¹⁹ which was immediately challenged before a federal court (March 2001).

Cases like CIPA, CALEA or *Carnivore* (an FBI-designed computer program to intercept Internet communications), and many others, sketch out quite clearly who the opposing parties are with regard to freedom of speech. On the one side, there is the federal and local law enforcement machinery, which, ideally, would prefer instant recovery of any type of individual communications, and a bipartisan combination of Congress members, who aim to show their constituencies that they take Children's safety seriously. On the other side, there are pro-liberties NGOs, which include, among others the ACLU, and often the prominent American Libraries Association and local libraries. Their goal is to block in court any initiative that can undermine the First Amendment and create precedents. The awkward spin-off of this policy is that racist and hatred Web sites cannot be banned or stopped on legal grounds. These circumstances are obviously unacceptable for Germany and Italy and

¹¹⁶ Judge John Reed, Memorandum, District Court, for the Eastern District of Pennsylvania (http://www.epic.org/free_speech/copa/pi_decision.html) v. January 27, 2000).

¹¹⁷ The Juvenile Justice bill contains an amendment that eliminates "e-rate" discounts for libraries and schools that do not implement filtering or blocking technology on computers with Internet access. At <http://www.cybertelecom.org/legis106.htm> (v. January 28 and 29, 2000)..

¹¹⁸ http://www.cdt.org/publications/pp_5.27.shtml (v. February 1, 2000).

their citizens. Consumers' organizations, the private sector and defense and intelligence agencies are only mildly involved in this issue, although the latter are concerned with the availability of terrorist propaganda.

4.5.2. Privacy

The approach to privacy could not be more different in the EU and in the United States: in the former information gathered by companies on individuals belongs to those individuals, while in the latter it becomes property of the company. On the other hand, while in the EU the goal is to defend the public from information misuse in the private sector, in the United States the focus is on safeguarding individuals from government's misuse of information.

In the United States, “[t]here is no explicit right to privacy in the U.S. Constitution...[and] no comprehensive privacy protection law for the private sector...[and] no oversight agency...[although a] patchwork of federal laws covers some specific categories of personal information” (EPIC, 1999:163/164). Despite that, “[p]rivacy plays a unique role in American law...[and is] considered a core value by most citizens...” (Cavazos and Morin, 1995:13), yet, “...laws that protect consumers from having their information resold or given away are very weak” (Berners-Lee, 1999:146).

As in other advanced democracies, surveillance of individuals for criminal investigation is strictly governed by federal laws, e.g. the Electronic Communication Privacy Act of 1986. The information-gathering capability of the intelligence community is well-known and impressive, and abuse and malpractice appears to be within the norm in democracies. Furthermore, most intelligence agencies cannot operate domestically and prefer to display their aptitude towards foreign communications.

Yet, the American public does appear to be more and more concerned about the progressive loss of its privacy and growing intrusion by the federal government. In September 1999, a Wall Street Journal/NBC News poll found that, at the beginning of the twenty-first century, the loss of personal privacy was the first concern of American citizens. “When asked what concerns them the most about the next century, twenty-nine percent of respondents answered the ‘loss of personal privacy,’” surpassing topics such as terrorist acts on U.S. soil or racial tensions.¹²⁰ In another survey, “...52% of the respondents answered

¹¹⁹ <http://www.ifea.net/cipa.html> (v. March 21, 2001).

¹²⁰ The Wall Street Journal/NBC News poll was based on nationwide

that government agencies were their greatest worry, while 40% said business."¹²¹ Finally, a Business Week/Harris Poll (conducted in 1998 and 2000) has shown that, among all the common means of communications, interviewees have expressed the highest concern for e-mail security as well as for increased on-line privacy protection.¹²² In fact, although in the United States there are over 500 commercial databases, "[d]ata collection by the US government dwarfs that by private enterprise" (Diffie and Landau, 1998:137).¹²³

Some major privacy bills, which, for instance, prohibit an interactive computer service from disclosing to a third party any personally identifiable information provided by a subscriber without the subscriber's informed written consent or that require the FTC to prescribe regulations to protect the privacy of personal information collected from and about private individuals who are not covered by the COPPA of 1998, have been presented before Congress. Americans are indeed more concerned with their privacy, and that attitude is reflected in Congress.

Even President Clinton, in his last State of the Union speech in January 2000, speaking of the most recent breakthroughs in advanced technologies, stated that "[f]irst and foremost, we have to safeguard our citizens' privacy."¹²⁴ Yet, despite all this concern, and the array of bills in Congress, there is no provision for a major privacy protection law or for a "European-style" agency.¹²⁵ With the other notable exception of medical information, only children's privacy enjoys specific protection through the Children's On-line Privacy Protection Act (COPPA) that was approved by Congress in the same bill that contained

telephone interviews of 2,025 adults. Reported in EPIC Alert Volume 6.15 September 24, 1999, available from <http://www.epic.org/alert/> (v. October, November, and December 1999, and January, February and March 2000).

¹²¹ Center for Social and Legal Research, *Privacy in American Business*, p.7, quoted in Diffie and Landau (1998:136). For a very detailed and informative Web site about surveys done by different organizations see, for instance, <http://www.cdt.org/privacy/survey/findings/surveyframe.html> (v. February 1 and 5, 2000).

¹²² The poll is entirely available at http://www.businessweek.com/2000/00_12/b3673010.htm (v. February 2, 2000).

¹²³ Federal agencies support 910 major databases (General Accounting Office, 1990, quoted in Diffie and Landau, 1998:137). With regards to the Internet, however, it seems that the private sector will rapidly close the gap. In fact, Double Click, an Internet advertising company may have tracked as many as 90 million U.S. households, mostly through "cookies". Furthermore, Double Click plan to match this information with data from other sources to create more precise customers (matching names with commercial preferences) profiles that could be "sold" to third parties. (Christopher Chiu, GLIC Alert, February 22, 2000, vol.4, n.2, cchiu@aclu.org). EPIC filed a public complaint against this plan and on March 2, 2000 Double Click announced its intention to abandon the plan

(http://www.doubleclick.net/company_info/press_kit/pr.00.03.02.htm and http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf v. February 22 and 23, 2000).

¹²⁴ <http://www.whitehouse.gov/WH/SOTU00/sotu-text.html> (v. February 27, 2000).

¹²⁵ "Privacy" is definitively culture-specific, as the differences among Europe and the United States show, including the dispute on how American companies should behave with regards to the treatment of personal data of Europeans, given the EU Directive on Personal Data Protection, entered in force October 1998 (Directive 97/66/EC).

COPA in October 1998.¹²⁶ At the time of this writing, the White House and the private sector believe that, for all other individuals, self-regulation is sufficient (GILC/EPIC, 1998:81, and Berners-Lee, 1999:146). Finally, after two years of negotiations, to meet the requests made by the EU that American companies comply with the EU Directive on Data Protection, the DOC has launched in 2000 the “safe harbor” proposal, under which American companies may voluntarily accept to adhere to the EU guidelines.¹²⁷

The privacy issue also delineates quite well who the main actors are. Stronger privacy protection implies greater obstacles in the activity of law enforcement and counterintelligence agencies, which do not see that option very favorably. Moreover, some companies are dubious about adopting EU privacy standards that may hinder their traditional business practices.

On the other hand, pro-liberties NGOs, consumers’ organizations and users’ groups are all unquestionably in favor of greater privacy protection.¹²⁸ Furthermore, many companies, including several of the most important, although still circumspect about the “safe harbor” idea, have recognized that offering greater guarantees for privacy can become a quality service that may attract consumers and help secure their loyalty.¹²⁹ Finally, several of those NGOs, consumers’ and users’ organizations have international ties. This fact and the whole question of “safe harbor” and EU privacy standards make it inevitable that the U.S. and EU governments will engage more and more in a two-level game about Internet privacy.

The main technical reason why there is such a grave lack of privacy on the Internet is that the TCP/IP traffic—the “blood” of the Net—is fully “in clear”. It is evident how the issue of free use of strong-key cryptography has become so paramount in the debate about Internet privacy, security of commercial transaction and statutory control.

¹²⁶ COPPA requires Web sites to get parental consent from visitors age 12 and under before using their personally identifiable information for any secondary purpose, while COPA (Children’s Online Protection Act) created a national “harmful to minors” standard for speech on the Internet. I am grateful to Ari Schwarz (ari@cdt.org, March 13, 2000) of CDT for clarifying the differences between COPA and COPPA (at http://www.cdt.org/publications/pp_5.27.shtml). Andrew Shen of EPIC (shen@epic.org, March 14, 2000) noted that “this is a very common problem in the Internet policy world.”

¹²⁷ The most recent version of the “safe harbor” proposal is available at <http://www.ita.doc.gov/td/ecom/menu1.html> (USA v. March 14 and 15, 2000) and http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm (EU v. March 14 and 15, 2000).

¹²⁸ In 2000, the National Consumer Association found that American on-line consumers are more concerned about privacy than health care, crime or taxes. (<http://www.natlconsumersleague.org/pressessentials.htm> v. March 21, 2001).

¹²⁹ In 2000, when the on-line company eToy failed, and had to sell its customers list (which contained names of parents and children, and credit card numbers), considerable concern arose within the public opinion. In the

4.5.3 Free Use of Cryptography

The free use of cryptography is one of the most controversial issues surrounding the Internet. If cryptography is fundamental to guarantee privacy on-line, it means that everyone—law-abiding citizens and criminals or terrorists alike—will be protected by using it. The U.S. government is torn between law enforcement (particularly the FBI) and national security communities (i.e. the NSA) on the one side that would like to maintain the *status quo*, and the civil libertarians (such as EPIC, EFF and CDT) who argue that, since privacy is a fundamental human right,¹³⁰ and cryptography is essential to safely communicate in a networked environment, there should be no restrictions on its availability and use. As mentioned at the beginning of this section, in this struggle the civil libertarians are joined by representatives of right wing movements (who are wary of any government action) and, more importantly, the private sector, including the big software and telecommunications companies.

Thanks to the Internet, after 1995, "...the market for cryptography has exploded" (Diffie and Landau, 1998:47). Internet commercial potential has indeed boosted the demand for strong cryptography. However, until 1996, cryptographic software produced in the United States could not be freely exported. In fact, it was required to be licensed and compared to "ammunitions" on the International Traffic in Arms Regulation managed by the DOD. In this respect, the case of encryption software application PGP (Pretty Good Privacy) is a meaningful example.

In June 1991, Phil Zimmerman, a long-time civil liberties activist, posted PGP ver.1 on a bulletin board on the Usenet—one of the networks of the Internet.¹³¹ Zimmerman had been developing PGP for years with a combination of DES-like symmetric and RSA asymmetric encryption algorithms, polishing that advanced piece of software with a user-friendly interface. As downloads of PGP grew, in February 1993, Zimmerman found himself under federal investigation for illegal export of a "weapon." The investigation lasted for three years and "...ignited a debate about the positive and negative effects of encryption in the Information Age. The spread galvanized cryptographers, politicians and civil libertarians and law enforcers into thinking about the implications of widespread encryption" (Singh, 1999:303).

What happened then is effectively described by Diffie and Landau (1999:206):

end, Disney bought the list and destroyed it to show that it cared about children' and parents' privacy.

¹³⁰ Article 12 of the Universal Declaration.

¹³¹ Zimmerman actually asked a friend to do so (Levy, 2001:197).

The MIT Press, with its thumbs firmly in its nose, published the code of PGP as a 600-page hardbound book...,and sold it through its usual worldwide distribution channels. Had the government prosecuted Zimmerman and not MIT, it would have invited scorn. But the MIT is three times as old as the NSA, just as well funded, and even more influential in the military-industrial complex.

Thus, in 1996, the U.S. the Attorney General's Office dropped the charges. The main direct consequences of this investigation were that Zimmerman became incredibly popular and was supported by an international fund for his legal expenses and, most of all, PGP turned into being one of the most frequently downloaded software programs from the Internet—"if the *feds* are scared, it must be really good!!" The U.S. government's action had indeed alerted a vast audience about the benefits of encryption and the risks of government control of on-line communications.

Another important, albeit less known outside the United States, case has been *Bernstein vs. the DOJ*.¹³² DOC regulations restricting the export of encryption products were challenged in 1995 by Daniel Bernstein, a computer science professor of the University of Illinois. Bernstein argued that computer source code is a form of speech and therefore not subject to censorship, while the U.S. government maintained that the code was more functional than an expression of ideas. In May 1999, the U.S. Court of Appeals for the Ninth Circuit ruled that U.S. controls on the export of encryption software violate the First Amendment. EPIC defined the outcome "...a long-awaited landmark decision...,"¹³³ but the controversy is still far from settled even under the latest liberalization rules announced in September 1999—and specified in January 2000 (see further, *ftn. 128*).

While the Zimmerman case was unfolding, the government, aware of the growing and more composite opposition to curbing the freest use of encryption software, proposed basically two desirable solutions, namely the "Clipper Chip" and the "Key Management/Key Recovery." The "Clipper" was a microcircuit "...that could be attached to an ordinary telephone....to protect private communications while permitting law enforcement officials to circumvent encryption devices that they claimed were hampering their ability to detect criminal activity."¹³⁴ The "Clipper" used a "key escrow" system; that is, two keys would be stored separately with two government agencies chosen by the Attorney General. This solution was highly criticized by civil liberties NGOs because it "[f]ailed to protect privacy rights of individuals....[c]reated [a] risky key escrow

¹³² In addition to the DOJ, the DOC, DOD and other U.S. agencies were actually involved.

¹³³ <http://www.epic.org/crypto/> (v. several times February and March, 2000).

¹³⁴ <http://www.cdt.org/crypto/admin/clipperchip.shtml> (v. several times February and March, 2000). See also the work of Abelson et al., (1998)—a group of highly knowledgeable experts that has thoroughly criticized

system....[u]sed [a] potentially insecure algorithm....[and] [v]iolated principles behind [the] Computer Security Act of 1987.”¹³⁵

Within the framework of the Clinton Administration’s announced plans for a new export control policy, in September 1995, the National Institute for Standards and Technology (NIST) presented “[t]he Commercial Key Escrow initiative, dubbed ‘Clipper II’ for its similarity to its policy predecessor....”¹³⁶ Clipper II relaxed export controls on key lengths up to 64 bits “...provided that an encryption key was escrowed with a US government certified agent.”¹³⁷ Clipper II met widespread criticism by civil liberties groups as did Clipper III in May 1996.¹³⁸ In both the Clipper II and III, “...a spare set of keys would be given to a ‘trusted third party’ who had been approved by the government and who would turn over keys in investigations. This software could then be freely exported to most countries.”¹³⁹ As further liberalization, the federal government freed the export of 56-bit DES equivalent products and higher to selected industries (e.g. banks and financial services) in September 1998 and of stronger key cryptography for certain users and certain countries in September 1999.¹⁴⁰

Overall, at the end of the 1990s, the policy of the Clinton Administration regarding export of encryption software was contained in three foremost notions, namely “...promoting electronic commerce, supporting law enforcement and national security, and protecting privacy.”¹⁴¹ Hence, in order to “...maintain the balance among privacy, commercial interests, public safety and national security...[the approach of the Administration will focus on three elements:] information security and privacy, a new framework for export controls, and updated tools for law enforcement.”¹⁴² With computing power more easily and cheaply available, the pretension of the federal government that DES-based cryptography software was sufficiently hard to break could no longer hold.

the Clipper/Key Escrow system.

¹³⁵ <http://www.cdt.org/crypto/admin/clipperchip.shtml> (v. several times February and March, 2000).

¹³⁶ <http://www.cdt.org/crypto/admin/clipper2.shtml> (v. several times February and March, 2000).

¹³⁷ <http://www.cdt.org/crypto/admin/clipper2.shtml> (v. several times February and March, 2000).

¹³⁸ <http://www.cdt.org/crypto/admin/clipper3.shtml> (v. several times February and March, 2000).

¹³⁹ http://www.epic.org/crypto/key_escrow/ (v. March 15 and 16, 2000).

¹⁴⁰ The liberalization rules announced September 1999 and specified in January 2000 are: (a) “retail” encryption products are widely exportable to all but certain “terrorist” nations though still subject to a government review and reporting requirements, (b) non-retail products are also exportable, subject to similar requirements, to most non-government users, (c) encryption products with less than 64-bits are freely exportable, (d) some non-proprietary source code is exportable to most countries after notice to the government (<http://www.cdt.org/crypto/admin/> v. February 57 and 7 and March 15 and 16, 2000).

¹⁴¹ <http://www.bxa.doc.gov/Encryption/whpr99.htm> (v. March 18, 2000).

¹⁴² <http://www.bxa.doc.gov/Encryption/whpr99.htm> (v. March 18, 2000).

In fact, the EFF has repeatedly shown how it is relatively easy to crack the 40-bit encryption technology that is the strongest form permitted for export.¹⁴³ In July 1998 the EFF DES Cracker—built for less than \$250,000—easily won RSA Laboratory's "DES Challenge II" contest and a \$10,000 cash prize.¹⁴⁴ In less than 3 days the machine completed the task, shattering the previous record of 39 days set by a massive network of tens of thousands of computers. Moreover, in January 1999, Distributed.Net, a worldwide coalition of computer enthusiasts, worked with EFF's DES Cracker and a worldwide network of nearly 100,000 PCs on the Internet, to win RSA's DES Challenge III in a record-breaking 22 hours and 15 minutes. The worldwide computing team deciphered a secret message encrypted with the United States government's Data Encryption Standard (DES) algorithm using commonly available technology.¹⁴⁵

In January 2000 (following the September 1999 declaration), the Clinton Administration announced the new encryption export regulations. In sum, the new rules assert that:

[a]ny encryption commodity or software, including components, of any key length can now be exported under a license exception after a technical review to any non-government end-user in any country except for the seven state supporters of terrorism... Exports to government end-users may be approved under a license... A new category of products called "Retail encryption commodities and software" can now be exported to any end user (except in the seven state supporters of terrorism)... Encryption source code [available to the public] may be exported under a license exception [but the] exporter must submit to the Bureau of Export Administration [BXA] a copy of the source code...¹⁴⁶

Export controls have been relaxed, but not completely removed. The DOC, through the BXA, will grant licenses, maintain copies of the source codes exported, and evaluate which encryption software could be classified as "retail". Hence, according to the CDT, "[t]he regulations do not decontrol encryption or remove complex requirements that may prove daunting to many individuals and small businesses [and some] types of encryption source code are still restricted".¹⁴⁷ Moreover, ACLU, EPIC and EFF have announced that "...new encryption export regulations released by the U.S. Commerce Department fall short

¹⁴³ <http://www.cpsr.org/cpsr/nii/cyber-rights/web/current-key.html> (v. March 20, 2000).

¹⁴⁴ <http://www.eff.org/descracker/> (v. March 19 and 20, 2000).

¹⁴⁵ <http://www.eff.org/descracker/>. (v. March 19 and 20, 2000).

¹⁴⁶ Finance-specific, 56-bit non-mass market products with a key exchange greater than 512 bits and up to 1024 bits, network-based applications and other products which are functionally equivalent to retail products are considered "retail products." See DOC Fact Sheet on Export Regulations, (<http://204.193.246.62/public.nsf/docs/60D6B47456BB389F852568640078B6C0#a> v. March 20, 2000).

¹⁴⁷ <http://www.cdt.org/crypto/admin/> (v. March 20, 2000).

of the Clinton Administration's promise to deregulate the privacy-enhancing technology [and that they] will continue to press their Constitutional cases".¹⁴⁸

The Security and Freedom through Encryption (SAFE) Act, discussed in 2000 in the House was planned to amend the Federal criminal code to permit individuals to sell any encryption in interstate commerce, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or median used. The Secretary of Commerce would receive exclusive authority to control exports of all computer hardware, software, computing devices, communications network equipment, and technology for information security (including encryption), except that which is specifically designed or modified for military use. However, "[w]ith various versions of the SAFE bill in the House, and different measure pending in the Senate, it [is] far from clear what direction Congress would take" (Diffie and Landau, 1999:223).

With regards to the evolution of the encryption dispute, to conclude, it is worth quoting the remarks of CPSR (Computer Professionals for Social Responsibility) NGO: "Every year, a law lifting restrictions is introduced into Congress—backed by intense support from software companies—but so far none has passed. On the other hand, the administration has failed to pass bills that include harsher provisions. *So the status quo mostly prevails...*"¹⁴⁹ As to further confirm this point, in September 1999 the White House announced its intention to remove restrictions for software marketed to commercial institutions—including limitations on the source code, thus making strong encryption freely available to foreign countries via Open Source software. However, "...commercial products must [still] be reviewed by the government, a regulation that erects a barrier and offers opportunities for meddling".¹⁵⁰

Overall, the cryptography debate brings clearly to light the rival coalitions in Internet control. On one side there are law enforcement/intelligence/defense departments and agencies that mostly oppose the widespread use and export of strong encryption software. These actors see these events as major impediments to their procedures, as well as preludes to more serious consequences such as deterioration of national security. On the other side, pro-liberties NGOs, consumers' organizations, users' groups, and the ICT industry are all in favor of unrestricted use, availability, and sale of strong encryption

¹⁴⁸ http://www.eff.org/11300_crypto_release.html (v. March 20, 2000).

¹⁴⁹ Emphasis added. <http://www.cpsr.org/cpsr/nii/cyber-rights/web/current-key.html> (v. March 21, 2000).

¹⁵⁰ <http://www.cpsr.org/cpsr/nii/cyber-rights/web/current-key.html> (v. March 21, 2000).

software, since such software is indispensable to provide security in today's Internet, from protecting individual communications to business transactions.

The outcome of the confrontation between such powerful coalitions is a stalemate in the United States, with a slight advantage for the "accidental coalition". The CPRS's remark mentioned above is thus undoubtedly correct. The *status quo*, although certainly not ideal, is still mostly favorable toward the stance of the accidental alliance, and as long as the partners of this "unofficial" alliance can find common ground to keep it together, the status quo will remain.

4.4.5 *Cyber-terrorism, Cyber-crime and the National Information Infrastructure (NII)*

A broad definition of "national security" in relation to the Internet can include (a) protecting crucial government and business communications using TCP/IP, (b) maintaining first-rate intelligence-gathering capabilities about foreign TCP/IP-based communications, (c) deterring or limiting the diffusion on the Net (particularly on the Web) of negative and unfriendly information about a country's government, political system, domestic situation, etc.¹⁵¹ and (d) fending off malicious TCP/IP-based attacks against a country's critical NII.¹⁵² The former two pertain to the issue area of "free use of cryptography," that is, the U.S. government wants to protect its communications via unbreakable encryption, and, at the same time, to be able to break other governments' encrypted communications. The latter item refers to the destruction that can be brought about in the U.S. NII via the Internet, and, along with (c), are included in the concept of "Information Warfare."¹⁵³ In fact, although "[t]he meaning of the term 'information warfare' is far from settled...", Diffie and Landau correctly maintain that "[t]he heart of information warfare today is the notion of attacking the enemy with information alone" (1999:101/102). This section will thus focus on point (d) of the definition of "national security."

As noted earlier, the United States is the country most dependent on information infrastructures in the whole world, and "[a]n opponent who is critically dependent on information will be catastrophically vulnerable to corruption of that information" (Diffie

¹⁵¹ In the United States, this is what it is called "perception management." Ghent personal interview.

¹⁵² "Critical Systems are computer, electronic or electromechanical systems whose failure has potentially disastrous effects, like injury or death to human beings, environmental hazards, economical loss. Examples of critical systems are train control systems, nuclear power station control systems, flight control systems" (Adolfo Villafiorita, Automated Reasoning Systems, *Istituto Trentino di Cultura*, Trento, Italy, http://sra.itc.it/application_area.epl?name=Critical+Systems v. January 11, 2001).

¹⁵³ Some experts have distinguished between "Cyber-war.." i.e. information-oriented military warfare, involving formal military forces against each other, and "Net-war," which is more likely to involve non-state, paramilitary or irregular forces (Arquilla et al., 1999:46).

and Landau, 1999:102). Practically, since 1988, when the Morris Worm¹⁵⁴ struck the Internet crashing circa 6,000 machines, American political leaders have been concerned with the possibility that domestic or foreign enemies could exploit the United States NII's exposed position "to bring the country to its knees." Consequently, "[t]he Department of Defense...must assume that any enemy it engages will attack DOD's computers to disrupt military operations" (Libicki, 1997:9).

Currently, in the United States, the NII includes (1) information and communications, (2) electrical power systems, (3) gas and oil transportation and storage, (4) banking and finance, (5) transportation, (6) water supply systems (7) emergency services, (8) and government services.¹⁵⁵ Hence, the NII comprises the Internet, as well as the public switched network, and cable, wireless, and satellite communications, both private and public.¹⁵⁶ Protection of the NII is said to be achieved when integrity, reliability, availability, and confidentiality—the four factors essential to attain computer security—are assured.

The first step taken by the Clinton Administration—the first U.S. Administration that has seriously tackled the problem—was, in July 1996, the creation of the President's Commission on Critical Infrastructure Protection (PCCIP, Executive Order 13010), including, among others, DOD, DOC, DOJ, CIA, FBI, and NSA.¹⁵⁷ Mission of the PCCIP would be to identify "physical and cyber threats" to the NII. Following the 1997 Critical Foundation Commission report, in May 1998, President Clinton issued the Presidential Decision Directive 63 (PDD-63), identifying as "critical infrastructures" "...those physical and cyber-based systems [that are] essential to the minimum operations of the economy and government. These systems are so vital, that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."¹⁵⁸ The ultimate goal of PDD-63 was to build the capability to protect the NII by 2003. Moreover, the PDD-63 created the Critical Infrastructure Assurance Office (CIAO) that took over most of the PCCIP's duties. CIAO has recognize the critical infrastructure assurance as "...new capability that resides at the point where our national security and economic security merge."¹⁵⁹

¹⁵⁴ The Morris Worm (it was long debated if it was a worm or a virus) was created in 1988 by Robert T. Morris, graduate student at Cornell University. It was not supposed to be a malicious piece of software and Morris spoke of an experiment gone wrong. Nonetheless, it set a precedent (Hafner and Markoff, 1991).

¹⁵⁵ <http://www.pccip.ncr.gov/glossary.html> (v. March 24 and 25, 2000).

¹⁵⁶ <http://nsi.org/Library/Compsec/nii.txt> (v. March 24, 2000).

¹⁵⁷ <http://www.pccip.ncr.gov/eo13010.html> (v. March 24 and 25, 2000).

¹⁵⁸ Presidential Decision Directive 63, May 22, 1998 Executive Order 13010, July 15, 1996 (<http://www.fbi.gov/nipc/nipc.htm> v. September 30, 1999 and March 25, 2000).

¹⁵⁹ http://www.ciao.ncr.gov/new_home.html (v. March 26, 2000).

Before PDD-63 was issued, in February 1998, following the PCCIP Critical Foundation report, the DOJ and the FBI had already constituted the National Infrastructure Protection Center (NIPC), located in the FBI building in Washington DC.¹⁶⁰ The mission of the NIPC is both a national security and law enforcement effort to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts both physical and "cyber," that threaten or target our critical infrastructures.¹⁶¹ The NIPC's duty is not only to investigate and respond to attacks after they occur, but to learn about preventing them. In fact, in PDD-63, President Clinton stated that "[t]he NIPC will provide a national focal point for gathering information on threats to the infrastructures...[and] the principal means for facilitating and coordinating the Federal Government's resources to an incident, mitigating attack."¹⁶²

As a partial fulfillment of its mission, the NIPC has ranked disruptions of NII operations according to their gravity and premeditation:

1. *Natural or Inadvertent Interruptions*: (a) Natural events and accidents; (b) Blunders, errors, and omissions.
2. *Intentional Interruptions* (by illegal or criminal sources); (c) Insiders: (d) Recreational hackers; (e) Criminal activity.
3. *Intentional Interruptions* (by terrorists or a nation-state); (f) Industrial espionage; (g) Terrorism; (h) National intelligence; (i) Information warfare.¹⁶³

This extensive list, however, remains still speculative. In fact, despite the impressive 115% increase in "...pending investigations that involve the exploitation of technology and represent a threat to the public and private sector," since the beginning of Fiscal Year 1997, this percentage translates in an absolute augmentation of cases from 260 to 559.¹⁶⁴ Compared with the millions of Net users and billions of billions of computer operations in the United States, these figures seem a rather weak basis to support the claim that serious damages to the NII are likely to occur.¹⁶⁵ Clearly, it does not contribute to a sober

¹⁶⁰ PDD-63 was published on May 22, 1998, citing NIPC at http://www.ciao.ncr.gov/press/WhiteHouseFactSheet_PDD63.htm (v. March 26, 2000).

¹⁶¹ <http://www.fbi.gov/nipc/mission.htm> (v. March 26 and 27, 2000).

¹⁶² Presidential Decision Directive 63, May 22, 1998, at <http://www.fbi.gov/nipc/nipc.htm>, and also <http://www.whitehouse.gov/WH/EOP/NSC/html/documents/NSCDOC3.html> (v. March 26 and 27, 2000).

¹⁶³ <http://www.fbi.gov/nipc/nipcfaq.htm> (v. March 28, 2000).

¹⁶⁴ <http://www.fbi.gov/nipc/nipcfaq.htm> (v. March 28, 2000).

¹⁶⁵ It is worth noting here that the organizations mentioned in this section have their main goal in the "protection" of the NII. The "development" and further modernization of the NII is competence of organizations, among others, such as the Information Infrastructure Task Force (IITF), supported by the DOC's NIST (<http://www.iitf.doc.gov/>), the Federal networking Council (FNC <http://www.fnc.gov/>) or the National Coordination Office (NCO, <http://www.ccic.gov/>) (all v. March 28 and 29, 2000).

assessment of the existing threat that Micheal Vatis, NIPC's director, has declared that an "electronic Pearl Harbor" is possible.¹⁶⁶ Approximately the same belief has been expressed by former national security advisor Anthony Lake (2000), who has put cyberterror and cybercrime on the list of the six most dangerous "nightmares" that the United States has to face.

Statements such as this are not unintended. They are often—albeit less colorfully—employed at the highest levels of the Administration. In January 1999, in an address delivered at the National Academy of Sciences, President Clinton equated the risk of attacks to the critical infrastructures, computer systems, and networks with the emerging threats posed by biological and chemical weapons.¹⁶⁷ A year later, in January 2000, launching the National Plan for Information System, President Clinton announced an increase in the critical infrastructure, funding up to \$2.3 billion by FY 2001. The plan included specific "...new initiatives to defend the nation's computer systems from cyber attack"¹⁶⁸ - that is, among others, the training and recruiting of IT experts by the Federal government and the creation of FIDNET—the cyber "burglar alarm" to alert the government of in-progress cyber attacks.

Perhaps incidentally, a month later, a much reported "cyber attack" was launched against some of the most famous web sites, including Yahoo, CNN, ZDNet, eBay, and Amazon. It was a distributed denial-of-service (DoS)¹⁶⁹ attack that considerably slowed down access to those web sites, in effect preventing them from continuing their business operations. The media coverage was extensive—and with a tendency toward overstatement—reporting how, if those attacks were to continue unopposed, such a situation could seriously compromise the taking-off of the "new economy."¹⁷⁰ The Federal government had to demonstrate that it took the episode seriously, particularly when it seemed that some of the malicious hackers were operating from Germany,¹⁷¹ thus FBI's

¹⁶⁶ Maria Seminerio "FBI Warns 'Electronic Pear Harbor' Possible", *ZDNet*, March 25, 1998 (<http://www.zdnet.com/zdnn/content/zdnn/0325/297989.html> v. March 26, 2000). Alternatively, one can also speak of an "electronic Waterloo" (Webster and Borchgrave, 1998).

¹⁶⁷ <http://www.ciao.ncr.gov/bcjn2299.html> (v. March 27, 2000)

¹⁶⁸ http://www.ciao.ncr.gov/press/WhiteHouseFactSheet_Cyber%20Security.html (v. March 27, 2000)

¹⁶⁹ In a DoS attack, the machine targeted is submersed with an overwhelming number of requests, which, eventually, lead to a complete blockage of the machine itself.

¹⁷⁰ E.g. *CNN.com* "Internet Attacks Raise Concerns about Risks of Growth", February 13, 2000 (at <http://europe.cnn.com/2000/TECH/computing/02/13/unsafeinternet.ap/index.html> v. February 15 and March 27, 2000) and *Washington Post* "Hackers Cause Costly Slow Down for E-Trade", February 10, 2000 (at <http://www.washingtonpost.com/wp-dyn/articles/A32515-2000Feb9.html>).

¹⁷¹ *CNN.com* "German Hunters Follow Lead to Germany", February 13, 2000 9 at <http://europe.cnn.com/2000/TECH/computing/02/13/hacker.trail.01/index.html> .

NIPC was in “full alert” and the White House convened a meeting with IT security experts and high-tech industry leaders on February 15, 2000. The disruption of commercial activity, however, turned out to be more feared than real,¹⁷² and hackers’ sites denounced the new “witch hunt” by Federal authorities.¹⁷³

The main consequences of those events were a further confirmation of the recurring pattern. On the one hand, President Clinton was reported by CNN.com to state that the attacks had been a source of concern, but not “Pearl Harbor,” and to agree with business executives that “...the government should not have too much control over the Internet.”¹⁷⁴ On the other hand, the FBI director and the Attorney General were to propose to Congress a five-year plan to prevent Internet attacks and a further increase of \$37 million to the \$100 million already being spent to combat all types of computer crimes.¹⁷⁵ The media frenzy coupled with the public opinion’s inability to grasp technical details and minutiae contributed towards reinforcing the Federal government’s protean attitude about Internet control.

Despite the noteworthy stress the federal government placed on the significance and relevance of protecting the NII, “...there has not yet been an example of information warfare in its pure form. No nation has attacked another nation’s computers using information” (Diffie and Landau, 1999:103). This assertion holds true also for terrorist groups. Yet, as Diffie and Landau have observed, “...information warfare is very real, and very alive as a subject of military speculation, planning and development. Not a month passes without a conference, meeting or war game devoted to the subject” (1999:103). In fact, if “[t]he vast majority of [current] attacks on infrastructures are by hackers whose motives run...from financial motives to, having some fun...infrastructures attacks can be quite serious if they are well planned and coordinated” (Alberts, 1996:29).¹⁷⁶ The U.S. military takes this topic so seriously that it speaks of a “Revolution in Military Affairs” (RMA) brought about by computers and communication networks, including the Internet.

¹⁷² *ZDNet News* “Online Shoppers Unfazed by recent Hacks”, February 11, 2000, (at <http://www.zdnet.com/zdnn/stories/news/0,4586,2436696,00.html>).

¹⁷³ *Hackers News Network* “Mixer Witch Hunt Begins”, February 14, 2000 (at <http://www.hackernews.com/arch.html?021400>).

¹⁷⁴ *CNN.com* “Clinton Administration Develops Internet Security Proposal As Investigators Pursue Hackers”, February 16, 2000, (at <http://europe.cnn.com/2000/TECH/computing/02/16/hacking.investigation.01/index.html>).

¹⁷⁵ *CNN.com* “Clinton Administration Develops Internet Security Proposal As Investigators Pursue Hackers”, February 16, 2000, (at <http://europe.cnn.com/2000/TECH/computing/02/16/hacking.investigation.01/index.html>).

¹⁷⁶ Such an event, however, “...would require an adversary with seriousness of purpose and with some sophistication and organization” (Alberts, 1996:29).

Since the Net is the current focus of constant attention by media and the general public, one might think that soon, the Internet will be used by various national armed forces, to gather open-source intelligence, to spread disinformation, and more seriously, to access and disrupt another country computer communications and operations. However, IW experts know that, in itself, “[t]he Internet, with its benign assumptions is hardly indicative of [communications] systems in general. It is hardly used for mission-critical tasks...”namely for tasks whose failure would imply loss of human lives, and all “military” information on the Net is unclassified and publicly available.¹⁷⁷

The DOD maintains a Computer Emergency Response Team (DOD-CERT) which, like the civilian CERTs—of which the best known is the Carnegie Mellon CERT—, is responsible for alerting DOD organizations about threats to and risks of military computer networks.¹⁷⁸ Moreover, the Army, Air Force and Navy all have their own specific CERTs. In the established pattern of “the more, the better”, another DOD important player is the Defense Information Security Agency (DISA), whose mission includes “... helping protect against, detect and react to threats to both its information infrastructure and information sources”.¹⁷⁹

Some independent experts do not agree with the military’s evaluation of the entity of the risk. John Pike of the Federation of American Scientists has identified two types of information warfare: (a) a weaker, and (b) a stronger version.¹⁸⁰ In the former, system managers are concerned with protecting their systems against “children playing.” However, given the US dependency on computer systems, they should rather worry about “professionals,”¹⁸¹ against which their computers are more often than not open and undefended. The latter version of information warfare is the “electronic Waterloo” (or alternatively “Pearl Harbor”)—namely the “switching off” of the whole United States. In this case, “a determined adversary can be extraordinarily annoying for the country,” provoking considerable financial losses and the loss of some human lives, but that same

¹⁷⁷ Military information on the Net is almost exclusively American. It might mean that either other countries’ militaries are less “Internet-enthusiastic,” or that they are suspicious of making even irrelevant information available to the vast audience of Netizens.

¹⁷⁸ “Protect, defend and restore the integrity and availability of the essential elements and applications of the DII [Defense Information Infrastructure] under the full spectrum of conflict in support of the War-fighter” (Mission Statement, http://www.ccrt.mil/about/mission_statement.htm v. March 30, 2000).

¹⁷⁹ <http://www.disa.mil/missman.html> (v. March 29, 2000).

¹⁸⁰ John Pike, Federation of American Scientists (FAS), personal interview, Washington, DC, July 15, 1999. Pike was also the principal investigator for FAS of the “Star Wars” project.

¹⁸¹ Both domestic and foreign. In fact, it seems that Israeli and French computer professionals are particularly active with American businesses. Pike personal interview.

adversary could not bring the country to its knees.¹⁸² Chapman (1998) shares this view as well.

The problem, according to Pike, with (b) is that decision makers, generally in their 50s and 60s and who are not very knowledgeable about how computers work, “do believe that the electronic Waterloo is possible.”¹⁸³ Consequently, their inability to understand the technology causes “a profound anxiety about the Internet.” This anxiety is reflected, for instance, by the fact that the DOD has withdrawn 80% of its unclassified information previously available on-line, but that information is still publicly available in hard copy upon individual request and without even recurring to the Freedom of Information Act.¹⁸⁴

To conclude this section, it is worth noting that in the interviews I conducted for this chapter, one aspect of information warfare was barely mentioned, let alone discussed; namely what the United States is doing in terms of *offensive* information warfare.¹⁸⁵ In fact, the vast majority of documents publicly available concern how reliant the United States is on the NII, how weak the NII is and what is necessary to do to protect it. Nothing is said by the DOD or other federal agencies about how much damage the United States would be able to inflict to the information infrastructures of other countries. Furthermore, it seems that the more a country is industrially advanced, the more it is dependent upon computer operations and networks, the more it would be vulnerable to information-based attacks.¹⁸⁶

Information warfare, cybercrime, cyberterrorism, etc. are the territory of national security. These are the areas on which the national security communities has the largest amount of classified information and greatest expertise. Indeed, it used to be that national security matters were never discussed outside that community, and those issue prevailed over any other concerns, including economic ones. Yet they have not been able to win over either the public opinion (which is skeptical about the menace) or the top level of the past Administration. One can better understand such circumstances, for instance, by reading Lake’s book (2000). Even a non-expert reader can see that in the book there is plenty of

¹⁸² Pike personal interview.

¹⁸³ “They think there is a little person in the computer.” Pike personal interview.

¹⁸⁴ That information is now termed “sensitive un-classified,” meaning that it cannot be uploaded into the Net. Pike’s interview.

¹⁸⁵ Alberts (1996: 4) defines “defensive” IW as “...all actions taken to defend against information attacks, that is, attacks on decision makers, the information and information-based processes they rely on, and their means of communicating their decisions”.

¹⁸⁶ Almost paradoxically, the RAND Corporation recommends the U.S. Air Force not modernize all communications nodes and avoid full connectivity, since the old USAF communication system is robust and unfamiliar for cyberterrorists and hackers (Arquilla et al., 1999:81).

common sense, but very little convincing evidence (even allowing for non disclosure of classified information)—and Lake was in the National Security Council for four years.

The debate on the Internet threats presents a different state of affairs, than past national security issues. Pro-liberties NGOs, consumers' organizations, users' groups, and private businesses are not willing to accept acritically the viewpoint of the other side. According to them, Internet threats should be properly debated and assessed, taking into consideration and evaluating contradictory views. The stalemate that has ensued is a testimony of their technical and legal proficiency, and their ability to mobilize support. This time, not even the powerful national security coalition has been able to win the day on such a flimsy argument such as Internet as a national security threat.

4.5.5 DNS (*the root*)

No one within the small, cohesive Internet community that originally developed the Domain Name System (to facilitate memorizing Internet addresses by users) could have ever envisaged that the DNS would become a major bone of contention within private industry, regulating authorities and users. When, in the early 1980s, the first documents (RFC) on the DNS began to appear, neither their authors, nor the federal government, nor the private sector, nor Netizens could foresee the enormous impact that the TLD/DNS would have on the commercial potential of the Internet and, undoubtedly, on the future of the Net itself.¹⁸⁷

As Mueller has written, "...the DNS, as a centralized point of interconnection, gave whoever controlled it the leverage to impose almost any terms they wished upon domain name registrants, registration services and registries"(1999:509). In fact, the Web's inventor, Tim Berners-Lee, has defined the DNS the "...one centralized Achilles' heel by which [the Web] can all be brought down or controlled" (1999:126).¹⁸⁸

In July 1997, following the Presidential Directive on electronic commerce, the Department of Commerce was designated the lead agency on domain names.¹⁸⁹ The "Framework for Global Electronic Commerce" directed the Secretary of Commerce to privatize the management of the DNS in a manner that increases competition and facilitates

¹⁸⁷ The full list of RFC for the DNS is at <http://www.dns.net/dnsrd/rfc/> (v. March 30, 2000, and January 9, 10 and 11, 2001).

¹⁸⁸ The Web in particular, but the whole Internet, in general, may be seriously affected by the Achilles' heel of DNS.

¹⁸⁹ http://www.whitehouse.gov/WH/EOP/OSTP/Technology/html/tech_proj.html (v. April 1, 2000).

international participation in its management. Affected by this decision were, probably, the four best known and most valuable TLDs, i.e. *.int*, *.org*, *.net* and, most of all, *.com*.

Following an extensive public consultation process, in June 1998, the DOC issued a Statement of Policy entitled Management of Internet Names and Addresses (the "White Paper").¹⁹⁰ The White Paper called upon the private sector to create a new, not-for-profit corporation to assume responsibility, over time, for the management of certain aspects of the domain name system. The White Paper also articulated the fundamental policies that would guide United States participation in the transfer of DNS management responsibility to the private sector: stability; competition; private, bottom-up coordination; and representation.¹⁹¹

The leading players in the DNS question are the DOC, the ICANN and the NSI. The DOC "inherited the Internet" in 1995 from the National Science Foundation (NSF) that, in turn, had inherited it from DOD ARPANET. In November 1998, the DOC "officially recognized the Internet Corporation for Assigned Names and Numbers (ICANN) as the global, non-profit consensus organization designed to carry on various administrative functions for the Internet name and address".¹⁹² This recognition was made possible by a Memorandum of Understanding (MoU) between DOC and ICANN that emphasized the management criteria highlighted by the White Paper.

