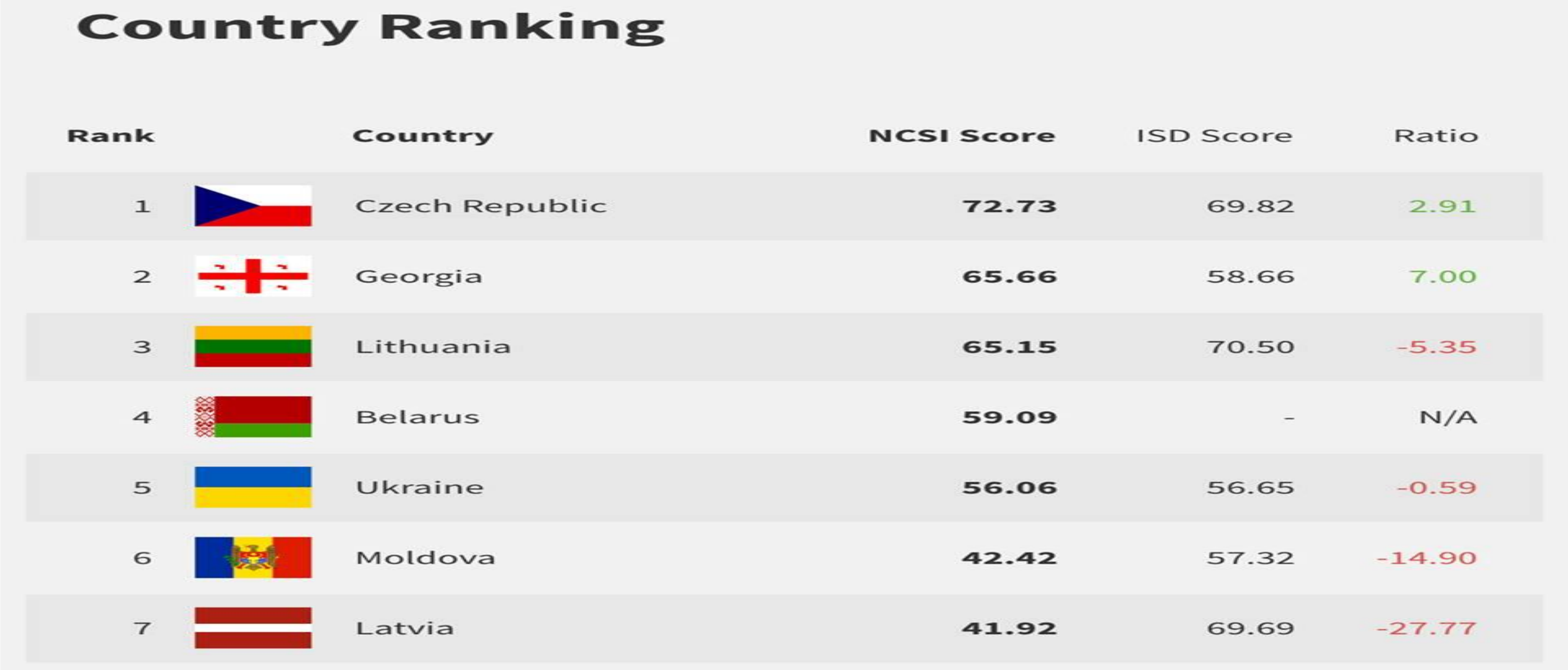
Ecosystem of Georgian Cyber Security

Internet Development Initiative IDI

Vladimer Svanadze

Georgia was entered the index in second place by the National Cyber Security Index. http://ncsi.ega.ee/georgia-enters-index-in-second-place/

Source: e – Governance Academy/eGA



Country Ranking

Rank	Country	NCSI Score	ISD Score	Ratio
1	Czech Republic	**72.73**	69.82	2.91
2	Georgia	**65.66**	58.66	7.00
3	Lithuania	**65.15**	70.50	-5.35
4	Belarus	**59.09**	-	N/A
5	Ukraine	**56.06**	56.65	-0.59
6	Moldova	**42.42**	57.32	-14.90
7	Latvia	**41.92**	69.69	-27.77

According to the Global Cybersecurity Index 2017 reported by the International Telecommunication Union (ITU), Georgia was placed 8th in the World, 2nd in the Europe, and 1st in the CIS

Top three ranked countries in Commonwealth of Independent States (CIS)

Country	*GCI Score*	*Legal*	*Technical*	*Organizational*	*Capacity Building*	*Cooperation*
Georgia	**0.81**	**0.91**	**0.77**	**0.82**	**0.9**	**0.7**
Russian Federation	0.78	0.82	0.67	0.85	0.91	0.7
Belarus	0.59	0.85	0.63	0.33	0.68	0.47

