CYBER SECURITY IN GEORGIA – CURRENT TRENDS AND FUTURE PLANS

David Kvatadze
Strasburg, 21 November 2019

INTERNATIONAL RECOGNITION OF GEORGIA'S CYBER ACHIEVEMENTS

ITU Global Cyber security Index 2017:

Georgia is in TOP TEN most committed countries in the world

Country
GEORGIA

Rank in Europe: **2**
Rank Worldwide: 8

- 0.91 Legal
- 0.77 Technical
- 0.82 Organizational
- 0.9 Capacity Building
- 0.7 Cooperation

Other Countries:

Country	Ranks EU	Score	Legal	Technical	Organizational	Capacity Building	Cooperation
ESTONIA	1	0.84	0.99	0.82	0.85	0.94	0.64
FRANCE	3	0.81	0.94	0.96	0.6	1	0.61
NORWAY	4	0.78	0.96	0.89	0.64	80.8	0.57

DEVELOPMENT OF A THIRD NATIONAL CYBERSECURITY STRATEGY 2020 - 2022 IS ONGOING

CYBERCULTURE, EDUCATION, AWARENESS RISING IN INFORMATION SOCIETY

PUBLIC-PRIVATE PARTNERSHIP, INFORMATION SHARING

SUSTAINABILITY OF CRITICAL INFORMATION SYSTEMS AND WHOLE GOVERNANCE MODEL

INTERNATIONAL COOPERATION, CENTER OF EXCELLENCE

CYBERSECURITY CAPACITY REVIEW BY GCSCC

Global Cyber Security Capacity Centre

CYBERSECURITY CAPACITY REVIEW OF GEORGIA BASED ON CYBERSECURITY CAPACITY MATURITY MODEL (CMM) 2018 -2019

❑ Dimension 1 - Cybersecurity Policy and Strategy

❑ Dimension 2 - Cyber Culture and Society

❑ Dimension 3 - Cybersecurity Education, Training and Skills

❑ Dimension 4 - Legal and Regulatory Frameworks

❑ Dimension 5 - Standards, Organisations, and Technologies

CMM RECOMMENDATIONS CONVERTED TO THE ACTIVITIES OF THE NATIONAL CYBER SECURITY STRATEGY

ORGANIZATIONAL FRAMEWORK

State Security and Crisis Management Council

Established in January 2014
Under the Direct Subordination of the Prime-Minister

Personal Data Protection Inspectorate

Established in January 2013

Ministry of Justice
Data Exchange Agency

Established in January 2010
Under Supervision on Ministry of Justice

Ministry of Internal Affair
Cyber Crime Division
24/7 International Contact Point

