Georgian Cyber Defense and Cyber Resilience

Lessons learned from the war and post-war situation

Office of the National Security Council of Georgia

Department of Information and Cybersecurity

David Sakhvadze. Telč , October 6, 2022

2008 Georgia-Russia War cyber dimension

Prior to and during the 2008 August war Russia used cyberattacks to halt communications, take down internet resources and disinform population in Georgia.

Georgia partially repelled cyberattacks – mirroring official internet sites on abroad servers and using additional resources (regular official TV statements) to avoid population disinformation.

In 2008 Georgian public/private services and population digitalization level were moderate and Russian cyberattacks achieved limited success.

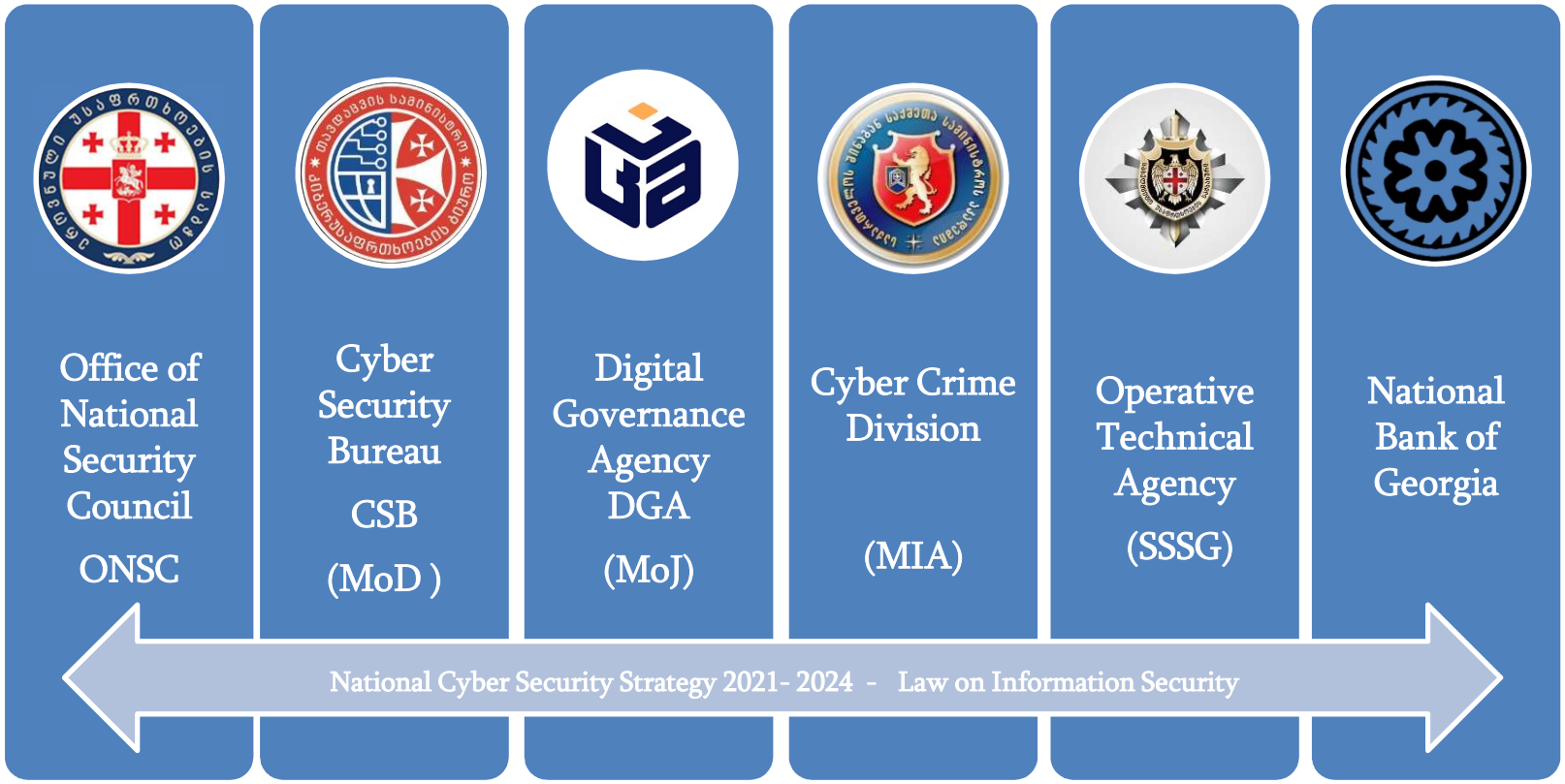
Current situation in society digitalization

