UN General Assembly Resolution 68/243

GEORGIA

General appreciation of the issues of information security

Widely publicized cyber attacks – and, to some expert opinions, cyber war - conducted against Georgia in 2008 put the protection of the critical infrastructure high on agenda of the Government of Georgia. Rapidly growing dependence of the critical infrastructure and government services on the IT increases vulnerability to cybercrime-related incidents. Accordingly, adequate protection of critical infrastructure from cyber threats is one of the priorities of the Government of Georgia.

The first targets of cyber attacks in 2008 were government and news media websites. Later, the attacks were expanded to include many more government websites, Georgian financial institutions, business associations, educational institutions, more news media websites and a Georgian hacking forum. These cyber attacks were intended to interrupt normal business operations. Nearly all of the most important government websites were successfully attacked, including the web-page of the President of Georgia, Ministries, Courts and Parliament. Apart from the two big banks, the business related targets were primarily organizations that could have been used to communicate and coordinate responses among different businesses. The educational institutions attacked included those devoted to science, technology and medicine. Five of the Georgian government websites, along with the national bank, were defaced with political propaganda.

The above described experience demonstrates that cyber attacks on the critical infrastructure of Georgia by state and private actors can cause a serious physical damage as well as significant financial damage for the public and private sectors. Therefore, Government of Georgia considers information/cyber security to be part of the general security policy of the country, especially in the view of its increased reliance on the IT as a vehicle for delivery of government services.

Voicing these concerns, the National Security Council hosted series of meetings of the special working group comprised of different Government agencies to develop the national Cyber Security Strategy of Georgia throughout 2011, as a part of the National Security Review. The Cyber Security Strategy and Action Plan for its implementation, presented to the public for discussion in March 2012 and finally adopted in January 2013 following a series of consultations on national and international levels, is a further testament of the high awareness of the Government of Georgia of information security matters.

A further step in institutionalizing information security was the establishment of the Data Exchange Agency of the Ministry of Justice of Georgia in 2010 as a central government entity responsible for development and implementation of e-governance policies and solutions. An important part of Agency’s mandate is information security for the public sector and the private entities (where the latter are a part of critical infrastructure), which includes:
• Adoption and implementation of information security policies and standards in public sector and critical infrastructure;
• Providing consultancy services in the field of information security and performing information security audit;
• Awareness raising activities about information security issues in public as well as civil sector;
• Cyber security mandate though national Computer Emergency Response Team (CERT).

**Efforts taken at the national level to strengthen information security and promote international cooperation in this field**

Besides already noted institutionalization of the information security matters through creation and operation of the Data Exchange Agency, further efforts were taken by the Government of Georgia to increase the level of protection of its information assets. Namely, in July 2012, the Law on Information Security has been adopted by the Parliament of Georgia, following preliminary and in-house consultations with the private and non-governmental players. The Law on Information Security is a central reference document for enforcing information security at government and private sector players comprising critical infrastructure, through adoption of internal policies, minimum standards, asset management, auditing, penetration testing, CERT operations, assignment of personnel, training and other related matters. The Law accords equal importance to both information and cyber security matters, treating them as an integral whole. The Law is currently under the process of revision in order to strengthen the implementation of regulations that pertain to the protection of confidential and internal use information at the critical information system subjects.

Besides already noted institutionalization of the information security matters through creation and operation of the Data Exchange Agency, further efforts were taken by the Government of Georgia to increase the level of protection of its critical information assets. The Data Exchange Agency has completed a large-scale project of information security policy development and implementation at the Ministry of Justice of Georgia in 2012. Similar projects are ongoing in the Ministry of Economic Development, Ministry of Health, Labor and Social Affairs and the Parliament of Georgia.

As regards protection of critical information systems objects from terrorism, sabotage and other cyber threats, there are separate agencies that deal with such threats. Terrorism and all its forms fall under exclusive competence of the Ministry of Internal Affairs of Georgia. All other incidents that involve sabotage or otherwise are directed against critical information systems are handled by the Data Exchange Agency of the Ministry of Justice of Georgia. Under “handling of incidents”, it is meant that the CERT.GOV.GE, operating within the Data Exchange Agency, takes steps to study, describe and respond to each incident, including prevention and mitigation of consequences. Whether these acts are legally assessed as a crime of sabotage or
cybercrime is a separate matter that is to be decided by the Ministry of Internal Affairs that has investigative jurisdiction over such offences.