Created in October 1998, the ICANN "is the non-profit corporation that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions now performed under U.S. Government contract by IANA and other entities".¹⁹³ Since then, ICANN has managed "...the responsibility for coordinating [the] four key functions for the Internet"¹⁹⁴ indicated in the MoU with DOC by supervising new TLDs (to be approved), and introducing competition in the TLDs-assignment process. Perhaps most important and laborious, however, is the oversight of the conduct of Network Solutions, Inc. (NSI), "the

¹⁹⁰ <http://www.ntia.doc.gov/ntiahome/domainname/dnsdrft.htm> (v. April 1 and 2, 2000).

¹⁹¹ <http://www.ntia.doc.gov/ntiahome/domainname/agreements/summary-factsheet.htm> (v. April 1 and 2, 2000).

¹⁹² <http://www.icann.org/general/statusreport-15june99.htm> (v. April 2, 2000).

¹⁹³ IANA was the "precursor" of ICANN and was "absorbed" into it (<http://www.iana.org/>). See also <http://www.icann.org/> (both v. several times, January, February March, August, September, October and November 2000).

¹⁹⁴ The U.S. government had resolved the complete transfer of competencies to ICANN by September 2000. These qualifications included the management of the domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system (<http://www.icann.org/general/fact-sheet.htm>) However, in September 1999, the DOC decided otherwise.

historical monopoly registry and registrar in these domains.”¹⁹⁵ So reluctant has the NSI been to abandon its monopoly that, in 1999, a report by ICANN to the DOC could but note that NSI had provided “...less than enthusiastic cooperation...”¹⁹⁶ to ICANN’s operations.

The detailed depiction of ISOC’s maneuvering to create ICANN, and ICANN’s attempts to impose its will on NSI is of marginal interest for the goal of this work, and has been extensively explored by other scholars (e.g. Mueller, 1999). Suffice to say that the federal government intervened with the “self-regulation” policy of the White Paper when ISOC and IANA failed to break NSI’s monopoly, and proved that they had no legal basis or jurisdiction to privatize the root. Mueller has described what happened as follows (1999:504):

[‘i]ndustry self-regulation’ was an appealing label for a process that could be more accurately described as the U.S. government brokering a behind-the-scene deal among what it perceived as the major players—both private and governmental...The ISOC-led coalition was one key player, and the real winner.

The White Paper, however, solved the “most disruptive and potentially dangerous issue” (Mueller, 1999:509), namely the future status of the NSI registry, by not addressing it, hence leaving ample room to the NSI to offer “less than enthusiastic cooperation”. In fact, as Mueller (1999:519) has noted,

[h]ad the Clinton Administration’s white paper explicitly and firmly distanced internet administration from trademark protection and other issues not directly related to technical coordination of the internet, then its policy of ‘industry self-regulation’ would have had some coherence. However, the white paper was first and foremost a political bargain: its commitment to self-regulation was mainly rhetorical.

The White Paper finally called in the WIPO “...to investigate domain name trademark conflicts and make recommendations about how to resolve disputes, and how new TLDs would affect trademark holders” (Mueller, 1999:504). To some extents, this move by the federal government was inevitable, since, in 1998, a dubious practice—nicknamed “cyber-squatting”—was starting to seriously disquiet the private sector.

Before the commercial potential of the Internet became manifest to private business and the larger public alike in 1994/1995, some clever individuals began to register well known brand names (such as Disney or McDonalds) as Internet gTLDs for an annual fee of \$35 to NSI. Around that period, being “visible” on the Net was quickly becoming a vital imperative for companies worldwide. “Sky-rocketing” anticipations of the Internet as the ultimate commercial miracle of the new millennium was obliging small as well as large

¹⁹⁵ <http://www.icann.org/general/statusreport-15june99.htm>

businesses to turn their attention to the Internet. It then happened that when a world-brand company turned to the NSI to register its domain, it might discover that what it considered “its” domain name (e.g. coca-cola.com or nike.com) was already “owned” by one of those individuals. These would then charge the company large sums of money to turn their rights on the domain over to the company itself. Sometimes, however, another company with the same name or ordinary individuals in “good faith” had no intention of yielding their rights on the domain, thus initiating lengthy legal battles.

So important has the copyright protection of brand names on the Net become that bills such as the Anti-Cyber-squatting Consumer Protection Act have started to appear before Congress. This specific act, for instance, has been intended as a “...crackdown on those who in bad faith register popular trademark names or names sufficiently similar to a trademark as Internet domain names and sell them...to companies who hold the trademarks.”¹⁹⁷ Indeed, at the end of 1999, the U.S. Congress approved a proposal that would prevent average citizens from using well-known names as domain names. The proposal—contained in a massive Consolidated Appropriations package (H. Rep. 106-479)—was intended to stop ordinary individuals from registering multiple domains associated with famous companies or people.

Several Internet organizations, —including the Electronic Frontier Foundation—have “...voiced strong objections to such legislation because it might curtail free speech. Other observers, including certain White House officials, were concerned that the proposal might severely hamper efforts by the ICANN to create global standards for domain names.”¹⁹⁸ It is still unclear whether this law will have an adverse impact on the Net, and particularly on the creators of web-sites.¹⁹⁹

Since the Fall of 1999, the DOC has pursued its stated policy of handing its “policy authority”²⁰⁰ over to ICANN, and abandoned the DNS dispute. ICANN will take over the supervision of NSI and other Registries’ activities. Overall, the handing in by the DOC of its “policy authority” over the root (the Web’s “Achilles’ heel”) has been another success

¹⁹⁶ <http://www.icann.org/general/statusreport-15june99.htm>

¹⁹⁷ <http://www.senate.gov/~abraham/cybersqp.html> (v. April 3, 2000)

¹⁹⁸ gilc-announce@gilc.org GILC Alert, Volume 3, Issue 8 December 14, 1999.

¹⁹⁹ Excerpts of the whole Act can be found at <http://thomas.loc.gov/home/omni99/12586.txt> (v. November 19, 20, 21, 22 and 23, 1999)..

²⁰⁰ The leading position of the DOC in this dispute was due to the fact that it basically “inherited the root” from the National Science Foundation network (NSFNET), which, in turned, had taken over the management of the Net from the DOD’s ARPANET.

for the private business/civil liberties supporters of Internet self-regulation and self-governance.

The DNS is the issue-area in which disagreement and quarrels among “partners” of the accidental alliance are most likely to occur. The private sector has huge stakes in the DNS and the impact on e-business of domain names is massive. Disagreement, however, is for pro-liberties NGOs and users’ groups mostly a matter of principle (anybody should be able to access the DNS and register names), whereas consumers’ organizations are generally worried about the risks of fraud or business malpractice. Hence, preserving the coalition should not be impossible, provided that the latter actors make extra efforts to meet the industry’s concerns.

4.5.6 The “e” economy (i.e. e-commerce and e-business)

In November 1999, two car industry giants, General Motors and Ford, announced that from that date on, they “preferred” to deal with their business partners only through TCP/IP based communications. This change was not mandatory, but they strongly “encouraged” those businesses that wanted to continue operating with them to increasingly rely on that method of doing business. *The Economist* (November 6, 1999:77/78) wrote about “the moment when e-business grew up,” since, rather soon, the 50,000 plus small and medium businesses working with the two giants will be obliged to switch to this new mode of communication and procurement. Given such a scenario, it would be unlikely that any government, parliament or politician in any country will feel comfortable ignoring e-commerce, which is a considerable portion of the “e-economy.”²⁰¹

The “electronic (or “Internet”) economy” is the big hype of which many business people, government officials and laymen talk when referring to the future of the Internet. In fact, “the e-economy is largely organized around the Net.”²⁰² Yet, the e-economy is not a reasonably precisely defined issue such as, for instance, “freedom of speech.” It is rather a “macro-issue” made of other sub-issues. Indeed, the outcomes of the current contentions on the DNS, cryptography, privacy, information infrastructure, open access and the like will determine the extent of the e-economy in the United States—which, incidentally, is the best

²⁰¹ It must be noted that there is not a universally accepted distinction among e-commerce, e-business, and similar terms (including e-economy). In fact there is still considerable confusion as the terms are used interchangeably. I use the term e-economy to describe the general phenomenon of an economy strongly based on information technology and telecommunications, retaining the designation of e-commerce for Internet-related business activities.

²⁰² Pike personal interview.

candidate to create such an result. At the same time, however, demands and expectations by private business and the general public will influence the contention in all those problems.

One of the most worthy attempts to define the e-economy (or Internet economy) has been a study—sponsored by Cisco System, a router manufacturer, in 1999—by the Center for the Research in Electronic Commerce of the University of Texas.²⁰³ Despite the considerable problems of “...the definition and enumeration of the universe of players in the Internet Economy,...”²⁰⁴ the investigators for this study have been able to identify four layers of the Internet Economy, namely:

1. the *Internet Infrastructure layer* (i.e. companies concerned with the network infrastructure, such as Cisco, MCI WorldCom, AOL, Network Associates, etc.);
2. the *Internet Applications layer* (i.e. companies with products that make on-line business possible, such as Microsoft, Netscape, Oracle, IBM, Adobe, etc.);
3. the *Internet Intermediary layer* (i.e. Internet intermediaries, such as Yahoo!, Geocities, ZDNet, E*trade, TravelWeb, etc.)
4. the *Internet Commerce layer* (i.e. vendors of services and products to users and businesses, such as Amazon, eToys, Cisco and Dell, etc.).

Many such companies operate in a multi-layer fashion. As anticipated in section 3.3, in 1999, the estimated total revenues for the four layers is \$301,393 million, with attributed Internet jobs of 1,203,799.²⁰⁵ Given these (estimated) data, it is not surprising that the federal government has taken great pains to encourage and protect the development of the e-economy.

As mentioned in section 2, the current stated policy of the federal government on e-commerce and the information economy in general has been minimal government intervention and the recognition of the leading role of the private sector. In the “Framework for Electronic Commerce” document issued by the White House in July 1997, it clearly expressed that:

... governments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the Internet...[they] should refrain from imposing new and unnecessary regulations, bureaucratic procedures, or taxes and tariffs on commercial activities that take place via the Internet...[and whenever government intervention is necessary] its goal should

²⁰³ “Measuring the Internet Economy: An Exploratory Study”, at <http://cism.bus.utexas.edu/>, and also http://www.InternetIndicators.com/the_indicators_oct_99.html (v. September 30, 1999 and April 7 and 8, 2000). The results of this study have been “mirrored” by other reliable web sites such as the Congress Internet Caucus, at <http://www.netcaucus.org/> . v. April 7, 2000)

²⁰⁴ See page 5 of the report at <http://cism.bus.utexas.edu/> (v. September 30, 1999 and April 7 and 8, 2000).

²⁰⁵ See page 7 of the report.

be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, support commercial transactions, and facilitate dispute resolution.²⁰⁶

Moreover, given the peculiar qualities of the Internet, namely its decentralized nature and its tradition of bottom-up governance, governments should recognize that “[t]hese same characteristics pose significant logistical and technological challenges to existing regulatory models.”²⁰⁷ And going against what other governments maintain, the federal government argues that “...the regulatory frameworks established over the past sixty years for telecommunications, radio and television [will not] fit the Internet”.²⁰⁸

To facilitate e-commerce on a global basis, the Administration asserts that there are “...nine areas where international agreements are needed to preserve the Internet as a non-regulatory medium.” These areas may be further clustered into (a) financial issues (customs and taxation, and electronic payments); (b) legal issues (a “Uniform Commercial Code”) for electronic commerce, intellectual property protection, privacy, and security; and (c) market access issues (telecommunications infrastructure and information technology, content, and technical standards).²⁰⁹

Congress has agreed with the federal government as regards the strategic vision of America as the leading player in—indeed the chief maker of—the new e-economy, as demonstrated by the growing number of bills pertinent to this topic currently on floor in Congress. To mention a few: (a) the Internet Regulatory Freedom Act of 1999, amending the Communications Act of 1934 so that it is U.S. policy to assure that all Americans have access to advanced Internet services at affordable rates;²¹⁰ (b) the Internet Growth and Development Act of 1999 (H.R.1685), providing for the recognition of electronic signatures for the conduct of interstate and foreign commerce, and authorizing the FTC to prescribe rules to protect the privacy of users of commercial Internet web-sites and other purposes;²¹¹ (c) the Internet Access Charge Prohibition Act of 1999, prohibiting the FTC from imposing on any interactive computer service or other information service provider any access charge for the support of universal service.²¹²

²⁰⁶ <http://www.ecommerce.gov/framework.htm> (v. April 10, 2000).

²⁰⁷ <http://www.ecommerce.gov/framework.htm> (v. April 10, 2000).

²⁰⁸ <http://www.ecommerce.gov/framework.htm> (v. April 10, 2000).

²⁰⁹ <http://www.ecommerce.gov/framework.htm> (v. April 10, 2000).

²¹⁰ <http://thomas.loc.gov/cgi-bin/bdquery/z?d106:SN01043:@@D> (v. November 19, 20, 21, 22 and 23, 1999 and April 10, 2000)

²¹¹ <http://www.cybertelecom.org/legis106.htm> (v. April 10 and 11, 2000)

²¹² <http://thomas.loc.gov/cgi-bin/bdquery/z?d106:HR01291:@@D> (v. November 19, 20, 21, 22 and 23, 1999 and April 10, 2000).

What I have written in the previous section for the DNS can also, more generally, be applied to e-business and the New Economy. Pro-liberties NGOs, consumers' organizations and some users' groups, provided that some ground rules are respected, do not have anything against e-business. Moreover, they are aware that the private sector is a very influential ally against government's intrusion on the Net, and such an ally is certainly indispensable when facing the national security community.

4.6 Conclusions

...I suspect that in the near future the pro-encryption lobby will initially win the argument, mainly because no country will want to have encryption laws that prohibit e-commerce. However, if this policy does turn out to be a mistake, then it will always be possible to reverse the laws....In short, there is no reason why we cannot change our policy to suit the political, economic and social climate. The deciding factor will be whom the public fears the most—*criminals or the government*.²¹³

These words by Simon Singh (1999:313) specifically refer to the cryptography debate, but they are equally valid for the whole debate on Internet control in the United States.

Cryptography and privacy have alerted users and NGOs about the dangers of relaxation in the activity of monitoring governments' actions. Singh's words have been confirmed by *The Economist* (May 1, 1999:19/23) with regards to the long standing quarrel between the supporters of free cryptography and law enforcers.²¹⁴ In fact, "...given the easy availability of increasingly complex codes, governments may just have to accept defeat, which would provide more privacy not just for innocent web users but for criminals as well" (p.23). However, this outcome will only restore the level of privacy protection normally enjoyed by ordinary mail, but privacy, in the broader sense, may continue to be eroded (*The Economist*, May 1, 2000:13/14). In the same way, other Internet issues such as the DNS or e-commerce, let alone the NII vulnerability, are quite far from being settled.

Although "the United States cannot function without the Net,"²¹⁵ its technical structure is still not clearly grasped by American decision makers—including the highest ranking offices. This mixed state of mind of admiration and fear for computers and computer networks, however, is also common among the general public, and does not contribute to a sober evaluation of the strengths and weaknesses of the Internet, and, above

²¹³ My emphasis.

²¹⁴ Ari Schwartz of the Center for Democracy and Technology has also confirmed this very same point, in the course of our personal interview.

²¹⁵ Pike personal interview.

all, of what should be deemed legal or illegal. Not surprisingly, Columbia University professor Eli Noam, interviewed by *Wired Magazine*, declared in October 1997:

Computers have always been this mysterious force, and people read into them their fears and hopes. In the past there was this 1984-style notion of Big Brother, that all data will be centralized and controlled by the government. That model was replaced by the hacker scenario, where 14-year-olds start nuclear wars on their own.²¹⁶

To many uninitiated Americans (in government and in the street), the solution to the problems outlined in this chapter simply appear as complex and arcane as the technology that makes up the Net itself. Quite inevitably, the future development of the Internet in the United States will be punctuated by “stop-and-gos,” and by “two-steps-forward, one-step-back.” It almost seems that the true American organizational philosophy, namely that everything must be “checked and balanced” to avoid concentration of power even at the cost of efficiency, has been applied *in toto* to the Internet.

As correctly noted (Delacourt, 1997: 208), “[a]lthough the United States is regarded among those nations placing the fewest restrictions on expression, it was among the first to approve legislation [the CDA] governing the content of on-line communications.” The CDA was eventually abandoned, and now it is COPA that threatens on-line freedom of speech. Along the same lines, the United States, even as it becomes more and more dependent on the NII and its protection, continues to develop concepts and instruments of offensive IW (e.g. network viruses) that could easily backfire and damage its very own NII. The examples could go on with the plans by the federal government to liberalize the DNS, while NSI (the company managing *.com* and other domains) is “dragging its feet” to maintain the *status quo*.

There are two noteworthy findings in this chapter: (a) the existence of the accidental, “unofficial” alliance of principles-oriented (pro-liberties NGOs, consumers’ organizations, users’ groups) and profit-oriented (private businesses) actors, which somehow “oppose” the law enforcement/intelligence/defense coalition on Internet control, and (b) the ensuing stalemate in government’s attempts to foster statutory control on the Net. Given (a), (b) has been inevitable, since both principle-oriented and profit-oriented actors have mastered technical and legal information, and have been very capable of “voicing” their interests in the appropriate settings. Neither party, however, is tough enough to overcome the other’s

²¹⁶ http://hotwired.lycos.com/collections/connectivity/5.10_eli_noam1.html (v. September 29 and April 10, 2000).

resistance, although sympathy of the American public (particularly in the case of new awareness for privacy protection) is slightly tending toward the “accidental alliance”.

These circumstances (and the other evidence presented in this chapter) highlight two other crucial factors that will determine the future direction of Internet control, both in the United States and thus in the rest of the world. The first one is the *intensity* of the undecided and swinging attitude towards Internet control, in the public, the Congress, and the federal government. Given the difficulty of categorization of the Internet with other media, and the legal, moral and technical intricacies of its nature, the opinion of citizens and administrators alike swings back and forth from, say, demanding more control to protect children, to fears of undermining the First Amendment. Different stake-holders—the ACLU, pro-family advocates, the business and intelligence community, etc.—demand attention on one aspect of the Net or another, generating a “Babel” of mixed and contradictory feelings in many individuals. The overall result of this struggle is that no final decision is made. The directions of Internet evolution are as numerous as the participants in this struggle. As Ira Magaziner, White House Internet guru, has remarked, “there is a lot of confusion.”²¹⁷

The Internet debate in the United States, however,—as well as in other democracies—is also critical for the second factor, namely for the *example* that it will set for “less” democratic states. If countries like the United States or Germany that, rightly or wrongly, are regarded by many as true instances in democratic behavior do activate restrictive legislation about Internet content or access, then what will happen in countries such as Iran, or China?²¹⁸ In fact their political leaders could then comfortably address their public opinions by noticing that even the “advanced” democracies that constantly lecture other governments about their human rights records and lack of personal liberties cannot withstand an unrestricted Internet. Moreover, given their unmatched presence in terms of contents, infrastructures and traffic, if the United States and Europe decided to set up control mechanisms of some kind, this would definitively facilitate the job of more “control-prone” governments.²¹⁹

With reference to the Internet, the most noteworthy difference between the “real enemies”²²⁰ of the Net (as defined by *Reporters Sans Frontieres*, RSF) and industrialized

²¹⁷ Quoted by Gary Chapman, Director, *XXI Century Project*, University of Texas, Austin, during a personal conversation at the ISODARCO Summer School, Rovereto (Trento, Italy), August 13, 1999.

²¹⁸ “Western democracies like the United States and Germany act especially irresponsibly in calling for restrictions” (Delacourt, 1997:220).

²¹⁹ Those governments could take advantage of control mechanisms, such as extensive filtering software, already operating and simply “add up” their capabilities to make control tighter and more efficient.

²²⁰ According to RSF, the 20 enemies are the countries of central Asia and Caucasus, Belarus, Burma, China,

democracies is that in the latter, “constitutional arguing” with one’s government is a perfectly acceptable procedure. Civil liberties groups and users can manifest their discontent with government initiatives on the Net, and try to change them in parliaments, or, if that fails, even before a court— another dynamic actors in the debate about Internet control. This instance is not accidental. In fact, established—as well as emerging—democracies have recently attributed more and more power to the judiciary (*The Economist*, August, 7, 1999:27/28). Harvard Law School professor Lawrence Lessig has explained these puzzling circumstances, where an un-elected body (the judiciary) is trusted by citizens more than the elected one (the government), as:

[w]e have lost faith in the idea that the product of representative government might be something more than mere interest...that ordinary government might work, and so deep is that thought that even the government doesn’t consider the idea that government might actually have a role in governing cyberspace (1999:136).

Given this state of affairs, it would have been extremely unlikely that a federal or even international agency would have been accepted by users and the private industry to oversee the DNS or the use of cryptography.

The findings presented in this chapter for the United States confirm the preliminary model derived from the quantitative analysis. That is, further liberalization of telecommunications in the larger sense—thus including further “privatization” of the Net, freer use of encryption software, and less governmental intervention—is on an increasingly colliding route with the exigencies of “national security.” However, as is often the case, the qualitative analysis has demonstrated that the overall picture of statutory control on the Internet is even more complex than what resulted from the previous quantitative analysis. In fact, the multiplicity of stakeholders combined with the multiplicity of issue-areas depict a condition of competing interests and multiple loyalties that my original model and the data could only remotely signal, thus demanding an in-depth investigation of the relevant cases.

All in all, the U.S. government will continue to look for ways to retain at least some influence on the long-term development of the Internet, since it could never accept before its constituency and Congress that the United States might lose its hegemony on an “all-American” invention such as the Net. But the federal government will have to pursue that goal with more and more subtlety, as more and more countries increase their share of Net

Cuba, Iran, Iraq, Lybia, North Korea, Saudi Arabia, Sierra Leone, Sudan, Syria, Tunisia, and Vietnam—all countries whose records of democracy is not very high (at <http://www.rsf.fr/uk/alaune/enemiesweb.htm> v. September 29, 1999 and April 11, 2000. See also Human Rights Watch’s “Freedom of Expression on the Internet”, (<http://www.hrw.org/worldreport99/special/internet.htm> v. September 29, 1999 and April 11, 2000).

contents and numbers of users and hosts. The relatively discrete position that the DOC is maintaining with ICANN and NSI is one such instance. The United States will preserve its ability to virtually assign the status of “country” to Palestine,²²¹ before it becomes so in the real world, or to shut down www.mukmin.com (an “Islamic portal” based in Malaysia)²²² as part of its “perception management” capabilities for yet long time to come. However, for better or worse, there will inevitably be less and less efficiency in that process.

²²¹ The DOC approved the “.ps” ccTLD for host computers based in Palestine in March 2000, after ICANN recommended it. Although “[t]he designation is not meant as a recognition of Palestinian statehood,...foreign-policy implications may be unavoidable”, <http://www.cnn.com/2000/WORLD/meast/03/22/palestinians.internet.ap/index.html> and <http://www.cnnitalia.it/2000/MONDO/mediooriento/03/23/internet.ap/index.html> (v. March 30 and April 11, 2000).

²²² <http://www.mukmin.com/> (v. April 10 and January 11, 2001).

CHAPTER FIVE - DAS NETZ ÜBER ALLES: GERMANY ON LINE

*"The information technology sector is
a key industry in the 21st century"
(Bundesregierung Deutschland, 2000).¹*

*"Deutschland Vorn im Internet!"
(Initiative D21, 2000).²*

5.1 Introduction

"Ist Deutschland fit für die digitale Ära?" asked the German magazine *Der Spiegel* in March 2000 (p.7), "is Germany in shape for the digital age?" The answer is that it is trying its best to get there—and to make the "Internet the norm for the German economy".³ To an external observer it indeed appears that Germans have literally "fallen in love" with *das Netz*. With the exception of the Scandinavians—who are in a league of their own—Germans are the most active surfers on the Web, possibly preferring contents in the German language. In fact, even though there are to be said more British users, Germans tend to spend more time (average 5.6 hours per month in 1999) on-line.⁴ T-Online—the Internet access provider owned by telecom giant *Deutsche Telekom AG (DTAG)*—is the most visited site of the home market,⁵ and the world's second-largest ISP (*The Economist*, April 15, 2000:67). Moreover, *Deutsche Telekom* is Europe's largest telecommunications company, and the third largest carrier world-wide.⁶ Quite naturally, DTAG has echoed and championed the federal government intention of making "...Germany one of the leading Internet countries" to launch its 2000 campaign "Germ@ny goes online".⁷

Finally, the ccTLD *.de* (the top-level domain for Germany) is the second most frequent domain on the Web—the first being *.com*.⁸ Consequently, when European countries are compared with the United States, Germany is consistently ranked the number one within Europe.⁹

¹ <http://eng.bundesregierung.de/frameset/index.jsp> (v. August 1, 2000).

² <http://www.initiatived21.de/> (v. August 1, 2000).

³ <http://www.europemedia.net/shownews.asp?ArticleID=722> (v. December 8, 2000).

⁴ <http://home.cnet.com/specialreports/0-6014-7-1538059.html?st.sr.6014-7-1538058.txt.6014-7-1538059> (v. August 1, 2000).

⁵ <http://www.mmx-europe.com/data/thetop.jsp> (v. August 1, 2000).

⁶ <http://www.deutsche-telekom.de/english/index.htm> (v. August 1, 2000). See also Natalicchi (1996:301).

⁷ <http://www.telekom.de/dtag/presse/artikel/0,1018,x528,00.html> (v. October 4, 2000).

⁸ http://www.securityspace.com/s_survey/data/200007/domain.html (v. August 1, 2000).

⁹ The 1999 study "The Net Revolution Goes Global" by CNET is a good example, at

These notable results are not incidental. On the contrary, they are the consequence of an impressive, conscious digitalization effort of the whole of German society and economy, planned and executed through a coordinated action by the government, private industry, schools, and the media. It is the traditional logic of German orchestration and consensus among social and economic actors, with a whole new goal, namely bringing Germany into the Information Age and the New Economy. Crucial to this endeavor is not only the full backing of the SPD-Green government but, even more, the “enthusiasm” of Germany’s industrial colossi (Tarquini, July 3, 2000:13). In Germany’s corporatist democracy model, institutional actors (i.e. trade unions, industrialists’ associations, consumers’ groups) have fairly good access to federal and local governments and legislatures. Once consensus is reached among all these players, it endures, and the resulting policies are highly likely to be implemented.

Two examples of this condition are Initiative D21 and the ICANN At-Large membership. The former case is a coherent project of the Federal government and the private sector to boost IT education in schools and the society in general. In the latter case, mainly thanks to the publicity given to the event by *Der Spiegel*, a considerable number of Germans registered for the election of the new Board of Directors of ICANN, the organization that is responsible for domain names.¹⁰

5.2 Historical Background

Germany’s telecommunications history does not differ much from that of Italy or other continental European countries. After the war, West Germany rebuilt its telephone system as a public service, thus as property of the government—a so-called “natural monopoly”. More precisely, “...telecommunication services have in the past been highly regulated by the German Government through its Ministry for Post and Telecommunication (BMPT) and controlled and owned by the Federal Telecommunication and Postal Offices

<http://home.cnet.com/specialreports/0-6014-7-1538059.html?st.sr.6014-7-1538058.txt.6014-7-1538059> (v. August 1, 2000).

¹⁰ The first, “original” article “I Can! eLectons 2000” was of May 2, 2000, at <http://www.spiegel.de/netzwelt/icann/0,1518,k-157-ab2000050214:32,00.html> (v. July 30 and August 21, 2000). Since then, Spiegel On Line has published numerous articles on the topic (see <http://www.spiegel.de/netzwelt/icann>, v. August 21, 2000). The overall number of German applicants (unverified by ICANN as of July, 2000) reached 20475, compared with Italy’s 1670 and America’s 19501 (at http://members.icann.org/pubstats_unverified.html, v. August 21, 2000). The three candidates for representing Europe in the ICANN Board of Directors were all Germans, and ultimately one of them, Andy Mueller-Maguhn, won the elections.

(*Deutsche Bundespost*)”.¹¹ In fact, article 87 of the Basic Law explicitly affirmed that the management and regulation of telecoms was reserved to the state. Furthermore, the Federal government’s traditional concern for maintaining the consensus of all the economic and social actors inevitably required state monopoly for services and oligopoly for equipment (Natalicchi, 1996:278). The long process of reform, and later on, liberalization took place in three stages (Werle, 1999:112).

The first phase (*Poststrukturgesetz* or *Postreform I*) took place in 1989/90 and “...established three separate operational units for the provision of postal services (*Postdienste*), banking services (*Postbank*) and telecommunications services (*Telekom*)” (Werle, 1999:112), while the *Bundespost* became a holding company. *Postreform II* was approved by the Parliament in 1994, since “[a]fter the German Unification, the pressures for reform accelerated, one reason being Telekom’s need of capital and entrepreneurial autonomy in order to build a modern telecommunications network in the former East Germany” (Werle, 1999:112).¹² In this phase all of the three former branches of *Bundespost* became independent joint stock companies, with all the shares held by the federal government until 2000—and the majority of shares even after that date.

The final stage, *Postreform III*, was the Telecommunications Act (TKG), voted for by the *Bundestag* in July 1996 (entering in force in August 1996), to replace the old *Postgesetz*. The TKG established the Regulatory Authority for Telecommunications and Posts (*Regulierungsbehörde*), and ended the telecommunications network and phone services monopoly by January 1998, as required by the EU Directive.....Given these circumstances and the fact that the last phase of liberalization of the telecom sectors began only in 1996—mainly because of external pressure—it is impressive that, by 1999, Germany had “...one of the most liberal’ regimes by European standards” (Natalicchi, 1996:301).¹³

A remarkable case in point of how that wave of liberalization has changed Germany’s telecom and multimedia industry has been the outcome of the *Vodafone-Mannesmann* case.¹⁴ Here, the British mobile phone group Vodafone Airtouch launched 124bn-euro bid for its German rival, *Mannesmann*, in a hostile take-over at a time when

¹¹ <http://www.ispo.cec.be/esis/Regulation/DEreg08.htm> (v. August 2, 2000).

¹² On this point see also Natalicchi, (1996:299).

¹³ See also <http://www.ispo.cec.be/esis/Regulation/DEreg08.htm> (v. August 2, 2000).

¹⁴ The evolution of the cellular phone market is significant for the Internet (especially in Europe), because the next generation (the third) of wireless phones will offer reliable Internet access, thus turning e-commerce into m-commerce (mobile).

such actions were practically unknown in Germany.¹⁵ *Mannesmann* fought back, supported by the press (*Bild* in particular) and, also by Chancellor Schröder.¹⁶ Actually, BBC described the federal government as openly hostile to the takeover.¹⁷ After an initial bitter battle—and since many of *Mannesmann* shareholders were non-German—the two companies managed somehow to agree to a merger at the beginning of 2000, creating the world's largest mobile operator.¹⁸ This event occurred against the opposition of the German press and government. As *The Economist* (July 15, 2000:16) remarked, the take-over of *Mannesman* was a coup that blew Germany's market for corporate control wide open.

Like any other on-line country—with the obvious exception of America—Germany's access to the Internet is a recent event. In fact, the Internet or, more generally, computer networks came to the attention of the general public in two major instances, that is in the late 1980s and again much later in 1996.

In the late 1980s—more exactly between 1986 and 1989—the topics of hackers' break-ins and espionage began to appear in the West German press. "West Germans came late to computer hacking, in the early 1980s" as noted by Hafner and Markoff (1995:156), and the Chaos Computer Club (CCC) was founded only in 1984. The CCC was "chaotic" only in name, since the club "...was the very picture of meticulous organization, with a hierarchy of officers and subofficers,..." (Hafner and Markoff, 1995:156). With markedly left-wing sympathies, and adhering to the Hacker Ethics,¹⁹ the first CCC members appealed to the West German public's awareness about new methods of gathering personal data and tried to expose how federal authorities' computers were not safe from outside intrusion—thus signaling that people's data were not protected.

Outsiders took an immediate interests in Chaos. They viewed the club as a symbol of harmless dissent in West Germany. Chaos seemed the very picture of clean fun when compared to the dread Red Army Faction,...Chaos welcomed the attention, using any opportunity to hold a press conference, and the 1985 Hamburg congress was no exception.... The nightly news carried reports of the latest gathering of technological wunderkinder (Hafner and Markoff, 1995:158/159).

¹⁵ http://news6.thdo.bbc.co.uk/hi/english/business/the_company_file/newsid_527000/527730.stm (v. August 21, 2000).

¹⁶ http://news6.thdo.bbc.co.uk/hi/english/business/the_company_file/newsid_527000/527852.stm (v. August 21, 2000).

¹⁷ http://news6.thdo.bbc.co.uk/hi/english/business/newsid_576000/576197.stm (v. August 21, 2000).

¹⁸ <http://news6.thdo.bbc.co.uk/hi/english/business/newsid%5F621000/621222.stm> (v. August 21, 2000).

¹⁹ The English version of the Hacker Ethics can be seen at <http://hoshi.cic.sfu.ca/%7Eguay/Paradigm/Hacker.html> (v. September 4, 2000), while the German version is at <https://www.ccc.de/Hackerethik.html> (v. September 4, 2000). The latter version includes norms on using public data and protecting private data, as well as on not searching through people's data.

The CCC got its first notoriety in 1984, showing how easy it would be for them to collect money from a bank using the federal post BTX payment system, convincing many Germans that "...their accounts were helpless victims in the hands of electronic hoodlums" (Hafner and Markoff, 1995:158). Then again in 1987, the news that CCC associates had penetrated NASA computers, forcing NASA to admit the intrusion.²⁰ But when in 1989 the revelation that a group of young West Germans more or less loosely associated with the club had been spying for the Soviet bloc breaking into U.S. computers, the news shocked the West German public, and enraged the leaders of CCC, who feared the club could definitively acquire a bad name.²¹ Eventually three individuals loosely associated with the group were indicted and tried in 1990, but the sentence was rather lenient. Furthermore, it appeared that all that they had sold to the Soviets was freeware or innocuous information. In the words of a NSA scientist, it "[looked] like the Russians got rooked" (quoted in Hafner and Markoff, 1995:238).

The highly publicized events described here have given the hackers' community in Germany a considerable, albeit controversial, popularity. The Chaos Computer Club has now become "an icon" in cyberculture, to the point that it can present itself as "...a galactic community of human beings including all ages, genders, races and social positions....[that]demand unlimited freedom and flow of information without censorship".²² The current spirit of CCC, however, seems more in tune with the many computer civil liberties groups that are now active in the United States more than with the unconventional attitude of its beginning.²³

The other major moment of notoriety of the Internet, before it became the catchword for technologically savvy countries, was the "infamous"²⁴ case of CompuServe Germany. In 1995, German authorities decided to take strong action against the proliferation of pornography and Neo-Nazi propaganda on the Net, and in December of that year, Bavaria's

²⁰ Before the news came out, however, CCC leaders informed the *Bundesamt für Verfassungsschutz* BfV, (at <http://www.verfassungsschutz.de/> v. September 4, 2000), the federal office for the defense of the constitution ("...roughly equivalent to a domestic CIA...", Hafner and Markoff, 1995:199). The BfV, anticipating a conduct of law enforcement agencies that would become common in Italy and other European countries facing the same dilemmas, simply did not know how to approach the problem.

²¹ The whole story seen from "the other side", i.e. the person that first discovered the break-ins, has been elegantly presented in Stoll, Cliff (2000 [1989]) *The Cuckoo's Egg. Tracking a Spy Through the Maze of Computer Espionage*, New York: Pocket Books. The "Cuckoo's Egg" has become a classic of cyberculture.

²² <https://www.ccc.de/WarmWelcome.html> (v. August 1, 2000). NB: as the reader can note it is a secure server (https) which requires some preliminary steps before accessing the page.

²³ Indeed, the current CCC speaker is one of Europe's leading candidates for the position of regional director for Europe at ICANN.

²⁴ <http://www.kuner.com/> in *Internet Regulation*, translated by Christopher Kuner, (v. August 3, 2000).

law enforcement officials searched CompuServe offices. At that time, Felix Somm was head of CompuServe Germany, and when “[p]rosecutors found examples of child pornography and other illegal images through its network...[they] charged Somm with knowingly allowing it to reach CompuServe’s customers”.²⁵

The *Bundestag* had already passed the new Multimedia Law that entailed the decriminalization of ISPs ignorance of exchanged contents in 1997, and many experts and users alike believed that Internet newsgroups and Web sites were almost impossible to block. Nonetheless, in May 1998, Felix Somm was found guilty by a Munich court for complicity in thirteen cases of distributing illegal pornography.²⁶ The court, however, declared that Somm had failed to block CompuServe customers’ access to those sites, thus allowing child pornography to be sent across the network. Consequently, he received a two-year suspended jail sentence, and a DM100,000 fine. After Somm’s had been charged, CompuServe sought to avoid prosecution in Germany by stopping access to 200 message boards, and announcing that it would install screening software to avoid the recurring of such circumstances. CompuServe users, however, did not endorse such decisions, which, on the contrary, “...led to cries of censorship”.²⁷

The sentence was highly criticized inside and outside Germany. SPD *Bundestag* member Joerg Tauss called the decision “a catastrophe”, and the then CDU technology minister declared that “[t]he development of the Internet in Germany must not be held back,...[and that] [t]his is about the jobs of the future”.²⁸ In the end, in November 1999, the appeal high court of Bavaria ruled to reverse the guilty verdict against Somm. As a *Wired* reporter noted, “[t]he case was so convincing, even the prosecution did an about-face and pleaded for Somm’s acquittal”.²⁹

Somm’s exoneration was greeted by civil liberties organizations as a victory for advocates of freedom of speech on the Net. The act of being accused of curbing a fundamental human right certainly did not suit the German public opinion well—and a considerable number of Germans are also Netizens—and such views probably were taken into consideration by the German judges. However, concerns for human rights provide only partial explanation for the ruling. The German telecom market is one of the largest in the

²⁵ http://news6.thdo.bbc.co.uk/hi/english/sci/tech/newsid_102000/102111.stm (v. August 21, 2000).

²⁶ <http://www.wired.com/news/politics/0,1283,12571,00.html> and <http://www.wired.com/news/politics/0,1283,12884,00.html> (v. August 21, 2000).

²⁷ http://news6.thdo.bbc.co.uk/hi/english/sci/tech/newsid_102000/102111.stm (v. August 21, 2000).

²⁸ Quoted in <http://www.wired.com/news/politics/0,1283,12571,00.html> (v. August 21, 2000).

²⁹ <http://www.wired.com/news/politics/0,1283,12884,00.html> (v. August 21, 2000).

world and the richest one in Europe (Werle, 1999:121 and Natalicchi, 1996:301), and “Internet experts warned that the verdict could be dangerous for Germany’s developing multimedia industry, which has been promoted as a source of growth and jobs for the 21st Century”.³⁰ Suddenly, the critical shift of Germany from the Industrial to the Information Age—along with the ensuing economic expectations—could be jeopardized by perceptions among trade and diplomatic partners that Germany is a technophobe, Internet-resistant, rigid society. The “high-precision technologists” of Europe—i.e. the way Germans prefer to be regarded—must have viewed this prospect as utterly unacceptable.

A crucial consequence of the CompuServe-Somm case can be identified, as mentioned above, in the multimedia law (Information and Communication Services Act—*Informations und Kommunikationsdienste-Gesetz*, or IuKDG) that was approved by the *Bundestag* in June 1997 (in force since August 1997). Article 5, section 2, of the Law states that service providers “...are only responsible for third-party content which they make available for use if they have knowledge of such content and blocking its use is both technically possible and can be reasonably expected”.³¹ While the federal government has since then considered the law a necessary step toward fair regulation of the sector, “...a number of companies and legal experts are [now] concerned that the Law has not been properly thought out and represents too much regulation too soon”.³²

In sum, at the time of writing, the German key laws relating to the Internet were (1) the Telecommunications Act (TKG), (2) the Multimedia Law, and (3) the Digital Signature Act (SigG), all passed by the *Bundestag* in the second half of the 1990s. The latter—a “technical law” that does not address the legal validity of documents signed “electronically”—was also adopted following the EU Directive on digital signature. Since it relies on public key cryptography and electronic transmission, the future developments of this law as well will certainly effect the more general status of the Internet.

Two more critical points that may have serious consequences for the diffusion of *das Netz* must be mentioned here, that is the division of competencies between the federal government and the *Länder*, and the structural inadequacies of the German educational system. The former problem is critical because both federal and state governments have competency in regulating media and broadcasting. More precisely, the federal government awards licenses (one sender-to-one receiver configuration) and regulate telecom services,

³⁰ <http://news6.thdo.bbc.co.uk/hi/english/world/europe/newsid%5F524000/524951.stm> (August 3, 2000).

³¹ <http://www.kuner.com> in *Internet Regulation*, translated by Christopher Kuner, (v. August 2, 2000).

³² <http://www.kuner.com/> in *Internet Regulation*, translated by Christopher Kuner, (v. August 2, 2000).

while states have authority on media and broadcasting (one sender-to-many receivers configuration). Overlaps and administrative conflicts have already been rather common, and they are likely to be even more numerous, given the unstoppable processes of multimedia merging and Internet wireless growth. Needless to say, since “[b]oth sides tend to define their jurisdiction extensively....new problems concerning the jurisdictional confines of the federal government and the *Länder* governments have emerged” (Werle, 1999:120).

The other probable obstacle is the structural rigidity of the German educational system. The system was already criticized in the past for its lateness in adapting to changes that are brought about by transformations in the society as well as in the economy (Kotch et al., March 27, 2000:40/64). In the case of information technologies, telecom, the Internet and the New Economy this disadvantage could be fatal for Germany. *Der Spiegel* even referred to it as “the digital education catastrophe” on its cover page (March 27, 2000). Unsurprisingly, the federal government has considered addressing this problem a top priority, and thus, through Initiative D21, has planned to give “every pupil a laptop” and draw new generations’ attention towards ICT (Koch et al, March 27, 2000:42/44).³³ The Chancellor himself has stated that his government “...would like to make mastery of the Internet part of overall education”.³⁴ *Deutsche Telekom* has enthusiastically echoed the proposal of wiring of all schools by 2001.³⁵ Such solutions, however, will take time—as will the necessary training of computer-literate (or “digerati”) teachers.

The following image represents the infrastructure of points-of-presence and the backbone connections of Xlink, a major ISP in Germany (now KPNQwest) (courtesy of Cybergeography).³⁶ Although the picture illustrates only one of the main networks of Germany, it also gives an indication of how the key cities are interconnected and how German (and European) Internet traffic leaves the Old Continent.