Established In December 2012 as a
Structural Unit of the Ministry of Internal Affairs
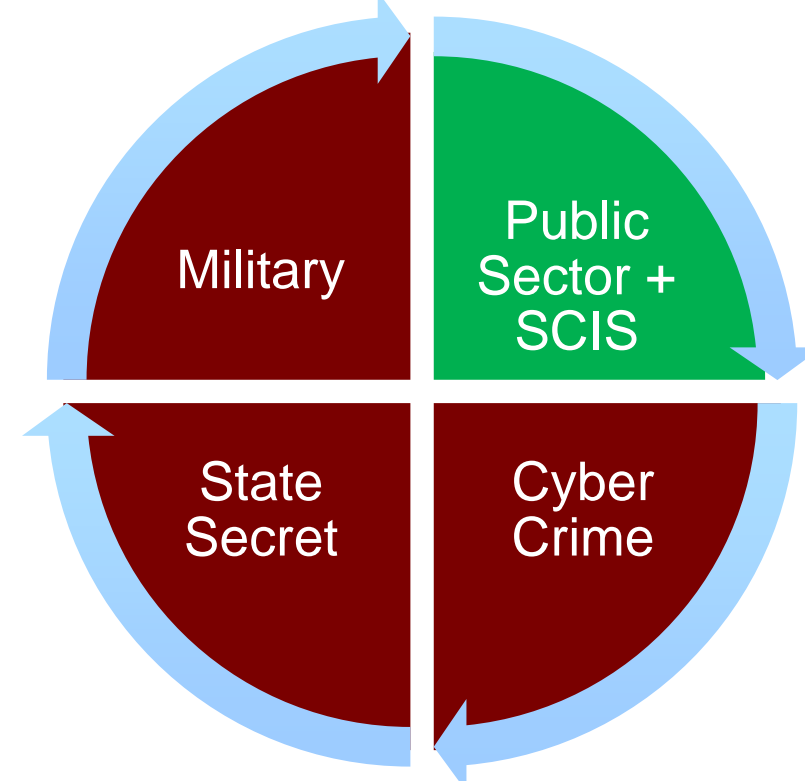
State Security
