Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 34 - 40 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

EVALUATING CYBER THREATS IN CAUCASUS
ACTORS POSING THREATS TO GEORGIAN CYBER SPACE

Salome Mikiashvili, PhD in American Studies
International Black Sea University

ABSTRACT. Cyber war is the action aimed at destroying information and communication systems, while web war is a deliberate action involving attempts by one or several actors via open or hidden channels, to transform the perception of the target actor so that the transformation will bring desirable results to the attacker. Apart from critical infrastructure of national importance, active membership of anti-terrorist coalition and considering the clear-cut Euro-Atlantic vector of the country, additional target is the Georgia-based information networks and infrastructure of other countries, international organizations and foreign businesses. In the paper is shown that the recent cyber security activities in the Caucasus region suggest that we are dealing with a completely new precedent related to the deployment of forces in the cyber security field. In fact, this case has clearly demonstrated the increasingly active use of cyber security elements in international relations, and primarily in terms of distribution of power.

Keywords: cyber, cyber threats, Caucasus, cyber space

Using cyber elements to reach political economic or military goals and to gain geopolitical advantage is the reality of the modern world. Western experts more and more frequently discuss the tendency accompanying transformation of cyber war into a web war. Cyber war is the action aimed at destroying information and communication systems, while web war is a deliberate action involving attempts by one or several actors via open or hidden channels, to transform the perception of the target actor so that the transformation will bring desirable results to the attacker. Georgian cyber space is not an exception from this. The recent conflicts on the post-soviet territories prove that politically motivated cyberattacks are relevant to Georgia as well. Apart from critical infrastructure of national importance, active membership of anti-terrorist coalition and considering the clear-cut Euro-Atlantic vector of the country, additional target is the Georgia-based information networks and infrastructure of other countries, international organizations and foreign businesses. The threat to the above-mentioned objects may be coming from such actors as:

- countries having well-developed, high cyber attacking potential (Russia, China Iran)
- cyber divisions of terrorist organisations and ideologically motivated or extremist hackers

•financially motivated cyber criminals. (L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi)

Let's discuss each actors separately. Studying their capabilities is very relevant for Georgia too. Russian Federation. The Ministry of Defence of Russia establishes its own cyber command, which according to the available information will be responsible for implementing attacking cyber events, including propaganda-based events and inserting malware in the administration and control systems of the adversary. Other divisions specializing in computer network operations are established in the armed forces of Russia. Reportedly, Russia is actively developing distance access tools for critical infrastructure industrial control system.(ICS)According to experts, unknown Russian actors have been successful in damaging several ICS manufacturers' software and inserting malicious code into legal software updates and thus providing direct access to the user's website.

"Today, there is no doubt that for political goals the Russian authorities are actively using the so-called method of information-psychological impact that Western scholars characterize as the initial phase of modern Russian conflict creation. This phase involves conducting unconventional operations to manipulate public opinion within the target country and in the international media. In light of the intensified activities, the Russian combat units begin to penetrate into the target area under the guise of local armed forces. This completes the unconventional operations phase. If the operation succeeds, the activities to legitimize intervention begins with the legend of " Defending Minority Rights".(L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi) [1]

"The second phase involves conventional actions, but the success of the first, non-conventional phase of the annexation of Crimea has greatly facilitated the conventional phase of the conflict in favour of Russia. Russia's political elite views information as a source of power, creating solid ground for implementing the country's information operations." (L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi). According to the national security concept, Russia views nationalist, separatist, and radical religious agitation measures as threat and considers it necessary to spread "true" information and develop a local platform (e.g its own social media). While analyzing future threats, the same document points out that "the global information battle will be intensified". Therefore, computer network operations are seen as an organic, unchanging part of information security. Russia seeks to process not only the technical part of the information, but also exercise control over the cognitive information constituent. For this reason, according to experts, the notion of "cyber security" in Russian doctrines and conceptual documents is replaced by the term "information security" .If we analyze the ongoing conflicts with Russia's involvement in the post-Soviet space, it becomes clear that it views the conflict areas as a type of polygon for probing kinetic types of weapons and cyberattack potential. Thus, for Georgia it is vitally necessary to perform a thorough analysis of the Russian cyber activities and information warfare and to manage the arising risks. It should be considered that even less technologically advanced attacks, such as DDoS attacks or so-called “defacement” of websites, should, as a rule, be considered part of Russia's cyber-information warfare [2].