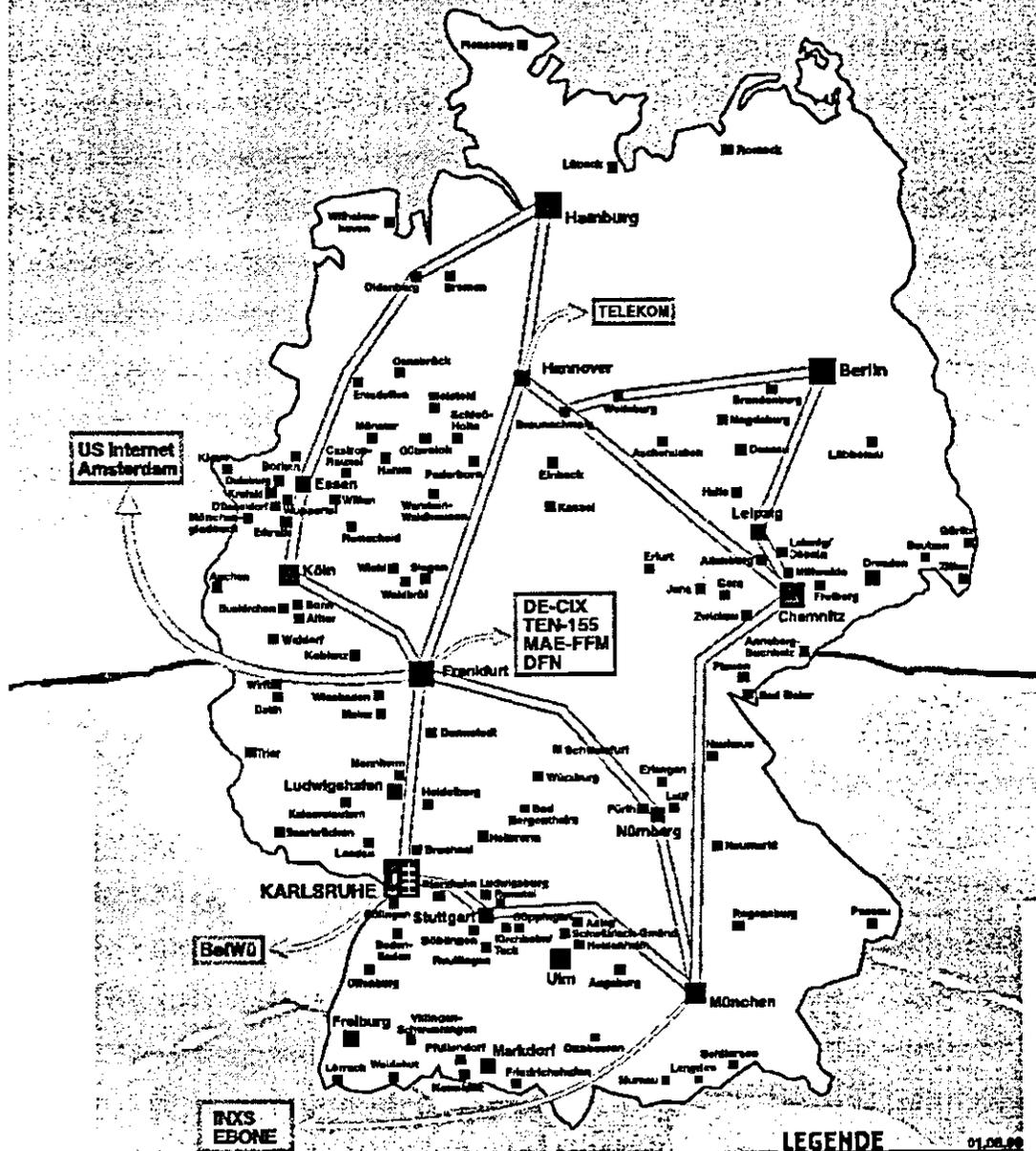
³³ <http://www.marktplatz-fuer-schulen.de/marktplatz/> (v. August 24, 2000). A similar initiative was launched in Italy in early 2000, at http://www.palazzochigi.it/fsi/eng/computer_x_student.htm (v. August 24, 2000). To interest more pupils and students in ICT, D21 (D21-Ambassador) has called for competent and enthusiastic volunteers that would visit schools presenting the Internet as well as the advantages of using computers, in “Projekte” at <http://www.initiaved21.de/> and <http://www.marktplatz-fuer-schulen.de/marktplatz/> (v. August 24, 2000).

³⁴ Quoted in <http://europe.cnn.com/2000/TECH/computing/09/18/germany.schroeder.reut/index.html> (v. October 4, 2000).

³⁵ <http://www.telekom.de/dtag/presse/artikel/0,1018,x528,00.html> (v. October 4, 2000).

³⁶ http://www.cybergeography.org/atlas/isp_maps.html (v. December 8, 2000, and several other times in the Fall 2000 and the Spring 2001).

XLINK VERBINDET!



XLINK POP-MAP

DAS POINT OF PRESENCE NETZ VON XLINK

LEGENDE 01.08.99

| | |
|--|------------------------------|
| | XLink Backbone bis 10 Gbit/s |
| | Feeder |
| | Hauptknotenstation Karlsruhe |
| | XLink POP mit Niederleistung |
| | XLink POP |

5.3 The Main Actors

The principal actors relevant for future Internet developments are the federal government and private industry, which are among the driving forces in the United States and Italy as well. Other important players are consumers' organizations and trade unions, and to a lesser extent, "counterculture" users' groups such as the Chaos Computer Club (CCC). The latter are important for the distribution of technical information.

Unlike the United States, where there is no official (or even unofficial) alliance between the federal government and the private sector, but rather a competitive "love-hate" relationship, and Italy where the government leads and the private sector is happy to follow, in Germany there is an unmistakable state-business coalition. What is peculiar in Germany is that the federal government and the private sector have agreed to co-ordinate their efforts to put Germany back in the forefront, among the small group of crucial countries that can seriously shape the future of the Internet.

A case in point is initiative D21, the project that has gathered together the government and private businesses to lead Germany in the transition from the Industrial to the Information Age.³⁷ As explained in the Introduction of this chapter, D21 perhaps represents the most noticeable instance of the co-ordination of forces and resources from different social, political, and economic actors to achieve the goal of "informatization" of Germany. D21 is further analyzed in section 3.2 on private industry—since the original idea came from that sector. The current government is as much involved in the initiative, as well as in various long-term projects that should open the way for Germany's entrance to the Information Age.

5.3.1 The Government (*Die Bunderegierung*) "at large"

Political scientists have long argued that national governments are not neutral actors. On the contrary, there are plenty of examples to show that they act differently according to which political parties are in power. Once again, this theory is confirmed by the stance of the current "red-green" coalition in Germany on the Internet. Former Chancellor Helmut Kohl's conservative government tended to be mostly concerned with issues such on-line criminal activities, in particular, child pornography and Nazi propaganda.³⁸ The new SPD-Green government of Gerard Schröder has tried to distinguish itself from the conservatives

³⁷ <http://www.initiatives21.de/content/memorandum-d21.pdf> (v. August 1, 2000).

³⁸ It should also be noted that after the CDU-CSU-FDP coalition came to power in 1982, it took it a few years (until the mid-1980s) to pursue its announced plan for telecom reform (Natalicchi, 1996:294).

by looking more "Internet-friendly" and by having an overall positive attitude to this new technology, emphasizing the noteworthy economic benefits that Germany may gather from moving into the Information Age and the New Economy.³⁹ Theory, however, is not always easily translated into praxis. Having a positive attitude toward the Internet does not mean that German ministries and undersecretaries of state are all comfortable with the Net, quite the contrary. According to *Der Spiegel* (Fischer, March 27, 2000:64/66), only a few in Gerhard Schröder's coalition government are really Internet wise. Among those few, the most notable representative is Foreign Affairs Minister and vice Chancellor, Joschka Fischer.

The world-wide notoriety of the CompuServe case is unequivocally seen by the present federal government as a "bad" start in the relationship between *das Netz* and Germany, which is also a government mission now to correct.⁴⁰ Overall, the SPD-Green government standpoint on the Internet can be summarized as "no (unnecessary) regulation" and that "the government should promote the Internet".⁴¹ To achieve this goal, the federal government has decided to cope with the many "technical" problems associated with the diffusion of the Net among the larger public in a particularly coordinated fashion. That is, data protection, cryptography, digital signature, etc. are all considered as different parts of the same challenge, therefore, they should be tackled with constancy, and with particular attention to their interdependent effects.⁴²

The main goal of the German government has been to implement "...a package of economic, training and technological measures aimed at moving Germany into a front-runner position in the international information society".⁴³ Hence, in 2000, the federal government approved DM 3 billion for the action plan "Innovation and Jobs in the Information Age" that should "...generate 350,000 new jobs in the multimedia field, triple the number of traineeships offered in this sector to 40,000 and boost the number of Internet users to 40 percent of the population".⁴⁴

³⁹ Joerg Tauss, SPD member of Parliament, and Chairman of the *Bundestag* Committee on the New Media, personal interview, Berlin, June 26, 2000. Mr. Tauss also remarked that the SPD has showed its commitment by devoting increasing resources and personnel to the solutions of Internet-related problems.

⁴⁰ Andreas Schaal, personal assistant to Parliamentary Secretary of State Siegmur Mosdorf, Federal Ministry of Economics and Technology (*Bundesministerium für Wirtschaft und Technologie*, BMWI), personal interview, Berlin, June 26, 2000.

⁴¹ Tauss, and Schaal, personal interviews.

⁴² Tauss, and Schaal, personal interviews.

⁴³ In "The Information Society", at <http://eng.bundesregierung.de/frameset/index.jsp> (v. August 21, 2000).

⁴⁴ <http://eng.bundesregierung.de/frameset/index.jsp> (v. August 1, 2000).

The federal government's program has been summarized in a document published by the BMWI and the BMBF meaningfully called "Information and Jobs in the Information Society of the Twenty-first Century" (1999). In the "Way to a Leading Position in Europe in the Information Society", the federal government intends to focus, among other factors, on:

1. "Internet for Everyone", i.e. making the Internet "...accessible to as wide a group in the population as possible..."; (24) mostly through
 - 1.1. the Information Society Forum, an organizational framework that should implement (1) through targeting special groups (such as women, and senior citizens) and subjects (education, development, democracy, art and culture, etc.), (26) and
 - 1.2. D21 (see next section); (26)
2. The need to promote multimedia technology in education (27) through:
 - 2.1. Linking schools to the Net, (28) and
 - 2.2. Computer networking and new technologies in universities (30) and vocational training; (32)
3. A better legal framework (34) in
 - 3.1. Telecommunications, (36)
 - 3.2. Competition and cartel legislation, (37)
 - 3.3. Data, consumer, and youth protection, (39-40)
 - 3.4. copyrights, (43)
 - 3.5. taxation, (44)
 - 3.6. civil, criminal, labor and social laws, (45-47)

etc. In this long list, three topics are of particular interest for this dissertation, namely, (a) e-government, (b) the "Green Card" scheme, and (c) IT security.

The idea of e-government in Europe (the first country in the world was the US) has been made fashionable by the British government, which has claimed that one-third of its services (in 2000) are available on line.⁴⁵ The format has been also adopted by the Italian and German governments, among others. The federal government has developed a multi-level approach to e-government that stresses the importance of

...equipping the administration with the modern electronic facilities for the conduct of its relations with the public and companies, and utilizing the possibilities offered by the network for democratic information, discussion and participation....People should be able to access original documents at any time on-line and perform transactions that are important for their daily lives with the administration via the Internet (BMWI and BMBF, 1999:71).

⁴⁵ <http://www.cabinet-office.gov.uk/index.htm> (v. August 30, 2000).

This plan incorporates practical, short-term actions such as tax declarations via the Net (ELSTER), and public tenders on the Net, as well as long term plans for tele-work in municipal administrations, and elections on the Internet. In this framework, a new communication link has been established between Bonn and Berlin (IVBV) that will represent the “essential technical basis” for the rationalization of the work of the government (BMW and BMBF, 1999:73). IVBV will also allow the federal government to achieve a leading position in the competition for efficiency among several European administrations.

Along the same lines, another most publicized initiative of the federal government to heighten Germany’s position in the global ITC competition has been the launch of the “Green Card”—a special working permit for non-German nationals. In May 2000 the German Cabinet approved two regulations (the so-called “Green Card”) regarding employment and “unbureaucratic” residence status of foreign IT specialists (the latter also requiring *Bundesrat* approval).⁴⁶ Under the Green Card scheme, these specialists must have a university degree, and the jobs for which they apply should generate an annual income of at least 100,000 DM. Finally, the visa for their employment period is initially for three years extendable to five (what happens next is unclear). During this time, they are free to change employers.⁴⁷

Although officially the Green Cards are available to all non-EU individuals, including, for instance, Americans or Canadians, the federal government is keen on attracting highly qualified computer scientists from developing countries, and in particular India (Baldas, July 29/30, 2000:I/II). This scheme, however, is bound to meet with considerable difficulties and criticism, locally and internationally. For instance, in early 2000 regional elections, the North Rhine-Westphalia Christian Democrats used the slogan *Kinder statt Inder* (“Children instead of Indians”). It was an apparent call for investing the money allocated for the Green Card program to train German pupils in software skills at school, rather than using it to attract IT professionals from India (Koch et al. March 27, 2000:41 and *The Economist*, August 5, 2000:32).

Moreover, the same people that the program should attract can, as easily, obtain jobs and working permits in the United States, which is seen as a more challenging and rewarding place for top-notch computer scientists. German media have lost no time “...in whipping out stories on Indian and other non-European software aces who had all turned up

⁴⁶ In “The Information Society”, at <http://eng.bundesregierung.de/frameset/index.jsp> (v. August 21, 2000).

⁴⁷ <http://eng.bundesregierung.de/frameset/index.jsp> (v. August 21, 2000).

their noses at Germany's blandishments, saying that if they were going anywhere it would be Silicon Valley" (*The Economist*, August 5, 2000:32). The perception of the United States as a more open, non (or less)-discriminatory society still holds true in a comparison with Germany. Certainly, Germany is a strong, modern democracy that has come a long way from its xenophobic past. Yet, the view that a mild racism is rooted in its society is still widespread in many countries, and racist occurrences—even against the very same people eligible for the Green Card (Baldas, July 29/30, 2000:I/II)—are likely to dishearten plenty of candidates. The same conclusions are likely to be reached by those that do not hold unfair views of the German society—as well as by the Germans themselves—but that, at the same time, are simply worried by the increasing activity of neo Nazi groups in Germany (*The Economist*, August 5, 2000:32).

Internet security, along with other items such as fast access or software user-friendliness, represents one of the crucial pillars on which the New Economy should be based. Indeed, with regard to Internet security, the federal government is fully aware that

[t]he worldwide network is...opening up an entirely new dimension of business and competitor espionage. The means of manipulating information of IT services is also growing rapidly.... Lack of security in information technology is causing damage worth billions every year at the expense of our economy and jobs....As the new information and communications technologies penetrate even further into every area of life entirely new dangers are being created, not only for the individual and for companies, but also for the state as well (BMWI and BMBF, 1999:41).

Unsurprisingly, the federal government has identified increasing Internet security as one of its critical objectives, and the digital signature and extensive use of encryption software (see section 4.3) are seen as key instruments to achieve that goal. The first agency earmarked for such task is the *Bundesamt für Sicherheit in Informationstechnik* (BSI).⁴⁸ The BSI is an *ad hoc* office that has been specifically set up to address threats to the security of government communications and the more general issue of Internet security in Germany. The other crucial player in such circumstances is the *Bundeskriminalamt* (BKA), Germany's federal police. The BKA and the BSI cooperative action is thus the primary instrument to enhance Internet security in Germany ((BMWI and BMBF, 1999:43).⁴⁹

⁴⁸ *Bundesamt für Sicherheit in der Informationstechnik* at <http://www.bsi.bund.de/> (v. August 1, 2000).

⁴⁹ It is worth noting here that the BSI and the BKA—along with the *Bundesamt für Verfassungsschutz*, BfV—all depend on the Ministry of Interior (BMI). The Chancellor, on the other hand, has direct control on the *Bundesnachrichtendienst* (BND), the federal intelligence agency. The BND has, among others, competence in international terrorism and organized crime that may include monitoring on-line activities.

The Bundesamt für Sicherheit in Informationstechnik and the Bundeskriminalamt

The Bonn-based *Bundesamt für Sicherheit in Informationstechnik* (BSI) was founded in 1990 with the mission of protecting the government communication networks and enhancing computer security awareness in general. The need for greater protection of computers and networks, however, had already become clear to the federal government and the parliament at the beginning of the 1980s.⁵⁰ Given its technical expertise—through the code office—and its institutional role, the BMI has assumed more and more responsibility in this field. By 1989 the IT security frame concept (*IT-Sicherheitsrahmenkonzept*) was fully developed, and the federal government made the decision that only a centralized federal office could implement that concept properly, and thus, in 1990 the BSI became operational.⁵¹

BSI is the main technical reference for (a) digital signature, (b) cryptography (whose use is unrestricted in Germany), (c) software for critical applications,⁵² (d) technical security in IT and computer systems, (e) teaching, training, and consulting in computer security in general. BSI is also the main administrator of the Internet-based government network between Bonn and Berlin (IVBV), and hosts a German CERT (Computer Emergency Response Team)—the other one, responsible for the German Research Network (DFN), is at the *Zentrum für sichere Netzdienste GmbH*, sponsored by the Federal Ministry for Education and Research (BMBF).⁵³

According to BSI experts, Germany's main problems with security are practically the same that all other countries where computer networks are present have, namely carelessness of users, and kids hacking Web sites whose security is lax.⁵⁴ In this respect, given the increasing reliance of Germany on computer networks, and the need for greater awareness of the general public of these problems, in 1999, the Federal Ministries for Economy and Technology (BMWi), the BMI, and the BSI have launched a joint initiative for Internet security (*Sicherheit im Internet*).⁵⁵ Such initiative aims to offer a “knowledge

⁵⁰ <http://www.bsi.bund.de/aufgaben/index.htm> (v. August 22, 2000).

⁵¹ <http://www.bsi.bund.de/aufgaben/index.htm> (v. August 22, 2000).

⁵² Software designed to run systems whose failure may imply loss of human lives.

⁵³ Stefan Wolf, Internet and Intranet security, BSI, personal interview, Bonn, August 11, 2000. The CERT is a structure present in many countries (CERT-IT is at the University of Milan and the oldest American CERT—there are plenty of them in the U.S.— is at the Carnegie Mellon University, which also acts as a coordinator center as FIST) and refers to a group of experts that are trained to tackle computer crises (e.g. viruses or DOS attacks). Many national CERTs are members of FIST (Forum of Incident Response and Security Teams) which works as a clearing house for information on computer attacks.

⁵⁴ Wolf personal interview.

⁵⁵ <http://www.sicherheit-im-internet.de/home.phtml> (v. August 1, 2000).

basis” to both experts as well as ordinary users (*Otto Normal-Surfer*).⁵⁶ Its Web site contains general information, thematic articles, and a list of brief and practical tips on how to make computers more secure.⁵⁷

Internet users, whether institutions or individuals, certainly need to develop a greater appreciation of the security procedures on the Net. However, there are organized groups of crackers⁵⁸ that cannot be stopped by ordinary security measures. These groups routinely try to penetrate governments’ and businesses’ computers to search for sensitive information. In the Federal Republic, these attacks against the government’s computer networks are contested by the technical experts of BSI.⁵⁹ On the one hand—the BSI staff admits—the next generation Internet (IPv6 or Internet II) with widespread use of public key cryptography will be more reliable and more difficult to crack. On the other hand, for the time being, the BSI is busy providing technical support every time there is suspicion of criminal activity on the Net. The actual investigative work is always carried out by BKA personnel.

According to the German Basic Law, police forces are primarily under the authority of the *Länder*, “[h]owever, since offenders move across state and national borders, it is necessary to have a central police agency for the whole of Germany—the *Bundeskriminalamt* (cf. Article 87 (1) of the German Basic Law)”.⁶⁰ The last amendment to the BKA’s competencies came with the BKA Law (BKAG) of 1997, which included several new specifications, particularly in the area of data protection.⁶¹ Since the BKA functions as the main hub and interface among the states and the federal police for the processing and transmission of data, it is small wonder that the Parliament has given particular attention to the treatment of individuals’ information once that information is no longer needed by the police. In addition to being the central exchange point for the police network in Germany (and thus giving it a very specialized competence), the BKA is actually conscious that

[t]he introduction of new technologies and methods can create new opportunities both for criminals and for law enforcement agencies. This is why the BKA analyzes new technologies in research and development projects with a view to possibilities for misuse by

⁵⁶ <http://www.sicherheit-im-internet.de/themen.phtml#20> (v. August 23, 2000).

⁵⁷ http://www.sicherheit-im-internet.de/showdoc.php3?doc=bmwi_theme_doc_1999938283743&page=1 (v. August 23, 2000).

⁵⁸ Malicious hackers are sometimes defined as “crackers”.

⁵⁹ Wolf personal interview. The understanding that it is always groups of several individuals that carry out the most dangerous attacks on computer networks is also based on personal observation.

⁶⁰ In *Das BKA/The Bundeskriminalamt—Facts and Figures* at <http://www.bka.de/> (v. August 5, 2000).

⁶¹ <http://www.datenschutz-berlin.de/gesetze/sonstige/bkag.htm#nr10> (v. August 5, 2000).

criminals and also with a view to possible applications in the field of police work. This information is put into an appropriate form for practical police work and applied.⁶²

As in other European countries, the opening up of the German market to European competitors has required the establishment of independent authorities. These agencies received powers of regulating market competition by the government. Two organizations are particularly relevant for the Internet, namely the Regulatory Authority for Telecommunication and Post, and the Antitrust Office.

The Regulatory Authority for Telecommunications and Post (RegTP)

On 1 January 1998, the Regulatory Authority (*Regulierungsbehörde*) became operational. The RegTP "...is tasked with promoting the development of the postal and telecommunications markets through liberalization and deregulation. It is equipped with...information and investigative rights as well as a set of sanctions".⁶³

The Regulatory Authority supposedly co-operates closely with the Federal Cartel Office (*Bundeskartellamt*), earmarked with the application of the federal law "against the limitation of competition" (*Gesetz gegen Wettbewerbsbeschränkungen* or *Kartellgesetz*—GWB). The GWB was approved in January 1958, and, to fulfil its provisions, the *Bundeskartellamt* was then created. The *Bundeskartellamt* is an "...independent higher Federal authority which is responsible to the Federal Ministry of Economics" (BMWi).⁶⁴ However, the exact realms of competence of the Cartel Office and of RegTP have never been laid out. Since the telecom sector has been a "natural monopoly" for years, and, thus, a predictable target for the Antitrust, disagreements and diversity of interpretations were to be expected.

In fact, according to Werle (1999:118), in March 1998, the RegTP approved a tariff scheme for *Deutsche Telekom*

...with the moderately reduced rates for national, long-distance calls and significantly lower rates for international and transatlantic calls. The scheme...[did] not provide for any reduction of the rates of local calls. This "unbalanced scheme was heavily criticized by the president of the Federal Cartel office (*Bundeskartellamt*) who suspects that DTAG abuses its dominance in the market for local calls. At the same time, the criticism was addressed to the NRA [National Regulating Authority, the RegTP] because—although expected by the TKG [Telecom Law] to do so—it did not ask the Cartel Office to file an assessment of the tariff scheme.⁶⁵

⁶² In *Das BKA/The Bundeskriminalamt—Facts and Figures* at <http://www.bka.de/> (v. August 5, 2000).

⁶³ http://www.regtp.de/en/behoerde/start/fs_01.html (v. August 2, 2000).

⁶⁴ http://www.bundeskartellamt.de/general_information.html (v. August 4, 2000).

⁶⁵ Exactly the same problem happened in Italy in 1998. *Telecom Italia* significantly decreased long distance and international calls (where competition was active) and only modestly reduced the cost of local calls that comprise the bulk of phone traffic.

Given the noteworthy relevance of the telecom sector for the New Economy, and the expectations of the federal government for the promotion of the *Informationgesellschaft*, clarification between the RegTP and the Cartel Office will be necessary. Overall, the attitude of the federal government toward the Internet is fairly positive, and not oriented toward excessive statutory control. On some issues such as open source, cryptography, the position of the German government is fairly "liberal". Still, on other topics, such as racist material on the Web, the government has a more repressive position.

5.3.2 *The Private Sector, Consumers' Organizations and Users' Groups*

The German post-war economy has been characterized by a "social consensus" system that required the cooperation of companies, trade unions and the government. More recently, it has undergone serious reassessment by its main actors. One of the clearest cases of such change is the information and communication technology (ICT) sector. Privatization of telecom started in 1998. The dimensions of, and the competition in, the German telecom market have since been remarkable, with more than 1800 registered telecom providers, and approximately 226,000 employees (1999/2000).⁶⁶ Unmistakably, what has happened in that market is a foretaste of what may happen to the whole German economy.

The *Vodafone-Mannesman* case has been a watershed and a "culture shock"⁶⁷ for the whole German industry, traditionally "aggressive" abroad but consensus-seeking on the home market. It signaled that social consensus and the prestige of the old industrial tradition clearly were no longer enough to guarantee a successful performance in the Information Age. Given open competition, the German telecom industry has begun this transformation. *Mannesmann* is one successful example of an engineering company that has become a leading telecom giant. *Deutsche Telekom* is a dominant telecom carrier in Europe that has been expanding globally (see, for instance, the acquisition of the largest GSM operator in the United States, Voice Stream). Yet, even DTAG's foreign acquisition policy has been criticized as "strategically bold, but tactically naïve" (*The Economist*, April 15, 2000:68), exemplifying how even the German telecom industry is still in the process of learning its trade in a liberalized world.

The most significant illustration of the process of transformation is Initiative D21, which started from the very beginning as a gathering of companies, including, but not

⁶⁶ In Mid-year 2000 Report, at http://www.regtp.de/en/market/start/fs_15.html (v. August 24, 2000).

⁶⁷ http://news6.thdo.bbc.co.uk/hi/english/business/newsid_602000/602406.stm (v. August 22, 2000).

limited to, the IT and telecom sectors.⁶⁸ D21 originated with IBM Germany at the end of 1998, when it became evident that, in information and communication technologies, Germany was falling behind not only the United States but also several OECD countries.⁶⁹ In early 1999, CEOs (Chief Executive Officers) from leading firms met informally for the first time, and quickly decided that for D21 to be successful, the federal government should be rapidly invited to join. In June 1999, the first meeting with Chancellor Schröder was held. A joint strategy was then outlined by D21 members that included (a) the adoption of an appropriate legal framework, (b) government's lead in e-commerce,⁷⁰ (c) supporting better education and qualification in schools (through providing PCs, educational software and training to all pupils as well), and (d) stressing acceptance of technology at all levels.⁷¹ The government backing of the initiative has been described as "enthusiastic", to the point that chairman of D21 is the Chancellor himself, and the BMI, the BMWI and the BMBF among others, are all members.⁷²

Particular attention is now being given by D21 members to (a) self-regulation of private industry, (b) the federal government as an IT leader, and (c) electronic democracy, (d) the Green Card project and (e) Internet security. D21 has financial resources for two to three years, after which period of time the initiative will undergo an effectiveness evaluation that will determine whether or not D21 has achieved its goals, should be extended or terminated.⁷³

Observers familiar with German economic behavior and traditions—coordination, consensus, and a broad effort of government and social and economic actors—see D21 as the predictable answer of Germany to the digital challenge. The EU is conspicuously absent

⁶⁸ Hans Jörg Denhardt, director of company activities with federal and regional governments, IBM Germany, personal interview, Berlin, June 28, 2000. Mr. Denhardt also stressed that individuals—who pay a 10,000 DM membership fee—and not companies are the actual members of D21. See also <http://www.initiatived21.de/> (v. August 22, 2000). Currently, the federal and *Länder* governments, banks, companies, universities, media and educational organizations are among the members. Whether the civil society is represented is an open question (the full list of members is at <http://www.initiatived21.de/home.php3?nav=profil/ucber&teaser=profil&text=profil/ucber/ucber.html> v. January 31, 2001).

⁶⁹ During the interview Mr. Denhardt remarked how, while it would be tolerable for Germany to lag behind the U.S., it would, on the other hand, be totally unacceptable to be behind any other European economy.

⁷⁰ The government is the principal buyer of many small enterprises' products and services. Hence, if the government moves toward purchasing on-line, all those firms will soon be obliged to follow suit. Denhardt personal interview.

⁷¹ Denhardt personal interview, and also <http://www.initiatived21.de/> (v. August 29 and 30, 2000 and March 24, 2001).

⁷² Denhardt personal interview. For the whole list of members see "Förderung" at <http://www.initiatived21.de/>.

⁷³ Two/three years is the delay period that has been estimated between Germany and the United States, that, however does not enjoy the same level of coordination as in D21. Denhardt personal interview.

in the D21 scheme, but this circumstance should be expected, since D21 is supposed to benefit Germany's own high-tech industry and not Europe's.⁷⁴

Consumers' protection is taken seriously in Germany. Two of the best known of such organizations began to operate in the sixties. The *Stiftung Warentest* was in fact founded as in 1964 by the (federal government) in Berlin, as an independent institute for carrying out comparative product tests and surveys on services, while the Association for Consumer Protection (*Verbraucherschutzverein*) began to function 1966.⁷⁵ The *Warentest*, whose scope is "to inform the public about objective characteristics of usefulness, functionality and environmental compatibility" of goods and services, provides, among other services, links to Web pages on secure e-commerce and other consumers' organizations.

One of the best known users' groups is the Chaos Computer Club (CCC). The CCC "...is a galactic community of human beings including all ages, genders, races and social positions....[which] demands freedom and flow of information without censorship".⁷⁶ The CCC's goal is to create "...a public awareness for the need to approach issues like (e.g.) security, privacy and key escrow from a more informed, open viewpoint".⁷⁷ The CCC's most recent (in 2000) "success" was the election of its spokesperson, Andy Müller-Maguhn as European representative to the ICANN's Board of Directors. Other important users' organizations include the Internet Society German Chapter (ISOC.DE).⁷⁸

Finally, the Open Source Privacy Guards project (GnuPG) is worth mentioning here, since, although federally funded, the effort of developing more secure software is left to a loose community of programmers and users so characteristic of many other Internet undertakings.

5.4. The Issues

The main Internet issues under discussion in the *Bundestag*, the federal government, the media and among the general public are not different from the themes being discussed in the United States, Italy or other advanced economies. They are freedom of speech,

⁷⁴ Needless to say that Germany is an active member of all EU R&D projects that will have spill-over effects for all the EU members without distinction.

⁷⁵ http://www.warentest.de/wtest/plsql/sw_selbst_selbst?kontaktnr=0&dateiname=sw_selbst_e_aufgaben.html (v. March 24, 2001).

⁷⁶ <http://www.ccc.de/faq.en.html> (v. March 24, 2001).

⁷⁷ <http://www.ccc.de/faq.en.html> (v. March 24, 2001).

⁷⁸ <http://www.isoc.de/> (v. March 24, 2001).

privacy and protection of personal data, electronic commerce and the New Economy. Cryptography is debated among more limited circles of advanced users, computer scientists and a few informed politicians, who are highly aware of the critical role that encryption software plays in all the other issues indicated above. Germany differs from the United States and Italy in that information is distributed fairly among institutional actors, while individuals have to rely on independent sources, of which, however, there are plenty. Another important distinction for Germany is that, among all the Internet issues, the most sensitive and discussed within the public is that of freedom of speech.

5.4.1 Freedom of Speech and Neo-Nazi Propaganda

Like any other democracy, freedom of speech is highly protected in Germany. Article 5 of the Basic Law clearly guarantees liberty of expression for all citizens, within the limits established by laws approved by the *Bundestag*. The same article explicitly states that there is no censorship.⁷⁹ As in many instances related to the Net, however, the concept of “freedom of speech” is not the same everywhere, and there are considerable differences even between the United States and Europe. More precisely, Web sites promoting hate or containing Nazi material are considered “free speech” in the U.S., but they are utterly illegal in Germany, which is, unsurprisingly, very sensitive about these issues.⁸⁰

Neo Nazi propaganda on the Internet, and the Web in particular, was, along with child pornography, the major concern of Kohl’s former government, and is progressively demanding more attention from Schröder’s coalition as well. That neo- Nazi activities are somehow co-ordinated at the international level through the Net is no news (*The Economist*, August 12, 2000a:16/17). The Blood & Honour network—with a Web page calling for the battle (“the call for terror”) against the “Zionist Occupation of Government”—has currently

⁷⁹ (1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt. (2) Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre. At <http://www.jura.uni-sb.de/BIJUS/grundgesetz/> (v. August 1, 2000). An English version of the Basic Law is available at <http://www.uni-wuerzburg.de/law/gm00000.html> (University of Wuerzburg, v. August 1, 2000).

⁸⁰ One of the best Web sites is that of Hate Watch at <http://www.hatewatch.org/frames.html> (v. August 1, 8, and 21, 2000), where excellent examples of pro-hatred and pro-Nazi Web sites are collected, such as <http://www.americannaziparty.com/>, <http://www.adolfhitler.com>, or <http://www.theneworder.org/> to name just a few. These Web sites only contain neo-Nazi propaganda, and there are more URLs on white supremacism, racial discrimination, anti-gay, anti-semitic, etc.

operational members in Germany (with the main group in Berlin),⁸¹ as well as in Scandinavia, Britain, and other countries (Kleffner, August 8, 2000:19).⁸²

Reference to Nazi ideology has begun to appear on Web pages actually based in Germany, and not simply downloaded or mirrored from sites in the U.S. For instance, in August 2000, a user registered the domain name www.heil-hitler.de with the Berlin ISP Strato, which managed more than a million names. After the news was reported on the media,⁸³ Strato unilaterally decided to cancel the registration of that domain (along with two other unspecified domains), even though no actual contents were present in that Web site (DPA, August 8, 2000:19). Strato stated that such action meant, "entering a new legal territory" (quoted in DPA, August 8, 2000:19), since active monitoring of what names are registered by users is not required to ISPs by current German law.⁸⁴

The need for effective international co-operation to tackle the issue of hatred and racist material on the Internet has not been missed by the federal government, whose representatives regularly call for a multilateral approach in such matters. For instance in June 2000, at a conference in Berlin on hate speech on the Web, Germany's Justice minister, restated the principle that "[w]hat is forbidden offline must be forbidden online", calling for global rules against hate speech on the Internet as well as stronger self-regulation by Web companies.⁸⁵ The width of this conundrum has truly become worryingly, according to Abraham Cooper, associate dean of the Los Angeles-based Simon Wiesenthal Center, who has remarked that the explosion of extremist Web sites in the United States proved the need for action, going from one hate site on the Internet in 1995 to over 2,000.⁸⁶ Yet, despite the gravity of the situation, the federal ministry of Justice had to admit that the goal of international regulation was a long way off, and that "it is very difficult to establish dialogue with the United States".⁸⁷

Unsurprisingly, the federal government is caught in a dilemma, that is, how to isolate or limit the channels of on-line diffusion of racist and hatred propaganda without

⁸¹ However, as of August 2000, the Berliner group's Web site <http://www.bloodandhonour.de/> is *nicht erreichbar* (not reachable).

⁸² The Web site is at <http://www.bloodandhonour.com/> (v. August 8, 2000)

⁸³ http://www.denic.de/doc/DENIC/presse/domain_geloescht.html (v. October 6, 2000), and <http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/fr-08.08.00-000/default.shtml&words=Hitler%20de> (v. October 6, 2000).

⁸⁴ The ISP Strato explained its delayed action by stressing that with over 200,000 new domains registered every month it was impossible to keep track of that particular name (<http://www.heise.de/newsticker/data/mbb-07.08.00-000/> v. October 6, 2000).

⁸⁵ Quoted in <http://www.wired.com/news/politics/0,1283,37251,00.html> (v. August 8, 2000).

⁸⁶ <http://www.wired.com/news/politics/0,1283,37251,00.html> (v. August 8, 2000).

⁸⁷ Quoted in <http://www.wired.com/news/politics/0,1283,37251,00.html> (v. August 8, 2000).

hindering the expansion of the Net in the country. Germany, like many other democracies, faces such dilemma, under different guises, every day. For instance, in the effort to curb neo Nazi activities, the Berlin major (CDU) has urged federal government to consider measures to restrict the right to manifest (Gessler, August 7, 2000:19 and Maschler, August 8, 2000:7). Moreover, the present *Bundesminister des Innern* Otto Schily (a former Green) has demanded the neo Nazi *Nationale Partei Deutschland* (NPD) be banned, and if the Constitutional Court agrees, it will be the first such instance in Germany in the last 50 years.

Such move, however, has been resisted from inside the red-green coalition on the basis that it could create a serious precedent that may be used to limit the rights to manifest for other causes. Indeed, Schily's former party colleagues have already argued that this solution could become a dangerous precedent for freedom of speech (both off and on line), and association, and the domino effect could continue.⁸⁸ Consistent with the Greens' view, *The Economist* (August 12, 2000a:17) has also observed that "...to uphold the freedom of expression, as Germany is committed to do, is also to uphold the freedom to offend—however vile that may be".⁸⁹

Because of its past, Germany and a large part of Europe are more sensitive to permitting hatred discourses on- or off-line. It is not a matter that Germany or Europe are more restrictive with free speech than the United States; it is more that certain free speech evokes memories that many Europeans find very hard to bear. Thus, Germans do not feel that their freedom of speech is diminished if their government wants to block hatred and racist Web sites. In fact the majority of Germans think that something should be done about the neo-Nazi problem, although there is disagreement about the solutions. All the major players of the debate on Internet control share these feelings, and consensus on some limits to racist and hatred propaganda on-line will likely appear in the short run.

While an international regime could be an effective answer to this problem, the consensus on definitions of "hatred" or "racism" would be hard to reach and, for example, Germany and the United States would certainly have the difficulty in working together. Blocking Web sites or canceling domain names in Germany could be effective measures against neo Nazi propaganda, but they have to be part of a larger, integrated strategy that

⁸⁸ These facts happened in the Summer of 2000 in relation to the decision of the NPD to march through the Brandenburg Gate on January 19, 2001, the Holocaust memorial Day. The words of a spokes-person for the Trade Union Association are indicative of what many Germans thought about such event: "in 1933 the SA marched through the Brandenburg Gate. And in January 2001 we should see the NPD in march? No way!" (Gessler, August 7, 2000:19, my translation). In the end, the government decided that it had no legal basis to prohibit the march as an expression of freedom of speech.

⁸⁹ The British view of freedom of speech is obviously closer to the U.S. interpretation.

includes addressing problems like unemployment in the new *Länder* and the education of new generations.⁹⁰

5.4.2 Privacy

Because of the Nazi experience and, later on, of the pervasive presence of secret police in the GDR—of which West Germans were also well aware—privacy, being it on- or off-line, is a crucial issue, and is taken extremely to heart in Germany. The right of the German people to their privacy is explicitly guaranteed in the Basic Law. Article 10 states that the privacy of letters as well as the secrecy of post and telecommunication are inviolable, and those restrictions may only be ordered by law.⁹¹ The main legal basis for protection of personal data is the *Bundesdatenschutzgesetz* (BDSG), i.e. the Federal Data Protection Act of December 20, 1990, further amended by law September 14, 1994. The BDSG specifically states that “[t]he purpose of this Act is to protect the individual against his right to privacy being impaired through the handling of his personal data”.⁹² In addition to that, each *Land* has its own state law on data protection that is drafted along the lines of the BDSG.⁹³

Having adopted the BDSG in the early 1990s, Germany has remained one of the few European countries that have not adopted the EU Directive 96/45EC on personal data protection. However, the prevalent German jurisprudence has emphasized that the BDSG should be interpreted according to the EU Directive.⁹⁴ The *Bundestag* has scheduled to discuss a new privacy law, integrating the EU Directive, in late 2000.⁹⁵

The 1996 Telecommunications Act itself asserts the secrecy of telecommunications (art.85), and the prohibition to intercept (art.86). These provisions also apply to telecommunications companies (“legal persons”) which gather detailed data on location of

⁹⁰ Regardless of the results, Germany’s fight against neo-Nazi propaganda and memorabilia will likely continue into the distant future. After France’s order to Yahoo! to ban French customers from auctioning Nazi memorabilia, once again, in November 2000, German prosecutors began to investigate Yahoo! on suspected on-line auctions of copies of Hitler’s *Mein Kampf* (<http://europe.cnn.com/2000/WORLD/europe/germany/11/27/berlin.yahoo/index.html> v. December 8, 2000).

⁹¹ (1) Das Briefgeheimnis sowie das Post und Fernmeldegeheimnis sind unverletzlich.
(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. At <http://www.jura.uni-sb.de/BIJUS/grundgesetz/> and also <http://www.uni-wuerzburg.de/law/gm00000.html> (v. August 1, 2000)

⁹² <http://www.datenschutz-berlin.de/gesetze/bdsg/bdsgeng.htm#nr1> (v. September 5, 2000) for the English version and <http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg1.htm#nr1> (v. September 5, 2000) for the German one.

⁹³ For instance, the law for the state of Berlin, the *Berliner Datenschutzgesetz* (BlnDSG), was approved by the local senate in 1995 (<http://www.datenschutz-berlin.de/recht/bln/blndsg/blndsg.htm>, v. September 5, 2000).

⁹⁴ See Puolo G. and L. Liguori, “Germania, Piu’ Attenzione ai Trattamenti Pubblici” in INTERLEX, October 5, 2000, (<http://WWW.INTERLEX.IT/675/psglaw5.htm> v. October 5, 2000).

users and traffic. These data may be collected, processed and used only for the proper functioning service offered (art.89).⁹⁶ Moreover, the 1997 Multimedia Law states that "...any personal data concerning the process of retrieval, access, or any other use are deleted immediately after termination, insofar as any further storage is not necessary for billing purposes".⁹⁷

Finally, to further strengthen the protection of individual privacy, as in other EU countries, independent data protection agencies (*Datenschutz*) have also been established in all the *Länder* as well as at the federal level (in Bonn). These agencies are competent for violation of privacy committed by public administration bodies, while the protection from such acts in the private sector is left to companies' self regulation—naturally, within the domain of federal (BDSG) and state laws. Undoubtedly, the *Datenschutz* take their role seriously and proficiently.

Generally speaking, the principle presently regulating the government's or law enforcement agencies' access to personal data is that of *principle of necessity*. That is, the police, under warrant, can have access to personal information of a specific individual, or individuals, but only with regard to that identifiable person, or persons. For instance, investigators cannot ask for the record of a month of phone calls of an entire building or block, only to monitor one suspect's activities.⁹⁸ In layer n. 2 (teleservices) and 3 (contents) of the telecommunications system, since data are differentiated—it can be distinguished which communication belongs to whom—and rules are strictly followed.

A noteworthy exception to this rule is presently in layer n.1, i.e. the transmission layer. There, bytes representing contents and bytes representing addresses are all mixed up together, making any distinction impossible. Nonetheless, by analyzing this communication traffic it is possible to pinpoint the exact location of callers and to follow their movements. At this level, law enforcement agencies do not need a warrant to access these data. This is an area of on-going quarrel between the data protection commissioners—who would like to

⁹⁵ The new law will include, for instance, the EU Directive provisions on personal data transferred outside the EU.

⁹⁶ <http://www.datenschutz-berlin.de/gesetze/tkg/tkge.htm#p85> (v. September 5, 2000). The federal and local organizations entitled to demand information on telecommunication traffic are (1) courts, public prosecutors' offices and other judicial authorities as well as other criminal prosecution authorities, (2) federal and state, police forces for purposes of averting danger, (3) customs investigation offices for criminal proceedings and the Customs Criminological Office, and (4) the federal and state authorities for the protection of the Constitution (e.g. BfV and BKA), the Federal Armed Forces Counter-Intelligence Office and the Federal Intelligence Service (*Bundesnachrichtendienst*, BND).

⁹⁷ <http://www.kuner.com/> in *Internet Regulation*, translated by Christopher Kuner (v. August 2, 2000).