Service of Georgia
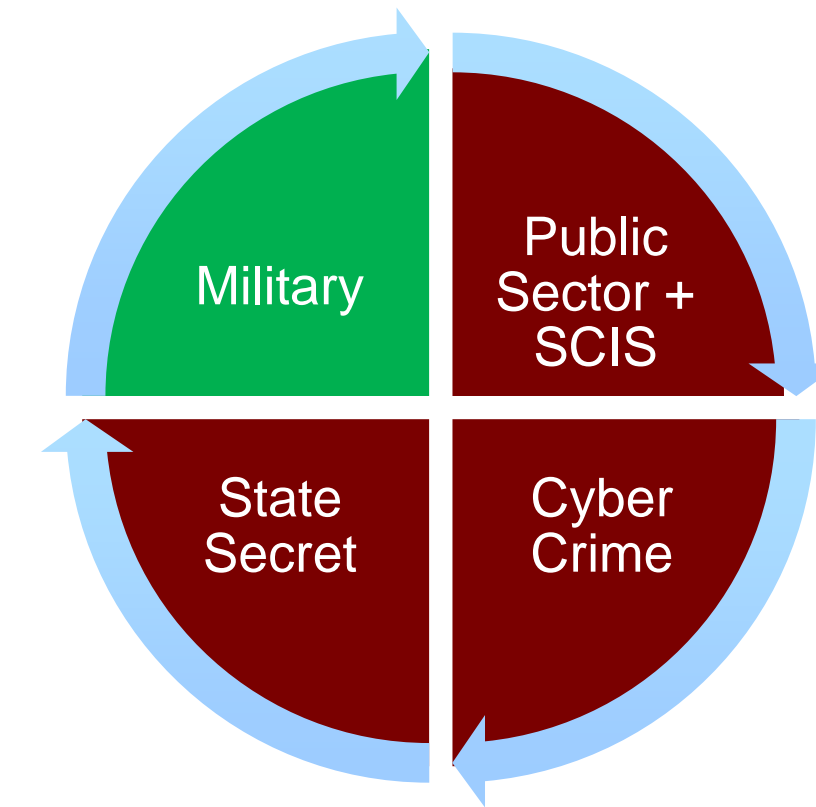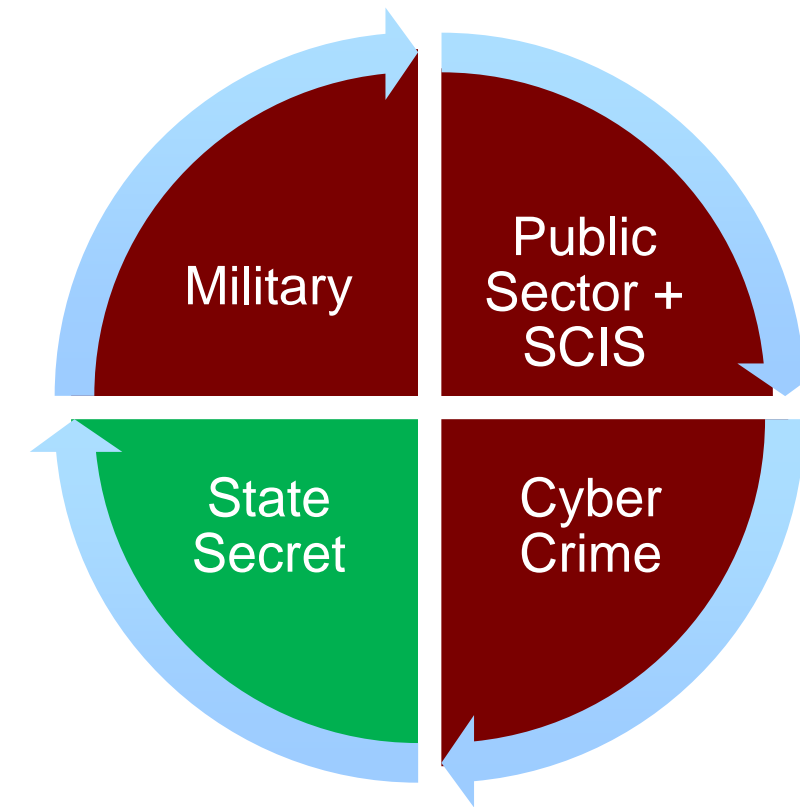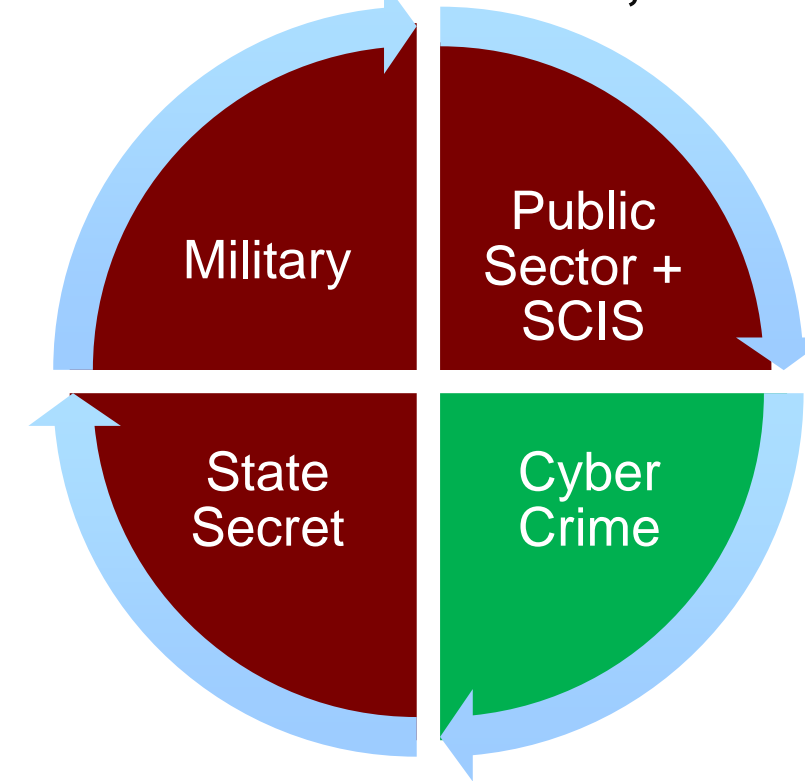
Established In 2015