Source: *Global Cybersecurity Index 2017*

Top ten most committed countries, GCI (normalized score)

Country	*GCI Score*	*Legal*	*Technical*	*Organizational*	*Capacity Building*	*Cooperation*
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

Source: Global Cybersecurity Index 2017

__The five pillars__ of the Global Cybersecurity Index (GCI)

- **Legal** Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime

- **Technical** Measured based on the existence of technical institutions and frameworks dealing with cybersecurity

- **Organizational** Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level

- **Capacity Building** Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building

- **Cooperation** Measured based on the existence of partnerships, cooperative frameworks and information sharing networks

Stakeholders of the Georgian Cybersecurity

- **Government** Data Exchange Agency, Cyber Security Bureau, Cybercrime Division, CERT.GOV.GE, The Personal Data Protection Inspector Office, State Security Services

- **Civil Society** Georgian Research and Educational Networking Association/GRENA, Internet Development Initiative/IDI, Scientific Cyber Security Association

- **Private Sector** Information Security Operations Center/ISOC – Mze, UGT, Orient Logic, GreenNet,

- **Academia** University of Georgia

- **Technical Society**

Georgian Cyber Security Entities

1. January, 2010 - LEPL Data Exchange Agency of the Ministry of Justice

2. January, 2011 - CERT.GOV.GE

3. December, 2012 - Department of Combating Cybercrime in the Central Criminal Police Department of the Ministry of Internal Affairs

4. 2013 - The Personal Data Protection Inspector Office

5. February, 2014 - LEPL Cyber Security Bureau of the Ministry of Defense

6. 2016, August – Division at the State Security Services

Georgia's legal space of cyber security

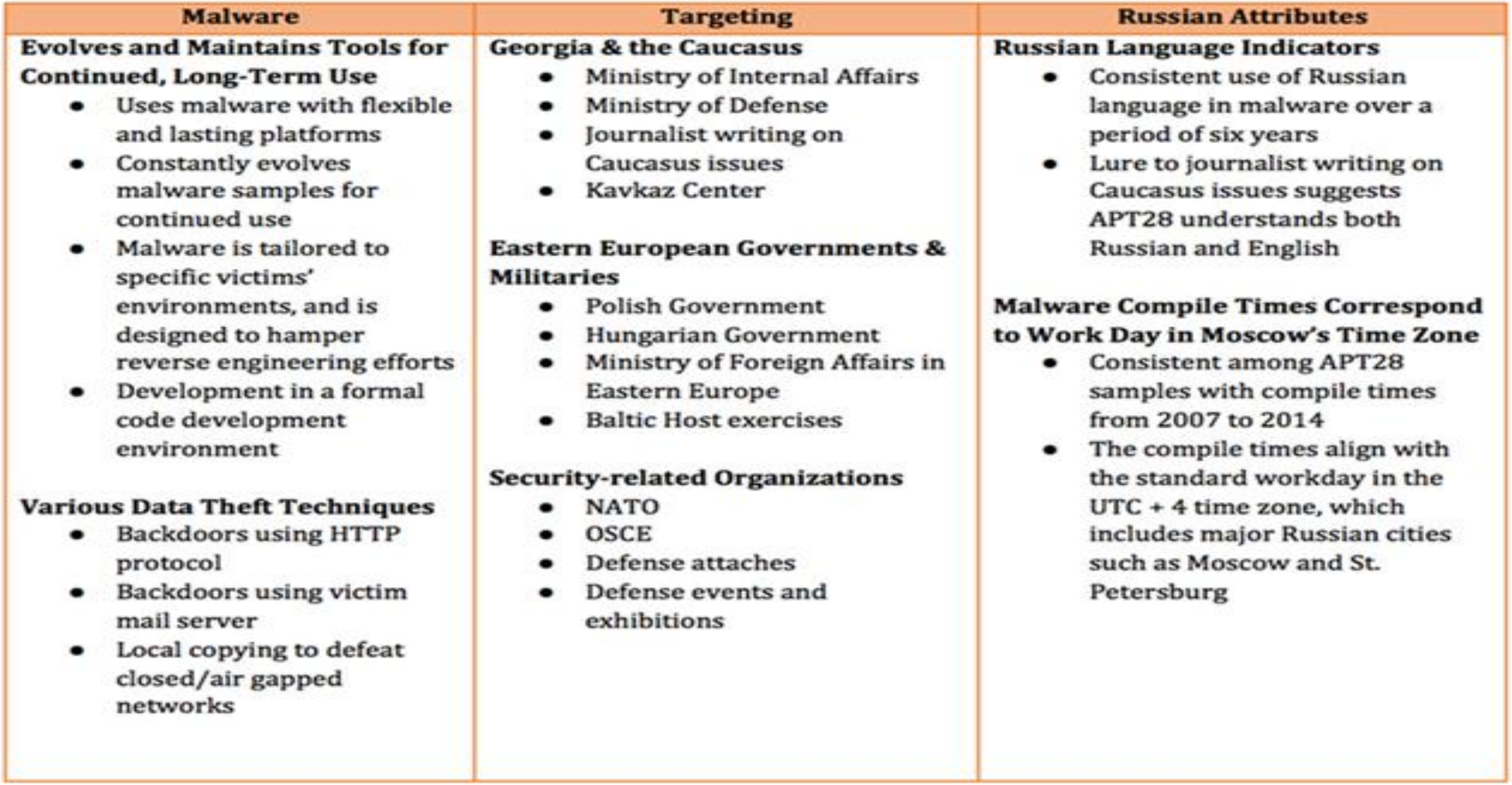
1. December, 2011 - National Security Concept of Georgia
2. June, 2012 - Law on Information Security
3. October, 2012 – Convention of Budapest
4. May, 2013 - Cyber Security Strategy and Action Plan for 2013 – 2015
5. 2013 - defined critical infrastructure subjects
6. August, 2014 - Association Agreement with the European Union (P7; P14)
7. January, 2017 - Cyber Security Strategy and Action Plan for 2016(7) – 2018