⁹⁸ Prof. Hansjürgen Garstaka, Data Protection and Information Access Commissioner of the State of Berlin, personal interview, Berlin June 27, 2000.

see this rule changed and limited only to heavy crime—and the police forces that would rather maintain the *status quo*.⁹⁹ Considering that with current GPS phones it is possible to pinpoint the exact location of a person within one-meter error, it is understandable why the difference of opinion between the BMI and the *Datenschützer* commissioners is so relevant.¹⁰⁰ In this respect, another significant theme significant for the protection of personal data is the current discussion among G8 governments about for how long those data should be stored and made available to law enforcement officers.

One last point of controversy is the behavior of companies not physically resident in the Federal Republic territory. In fact, while German companies do not come under the scrutiny of *Datenschutz* agencies, they are nonetheless obliged to comply with German laws. What about foreign companies, which are legally not compelled to do so? The circumstance is less problematic than it first appears. Although foreign companies could gather data about German citizens and then sell them, most companies are eager to do business in Germany or have German associates.¹⁰¹ Therefore, it is important for those companies not to appear to be breaking German laws, but, on the contrary, that they demonstrate full adherence to German rules as a sign of respect for their business partners.¹⁰²

To conclude, the German attitude towards and legislation on the treatment of personal data is stricter than that of the United States, where company self-regulation is the rule, and where individuals are not even alerted that information about them is collected. This outcome clearly emerged in the quantitative analysis, where Germany (and Italy) scored higher than the United States in the Privacy Index. More interestingly, however, is the fact that the German position on privacy is also different from Italy's, a fellow EU member. In the latter the treatment of personal information is in general allowed with the consent of the selected person (the law on privacy fostering the protection of the individual's rights). In the former, the handling of personal records is in general forbidden, within the exceptions built in the law itself.¹⁰³ Privacy is valued by all players of the Internet debate. In fact, requests by federal and local law enforcement agencies for more monitoring powers are usually met with the fierce resistance of the data protection

⁹⁹ Garstka, personal interview.

¹⁰⁰ Garstka, personal interview.

¹⁰¹ See, for instance, how key Internet companies like Yahoo! or Amazon have been eager to establish German branches of their business.

¹⁰² Garstka, personal interview.

¹⁰³ See Puolo G. and L. Liguori, "Germania, Piu' Attenzione ai Trattamenti Pubblici" in INTERLEX, October 5, 2000, (<http://WWW.INTERLEX.IT/675/pselaw5.htm> v. October 5, 2000).

commissars, and opposition by pro-liberties and users' groups. The private sector is not inclined to support those requests either.

5.4.3 Encryption and Digital Signature

A logical consequence of what has been described in the previous section is that the availability and use of strong cryptography is completely unrestricted. According to EPIC's "Cryptography and Liberty" report, "Germany has been at the forefront of countries opposing restrictions on encryption. It has been a counter-balance to U.S. efforts to promote key escrow and international restrictions".¹⁰⁴ In fact, from 1998 to 2000, Germany's score in the Cryptography Index has consistently been "green", that is "no restriction".¹⁰⁵ "No restriction" to use, and support for Germany's encryption products have been, since June 1999, the mainstay of the federal government's official policy on encryption (BMWI and BMBF, 1999:42).

Not content with allowing free use of encryption software for individuals, the federal government has actually taken a considerably different stance on cryptography than the U.S. government, by providing a substantial research grant for open source software to independent software developers.¹⁰⁶ In November 1999, the BMWI awarded 318,000 DM (circa \$170,000) to the German Unix Users Group (GUUG) to help them enhance a program known as GNU Privacy Guard, which is an open version of the widely popular software package Pretty Good Privacy (PGP). According to the *New York Times*,

[t]he move is controversial because the United States government has been lobbying the German government to restrict such technology for fear that criminals and terrorists will use it to cloak their actions. The German government cited the need to protect electronic commerce and private communications against these same criminals and terrorists.¹⁰⁷

The decision to intensify research on open source software—including the progressively more popular Linux operating system—has also been made to decrease the reliance on only U.S.-made software, after it appeared that some of that software was not entirely secure. In fact, "[in] 1997, the Swedish government was astounded to learn that the version of Lotus Notes that they were using came with a "key escrow" feature that

¹⁰⁴ <http://www2.epic.org/reports/crypto2000/countries.html#Heading40> (v. August 23, 2000).

¹⁰⁵ <http://www2.epic.org/reports/crypto2000/countries.html#Heading40> (v. August 23, 2000).

¹⁰⁶ Open source software means that the source code of programs is publicly available and can be modified by developers other than the ones that wrote the software originally.

¹⁰⁷ Reproduced in http://www.sicherheit-im-internet.de/showdoc.php3?doc=bmwi_theme_doc_2000947923935&page=1 (v. August 31, 2000).

apparently made it easy for the U.S. government to read documents".¹⁰⁸ Apparently, even Microsoft has hidden a "NSAkey" instruction into the encryption interface for its software.¹⁰⁹ Given such circumstances, expectations for increasing security through open source software development are understandable. This action will also foster Germany's position as leader in encryption software. According to a representative of GUUG, in fact, the "United States is the land of software, but not in the field of cryptography anymore.... Other countries like Germany are much better now".¹¹⁰

To implement the EU Directive 1999/93/EC (December 13, 1999) on a "Community Framework for Electronic Signatures", Germany adopted the Digital Signature Act (SigG) in June 1997 to establish a uniform legal framework for electronic signatures. The "Digital signature" is "...a seal affixed to digital data which is generated by a private signature key and establishes the owner of the signature key and the integrity of the data...".¹¹¹ The signature key certificate is awarded to individuals by a certification authority, recognized by the RegTP, while technical studies on reliability and security digital signatures are conducted by the BSI.¹¹² The technology adopted for digital signatures is based on public key cryptography, which is one of the most common ways of producing digital signatures.

The SigG does not affirm the legal validity of digital signatures. Rather, as a "technical law",

...its purpose is to provide the conditions for a secure infrastructure for the use of digital signatures in Germany. While compliance with the Law is "voluntary", the German government is open about its intention to create a de facto standard for the use of digital signatures; for this reason, it is a matter for concern that the Federal Office for Information Security (BSI), an NSA-type government agency, is deeply involved in setting technical standards under the law. Thus, there is reason to doubt that the Law will lead to a competitive, market-driven procedure for digital signatures in Germany.¹¹³

After two years since the implementation of the Act, the *Regulierungsbehörde* (the Regulatory Authority for Telecommunications and Posts, RegTP) has licensed two

¹⁰⁸ Reproduced in http://www.sicherheit-im-internet.de/showdoc.php3?doc=bmwi_theme_doc_2000947923935&page=1 (v. August 31, 2000). Lotus was used by the Swedish parliament and the military.

¹⁰⁹ <http://www.spiegel.de/netzwelt/politik/nf/0,1518,53395,00.html> (v. August 31, 2000). Interestingly enough, it is public domain that the BSI cooperates with the NSA on problems related to protecting communications (Wolf, personal interview).

¹¹⁰ Quoted in http://www.sicherheit-im-internet.de/showdoc.php3?doc=bmwi_theme_doc_2000947923935&page=1 (v. August 31, 2000).

¹¹¹ http://www.regtp.de/en/gesetze/start/fs_04.html (v. August 3, 2000).

¹¹² <http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/index.htm> (v. August 31, 2000). The RegPT and the BSI are also closely located in Bonn.

¹¹³ Christopher Kuner' in *Digital Signature*, at <http://www.kuner.com/> (v August 3, 2000).

certification authorities, namely the *Deutsche Telekom AG* and *Deutsche Post AG*, which currently provide nationwide services under the Signature Act.¹¹⁴ Five more potential certification authorities have accepted the common technical standard for signatures required by the Act. Furthermore, the federal government approved giving the same status to the electronic and pen signatures in August 2000, while the *Bundestag* is expected to pass the law in the Fall.¹¹⁵

The combination of two-year practice of the digital signature and of on-line payment (albeit throughout the disappointing *Deutsche Post* BTX system) has provided Germany with a comprehensive experience in ICT security infrastructure based on encryption software. This experience may not be as advanced as the United States, but it is certainly far superior to that of Italy and most of the other European countries.

Germany has a more favorable view of individual users' access to encryption software, and such circumstance stands out clearly in my database as well as in the case study. Indeed, of all the case-studies considered here, Germany has the most liberal regime on encryption, to the point that the federal government has financed an open source project (the GnuPG) for public key encryption. As in Italy and the United States, also in Germany, the private sector, pro-liberties NGOs, consumers' organizations and users' groups are all in support of unrestricted encryption. In addition, data protection agencies and even the federal government support this position. It would be very hard for the law enforcement/national security community to oppose such coalition.

5.4.4 *New Economy, e-commerce and ICANN*

As mentioned earlier, Germany sees itself as the leading European actor for the New Economy, e-commerce, telecom and multimedia, a goal of both government and industry. The Italian newspaper, *La Repubblica*, has recognized that the decisive element that has re-launched the German economy in 2000 has been the joint effects of government support, biotechnology research, and the Internet (Tarquini, July 3, 2000:9). In fact, by the end of 2000, Germany could maintain that "[t]he German economy has taken well to the internet, with only 2 per cent of all companies without it, or not planning to launch online activities,...".¹¹⁶ As in Italy where the New Economy is seen as a key opportunity for its

¹¹⁴ http://www.sicherheit-im-internet.de/download/SigGEckpunkte_eng.pdf (v. August 1, 2000).

¹¹⁵ http://dailynews.yahoo.com/h/ap/20000816/tc/germany_e_signatures_1.html (August 31, 2000).

¹¹⁶ <http://www.europemedia.net/shownews.asp?ArticleID=722> (v. December 8, 2000). The study—*"eBusiness in der deutschen Wirtschaft - Status quo und Perspektiven 2001"*—was commissioned by the German Employers Association (*Bundesvereinigung der Deutschen Arbeitgeberverbände*, BDA) and the

Southern areas, the German federal government has high hopes that bringing Germany into the Information Age will help foster the economic development of the new *Länder*—particularly in those areas that seem already technologically more prepared such as around Jena (Tarquini, July 3, 2000:13). Overall, Germany's strategy for success in the New Economy appears based on a twofold approach: reinforcing those areas in which Germany has already a comparative advantage, and entering and consolidating those fields that are essential for the future development of the Net.

According to some observers, an area of the New Economy in which Germany may take the lead is that of handling online micro-payments.¹¹⁷ In fact, *Deutsche Telekom* has moved its old, text-based network of online services, BTX, to the Internet, including BTX's secure system of micro-payments. Now, T-Online users can "...download special software and are then able to purchase useful services or content with a single click, no cookies or authorization necessary. Charges show up on users' telephone bills".¹¹⁸ However, this system will have to contend with other U.S.-based ones such as Billpoint,¹¹⁹ an undertaking by eBay, the best known auction site on the Web, or eBillPay,¹²⁰ which is an initiative of the U.S. Postal Service. Competition from these established services will hence be stiff for German products. Moreover, despite current claims, in the past, the federal government has conceded that the BTX investment had been an "extravagant failure" (Hafner and Markoff, 1995:158).

On the other hand, an instance of Germany's new boldness in crucial Internet matters is the German participation in elections for ICANN's new board of directors. In February 2000, ICANN began inconspicuously to prepare the election. It launched its call for "voters" from five geographical "regions", with the goal of registering between 5,000 and 10,000 overall by July 31.¹²¹ The initiative remained relatively unknown to most Internet users until quite late, that is the spring. In May 2000, however, *Der Spiegel* decided

consulting firm KPMG on a sample of 2,852 companies in September/October 2000 (<http://www.kpmg.de/about/press-office/2000/11/20.html> v. December 8, 2000).

¹¹⁷ <http://home.cnet.com/specialreports/0-6014-7-1538059.html?st.sr.6014-7-1538058.txt.6014-7-1538059> (v. August 1, 2000).

¹¹⁸ <http://home.cnet.com/specialreports/0-6014-7-1538059.html?st.sr.6014-7-1538058.txt.6014-7-1538059> (v. August 1, 2000).

¹¹⁹ <http://www.billpoint.com/> (v. September 1, 2000).

¹²⁰ <http://www.usps.com/ebpp/welcome.htm> (v. September 1, 2000).

¹²¹ <http://members.icann.org/news.htm#exceeds> (v. September 6, 2000). The "regions" were Europe, North America, Latin America, Asia and Pacific, and Africa. In the end, *ICANN@large* had more than 158,000 applicants, of whom over 50% were verified (i.e. their email address was matched by, and verified through a physical postal address). According to the organization, it was "an overwhelming success", although one may wonder if ICANN has really been pleased with being confronted with such a large number of users, instead of

to publicize and promote (“I can! eLlection 2000”) the event with weekly coverage, and interviews with several candidates.¹²² The idea was tremendously successful, and in the end Europe had almost 36,000 applicants—more than any other region but Asia—57% of which were Germans.¹²³ Moreover, not only the majority of European candidates were Germans, but the three most likely were all Germans.¹²⁴ Two of these candidates had strong “civil society background”—that is probably why they were endorsed in first place—and have stated that they want to represent Internet’s ordinary users, not the corporate world.¹²⁵ The most popular of them, Andy Mueller-Maguhn speaker of the Chaos Computer Club, was ultimately elected to the post of European representative at ICANN with 5948 (on 11309) valid votes.¹²⁶ Given ICANN’s competence on domain names, such programmatic platforms may have significant effects for the future of Internet companies in Germany, and elsewhere.

While waiting for the New Economy and the Information Society to become realities for the whole of Germany, in August 2000, the federal government reaped some of the benefits of this “business revolution” (Woodall, September 23, 2000). In fact, the new generation of telecom devices that should make the Internet truly mobile, the UMTS, went to auction. “The auction of third generation mobile phone licenses for Germany has ended with record takings for the government....[since, in the end]...the combined value of the bids was more than 50.5bn euros (\$46.1bn or £30.4bn)”.¹²⁷ The total sum was higher than

the small-technical group approach so typical of the past (<http://members.icann.org/index.html> v. September 6, 2000).

¹²² <http://www.spiegel.de/netzwelt/politik/nf/0,1518,74725,00.html> (v. September 6, 2000). *Der Spiegel* special section on ICANN is at <http://www.spiegel.de/netzwelt/icann/> (v. September 6, 2000). Germany’s example was also followed by Italy, but only in mid-July.

¹²³ This figure represents “unverified” voters, i.e. individuals that submitted the on-line applications but did not complete all the steps of the procedure. 21,600 voters were from North America (19,500, or 90% from the U.S.), and 93,800 from Asia and Pacific. In the European quota, Italy counted for roughly 5%. My calculations are based on figures available at ICANN public statistics.

http://members.icann.org/pubstats_unverified.html (v. September 6, 2000 and January 31, 2001).

¹²⁴ Candidates have to be “endorsed” by registered voters. This evaluation is based on candidates that have received the highest numbers of endorsements (<http://www.ICANNnot.org/icanncl.cgi?s=e&r=EU&l=e> v. September 6, 2000). The high numbers of German voters and candidates, however, should be explained not only by the attention given by German media, but also by the fact that Germany is Europe’s largest country, and in all the other regions the most likely winners came from large countries with many voters, i.e. Brazil, the United States, South Africa, China and Japan.

¹²⁵ See the interview with Andy Müller-Maguhn, speaker of the CCC, at <http://www.spiegel.de/netzwelt/politik/nf/0,1518,90471,00.html> (v. September 6, 2000), and his program at <http://members.icann.org/nom/cp/84.html> (v. September 6, 2000), as well as Jeanette Hofmann interview at <http://www.spiegel.de/netzwelt/politik/nf/0,1518,89936,00.html> (v. September 6, 2000) and her program at <http://members.icann.org/nom/cp/86.html> (v. September 6, 2000).

¹²⁶ <http://www.election.com/us/icann/region2.html> (v. November 7, 2000).

¹²⁷ <http://news6.thdo.bbc.co.uk/hi/english/business/newsid%5F884000/884203.stm> (v. August 24, 2000). The six winners are: *Deutsche Telekom*, *Mobilfunk (Vodafone-Mannesmann)*, *E-Plus (Hutchinson Whampoa)*,

many—including the bidding companies themselves—expected, and higher than the already rich auction that the British government had launched in April 2000 (£22.47bn or \$35.4bn).¹²⁸

Even if it takes Germany some effort and time to narrow the gap with the United States in the New Economy, signs that the goal can actually be accomplished are emerging. When in 1996-99, American on-line brokers started to expand in Europe, they quite naturally looked at Britain, since it was English-speaking, Internet hip and with a broad-based “shareholder culture” (*The Economist*, August 12, 2000b:73). Nonetheless, Britain is now behind a number of places for on-line share dealing accounts, and most notably Germany, where on-line brokering is quickly taking off along with the Net. Germany’s mission may be quite possible, after all.

The large majority of actors is in favor of e-business and the New Economy, as one would expect. This party includes the private sector, the federal and governments, and, with some cautiousness, also consumers’ organizations and users’ groups (particularly for the marketing of the open source project). Once again, with the notable exception of dangers of cybercrime (which is nevertheless exclusive competence of law enforcement), the national security side has hardly expressed any disagreement on this topic.

5.5 Conclusions

To a large extent, Germany’s more recent experience with the Internet reveals many similarities with Italy and, even if less so, with the United States. With reference to the broader area of telecom, some observers have noted that “[a]lthough Germany was no driving force in the 1980s,....[it] was one of the countries which viewed the liberalization process as part of an effort to make Germany more competitive in a market economy” (Eliassen and Sjovaag, 1999:260). Allowing for technical as well as political differences between the CDU-led government of the 1980s and the current leadership, the SPD-Green coalition has displayed the same determination of Kohl’s era with specific regards to the Net and the New Economy. To dismiss any doubts, Chancellor Schröder himself has repeatedly stated that he and the industries “...are resolved to make Germany a leading

KPN), *Viag Interkom* (BT, E.On, Telenor), *MobilCom* (with *France Telecom*), and Group 3G (*Sonera, Telefonica* etc).

¹²⁸ <http://news6.thdo.bbc.co.uk/hi/english/business/newsid%5F884000/884203.stm> (v. August 24, 2000).

Internet country, because only the new technologies guarantee job security and long-term prosperity” (quoted in Tarquini, July 3, 2000:13).¹²⁹

The process of achieving consensus has been rather long, but, as expected, once reached, policies have been adopted and are being implemented—albeit with mixed success as the Green Card experience seems to suggest. Germany’s “Net enthusiasm” has matured within a consensus-oriented, traditional alliance of private business and government, with the addition—and this is the innovative element—of pro-liberties NGOs, consumers’ and users’ groups. These conditions have allowed Germany, despite a “bumpy” start (the CompuServ case) and some disagreement (particularly on the free speech issue), to acquire one of the most liberal regimes on the Internet in Europe and in the world, with a low level of Net control. Obviously, Germany has once again demonstrated that positive or “good” use of the Internet and its expected economic benefits cannot be separated from its drawbacks, i.e. neo-Nazi and racist propaganda, scant privacy, lack of security and criminal activity. Attempts at presenting the Internet as an instrument of criminals or an economic panacea would actually be smoke in the eyes of the public opinion rather than helping to address those societal flaws.

The main hypotheses of this dissertation have been confirmed in the case of Germany: a highly developed and liberalized telecom sector, and great expectations for economic benefits from the New Economy are inversely correlated with the classification of the Net as a threat to national security. Measured against the Cryptography Index as an indicator of the level of statutory control, of the three case studies presented in this work, Germany scores at the lowest on Internet control. In addition, by officially financing research on open-source software, Germany seems to be taking a rather different approach than the United States that may give more relevance to grass-root groups. This circumstance, coupled with the importance of the CCC, and, the election at ICANN, as well as with the determination showed by the German industry to reoccupy a leading position in the Information Age, could give Germany a valuable standing in shaping the future of the Internet. Moving forward simultaneously at the corporate as well as the user—including software developers—levels seems to be a masterful tactic that well may reward Germany with considerable benefits.

With respect to national security, Germany’s stance is considerably different than the United States—and closer to Italy’s and other European countries’ with the notable

¹²⁹ My translation. See also <http://www.telekom.de/dtag/presse/artikel/0.1018,x528.00.html> (v. October 6, 2000).

exception of Britain (and to lesser extent, France). Internet security is definitively one of the crucial topics that demands the federal government's constant attention, but in no instance has the "national security" issue been called in to justify increasing control on the Net. On the contrary, it is quite clear for the German government that the implementation of the New Economy and the Information Society can be achieved only by liberalizing telecommunications, limiting Internet control to the most critical cases (e.g. child-pornography and neo Nazism), and, more generally, showing a "positive" and engaging attitude toward the digital challenge. After a controversial start, Germany might well become the motivating example for other governments on-line.

CHAPTER SIX - ITALY: THE ELUSIVE INFORMATION SOCIETY?

*"The development of the Information Society
is a major goal of the Italian Government"*

*Massimo D'Alema, Presidente del
Consiglio dei Ministri (February 1999)¹*

*"No European telecommunications system has
been institutionally more complex than Italy's"
Eli Noam (1992:239)*

6.1 Introduction

The fact that modern Italy has consistently suffered from unstable governments and frequent cabinet reshuffles is an empirical observation widely accepted by political scientists. Indeed, there have been more than fifty governments after Second World War, with an average tenure of less than one year (Koff and Koff, 2000:130). Even the case of the 1996-2001 legislature—in which two governments lasted for almost two years—confirms this finding. In 1996, the center-left *Ulivo* (Olive Tree) coalition won the general election. Its acclaimed leader, Romano Prodi, promised that his government would last the full five years. In 1998, premier Prodi lost to a vote of confidence, and was replaced by Massimo D'Alema (of the Democrats of the Left) who also promised that his government would reach the natural deadline of the legislation.

In April 2000, following a serious defeat in local elections, Giuliano Amato (former Socialist), took the place of D'Alema. Amato, small wonder, promised he would lead his government until the next general election scheduled for 2001. Thus, the *Ulivo* coalition that had guaranteed the Italian electorate that its government would, at last, follow the example of other European countries and last the full five years, was shattered after two years, its leader Prodi removed (to the new post of EU Commission president) and replaced by a premier that, at the general elections in 1996 was a law professor that did not even

¹ Presidency of the Council of Ministries, *Forum sulla Societa' dell'Informazione* at <http://www.palazzochigi.it/fsi/> (v. April 5, 2000). On October 30, 2000, the "old" Web site of the Italian government ("Palazzo Chigi") was replaced by a new Web site: www.governo.it/, which is better designed and more user-friendly. In so doing, the Italian government intended to stress an even more positive approach to the Net and Italian Netizens (Cammarrata, M. "E' Necessario Dominare il Futuro", November 9, 2000 at <http://WWW.INTERLEX.IT/attualit/dominare.htm> v. November 10, 2000).

run.² Instead of the promised one government for the full tenure, Italians had to cope with three cabinets. A marked improvement, but still a far cry from the praxis of other industrialized democracies.

Judging by Italian standards, the center-left governments that have ruled Italy between 1996 and 2000 have been alluded to as exemplary long-standing governments, since they lasted, on average, two years (Koff and Koff, 2000). Yet, even they have been perceived by the electorate as so entangled in the coalition partners' petty in-fighting that they also gave the image of being feeble, shaky and about to be replaced. Perhaps even more important, they were seen as no less paternalistic, clientelistic and aloof than the previous governments they had despised so much. On the one hand, scholars writing about the composition of modern Italy's governments fear that what they write today will no longer be (literally) the case by the time they publish their analysis. On the other hand, ironically, some features never change. It is the old principle of change without change popularized by Giuseppe Tomasi di Lampedusa in his book, *Il Gattopardo*.³

More than in any other European country, Italian politics was a strong presence in the telecom sector. Many government parties saw such opportunity as a useful economic base for their political activities. Despite this strong interference, the Italian government "...had a less direct control over public telecoms than in other countries....[because the] bureaucratic elites which ran those [telecom] organizations had a vested interest to maintain autonomy from the government" (Natalicchi, 1996:306). Moreover, "[o]n-going government crises prevented continuity of policy action" in the modernization and reorganization of public telecommunications (Natalicchi, 1996:307).

To some extent Italy's malaise, however, is common to most of Europe. Attitudes toward information and communication technologies, for instance, are quite similar. As Eli Noam (1986:256) wrote:

European leaders are aware of the importance of this sector [telecommunications], and they realize that the United States and Japan are making impressive gains in it. They want to do "something" in order to attain rapid results, and are willing to commit money and prestige. In the end, however, these efforts cannot transcend fundamental constraints: the self-interests of bureaucracies, the bureaucratic and hierarchical style of decision making, the short-term interests of domestic manufacturers, and scientific nationalism.

² More precisely, the governments in the legislature should be numbered five, since both Prodi and D'Alema had to undergo two cabinet reshuffles (albeit maintaining the same premiership and most of the ministers).

³ Tomasi di Lampedusa described the fortunes of a noble Southern family during Italy's nineteenth century *Risorgimento*. Commenting the change of ruling from the *ancient regime* to the new kingdom of Italy (dominated by Piedmont's royal family), one character noted that the new rulers would be exactly like the old ones since nothing ever really changed. On this point, see for instance McCarthy (1995:8).

Koff and Koff (2000:133) have noted that part of the problem with the 'executive lies on the fact that the Constitution does not clearly spell out the functions of government. Unsurprisingly, the formation of a government "...can be a very complex matter". Under these conditions, the Prime Minister becomes a "limited leader".

The Italian case provides a valuable contribution to the generalizations of this study. Italy's structurally "weak" governments represent a remarkable juxtaposition to the United States' and Germany's traditionally stable governments. The Italian state has also a tradition of intrusion in the economy. For a long time, most political parties (with the exception of the extreme right and left) and their large apparatus of middle-men and intermediaries have operated to extract maximum benefits from such situation. Confronting the statutory control policies of the two strong governments with Italy's weak one would further strengthen the accuracy of my findings.

Finally, the Italian contribution to the explanations offered in this work is relevant for another reason. Since Italy is a "new-comer" to the Internet, a proper legal framework on as well as widespread social acceptance of the Internet are still being developed. These circumstances could have favored greater activism and powers of control by law enforcement/intelligence personnel, or, at least, one would expect such outcome, were a realist interpretation correct. Evidence presented in this chapter proves otherwise.

6.2 Historical Background

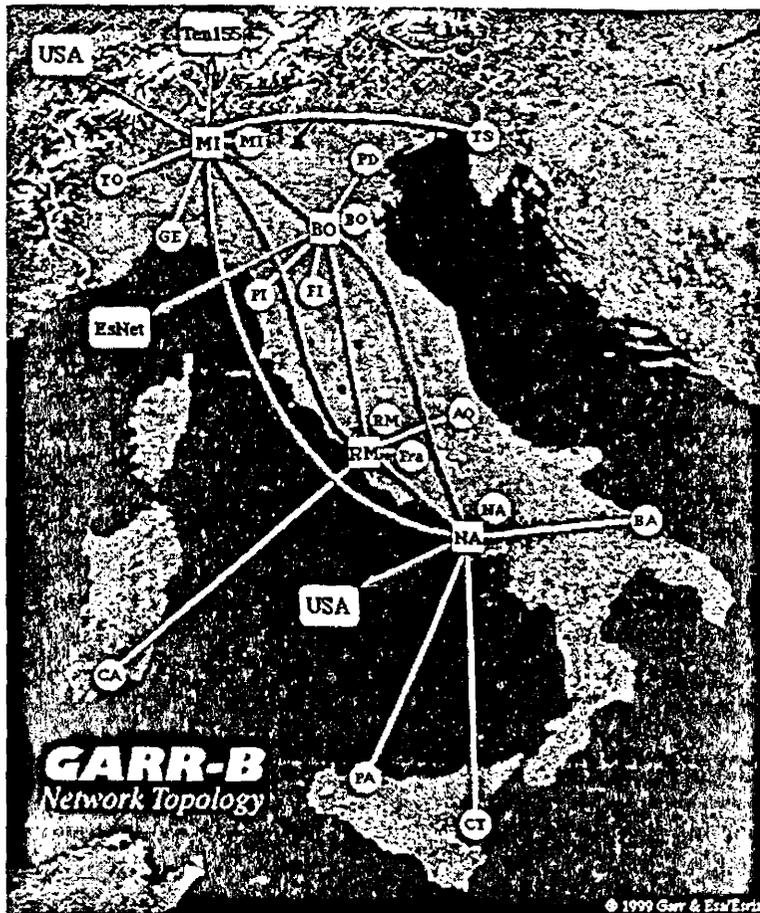
Consistent with its historical tradition, the Internet was introduced in Italy by scientists in the 1980s, and, more precisely, by nuclear physicists, whose field has a strong historical heritage of research and innovation. Nuclear physicists were the first in Italy to think in terms of developing a scientific knowledge network, and thus created the INFNet⁴ in 1980 to link all the nuclear physics institutes, locating the main node in Bologna (Siroli et al. 1997). In 1988, the Ministry for University launched the Group for Research Network Harmonization (GARR)⁵ with the goal of integrating INFNet with other Italian research networks. The next map shows the Italy's main scientific network, the GARR in 1999 (courtesy of Cybergeography).⁶ As the maps included in this work, the picture highlights

⁴ *Istituto Nazionale di Fisica Nucleare Net* (National Institute of Nuclear Physics).

⁵ *Gruppo Armonizzazione Reti di Ricerca*. INFNeUGARR are linked, through Bologna, with Princeton, NJ (USA) for the extra European traffic, and INFNet with Geneva's CERN and GARR with Europe-Net (British telecom) for the European traffic (Siroli et al. 1997).

⁶ http://www.cybergeography.org/atlas/isp_maps.html (v. several times between Fall 2000 and Spring 2001).

the structure of Internet backbones in Italy, and which the main “exit points” are for Internet traffic toward the rest of Europe (North), and the United States.



For a long time, as in the United States and other industrialized countries, the Internet was an almost exclusive domain of Italian scientists and researchers. The Internet was not, however, Italy’s only packet-switching network. Telecommunications were a state monopoly, and thus, in 1986, the telephone company SIP (*Societa’ Italiana per L’Esercizio Telefonico*, forefather of today’s *Telecom Italia*) and the Ministry for Post and Telecommunications launched their proprietary packet network, Itapac, reserved predominantly for business users. With initiatives such as Itapac, SIP/Telecom intended to take maximum advantage of its monopolist position that allowed it to offer high value added services to the business sector, providing only basic telephony to the rest of the country.

SIP/Telecom fought a hard rearguard battle to defend its monopoly until 1995/96, when, following EU directives, it was privatized.⁷ Overall, this outcome is quite surprising. For a long time in Italy, "...market forces were virtually absent from the telecoms policy process" (Natalicchi, 1996:306). Giuseppe Rao, head of the government's Forum for the Information Society, has been rather outspoken in stressing SIP/Telecom's responsibilities in shaping the current status of telecom in Italy ("a violent monopoly").⁸ The privatization battle is now over, since only 6% of the telecom sector is in public hands.⁹ *Telecom Italia* and its cellular phone associate TIM (*Telecom Italia Mobile*) still have the largest share of the fixed and mobile telecom markets—followed by *Infostrada*, Wind, Blue and others—with some 3 million subscribers to the TIN (*Telecom Italia Network*) ISP. For these reasons, Telecom Italia is still one of the crucial interlocutors of the government when it comes to telecom and the Net.¹⁰

The period between 1995 and 1996 was particularly crucial for Italy since, like other European countries, in addition to the privatization of telecom, the Net also began to take off for a larger audience. The years 1994 and 1995 were characterized by growing media attention to the Internet. Such attention, however, did not translate into a better understanding of the potential uses of the Net. Monti and Chiccarelli (1997) have identified three main periods in the first 10 years of life of the Italian hackers' movement.

The years 1988/1993 are called "the golden age", because a relatively small community of hackers could freely roam on the undersized but open early networks (most hosts were universities, not too concerned with security but with sharing research). The second period, 1994, is "the busting", because the sudden notoriety of the Internet in the United States had drawn the attention of the media principally for child-pornography, and the public demanded some response. Thus, law enforcement officers and the judiciary heavily investigated the hackers' scene. Inexperience and ignorance of technical matters among police officers and judges were high, and a proper legal framework was missing.

⁷ Natalicchi (1996:307/308) has noted that "Italy's adaptation to the changes introduced by the [EC] Commission was troublesome....[but] Italy's failure to adapt to EC regulatory change was not simply the result of differences between the Italian and the Commission's approach to telecoms. It was also the result of Italy's limited participation in the EC policy process".

⁸ Giuseppe Rao, Head, *Forum per la Societa' dell'Informazione*, personal interview, Rome, May 3, 2000 (my translation).

⁹ Maurizio Bonanni, Italian Ministry of Communications, personal interview, Rome, July 17, 2000. Not so, however, for the quasi-monopolist position of *Telecom Italia* on local calls and on the leasing of its infrastructures to other telecom carriers.

¹⁰ Roberto Perrella, *Telecom Italia*, personal interview, Rome July 17, 2000. *Telecom Italia* influence has considerably declined however, since its days as state company, when government officials could not afford to ignore Telecom's opinion on economic issues. Rao, personal interview.

Thus excesses and mistakes happened. Then, in 1997, there was the “new generation” Internet, with the fast growth of users and the arrival of the private sector. This progression shows how, in absence of a proper legal framework and awareness within the society, to overcome their technical deficiencies, law enforcement agencies could have simply asked for and obtained more the control on the Net.

Among the first “laypersons” (that is, non-academic) that recognized the Internet as a new tool for providing the public with access to information were local administrators in a few municipalities. In 1995, Bologna was the first Italian city (the second in Europe after Amsterdam) to implement the ideas of “civic network”¹¹ (*Iperbole*), which allowed all residents with quasi-free access to the Net, and of “cyberdemocracy”. Had the project been really understood, it might have met stronger opposition, but “[t]he arguments *against* the provision of Internet access were indeed few, since the project was relatively cheap, and promised to win Bologna prestige...”¹² (Tambini, 1998:86).

The example of Bologna has slowly been followed by other municipalities, with varying degrees of success. More recently, the rush for the Internet and the New Economy¹³ have brought a large numbers of operators to offer services and high speed access for discounted prices, thus eroding the main *raison d'être* for the civic networks. Even the long standing Bologna's *Iperbole* has only 17,000 subscribers in 2000—out of a population of near 400,000. In all likelihood, to survive, Italy's Internet civic networks will have to shift their mission from providing plain Internet access to offering content services that could not be better carried out by private ISPs.¹⁴ Clearly, *Iperbole* is now “in search of a new identity”.¹⁵

The Prodi government began to recognize the potentialities of the Internet in the mid-90s, and established the Forum for the Information Society, in the framework of the *Accordo per il Lavoro*.¹⁶ The Forum was activated by a governmental decree in February

¹¹ *Reti Civiche*. Bologna took advantage of having a local administration recognised at national level for its efficiency and openness.

¹² Emphasis in the original.

¹³ The “New Economy” has become the catch-phrase that connotes a certain kind of lifestyle. It is always used in English, in almost any conceivable area of Italian interactions—including TV commercials with young couples looking at laptops' screen trying to understand the “New Economy”. The concept has permeated public consciousness.

¹⁴ Personal interview with Leda Guidi, Head of *Bologna's Iperbole*, Bologna, May 5, 2000.

¹⁵ Guidi, personal interview.

¹⁶ *Forum per la Societa' dell'Informazione*. The *Accordo per il Lavoro* (Labour Agreement) is a planned, regularly updated agreement between the government and social and economic actors (mainly the trade unions and employers' organizations) that aims to reduce unemployment.

1999,¹⁷ and represents “...a permanent workshop open to public institutions, businesses, unions, universities and research institutes, the service sector, associations and private citizens”.¹⁸ Since then the goal of the Forum has been the active monitoring and promoting developments in information and communications technologies (ICT) that could benefit Italy.

Another noteworthy sign of the change in the Italian TLC market happened in Spring 1999, when Olivetti, via a public offer, took control (51% stakes) of the incumbent operator, *Telecom Italia*— then a public company with the Treasury holding only a 3,6% stake. At the same time, *Olivetti* sold *Omnitel* and *Infostrada* to *Mannesmann GmbH*.¹⁹ Only five years earlier such an occurrence would have been considered impossible by the company itself and the public as well. In the general European process of increased liberalization in the TLC sector, users and economic operators welcomed such a move. Nonetheless, the new ownership has ruthlessly taken advantage of the still quasi-monopolist position of *Telecom Italia* in the local call market, disappointing many users who had hoped to benefit from the definitive dismissal of the state involvement in the TLC market. Moreover, While claiming to be a telecom carrier just like any other, *Telecom Italia* uses its predominant position in local calls to boost its business as the major Italian ISP.²⁰

The first national conference on the Information Society in June 1999 outlined some of the crucial problems for Italy: (a) computer illiteracy (including insufficient knowledge of English), (b) lack of attention on behalf of the local authority, (c) cultural conservatism in the productive system (industry, credit, finance), and (d) rigid and unbalanced structure related to TLC rates.²¹ Overall, “[c]ompared with the United States, Europe is in a considerably disadvantageous position regarding spending, innovation and in particular, the diffusion of technology. And in comparison with the rest of Europe, Italy is even more behind.”²² In fact, in one of the many tests done to measure Internet penetration in Europe,

¹⁷ http://www.palazzochigi.it/fsi/ita/info/decreto_ita.html (v. April 5, 2000).

¹⁸ http://www.palazzochigi.it/fsi/eng/dpof_eng.html (v. April 5, 2000).

¹⁹ http://www.agcom.it/eng/regul_tlc.htm#01 (v. July 18, 2000). *Mannesmann* was then bought by the British *Vodafone*.

²⁰ *Telecom Italia* offers inexpensive rates for Internet connections, but only if the provider is *Telecom Italia* Network (TIN). Since Internet calls to ISPs are all local calls, customers are very tempted to switch to TIN and reap the benefits of cheaper tariffs on those calls. TIN has also been permitted (albeit with a conditioned approval) by the Antitrust Authority to merge with SEAT, the company that publishes the Italian Yellow Pages, keeps a considerable databases of businesses using its advertisement services, and is the owner of *Virgilio*, the main Italian search engine and one of the most visited Italian Web sites. TIN-SEAT is then likely to soon be running most of the Italian Internet traffic. The company also plans to expand its multimedia basis, by the acquisition of a national private broadcasting company (*TeleMonteCarlo*).

²¹ http://www.palazzochigi.it/fsi/eng/archivi/conferenza/relazione_1_eng.html (v. April 5, 2000).

²² http://www.palazzochigi.it/fsi/eng/archivi/conferenza/relazione_3_eng.html (v. April 5, 2000).

Italy, in 2000, ranks only eleventh (Germany is ninth) with almost 28% of inhabitants using the Net, well after the Scandinavian countries that are all above 50%.²³ The development of ITC and the Internet for the job market in Southern Italy has merited considerable attention—thanks also to the University of Catania (Sicily) that is among the most active centers for ITC research in Italy and highly contributed to the development of the so-called “Etna Valley”.²⁴ Among the solutions suggested at the conference were increasing digitalization, development of broad-band networks (as well as an Italian IP protocol for research), and new regulations and policies aimed at telephone tariffs.

It was clear to many that, despite much emphasis and enthusiasm, on the eve of the new millennium, Italy still lagged behind most Northern European countries in terms of computer literacy.²⁵ Computer users have still been but a minority of the population, and Netizens have been even a tinier minority, despite claims to the contrary.²⁶ To address the problem of the Italians’ attitude toward the computer, one of the last initiatives of the D’Alema’s government was that of launching the “PC for students” project. Within this

²³ The figure is based on the number of inhabitants older than 15. See <http://www.proactiveinternational.com/index.html> (v. July 11, 2000). As usual when evaluating numbers relative to Internet use, one should exercise caution.

²⁴ http://www.palazzochigi.it/fsi/doc_piano/catania.html (v. July 5, 2000).

²⁵ Until 1995, among OECD countries, Italy had more computers per 1,000 people only than Spain, Portugal, Greece, Poland, Hungary and the Czech Republic, Mexico and Turkey (83.72 compared with an OECD average of 169.1 and an EU average of 137.6) (<http://www.undp.org/hdro/iinfo.htm> v. October 3, 2000). Even small countries such as Ireland, Finland or Austria had more PCs than Italy. Remarkably, in August 2000, the Internet Consulting firm Forrester Research came out with a novel explanation for slow Internet adoption in Southern European countries (France, Spain and Italy). The hindrance was due to “Latin culture and climate”. In fact, according to a Forrester spokesperson, “[t]he main North-South cultural divide between the ‘Catholic South’ and ‘Protestant North’ applies most strongly to middle-aged consumers. Older consumers in the Southern European markets find it more difficult to become familiar with new technologies”. Moreover, “...climatic factors favor technologies that can be used outdoors in Southern Europe. On a sunny day, Southern Europeans may not be tempted to stay inside and shop online, while Northern Europeans often don’t have that choice”. This explanation, they claim, is further supported by the marked divergence between mobile phone and Internet adoption in the Southern European, at <http://www.forrester.com/ER/Press/Release/0,1769,377,FF.html> (v. September 14, 2000). However, Beppe Severgnini, an Italian journalist, has proposed a somehow different explanation: “Italians have no tradition of mail order, distrust credit cards, love cash and adore the social side of shopping in *vie* and *piazze*. If you add slow delivery, you can see what Internet shopping is up against” (2000:50).

²⁶ The Bocconi University, *Osservatorio Internet*, (<http://sdawww.sda.uni-bocconi.it/oii/archivio/Conf%2099/Methodolog2.htm#Inizio> v. July 18, 2000) and Between Spa, an ICT broker (<http://www.quadrante.net/between/wow11.htm> v. July 18, 2000), publish research about the number of Internet users and e-commerce in Italy by using telephone interviews. As already explained, determining the correct number of users and the real size of the Net are tricky exercise that are all too often employ by media and other interested parties to give a rosier picture of the situation in Italy. Moreover, the Bocconi University and Between Spa conclusions seem to lead to contradictory deductions that those elaborated by Forrester. Finally, if it is true that Italy is not a highly computerized country, however, Italy’s presence on the Web, according to the July 2000 Survey by Network Wizards, is rather ample, being surpassed (based on counting country specific TLD only) by Japan, the United States, Britain, Germany and Canada (<http://www.isc.org/ds/WWW-200007/dist-byinum.html> v. October 3, 2000).

framework, students entering secondary schools are offered the possibility of purchasing computers at subsidized prices.²⁷

If Italy undoubtedly sits at the bottom end of Europe's most computerized countries, Italians are among the first of the class in one area of ICT, namely portable phones. The monopolist SIP/Telecom introduced car phones in Italy at the beginning of the 1990s, targeting business customers, and despite their cost and impediment they proved to be a considerable success. Not much later, the Italian carrier began to commercialize cellular phones, whose popularity soon dwarfed that of car phones. Such was the fondness of business customers for the new communication device that it attracted attention by non-business users and quickly became a fashionable status symbol.

That exclusivity, however, did not last long, since cellular phones turned out to be the most popular invention in telecom since the telephone itself. Telecom carries and national and EU regulators realized that potential almost synchronically. Consequently, as the offer from state phone companies attracted more and more customers and telecom became *the* market for the 1990s, their monopolies started to be questioned at the EU level, allowing new and aggressive competitors in the market itself.²⁸

In 1997, Italy had almost 12 million cell phone subscribers and *Telecom Italia Mobile* (TIM) was the third carrier in the OECD area (OECD, 1999:75 and 20), reaching the exceptional number of 30 million (in a population of 55 million) by 2000. The market has accommodated a third cell phone carrier, Wind, which began operations in March 1999, and a fourth one, Blue, which was operational in the summer 2000. By that time, TIM was the largest operator in Europe (over 18,5 million subscribers), whit *Omnitel* following with over 10 million. Wind, the third mobile operator, reached more than 1 million customers in less than one year of operations.²⁹

Italians have fallen in love with cellular phones for various reasons. Economies of scale have allowed for lower tariffs and diversified offers while the demand has steadily grown. Taking advantage of pre-paid cards and falling prices of handsets, parents have discovered an attractive way to keep in touch with—and also keep track of—their adolescent children, who have become adept at exploiting the convenience of instant

²⁷ *Iniziativa PC Agli Studenti*, at http://www.palazzochigi.it/fsi/eng/computer_x_student.htm (v. May 10, 2000).