According to 2022 statistical data, 93% of urban and 82% of rural households are connected to internet (mostly using smartphones, but majority also having computers).

In absolute majority of cases (well over 90%) internet is used for social media and communications and in almost 50% cases for information/news or commercial transactions (shopping, baking, etc).

Over 84% of business entities are connected and use internets for business purposes.

Cybersecurity Architecture of Georgia



Legal Framework - Law of Georgia on Information Security

- State Agencies and Local Municipalities — I
- Communications and ISPs — II
- Private businesses (Banks, Energy, Transport..) — III
- Defense sector (MoD critical infrastructure)

GCSS has 4 priority goals

- Development of cyberculture among information society and organizations and their capacity building;
- Resilience of cybersecurity governance system/framework and enhancement of public-private partnership (PPP)
- Enhancing cyber capabilities with strong cyber workforce and relevant technical support
- Strengthening Georgia's position, as a net contributor to cybersecurity, on the international plane

Cybersecurity-related threats

Georgian Cybersecurity Strategy defines several types of cyberthreats:

Cyber warfare, information warfare, cyber espionage, cybercrime.

Steady and constant threat of cyber attacks on Georgian critical information assets.
(Often hard to attribute, yet, is several times it was clearly defined that Russian state actors were conducting such activities).

2011 Russian cyberespionage operations against Georgia;

2016 large-scale DDoS cyberattacks on Georgian public and commercial digital infrastructure (by GRU of Russia MoD);

2020 cyberattacks on Georgian State Agencies, media, educational institutions, Lugar Lab;

2021 cyberattack on Georgian Parliament, Supreme Court;

2022 cyberattacks on media, private businesses, National Bank, MoD.

Cybersecurity-related challenges

Technical personnel qualification and workforce drain.

Need for regular technical and technologic upgrade.

Need for establishing a footprint in the cutting-edge IT technologic areas (Quantum Computing, Artificial Intelligence, etc).

Need for development of efficient and world-level competitive IT/Cyber technology businesses companies.

International cooperation (1)

Georgia actively cooperates with Western partners in cybersecurity capacity/capabilities development.

2021 and onward – UK supports Georgia in cybersecurity reforms. UK funded Torchlight project is underway, to support Georgian Agencies (NSC included) to implement some Activities of Georgian Cybersecurity Strategy Action Plan.

EU-funded Twining and CyberEast projects support Digital Governance Agency (DGA), in institutional development and capacity building, as well as MIA cybercrime division training support.

International cooperation (2)

MoD Cybersecurity Bureau (CSB) receives support from US in training and technologies.

US and UK support buildup of CSB CSOC (Cyber Security Operation Center).

Estonia provides cyber-trainings and cyberexercises.

Lithuania cooperates with Cyber Defense Regional Center (RCDC), cyberexercises.

NATO CDC (Cyber Defense Committee), PDP (Professional Development Program), cyberexercises.

SNGP (Substantial NATO-Georgia Package) Cybersecurity Initiative is upgrading on a national level.

Current processes in Georgian cybersecurity system (1)

Trainings of technical staff (different fields, certifications).

Upgrade of technical resources, hardware and software.

Development of automatized processes and SOPs for cyberincident response.

Digital forensic capacity building.

Update of a methodology and approaches to fight cybercrime.

Current processes in Georgian cybersecurity system (2)

Diversification and resilience of internet infrastructure.

Develop the safe supply-chains for ICT products and technologies.

Public awareness rising in cyberthreats/cybercrime.

Better domestic inter-agency and international cooperation.

Thank you for attention!