Georgian Cyber Security Strategy

Main directions

- Research and analysis
- New legislative - normative base
- Institutional coordination of cyber security
- Raising public awareness and formulation of educational base
- International cooperation

Cyber attacks 2008 – 2014 by APT28/FireEye



Malware	Targeting	Russian Attributes
Evolves and Maintains Tools for Continued, Long-Term Use • Uses malware with flexible and lasting platforms • Constantly evolves malware samples for continued use • Malware is tailored to specific victims' environments, and is designed to hamper reverse engineering efforts • Development in a formal code development environment **Various Data Theft Techniques** • Backdoors using HTTP protocol • Backdoors using victim mail server • Local copying to defeat closed/air gapped networks	**Georgia & the Caucasus** • Ministry of Internal Affairs • Ministry of Defense • Journalist writing on Caucasus issues • Kavkaz Center **Eastern European Governments & Militaries** • Polish Government • Hungarian Government • Ministry of Foreign Affairs in Eastern Europe • Baltic Host exercises **Security-related Organizations** • NATO • OSCE • Defense attaches • Defense events and exhibitions	**Russian Language Indicators** • Consistent use of Russian language in malware over a period of six years • Lure to journalist writing on Caucasus issues suggests APT28 understands both Russian and English **Malware Compile Times Correspond to Work Day in Moscow's Time Zone** • Consistent among APT28 samples with compile times from 2007 to 2014 • The compile times align with the standard workday in the UTC + 4 time zone, which includes major Russian cities such as Moscow and St. Petersburg

Internet Development Initiative - IDI is a membership-based Non-entrepreneurial (Non-commercial) Legal Entity. It has established in July, 2015, in accordance with the Civil Code of Georgia. Member of APRALO/ICANN, and NCGO/ICANN, also Scientific Cyber Security Association

The Objectives of the Organization Activities:

a. Support growth concentration of the internet;
b. Promote the development of standards of cyber security, and support to improve skills in cyber security. Organize trainings and study courses;
c. Study and analysis of threats in cyberspace. Write recommendations for government and private sector. Public awareness raising;
d. Encourage the process of protection and advocacy for internet users' rights;
e. Support the development of online media;
f. Initiative of projects of information and communication technology. Search for new technologies, analysis and promotion for implementation;
g. Initiative of projects with government and private sector in Information technology and innovation;
h. Support for print and online publications, organizing conferences, seminars, forums in ICT and cyber security.

Projects

a. Georgian Internet Governance Forum - GeoIGF Tbilisi 2016;
b. The Project for Broadband Rollout in Tusheti Region;
c. The National Cyber Security Strategy of Georgia (2016 - 2018);
d. Studying course on "Investigating DNS Abuse & Criminal use of the DNS“ (X2);
e. The First Cyber Security Festival for Georgian Students;
f. Center for Study & Research of Internet;
g. Raising Awareness of Students – Teenagers in Cyberspace-Related Threa;
h. Cyber Security Laboratory.

Q&A

Vladimer Svanadze

Chairman of the Board

Internet Development Initiative IDI

106, Beliashvili street, Tbilisi 0159, Georgia

info@indein.net