²⁸ Without EU intervention national telecom monopolies would have never opened such a profitable market. Their influence on national governments was so unmitigated that only an EU intervention could change the situation. The case of Italy was effectively outlined by Rao, personal interview.

²⁹ http://www.agcom.it/eng/regul_tlc.htm#ann2 (v. July 5, 2000).

messaging (SMS) to communicate with their peers. Overall, as of 2000, more than half of the Italian population use cellular phones.³⁰ Only Scandinavians are more eager users.

Internet on cellular phones is the chance that European telecom carriers are taking to bring Europe at the level of Internet use of the United States, which, according to *The Economist* (March 11, 2000:85) is 18 months beyond Europe—which is 18 months beyond Japan. As explained in the Introduction (Chapter 1), since the pace of computer penetration in Europe is still very slow, only by the diffusion of Internet on cellular phone can Europe hope to catch up with the United States and compete with it in the New Economy (Woolridge, October 9, 1999, and *The Economist*, October 23, 1999:20).

In July 1999, the “Economics and Finance Program Document 2000-2003”³¹ reported that “Italy has so far delayed the widespread introduction of this communication technology which is the driving force behind the new digital economy. However, presently this trend is undergoing a significant reversal”.³² Noting the cascade effects of ICT and the Net for other industry (e.g. electronics) and the economy at large, and the need to coordinate various local and governmental bodies, the government identified three principal areas on which to concentrate its action. These areas were (a) diffusion of computer and digital information to consumers, (b) development of the use of ICT and networks, and (c) promotion of services, contents and research.³³

On 23 and 24 March 2000 in Lisbon, a whole Special European Council was dedicated to “a Europe based on innovation and knowledge”,³⁴ which also further endorsed these guidelines by the Italian government. The goal of the Special Council was “...to respond to those needs that are more pressing: the definition of efficient actions to stimulate the innovation and knowledge economy, and ensuring skilled jobs and maintaining social cohesion”.³⁵ The Council was then followed, in April, by an *ad hoc* Ministerial Conference on the Information and Knowledge Society, also in Lisbon that, among others, addressed

³⁰ 30 million handsets are, at the time of writing, in use, according to the Telecom Authority, http://www.agcom.it/eng/regul_tlc.htm (v. July 10, 2000).

³¹ Documento di Programazione Economica e Finanziaria” (Dpef), at http://www.tesoro.it/Docu/1999/pdf/DPEF_2000-2003/Dpef2000-2003.pdf. (v. April 20, 2000). The Dpef “...can be defined as a ‘declaration of intents’; an act containing specific political economic objectives and which outlines the public finance measures which the Government intends to impose over the next few years” (at http://www.palazzochigi.it/fsi/eng/dpef_eng.html).

³² http://www.palazzochigi.it/fsi/eng/dpef_eng.html (v. April 20, 2000).

³³ The actions to be undertaken in those areas involve, among the others, modernization of telecom infrastructures, Internet diffusion in small and medium enterprises (SMEs), boosting electronic commerce, computer courses available in schools for students and teachers, and teleworking, at http://www.palazzochigi.it/fsi/eng/dpef_eng.html (v. April 5, 2000).

³⁴ http://www.portugal.ue-2000.pt/uk/docmne_main01.htm (v. July 18, 2000).

³⁵ <http://www.palazzochigi.it/fsi/eng/eEurope-conference.htm#ministerial> (v. April 5, 2000).

problems such as literacy campaigns in schools, the development of applied research, the application of new technology in public administration, the creation of new work opportunities, and the promotion of Internet. The final objectives of these EU initiatives are the promotion of social inclusion and respect for cultural diversity in the Information Society, which exactly parallels the priorities set by the Italian government. After these meetings, however, such “Eurospeak” failed to impress some observers, who remarked that encouraging innovation as partial substitute for economic—and labor-market in particular—reforms is a strategy doomed to fail (*The Economist*, April 1, 2000:15/16).

On the surface, Italy’s attitude toward controlling the Internet has been a rather benign one compared to that of the United States, and more like Germany’s. However, that position of apparent laxity and *laissez faire* was more due to a lack of understanding of the Internet than to a true appreciation for a control-free Net.³⁶ In fact, in the mid-1990s, the first perception of the Net by the Italian public was far from positive, since the word “Internet” became synonymous of “child-pornography”—a phenomenon encouraged by sensationalist journalists. Popular reactions obliged governments to take action at national and EU levels.³⁷

After initial “Internet-phobia”, in 1999-2000 an “Internet-mania” exploded in Italy.³⁸ Even the Central Bank Governor, Antonio Fazio, went as far as declaring to one of the most influential Italian newspapers, *Il Corriere della Sera*, that the new economy could bring Italy to an economic growth 1950s’ style; that is, when post-war Italy was booming (de Bortoli, February 27, 2000:3). Words like New Economy, net-economy, Web, and Internet entered the daily vocabulary of most Italians. Not surprisingly, going from scarce (or distorted, as in the case of child pornography) knowledge of the matter by the public, to a frenzied and emotional popularity of the Net, has yielded some questionable initiatives. As one observer has noted, with the new economy, “somebody has ‘smelled’ money and

³⁶ See, for instance, the case lack of opposition to *Iperbole* (see p.3) due to little technical understanding of the network by local public administrators.

³⁷ The problem is now only rarely mentioned by other media, but it is far from solved. It is still possible to find illegal pornographic material through the most popular search engines. Because the Net is no longer only associated with child-pornography but also more positively with the New Economy, there is not the same public pressure to control its contents. Bonanni, personal interview. Another example of the emphasis on the Internet as a tool for pornographers is the Italian criminal law on sexual exploitation of minors that forbids the possession or trade of such material, explicitly mentioning telematics exchange. Technically, this specification is not necessary, since specific exchange included in the general provision, but the legislator probably wanted major emphasis on the attention given to the Internet. Andrea Monti, Attorney-at-Law and President, ALCEI-Electronic Frontier Italy, personal interview, Rome July 17, 2000.

³⁸ Cammarata M. “L’Opposizione Progetta la Secessione del World Wide Web”, March 23, 2000, at <http://WWW.INTERLEX.IT/attualit/secess.htm>, (v. April 13, 2000).

has convinced the government to act, to the point of nominating an *ad hoc* [Internet] undersecretary”.³⁹ That is, the Italian government almost went to the other extreme, all too ready to intervene about this new “area of competence”. Two events, in particular, are representative of the government’s new bustle, namely the proposal for a “state portal” and a government bill to regulate Italy’s ccTLD *.it*.

In the former case, the government put forward the idea of creating *Portale Italia*, i.e. a free portal for Italian SMEs. The political opposition and, more importantly, bipartisan experts criticized proposal. The main evaluations were that the (a) the portal did not have any value added for many firms that already have their Web pages (a service offered by many Internet operators), (b) it unfairly competed against advertising companies, which cannot offer their products “for free”, and (c) since the Ministry of Finance—the “network administrator” in this case—did not have its own network infrastructure, and it would thus rely on the service of its usual provider (a subsidiary company of *Telecom Italia*). The Ministry would then give public money to a private company without fair competition.⁴⁰

The government’s bill on Italy’s TLD and the subsequent discussion are also worth mentioning here. In that circumstance, the government first “liberalized” the access and ownership of domain names under the TLD. Then other media reported the rush to “own” domains, and hence the government announced a bill to regulate ownership of domain names. This solution was inadequate because (a) it overlooked consideration the technical nature of the Net, (b) it rendered more complicated an already complex state of affairs. Moreover, if the bill had been passed by the Parliament, it would have contradicted the indications given by ICANN on DNS management—i.e. names are registered on a first-come-first-serve basis.

Overall, despite some evident drawbacks (a strong regulatory tradition, small use of PCs, quality of human capital,⁴¹ etc.), Italy does enjoy some distinctive advantages on its path to the Information Society: the telecom market is fully liberalized, Italians have a passion for cellular communications, and Italian universities seem to perform well in

³⁹ Cammarata M. “Il Problema Non e’ Costruire un Portale”, April 20, 2000, at <http://WWW.INTERLEX.IT/attualit/portal2.htm>, (v. April 20, 2000) (my translation). Another observer has described the attitude by some government institutions towards the Internet and e-commerce as if they were looking at “a big bone with a lot of meat around” (my translation). Bonanni, personal interview.

⁴⁰ Cammarata M. “Una Proposta Sbagliata da Ritirare Subito”, <http://WWW.INTERLEX.IT/attualit/propind.htm> March 9, 2000.

⁴¹ As Giuseppe Rao remarked “...too many humanities, too few polytechnics...”(my translation). Rao, personal interview.

scientific publications on ICT.⁴² Last, but not least, the predominant role of SMEs and the concept of networked firms seem to give evidence that also the economy has a more appropriate structure to take advantage of the Net. Hence, observing the country's planning and actions in this respect could contribute to a better understanding of the overall role of the governments and the reasons of statutory control on the Internet.

6.3 The Main Actors

This section describes the primary actors relevant for telecommunications and Internet developments in Italy. As in the case of the United States and Germany, this is a non-exhaustive list, since more and more actors find themselves affected by the Net and therefore have to devise new conducts to accommodate the network in their daily operations. The main players here belong to the same typologies as actors in Germany and the United States: pro-liberties NGOs, consumers' and users' groups, the private industry, government agencies and authorities etc. As in Germany, many of the government initiatives in the field of IT and telecomm are planned and implemented within the EU framework for *e-Europe*, which was launched by the current EU Commission president, Romano Prodi in December 1999.

6.3.1 The Government

The starting point of analysis of the Italian government structure concerned with the Internet should start with the Presidency of the Council of Ministry,⁴³ that is the operational structure available to the Italian premier. Within *Palazzo Chigi*, the main office assigned specifically to the task of synchronizing the government efforts for the development of the information society is the *Forum Per la Societa' dell'Informazione* (Forum for the Information Society). The Forum was launched by the then Prime Minister Massimo D'Alema at the first National Conference on the Information Society in June 1999, while the official Web page was presented to the media in september 1998. The Forum "...—chaired by [the then] Prime Minister, the Rt. Hon Massimo D'Alema, MP—is a working 'forum' open to public institutions (including territorial ones such as Regions, Provinces,

⁴² According to the American Association for Computing Machinery (ACM) and the Institute for Electronic and Electric Engineering (IEEE)—two of the most respected organizations in ICT—Italian universities come second (after the Americans) for numbers of publications in ITC scientific journals, http://www.palazzochigi.it/fsi/doc_piano/cap2.htm (v. July 5, 2000).

⁴³ Commonly called "*Palazzo Chigi*", from the name of the building in Rome where it is located.

Municipalities), social partners, universities, research institutes and private citizens".⁴⁴ The Forum has a small staff (the "task force") in *Palazzo Chigi* and coordinates five thematic working groups on infrastructures, employment, IT literacy, services and contents, and public administration.

Despite the change in premiership in the Spring of 2000, the Forum has remained central to the government's plans for the development of the Information Society, and so has the action plan for PA modernization, increasing the quality of human capital, making Italy a "learning society"⁴⁵ and, in general, bringing Italy into the New Economy for the Amato government.⁴⁶ In December 1999, the *Presidenza del Consiglio* established an *ad hoc* committee of Internet experts (COESIN, *Comitato Esperti Internet*) with representatives from various ministries (Industry, University, and Communications) as well as public authorities (AIPA and Communications). The assignment of COESIN is to indicate the approach strategy to the Net for the Italian government.

The Amato government further strengthened its commitment to the Internet in May 2000, by becoming a full member of the World Wide Web (W3) Consortium (headed by Tim Berners-Lee, inventor of the Web).⁴⁷ Overall, with reference to telecom and the Internet, the major change between the D'Alema and Amato governments has been their attitudes toward the allotment of the licenses for the third generation cellular phones (UMTS).⁴⁸

The economic newspaper *Il Sole 24 Ore* has rated the Italian government's web sites, with *Palazzo Chigi* and the Ministry of Finance scoring highest (4 out of 4), followed by Treasury and Foreign Affairs.⁴⁹ The Ministries of Industry, University, and

⁴⁴ At http://www.palazzochigi.it/fsi/eng/info/forum_conf_eng.html (v. April 20, 2000).

⁴⁵ The "learning society" (English in the original) is one of the foremost long term ideas of premier Amato. In an interview with *Il Sole 24 Ore*, Mr. Amato argued that the learning society is the only viable choice if Italy wants to succeed in the New Economy (Forquet and Orioli, July 14, 2000:7).

⁴⁶ http://www.palazzochigi.it/fsi/eng/actionplan/government_reports_summary.html (v. July 20, 2000). The action plan is also referred to as *Progetto di Legge Bassanini* from the name of the first initiator of the plan in the D'Alema government. A good reference for the early experience of the Forum is the *e-Italia* report, published in collaboration with *Il Sole 24 Ore* in 2000. For a more subtle description of the D'Alema government with the net see Caprara and Picci (2001 forthcoming).

⁴⁷ http://www.governo.it/sito_internet/w3c.html (v. November 10, 2000).

⁴⁸ Universal Mobile Telecommunication System. The former had planned a so-called "beauty contest" where a selected number of telecom companies would be assigned the new licenses, while the latter—following the example of Britain where the auction system supplied the government with 75,000 billion Lira—opted for the auction with incumbents bid for licenses. In Summer 2000, the bidders were (the main shareholder) *Telecom Italia Mobile* (TIM), *Omnitel* (Vodafone), *Dix.it*, *Blu* (British Telecom), *Atlanet* (Telefonica, the Spanish telecom carrier), *Andala* (Tiscali, another private Italian carrier), and *Wind* (France Telecom and Deutsche Telekom). In Fall 2000, however, only six bidders participated (*Telecom Italia*, *Omnitel*, *Wind*, *Blu*, *Andala* and *Ipse* 2000) in the actual contest.

⁴⁹ http://www.ilsole24ore.it/24oreinformatica/indagine_ministeri/default.shtm (v. May 11, 2000).

Communications are located mid-list, with Defense coming last (1/2). Base on this ranking, it is fairly evident how much the Italian government considers the Net as an instrument for business and economic development, overlooking its national security and, to some extents, also law enforcement implications.

Overall, the accomplishments of the D'Alema executive are significant in clarifying the attitude with which the Italian government has tried "to take the lead" in spreading the Internet. Recalling their experience with the government's early attempts to fostering the growth of Internet in Italy and providing the image of a more Internet-friendly administration, Caprara e Picci (2001 forthcoming) have highlighted a genuine enthusiasm within the team of experts, as well as the awareness of participating in a truly innovative experimentation for Italy. In addition to *Palazzo Chigi*, the key ministries for Internet development are summarized below in Fig.1.

| | |
|---|--|
| 1) Public Administration (<i>Funzione Pubblica</i>) | 7) Industry (<i>Industria</i>) |
| 2) European Policies (<i>Politiche Europee</i>) | 8) Foreign Trade (<i>Commercio Estero</i>) |
| 3) Communications (<i>Comunicazione</i>) | 9) Labor and Social Security (<i>Lavoro</i>) |
| 4) Education (<i>Istruzione</i>) | 10) Foreign Affairs (<i>Affari Esteri</i>) |
| 5) Economics (<i>Economia/Tesoro</i>) | 11) Research and University (<i>Universita' e Ricerca Scientifica</i>) |
| 6) Finance (<i>Finanze</i>) | |

Fig. 1 Italian Government's Ministries Relevant for the Internet

Following the example spelled out by the U.S. Department of Commerce, the Minister of Industry has been earmarked by the Council of Ministers as the main actor in the fulfillment of a favorable environment for the "taking off" of e-commerce in Italy.⁵⁰ The Ministry for Industry has reckoned that the government of a modern economy should clearly outline the rules and procedures that will guide the development of e-commerce. Thus, the Ministry has activated an "observatory for electronic commerce", on whose web sites, entrepreneurs should be able to gather all the necessary information about that type of business activity.⁵¹

⁵⁰ "Decreto Legislativo.114/98", at <http://www.minindustria.it/Osservatorio/obiettivi.html>.

⁵¹ <http://www.minindustria.it/Osservatorio/osservat.htm>.

Similarly, as in the United States, the Ministry of Interior and of Justice are actively engaged in fighting crime.⁵² To this end, two inter-ministerial groups (IMG) have been activated at the Ministry of Communication, namely the IMG on information networks security and the IMG on cryptography. The former regularly gathers together 15-20 experts from the Ministries of Interior, Justice, Industry, Communications, the anti-mafia national directorate, telecom law enforcement agency (*Polizia delle Comunicazioni*), the Authority for communications, and the National Research Council (CNR). The latter IMG includes, among others, specialists from the Ministries of Interior, Justice, Communications, the Authority for privacy, and AIPA (public administration).⁵³

Conspicuous for its absence in these groups—and in the whole issue of Internet security in general—is the Minister of Defense (MOD). The explanation is straightforward: to date, the MOD (and the government itself) does not believe that the threat of information warfare through the Internet is a “clear and present danger”.⁵⁴ Uninhibited cybercrime could be a problem, but that is still the domain of law enforcement officers, not the military—although the *Carabinieri* in their function of military police may have a word. The MOD has just begun to consider the Internet merely as a tool for self-promotion of the Armed Forces, and its web sites reflects this circumstance. *Il Sole 24 Ore* in its classification of government web sites has remarked that “Internet originated in the Pentagon military networks, but there is no evidence in the web sites of the MOD of these origins. A very poor home page for a generic image of the Armed Forces”.⁵⁵ The failure of the Italian services in recognizing the relevance of the Net for their competencies is evident in other instances.

Major General (Air Force) Carlo Finizio at the Military Center for Strategic Studies has noted that “there is certainly awareness [within the military] about how information travels, because the network is open and public...[however], specifically [on information warfare], there is nothing”.⁵⁶ In fact, Italian troops participating in the peace-keeping operation in Timor East in the Spring 2000 could, for the first time, rely on the Internet for communicating with Italy—mostly for personal communications. Moreover, there seems to

⁵² The “old” crime of child-pornography has been superseded by gambling, money laundering, drugs and arms dealing that are routinely carried out on-line. Bonanni, personal interview.

⁵³ Bonanni, personal interview.

⁵⁴ A well-informed person with contacts to the Italian intelligence community has explained to me that there is widespread skepticism and disbelief about topics such as information warfare and the hackers’ threat within that community, also due to “excessive spectacularization” of these topics on the media (personal communication, March 27, 2001).

⁵⁵ http://www.ilsole24ore.it/24oreinformatica/indagine_ministeri/difesa.htm (v. May 11, 2000).

⁵⁶ Major General Carlo Finizio, deputy director, *Centro Militare Studi Strategici* (CEMISS), Rome, May 3, 2000, personal interview (my translation).

be no concern about the United States, undisputed hegemon on the Internet. However, “if that information superiority is mismanaged, it can cause a serious backlash against the United States”.⁵⁷ Overall, it seems that the issue of Internet security in Italy is almost exclusively synonymous with cybercrimes such as credit card frauds, unauthorized access to companies or universities computers, or pedophilia. The military may soon decide to look into the problem, but, thus far, consideration for it is limited to law enforcement agencies.⁵⁸

6.3.2 Public Administration and Independent Authorities

The Authority for Public Administration

In February 1993, the government established AIPA (*Autorita' per l'Informatica nella Pubblica Amministrazione*),⁵⁹ as “*autorità indipendente*” (independent authority)—that is, it is part of the public administration, but operates without interference from the government. AIPA’s goal was a better integration of the public administration information systems, with the ultimate end of improving the quality of services offered to the public, which is notoriously highly unconvinced of the Italian bureaucracy’s performance.⁶⁰ The five members of AIPA are nominated by the President of the Council of Ministers, after deliberation by the Council itself. The most recent tasks that AIPA intends to fulfill, in the overall framework of improving the quality of the PA services, have been the digital signature and electronic documents and the implementation of the PA unified network.⁶¹

Another decisive area of the Internet where AIPA plays a primary role is that of authorizing “trusted third parties” (*certificatori*) that will supply official digital signatures to individuals—in Summer 2000 these numbered four, mostly banks or financial institutions, with three more expected shortly. Electronic documents containing the digital signatures would then have the same legal validity as other hard copy documents. It is thus small wonder that “AIPA...supports the public administrations in their use of information systems, but all private subjects (citizens, companies) are indirectly affected by its activities”.⁶² Last but not least, in May 2000, AIPA published a very detailed ten-point guideline about how

⁵⁷ Finizio, personal interview (my translation).

⁵⁸ To my knowledge, the Italian Navy began to look at the prospects of information warfare in 2000, and still only with exploratory studies. No significant investments in this direction have yet been scheduled by the MOD.

⁵⁹ “Decreto Legislativo 12 febbraio 1993, n. 39” at <http://www.aipa.it/servizi/3/autorita/1/norma/1/index.asp>.

⁶⁰ The first and major project of AIPA has been the planning and implementation of a dedicated network (*rete unificata*) for the PA.

⁶¹ <http://www.aipa.it/> (v. April 10, 2000).

⁶² <http://www.aipa.it/english/4/> (v. May 11, 2000).

system managers in the PA—and not less so in the private sector—should conduct themselves.⁶³

The Antitrust Authority (Autorita' Garante per la Concorrenza ed il Mercato)

The “Antitrust” was established in Italy in October 1990 and led for a long time by Italy’s present premier, Giuliano Amato. The Antitrust was the first of the “Regulating Authorities”, (RA) that is agencies “...that perform their activities and adopt decisions independently from the Government”.⁶⁴ The Antitrust’s main competencies include bank merges and acquisitions (authorized by the Bank of Italy), misleading advertising, insurance, cartels and monopolies, etc.⁶⁵ Its monitoring activity has recently taken up e-commerce and Internet business. As the oldest RA has been able to acquire considerable technical competence in all these fields. The success of several privatization campaigns first for telecom services, and then for other public utilities providers should thus be ascribed to the high quality work done by the Antitrust and its prestige held by government and public alike.

The Authority for Communications (Autorita' Garante per le Comunicazioni AGCOM)

The Authority for Communications (roughly equivalent to the American FCC) was the second one of its type to be established through the Law n.249 in July 1997, and is “...fully autonomous and independent in its judgements and evaluations”.⁶⁶ The AGCOM is earmarked “...to carry out the tasks assigned under EU directives, both in the field of the telecommunications market and of audiovisual de-regulation”.⁶⁷ More precisely, the AGCOM is expected (a) to provide advice to the Ministry for Communications, (b) oversee security of communications, (c) maintain the registry of communications operators, (d) define criteria of openness and non-discrimination in access, (e) regulate relations between operators and users, (f) supervise the frequency ceilings and (g) promote integration of national networks with international ones.⁶⁸

⁶³ http://www.aipa.it/servizi/3/pubblicazioni/5/quaderni/3/quaderni_2.pdf (v. July 11, 2000). The guidelines, however, were not readily implemented by the whole administration, since, right at the end of May 2000, allegedly Brazilian crackers penetrated the web sites of the Communication Authority and of the Ministry of Communications. See, for instance, Cammarata M. “Questa Volta E’ Andata Bene, Ma la Prossima?” InterLex, May 31, 2000, at <http://WWW.INTERLEX.IT/attualit/sitipa.htm> (v. July 11, 2000).

⁶⁴ <http://www.agcm.it/eng/tema011.htm> (v. May 10, 2000).

⁶⁵ <http://www.agcm.it/eng/tema013.htm> (v. May 11, 2000).

⁶⁶ http://www.agcom.it/eng/l_249_97.htm (v. May 10, 2000).

⁶⁷ http://www.agcom.it/eng/resp_reg.htm (v. May 10, 2000).

⁶⁸ http://www.agcom.it/eng/l_249_97.htm (v. May 10, 2000).

Currently, the AGCOM is occupied with supervising the developments of satellite and digital televisions, the protection of minors, and equal political access (*par condicio*). The most controversial issue confronting the Authority, however, is the allocation of the frequencies for the new cellular phone system (UMTS) that is sparking an intense debate between the government and the incumbents about the final costs of the frequencies.

The Authority for Privacy Protection (Autorita' per la Protezione della Privacy, Privacy)

The Authority for Privacy Protection has been the last one RA to be established, and, from the beginning, has been led by one of Italy's leading expert on the topic, Stefano Rodota'. As the other RAs, the APP finds its rationale in two EU directives, more precisely the Directive 95/46/CE (October 24, 1995) on personal data protection and the Directive 97/66/CE (December 15, 1997) that aims to homogenize the member countries legislation on personal privacy.⁶⁹ The agency's main mission can be thus summarized as to guarantee that the treatment of individuals personal information by the PA and private business is fair and on a "strictly necessary" basis. That is, personal information can be processed by those who gathered it only for the purpose it was gathered (e.g. the identification of participants registered for a conference) and only after the targeted person has provided his/her explicit permission.

The existence of specialized agencies to protect personal data, especially in Europe, has been a consequence of the most noticeable effects of the rising number of people affected by or interested in the Information Society and the New Economy. That is, the capability of matching huge amounts of information stored in different databases endows those who manage those databases with an unprecedented knowledge power. In this respect, in February 2000, the Privacy has been asked by the European Parliament to provide its opinion on the Echelon intelligence organization. Moreover, the Privacy is a national member of the Joint Supervisory Body, the controlling committee on EUROPOL—the European organization that coordinate national law enforcement agencies within the Schengen area.⁷⁰

⁶⁹ <http://www.garanteprivacy.it/garante/frontdoor/1.1003.00.html?LANG=1> (v. May 11, 2000). At the time of writing, this Authority's Web page is still rather crude and contains only limited information.

⁷⁰ <http://www.europol.eu.int/content.htm?facts/en.htm> (v. September 15, 2000).

6.3.3 Law Enforcement

Postal and Communications Police Service

The Postal Police, a specialized Branch of the *Polizia di Stato* (Italian National Police) was established in 1981 to safeguard postal and telecommunications services. It then became further specialized in March 1998, as the Postal and Communications Police Service, with an ad hoc Interior Ministry Decree. More specifically, its tasks include: (a) coordination of operational activities of Postal Police Field Offices, (b) analysis of high-tech crime, (c) definition of appropriate countering strategies.⁷¹

Within, the organization, a key role is played by the Investigation division staff that is responsible for researching and investigating computer crime, with particular reference to e-commerce and Internet fraud. At the time of writing, the territorial organization of the Postal Police includes 19 Field Offices and 76 Postal Police Sections located in the major Italian cities.⁷² The legal basis for the activity of law enforcement agencies is the law n. 547/93 of December 1993, "...which introduced new offences (computer crime) and made more investigative tools available to police forces by amending and adding new provisions to the Italian Penal Code and Penal Procedure Code".⁷³ In addition to unauthorized access codes for computer or computer communications systems other provisions were the criminal liability of

...the conduct of anyone who steals or uses codes, passwords or other means to access a computer or computer telecommunications system protected by security measures.... [the obligation] for the safeguard against the diffusion of software programs designed to damage or destroy computer or computer telecommunications systems...[the] confidentiality of computer communications by punishing illicit interception or interruption the integrity of systems, by punishing those who physically and functionally damage such systems...[and finally the] economic aspects of new technologies have also been taken into account by envisaging the offence of computer fraud...⁷⁴

The law n. 547/93 is marked by the period of time in which it was approved by the Parliament. That is, the technical advice to the legislators was probably sketchy, and the implementation of the law has turned out to be "unnecessarily complicated" (Corasaniti, 1998:137).⁷⁵ Indeed, in the first executions of the law, in the mid-1990s, police investigators

⁷¹ http://www.poliziastato.it/informatica/1%20-%20Servizio_eng.htm (v. May 12, 2000)

⁷² http://www.poliziastato.it/informatica/4%20-%20Compartimenti_eng.htm (v. May 12, 2000)

⁷³ Unauthorized access to a computer was considered equivalent to trespassing, at http://www.poliziastato.it/informatica/5%20-%20Strumenti%20legislativi_eng.htm (v. May 12, 2000).

⁷⁴ http://www.poliziastato.it/informatica/5%20-%20Strumenti%20legislativi_eng.htm (v. may 12, 2000).

⁷⁵ The author is one of the most knowledgeable Italian magistrates on computer crime. He is also the leading scholar behind the LUISS university of Rome's project on law and the media (MediaLaw at <http://www.luiss.it/medialaw/uk/index.htm> v. July 29, 2000).

confiscated all the objects related to computers from suspects, including the mouse pad.⁷⁶ They ordered the shut down of all the activities of unaware ISPs that had been used by suspects, depriving blameless and surprised Netizens of their access to the Internet. Small wonder then that some observers have demanded that these operations should be performed by properly trained personnel (Corasaniti, 1998).

Things should have improved since then. Currently, according to the Ministry of Interior, “[t]he personnel of the Investigations Division are highly-skilled and have specific legal and technical knowledge....[and its] selection is made with rigorous criteria...”⁷⁷ However, as late as 1998, the preferred way of action of Italian Police personnel was still that of seizing everything.⁷⁸ In Germany, the last of such instances happened in 1996 (the Somm-CompuServe case). It seems that, since 1996, German law enforcers have improved their skills in this kind of investigation.

Another important Police branch assigned to monitoring Internet activities is the *Guardia di Finanza* (GdF),⁷⁹ under the authority of the Ministry of Finance. In one of its areas of competence, as judicial police, there are specific provisions to fight software and audiovisual piracy, as well as economic criminality.⁸⁰ In spring 2000, the GdF ‘s special unit for fiscal crimes produced a report highlighting the major crimes that are likely to occur on line (various types of frauds and money laundering).⁸¹ The most interesting element of the report was its clear acknowledgment of the inherently unsuitable structure of modern law enforcement agencies to cope with IT-related issues. Recommendations focused not only on the development of different techniques of monitoring, but also on training of a whole class of qualified investigators.

⁷⁶ An updated list of Police operations is available at <http://www.poliziastato.it/informatica/operations.htm> v. July 29, 2000).

⁷⁷ http://www.poliziastato.it/informatica/3%20-%20II^%20Divisione_eng.htm (v. May 12, 2000).

⁷⁸ In June 1998, on a judge’s warrant, the Bologna Postal Police seized the server machine of the non-profit provider, *Isole Nella Rete*, depriving ordinary users—mostly oblivious of the circumstances— of their Internet services for days. The justification for the seizure was legal action the taken by a travel agency for “continuous defamation” by a left-wing activist group using the server to urge the boycott of the agency for providing travels to Turkey, a country commonly known for disregarding human rights. The machine remained for days in the Police offices, so that, once the machine was returned, the provider recommended all the users to change their passwords since it could not guarantee that unauthorized individuals had not accessed their files (being extraneous to the investigations most users should have been protected by privacy laws against snooping in their accounts) (<http://www.ecn.org/inr/nodo50/inr.html> v. September 18, 2000). The case was also briefly mentioned by the *Washington Post* (copy of the article is at <http://www.ecn.org/inr/nodo50/stampa.htm#washington> v. September 18, 2000).

⁷⁹ The GdF could be loosely compared with the United States’ Internal Revenue Service (IRS). In November 2000, the GdF created the ad hoc *Gruppo Anticrimine Tecnologico* (anti-technology crime group) to specifically fight cybercrime.

⁸⁰ <http://www.gdf.it/> (v. May 11, 2000).

⁸¹ http://www.ilsole24ore.it/norme/secit_ecommerce/ (v. July 28, 2000). The whole report (zipped file) is downloadable from this Web sites.

6.3.4 Political Parties and NGOs

Like in the United States and Germany, Italian Netizens are a sought-after target by political parties: they are usually young, educated, and interested. They are also more willing to volunteer or donate for campaigns,⁸² and vote.⁸³ Small wonder, then, that all the political parties have been looking at the Internet with growing interest.⁸⁴ The Internet also is watched carefully by the right and the left alike because (a) the center-right leader and media-mogul, Silvio Berlusconi, has an immediate interest in the convergence of media, telecom and the Internet,⁸⁵ (b) a good performance of the New Economy—lower unemployment, rising GNP, etc.—it was hoped, might help the center-left government in the 2001 elections. In one crucial instance, however, the Italian case differs from the United States, that is voting on telecom bills in Parliament. In the United States voting on telecom bills in Congress is usually bipartisan, with both Democrats and Republicans siding together; in the Italian Parliament, telecom issues are subject to the same potential struggle as any other issue.⁸⁶

A considerable discussion on political propaganda on the Internet ensued before the April 2000 administrative elections in Italy. The center-left coalition in Parliament passed the so-called *par conditio* law in February 2000. The law imposed an equal “quota” of

⁸² For instance, the majority of the Web sites of political parties discretely invite viewers to send their emails, have specific sections on the New Economy, and an English version of the Web page.

⁸³ In the United States—the only country where these figures are available—according to the Internet research company Media Metrix, “...88 percent of Web users 18 and older plan to vote in this year’s elections, compared to 55.7 percent who reported voting in federal, state or local elections in 1999” (<http://www.mediametrix.com/press/releases/20001011.jsp?language=us> v. November 3, 2000).

⁸⁴ The oldest “wired” party, however, has been the *Radicali* (a liberal-radical party). They were the first to value the Internet as communication medium. Their current Web site (a banner reads “Radicali.it: toward the Net party and a Radical community on-line”—my translation—<http://www.radicali.it/> v. November 23, 2000) is one of the most pleasant and informative and *Radio Radicale* (their radio station at <http://www.radioradicale.it/index.shtml> v. November 23, 2000) has its own CNN-style Web site (also high-quality). Finally, one of the *Radicali*’s leaders set up in 1995, and still maintains, a rather popular and well-linked Web page on a list of political sites on the Internet sorted by country (<http://www.politicalresources.net/> v. November 23, 2000).

⁸⁵ True to an American-style “hands-off” approach, the center-right alliance, *Polo/Casa delle Libera*’, has indicated in its political program that “the Internet should be left alone” (*The Economist*, October 14, 2000:41).

⁸⁶ For instance, the government was outvoted by the opposition in Parliament on how to use revenues from UMTS licensing, in July 2000 (<http://www.repubblica.it/online/economia/umts/reazioni/reazioni.html>, <http://www.repubblica.it/online/economia/umts/mozione/mozione.html>, and <http://www.ilsole24ore.it/24oreinformatica/umts/default.htm> v. July 24, 2000). Similarly, a new political struggle has unfolded about the prospect that *Telecom Italia*, through its ISP *Seat-Tin.it*, may also acquire a private television channel (*Tele Montecarlo*), and thus may become a third media/Internet pole, along with RAI and *Mediaset* (<http://www.repubblica.it/online/economia/seat2/conferma/conferma.html> and <http://www.ilsole24ore.it/finanzaemercati/telecom/tmc.htm>, v. July 24, 2000). Such an eventuality is opposed by the center-right (the third pole might compete with Berlusconi’s *Mediaset*) and supported by the center-left (for the same reasons). Such a struggle will definitively soon have effects in Parliament.

political commercials on all TV broadcasters—private (*Mediaset*) and public (RAI) alike—for all the institutional parties. The goal of this law was to grant

...equal access to programs on radio and television broadcasting containing political opinions, such as party political broadcasts, debates, round tables etc. and other programs where the expression of political views appears to be relevant to all political parties involved in the elections (as well as those involved in the popular referendum). According to article 2, the transmission of such programs is compulsory for the public service (RAI) and for private national concessionaires transmitting free on air.⁸⁷

As a consequence of that decision, the center-right alliance could not take advantage of the privileged position of its leader, Silvio Berlusconi,⁸⁸ as Italy's media-mogul, flooding all the private television channels with political spots in favor of the alliance. The Internet, however, was not mentioned. The reasons for the exclusion of the Internet from the *par conditio* could be the result of the fact that no comparable media monopoly is currently present on-line. Therefore, all parties have more or less equal access to the Net and are ready to exploit it for their political agendas.⁸⁹

The *Democratici di Sinistra*,⁹⁰ (DS, formerly PDS) was the first political party to be attracted by the new medium, longer before *Forza Italia*,⁹¹ the other major Italian party. The Net non-hierarchical, non-profit, and “young” nature could not fail to intrigue left-wing activists who enthusiastically embraced it.⁹² As mentioned earlier, Bologna—the last bastion (until 1999) of good communist (and post-communist) administration—was the first to experiment a metropolitan network. Long term visions of tele-referenda, and tele-polls

⁸⁷ http://www.agcom.it/eng/resp_reg.htm (v. July 10, 2000).

⁸⁸ Almost unexpectedly, the Net made its “own” contribution to the Spring 2001 electoral campaign. As early as Fall 2000, as Mr. Berlusconi opened up the campaign with numerous giant posters outlining a brief message (e.g. “less taxes for everybody”) summarizing his political programs on the walls of Italian cities, images of the same posters but with considerable different messages began to appear on the Net (I received plenty of copies). Most of the messages were humorous or ironic. With good sense of humor, the *Forza Italia* Web site collected most of the altered posters and made them available on-line.

⁸⁹ During the same electoral campaign *Forza Italia* (Mr. Berlusconi's party), one of the posters read “le tre ‘I’: Inglese, Internet, Impresa” (the three “Is”: English, Internet, Enterprise), which should be the goals of tomorrow's Italian schools. *Forza Italia*, following the example of the government itself, “recruited the Net” as asset for its political program.

⁹⁰ Official site at http://www.democraticidisinistra.it/default_ds.htm (v. July 24, 2000).

⁹¹ Official site at <http://www.forza-italia.it/> (v. July 24, 2000).

⁹² It seems that there is a convergence among industrialized democracies that are currently governed by the left on presenting the same young, positive, modern image. Giuliano Amato stepped back in September 2000 in favor of Francesco Rutelli, mayor of Rome, as the lead candidate of the left wing coalition for the 2001 elections. Rutelli, in contrast to Amato, seeks to present himself across as a man of the people rather than a professional politician. Yet he is very much in the mould of Bill Clinton and Tony Blair, vigorous, telegenic, outgoing, modern-minded, good at appealing to the new middle class” (*The Economist*, September 16, 2000:39). U. S. Vice President and Presidential Candidate for 2000 Al Gore belongs to the same class—the man that “thought he invented the Internet”, according to the other Presidential Candidate George Bush Jr. (<http://www.cnn.com/2000/ALLPOLITICS/stories/10/04/campaign.wrap/index.html> v. November 3, 2000). Needless to say, true to its own “breed”, Rutelli is also “a whizz on the Internet” (*The Economist*, October 21, 2000:44).

(Tambini, 1998)—among other services (e.g. discussion groups, computer-literacy programs, access to municipality files, etc.)—probably elated Bologna’s local administrators.⁹³ Those hopes, however, were never fulfilled, as, since 1994/95, the use and diffusion of the Internet in Italy have drastically changed.

In the Italian political scene, the oldest Italian NGO tackling civil liberties and electronic communications is ALCEI, the association for free electronic communication (*Associazione per la Libera Comunicazione Elettronica*).⁹⁴ ALCEI was established in July 1994 by a group electronic communications users.⁹⁵ The association, roughly similar to the American Electronic Frontier Foundation (EFF) is founded entirely through members’ fees and has no corporate sponsors. The association’s philosophy can be summarized in the words of Andrea Monti, a lawyer and its president, “the Internet brings out the attitudes of many governments toward civil rights”.⁹⁶ The association (i.e. its president) has been accused by technical experts in the PA of “being too concerned” with the defense of freedom of communications—small wonder, since it is a civil rights organization.⁹⁷ In this respect, however, ALCEI’s actions have consistently appeared to be well-informed and competent.⁹⁸ Finally, ALCEI is also one of the founding members of GILC, the international “umbrella” organization gathering several pro-liberties NGOs around the world.

6.3.5 *The Industry and Private Sector*

Before the 1990s privatization, the Italian private industry only played a limited role in telecommunications (Natalicchi, 1996:317). Since then, that situation has been reversed, and now the private sector is dominant. Within it, the actors that are most likely to benefit

⁹³ At a conference of the Italian Society for Contemporary History, April 6, 2000, at the European University Institute, Michelangelo Vasta, an economic historian of the University of Siena, stated that the civic networks in left-wing cities such as Bologna might have been a consequence of the predominance of right-wing parties on other media, i.e. the television. The left might have tried to ensure “alternative” channels of communications. I presented this theory to Leda Guidi, Head of the *Iperbole* who absolutely rejected its validity (personal interview).

⁹⁴ There is also an Internet Society Italy (<http://www.isoc.it/>), chapter of the Internet Society, but it is still in its infancy.

⁹⁵ <http://www.alcei.it/default.html> (v. July 24, 2000). The originating event was continuous action by Italian police forces against BBS (bulletin board systems) providers, under suspicious of offering pornographic material. ALCEI is also one of the founding members of the Global Internet Liberties Campaign (at <http://www.gilc.org/about/members.html> v. July 24, 2000), which co-ordinate Internet civil liberties initiative internationally.

⁹⁶ Monti, personal interview.

⁹⁷ Bonanni, personal interview.

⁹⁸ One of the most informative Web sites for laws and commentaries on the Information Society in Italy is INTERLEX (<http://WWW.INTERLEX.IT/index.htm>), which has very close ties with ALCEI.

from the spin off of the New Economy and the TLC are the big industry (that is FIAT), the IT and TLC companies,⁹⁹ and the banking system. The former because it has the capital and managerial expertise to slowly shift its weight from a mature market (cars) to the more lucrative new economy, the latter ones because they provide the services and infrastructures indispensable to the new economy.

Under increasing competition, in March 2000, Italy's main company, the car-producer FIAT, allied with General Motors. This move put an end to FIAT's policy of no-alliance, founded on its supremacy in the home car market. Such reorganizations have become common in the highly mature car market, requiring more efficiency and lower costs that are cut, among other things, by rationalizing the production and exchange of spare parts. In such circumstances, all major car companies have embraced business-to-business (B2B) electronic commerce, and GM and FIAT have announced plans in that respect (White and Ball, 2000:1 and 12). Growing reliance on B2B is, however, only the most noticeable move of a strategy of progressive change by "Internet-enthusiastic" car companies. The ultimate goal of this strategy is to shift car sales on-line and achieve production on-demand conditions (Nobis, 2000:4).¹⁰⁰

Like other industrialized countries, in the last twenty years Italy has experienced an economic "boom" of the IT sector, up to the point that there are currently 120 licensed telecom operators (mobile and fixed).¹⁰¹ Thanks to the fast growing diffusion of telecom services and information technologies, the IT industry has undoubtedly become one of the critical factors in the Italian economy. According to Assintel, a telecom business association, in 1998, the IT sector was worth 17,790 billion Lira, and growing around 10% a year.¹⁰² The report concluded that the New Economy would be one of the most outstanding economic opportunities for Italy. However, the overall depiction of Italian businesses is not so rosy.

If Italian "old economy" large companies, as FIAT, have begun to integrate the Internet in their long-terms plans, such forbearance seems totally lacking among small and

⁹⁹ Telecommunication companies are a very recent (1990s) manifestation of Italy's industrial sector. In the past, "[t]he Italian government's indecisive industrial policy prevented the development of strong manufacturing industry" (Natalicchi, 1996:331).