Since the concepts of information and cyber security have been only recently introduced in Georgia, most of issues related to protection of critical information systems against cyber threats involve a common approach involving both information and cyber security dimensions. Such measures, most of which are provided as services of the Data Exchange Agency, include the following:

1. Information Security Services:
   a. Awareness raising activities in both critical information system subjects, the rest of the government, local IT businesses and the general population (PSAs, calendars, meetings, presentations, Cyber Security Forum, etc.)
   b. Supporting government agencies in adoption of Information Security Policies as well as implementation (asset management, policy reviews, etc.)
   c. Developing state-wide standards and procedures for Information Security through legislation and by-laws (based on ISO 27000 family of standards);
   d. Delivery of initial training course on Information Security to government officials representing critical infrastructure.

2. Cyber Security Services (provided mostly through CERT.GOV.GE):
   a. Responding to cyber incidents on request cyber incidents;
   b. Monitoring Georgian cyberspace and analyzing cyber resources for vulnerabilities;
   b. Providing Penetration Test Service on the basis of written contract;
   c. Providing IP monitoring services for identification of malicious traffic;
   d. Conducting Static Source Code Analysis services;
   e. Malware Analysis Service;
   f. Providing training in Incident Handling to critical information system representatives.

All of these services are currently available for the critical information system subjects, as well as for the rest of the Government agencies who wish to avail themselves of obligations and benefits deriving from the Information Security Law. Some examples of currently offered and implemented services are listed below.

No training master plan has been put into place on the level of the government. However, the Data Exchange Agency, on its own accord and funding, has started to deliver basic training to state agencies identified as critical in terms of information system operation. Staff members of the Information Security Department of the Data Exchange Agency, who have proven and certified experience in their respective areas, conduct trainings on matters of information security policy drafting, internal audit, asset management, and other subjects covered by ISO 27000. Several groups of representatives of state agencies have been already trained and received relevant certificates of completion of the course. This program will be continued for other agencies as well.
CERT trainings have been delivered to a mixed group of IT personnel from both government and private agencies which represent critical information systems. Incident response and analysis have been the major topics covered. The training was conducted by the CERT staff of the Data Exchange Agency and participants received certificates as well.

Data Exchange Agency actively takes part internationally in training and educational development programs in information and cyber security. Particularly noteworthy is DEA’s contribution to NATO Science for Peace and Security (SPS) Program; with the partnership of NATO SPS and the Informatics Institute of the Middle East Technical University (METU) in Ankara, DEA regularly provides trainings in information and cyber security to foreign participants. In 2013, DEA has trained representatives from Afghanistan, Montenegro and Macedonia; trainings for Moldovan professionals are planned in January 2014.

No cyber exercises involving blue/red team scenarios of cyber attacks and defense have been conducted so far. However, at the first two meetings of the Cyber Security Forum (July 2012 and June 2013), the participants agreed to organize and participate in these exercises in the framework of the Forum educational activities. The Cyber Security Forum is a public-private initiative aimed to bring together leading experts from the entire IT industry in Georgia and exercises will be the first tangible result part of this partnership.

Penetration testing has been conducted at several government agencies as a part of target hardening of critical information systems. All tests have been conducted on a basis of formal agreements and the results have been duly reported to the beneficiary institutions. Since penetration testing is performed on the condition of confidentiality, these institutions cannot be identified in this report.

The Cyber Security Strategy of Georgia has been already noted above. However, an integral part of the Strategy is also its Action Plan for implementation, which lists research, training, institutional coordination, legislative framework and international cooperation activities as basic pillars upon which the cyber security will be built throughout 2012-2015.

Besides, Georgia has adopted specialized cybercrime legislation to ensure compliance with the 2001 Council of Europe Convention against Cybercrime (the Budapest Convention). Numerous changes were entered into the substantive and procedural criminal law in 2010; in 2011, specialized investigative unit (high-tech crime unit) was created within the national police force; since 2009, numerous training and awareness raising activities were undertaken with the support of the Council of Europe and the European Union. Georgia has ratified the Budapest Convention in 2012 to avail itself of all cooperation modalities available under the Convention to effectively fight cybercrime.
on an international level; the Convention went into force for Georgia on 1 October 2012.