Generally the interests of the Russian hacking groups such as: APT28 are progovernmental. It serves the interests of Russian federation. The spheres of interests are: Eastern European governments and Caucasus as a whole (especially Georgia). The Caucasus, a region that includes independent states of Georgia, Armenia, and Azerbaijan continues to experience political disruption. The Georgian government’s strings to the West are a the reason of Moscow’s frustration, especially after the 2008 war. Overall, issues in the Caucasus likely serve as focal points for Russian intelligence collection efforts.

Since 2011, APT28 has been using bait written in Georgian makes us think that the targets are government agencies of Georgia as well as citizens of Georgia. According to the Fireeye report, called: “A Window Into Russia’s Cyber Espionage Operations”, APT28 is expected to seek information on Georgia's security and diplomatic positions. In particular, the group attacked the Ministry of Internal Affairs (MIA) and the Ministry of Defense. There was also an attempt to target a journalist working on the Caucasus problems and controversial news from Chechnya. “APT28 to the Ministry of Internal Affairs (MIA). The MIA possesses sensitive information on the internal structure of Georgia's security operations, its involvement in multilateral institutions, and the basis for government communications.” (FireEye, APT28: A Window into Russia’s Cyber Epionage Operations). According to the FIreeye investigation the hacking group APT28 had at least two specific attempts to attack the MIA. In one case, it was found that APT28 used malicious programs that attempted to disguise its activity as MIA legitimate mail. “This bait contained an Excel file containing malware, which was a bait document with a list of Georgian drivers. Backdoor attempted to establish a connection with the Georgian MIA Post Server and communicate with the MIA email addresses ending with mia.ge.gov ". After connecting to the Mail Server, the APT28 forwarder sent an email using the Driver License Title field (in Georgian).) And attach a file containing the system intelligence info This tactic could have allowed APT28 to obtain data from the MIA in a less verifiable way, limiting the ability of the MIA's Department of Network Security to detect traffic. - Domain "MIA Users \ Ortachala ..." (Su Ten 1). This is probably the Interior Ministry in the object Ortachala district. bait document also contains metadata, which is named "Internal Affairs", as the company name and "Beka Nozadze" 4, as the author, it is the system administrator of a possible reference. The text of the document is intended to create a domain and user group [3].” (FireEye, APT28: A Window into Russia’s Cyber Epionage Operations). Since the Russo-Georgian War of 2008, Georgia and Russia have severed diplomatic relations, and Georgia has since sought to establish closer ties with Western security organizations. In in

June 2014, despite Russia's open political stance, Georgia, together with Ukraine and Moldova, signed association agreements with the EU. This move strengthened ties between these three countries and EU's political, economic and security spheres. Russian hacking groups are trying to steal information that exposes topics about US Georgia military cooperation and NATO. APT28 attacked a journalist covering the Caucasus news. Apt28s target became the journalist covering issues in the Caucasus region. In 2013, APT28 sent the false letter stating that the letter was authored by Reason magazine's "Principal Coordinator for the Caucasus Affairs Department". This section does not appear to exist. (Reason Magazine is American.) The letter invited the journalist as a journal contributor and was asking for the information regarding abovementioned political subject. Meanwhile, the bait-doc installed a SOURFACE backdoor in the victim's system. “From the content of the letter the experts came to conclusion that APT28 actors can read in at least two languages - Russian and English. The letter's grammar also indicates that English is not the author's native language, even though it appears to be from American journal. This fact clearly indicates that Russian may be the language preferred by the author APT28. Cyber Attacks on journalism can allow APT28 and its sponsors to monitor public opinion, identify dissidents, disseminate misinformation, or plan further attacks.” (FireEye, APT28: A Window into Russia’s Cyber Epionage Operations)