¹⁰⁰ FIAT launched a campaign ("buy@fiat") for on-line purchasing in July 2000 (<http://www.fiat.com/ita/vorrei/default.htm> v. July 24, 2000).

¹⁰¹ Bonanni, personal interview.

¹⁰² A summary of the report is available at http://www.ilsole24ore.it/24oreinformatica/speciale_3d.20000505/INFORMATICA/inf_e_telecomunicazio ni_inf /Aaa.htm (v. May 11, 2000).

medium enterprises (SMES), the mainstay of the Italian economy. In Spring 2000—a period of hectic interest in the media for “the New Economy”—the Italian Statistical Office (ISTAT) published a survey on the census of SMES (between 1 and 250 personnel) which included figures on the use of information technologies (IT).¹⁰³ While 22.8% of companies did use them for different tasks, a striking 77.8% had no use for IT. More precisely, while only 21% of very small companies (1-19) had applied IT in its production, 95.6% of those with more than 250 employees did (in 1999). The bleak picture did not change for R&D. On the contrary it got worse. Only 1.4% of those companies had invested in R&D, while 98.6% had not (in 1997). It is thus not surprising that still in 2000 the business consulting company Merrill Lynch ranked Italy the last industrialized country for growth rate of the New Economy (*Il Sole 24 Ore*, 2000:1).

As of May 2000, according to the association representing the Italian Chambers of Commerce, there were 72,656 companies on the Internet, 24,065 Internet IP numbers (URLs) and 48,591 e-mail addresses.¹⁰⁴ Much to the disappointment of the New Economy enthusiasts, for a considerable number of companies, e-commerce is still considered to be “a waste of time, a game, or, at the most, the illusion of being part of the global market”, since 49% of small and medium Italian entrepreneurs still consider the Internet and the New Economy as “an option”.¹⁰⁵ In the Fall of the same year, another study (Lo Presti, November 3, 2000:XIII) summarized the attitude of Italy’s e-business as “many unrealized ideas”, criticizing the “detached” position of many Italian entrepreneurs who see the Net as a positive economic factor but do not really know what to do with it.

Another actor that will benefit from the new economy and the Net will be the banking system. The Italian Banking Association (ABI),¹⁰⁶ founded in 1919, currently comprises 1015 banks (including foreign banks operating in Italy) and other financial intermediaries, thus a formidable economic actor. Given the nature of the Internet and of electronic payments, one expects a major involvement of banks in the debate about the New Economy, and Internet in general in Italy. Credit cards, digital signature, and home banking are “natural” domain for the banking system. In this respect, Italians have shown unexpected adaptability, since in 1999, 28 millions of them had bank or credit cards and,

¹⁰³ <http://www.istat.it/note/cens.pdf>, (v. April 27, 2000).

¹⁰⁴ *Infocamere* is at <http://www.infocamere.it/> and also http://www.ilsole24ore.it/24oreinformatica/neweconomy/archivio/maggio00/090500_2.htm (v. May 11, 2000).

¹⁰⁵ According to a survey conducted by George S. May International on 350 Italian entrepreneurs (quoted in *Il Sole 24 Ore*, May 9, 2000:12) (my translation).

¹⁰⁶ *Associazione Bancaria Italiana*, at <http://www.abi.it/> (v. May 11, 2000).

surprisingly, up to 2 million routinely operated on-line banking (*Il Sole 24 Ore*, May 9, 2000:31).

Finally, the industry's representation is mainly carried out by two organizations, namely Assinform and Anasin—the former was founded in 1947 by office furniture producers and slowly evolved into an ITC business association.¹⁰⁷ In 1998, both organizations joined Federcomin (Federation of Communication and Informatics Industries) along with other telecom companies such as *Telecom Italia*, *TIM*, *Olivetti*, *Infostrada*, and *Tiscali*. Even more companies such as *Wind*, *IBM Italia*, *Siemens*, *Italtel*, *Blu*, *Microsoft Italia*, *RAI*, etc. as well as associations (e.g. the Italian Association of ISP) joined later on. All these organizations are currently active in winning over the general public, the government and the PA to the use and “culture” of ICT, and the development of an information society as vital choice for the Italian economy.

6.4 The Issues

At first glance, as of Spring 2000, the overall number of Italian Netizens seems impressive: 10 million people and growing, a figure quoted, with some variations, by other media and general Internet enthusiasts. However, a closer look reveals that the figure of 10 million includes also those individuals that have browsed the Net only *once*, and, perhaps, after that have decided that it is not worth their time and attention.¹⁰⁸ Nonetheless, it cannot be denied that the number of Italians who, for diverse reasons, have become Internet stakeholders is fast increasing.

Finding competent information and diversity of opinions on these issues is quite straightforward, since independent sources of information abound. What it is problematic in the Italian case is that Italians are not accustomed to check for alternative sources, and often simply do not bother to acquire information on topics that they consider marginal. Hence, despite the growing diffusion of the Net in Italy, the issue-areas presented in this section are still debated among a relatively small group of more or less well-informed actors.

¹⁰⁷ *Olivetti* began as producer of office furniture and typewriters, entered the computer business, and later the telecom sector and also gave birth to *Inforstrada*, later on bought by the British *Vodafone*. More recently, *Olivetti* has abandoned the computer business and is now only active in telecoms, while *Vodafone* may soon sell *Infostrada* to the Italian Electricity producer ENEL. Interestingly enough, ENEL is still a state-owned company, and thus, the government may own again another telecom company after selling *Telecom Italia*.

¹⁰⁸ Weekly Observatory of the Web Report #5.2, *Between/MT&T*, at <http://www.quadrante.net/between/wow22.asp> (v. May 11, 2000). In July 2000, according to the Weekly Observatory there were 11,6 millions of Italians that have logged on at least once in their lives (Weekly Observatory of the Web report #8.1, received July 28, 2000).

6.4.1 Italy's Top-Level-Domain (.it)

In Italy, as is the case in other countries, the “un-official” ranking of domain names after dot-com values the prestige of the generic top level .it. Since the mid-1980s, Italy’s “country Top-Level-Domain” (ccTLD) has been administered by “a chosen few” of the National Research Council (*Consiglio Nazionale delle Ricerche*, CNR),¹⁰⁹ after signing and agreement with IANA (Internet Assigned Names Authority, forebear of ICANN). Given that the registration law excluded individuals from owing it-domains, the CNR main interlocutors were mostly universities followed by a few large companies. Despite relatively restrictive procedures, the percentage of registered domains has grown considerably in the period 1994-2000, going from a few hundred to a predicted 180,000 of mid-2000.

Currently, similar to other countries, there are two agencies responsible for assigning the Italian TLD are two, the Naming Authority (NA)¹¹⁰ and the Registration Authority (RA).¹¹¹ Both are hosted by the CNR Institute for Telematics Applications in Pisa under the domain *nic.it*.¹¹² Established in 1994,

...the Naming Authority is the body which establishes the operational procedures and rules to which the national Registration Authority conforms. Because of this precise distinction of roles, the Naming Authority must be a body separate and independent from the Registration Authority.¹¹³

The NA thus determines the general rules that the RA has to follow in assigning domain names. More specifically,

[d]omain names are assigned by the RA to registrants following the requests chronological order, as defined by the Technical Registration Procedures...[and] have the only purpose to identify uniquely groups of objects (services, machines, post boxes etc.) located on the net....[The registration of] the ccTLD “it” can be assigned to subjects belonging to a member state of the European Union. Associations without VAT numbers or fiscal code (or equivalent) and persons not owning a VAT number (or equivalent) can register a single domain name, only.¹¹⁴

Names are assigned on a *first come-first served* basis with all the rules for the protection of well known names and brands applying of the Italian civil code for all those individuals that

¹⁰⁹ Monti A., “Gli Accaparramenti dei Nomi a Dominio: Lei Non Sa Chi Sono Io”, InterLex, March 16, 2000, at <http://WWW.INTERLEX.IT/regole/amonti33.htm> (v. July 13, 2000).

¹¹⁰ “the organisation defining the rules for the domain names assignment and for the operating procedures of the Italian Registration Authority”, at <http://www.nic.it/home.html> (v. July 12, 2000).

¹¹¹ “the organisation responsible for the assignment of domain names and the management of the registry and the primary name-server for the Top Level Domain .it” at <http://www.nic.it/home.html> (v. July 12, 2000).

¹¹² <http://www.nic.it/> (v. July 12, 2000).

¹¹³ <http://www.nic.it/NA/nastory-engl.html> (v. July 12, 2000).

¹¹⁴ <http://www.nic.it/NA/regole-naming-v32-engl.txt> (v. July 12, 2000).

are resident in Italy.¹¹⁵ That is, it would not be possible to register the domain *fiat.it* by an early comer because the name “Fiat” is already protected by the civil code. Overall, it can be said that the NA and the RA operate in the “self-governance” spirit so common on the Internet.

With the goal of overall liberalization, the rules to register domain names were changed by the NA in December 1999 (effective January 2000), after an open assembly in which two observers from the government participated. The major modifications were that individuals without VAT registration numbers could sign in,¹¹⁶ and that it was possible for one individual to register more than one domain (the one person-one domain rule). The RA, on its part, had only to verify if the required names for registration were available. The news arrived on the media, and, unsurprisingly, a rush to register names ensued, including “domain-grabbing” acts.¹¹⁷ Some of these acts involved names of politicians who, according to some sources, urged the government to intervene.¹¹⁸ The premier’s office did intervene with a letter to the RA urging “strict limits” in assigning names, until a proper law shall be passed.¹¹⁹

The core of the problem with Italy’s TLD is that some government members seem convinced that only a national law should be the solution, since self-government has a previously established record of inefficiency, and the protection of names in the civil code requires the claimant to go to court—with no guarantee of success. Many Netizens and Internet organizations have opposed this, on the point of view that such a move would unnecessarily complicate matters. Instead they propose that a better solution is to enhance existing rules. They claim also that the proposed legislation would simply increase statutory control on the Net. In this issue-area, the two main competing forces are the government, on one side, and several users’ groups, and some consumers’ organizations and pro-liberties NGOs, on the other. The private sector has sought contacts with both parties, showing a

¹¹⁵ As it is the case elsewhere, individuals breaking the Italian law from abroad cannot be persecuted, as long as they are not physically on the Italian soil.

¹¹⁶ VAT registration numbers are usually owned by companies, or professionals due to tax requirements. Many Italians do not have them, and therefore were somehow not allowed to register under the *.it* domain.

¹¹⁷ “Domain-grabbing” (or “cybersquatting”) is the U.S. definition of the act, by an individual or a group, of registering a large number of domains of famous trademark names, with the goal of re-selling them to the original companies or well-known personalities—e.g. *juliaroberts.com* or *madonna.com* (for a while a pornographic Web site) were true instances.

¹¹⁸ <http://www.andreamonti.net/pcpro/pcpro109-2.htm> (v. July 13, 2000).

¹¹⁹ The original of the letter can be seen at <http://www.nic.it/RA/documenti/nomi.jpg> (v. July 13, 2000).

preference to “cosy-up” with the government, with the hope of winning a better deal.¹²⁰ Much like the United States case, the DNS is also for Italy the issue-area over which the interests represented pro-liberties NGOs, consumers’ organizations and users’ groups and those of the private sector are most likely to clash.

6.4.2 *The “New Economy” and e-commerce*

As stated in the introduction to this chapter, between 1999 and 2000, Italy’s media, stock market investors, banks and, many ordinary citizens caught the “New Economy” fever. In mid-2000, according to a market research institute,¹²¹ there were fifty-eight trading operators and 190,000 trading accounts in banks (La Posta, July 7, 2000:IX). On newspapers and television commercials the Internet and the New Economy were mentioned endless times, and it was enough that companies had the words “Internet”, “Net” or “Web” included in their trademarks to achieve spectacular performances on the Italian stock exchange.

As Giuseppe Rao has put it, “everybody started lecturing about the Internet. Journalists and entrepreneurs, who a year earlier had no idea of what the Internet was, began to explain what the New Economy was”.¹²² Generally speaking, the other media have launched “campaigns” to explain to the large public what these new terms means. The success of these attempts, however, has been thus far limited at the most, since even those that claim first-hand business experience seem to have a narrow view of the Internet and fail to comprehend that the Internet is not only “New Economy” (Alvi et al., 2000).¹²³

Despite high hope that, according to Forrest Research consulting for instance, in the next two years the Net will become a mass phenomenon in Italy and Europe (Caravita, June 23, 2000:I) or that UMTS will bring Internet to millions of Italian phone enthusiasts, serious structural obstacles exist to meet those goals. In the classification of the forty-six “venture capitals”—the world locations for the New Economy—charted by *Wired* in July 2000 not one single Italian location was mentioned. Europe’s “Silicon Valleys” seem only to be near Stockholm, London or Helsinki, while Milan, Turin or Ivrea failed to meet the magazine’s

¹²⁰ This is another characteristic feature of Italy’s private sector. A former president of the influential Italian Confederation of Industries (*Confindustria*) once remarked that his association could not help it but being “naturally pro-government”.

¹²¹ <http://www.irs-online.it/pubbli/trading.htm> (v. July 21, 2000).

¹²² Rao, personal interview (my translation).

¹²³ The reference is about a round table of experts on the economic journal *Surplus*. Reading their conclusions is rather straightforward about the limits of their views.

criteria.¹²⁴ Moreover, in the list of the ten world “colossi” of the New Economy, not one Italian ITC company is quoted, with Britain (*Vodafone-Airtouch*), Germany (*Deutsche Telekom*) and Finland (*Nokia*) representing Europe (Zampaglione, July 3, 2000:38). Furthermore, according to *Time*, among the “Europe’s fifty hottest tech firms”, not one is Italian.¹²⁵

Finally, all too many users and telecom operators seem to concentrate their criticism, for instance, on the time tariff that *Telecom Italia*—still a *de facto* monopoly¹²⁶ on local calls—applies, demanding its substitution with a fixed flat rate. This is only one aspect of the problem. If users could enjoy broadband access (i.e. fast speed) to the Net, without delays and interruptions, then the basis cost per minute of a local phone call would not cause such annoyance. Broadband access is a relatively minor problem for businesses, which, generally speaking, are willing to sustain the expenses for wiring up “the last mile”—i.e. the distance between the local switching point and the private user. Such cost, however, does discourage private users from requesting broadband access, who think that the wiring up of their building and houses should be done by telecom companies. Being fully privatized, however, the main owner of the physical infrastructure, i.e. *Telecom Italia*, does not see this service any longer as a part of its role of “public service”, and therefore it intends to do it only as long as it is profitable. With neither users and nor the carrier neither willing to sustain most of the cost, an exasperating deadlock ensues.¹²⁷

At the beginning of June 2000, the Italian government introduced its program for the New Economy. According to premier Giuliano Amato, since the appearance “on the surface” of the New Economy (“it is like a mole working underground before going up”) is still some time away, the government has a crucial role in promoting all that.¹²⁸ The plan is divided into four areas: (1) human capital, (2) e-government (see section 3.3), (3) e-commerce, (4) infrastructures, access and competition. Among the activities targeted to

¹²⁴ Proximity to universities and research centers, presence of large companies providing marketing skills and economic stability, residents propensity toward entrepreneurial risks, and availability of venture capital, <http://www.wired.com/wired/archive/8.07/silicon.html> (v. May 12, 2000).

¹²⁵ “Fifty firms to watch as the Web goes wireless and e-commerce becomes a mainstream way of doing business”, at <http://www.time.com/time/europe/specials/eeurope/field/top50.html> (v. September 18, 2000).

¹²⁶ *Telecom Italia* now faces competition on local calls too from carriers such as *Infostrada* and *Wind*. However, these new carries will have to limit their operations to large urban areas, since they are still negotiating with *Telecom* the fees that they should pay to reach small urban or rural areas, which, by far represent the largest pool of customers, although not the most profitable.

¹²⁷ Rao, personal interview.

¹²⁸ Quoted in http://www.ilsole24ore.it/24oreinformatica/neweconomy/soc_inf.htm (v. July 4, 2000) (my translation), and also http://www.palazzochigi.it/fsi/eng/actionplan/government_reports_summary.html (v. July 4, 2000).

improve the quality of human capital were a better computers-to-students ratio,¹²⁹ mobility of researchers to industry (and better coordination between private and public research) and spin-off of academic investigation for companies, as well as training and re-training in ITC for unemployed or unskilled workers. In these respects, particular attention in planning and investment would go to Southern Italy, since the government has repetitively stated that the New Economy represents clear opportunities for that area. The main financial source for these initiatives should have been a 10% quota of the profit expected by the government (40/50 thousand billion Lire, roughly 20/25 billion euros) from the auction of UMTS licenses in the Fall 2000.¹³⁰

The UMTS auction, however, did not produce the expected results for the government. The Italian government hoped to imitate the successful auctions of Germany and Britain, albeit on a smaller scale. At the end of October 2000, the auction lasted only a few days, and in the end the five licenses were awarded to five of the six participants (one of the contestants withdrew) for circa 23,550 billion Lira (slightly over 12 billion euros).¹³¹ It was a serious blow for the Amato government, which was highly criticized by the opposition¹³² as well as by the international press for not considering those auction cases with disappointing results. The participation of too few bidders had yielded poor results for the auctions in the Netherlands,¹³³ which might be the case for Austria as well,¹³⁴ and suspicions have been raised that telecom carriers have agreed among themselves to put a ceiling on bids after seeing the British and German experiences.¹³⁵

Much like in Germany and the United States, all the main actors of the Internet debate are overall in favor of the New Economy. Several ICT businesses (from small ISPs

¹²⁹ Currently 1 to 15, to be improved to 1 to 10.

¹³⁰ <http://www.ilsole24ore.com/art.jhtml?codid=22.0.51332801> (v. November 7, 2000). *The Financial Times* put the Italian government's expectations as high as 50/80 billion Liras (quoted in <http://www.ilsole24ore.com/art.jhtml?codid=22.0.51542791> v. November 7, 2000). These figures, however, were discarded by one Mr. Amato's economic advisers, who put the amount expected by the Italian government for the UMTS auction to 25,000 billion Liras, i.e. close to the final total of the auction (the letter is at <http://globalarchive.ft.com/globalarchive/articles.html?id=001027001264&query=UMTS> v. November 7, 2000).

¹³¹ The total sum might be higher if the government retains for compensation the 4,000 billion Liras deposit that company *Blu*, which withdrew from the auction, had to provide in order to participate in the competition.

¹³² <http://www.ilsole24ore.com/art.jhtml?codid=22.0.51332801> (v. November 7, 2000).

¹³³ *The Financial Times* quoted in <http://www.ilsole24ore.com/art.jhtml?codid=22.0.51542791> (v. November 7, 2000).

¹³⁴ <http://globalarchive.ft.com/globalarchive/articles.html?id=001103003966&query=UMTS> (v. November 7, 2000).

¹³⁵ [http://www.ilsole24ore.com/art.jhtml;\\$sessionid\\$YZWCREIAAPOSSCTCAIFSFYKMIBAYIV3?codid=22.0.54495833](http://www.ilsole24ore.com/art.jhtml;$sessionid$YZWCREIAAPOSSCTCAIFSFYKMIBAYIV3?codid=22.0.54495833) (v. November 7, 2000).

to large telecom carries), consumers' organizations and pro-liberties NGOs have been battling against *Telecom Italia* still quasi-monopoly, demanding more competition and greater transparency for tariffs. The government, after the privatization of *Telecom Italia*, has tried to remain neutral, but it has also re-entered the telecom sector, with the acquisition of two of the great telecom giants, *Wind* and *Omnitel* by the only half-privatized energy provider, *Enel* in 2000. The anti-*Telecom Italia* front has obviously harshly criticized this move.

6.4.3 Privacy, Cryptography, Digital Signature and the e-government

Like the constitutions of the majority of European countries, the Italian Constitution includes two articles that contribute to protect personal (art.14 and 15). Moreover, Italy received the EU Directive 95/46/CE (October 24, 1995) on the Protection of Personal Data, which was adopted with the law n. 675 of December 31, 1996 (675/96).¹³⁶ With specific reference to privacy on the Net, there are three levels, or layers, of Internet communications, namely (1) the telecom provider, (2) the Internet provider, and (3) the content provider. At each of these levels, the service provider may come under government control. Layer 1 carries data only on the telephone traffic, and the service provider does not know—nor it is interested in— the identity of the caller; in n.2, the provider could gather detailed information in the log files about the “on-line behavior” of the caller and is thus subject to art.12 of the law.¹³⁷ Finally, at level n.3, when his/her Web site is accessed, the provider could ask individual users to “register”, i.e. send personal information, and hence he/she too is able to accumulate data on users' behavior and is subject to the privacy law.¹³⁸

Law 675/96 also laid the ground for the approval of the law n. 59 of March 15, 1997 (59/97) on electronic documents and public acts (*documento informatico*) and the electronic signature. Both these features would be impossible without public key cryptography. The specific problem for Italy here is that, while there are no prohibitions to access strong encryption software, there is little awareness of how crucial cryptography is for the whole

¹³⁶ The EU Directive 95/46 EC was further strengthened by the EU Directive 97/66/EC of December 15, 1997, on the transmission and elaboration of personal data. Since its approval, the 97/66 has been the a topic of negotiations and discussion between Europeans and Americans. The former wanted U.S. companies treating data on EU citizens to abide the EU directive, while the latter refused. The “safe harbor” proposal is the result of the negotiations, but the problem is far from solved (see also chapter 4 on the United States).

¹³⁷ These log files are crucial for law enforcement officials to fight cybercrime, since the files keep accurate track of an individual's on-line behavior. If not subject to judicial warrants, however, they could also lead to abuse and serious privacy infringements.

¹³⁸ For an accurate description, see Monti A. “La Trave nell'Occhio: il Garante Controlla Internet”, *InterLex*, June 22, 2000, at <http://WWW.INTERLEX.IT/675/amonti37.htm> (v. July 11, 2000).

Internet. Therefore, attempts to resist the government's change of the legislation would be more difficult to organize. Cryptography is likewise indispensable for e-government.

In mid-June 2000, the government revealed its plan for the e-government. The plan should allow the government, within ten to twelve months from its presentation (a) to improve the efficiency of the public administration, (b) to integrate different administrative services offered to the public, and (c) to guarantee the public maximum access to information. In addition to access to the PA databases and services, individuals will be provided by the PA with electronic IDs to facilitate access to those services, and their digital signatures will be commonly accepted by PA offices for any kind of operations. The estimated cost would be 1335 billion Lira (roughly 690 million euros) that would mostly cover the costs of building and operating the PA Extranet and of training 400.000 employees every year.¹³⁹ This initiative was taken within the framework of the G8 Government-on-Line project, launched by the G8 in the mid-1990s to provide better government services.¹⁴⁰ Doubts that, in the short term, an organization "deaf to its clientele" (Koff and Koff, 2000:152) may release its control on its main source of prestige and influence are nonetheless legitimate. It is unlikely that the supply of PA on-line services will be implemented before the current generation of civil servants, mostly unfamiliar with ICT, retires. The twelve month deadline thus appears to be little more than lip-service to the G8 grand initiative.

To implement all these projects (*documento informatico*, e-government, etc.), to render the New Economy and e-commerce a reality for Italian customers, and, in general, make Italian users feel more secure in using the Net, one factor is indispensable: unrestricted access to strong cryptography.¹⁴¹ As in the case of Germany, the situation appears inconsistent. Strong cryptography in wired communications is freely available and has never been restricted in Italy—as the dataset shows. At the same time, law enforcement agencies try to urge the government that wireless communications should use only a limited set of encryption codes, with which are supposed to be very familiar.¹⁴²

Organized crime has always had the financial resources to acquire strong encryption codes for its secret communications. With the military and diplomats, they form to a

¹³⁹ <http://WWW.INTERLEX.IT/attualit/egovsint.htm>
and http://www.ilsole24ore.it/24oreinformatica/neweconomy/archivio/giugno00/art_230600.htm (v. July 4, 2000).

¹⁴⁰ <http://www.open.gov.uk/govoline/welcome.html> (v. July 5, 2000).

¹⁴¹ Substantial security guidelines on encryption and public key cryptography have been published by AIPA on its Web sites (at [http://www.aipa.it/attivita\[2/standard\[5/archiviazioneottica\[1/firmaweb.asp](http://www.aipa.it/attivita[2/standard[5/archiviazioneottica[1/firmaweb.asp) v. July 25, 2000).

restricted, and clearly identifiable, group. Thus, law enforcement officers have been able, at least, to monitor organized crime encrypted communications—even if they could not decipher it—to see who is talking to whom. Now, with the greater availability of strong public key encryption for individuals, it has become increasingly difficult to distinguish between the messages of law abiding citizens and those of drug dealers, and this occurrence will only deteriorate. In other words, the police “has come up against a wall” with rapidly falling capabilities to see through it.¹⁴³ Small wonder that ALCEI has noted that “[in] this uncertain legal environment, some control advocates are aggressively clamoring on the doomsday risks of ‘criminal’ or ‘immoral’ use of communication and demanding controls on encryption”.¹⁴⁴

Italy, however, is not alone in facing this obstacle, since the situation is the same in the in many countries, within and without the OECD. On-line and off-line attempts to address the problem have slowed down networks, have left criminals nonplussed, and, in general, have been contested by users and civil liberties organizations due to their privacy endangering potential. Once again, as in the United States and Germany, there is no one “perfect” solution to this predicament. These imperfect solutions come closer either to protecting personal privacy and individual communications, or to enhancing security and facilitating the work of law enforcement, depending which elements a government and its constituency value as more important at any given time.

The parties involved in debate on free cryptography and privacy mostly resemble the situation in both Germany and, to some extents, the United States. The private sector, pro-liberties NGOs, and users’ groups are all in favor of unrestricted availability and sale of encryption software, while law enforcement agencies mostly argue that their interception capabilities should be preserved. Similarly, the former value privacy protection at premium (even the private sector has understood that customers are highly concerned about it). On the other hand, the latter are increasing inter-EU cooperation with other law enforcement agencies, and connecting together their databases (particularly in Europol). Obviously this developments are seen with greater apprehension by pro-liberties NGOs and users’ groups which are afraid of lack of accountability of Europol and demand even stronger EU privacy guarantees.

¹⁴² Monti, personal interview and also <http://www.gandalf.it/free/monticfp.htm> (v. July 25, 2000).

¹⁴³ Bonanni, personal interview.

¹⁴⁴ <http://www.gandalf.it/free/monticfp.htm> (v. July 25, 2000).

The government tries to accommodate both positions, and is mostly concerned with not hampering the take-off of e-business. Like in the case of Germany, however, the Italian national security community mostly worries about the possible (but not certain) risk of cybercrime. This state of affairs explain why it is law enforcement officers that are active in the debate, more than intelligence and defense departments, which do not seem willing to give any credibility to other cyberthreats.

6.5 Conclusions

As in the case of Germany, but only partially as in the case of the United States, the main conclusions that the reader can draw from the Italian experience are two. First, the stakes in the New Economy are so high that the Italian government would do nothing that might undermine the diffusion of the Net among the population and shatter the expected economic returns. Second, security is a relatively minor issue, mostly of concern for computer experts, and for some sections of law enforcement and the judiciary. At the time of writing, the perceptions of the Internet as a threat to national security, or that "the sole information superpower" may take unfair advantage from its hegemonic position have been rather unfounded for the Italian government.¹⁴⁵

Like the American and other European counterparts, the Italian government seems now convinced that the New Economy, e-commerce, and Internet have become indispensable concepts of modern industrial, or post-industrial, economies. Hence, like its foreign equivalents, the Italian government is trying to manage this transition. The main obstacles on the path of Italy are (a) the rather large number of members of Parliament, of local administrations, of political parties and of the government itself that still have a poor understanding of modern technologies, and the Internet in particular, and (b) the die-hard habit of believing in the indispensability of strong government supervision on unfolding events. While the former problem may be solved by a generation change, the latter is more likely to persist longer.

There is widespread agreement at all levels of the state that this transition to the New Economy is possible through strict cooperation by public institutions and private

¹⁴⁵ One does not have to go too far to find proofs of this fact. The OECD also issues directives about the Net for member countries, and although not binding as EU directives, they are always very carefully considered by OECD governments. The drawback in this case, however, is that the OECD is an organization run mostly by English-speaking countries, and by the United States in particular, which is very aware of the business priorities of its companies. Bonanni, personal interview.

businesses. The reality, however, does not reflect that attitude. In fact, also due to the intervening effects of the former problem, it seems almost inconceivable to many public figures in parties and Parliament that the government could have only a supporting role, as a true governance player, getting involved in the process only to avert major law infringements or the manifest exclusion of weaker economic actors. At the same time, the fact that in Italy, one of the most “regulated” countries in the world, the Antitrust and the Authority for Communications have managed to completely liberalize the telecom market may bode well for the future of Italy’s Information Society.¹⁴⁶

Another crucial consequence of this state of affairs is that, just like the United States and Germany, the business dimension of the Internet has become paramount. The expectations for growth and economic returns are so high, and the “money” and investment so large, that the Italian government is afraid of doing anything that might hamper such perceived benefits. At the same time, only a fraction of law enforcement personnel is aware of and trained for fighting cybercrimes—the same applies for most of the judiciary. Or, in another significant occurrence, i.e. the ICANN “At-Large” membership for the election of ICANN Board of Directors, the government, business association and the media began to advocate Italian memberships only in mid-July 2000 (the deadline for membership was July 31).¹⁴⁷

The same state of affairs is true for many political leaders, members of Parliament, and civil servants. Only a minority of them is comfortable with the understanding that the same strong cryptography that is indispensable for e-commerce and on-line credit card payments will also be used for money laundering or arms deals, and that positive benefits of that technology can hardly be separated from its negative downside. Furthermore, the possibility that a growing reliance of the country and its economy on information and telecom infrastructures may also mean greater vulnerability and exposure to malicious

¹⁴⁶ On the other hand, it might be also the case that telecommunications have been one of a few successful exceptions in the Italian privatization process, since other sectors (like Enel’s electricity) have not been handled as well (*The Economist*, October 14, 2000:85). Enel may even increase the size of the state’s presence in the economy. In fact, Enel has acquired Italy’s third largest telecom carrier Wind, and may also purchase *Omnitel* (the second largest carrier) from Germany’s Mannesmann.

¹⁴⁷ The Italian participation to the “At-Large” membership (only 1670 “unverified” applicants) became an issue only after government, associations and business realized that, by July, only a few hundreds of Italian users had bothered to apply, compared with tens of thousands of Japanese (over 38,000), Chinese (over 33,000), Americans (19,500), and Germans (20475)—all these figures indicate “unverified” applicants—(<http://members.icann.org/pubstats.html> v. July 28, 2000). At least, the Italian newspaper *La Repubblica* admitted that, if, on the one hand, ICANN had not been ready and willing to accept help from volunteers to make easier to register and participate in the elections, on the other hand, Italian media were also to blame for their late and lukewarm attention to such a crucial issue (http://www.repubblica.it/online/tecnologie_internet/icann/icann/icann.html v. July 28, 2000).

hacker (crackers) attacks, and cybercrime is taken into consideration by only a handful of PA and government officials.¹⁴⁸

Within the group of advanced economies, Italy has been among the late-comers to the Internet. This is an important dissimilarity with Germany that I will soon explain. With the New Economy (as, to some extents, with the nineteenth century industrialization of the country), the Italian government has taken the lead. While ICT-related businesses, such as ISPs and software companies, has immediately followed suit, the more established firms (including the telecom giants, *Telecom Italia* and *Infostrada*) were even slower than the government in discovering the Net. As in Germany, the government has been highly hopeful to reap the economic benefits of the Net, and has not seen any threats to national security coming from cyberspace.

Hence, unlike the United States and several other European countries, including Germany, Internet's popularity in Italy is literally a recent phenomenon. Only in 1999/2000, the Net truly became fashionable and widespread both with the large public and the more traditional entrepreneurial community. By looking at the raise of IP hosts (with the domain name *.it*) it is possible to observe how much the phenomenon has grown in a very short period of time. The inertia of the Italian society and business while the Internet stretched outside the scientific community and among the larger public should have allowed the national security/law enforcement community to be more forceful with, and perhaps to exercise more pressure on, the government to seize greater investigative powers and interceptions capabilities. After all, it is not entirely uncommon that when national governments are faced with unfamiliar occurrences, they tend to act conservatively and are more prone to listen to the "security experts". Indeed, as I described above, in the early phase of Internet growth, law enforcement officials and the judiciary did sometime act quite indiscriminately. Nevertheless, police excesses have been rather scant, and the MOD has been totally absent from the debate on Internet threats.

This situation has not been due to a lack of possible menaces. Italy, being an advanced, computer-dependent economy like Germany and the United States, could be a prime victim of cybercrime, especially if such crime might expand to become a "national security" threat. However, much like Germany's, Italy's center-left governments have concluded that (a) there is no strong evidence that cybercrime can grow unchecked to

¹⁴⁸ Although the potentialities of cyberwarfare or cyber-terrorism are still only speculative, it does not mean that these circumstances will not change in the future with a larger number of countries more critically vulnerable.

become a national security problem, and (b) other than that, risks from cyberspace are mostly speculative and should not hinder Italy's path to the New Economy. If it is true that the United States' Internet model is often the example to follow, certainly the Europeans are still unconvinced about cyberthreats, perhaps with the exception of cybercrime.

The Italian government's first attempts at helping the diffusion of the Net have been somehow naïve, genuinely interested (most of the time) and almost bold for an institution traditionally reactive and procrastinating. Some of the benefits of those decisions are now coming to the surface.¹⁴⁹ If the Italian government conceives that it can do a better job at coordinating the actions of the private sector, pro-liberties NGOs, consumers' organizations and users' groups by honestly listening to them, much more will be achieved.

Perhaps, in the end, Italy's infatuation with the New Economy and the Internet will offer new opportunities for Italians to truly become dedicated Netizens. Nonetheless, judging from the ICANN or UMTS cases, the road to Internet citizenship seems still quite long.

¹⁴⁹ In April 2001, an OECD report openly praised Italy's liberalization of the telecom sector and progress in modernizing the public administration (http://www.governo.it/sez_dossier/ocse_roma/rapporto/prefazione.html and <http://www.repubblica.it/online/economia/ocseitalia/ocseitalia/ocseitalia.html> v. April 5, 2001).

Vertical line on the left side of the page.

Vertical line with small dashes on the left side of the page.

Vertical line on the right side of the page.

**CHAPTER SEVEN - CONCLUSIONS:
DIGITAL WINNERS, VIRTUAL LOSERS**

*Internet IS for everyone –
but it won't be unless WE make it so.
(Vint Cerf, Co-founder,
Internet Society, and
Co-inventor of TCP/IP,
April 7, 1999)¹*

7.1 Now, Where Do We Stand?

This work has compared how two of main theories of IR, namely realism and liberalism, could answer the question of why national governments want to control the Internet. Competing hypotheses linked to the two theories have been tested with quantitative investigation in the first part of this dissertation. In this part, the unit of analysis was the state, intended as a unitary actor.²

The results, however, plainly showed that to properly address the research question, studying the state level (with the national government to represent it) would not suffice. Domestic factors, as confirmed by the case-studies, have had a tremendous impact on the problem of Internet control. Political leaders know well that all politics (whether at home or abroad) require extensive bargaining, and the result is often a compromise. Under such circumstances, liberalism would, as expected, score higher in terms of explanatory power.

Generally speaking, within the domestic politics theory, two explanatory approaches are well-established and widely accepted: (a) one focusing on domestic structures and (b) one privileging domestic interest configurations. In my investigation, I have combined the two, because, in the three case studies, domestic structures and interest configurations have appeared to be equally relevant to fully address my research question.

Focusing only at the domestic level, however, would have overlooked some important features of the problem: the Internet, in fact, is “naturally” very international as well as very domestic. All the actors here concerned, national governments, ICT companies;

¹ <http://www.isoc.org/isoc/media/speeches/foreveryone.shtml> (v. October 10, 2000).

² This assumption is common to both theories. However, it is more frequently applied by realist scholars.

and NGOs, have developed international ties with reference to Internet control.³ The adoption of a research design that monitored both dimensions has thus become essential. Finally, information distribution and how information distribution asymmetries influence domestic as well as foreign policy decisions have also been central to this dissertation. They both create political advantage or penalize certain actors. In this respect, I have loosely adopted Milner's viewpoint (1997) on information asymmetries.

It seems paradoxical that one could talk about incomplete information: in the case of the Internet, there is too much information available. Common sense suggests that too much information almost equals no information, since there are limits to absorbing it. Nevertheless, while the Internet is not a case of incomplete information, there are information asymmetries.⁴ Abundant information in fact produces a multitude of informed actors that, in turn, multiply the levels of bargaining and further subdivide the issue-areas. Such an outcome is certainly not efficient, but it is unquestionably consistent with the decision-making process in democracies.

In this last chapter, I will first briefly summarize my findings, and then outline their policy implications as well as the direction of future research about statutory control on the Internet.

7.2 Explaining The Cases

For the case studies, I have examined three democratic countries with varying degrees of domestic structures. Out of my sample, only democracies were selected because, with the exception of a few autocratic states such as China and Singapore, for the time being, only advanced democracies face the three (potentially) conflicting goals that have emerged from my analysis: (a) exploit the opportunities of the New Economy, (b) preserve the privacy and freedom of speech of their citizens, and (c) safeguard national security (both internal and external). The political-economic actors representing the social interests of (a) and (b) (i.e. users', and consumers' groups, pro-liberties NGOs, ICT companies and business associations) have somehow joined forces to form powerful, albeit not official, coalitions. Such an outcome is mostly manifest in the United States, and, to a less extent, in

³ For instance, governments try to fight cybercrime (the FBI and NSA are cooperating with their counterparts in other democracies); companies such as Yahoo, eBay, or Amazon have now branches located in other countries than the United States; and users' and consumers' NGOs have coordinated their actions, as it is done by the Global Internet Liberties Campaign which has a large membership of NGOs.

⁴ In her model, Milner (1997) considers incomplete information and information asymmetries as synonymous.

Germany and Italy too. The national security interests are embodied by law enforcement and intelligence agencies (all three countries) and defense departments (predominantly in the United States).

The United States is a society-dominated structure, with powerful interest groups, as well as the foremost "national security" state of all three cases. In addition, it is still the "number one" country on the Internet, for network traffic and content produced. Much like transnational alliances, intrasectoral alliances can quickly be established there. Access to government, legislature and bureaucracy is ample. Due to these conditions, however, interest groups' alliances influence policy for brief periods, before new coalitions emerge and the focus of government and groups shift to new issues. Information (particularly on domestic issues) is distributed quite evenly; individuals can thus rely on plenty of independent sources.

Germany is a democratic corporatist model. Actors in the system, whether the federal or local governments, trade unions, industrialists' associations, etc., slowly build consensus on specific policies. The process obviously takes considerable time and, more often than not, the outcomes are compromise solutions. Nevertheless, once consensus is reached on some issues, it endures, and the deriving policies have a high likelihood of being implemented. Information is disseminated among the institutional actors, which tend to exclude individuals—who, however, can easily fall back on several independent sources. Germany has become the "number one" Internet country in Europe.

Finally, Italy despite its unstable governments has had a long tradition of government intervention in the economy—as its record of privatization and liberalization has clearly shown. Policies are the outcome of compromises within coalition governments, and are based on the mutual exchange of political favors ("I'll scratch your back, if you scratch mine", or *do ut des*). However, certain long-term policies (such as intervening in the economy) have not been dependent on the specific government but have been followed by most executives. Only in the last 10 years, and thanks to EU pressures and initiative, has the process of privatization begun, albeit slowly.

Access to government and the legislature is mediated by a full array of middlemen and intermediaries, both within and without the state bureaucracy. Information is obviously filtered by these intermediaries to their own ends. Independent sources abound, but relatively few individuals avail themselves of them. Among Internet countries, in Europe and elsewhere, Italy is a "late-comer" that has quickly recovered many positions.

Thus far, the United States has enjoyed an unmatched supremacy on any aspects related to the functioning, contents, and future developments of the Internet. It is not only that the U.S. invented the Net, that most of the host computers are based there, that most of the traffic goes through it, that half of the American population is on-line, or that it produces most of on-line contents. America's dominance is also manifest in areas such as the domain name system (ICANN operates under Californian laws) and technical innovation.⁵ Even the European advantage in mobile phone technology and diffusion is not as secure as many think (*The Economist*, April 29, 2000:65/66), and when it comes to waging wars through computer networks, the United States' superiority is simply overwhelming.

Globally, the United States is the country that is most reliant on computer networks—which are indispensable to managing all other networks—and, thus, also the most vulnerable.⁶ Logically, the U.S. federal government is concerned about the protection of its information infrastructures and what economic and social consequences a serious disruption of them would entail, and it is raising the budget to protect those infrastructures.

Despite claims from the U.S. national security/defense community, and because of the strong arguments put forward by the business-NGOs alliance, the federal government and the larger public have only partially accepted the thesis that the Internet can pose a threat to national security. This outcome has been achieved mostly thanks to the impressive collection of technical and legal information gathered and displayed by the alliance. Stalemate has thus ensued in the United States. The U.S. intelligence/law enforcement establishment has certainly persuaded other countries' law enforcement officials that cybercrime can seriously hinder electronic commerce and that it should be actively opposed. However, calls by the United States to fight cyberterrorism or to take a restraining stance on the sale and availability of strong encryption software have fallen on deaf ears in several industrial countries.

Hence, the two most remarkable findings in the United States case were the existence of the unusual alliance between the private industry and pro-freedom and consumers' NGOs, and the stalemate that has ensued government's attempts to foster statutory control on the Net. Multiplicity of access points to the federal government, the

⁵ Even Tim Berners-Lee, first inventor of the World Wide Web, had to move to the United States from the CERN in Geneva to continue his research (the W3 Consortium at the M.I.T.).

⁶ Thus far, that threat is summarized as follows: “[t]errorists also are embracing the opportunities offered by recent leaps in information technology. To a greater and greater degree, terrorist groups, including Hizballah, HAMAS, the Abu Nidal organization, and Bin Ladin's al Qa'ida organization are using computerized files, e-mail, and encryption to support their operations.”

(http://www.odci.gov/cia/public_affairs/speeches/dci_speech_032100.html v. October 12, 2000).

legislature, and the availability and exchange of abundant technical information have made actions by pro-freedom and consumers' NGOs and the ICT industry highly effective.

So well-informed and competent have been the arguments presented by these actors that they have been able to match the national security/defense community's claims. Neither side has been able to outpace the other (although the American public seems more inclined toward the NGO groups). This is an unprecedented outcome, since in several other instances, this community has enjoyed superiority in information distribution (i.e. "trust us, we know best") to easily win the day. The debate on Internet control is the first and most substantial exception to that practice.

Realist theory claims that, because of its position in the world, the United States ("high security" case) must be concerned with Internet threats, while Italy and Germany ("low security" cases) can overlook them. Germany and Italy are highly dependent on computer networks—not as much as the United States, but considerably more than several other countries.⁷ Were these countries to ignore cyberthreats that the U.S. seems to be taking seriously, one could only conclude that they would be doing a lousy job of protecting the security of their infrastructures. This scenario, however, does not describe the actual situation.

Cybercrime is, in fact, considered a credible risk by the two European governments, which have acted accordingly, adopting several countermeasures, but only within the scope of normal law enforcement jurisdiction. Fighting cybercrime is crucial to the establishment of the Information Society, and the German, Italian as well as American governments know full well that if individuals perceive the Internet as an extension of "Big Brother", they will never embrace the Net *en masse*. Therefore, all the potential economic returns of the Internet would be lost.

