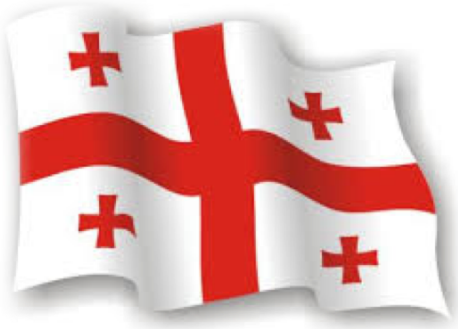


New Cybersecurity Strategy of Georgia

Tallinn E-governance Conference

Giorgi Tielidze

Tallinn
2016

Importance of Georgian Cybersecurity Strategy

- Cyber Strategy Constitutes the Main Document Defining State Policy and Priorities as well as Measures for Their Implementation;
- Cybersecurity Strategy is Based on National Threat Assessment Document – Guiding Document Defining and Measuring National Security Threats facing Georgia.

Main Parts of the Strategy

- Introduction;
- Goals and Principles;
- Georgian Cybersecurity Environment (Current Threat Landscape);
- Main Directions of Georgian Cybersecurity Policy;
- Action Plan

Goals and Principles

GOALS:

- Ensuring Cybersecurity System Confidentiality, Integrity and Availability
- Ensuring Mitigation of Negative Results entailed by Cyber Attacks and Fast Recovery Thereby;

PRINCIPLES:

- Cybersecurity as Integral Part of National Security;
- Whole of Government Approach;
- Active Public-Private Partnership and International Cooperation;
- Provision of the Tools Necessary for Implementing the Goals and the Priorities set forth in the Strategy;

Current Threat Landscape and Threat Actors

- Cyberwar – 2008 August Experience;
- Attacks Directed Against Critical Information Infrastructure;
- Cyber Espionage and Theft of Other Sensitive Information – Georbot Case
- Most Serious Cybercrimes and Cyber-Enabled Offences.
- ***Primary Adversary of Georgia in Cyber Domain is the Russian Federation;***
- ***Kremlin Carries Out Well-Organized PSYOPs against Georgia in Cyberspace.***

Main Directions of Georgian Cybersecurity Policy

- Research and Analyses;
- Modernizing Legal Framework;
- Cybersecurity Capacity Building;
- Raising Public Awareness;
- Strengthening International Cooperation.

Research and Analyses

- Regular Assessment of the Cyber Threats;
- Analyses of Sustainability of Critical Information Infrastructure;
- Testing the Readiness of Relevant Agencies in Times of Cyber Incident Related Crisis.

Legal Framework

- Regulations Aiming Strengthening Critical Information Infrastructure Sustainability;
- Regulations on Information Classification Issues;
- Procedures Prescribing Roles and Responsibilities in time of Crisis.

Capacity Building

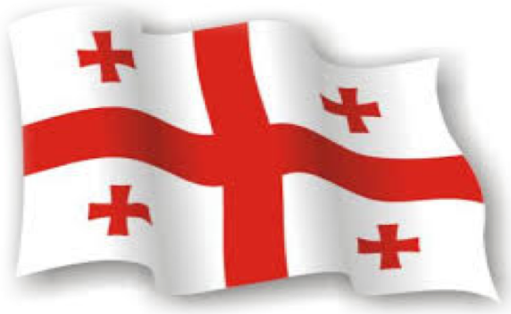
- Establishment of Cyber Lab;
- Creation of Cyber Reserve Program;
- Institutionalizing PPP Cooperation Process;
- Launching Special Trainings and Exercises Focused on Practical Aspects of Cybersecurity Assurance.

Raising Public Awareness and Enhancing International Cooperation

- Launching Awareness Campaigns using Media Channels;
- Trainings of Public Employees Regarding Basic Norms of Cybersecurity;
- Creation of Graduate and Postgraduate Cybersecurity Programs;
- Enhancing International Cooperation on Bilateral and Multilateral Level;
- Establishment of Regional Cybersecurity Research Center;

Implementation Tool – Action Plan

- Action Plan - Integral Part of the Strategy;
- Valid for 2016-2018;
- Action Plan Defines Time, Resources and Responsible Agency (Agencies) for Achieving the Goals provided by the Strategy;
- Performance Indicators as the Progress Measurement Tool.



Thank You For Your Attention!