საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

52

NEW CHALLENGES FOR THE GEORGIAN CYBERSPACE

VLADIMER SVANADZE

EXPERT OPINION

2016

GFSIS
საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

EXPERT OPINION

VLADIMER SVANADZE

NEW CHALLENGES FOR THE GEORGIAN CYBERSPACE

52

2016

The publication is made possible with the support of the US Embassy in Georgia.

Editor:	Carole Neves
Technical Editor:	Artem Melik-Nubarov

ISSN 1512-4835
ISBN 978-9941-0-8512-3

The global community has come to face a new cyber threat, emanating from Islamist hacker groups and factions. In this regard, it is noteworthy that in recent years, especially following the hostilities in Syria and the emergence of the so-called "Islamic State" (ISIS) in the Middle East, the number of cyber attacks has somewhat increased. Especially active in this field are the Middle Eastern Cyber Army (MECA), the Fallaga Hackers Team and the Cyber Caliphate, as well as the Syrian Electronic Army (SEA), which receives considerable backing from the Iranian Cyber Army (ICA).

In the nearest future, the Georgian web space will also face similar threats; as its foreign policy is aimed at the integration into European institutions, The country strives to become a member of the European Union and the North Atlantic Treaty Organization (NATO). Last year, Georgia signed the EU Association Agreement, where one of the points includes the provision of security (Association Agreement between the European Union and Georgia, Article 1, Paragraph (f)), including the protection of personal data (Association Agreement between the European Union and Georgia, Title 3, Article 14) and combating cybercrime (Association Agreement between the European Union and Georgia, Title 3, Article 17, Paragraph (g)).

All of the above will lead to the opening of new missions and representative offices of Western state institutions and companies in Georgia. The process will be increasingly expanding, which, in turn, will further increase threats to Georgia on the part of potentially hostile countries, as well as Islamic fundamentalists. In parallel to all of the above, the level of cyber threats will also continuously increase.

According to statistical data, Russia accounted for a significant number of cyber attacks conducted in Georgia in 2008-2014. The systematic cyber attacks were carried out on the web pages of the Ministries of Internal and Foreign affairs of Georgia, as well as of a number of non-governmental organizations working on Caucasus issues.

Several websites and persons protecting the Georgian statehood and interests in cyberspace were targets of Russian hackers. Noteworthy, in this regard, is the cyber attack implemented by Russian hackers on August 6-7, 2009 against popular Georgian social networks, triggered by the political stance of the Georgian blogger "Cyxymu" ("Sukhumi"). The cyber assault was launched on August 7, when it became clear that it was being carried out by the Russian secret service, which blocked information distributed by the blogger “Cyxymu” in relation to the anniversary of the August War. All specialists now confirm that the attack was implemented by Russia and was so well-organized, that authorship by individual hackers was essentially ruled out.

Cyber attacks from Russia employed cyber espionage to obtain and collect information on Georgia-US, Georgia-EU, and Georgia-NATO relations and future activities.

In 2015, no Russian activity was detected in the Georgian cyberspace, as no infiltration attempts were officially recorded. Although, on May 21-25, 2015, a massive Distributed Denial of Service (DDoS) attack on Georgian financial organizations was registered. A total of up to 300,000 unique IP addresses from over 160 countries participated in the attack. Given the scale and development level of the attack, as well as Russia’s interest in the region, it can be assumed that a Russia-affiliated hacker group was behind the endeavor. Because the large-scale attack was not focused on incurring financial damage, it appears as if it was intended to divert attention from possibly another, more detrimental attack.

Islamist hackers emerged among the organizers of intrusions in the Georgian web space in 2015. On January 10, 2015, a cyber attack was carried out by the Middle East Cyber Army on the web page of the Georgian branch of the French company “Carrefour”. An extensive cyber attack on French organizations was implemented and their representative offices around the world occurred including an attack on the Georgian branch of Carrefour. The incident is regarded as the first major precedent of a cyber attack on a Western firm in Georgia.

In addition, worth mentioning is another incident, an attack carried out by the Islamist hacker group “Al Muhajir” on April 16, 2015 on the website of the Association “Unity of Judges of Georgia”. The cyber assault was used for intimidation and propaganda purposes.

A cyber attack was also carried out by ISIS hackers on July 6 on the webpage of the Office of the Georgian State Minister on European and Euro-Atlantic Integration.

In the future, the number of incidents conducted by Islamist groups and factions is likely to increase, which should be viewed as a major challenge to Georgian national security. In this context, the objectives and capacities of the Yemen Cyber Army should be taken into account. The latter is a newly established organization with the aim to hijack electronic correspondence on relations among the United States, EU-member states and their strategic partners via cyber attacks, carried out from countries whose cyberspace is relatively more vulnerable and sensitive. For instance, in June 2015, the organization conducted a cyber assault on the Ministry of Foreign Affairs of Saudi Arabia, wherein it obtained approximately up to ten thousand strategic documents of electronic correspondence with the United States and the European Union. The Georgian state agencies may face a similar danger.

The following incidents can be singled out among illegitimate attacks carried out in 2015 in the Georgian cyberspace:

- On January 19, a cyber assault was undertaken on the web-page of the State Minister of Georgia for Diaspora Issues;
- On February 2, a large scale cyber attack was carried out on electronic mail. In particular, the attack entailed the spread of a new computer virus, which sent electronic mail in various languages, including Georgian. The email specified a 96 target to transfer a specified amount of files, alternatively, the files would be permanently deleted;
- On February 5, the official website of the Ministry of Foreign Affairs of Georgia was attacked. Efforts to launch a new web page are being undertaken. At this stage, the source of the above mentioned cyber attack is undetermined;
- In the first half of the year, several cyber assaults were instigated against the web-page of the Ministry of Agriculture of Georgia.

According to statistics provided by the Ministry of Foreign Affairs, cybercrime rates are steadily increasing. However, the percentage of solved crimes may have decreased. In January to August 2015, the MFA recorded an 11.11% increase in the number of cybercrimes as compared to the same period in 2014. In 2014, the number of resolved crimes was 59.26%, while in January-August 2015, the figure stood at 34.44%. Data for the entire year of 2015 were unavailable.

Besides the attacks mentioned above, several, smaller-scale cyber assaults on the private sector occurred. According to the internet security portal "Zone-H", in the period of January-October 2015, Georgian cyberspace experienced 489 illegitimate intrusions. This figure would be insignificant for large countries, such as US, United Kingdom, or China. However, intrusions in Georgia cyberspace are troubling. Cyber incidents occur daily in Georgia.

Given threats and challenges to date, planning and implementation of an effective security policy requires attention in three critical areas:

- Cyber war and/or cyber attacks causing damage to Georgian cyberspace and rendering them inoperative. Cyber terrorism, which poses a major threat to the country's national security via the possibility of cyber attacks on critical information infrastructure;
- Activities which damage individual units of critical information infrastructure, such as inoperability of economic, social and other sectors.
- The Georgian government is currently developing a new Cyber Security Strategy and Action Plan for the period of 2016-2018.

References

1. Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part, 2014, www.eeas.europa.eu/georgia/pdf/eu-ge_aa-dcfta_en.pdf;
2. United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk, Washington DC:US GAO, 2009;
3. Democratic Governance Challenges of Cyber Security, Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler, DCAF 2010, DCAF Horizon 2015 Working Paper Series;
4. APT28: A Window into Russia's Cyber Espionage Operations? FireEye, October 27, 2014 www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html;
5. Law of Georgia on Information Security;
6. Georgian Cyber Security Strategy.