Overall, Italy and Germany are both "late-comers" to the Internet—Italy more so than Germany. Unsurprisingly, both have tried to "catch up" with the United States, possibly overlooking the security faults of the Net. In fact, while the cybercrime issue elicits some interest among German and Italian authorities, concerns for other on-line menaces to national security are definitively not on the agenda for those governments. In addition, they

⁷ In cyberspace, industrialized democracies are somehow more equal than in the real world, i.e. they are all increasingly dependent on computers and computer networks. Their economies could never survive without computer and their networks. Paradoxically, developing and underdeveloped countries are even more penalized in cyberspace than in the real world, because they are not as "computerized" as industrialized countries (thus they are not as vulnerable), but they need to become so, if they want their economies to grow (thus they will become more vulnerable).

have preferred a more relaxed attitude about the Internet and national security, not because they cannot be threatened or blackmailed.⁸ Rather, they have accepted the evidence presented in several instances by the ICT industry, pro-freedom NGOs and users' groups that the Net is an improbable a threat to national security. The scores of the Cryptography Index and the case studies all support this conclusion.

As in the United States, the political structure and distribution of information have played important roles in Germany and Italy too. In Germany, "Net enthusiasm" has stemmed from a joint coalition of government and business in the traditional consensus-oriented fashion. Indeed, the private sector has taken the initiative, asking for government support from the very beginning. The civil society (represented by educational organizations and schools) have also been quickly asked to join the effort. The Red-Green alliance has made it clear that if Germany truly wants to move into the Information Age, it is a "collective mission" that cannot afford to leave behind the many computer illiterate members of the society. As expected, the consensus-building process has taken time, but once accord was reached, all of the German society now seems committed to that goal. The Internet as a threat to national security is the last thing German users, industry, and the federal government would believe. An important variation in this case was the freedom of speech issue, which, for well-known historical/cultural reasons, Germany has been obliged to address by increasing the limits to neo-Nazi language and material.

Italy is the late-comer case. Until 1998/99 (thus quite late in Internet history), managing the Internet was basically left in the hand of mid-level bureaucrats, inexperienced police officers and judges. Enthusiastic ISPs, and users' groups often operated in the ignorance of what the status of legislation on the Net was, and the few, filtered access points to the government and the legislature did not improve the situation. Internet did not belong to high politics or serious business circles. In the last years of the past century, big ICT companies and the government came almost simultaneously to the conclusions that Italy risked failing to construct the Information Society and being excluded from the benefits of the New Economy. Despite a consolidated image of "weak government", Italy's executives have endorsed several steps to spread the use of the Internet, particularly among students and pupils—although the current situation is still far from satisfactory. Italian political parties, after long-standing disinterest, have all embraced the Internet, much like their

⁸ In terms of organized, mafia-style crime moving to the Net, for instance, Italy could be as concerned as the United States.

counterparts in Germany and the United States. However, viewpoints of what the necessary steps to spread the Net in Italy frequently diverge.

Italy's late arrival to the Internet, a significant distinction between Italy and Germany cases, means so a proper legal framework for the diffusion of the Net is still being developed there. Given states' tendency towards skeptical conservatism vis-à-vis new institutional structures, one might have expected more "activism" by the Italian law enforcement and defense personnel in controlling the Net. Undoubtedly, this outcome would have been coherent with a realist interpretation of the issue. Yet, this condition failed to materialize. There have been instances of abuses by law enforcement officials, and of incompetence by some judges, but these have been few, certainly not more than anyone would normally anticipate in such a state of affairs. Despite different conditions, Italy has thus acted more like Germany and, as the indicator for my dependent variable has showed, the Italian government has retained a low level of control on the Internet.

7.2.1 Democracies and Autocracies

Some authors (Kehoane and Nye, 1998) have argued that democracies fare better in the Information Society than non-democracies because the former can "take more information" without their social fabric being disrupted. Although the results of the quantitative analysis were not clear-cut in this respect, the democracy-level hypothesis has contributed considerably to explaining why governments control the Net. Overall, the political configuration of governments (i.e. whether or not they are democratic) does make a difference.

The case studies confirmed that democratic countries have their own problems in determining how much statutory control should be put on the Internet and what should be controlled. In some instances, democratic governments, mirroring conflicting requests from the public opinion, have been keen to reinforce the monitoring of the Net in order to increase their effectiveness on what takes place on-line.⁹

Examining the scores on the Cryptography Index, it becomes clear how democracies do have a consistently less restrictive attitude on encryption, and thus a lower level of control. It can be argued that, since encryption software is crucial for e-business, many

⁹ The most recent report "The Enemies of the Internet" on 59 countries by *Reporters Sans Frontiers*, in fact, also identifies all the major Western democracies (Australia, France, Germany, Italy, Japan, the United Kingdom and the United States) as "enemies", albeit in a milder form than e.g. China or Saudi Arabia (the list is at <http://www.00h00.com/direct.cfm?titre=4802011802> and also <http://www.rsf.fr/uk/home.html> v. May 5, 2001).

democracies, as industrialized countries, have a light hand on cryptography. Commercial interests, however, do not always coincide with those of the law enforcement and intelligence communities, which hold influential views on this topic with heads of governments. In addition, users' groups and pro-freedom NGOs also disagree with the image of the Internet—riddled with cybercriminals and terrorists—presented by the national security communities.

The confrontation has become polarized, with the private sector siding with NGOs. When such conditions occurred in the past, national leaders (in democracies too) have been inclined to favor the national security/defense party. However, availability of government access, accessibility of independent information sources, and the presence of highly organized interest groups have all contributed to making democracies more open to individuals' actions. In the case of the Internet, the national security/defense communities have not had their way, and the result has been a stalemate (like in the United States) or failing to notice that faction's argument (as in Italy and Germany). The problem of control in democracies is never settled once and for all. It is an on-going process where governments try to meet the demands of law enforcement officials, business people, and civil liberties activists, most of the time producing unsatisfactory compromises. That has always been the very nature of true democracies.

Autocratic governments face the same dilemmas, albeit in simpler forms. They enjoy centralized state structures which allow fewer access points to political leaders (Risse-Kappen, 1995b). Furthermore, the number of "arguing actors" is also much smaller. As China and Singapore have amply demonstrated, autocracies too, want to spread out the Internet and build their own version of the Information Society and collect the benefits of the New Economy. However, those governments wonder, how many people then should be allowed to have access? Should they be only the politically reliable ones? How much, and what kind of information would companies really need? The list could go on considerably.

For the time being, autocracies can centralize Internet control, restrain users, and resist pressure from interests groups. There is no guarantee that once the percentage of users has achieved the size of the Internet public in industrialized democracies, the same efficiency and intensity of control can be maintained. Such circumstances will make for an interesting test for the theses presented in this work.

7.2.2 The False Promise of the Internet Threat to National Security

An uncontrolled Internet could be the medium through which attacks to national information infrastructures are launched, or substantially boost the efficiency and reach of organized crime. Both instances constitute threats to the security of states: therefore, states are obliged to control the Internet. This, in brief, is the explanation offered by a realist theory of why governments want to control the Internet. Until now, whenever economic exigencies have clashed against the requirements of national security, the latter have usually prevailed. This outcome occurred throughout the whole period of the Cold War, when the world economy was "militarized".¹⁰

Since the designation of what constitutes "national security" is an act exclusively reserved to national governments, a state's political leaders may include in that concept whatever occurrence they see fit. For instance, the "first democracy", i.e. the United States, has considered a new piece of legislation that, if passed, would make computer attacks against the DOD a national security violation instead of just a criminal action.¹¹

Given this complex economic, cultural and security framework that the Internet is creating in many societies, it is not surprising that some national governments are tempted, at different moments, to use the label "national security". At the time of writing, the Internet as a perceived threat to national security, however, is mostly an excuse to justify statutory control on issues that have little or nothing to do with the survival of a country. National security is, first and foremost, still a job for military personnel. Few countries, as the quantitative analysis and the case-studies demonstrated, have yet bothered to set up information warfare plans or have increased their military spending to cope with this new threat.

By increasing the reliance of their economies and societies on computer networks, countries also increase their vulnerability to malicious computer attacks. Many governments seem oblivious to such conditions. At least for the time being, they prefer to believe that probable economic returns outweigh the risks of that vulnerability. National security remains a handy, *ad hoc* tag that national governments may use to preserve their unconstrained freedom of action on whichever issue, whether on- or off-line, they deem necessary.

¹⁰ Such approach viewed international trade with the Soviet bloc as a zero-sum game. It is significant that in the 1990s, the United States changed its policy to constructively engage China as a trade partner, to the point of strongly supporting China's application to the WTO.

¹¹ <http://europe.cnn.com/2000/TECH/computing/08/01/pentagon.at.defcon.idg/index.html> (v. October 10, 2000).

7.2.3 Any International Regimes, Anytime Soon?

The starting point of this research was the indication that it would have been impossible for all, or the majority, of on-line countries to decide on an international agreement designating what behaviors should be labeled criminal and which are legitimate. Although international frameworks for such a treaty were available—the United Nations or the ITU for instance (Ferguson, 1998)—the main obstacles here were for governments to decide whose standards and whose legislation to adopt. Identifying criminal categories is so tightly associated with a country's society, culture, and tradition that even among countries with fairly similar features such as Western, industrialized democracies,¹² it would be very hard for governments to strike common ground.

Within this group, there are considerable differences on the treatment of personal data—in Europe it is more strictly regulated—or in defining free speech, which traditionally, the United States identifies more broadly than Europe does. Other important dissimilarities have emerged in the group on taxation—the United States would prefer little or no taxes on the Net—or, more generally, on “self-governance”. This latter instance means for the Americans that businesses should be left to regulate themselves, while the market should set prices and priorities for the Internet's use.¹³ The Europeans have a more consensual approach, and, to some extent, would like to see their governments more active in managing the Net. Divergences of opinions also are present among the Europeans themselves and should not be underestimated.

The circumstances above described apply entirely to international treaties, signed by national governments, sometimes within the framework of international government organizations. In addition to cultural, legal, and political differences, another important reason to explain why governments have not yet finalized international agreements on the Internet is that, during negotiations for treaties about the Net, states have excluded users' groups and NGOs. These organizations have been able secure support by a large number of individual users as well as, on certain issues relating to governments' presence on the Net, the backing of the private industry, making their resistance to states' international initiatives

¹² This group can be roughly identified with the OECD countries. However, even a more “exclusive” club, the G7/G8 has discussed fighting cybercrime since 1995 without much more efficiency (for a list of events see <http://www.privacyinternational.org/issues/cybercrime/> v. October 11, 2000). Finally, even if all the EU members have their common ground in the Maastricht Treaty's Third Pillar (justice and home affairs), considerable differences among their criminal codes persist.

¹³ Americans are also well aware of the importance of universal access and providing connectivity to as many countries as possible.

more effective.¹⁴ The key factor to achieving such positive results has been the ability of pro-freedom NGOs to provide a highly knowledgeable technical presence, convincing many users and several private companies of the validity of their requests.

At the moment of writing, the nearest occurrence resembling an international agreement on governing the Internet that exists is the draft of Council of Europe Convention of Cybercrime, which should be approved in August 2001 by member countries of the Council. Given the relevance of the topic, Canada, Japan, South Africa, and the United States are also actively participating in the negotiations—in fact, the FBI has considerably contributed to the drafting.¹⁵ It is impossible to forecast whether such a convention will be successful: for now, it is being actively opposed by many pro-freedom NGOs.¹⁶

Any comprehensive international regime for the Internet would have to take into account the views of many more countries with quite distinct religious, cultural and historical values. Such circumstances considerably hinder reaching a multilateral agreement on how to control the Net.¹⁷ Most of all, such an international regime should ideally enjoy the support of users' and Internet and civil liberties NGOs. For the time being, the possibility of an international treaty that would reassure all the various countries with Internet access has been, at least temporarily, taken off the states' international agenda. National governments have been left with little alternative but to adopt a national approach to controlling the Net. In other words, they had to accept a "digital challenge"—accepting the Net with all its pros and cons—on their territory, and this decision will present them with some hard-to-make choices.

Actually, the Internet (and ICT) have emerged as the most promising sources for the greatest technological revolution since the invention of electricity or the steam engine (Woodall, September 23, 2000). The New Economy is just an early spin-off of this

¹⁴ Obviously, non-democracies do not operate under the same constraints. However, the dominant position of OECD countries (all, more or less, democracies) would make impossible to sign any treaty about the Internet.

¹⁵ <http://conventions.coe.int/treaty/en/projects/cyber.htm> (v. October 18, 2000). The "regional" (i.e. within Europe) or, at the most the "transatlantic" (between the U.S. and Europe/EU) dimensions are the most likely to succeed in reaching an agreement on limited issues (such as child pornography for instance) for an international regime.

¹⁶ See for instance, the December 2000 letter by the Global Internet Liberties Campaign (GILC) to the Council of Europe Secretary General, explaining the risks of such convention (<http://www.gilc.org/privacy/coe-letter-1200.html>).

¹⁷ The bulk of Internet traffic as well as Web sites and host computers are in OECD countries which, might well decide to implement an "OECD regime"—at least for the time being. This action, however, would simply enrage non-OECD countries, which would feel even more excluded from cyberspace and would probably start calling OECD members "on-line imperialists".

revolution in its infancy, which many hope may give way to an economic growth of unprecedented scale with tremendous human and social benefits. Clearly, no government wants to be left out from such bonanza. Nonetheless, as all the technological innovations before them, the Net and ITC will also produce intense structural changes in many societies, particularly in the long term.

Not all these changes (or others that are impossible to forecast now) will be welcomed by all the governments. China is a textbook example: the Chinese government is promoting the diffusion of the Internet, while trying to suppress undesired material such as, the Web sites of some newspapers and magazines.¹⁸ These circumstances were exposed in chapter three by the negative correlation between liberalization in the telecom sectors and the requirements of national security in the quantitative analysis.

The overall outcome of this state of affairs is that national governments are torn between expected benefits and drawbacks, the “negative” and “positive” sides of the Internet. In most cases they simply react to the stimuli, trying to please public opinion, law enforcement and business communities, with their often competing and sometimes irreconcilable agendas. All in all reverting to the “national security” justification will appeal to many states as the ultimate and, perhaps the only way out of that digital challenge.

7.3 Internet-ional Relations?

Do these findings have a long-term impact on the field of International Relations? First and foremost, the Net has joined the many other factors (finance and trade, tourism, telecommunications, etc.) that have contributed to making the world a smaller place. The Internet alone would not bring about the ultimate demise of the nation-state. But, just like any other organizational structure, as the Net expands, it is certain to affect more and more than the organization called “the state”. If necessary (and provided that adequate technical and financial resources are available), states can still profoundly influence the future developments of the Net. Some states could do more than others, but this is hardly a new

¹⁸ This method can be successful as long as there are relatively few users. If half of China’s population were on-line (as is the case in the United States), that method would not work. Consulting for a French court on the Yahoo! case (where the American company was ordered by the court to ban French customers from buying Nazi memorabilia), Vint Cerf, one of the top experts on the Internet, argued that only control performed by human beings in addition to software filtering could guarantee the full effectiveness of the court’s order (*The Economist*, November 25, 2000:102). China can easily afford the “human control” on its (still) small number of users.

feature in world politics. For the moment, as the nation-state has adapted to other challenges, it seems it may also learn to adapt to the Internet.

The Internet has contributed to reducing statutory control of governments on how their citizens have access to information and what information they exchange. Consequently, national governments have seen their freedom of action diminished, both domestically and internationally. Internationally, NGOs working on human rights or environmental issues have found an excellent tool in the Internet to keep contact and organize actions such as the boycott of the Multilateral Agreement on Investments or the WTO Seattle meeting of December 1999. Old style, inter-state diplomacy has thus become harder to accomplish without being under real-time monitoring by NGOs with Internet access.

The presence of one hegemonic state, the sole information superpower, does not facilitate cooperation on the Internet—as claimed for instance by neorealist theory. This is a “capacity gap” quite worthy of note: the supremacy and power of pressure that the United States enjoys on the Net are undisputed. Yet, the U.S. cannot translate all its predominance into having its own way with the other relevant actors of cyberspace, i.e. Europe and Japan—as in the case of the still unresolved EU-U.S. dispute on the treatment of personal data.

The choice of governments to make use of the “national security” label with regards to some aspects of the Net indicates an attempt on their side to secure some exclusive authority on at least certain areas of computer networks. This effort may be applied to such different issues as protecting the information infrastructure, or censoring free press on-line, but it does confirm the states’ effort to maintain some control on the Net as well as some unhampered freedom of action. With specific reference to military security and information warfare, governments have retained the last word. However, once more, the nature of the Internet makes the situation distinctive: unlike conventional or mass destruction weapons, which are firmly in the hands of states, some skilled individuals may wreck states’ information infrastructures.¹⁹ Never before in the history of states, have those in charge of

¹⁹ There would be relatively few victims, however. This outcome may help explain why international terrorists—who are also in the process of understanding this new technology—have been reluctant users of the Net so far.

defending the well-being of the state itself been so alarmed by the actions of a relatively few persons.²⁰

Despite these worries, thus far, governments have shown that, with regards to the growth of Internet, economic gains are more important than national security. National governments are conscious that, at least for the time being, those *expected* economic gains from the diffusion of the Internet are more likely to occur than the foreign or criminal threats that may come through the Net. In this respect, national governments are concentrated more on maximizing the gains than reducing the risks, as demanded by their national constituencies, and are still rather oblivious to what other actors do in the international arena.

Such an interpretation of changes in world politics after the Internet are consistent with a liberal-domestic approach to international relations theory. However, the partition between domestic and international levels of explanation will have to be progressively abandoned by scholars in researching the effects of the Internet on world politics, since these realms will merge more and more in cyberspace. In the end, a considerable part of governments' activities will become "digital". The organizational structure of "the state" will change, and countries will have to learn how to defend "their" cyberspace. This change may well result in a major watershed for a discipline, international relations, that has based its fortunes on the identification of its main subject, those states with territorial sovereignty.

7.4 A Slightly Normative Ending (Or, What the Internet Can And Cannot Do)

In August 2000, *The Economist* assessed the early period of the "Internet's coming of age". The Internet's days as a predominantly scholarly research network was over, and the Net seemed to be omnipresent in people's lives, finances and entertainment. *The Economist* entitled its review "What the Internet cannot do" (August 19, 2000:9/10). As with all new technologies, a wave of enthusiasm and hope has greeted the Internet. Many optimistic prophets have foreseen the Net prevent wars, reduce pollution, and fight inequality.²¹ Some authors have also identify the Internet as the end of the nation-state

²⁰ The actual threat posed by those users is not relevant here. What matters is that state officials responsible for defense have never been so concerned by individuals unaffiliated with any governments or political organizations, and this situation is entirely new for states.

²¹ See, for instance, Negroponte (1995) Naisbitt (1995), Cairncross (1997), and Burton (1997). Shapiro (1999) belongs to a more moderate group, which nonetheless foresees major changes in the world as we know it.

system (Naisbitt, 1994 and Burton, 1997), and the beginning of a new brave "wired world" (Burton, 1997).²²

The Internet has indeed changed businesses' operations and organizations, empowered grass-root groups, and facilitated people's communications. Its effects on economies and societies will be even more profound in the long run. Unfortunately, the Net cannot "eradicate all the world's problems".

As new gizmos come and go, human nature seems to remain stubbornly unchanged: despite the claims of the techno-prophets, humanity cannot simply invent away its failings. The Internet is not the first technology to have been hailed as a panacea—and it will certainly not be the last (*The Economist*, August 19, 2000:10).

The Internet, as any other technology, is fundamentally neutral.²³ It can be used to improve peoples' lives, through spreading education and telemedicine, or to ruin them, through serving gamblers, pornographers, and drug dealers. It can boost economic growth and productivity, but also threaten national security. Thus, where do all these conflicting circumstances leave national governments when coping with the Net?

If technology is neutral, decisions regarding technology are entirely political. And the principal decision-makers in this arena are still national governments. As Daniel Yergin has put it, "[g]overnments will continue to tax, regulate and pursue much of their current social agenda.... This trend is not the end of government; it is just a redefinition".²⁴ This situation implies that extrapolating from the past attitudes of states on the Internet may help clarify the future of the Internet, and, conversely, what new digital challenges national governments will, in turn, have to face.

With regards to the future of the Net, control is the most powerful tool in the hands of national governments. Luckily, not all the governments think and act in the same way. The goal of this research was to take a "global" view, allowing for generalizations. Thus, I have treated governments monitoring the Net to eliminate child pornography, neo-Nazi material, or computer frauds in the same way as states that want to prevent the publication of a report on human rights abuse or spy on their citizens' lives. Clearly, though

²² On the other hand, Waltz (2000) has refused to see any changes in the international system—the Internet or anything else. Also the neo-institutionalist Nye and Keohane (1998) seem to imply that there is an information revolution and "soft power" is more and more relevant, but, after all, states are still the most important players in the international arena and these changes should not be overstated.

²³ Rosenau, J., *The Information Revolution: Both Powerful and Neutral*, paper presented at the 42nd Annual Convention of the International Studies Association (ISA), Chicago, IL, February 22, 2001.

²⁴ http://www.ml.com/woml/forum/yerg_int3.htm (v. October 10, 2000).

governments are useful units of analysis in political science, there are considerable differences among them.

Complexity and intricacies abound in working with the Internet. The same civil liberties organizations that demand “hands-off” policies regarding free speech on the Net call for governmental regulation when on-line privacy is threatened by the industry’s own hands-off, self-governance policy. The fact is that political leaders, lawmakers, scholars and users will keep facing thorny issues about the Internet: there will never be a fully harmless, positive, law-abiding Net, nor an entirely negative, criminal one. Although it is problematic to assess the validity of the statement that democracies can “take more information”, it is appropriate to expect democratic countries to behave correctly when dealing with the Internet.

These states have indeed a “moral imperative” to defend users’ privacy, freedom of speech, and free choice. If democratic governments impose too many limits on the Net, non-democracies will see themselves even more justified in enforcing their own national standards of control.²⁵ Clearly, free speech cannot be completely unrestricted or that personal privacy can be breached to collect criminal evidence. These actions, however, should be encompassed in a few clear, unambiguous, and specific legal guidelines, and governments should enforce them without exceptions.

Unfortunately, given the domestic-international, public-individual nature of the Internet, governments’ recourse to the all-encompassing notion of “national security” will not go away. The Internet, the argument goes, has made national computer networks more vulnerable, and thus has put national security at risk. The prohibition of the U.S. federal government to export encryption software—claiming that it was a breach of U.S. national security—has been an example of those improper limits and an escalation in the level of Internet control by that government. The evaluation of malicious attacks on national information infrastructures should also become more sober, and based on a more convincing substantiation of actual damage than it is now.

While some of the Internet’s features, such as freedom of speech, mostly require passive protection (“do not increase censorship”), other attributes such as individual privacy demand positive, active engagement by democratic governments (more guarantees). In fact, government agencies have not been alone in collecting information on users: private

²⁵ For instance, it would be all too easy for the Chinese or Saudi Arabian governments to point out that not even human rights champions like Western democracies can take unrestricted free speech or comprehensively protect personal privacy.

Internet companies have been even more active and even less accountable.²⁶ In this situation, more involvement by democratic governments seems inevitable. These governments should restrain both public and private actors that aim to gather information on individuals unchecked, and set forth the precise cases in which collecting information is allowed

To fulfill that mission, democratic governments may begin by agreeing on the definition of issues such as "privacy" or "computer crime". If the private sector and the users' and consumers' organization are actively involved in the process of creating an international regime, chances for success will be higher. Another easy step in this direction would be to sign a treaty between the U.S. and Europe on banning child pornography on their territories.²⁷ They have similar views on protecting children, and thus some common ground could be found. Once this goal is achieved, it would be possible to move step by step to reduce on-line crime. The guiding principle of these agreements, however, should be to regulate as little as possible, protecting individuals' rights (more than companies) and set out clearly the criteria followed to determine this level of Internet control.

7.5 Finally, Where Do We Go from Here?

This has been the first comprehensive study analyzing national governments' behavior on the Internet from a comparative perspective. Currently more studies on the Internet are being published. But what are the critical areas to be explored to better understand the Internet's socio-economic impacts? Here I want to highlight some of the possible directions of further research in this field.

First of all, there is the fundamental problem with the quality of data available on the Internet. It is not that there are too few data: there are too many. Some of those data, however, are of dubious quality, while others can be only partially useful to scholars. For instance, my Cryptography Index as an indicator of my dependent variable, i.e. the level of "Internet control", has only partially captured the real situation, since control exercised through hidden barriers to access was excluded. Moreover, I have cited as few figures as possible about numbers of users, Web pages, traffic, etc. because their reliability has been,

²⁶ At least (and with many exceptions), in democracies, intelligence and law enforcement services respond to political leaders that are accountable to parliaments.

²⁷ The EU itself is considering a number of "regional" (i.e. intra-EU) agreements such as on e-commerce or illegal and harmful contents on the Net, or intellectual property rights.

thus far, unquestioned. More research is then needed in comparing the different sources, methods and elaboration techniques of data on the size and attributes of the Internet. By assessing quality and presenting findings to the academic community and the general public, Internet scholars can make sure that the scope and explanatory power of future research on the topic will increase considerably.

Second, as more countries go on-line, and more governments have to face the typical Internet dilemmas, it will be interesting to better assess the variations between democracies and non-democracies. Currently, this differentiation is arduous to make since, as I have explained, the Internet is still mostly a venture of the "OECD club" of industrialized countries. If the statement that democracies do display more distinct behavior than non-democracies with regards to on-line privacy or freedom of speech holds true, it is nonetheless still unclear how far democratic governments are willing to go to protect those rights. Estimating their attitudes in these respects would also provide interesting findings about how solid the social fabrics of many democratic societies are.

Third, the Internet will force extensive reorganizations of governments' structures and functions. This restructuring will affect the size, and therefore spending of national executives, which will be able to offer faster and cheaper administrative services to their public—and these are the main anticipations for e-government. More important, it will also have effects on jurisdictions and competencies of the states' various departments and agencies. Some national governments have already begun "outsourcing" some of their traditional tasks of protecting and modernizing information infrastructures to the private industry. The militaries, at the same time, rely more and more on commercial computer networks for at least some of their communication traffic.

The three case studies have also revealed another key feature of this in-flux situation: the blurring of jurisdictions within the same governments. Most governments have fairly precise, and jealously defended, institutional boundaries among their branches. Moreover, there are still (albeit not always clear-cut) divisions between competencies in domestic or foreign matters. Economics, culture, and public security are all blended together on the Internet. Several government bodies have been obliged to increase cooperation, thus creating departmental jealousies, and impediments to executing tasks more accurately. The problem is more severe for many democracies, which usually have institutional limits and constitutions that are harder to bend or modify—for instance, in the separation between civil and military spheres.

States will have to learn how to cope with overlapping administrative responsibilities, not only domestically but also internationally, since their national laws on the Internet may have an impact on other states as well. The cases of ICANN functioning on American laws and the EU Directive on personal data affecting American businesses are just two such instances.

To conclude, the Internet and information warfare (IW) will necessitate more research clarity in the appliance of “national” security, as well as more focused investigation in the subject area of security studies. In the former occurrence, scholars should explore in more depth the conditions under which governments fall back on the concept of national security. Furthermore, persistence by governments in applying that concept—ultimate manifestation of the nation-state—would unavoidably have repercussions on the international network of computers, and vice versa.

The Internet and IW have already transformed the area of security studies, and information warfare studies are definitively gaining momentum. However, most of the studies thus far have failed to produce convincing evidence that IW is an effective method to wage war. Furthermore, most of the funds allocated—almost exclusively in the United States—to study the subject have been spent to support the demand of more funds, without properly assessing possible foes and threats.

When I first met the Net, it was the primarily secret passion of a restricted community of dedicated users. I thought that it would be fascinating to witness how the Internet, slowly, would change my field of study, and I thought that I should contribute to that change. It all happened very quickly then, and the Net is now a common word—albeit not a well understood concept—for the general public. This study has been one of the early attempts to make sense of this unforeseen and unexpected phenomenon.

Quite encouragingly, what the rock band U2 praised in their 1993 song “Stay”—that we can now go *anywhere*—has ultimately become true.²⁸ Only it has not been thanks to Satellite Television, the object of their praise. It has been thanks to the Internet.

²⁸ “.../With Satellite Television/You Can Go Anywhere”, from *Stay (So Far, So Close!)*, music and words by the U2, Island Records, 1993.



GENERAL BIBLIOGRAPHY

1. Abelson, H. and et al. (1998). *The Risks of Key Recovery, Key Escrow, Trusted Third Party and Encryption*. Digital Issues n.3 ed. Washington, DC: Centre for Democracy and Technology (CDT).
2. Achen, C. (1982). *Interpreting and Using Regression*. Beverly Hills, London, New Delhi: SAGE Publications.
3. Agnew, J. and S. Corbrige . (1995). *Mastering Space. Hegemony, Territory, and International Political Economy*. London: Routledge .
4. Alberganti, M. (21 Jan 1999). "La France Renonce à Controler Les Communications Sur Internet." *Le Monde Interactif* (Paris).
Notes: <http://www.lemonde.fr/nvtechno/branche/crypto/control.html>
5. Alberts, David S. (1996). *Defensive Information Warfare*. Washington DC: National Defense University.
6. Alvi, G. and et al. (2000). "Dossier: L'Epica Della Net-Economia." *Surplus* 2(6):31-54.
7. Anderson, C. (1995). *The Accidental Superhighway. A Survey of the Internet*. London: The Economist.
8. ———. (1997). *In Search of the Perfect Market: A Survey of Electronic Commerce*. London: The Economist.
9. Anderson, M. (1996). *Frontiers: Territory and State Formation in the Modern World*. Cambridge, UK: Polity Press.
10. Arquilla, J. and et al. (1999). "Networks, Netwar and Information Age Terrorism." *Countering the New Terrorism*. MR-989-AF. Santa Monica, CA: RAND Corp.
Notes: <http://www.rand.org/publications/MR/MR989/MR989.pdf>
11. Asher H. (1976). *Causal Modelling*. Beverly Hills, London UK: Sage Publications.
12. Babbie, E. and F. Halley. (1995). *Adventures in Social Research: Data Analysis Using SPSS for Windows*. Thousand Oaks, CA, London, New Delhi: Pine Forge Press.
13. Baldas, B. (29 Jul 2000-30 Jul 2000). "Indische Revolution in Deutschland." *Die Tageszeitung* (Berlin), Tazmag, p. I/II.
14. Baldwin, D., ed. (1993). *Neorealism and Neoliberalism: The Contemporary Debate*. New York: Columbia University Press.
15. Bamford, J. (1983). *The Puzzle Palace. America's National Security Agency and Its Special Relationship With Britain's GCHQ*. London: Sidgwick and Jakson.

16. Barth, R. and C. Smith. (1997). "International Regulation of Encryption: Technology Will Drive Policy." Pp. 283-99 in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, eds. B. Kahin and C. Nesson . Cambridge, MA and London, England: the MIT Press.
17. Bennett, C. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca and London: Cornell University Press.
18. Berners-Lee, T. (1999). *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. New York: Harper San Francisco.
19. Bishop, M. (2000). *The Mystery of the Vanishing Taxpayer: A Survey of Globalisation and Tax*. London: The Economist.
20. Black, J. and D. Champion. (1976). *Methods and Issues in Social Research*. New York et al.: John Wiley & Sons, Inc.
21. Blalock, H. (1960). *Social Statistics*. New York: McGraw-Hill Inc.
22. Blalock H. (1964). *Causal Inferences in Nonexperimental Research*. Chapel Hill , NC.: University of North Carolina.
23. Borhnstedt, G. and D. Knoke. (1982). *Statistics for Social Data Analysis*. Ithaca IL: F.E. Peacock Publishers, Inc.
24. Bowles, Nigel. (1993). *The Government and Politics of the United States*. London: McMillian.
25. Burton, D. (1997). "The Brave New Wired World." *Foreign Policy*(106):23-37.
26. Cairncross F. (1997). *The Death of Distance*. Boston, MA: Harvard Business School.
27. Camilleri, J. and J. Falk. (1992). *The End of Sovereignty? The Politics of a Shrinking and Fragmenting World*. Hants, England: Edward Elgar Publishing.
28. Campbell D. (1999). *Interception Capabilities 2000*. Bruxelles and Strasboug: Scientific and Technological Options Assessment Panel of the European Parliament (STOA).
Notes: http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm
29. Caprara, C. and L. Picci. (2001). "Internet Al Governo." *Geografia Della Comunicazione*, ed P. Bonora. Bologna: Baskerville.
30. Caravita, G. (23 Jun 2000). "Italia a Due Anni Dal "Cyberboom"." *Il Sole 24 Ore* (Milan), New Economy Supplement, p. I.
31. Castells, M. (1997). *The Power of Identity: The Information Age: Economy, Society and Culture* . Malden, MA and Oxford, UK: Blackwell Publishers.
32. Cavazos, E. and G. Morin. (1995). *Cyberspace and the Law: Your Rights and Duties in the On-Line World*. Cambridge, MA and London: The MIT Press.

33. Chamorel, P. (1994). "The Integration of the U.S. Political System in Comparative Perspective." Pp. 49-86 in *The New American Political (Dis) Order*, (ed) R. Dahl. Berkeley, CA: Institute of Governmental Studies Press (UCB).
34. Chapman, G. (1998). "National Security and the Internet." *Internet Society Annual Meeting* (Geneva, Switzerland).
Notes: mimeo
35. Ciccarelli, S. and A. Monti. (1997). *Spaghetti Hacker*. Milano: Edizioni Apogeo.
36. Cioffi-Revilla, C. and et al. (1987). *Communication and Interactions In Global Politics*. Urbana, IL: University of Illinois Press.
37. Committee for Information, Computer, and Communications Policy. (1997). *Measuring Electronic Commerce*. Paris: OECD.
38. Corasaniti, G. (1998). "La Tutela Penale Dei Sistemi Informatici e Telematici." *Informatica e Riservatezza*, eds. Parodi C. et al. Pisa: University of Pisa/Cnuce/IEI-CNR.
39. Cox, A. (1981). *Freedom of Expression*. Cambridge, MA and London, England: Harvard University Press.
40. Crawford, D. (1997). "Internet Services: A Market for Bandwidth or Communications?" Pp. 379-400 in *Internet Economics*, editors L. a. McKnight and J. Bailey. Cambridge, MA: The MIT Press.
41. Dahl, R. (1994). "The New American Political (Dis)Order." Pp. 1-24 in *The New American Political (Dis)Order*, (ed) R. Dahl. Berkeley, CA: Institute of Governmental Studies Press (UCB).
42. de Bortoli, F. (2000, February 27). ""Si, Puo' Ripetersi Il Miracolo Degli Anni '50"." *Il Corriere Della Sera* (Milan), In Primo Piano, p. 3.
43. de Sola Pool, I. (1983). *Technologies of Freedom*. Cambridge, MA: Harvard University Press.
44. ———. (1990). *Technologies Without Boundaries: On Telecommunications in a Global Age*. ed. E. Noam. Cambridge, MA and London: Harvard University Press.
45. December, J. (1996). "Units of Analysis for Internet Communication." *Journal Of Communication* 46:14-38.
46. Delacourt, J. (1997). "The International Impact of Internet Regulation." *Harvard International Law Journal* 38(1):207-35.
47. Denning D. (1997). "The Future of Cryptography ." Pp. ??? in *The Governance of Cyberspace: Politics, Technology and Global Restructuring*, editor B. Loader. London & New York: Routledge.
48. Deutsch, K. (1966). *The Nerves of Government: Models of Political Communication*

and Control. New York: Free Press.

49. ———. (1968). "The Impact of Communications Upon the Theory of International Relations ." Pp. 74-92 in *Theory of International Relations*, Abdul A. S. Englewood Cliffs, NJ: Prentice-Hall .
50. ———. (1980). *Politics and Government. How People Decide Their Fate*. Third ed. Boston, etc.: Houghton Mifflin Company.
51. ———. (1988). *The Analysis of International Relations*. Englewood Cliffs: Prentice Hall.
52. Di Nicola A. (20 May 1999). "Il Grande Difetto Di Internet 2: Superveloce Ma Meno Libera." *Computer, Internet e Altro* (Rome) [Weekly Supplement of *La Repubblica*], p. 10.
53. Dickinson Gibbons, J. (1993). *Nonparametric Measures of Association*. Newbury Park, London, New Delhi: Sage Publications.
54. Diffie, W. and S. Landau. (1998). *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge MA., and London: The MIT Press.
55. DPA. (8 Aug 2000). "Rechte Fliegen Aus Dem Internet." *Die Tageszeitung* (Berlin), Taz Berlin, p. 19.
56. Economist (The). (19 Oct 1996a). "The Economics of the Internet. Too Cheap to Meter?" *The Economist* (London), pp. 21-24.
57. ———. (19 Oct 1996b). "Too Cheap To Meter?" *The Economist*, pp. 21-24.
58. ———. (19 Oct 1996c). "Why the Net Should Grow Up." *The Economist* (London), pp. 15-16.
59. ———. (5 Apr 1997a). "Waiting for the Call." *The Economist* (London), p. 88.
60. ———. (5 Jul 1997b). "Hands Off the Internet." *The Economist* (London), p. 13.
61. ———. (7 Mar 1998). "Privacy on the Internet." *The Economist* (London), pp. 18-19.
62. ———. (9 Jan 1999a). "Data Dogfights." *The Economist*, pp. 15-16.
63. ———. (20 Feb 1999b). "Hackers Rule." *The Economist*, pp. 73-74.
64. ———. (1 May 1999c). "The Surveillance Society." *The Economist* (London), pp. 19-23.
65. ———. (7 Aug 1999d). "The Gavel and the Robe." *The Economist* (London), pp. 27-28.
66. ———. (23 Oct 1999e). "Walking on Air." *The Economist* (London), p. 20.
67. ———. (6 Nov 1999f). "Riding the Storm." *The Economist* (London), pp. 77-78.

68. ———. (11 Mar 2000a). "I-Modest Success." *The Economist* (London), p. 85.
69. ———. (1 Apr 2000b). "Europe in Cyberspace." *The Economist* (London), p. ????
70. ———. (15 Apr 2000c). "The World Beyond Deutsche Telekom." *The Economist* (London), pp. 67-68.
71. ———. (29 Apr 2000d). "America Rides the Wireless Wave." *The Economist* (London), pp. 65-66.
72. ———. (1 May 2000e). "The End of Privacy." *The Economist* (London), pp. 13-14.
73. ———. (10 Jun 2000f). "Regulating the Internet." *The Economist* (London), pp. 18-19 and 99/101.
74. ———. (24 Jun 2000g). "Phoney Democracies." *The Economist* (London), pp. 17-18.
75. ———. (15 Jul 2000h). "Vodafone's Folly." *The Economist* (London, UK), pp. 16-17.
76. ———. (5 Aug 2000i). "Fighting Racism." *The Economist* (London), p. 32.
77. ———. (12 Aug 2000j). "Don't Email Sid." *The Economist* (London), p. 73.
78. ———. (12 Aug 2000). "Germany's Neo-Nazi." *The Economist* (London), pp. 16-17.
79. ———. (19 Aug 2000a). "What The Internet Cannot Do." *The Economist* (London), pp. 9-10.
80. ———. (16 Sep 2000b). "A New Left Leader?" *The Economist* (London), pp. 34-39.
81. ———. (14 Oct 2000c). "Enel's Not-So-New Look." *The Economist* (London), p. 85.
82. ———. (14 Oct 2000d). "Right Stuff." *The Economist* (London), p. 41.
83. ———. (21 Oct 2000e). "Francesco Rutelli, Italy's Would-Be Prime Minister." *The Economist* (London), p. 44.
84. ———. (11 Nov 2000f). "The Internet's Chastened Child." *The Economist* (London), p. 104.
85. ———. (25 Nov 2000g). "Vive La Liberte!" *The Economist* (London), pp. 101-2.
86. ———. (13 Jan 2001). "Stop Signs on the Web." *The Economist* (London), pp. 19-23.
87. Electronic Privacy Information Center (EPIC). (1998). *Critical Infrastructure Protection and the Endangerment of Civil Liberties. An Assessment of the President's Commission on Critical Infrastructure Protection (PCCIP)*. Washington, DC: Electronic Privacy Information Center.
88. ———. (1999a). *Cryptography and Liberty 1999: An International Survey of Encryption Policy*. Washington, DC: EPIC.
Notes: <http://www.epic.org/bookstore/crypto99%26/default.html>

89. Electronic Privacy Information Center (EPIC). (1999b). *Privacy and Human Rights: an International Survey of Privacy Laws and Developments*. Washington, DC: EPIC.
Notes: <http://www.epic.org/bookstore/privacy%26humanrights99/default.html>
90. Eliassen, K. and M. Sjovaag. (1999). "Conclusion." Pp. 257-72 in *European Telecommunications Liberalization*, eds. K Eliassen and M. Sjovaag. London and New York: Routledge.
91. Evans, P. and et al., eds. (1993). *Double-Edged Diplomacy*. Berkeley, CA: University of California Press.
92. Everard, J. (2000). *Virtual States. The Internet and Boundaries of the Nation-State*. London and New York: Routledge.
93. Federal Ministry of Economic and Technology and Federal Ministry for Education and Research. (1999). *Innovation and Jobs in the Information Society of the 21st Century. Action Programme by the German Government*. Bonn and Berlin: Federal Ministry for Education and Technology and Federal Ministry of Economics and Technology.
94. Ferguson, K. (1998). "World Information Flows and the Impact of Net Technology." *Social Science Computer Review* 16(3):252-67.
95. Fischer, S. (27 Mar 2000). "Gute Nacht Im Netz." *Der Spiegel* (Hamburg) (13), pp. 64-66.
96. Forquet, F. and A. Orioli. (14 Jul 2000). "'Competitività', Non E' Solo Un Fatto Di Costi." *Il Sole 24 Ore* (Milan), Commenti e Inchieste, p. 7.
97. Frederick, H. (1993). *Global Communications and International Relations*. Celmont, CA: Wadsworth Publishing Company.
98. Gessler, P. (7 Aug 2000). "NPD Trifft Auf Widerstand." *Die Tageszeitung* (Berlin), Taz Berlin, p. 19.
99. Gewirtz, P. (1997). "Constitutional Law and New Technology." *Social Research* 64(3):1191-217.
100. Gibbs, J. (1982). "Law As a Means of Social Control." Pp. 83-113 in *Social Control: Views From the Social Sciences*, ed. J. Gibbs. London and Beverly Hills, CA: Sage.
101. Gillet, S. and M. Kapor. (1997). "The Self-Governing Internet: Coordination by Design." Pp. 3-38 in *Coordinating the Internet*, first ed. editors Kahin B. and J. Keller. Cambridge, MA and London, England: The MIT Press.
102. Global Internet Liberties Campaign (GILC) . (1999). *News Alert*. Washington, DC.
103. Global Internet Liberties Campaign (GILC) and Electronic Privacy Information Center. (1998a). *Cryptography and Liberty: An International Survey of Encryption Policy*. Washington, DC: Electronic Privacy Information Center.

