DEFENDING
Cyberspace *in Georgia*

A strong cyber defense requires infrastructure, legal support and multinational cooperation

BY ANDRIA GOTSIRIDZE,
director of the Cyber Security Bureau, Georgia Ministry of Defense

The cyberspace domain is growing rapidly, and with it the level and complexity of the threat to states, their information technology (IT) systems and associated critical infrastructure. Likewise, the number of cyberspace actors has grown, widening the scope of attack methods and the number of potential targeted systems. Government information/communication networks, military, and commercial projects are becoming more vulnerable to cyber attacks or cyber espionage. Governments must respond by building stronger cyber defense systems.

For a country like Georgia, in the process of ongoing digitization, these trends are a major concern, as is the potential deployment of cyber assaults by adversaries in recent conflicts and in geopolitical confrontations.

Georgia's government building in Tbilisi, where the government has adopted a cyber security policy that stresses cooperation among state, private and international organizations. REUTERS

THE THREAT

The use of cyber elements to achieve political, economic or military goals — or for gaining geopolitical advantage — is a modern day reality. Georgia's cyberspace is no exception. The nation's critical infrastructure, existing information systems, networks and infrastructure belonging to other countries and international organizations, along with foreign commercial structures, are all targets because of Georgia's membership in anti-terrorist coalitions and the Euro-Atlantic course it has taken.

The following actors pose a potential threat:

- Countries with a highly developed offensive cyber potential (Especially from Russia)
- Cyber operations of terrorist organizations
- Financially motivated cyber criminals

Cyberspace has become an important component of war and conflict. Because the Kremlin considers Georgia to be within its sphere of influence, protecting our cyberspace should be a top national security priority. Cyberspace is one sphere where a small country can confront a much larger aggressor and mount an asymmetric response.

CYBER SECURITY INFRASTRUCTURE

Good cyber defense requires a sizable investment, starting with the development of cyber architecture and modern strategic documents and ending with the integration of cyber capabilities into military operations. Georgia fully supports NATO's position that the first step toward successful joint cyber security development is building one's own cyber defense mechanism.

Georgia's first cyber security strategy and action plan was developed in 2013. This 2013-2015 document defines Georgian government policy on cyber security, reflecting the strategic goals and main principles, as well as establishing action plans. The primary strategy goal is cooperation among state, private and international organizations. Cyber security strategy involves five essential elements: research and analysis, a legal foundation, coordination on an institutional level, raising public awareness with outreach and education, and international cooperation.

At the end of 2015, at the initiative of the State Security and Crisis Management Council, Georgia's Cyber Security Strategy and Development Action Plan (2016-2018) was developed. It covers new projects and necessary events to provide cyber security.

Legal framework

The main legal framework for the sphere of cyber security is the law on information security — the purpose of which is to support effective implementation of information security, establish duties and responsibilities for the public and private sectors, and establish state control mechanisms that ensure information security policy. The law defines the Data Exchange Agency and Cybersecurity Bureau of the Ministry of Defense (MoD) as the government agencies responsible for the country's cyber security.

Under the Criminal Code of Georgia, unauthorized access to computer information; creation, utilization or distribution of malware; and the exploitation of network systems are considered crimes, as is cyber terrorism. On the international level, in 2012 Georgia ratified the Convention on Cybercrime, which was developed by the Council of Europe. Georgia now shares the common governing principles of the convention's member states and aims to create a comprehensive legal foundation on the national level while strengthening international cooperation.

Institutional infrastructure

The "Law of Georgia on National Security Planning and Coordination" defines information security as a component of national security and designates the National Security Council and the State Security and Crisis Management Council as the national security policy planning bodies. The National Security Council is a presidential advisory body, headed by the president, created to manage military development and the country's defense.

