Cyber Security Strategy of Georgia

2012-2015

1. Introduction

The Government of Georgia publishes its Cyber Security Strategy for the first time. Large-scale cyber attacks launched by Russia against Georgia in August 2008 have clearly demonstrated that the national security of Georgia cannot be achieved without ensuring security of its cyberspace.

In the course of the Russian-Georgian war, Russian Federation engaged in targeted and massive cyber attacks against Georgia alongside land, aerial and naval assault. These attacks showed that the protection of cyberspace is as important for national security as land, maritime, and air defenses.

The Georgian Cyber Security Strategy is a principal document outlining state policy in the area of cyber-security, reflecting strategic goals and guiding principles, and laying down action plans and tasks. Based on this Strategy, the Government of Georgia will undertake actions facilitating safe operation of state agencies, private sector and the public in cyberspace, secure electronic transactions and unhindered functioning of Georgian economy and business.

The Georgian Cyber Security Strategy represents a part of the package of conceptual and strategic documents developed in the framework of the National Security Review process. Consequently, the Strategy is based upon the Threat Assessment Document for 2010-2013 and the National Security Concept of Georgia.

The Strategy has been developed by the Permanent Inter-agency Commission under the auspices of the National Security Council tasked to coordinate drafting national security strategic documents.

2. Basic Principles of Implementing the Georgian Cyber Security Policy

The National Security Concept of Georgia defines cyber security as one of the principal directions of its security policy. Georgia aims to set up a system of cyber security that will facilitate resilience of cyber infrastructure against cyber threats as well as will represent additional factor in the economic growth and social development of the country. In this regard, it is necessary to adhere to the following principles of cooperation:

- **Whole-of-Government Approach.** The Government of Georgia attaches great importance to the security policy as well as institutionalization of mechanisms for implementation of the policy components. In this regard, development of cooperation modalities between state agencies is essential for ensuring cyber security, where such modalities facilitate whole-of-government approach and unhindered, coordinated work of different state agencies in planning and implementing cyber security policy.

- **Public-private cooperation.** Development of mechanisms for cooperation extending beyond governmental agencies to public-private partnership is essential for ensuring cyber security. Larger part of critical information systems of Georgia is owned by private businesses and relevant experience and knowledge is mainly available in private companies. Consequently, it is important to develop cooperation modalities that facilitate proper operation of critical information systems as well as will offer additional incentives for economic growth.

- **Active international cooperation.** The Government of Georgia acknowledges that the no single government can solely rely on its own resources in overcoming current challenges and threats to cyber security. Georgia is a part of the global democratic community and therefore is vulnerable to threats against this community. Accordingly, Georgia aims to actively cooperate with its partners on cyber security issues in bilateral and multilateral formats.

3. Cyber Threats and Challenges

Georgia aims to develop a system of information security that is able to minimize harmful effects of any cyber attack and allows rapid recovery of information infrastructure to being fully operational in the aftermath of such attacks.

Establishment of electronic government leads to increased threats and challenges to critical information systems of Georgia. At the same time, Georgia faces global threats and challenges that endanger democratic societies in the international community. Therefore, planning and implementation of the Georgian security policy should pay significant attention to the following threats and challenges in cyberspace:

- **Cyber war.** In 2008, parallel to the military attacks, Georgian cyber space was exposed to the Russian aggression. Potential adversaries of Georgia possess significant capabilities for conducting new types of warfare in cyberspace. At the same time, Georgia faces recurrent risk of massive cyber attacks.

- **Cyber terrorism.** Growing dependence of important areas of Georgian state management and business on critical information systems leads to elevated cyber terrorism threats. Attacks launched in cyberspace against the objects of critical information systems can significantly affect state security.

- **Cybercrime and other security threats.** Security challenges for Georgia include categories of cybercrime directed against critical information systems of Georgia and/or for the purpose of obtaining secret information, economic sabotage and other politically motivated means. Also lower-level acts against information/cyber security that jeopardize access to information and proper operation of information systems.

4. Major Directions of the Georgian Cyber Security Policy

The main directions of the Georgian Cyber Security policy are as follows:

- Research and analysis;
- New legislative and regulatory framework;
- Institutional coordination for ensuring cyber security;
- Public awareness and education;
- International cooperation.

4.1. Research and analysis

It is important to ensure that the legislative drafts, by-laws, guidelines, recommendations and actions undertaken by Georgia in the area of cyber security are based upon research and analysis as a prerequisite for efficiency of the cyber security policy.

In this regard, the following directions of research and analysis are necessary to implement state policy in cyber security:

- Study of other states' best practices and sharing experience;
- Research the criteria and standards to identify objects of critical information systems;
- Resilience analysis of critical information systems;
- Analysis of the problems in the region regarding the cyber security.

4.2. New legislative framework

As of 2012, Georgia has not yet introduced specialized national cyber security laws. It is important to establish legislative framework of cyber security that would facilitate development of effective and efficient security mechanisms.

To improve legislative framework in the field cyber security, it is necessary to undertake the following steps:

- Introduction of legislative acts on information security;
- Development of the regulatory framework to identify the critical information systems and actions necessary for ensuring cyber security;
- Introduction of the legal basis for Computer Emergency Response Team operations;
- Ratification of the 2001 Council of Europe Convention Against Cybercrime;
- Legal identification of an agency or agencies responsible for designation of information security policies and undertaking coordinating functions;
- Development of the contingency plans and recovery procedures.