**Concepts aimed at strengthening the security of global information and telecommunication systems**

Major concepts used by Georgian legislative and regulatory framework, as well as internal documents detailing information security policies, are fully derived from the ISO 27000 family of standards, down to the interpretation of the terms used. All practical policy documents developed in this regard use the language of ISO 27000 to the maximum extent.

In addition, the Law on Information Security that was adopted by the Parliament and went into force on 1 July 2012, offers a range of new terms and concepts related to information security. E.g. information security is defined as “a unity of actions aimed at maintenance of state defense capabilities, economic security, normal functioning of state and society”, while information security policy is a set of “provisions, principles and practices contained in [Information Security] Law, other normative acts of Georgia and international agreements, aimed at maintenance of state defense capabilities, economic security, normal functioning of state and society, and protection of individuals in the context of current and potential information risks and threats”. Cyberspace is defined as an “environment characterized by use of electronic devices and electromagnetic spectrum for storage, alteration or exchange of data by use of networked systems and supporting physical infrastructure”, and cyber attack – as an “action that uses electronic device and/or connected network or system in order to breach integrity of critical information systems, property or functions, as well as to obstruct, destroy or illegally obtain information from such systems, property or functions”. Real or potential violations of information security policy that is carried out by use of information technology and causes unauthorized access to information, information leakage, suspension of service or appropriation of resource are defined as “computer (cyber) incident”.

Finally, the concepts related to information classifications under the Law on State Secrets of Georgia, as well as management of classified information assets, are thought to be in full compliance with NATO standards applicable, and use the same language to a large extent.

**Possible measures that could be taken by the international community to strengthen information security at the global level**

Georgia has consistently maintained that current threats to and trends of information security are to be dealt with on the basis of already existing principles, agreements and customs of Public International Law, including mechanisms provided by the Charter of the United Nations (in particular, Chapter VII) and Articles on Responsibility of States for
Internationally Wrongful Acts. Doing otherwise, i.e. adopting separate instruments of information and/or cyber security will cause unnecessary and undesirable fragmentation of information security issues from the core issues of global security, where they naturally belong. Challenges to information and cyber security of states need to be dealt with the same principles in mind that are used for other threats against state and global security.

We wish to underline that Georgia sees the ISO 27000 family of standards as a cornerstone of information security and as an accepted and practically tested set of consolidated rules and best practices that, if implemented globally, will have tangible preventive effect against global and local threats to information and cyber security. Wide adoption of national and organizational rules in compliance with ISO 27000 will also have a positive effect in harmonizing measures for handling information security incidents and thus will help to develop efficient international cooperation in these important matters.

Finally, wider accession to/ratification of the 2001 Council of Europe Convention against Cybercrime by the global community – a possibility that the Convention itself leaves open – will be an important step toward deterring and combating modern information and cyber security threats.

**Executive summary**

Against the background of cyber-war of August 2008, the Government of Georgia considers information/cyber security to be part of the general security policy of the country, especially in the view of its increased reliance on the IT as a vehicle for delivery of government services. Therefore, Georgia took steps to develop a National Cyber Security Strategy and its Action Plan (adopted in 2013), which is an integral part of the National Security Review process, and established a central government entity tasked with information security policy and implementation – the Data Exchange Agency (in 2010).

The reference point for specific efforts and activities in information and cyber security is the Georgian Law on Information Security, adopted in 2012. As a main implementer under the Law, the Data Exchange Agency is enforcing information security at government and private sector players comprising critical infrastructure through help with adoption of internal policies, setting minimum standards, conducting asset management, auditing, penetration testing, CERT operations, as well as delivering training to the institutions in question.

Major concepts used by Georgian legislative and regulatory framework, as well as internal documents detailing information security policies, are fully derived from the ISO 27000 family of standards, including interpretation of terms. The Georgian Law on Information Security and its implementing acts are a central reference for the terms
such as information security, critical information subject, cyberspace, computer incident and others.

The Government of Georgia repeatedly maintains that current threats to and trends of information security are to be dealt with on the basis of already existing principles, agreements and customs of Public International Law, including mechanisms provided by the Charter of the United Nations (in particular, Chapter VII) and Articles on Responsibility of States for Internationally Wrongful Acts. ISO 27000 standards and the Council of Europe Convention on Cybercrime are also equally important mechanisms for ensuring information and cyber security at international, regional and local levels.