Notes: <http://www.gilc.org/crypto/cryptosurvey.html>

104. Global Internet Liberties Campaign (GILC) and Electronic Privacy Information Center. (1998b). *Privacy and Human Rights 1998: An International Survey of Privacy Laws and Developments*. United States: Electronic Privacy Information Center (EPIC).
Notes: <http://www.epic.org/> and <http://www.gilc.org/>
105. Hafner, K. and M. Lyon. (1996). *Where Wizards Stay Up Late: The Origins of the Internet*. New York NY: Simon & Schuster.
106. Hafner, K. and J. Markoff. (1995). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Touchstone.
107. Haiman, F. (1978). *Freedom of Speech*. Skokie, IL: National Textbook Company.
108. Hallgren, M. and A. McAdams. (1997). "The Economic Efficiency of Internet Public Good." Pp. 455-78 in *Internet Economics*, editors L. McKnight and J. Bailey. Cambridge, MA and London : The MIT Press.
109. Heise, D. (1975). *Causal Analysis*. New York: John Wiley and Sons.
110. Hick, S. and et al., eds. (2000). *Human Rights and the Internet*. Houdmills and London: MacMillian Press.
111. Hofstede, G. (1984). *Culture's Consequences: International Differences in Work-Related Values*. Beverly Hills, London and New Delhi : Sage Publications.
Notes: (abridged edition)
112. Hofstede, G. (1991). *Cultures and Organisations: Software of the Mind*. New York: McGraw-Hill.
113. Horak, R. (1997). *Communications Systems and Networks. Voice, Data and Broadband Technologies*. New York, NY: M & T Books.
114. Horowitz, A. (1990). *The Logic of Social Control*. New York and London: Plenum Press.
115. Hundt, R. (2000). *You Say You Want a Revolution: A Story of Information Age Politics*. New Haven and London: Yale University Press.
116. Il Sole 24 Ore. (11 Sep 2000). "L'Italia Maglia Nera Della New Economy." *Il Sole 24 Ore* (Milan), p. 1 and 2.
117. ———. (9 May 2000a). "Banking on Line, Un '99 Da Boom." *Il Sole 24 Ore* (Milan), p. 31.
118. ———. (9 May 2000b). "E-Commerce Lontano Per Piccole Imprese." *Il Sole 24 Ore* (Milan), In Breve, p. 12.
119. Info2000. (1996). "Illegal and Harmful Contents on the Internet." *Communication to the European Parliament, the Council, the Economic and Social Committee,*

and the Committee of Regions . Luxembourg: Echo.

120. Inglehart, R. and et al. (1998). *Human Values and Beliefs: A Cross-Cultural Sourcebook*. Ann Arbor, Michigan: The University of Michigan Press.
121. International Telecommunication Union (ITU). (1995). *World Telecommunications Development Report*. Geneva, CH: ITU.
122. ———. (1998). *General Trends in Telecommunication Reform 1998*. Geneva, Switzerland: ITU.
123. ———. (1999). *Challenges to the Network. Internet for Development*. Geneva, CH: International Telecommunication Union.
124. Jervis, R. (1976). *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press.
125. Jick, T. (1983). "Mixing Qualitative and Quantitative Methods: Triangulation in Action." Pp. 135-48 in *Qualitative Methodology*, ed. J. Van Maanen. Beverly Hills et al.: SAGE Publications.
126. Johnson, D. and D. Post . (1997). "The Rise of Law on the Global Network." Pp. 3-47 in *Borders in Cyberspace*, eds. B. Kahin and C. Nesson . Cambridge, MA: the MIT Press.
127. Jonquieres, G. and L. Kehoe. (8 Oct 1998). "Regulators@Odds." *Financial Times* (London), p. 14.
128. Jordan, T. (1999). *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. London and New York: Routledge.
129. Kahin, B. and C. Nesson. (1997). "Preface." Pp. ???? in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, eds. B. Kahin and C. Nesson. Cambridge, MA: the MIT Press.
130. Kalton, G. (1983). *Introduction to Survey Sampling*. Beverly Hills, London, New Delhi: Sage Publications.
131. Katzstein, P., ed. (1996). *The Culture of National Security. Norms and Identity in World Politics*. New York: Columbia University Press.
132. Kedzie, C. (1996). "Communication and Democracy: Coincident Revolution and the Emergence of the Dictator's Dilemma." RAND Graduate School, Santa Monica, CA.
Notes: PhD dissertation
133. Keohane, R. , ed. (1986). *Neorealism and Its Critics*. New York : Columbia University Press.
134. Keohane, R. and J. Nye. (1998). "Power and Interdependence in the Information Age." *Foreign Affairs* 77(5):81-94.

135. King, G. and et al. (1994). *Designing Social Inquiry. Scientific Inference in Qualitative Research*. Princeton, NJ.: Princeton University Press.
136. King, N. (1994). "The Qualitative Research Interview." Pp. 14-36 in *Qualitative Methods in Organizational Research. A Practical Guide*, eds. C. Cassell and G. Symon . London, et al.: SAGE Publications .
137. Kleffner, H. (8 Aug 2000). "Terroraufruf Ubers Internet." *Die Tageszeitung* (Berlin), Taz Berlin, p. 19.
138. Koch J. et al. 2000. "Ausfall Im System." Pp. 40-61 in Hamburg.
139. Koff S. and S. Koff. (2000). *Italy: From the First to the Second Republic*. London and New York: Routledge.
140. Kozak, D. and J. Keagle, eds. (1988). *Bureaucratic Politics and National Security*. Boulder, CO and London: Lynne Rienner Publisher.
141. Krasner, S. (1990). "Global Communications and National Power: Life on the Pareto Frontier." *World Politics* 43(3):336-66.
142. ———. (1995). "Power Politics: Institutions and Transnational Relations." Pp. 257-279 in *Bringing Transnational Relations Back In*, ed. T. Risse-Kappen . Cambridge, UK: Cambridge University Press .
143. Lake, A. (2000). *Six Nightmares: Real Threats in a Dangerous World and How America Can Meet Them*. Boston: Little Brown.
144. Lees, J. D. (1975). *The Political System of the United States*. Second ed. London: Faber and Faber.
145. Leiner, B. e. al. *. (1998). *A Brief History of the Internet: Version 3.1*. Washington, DC: The Internet Society.
Notes: <http://www.isoc.org/internet/history/brief.html>; *(V. Cerf, D. Clark, R. Kahn, L. Kleinrock, D. Lynch, J. Postel, L. Roberts, S. Wolff)
146. Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York, NY: Basic Books.
147. Levy, S. (2001). *Crypto. How the Code Rebels Beat the Government-Saving Privacy in the Digital Age*. New York et al.: Viking.
148. Lewis-Beck M. (1980). *Applied Regression: An Introduction*. Newbury Park, London, New Delhi: Sage Publications.
149. ———. (1995). *Data Analysis: An Introduction*. Thousand Oaks, London, New Delhi: Sage Publications.
150. Libicki, M. (1997). *Defending Cyberspace and Other Metaphors*. Washington DC: National Defense University.
151. Loader, B., ed. (1998). *Cyberspace Divide: Equality, Agency and Policy in the Information Society*. London and New York: Routledge.

152. Long, S. (2000). *The Virtual Threat: A Survey of Online Finance*. London: The Economist.
153. Loshin, P. (1997). *TCP/IP Clearly Explained*. 2nd edition ed. London: Academic Press.
154. Mann, B. (1995). *Politics on the Net: Surfing the World of Internet Politics*. Indianapolis, IN: QUE Corp.
155. Maschler, N. (8 Aug 2000). "Streit Um Bannmeile." *Die Tageszeitung* (Berlin), Inland, p. 7.
156. Mayer-Schönberger, V. and T. Foster . (1997). "A Regulatory Web: Free Speech and the Global Information Infrastructure." Pp. 235-54 in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, eds. B. Kahin and C. Nesson . Cambridge, MA and London: the MIT Press.
157. Mayers, D. (1994). "Communication Technology and Social Movements: Contribution of Computer Networks to Activism." *Social Science Computer Review* 12(2):250-260.
158. McCarthy, P. (1995). *The Crisis of the Italian State. From the Origins of the Cold War to the Fall of Berlusconi*. New York: St. Martin's Press.
159. Metzl, J. (1996). "Information Technology and Human Rights." *Human Rights Quarterly* 18:705-46.
160. Milner, H. (1997). *Interests, Institutions, and Information: Domestic Politics and International Relations*. Princeton, NJ: Princeton University Press.
161. Mock, K. (2000). "Hate on the Internet." Pp. 141-52 in *Human Rights and the Internet*, eds. Hick S. et al. London: MacMillian Press Ltd.
162. Moisy, C. (1996). "Myths of the Global Village." *Foreign Policy*(107 Summer):78-87.
163. Moravcsik, A. (1993). "Introduction." *Double-Edged Diplomacy*, eds. P. e. al. Evans. Berkeley, CA: University of California Press.
164. ———. (1995). "Domestic Institutions and International Bargaining: The Role of Agent Veto in Two-Level Games ." *American Political Science Review* 89:914-24.
165. Morgan, R. and J. Connor, eds. (1971). *The American Political System. Introductory Readings*. New York: Harcourt Brace Jovanovich, Inc.
166. Morris, M. and C. Ogan. (1996). "The Internet As a Mass Medium." *Journal Of Communication* 46:39-50.
167. Mowlana, H. (1997). *Global Information and World Communication*. London et al.: SAGE.
168. Mueller, M. (1999). "ICANN and Internet Governance. Sorting Throught the Debris

of "Self-Regulation". *Info* 1(6):497-520.
Notes: <http://www.camfordpublishing.com>

169. Mulgan, G. (1991). *Communication and Control*. Cambridge, UK: Polity Press.
170. Naisbitt, J. (1994). *Global Paradox*. New York: Avon Books.
171. Natalicchi, G. (1996). "Telecommunications Policy and Integration Processes in The European Union." City University of New York, Ann Arbor, MI .
Notes: Unpublished Dissertation
172. Negroponte, N. (1995). *Being Digital*. New York: Knopf.
173. Newhagen, J. and S. Rafaeli. (1996). "Why Communication Researchers Should Study the Internet. A Dialogue." *Journal Of Communication* 46:4-13.
174. Noam, E. (1986). "Telecommunications Policy on Both Sides of the Atlantic: Divergence and Outlook." Pp. 255-74 in *Marketplace for Telecommunications: Regulation and Deregulation in Industrialised Democracies*, editor S. Snow. New York and London: Longman.
175. ———. (1990). "Preface." Pp. v/ix in *Technologies Without Boundaries*, I. de Sola Pool. Cambridge, MA: Harvard University Press.
176. ———. (1992). *Telecommunications in Europe*. New York and Oxford: Oxford University Press.
177. Nobis, C. (22 Apr 2000). "Internet, Ora e Per Forza." *La Repubblica* (Rome), p. 4.
Notes: (special supplement on car industry)
178. Norusis, M.(1990). *SPSS Base System User's Guide* Chicago : SPSS Inc.
179. ———.(1992). *SPSS for Windows : Base System User's Guide : Release 5.0* Chicago : SPSS Inc.
180. Nua Survey. (1998). *Nua Newsletter*. Volume 3 No. 41 . Ireland: Nua Ltd.
Notes: <http://www.nua.ie/survey/>
181. ———. (1999). *Nua Newsletter* . Volume 4 No. 3. Ireland: Nua Ltd.
Notes: <http://www.nua.ie/surveys/>
182. Nua Survey . (1999b). *Newsletter Review Edition*. Ireland: Nua Ltd.
Notes: <http://www.nua.ie/survey/>
183. Nye, J. and W. Owens . (1996). "America's Information Edge." *Foreign Affairs* 75(2):20-36 .
184. OECD. (1994). *Privacy and Data Protection: Issues and Challenges*. Paris: OECD.
185. ———. (1999). *Communications Outlook 1999*. Paris: Organisation for Economic Cooperation and Development (OECD).

186. Omaha, K. ((1997?)). *The End of the Nation-State: The Rise of Regional Economies*. New York: Free Press.
187. Oppendahl, C. (1997). "Trademark Disputes in the Assignment of Domain Names." Pp. 154-86 in *Coordinating the Internet*, editors B. Kahin and J. Keller. Cambridge, MA and London : The MIT Press.
188. Parks M. and K. Floyd . (1996). "Making Friends in Cyberspace." *Journal of Communication* 46:51-79.
189. Peet, J. (2000). *Shopping Around the Web. A Survey of E-Commerce*. The Economist Survey ed. London: The Economist .
190. Ploch D. R. (1974). "Ordinal Measures of Association and the General Linear Model." *Measurement in the Social Sciences. Theories and Strategies*, editor Blalock H.M. New York: MacMillian Press.
191. Pound, R. (1997). *Social Control Through Law*. New Brunswick (USA) and London : Transaction Publishers.
192. Putnam, R. (1988). "Diplomacy and Domestic Politics." *International Organization* 42:427-60.
193. Putnam, R. (1993). *Making Democracy Work: Civic Tradition in Modern Italy*. Princeton, NJ: Princeton University Press.
194. Quade, D. (1974). "Nonparametric Partial Correlation." Pp. 399-423 in *Measurement in the Social Sciences. Theories and Strategies*, first ed. editor H. Blalock. New York: MacMillian Press.
195. Quinn, D. (1997). "The Correlates of Change in International Financial Regulation." *American Political Science Review* 91(3):531-50.
196. Ransom, H. (1970). *The Intelligence Establishment*. Cambridge, MA: Harvard University Press.
197. Reid, R. (1997). *Architects of the Web: 1,000 Days That Built the Future of Business*. New York: John Wiley & Sons, Inc.
198. Reiss, A. (1984). "Selecting Strategies of Social Control Over Organizational Life." Pp. 23-35 in *Enforcing Regulation*, eds. K. Hawkins and J. Thomas . Boston et al.: Kluwer-Nijhoff Publishing.
199. Resnick, M. (1994). *Turtles, Termites, and Traffic Jams: Explorations in Massive Parallel Microworlds*. Cambridge MA, London: The MIT Press.
200. Risse-Kappen, T., ed. (1995a). *Bringing Transnational Relations Back in. Non-State Actors, Domestic Structures and International Institutions*. Cambridge: Cambridge University Press.
201. ———. (1995b). "Ideas Do Not Float Freely. Transnational Coalition, Domestic Structure, and the End of the Cold War ." Pp. 187-222 in *International*

Relations Theory and the End of the Cold War, eds R. Ned-Lebow and T. Risse-Kappen. New York: Columbia University Press .

202. Robert, C. (1995). "Legal Structure of the Internet." *ASLIB Proceedings* (47):235-40.
203. Rosenzweig, R. (1998). "Wizards, Bureaucrats, Warriors and Hackers: Writing the History of the Internet." *American Historical Review* 103(5):1530-1552.
204. Ruiz, B. (1997). *Privacy in Telecommunications: A European and an American Approach*. The Hague et al: Kluwer Law International.
205. Saris, W. and H. Stronkhorst. (1984). *Causal Modelling in Nonexperimental Research*. Amsterdam, The Netherlands: Sociometric Research Foundation.
206. Saurin, J. (1995). "The End of International Relations?" Pp. 244-61 in *Boundaries in Question: New Directions in International Relations*, eds. J. MacMillan and Linklater A. London: Pinter.
207. Saye, A. and et al. (1966). *Principles of American Government*. Englewood Cliffs, NJ: Prentice-Hall, Inc.
208. Schneier, B. (2000). *Secrets and Lies. Digital Security in a Networked World*. New York et al.: John Wiley and Sons .
209. Schroeder, L. and et al. (1986). *Understanding Regression Analysis. An Introductory Guide*. Beverly Hills, London and New Delhi: Sage Publications.
210. Schwartz A. (1999a, February 3). "Philadelphia Court Blocks Enforcement of the Child Online Protection Act." *CDT POLICY POST* . Volume 5, Number 3 . Washington DC: Center for Democracy and Technology.
Notes: e-mail: ari@cdt.org
211. Schwartz, A. (1999b, February 25). "Bill Lifting Encryption Controls Re-Introduced in Congress." *CDT POLICY POST*. Volume 5, Number 4 . Washington, DC: Center for Democracy and Technology.
212. Schwarz, E. (1997). *Webonomics: Nine Essential Principles for Growing Your Business on the World Wide Web*. London: Penguin Books.
213. Severgnini, B. (2000). "Modern Italy's Old-fashioned Ways." Pp. 49-50 in *The Economist -The World in 2001*, London: The Economist Publications.
214. Shapiro, C. and H. Varian. (1999). *Information Rules: A Strategic Guide to the Network Economy*. Boston, MA: Harvard Business School Press.
215. Shaw, R. (1997). "Internet Domain Names: Whose Domain Is This?" Pp. 107-34 in *Coordinating the Internet*, editors B. Kahin and J. Keller. Cambridge, MA and London : the MIT Press.
216. Shinn, A. (1974). "Relations Between Scales." Pp. 121-58 in *Measurement in the Social Sciences. Theories and Strategies*, first ed. ed. Blalock H.M. New York : MacMillian Press .

217. Siegele, L. (2001). *The Age of the Cloud. A Survey of Software*. London: The Economist .
218. Singh, S. (1999). *The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography*. London: Fourth Estate.
219. SIPRI. (1998). *SIPRI Yearbook 1998*. Oxford, UK: Oxford University Press.
220. Siroli, G. and et al. (1997). "Internet e World Wide Web." *Reti Informatiche, Le Scienze Quaderni n.95* ed. ed. P. Capiluppi. Milan, Italy: Le Scienze.
221. Smith, H. (1975). *Strategies of Social Research. The Methodological Imagination*. Englewood Cliffs, NJ: Prentice-Hall, Inc.
222. Steeves, V. (2000). "Privacy, Free Speech and Community: Applying Human Rights Law to Cyberspace". Pp. 187-99 in *Human Rights and the Internet*, eds. S. Hick and et al. London: MacMillian Press Ltd.
223. Stone, A. (1997). *How America Got On-Line: Politics, Markets and the Revolution in Telecommunications*. Armonk, NY and London: M.E. Sharpe.
224. Supperstone, M. (1981). *Brownlies Law of Public Order and National Security*. London: Butterworths.
225. Symonds, M. (1999). *The Net Imperative: A Survey of Business and the Internet*. The Economist Survey ed. London: The Economist.
226. ———. (2000). *The Next Revolution: A Survey of Government and the Internet*. The Economist Newspaper Publishing Ltd.
Notes: The Economist Survey
227. Szafran, E. (1998). "Regulatory Issues Raised by Cryptography on the Internet." *Communications Law* 3(2):38-49.
228. Tambini, D. (1998). "Civic Networking and Universal Rights to Connectivity: Bologna." Pp. 84-109 in *Cyberdemocracy: Technology, Cities and Civic Networks*, eds. R. D. T. a. C. B. Tsagarousianou. London and New York: Routledge.
229. Tarquini, A. (3 Jul 2000a). "Il Risveglio Del Panzer E' Nella Nuova Medicina." *La Repubblica Affari e Finanza* (Rome), p. 9.
230. ———. (3 Jul 2000b). "Il Web Conquista Anche i Giganti." *La Repubblica Affari e Finanza* (Rome), p. 13.
231. Tengelin, V. (1981). "The Vulnerability of the Computerised Society." Pp. 205-13 in *Information, Computer and Communication Policies for the '80s*, editor H. Gassmann. Amsterdam, NL: North Holland Publishing Company.
232. Trochim W. (1999). *Research Methods Knowledge Base*. Cincinnati, OH. Atomic Dog Publishing.

233. U.S. Department of Commerce (DOC) and Internet Corporation for Assigned Names and Numbers (ICANN). (1998). *Memorandum of Understanding*. Washington, D.C.: DOC.
234. Van Evera, S. (1997). *Guide to Methods for Students of Political Science*. Ithaca and London: Cornell University Press.
235. Viotti, P. and M. Kauppi. (1999). *International Relations Theory. Realism, Pluralism, Globalism, and Beyond*. Boston et al.: Allyn and Bacon.
236. Wallace J. (1997). *Overdrive: Bill Gates and the Race to Control Cyberspace*. New York, NY: John Wiley & Sons, Inc.
237. Werle, R. (1999). "Liberalisation of Telecommunications in Germany." Pp. 110-127 in *European Telecommunications Liberalisation*, eds. Eliassen K. and M. Sjovaag. London and New York: Routledge.
238. White, G. and D. Ball. (16 Mar 2000). "Fiat and GM May Join Major Parts Programs." *The Wall Street Journal Europe* (Brussels, Belgium), p. 1 and 12.
239. Woodall, P. (1996). *The Hitchhiker's Guide to Cybereconomics: A Survey of World Economy*. London: The Economist.
240. ———. (2000). *Untangling E-Conomics: A Survey of the New Economy*. London: The Economist.
Notes: The Economist Survey Series
241. Woolridge, A. (1999). *The World in Your Pocket: A Survey of Telecommunications*. London: The Economist.
242. World Bank. (1998). *World Bank Indicators 1997*. Washington, DC: World Bank.
Notes: <http://www.worldbank.org/data/databytopic/databytopic.html>
243. Wright, S. (2000). "Political Control and the Internet." Pp. 200-210 in *Human Rights and the Internet*, eds. S. Hick et al. Houndmills and London: MacMillian Press.
244. Yergin, D. and J. Stanislaw. (1998). *The Commanding Heights*. New York: Touchstone.
245. Zampaglione, A. (3 Jul 2000). "New Economy: Ecco Le 'Top Ten'. Dopo Gli USA, Stoccolma e Israele." *La Repubblica* (Rome), Economia, p. 38.
246. Zeller, R. and E. Carmines. (1978). *Statistical Analysis of Social Data*. Chicago: Rand McNally College Publishing.

APPENDIX A
LIST OF INTERVIEWS

1. United States

- 1 Tamar Frankel (Professor)
Boston University Law School and
Berkman Center for Internet and Society
Boston, MA, July 13, 1999

- 2 Robert Ghent (Lt. Colonel)
U.S. Army War College,
Carlisle, PA, July 20, 1999

- 3 John Pike
Federation of American Scientists (FAS)
Washington, D.C. July 15, 1999

- 4 Marc Rotenberg (Executive Director) and Wayne Madsen (Senior Researcher)
Electronic Privacy Information Center (EPIC)
Washington, D.C. July 16, 1999

- 5 Ari Schwarz
Policy Analyst
Center for Democracy and Technology (CDT)
Washington, D.C. July 12, 1999

2. Germany

- 6 Hans Jörg Denhardt,
Director of company activities with federal and regional governments,
IBM Germany
Berlin, June 28, 2000

- 7 Hansjürgen Garstaka (Professor)
Data Protection and Information Access Commissioner of the State of Berlin
Berlin June 27, 2000

- 8 Andreas Schwaab
Personal assistant to
Parliamentary Secretary of State Siegmur Mosdorf

Federal Ministry of Economics and Technology
Berlin, June 26, 2000

9 Joerg Tauss
SPD Member of Parliament
Chairman of the *Bundestag* Committee on the New Media
Berlin, June 26, 2000

10 Stephen Wolf
Internet and Intranet security,
Bundesamt Sicherheit in Informationstechnik
Bonn, August 11, 2000

3. Italy

11 Maurizio Bonanni
Italian Ministry of Communications
Rome, July 17, 2000

12 Carlo Fininzio (Maj. General)
Italian Air Force
Centro Militare Studi Strategici (CEMISS)
Roma, May 3, 2000

13 Leda Guidi (Head)
Iperbole, Comune di Bologna
Bologna, May 5, 2000

14 Andrea Monti (Attorney-at-Law and President)
Associazione per la Libera Comunicazione Elettronica (ALCEI)
Roma, July 17, 2000

15 Roberto Perrella,
Telecom Italia
Rome, July 17, 2000

16 Lucio Picci (Assistant Professor)
Department of Economics
University of Bologna
Bologna, September 30, 2000

17 Giuseppe Rao (Head)
Forum for the Information Society
Presidency of the Council of Ministers
Rome, May 3, 2000

APPENDIX B

The Codebook¹ All Variables

1. **Hypothesis 1 (X1): *defense*.** X1 is represented by the % of GDP in USD devoted to defence expenditures by each countries (SIPRI 1998). Higher percentage means greater military expenditures, and thus higher propensity toward national security. **The variable is continuous. Column H in the database.**
2. **Hypothesis 2 (X2): *individ*.** X2 is operationalized via the Individualism Index created by G. Hofstede (1984:158, and 1991). Hofstede used for his analysis two surveys conducted among IBM employees in the 1970s to investigate how the assessment of being individualistic changed across countries. As far as I know Hofstede's has been the only large, cross-country study on individualism. Higher scores mean a higher level of individualism.² **Discrete variable. Column L in the database.**
3. **Hypothesis 3 (X3): *democry*.** X3 is indexed by the Democracy Scores (0=no democracy at all, 10=maximum level of democracy)³ of the Polity III database prepared by Ted Gurr (1994), and downloaded by the ICPSR (Excel Formatted) at <ftp://isere.colorado.edu/pub/datasets/polity3/politymay96.data>.⁴ The higher marks, the more democratic the country. **Discrete variable. Column K in the database.**
4. **Hypothesis 4 (X4): *telecomp*.** X4 is the level of privatization/liberalization in the telecommunications and broadcasting sectors, (ITU World Telecommunication Development Report 1995, and 1997). The higher the numbers, the more liberalised the telecom sector is.⁵ **Discrete variable. Column M in the database.**

¹ The codebook has been prepared according to Throchim's (1999) specifications (also available at <http://trochim.human.cornell.edu/kb/statprep.htm>, v. several times between January 1999 and March 2001).

² In the database, for all the former Yugoslav republics, I have introduced the same value of the old Federal republic.

³ The Autocracy Score is also available but not used here.

⁴ See also <http://www.unimich.edu/icpsr/>

⁵ C=Competition (3), PC=Partial Competition (2), M=Monopoly (1) in the database. These values were weighted with the number of sectors (max.11) to provide the final figure. The final range was from a minimum of 11 (all sectors, M) to a maximum of 33 (all sectors, C).

5. **Hypothesis 5 (X5a) and (X5b): *tradepro* and *econfree*.** X5 was tested with two indicators: the former (X5a) is the countries' trade % of PPP GDP (Table 6.1, World Bank Development Indicators 1998), the higher the percentage, the greater the trade propensivity.⁶ **Continuous variable.** The latter is the Index of Economic Freedom, by the Heritage Foundation/The Wall Street Journal (1998). Here too, the higher score stands for greater economic freedom in the countries considered.⁷ **Discrete variable. Columns I and N in the database.**

The **first indicator** for my dependent variable (Y1) is *crypto*. Y1 is given by national legal conditions to use of encryption software for private communications. The first survey was conducted by the Global Internet Liberties Campaign (GILC/EPIC, 1998).⁸ The survey ranked countries from *green* (value 5 in my database, most free and uncontrolled) to *red* (1, most restricted and controlled). **Discrete variable. Column D in the database.** The **second indicator (Y2): *privacy*.** Y2 is the level of legal protection that personal privacy is granted in diverse countries. This survey as well has been conducted by GILC/EPIC (GILC/EPIC, 1998), and higher numbers mean a greater degree of protection for personal privacy.⁹ **Discrete variable. Column F in the database.**

8. The **third indicator (Y3): *iphosts*.** Y3 is the ratio between the number of Internet hosts (IP-Hosts) and the population of a given country (Table 5.11, World Development Indicators, World Bank, 1998). The higher figures indicates large numbers of IP host computers, and hence easier access to the Net, and few or no obstacles to set up a host. **Continuous variable. Column G in the database.**

⁶ <http://www.worldbank.org/> (v. various days, November, and December 1998, and January 1999).

⁷ The survey on economic freedom has been performed by the Heritage Foundation since 1995. I have used the 1998 figures. The data from the years are available on line at <http://www.heritage.org/index/> (v. various times, in September, October and November 1998, and April 1, 2001). I have reversed the order of the scores (in the original, the lowest the score, the greater the freedom).

⁸ <http://www.gilc.org/crypto/cryptosurvey.html> (v. various days, October, November, December 1998 and January 1999). The GILC is a transnational, umbrella-organization that includes several pro-liberties NGOs. The survey was actually organized and run by the civil liberties NGO, EPIC in 1998, on behalf of GILC. In 1999 and 2000, EPIC conducted two more surveys, but this time under its own name.

⁹ <http://www.gilc.org/privacy/survey.html> (v. various days, October, November, December 1998) and <http://www.privacyexchange.org/iss/surveys/codesum.html> sample of countries (v. various days, October and November 1998).

9. The first control variable (C1): *income*. C1 is represented by the 1997 GNP per capita in PPP by the World Development Indicators (World Bank, 1998). **Continuous variable.** Column E of the database.

10. The second control variable (C2): *educ*. C2 is the level of education as % of the relevant population enrolled in secondary school (Table 2.10 of the World Development Indicators, World Bank, 1998). The higher the number, the more educated (thanks to more school-years) the population. **Continuous variable.** Column J in the database.

11. The third control variable (C3): *mulmedia*. C3 is the 1995 index of access to multimedia (as calculated in Table 2 of the World Telecommunication Development Report, International Telecommunication Union, 1995:4) as number of telephone lines and computers per 100 people in the observed countries. The greater the score, the more "wired" the country is. **Discrete variable.** Column O in the database.

The Digital Challenge
Summary Table

All Variables

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | |
|----|------------|--------------|---|-----------------|----------------|---------------|---------------|----------------|---------------|-------------|--------------|------------------|-----------|--------------|-------------|---------|
| | COUNTRIES | COUNTRY CODE | | CRYPTO SCORE 98 | NATION. INCOME | PRIVACY SCORE | IP-HOST COUNT | DEFENCE BUDGET | TRADE PROPENS | EDUC. LEVEL | DEMOCY SCORE | INDIVIDUAL SCORE | TELECOMPT | ECONM FREEDM | MULTI MEDIA | |
| 1 | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | |
| 3 | | | | | | | | | | | | | | | | |
| 4 | ANGUILLA | ai | | 5 | 8,720 | unknown | 0 | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 5 | ANTIGUA | ag | | 5 | 9,950 | unknown | 25.56 | unknown | unknown | unknown | unknown | unknown | 0 | unknown | unknown | 42.34 |
| 6 | ARGENTINA | ar | | 3 | 2,280 | 3.5 | 3.6 | 1.2 | 14 | 72 | 8 | 46 | 1.9 | 2.6 | 20.79 | |
| 7 | ARMENIA | am | | 3 | 20,170 | unknown | 0.47 | unknown | 14 | 79 | 7 | unknown | 1.36 | 3.45 | 15.4 | |
| 8 | AUSTRALIA | au | | 4 | 21,980 | 5 | 281.11 | 2.3 | 34 | 147 | 10 | 90 | 3 | 2.05 | 83.01 | |
| 9 | AUSTRIA | at | | 3 | 4,840 | 6.5 | 110.2 | 0.9 | 71.6 | 104 | 10 | 55 | 3 | 2.15 | 61.78 | |
| 10 | BELARUS | by | | 1 | 22,370 | unknown | 0.25 | 1.2 | 26.3 | unknown | 4 | unknown | 2.27 | 4.05 | 20.77 | |
| 11 | BELGIUM | be | | 5 | 4,110 | 6.5 | 64.05 | 1.6 | unknown | 144 | 10 | 75 | 3 | 2.1 | 63.25 | |
| 12 | BELIZE | bz | | 5 | 6,240 | unknown | 0.54 | 1.5 | unknown | unknown | unknown | unknown | 1.18 | 2.8 | 16.11 | |
| 13 | BRAZIL | br | | 5 | 3,860 | 4 | 4.89 | 1.9 | 10.2 | 45 | 10 | 38 | 2.3 | 3.35 | 11.41 | |
| 14 | BULGARIA | bg | | 4 | 21,860 | 4 | 3.92 | 1.8 | 23.8 | 78 | 8 | unknown | 1.45 | 3.65 | 34.24 | |
| 15 | CANADA | ca | | 4 | 12,080 | 6 | 201.35 | 1.4 | 58.5 | 106 | 10 | 80 | 2.81 | 2.1 | 84.6 | |
| 16 | CHILE | cl | | unknown | 3,570 | 5 | 11.02 | 1.6 | 18.9 | 69 | 9 | 23 | 3 | 2.15 | 20.1 | |
| 17 | CHINA | cn | | 1 | | unknown | 0.16 | 1.1 | 7.1 | 67 | 0 | unknown | 2.25 | 3.75 | 4.76 | |
| 18 | CROATIA | hr | | 5 | | unknown | 10.29 | 14.5 | 59.9 | 82 | 2 | 27 | 1.12 | 3.75 | 32.95 | |
| 19 | CYPRUS | cy | | 4 | | unknown | 19.26 | 3.4 | unknown | unknown | 10 | unknown | 0 | 2.6 | 52.55 | |
| 20 | CZECH REP. | cz | | 4 | 11,380 | 5 | 39.6 | 1.8 | 46.3 | 96 | 10 | unknown | 2.27 | 2.2 | 34.1 | |
| 21 | DENMARK | dk | | 5 | 22,740 | 6.5 | 202.84 | 1.8 | 73.7 | 118 | 10 | 74 | 3 | 2.25 | 92.2 | |
| 22 | ESTONIA | ee | | 5 | 5,010 | 6.5 | 54.29 | 1.2 | 77.4 | 86 | 8 | unknown | 2.36 | 2.15 | 30.52 | |
| 23 | FINLAND | fi | | 5 | 18,980 | 6.5 | 613.08 | 1.6 | 70.1 | 116 | 10 | 63 | 3 | 2.25 | 74.42 | |
| 24 | FRANCE | fr | | 2 | 21,860 | 7 | 40.58 | 3 | 45.4 | 111 | 9 | 71 | 3 | 2.5 | 71.43 | |
| 25 | GERMANY | de | | 5 | 21,300 | 7 | 84.46 | 1.7 | 55.1 | 103 | 10 | 67 | 3 | 2.3 | 77.16 | |
| 26 | GREECE | gr | | 4 | 13,080 | 6 | 15.98 | 4.5 | 27.9 | 95 | 10 | 35 | 2.45 | 2.9 | 54.4 | |
| 27 | HONG KONG | hk | | 3 | 24,540 | 5 | 77.9 | unknown | 247.6 | 75 | 10 | 25 | 1.88 | 1.25 | 69.74 | |
| 28 | HUNGARY | hu | | 4 | 7,000 | 6.5 | 29.22 | 1.6 | 41.4 | 81 | 10 | unknown | 2.3 | 2.9 | 30.47 | |
| 29 | ICELAND | is | | 5 | 22,500 | 6 | 427.91 | unknown | unknown | unknown | 10 | unknown | 1.77 | 2.3 | 78.15 | |
| 30 | INDIA | in | | 2 | 1,650 | 3 | 0.03 | 2.5 | 4.5 | 49 | 8 | 48 | 2.42 | 3.7 | 1.69 | |
| 31 | INDONESIA | id | | 3 | 3,450 | unknown | 0.49 | 1.3 | 13.6 | 48 | 0 | 14 | 2.36 | 2.85 | 2.61 | |
| 32 | IRELAND | ie | | 4 | 16,740 | 6.5 | 76.38 | 1.1 | 121.6 | 114 | 10 | 70 | 2.33 | 2 | 56.52 | |
| 33 | ISRAEL | il | | 1 | 16,960 | 5 | 85.49 | 8.7 | 47.5 | 89 | 9 | 54 | 1.6 | 2.8 | 55.72 | |
| 34 | ITALY | it | | 4 | 20,060 | 6 | 25.76 | 1.9 | 39.6 | 74 | 10 | 76 | 3 | 2.5 | 53.24 | |
| 35 | JAPAN | jp | | 3 | 23,400 | 5.5 | 58.4 | 0.1 | 26.1 | 99 | 10 | 46 | 2.9 | 2.05 | 61.72 | |

Summary Table

The Digital Challenge
Summary Table
All Variables

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|----|-------------|----|---|---------|--------|---------|--------|---------|---------|---------|----|---------|---------|---------|--------|
| 36 | KOREA ROK | kr | | 3 | 13,500 | 4 | 14.55 | 3.2 | 46.7 | 101 | 10 | 18 | 2 | 2.3 | 56.21 |
| 37 | LATVIA | lv | | 5 | 3,650 | 3 | 23.31 | 0.8 | 41.1 | 85 | 8 | unknown | 2 | 2.85 | 30.6 |
| 38 | LIECHTENST | li | | 5 | . | 6.5 | 187.22 | unknown | 89.9 | 91 | 10 | 68 | 2.9 | 1.9 | 76.34 |
| 39 | LITHUANIA | lt | | 5 | 4,510 | 5.5 | 4.67 | 0.5 | 46.6 | 84 | 10 | unknown | 2.54 | 3 | 27.43 |
| 40 | LUXEMBOUR | lu | | 4 | 34,460 | 5 | 85.22 | 0.7 | unknown | unknown | 10 | unknown | 2.8 | 1.95 | 59.16 |
| 41 | MALAYSIA | my | | 3 | 10,920 | 2 | 12.24 | 2.4 | 70.2 | 61 | 8 | 26 | 3 | 2.4 | 22.6 |
| 42 | MEXICO | mx | | 5 | 8,120 | 2.5 | 3.21 | 0.4 | 26.1 | 58 | 1 | 30 | 1.9 | 3.25 | 12.38 |
| 43 | NAURU | nr | | 5 | . | unknown | 0 | unknown | unknown | unknown | | unknown | 0 | unknown | 15.65 |
| 44 | NETHERLAN | nl | | 4 | 21,340 | 6.5 | 174.33 | 2 | 106.4 | 139 | 10 | 80 | 3 | 2.2 | 77.53 |
| 45 | NEW ZEALAN | nz | | 4 | 16,600 | 6 | 236.78 | 1.2 | 45 | 117 | 10 | 79 | 3 | 1.75 | 76.53 |
| 46 | NORWAY | no | | 5 | 23,940 | 6 | 341.75 | 2.3 | 80.3 | 92 | 10 | 69 | 3 | 2.35 | 84 |
| 47 | PAKISTAN | pk | | 1 | 1,590 | unknown | 0.04 | 5.6 | 10 | 26 | 8 | 14 | 1.66 | 3.2 | 1.89 |
| 48 | PAPUA N.G. | pg | | 5 | 2,390 | unknown | 0 | 1.1 | 33 | 14 | 10 | unknown | 2.77 | 3.15 | 1.07 |
| 49 | PHILIPPINES | ph | | 5 | 3,670 | 3 | 0.5 | 1.6 | 21.3 | 79 | 8 | 32 | 3 | 2.65 | 3.42 |
| 50 | POLAND | pl | | 4 | 6,380 | 5 | 13.68 | 2.8 | 26.5 | 96 | 8 | unknown | 2.4 | 2.95 | 20.53 |
| 51 | PORTUGAL | pt | | 4 | 13,840 | 7 | 23.64 | 2.4 | 43.1 | 102 | 10 | 27 | 2.09 | 2.6 | 44.23 |
| 52 | ROMANIA | ro | | 4 | 4,290 | unknown | 3.46 | 3.5 | 16.8 | 66 | 5 | unknown | 2.1 | 3.3 | 14.51 |
| 53 | RUSSIA | ru | | 1 | 4,190 | 3.5 | 3.93 | 3.7 | 19.8 | 87 | 8 | unknown | 2.27 | 3.45 | 19.91 |
| 54 | SAUDI ARAB | sa | | 5 | . | unknown | 0.15 | 13.2 | 41.2 | 58 | 0 | 38 | 0 | 2.8 | 14.36 |
| 55 | SINGAPORE | sg | | 1 | 29,000 | 2 | 94.91 | 4.3 | 316 | 62 | 2 | 20 | 1.88 | 1.3 | 73.01 |
| 56 | SLOVAKIA | sk | | 4 | 7,850 | 4 | 14.77 | 2.3 | 52.2 | 91 | 8 | unknown | 2.27 | 3.05 | 23.19 |
| 57 | SLOVENIA | si | | 5 | 12,520 | 5.5 | 69.35 | 1.6 | 74 | 91 | 10 | 27 | 2.09 | 3.1 | 38.11 |
| 58 | SOUTH AFRI | za | | 3 | 7,490 | 3.5 | 23.42 | 2.1 | 20.7 | 84 | 8 | 65 | 2 | 2.9 | 13.82 |
| 59 | SPAIN | es | | 3 | 15,720 | 6.5 | 28.83 | 1.5 | 36.8 | 118 | 9 | 51 | 2.54 | 2.5 | 48.67 |
| 60 | SWAZILAND | sz | | 5 | 3,560 | unknown | 2.41 | 2.3 | unknown | unknown | 0 | 20 | 1.28 | 2.7 | 2.19 |
| 61 | SWEDEN | se | | 5 | 19,030 | 7 | 268.95 | 2.4 | 87.2 | 132 | 10 | 71 | 3 | 2.45 | 89.7 |
| 62 | SWITZERLAN | ch | | 5 | 26,320 | 6.5 | 187.22 | 1.5 | 89.9 | 91 | 10 | 68 | 2.9 | 1.9 | 104.89 |
| 63 | TAIWAN | tw | | 3 | . | 2.5 | 16.14 | 3.7 | unknown | unknown | 6 | 17 | unknown | 1.95 | 55.47 |
| 64 | THAILAND | th | | unknown | 6,590 | 3 | 1.54 | 1.9 | 31.3 | 55 | 6 | 20 | 1.45 | 2.4 | 8.67 |
| 65 | TURKEY | tr | | 3 | 6,430 | 3 | 2.74 | 4.3 | 17.5 | 56 | 9 | 37 | 1.27 | 2.8 | 23.74 |
| 66 | UKRAINE | ua | | 3 | 2,170 | unknown | 1.29 | 4.5 | 35 | 91 | 8 | unknown | 1.9 | 3.8 | 19.45 |
| 67 | UNITED KING | uk | | 4 | 20,520 | 6.5 | 123.72 | 3 | 46.3 | 134 | 10 | 89 | 2.9 | 1.95 | 72.02 |
| 68 | UNITED STA | us | | 2 | 28,740 | 2.5 | 379.39 | 3.6 | 19.4 | 97 | 10 | 91 | 2.81 | 1.9 | 100.23 |

The Digital Challenge
Summary Table
All Variables

Cell: B1

Comment: 1) ISO Country Code

Cell: D1

Comment: 2) Global Internet Liberties Campaign (GILC) Survey, 1998 (www.gilc.org/survey.html); scores 1=red (controlled) to 5=green (free)

Cell: F1

Comment: 3) GILC Privacy and Human Rights 1998 Survey (www.gilc.org/survey); scores: 1 to 7

Cell: G1

Comment: 4) IP Host Count per Population, World Bank Indicators 1997, Table 5.11

Cell: H1

Comment: 5) Defence Expenditure as % of GDP in USD), SIPRI Yearbook 1998

Cell: I1

Comment: 6) Trade as % of PPP GDP, World Bank Indicators 1997, table 6.1

Cell: J1

Comment: 7) % of Relevant Age Group Enrolled in Secondary School, World Bank Indicators 1997, Table 2.10

Cell: K1

Comment: 8) Polity III Database, 1994 (www.unimich.edu/icpsr/)

Cell: L1

Comment: 9) Individualism Index 1991 Source: G. Hofstede (Software of the Mind). The values of former Yugoslav republics is equal to the value of old Yugoslavia.

Cell: M1

Comment: 10) Results were weighted according to the number of telecom sectors active in each country

Cell: N1

Comment: 11) Index of Economic Freedom. The Heritage Foundation/Financial Times, 1998

Cell: O1

Comment: 12) Multimedia Score. Number of PCs per 100 inhabitants plus number of telephone lines per 100 inhabitants. Source: ITU World Telecommunication Development Report, 1998

Summary Table