After the 2009 Russo-Georgian war, a national security review process began in coordination with the National Security Council. Cyber security was recognized as an important component of national security, and the National Security Council took on the responsibility of coordinating cyber security on a national level. However, after constitutional changes in 2014, the prime minister became the head of government. An advisory board to the Prime Minister State Security and Crisis Management Council was created, and cyber security became its responsibility. The council manages information security and is responsible for identifying and preventing internal and external threats. It also coordinates the development of a national strategy for cyber security.

In 2010, the Data Exchange Agency (DEA) of the Ministry of Justice was established to develop standards in Georgia for e-governance, data exchange infrastructures and the information and communication spheres, along with creating and implementing an information-security policy. The data exchange agency is one of the main bodies responsible for the implementation and

development of cyber security. It is within the agency's purview to ensure the cyber security of the entire government network (except for the defense sphere), which includes 36 critical infrastructure concerns.

The Computer Emergency Response Team (CERT) operates under the DEA and is responsible for responding to cyber incidents and monitoring the functionality of Georgia's governmental network. CERT has the right to demand access to critical information systems or assets. DEA sets minimum information security requirements for critical information systems.

Criminal prosecution and cyber crime investigations are conducted by the Central Criminal Police Department Division for the Fight against Cybercrime (of the Ministry of Internal Affairs). The division staffs the 24/7 contact point, which exchanges information about cyber crime with members of the Council of Europe Convention on Cybercrime.

Georgia fully supports NATO's position that the first step toward successful joint cyber security development is building one's own cyber defense mechanism.

Implementation

In 2014, the Cyber Security Bureau implemented a cyber security policy that defines Georgia's defense sector approaches and priorities for cyber security and strategic issues, and the execution of effective, stable and secure functioning of the defense sector. Since then, the Cyber Security Bureau of the MoD has been developing effective and secure information and communication technology systems for the Civil Office of the MoD and for structural subdivisions of the military's general staff. The bureau's Computer Security Incident Response Team monitors and protects the MoD's critical information and communication technology infrastructure from cyber threats and risks.

A Cyber Security Development action plan was developed based on the cyber security policy. It includes the Cyber Security Bureau's main objectives for the years 2016-2018: effective development of cyber defense capabilities, awareness building, inter-division coordination, creation of the necessary legal framework, and deepening of international cooperation. The main objective is to ensure information confidentiality, authentication and unity, including the defense of human rights.

COOPERATION

An analysis of recent conflicts involving Russia makes clear the challenges Georgia will face while developing cyber capacities. The primary challenge, as noted above, is integration of cyber security into broader strategic and practical aspects, within offensive, as well as defensive operations. Unfortunately, the best example of strategic integration that NATO can provide is Russia's actions during the Ukraine crisis. The cyber element, as events in Ukraine have shown, plays a key tactical role and is being utilized with greater frequency. The recent incorporation of cyberspace within military training, and the involvement of government departments in international cyber exercises, bodes well for cyber security development in Georgia.

The first time cyber-defense elements were used was during Exercise Didgori in 2014-2015. Alongside the general staff of Georgia were the Ministry of Internal Affairs, the State Security and Crisis Management Council and other agencies.

For the development of the Georgian Cyber Defense sphere, cooperation in information sharing, participation in technical exercises such as Locked Shields and Cyber Coalition, valued cooperation with the NATO Cooperative Cyber Defence Centre of Excellence, as well as participation in NATO Smart Defense programs, are of vital importance. In 2014, the bureau's representatives participated in the above-mentioned exercises as observers. Georgia is looking forward to strengthening cooperation with NATO in order to become full participants in Alliance exercises.

The 2014 NATO Summit in Wales asserted the fundamental importance of cyber security to NATO's future and the development of a unified defense. The Alliance has declared that joint cyber operations are not only desired but necessary. Georgia, which has experienced the results of cyber attacks and cyber espionage, realizes the importance of cyber security and shares NATO's understanding that cyber security is a global challenge that transcends national borders and demands cooperation on an international level. □