Minister of Defense
Cyber Security Bureau

Established in 2014 Under Supervision of Ministry of Defense of Georgia

Information Security Development.
and management of CERT.GOV.GE

Cybercrime division is the only agency that has Investigatory functions on all types of Cyber Incidents;

CRITICAL INFORMATION SYSTEM SUBJECTS IN GEORGIA

GOVERNMANT → BANKING&FINANCE ENERGY SECTOR INFORMATION&COMMUNICATION → HEALTH SERVICES

CYBER SECURITYSERVICES FOR CISS

Blacklist Service

IP and Domain blacklist.

Different formats for different software.

Available for Organization's.

http://blacklists.cert.gov.ge

Network Monitoring Services

NetFlow Sensors (NfDump & NfSen)
Network Analyze NetFlow Data For Security.
Detects:
- ✓ SSH Brute Force Attacks.
- ✓ Botnets.
- ✓ dDoS Attacks.

Safe DNS & Safe Internet

Integrated with Collective Intelligence Framework.

Blocks malware domains and redirecting to warning page.

First DNSSEC Enabled Resolver In Georgia.

5.159.16.16
5.159.20.20

IDS Network Sensors

- ✓ Automated analysis of the security of the network flow problems.
- ✓ VRT rules of the Securities and install for free.
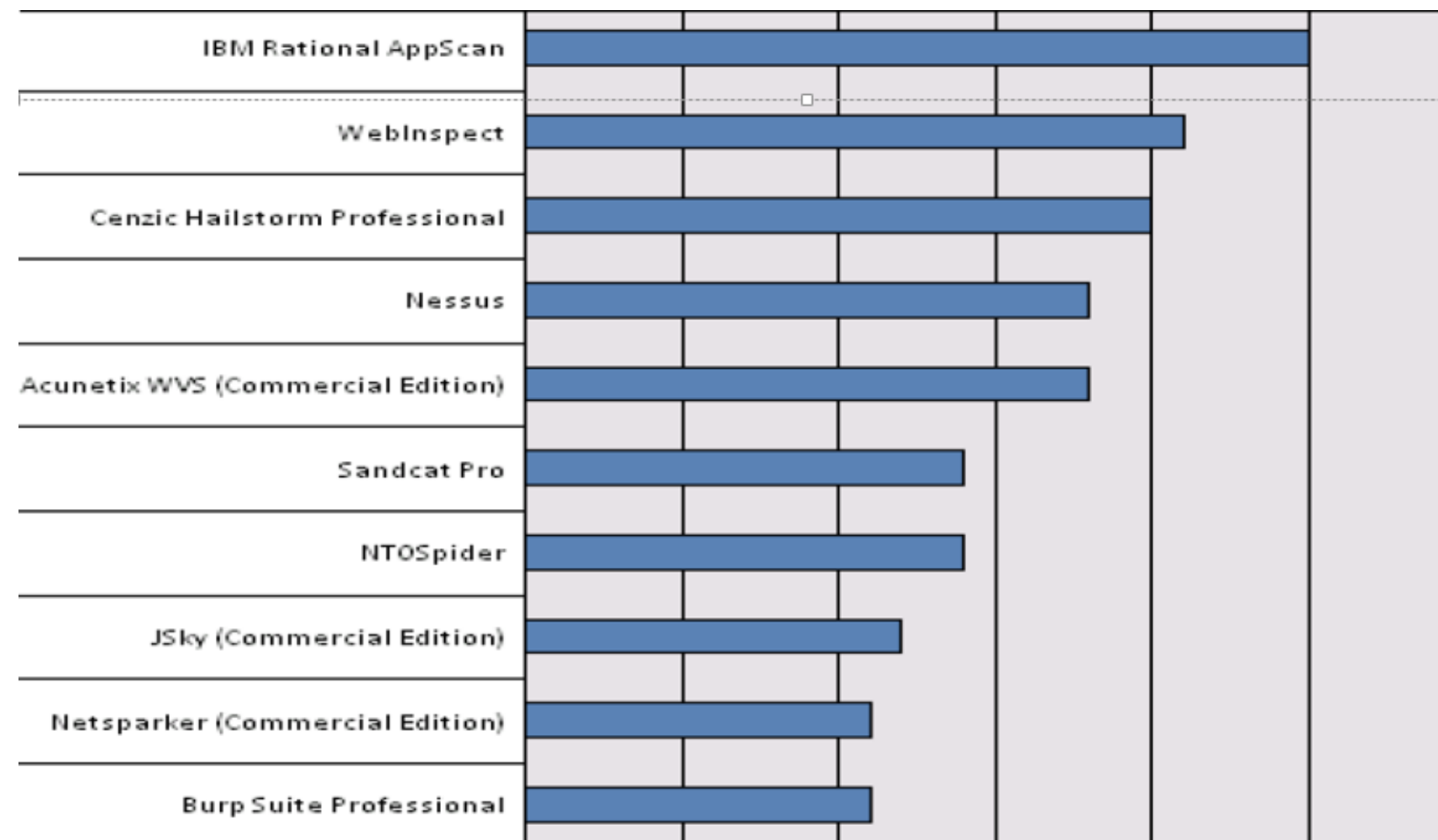- ✓ If you wish to separate physical server for the organization.

CRITICAL INFORMATION SYSTEM SUBJECTS IN GEORGIA

Fishing As A Service

- Sending e-mail phishing links.
- Phishing attacks by the organization to personalize.
- Any WEB mobile Simulation Built-in educational page.
- Statistics.

Web App & Network Penetration Test

INFORMATION SHARING FOR CISS

TRAININGS FOR CISS

➔ **3 Day Course for our CISS:**

- **CSIRT introduction**
- **Incident Handling**
- **Basic Malware Analysis**
- **Sysinternal Tools**
- **Forensics with Linux**
- **Forensics with Windows**
- **Case Studies**
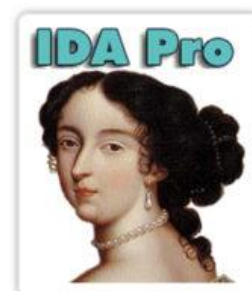
CYBER EXERCISES FOR CISS

Cyber EXE Topics:

➢ **Cryptography**
➢ **Malware Analysis**
➢ **Log File Analysis**
➢ **Reverse Engineering**
➢ **Network Analysis**
➢ **Various Content**

Number of Exercises:

➢ **32 Case**
➢ **88 Questions**
➢ **6 Houers and 15 Minutes**

Recommended Tools and Applications:

Data Exchange Agency:
Address: University Street#50, Tbilisi, Georgia
Phone: +995 (32) 2 91 51 40
E-mail: cert@dea.gov.ge   dkvatadze@dea.gov.ge
Web: www.dea.gov.ge / www.cert.gov.ge
FB.: მონაცემთა გაცვლის სააგენტო • Data Exchange Agency / CERT.GOV.GE