4.3 Institutional coordination for ensuring cyber security

Ensuring cyber security requires clear definition of functions of the state agencies, establishment of the inter-agency coordination mechanism to implement whole-of-government approach, and public-private cooperation.

The following actions are necessary to ensure the coordination in cyber security field:

- Further development of the Computer Emergency Response Team (CERT.GOV.GE);
- Establishment of the 24/7 high-tech crime (cybercrime) international contact point as required by the 2001Convention against Cybercrime;
- Designation of the expert support team/unit in cybercrime cases;
- Establishment of the format and modalities for public-private cooperation.

4.4. Public awareness and education

An important part of the Cyber Security Strategy of Georgia is to raise the public awareness and increase relevant professional capacity.

In this regard, it is important to undertake the following actions:

- Establishment of the public awareness and educational programs on cyber security;

- Training of the staff and technical personnel of the critical information system subjects and other interested organizations in order to learn international and local standards of information security;

- Training of the specialized cybercrime experts in the area of handling electronic evidence (cyber forensics);

- Support the science and research projects in cyber security;

- Creation of the research lab.

4.5. International cooperation

To develop the international cooperation in cyber security Georgia undertakes the following actions:

- Strengthening relations on cyber security issues with international organizations (OECD, EU, OSCE, NATO, UN, ITU) working in cyber security field as well as relevant national authorities;

- Active participation in international activities related to cyber security and support of the relevant initiatives on a regional scale;

- Initiating bilateral and multilateral cooperation with national CERTs in the area of cyber security.

5. Mechanisms and Time-frames for Strategy Implementation

The Strategy will be implemented in 2012-2015. Agencies responsible for implementation of the Strategy will take into account actions necessary for implementing this Strategy within relevant policy areas.

Results of the Strategy implementation will be assessed annually and the annual assessment report will be presented to the Permanent Inter-agency Commission for coordination of drafting national security strategic documents at the National Security Council of Georgia.

Action Plan for the Cyber Security Strategy of Georgia (2012–2015)

#	Goal	Activity	Period	Responsible agency
1	**Research and analysis**			
1.1		Study of other states' best practices and sharing experience	2012	Data Exchange Agency
1.2		Research into criteria and standards for identifying objects of critical information systems	2012	Data Exchange Agency
1.3		Resiliency analysis of critical information systems	2012	Data Exchange Agency
1.4		Analysis of the problems in the region regarding the cyber security.	2012-2013	Data Exchange Agency
2	**New legislative framework**			
2.1		Initiating legislative acts on information security	2012	Ministry of Justice
2.2		Laying down regulatory framework for identifying critical information systems and actions necessary for ensuring cyber security	2012-2013	Ministry of Justice

2.3		Ensuring legal basis for Computer Emergency Response Team operations	2012	Ministry of Justice
2.4		Ratification of the 2001 Council of Europe Convention Against Cybercrime	2012	Parliament
2.5		Identifying, by legal act, an agency or agencies whose competence includes designation of information security policies and undertaking coordinating functions	2012-2013	Relevant state agencies
2.6		Developing cyber security disaster recovery plans and procedures	2013-2015	Relevant state agencies
3	**Institutional coordination in cyber security**			
3.1		Further development of the Computer Emergency Response Team (CERT.GOV.GE)	2012	Data Exchange Agency
3.2		Establishment of the 24/7 high-tech crime (cybercrime) international contact point as required by the 2001Convention against Cybercrime	2012-2013	Ministry of Internal Affairs
3.3		Designation of the expert support team/unit in cybercrime cases	2013	Relevant state agencies
3.4		Establishing format and modalities for public-private cooperation	2013-2014	Data Exchange Agency
4	**Public awareness and**			

	education			
4.1		Establishment of public awareness and educational programs on cyber security	2012-2015	Data Exchange Agency, Ministry of Education and Science and international assistance
4.2		Training of staff and technical personnel of critical information system subjects and other interested organizations in international and local standards of information security	2012-2015	Data Exchange Agency and international assistance
4.3		Specialized training of cybercrime experts in handling digital evidence (cyber forensics)	2012-2015	Relevant state agencies and international assistance
4.4		Facilitating science and research projects in cyber security	2012-2015	Data Exchange Agency, Ministry of Education and Science and international assistance
4.5		Creation of the research lab	2014-2015	Relevant state agencies and international

				assistance
5	**International cooperation**			
5.1		Strengthening relations in cyber security matters with international organizations working in cyber security (OECD, EU, OSCE, NATO, UN, ITU) as well as relevant national authorities	2012-2015	Ministry of Foreign Affairs, Data Exchange Agency, National Security Council administration, other state agencies
5.2		Active participation in international activities related to cyber security and supporting relevant initiatives on a regional scale	2012-2015	Ministry of Foreign Affairs, Data Exchange Agency, National Security Council administration, other state agencies
5.3		Initiating bilateral and multilateral cooperation with national CERTs in the area of cyber security	2012-2015	Data Exchange Agency and CERT Georgia