Chapter 8
Access to Information in the Republic of Macedonia:
Between Transparency and Secrecy

Stojan Slaveski
Europian University, Macedonia

Biljana Popovska
MoD, Macedonia

ABSTRACT

Certain information and personal data, held by the government, needs to be kept secret because its disclosure to the general public could jeopardize the operation of the state. On the other hand, the state should allow the public to have free access to all other state-held information. To ensure a balance between these two claims of modern democratic societies, there is a need to legally regulate this matter. The state should have a law on access to public information and a law that will regulate the classification, access to and storage of information which should be kept secret. This chapter analyzes the global experiences in regulating this matter, with a particular emphasis on the practice in the Republic of Macedonia.

INTRODUCTION

Functioning of the society in the modern world is based on interrelated national and international information infrastructures. There is a global trend for integration of communication and information technologies, thus enhancing their efficiency on one hand and their vulnerability on the other. The possibility for failure of system segments entails the danger of interrupting the performances of the system as a whole. Constant increasing of the importance of the information makes the communication and information systems irreplaceable and, at the same time, suitable targets for attack by individuals, groups and states, whose aim is interruption of the normal rhythm of life and society. It is the reason why it is necessary to define a common and comprehensive policy and normative framework for the protection of information and communications.

Information infrastructures are an essential part of the overall infrastructures supporting modern society. These infrastructures and the services they support face increasing security threats.

DOI: 10.4018/978-1-4666-8793-6.ch008

Ever more critical information technologies (IT) resources are supplied and operated in partnership between the public and private sectors and across national borders. In this way, IT and the marketplace for it, have become truly global, and thus have security risks. Unauthorized disclosure, corruption, theft, disruption, or denials of IT resources have the potential to impact the public and private sectors and society as a whole. One of the objectives of every modern society is to promote the development of a culture of security across society. Among all information systems, some are critical because their disruption or destruction would have a serious impact on the health, safety, security, the economic well-being of citizens, or the effective functioning of government or the economy. These information systems constitute the critical information infrastructure (CII).

Commercial, government, and military secrets are part of the background of the modern system. Partly, this secrecy was imposed by governments, but scientists, on their own initiative, practiced self-censorship on matters related to nuclear research. Along with "nuclear secrecy", came another fundamental category "information relating to the national security of the state". So some information that is of great importance for the country needs to be kept secret because its disclosure to the general public could jeopardize the operation of the state.

On the other hand, the state should allow citizens to have free access to all other information. Transparency is one of the linchpins of democracy. It is a particularly important factor for the success of the reforms in the security sector in the Republic of Macedonia. Of the security services it is frequently said that they are "a state within a state", and in some cases "a state above the state". Hence, it is very difficult to change anything until the system is opened up to public scrutiny. When combined with new people and practices, transparency increases public interest in the way security is managed, and in this way contributes to overcoming people's prejudices and fears concerning the security sector. Chapter analyzes the global experiences in regulating this matter, with a particular emphasis on the practice in the Republic of Macedonia. Also it suggests some changes that should be made in order to improve current practice.

CRITICAL INFRASTRUCTURE VERSUS CRITICAL INFORMATION INFRASTRUCTURE

Critical infrastructure (CI) and critical information infrastructure protection have been a focus of attention in many countries in recent years. Many developed countries generally define their critical infrastructure in terms of the criticality of particular sectors or services to the safety and security of their society, government and economy. While countries widely use the term "critical infrastructure", the term "critical information infrastructure" is less common in national policies, strategies and structures. However, "critical information infrastructure" has emerged as a somewhat neutral and general term in the international community although no formal attempt has been made to reach a common definition or understanding. The diversity of input across the different countries does not allow us for a single common formal definition. Most of the countries have formulated policy and developed good practices to safeguard the information systems and networks that can be considered as critical information infrastructure. However, there are different approaches to the problem (Auerswald, Branscomb, Porte, & Michel-Kerjan, 2005).

Many factors such as policy, strategy, and the existing structure of authorities and agencies shape the way governments identify their critical information infrastructure and respond to the need to protect it. These factors reflect the priorities, style and culture of the country and government.