China. According to Chinese data, Chinese cyber operations are mainly for commercial purposes and therefore are not a direct threat to Georgia, although the networks of governmental and commercial structures of developed countries based in our country and information contained in their databases should not be overlooked. The Islamic Republic of Iran. Unlike China and Russia, Iran has trained hackers mainly on the basis of religious ideology. In particular, Iran has trained about a thousand hackers over the past five years with the influence of fundamental religious pathos. Their goal is to destroy critical infrastructure of their ideological adversary.” Iran is responsible for the DDoS attacks on US financial institutions in 2012-2013 and the February 2014 attack on the Las Vegas Sands Casino. According to the US intelligence community, Iran views its cyber project as a way to conduct asymmetric but proportionate actions against political adversaries and to seek intelligence. The fact that the US intends to ease sanctions on Iran and return it to the international oil market will not diminish the confrontation between the West and Israel in cyberspace. Authoritative US experts say Iran will increase cyberattacks, regardless of whether sanctions are in place. Moreover, if sanctions are eased, Iran will be able to mobilize and use its financial resources to develop its cyber capabilities, which in itself will increase the qualification of hacker groups and improve their methods of action.” (L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi. For Georgia, Iran's cyberattacks may pose a threat because, as Iran views it, there is infrastructure of hostile countries on our territory [4]. Also, given current trends, it is quite realistic for Iranian-backed terrorist organizations to exploit Georgian cyber networks for propaganda purposes. Given the above-mentioned, the scale of cyber threats facing Georgia is increasing in complexity and diversity. Special attention should be paid to developing a mechanism for obtaining and analyzing information on cybercriminals' intentions, capabilities or activities and conducting active work in this regard.

The most real threat to Georgia's cyberspace is Russia's cyber activities, which are aimed at both disrupting critical infrastructure and using it for its own purposes.) It should be emphasized that even low-tech attacks, such as DDoS and Defacement attacks, can lead to disproportionate loss in poorly protected infrastructure. It should be noted that the Russian-implemented or backed cyberattack in Georgia could cause significant damages and even casualties. As for the cyber threats coming from Iran and China, first of all, we should not overlook the infrastructure and databases of the countries in Georgia, which these countries consider as their adversaries. These include Georgia's strategic partner USA, NATO member states and the European Union and the systems of these international organizations. “China's cyberattacks by major terrorist organizations [5,6]. There is a high probability of implementing a cyberattack that could lead to temporary, local damage to electronic services and websites. Organizing and executing cyberattacks that cause mass damage or casualties is unlikely at this stage. The probability of threats coming from profit-oriented cybercriminals is hard to predict. Raising public awareness, constant contact with critical infrastructure in the private sector, harmonization of local legislation with international one, active usage of international cooperation mechanisms for the fight against cybercrime are important. “(L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi)

One of the latest cyber-attacks conducted by Russia was on 28 October 2019, when a large scale cyber-attack was launched against the websites, servers and other operating systems of the Administration of the President of Georgia, the courts, various municipal assemblies, state bodies, private sector organisations and media outlets. As a result of the cyber-attack, the servers and operating systems of these organisations were significantly damaged, severely affecting their functionality.

“The above-mentioned cyber-attack was targeted at Georgia’s national security and was intended to harm Georgian citizens and government structures by disrupting and paralysing the functionality of various organisations, thereby causing anxiety among the general public. The investigation conducted by the Georgian authorities, together with information gathered through cooperation with partners, concluded that this cyber-attack was planned and carried out by the Main Division of the General Staff of the Armed Forces of the Russian Federation. Georgia condemns this cyber-attack, which goes against international norms and principles, once again infringing Georgia’s sovereignty in order to hinder the country’s European and Euro-Atlantic integration and democratic development.

The above-mentioned incident emphasises the importance of the Georgian Government’s efforts to strengthen cyber security at the national level and again demonstrates the need to build international partnerships on cyber-security. Georgia, for its part, will continue close cooperation with partners, strengthening cyber-security at the national level in order to minimise such risks and potential threats in the future. We call on the international community to give an appropriate reaction to this development.” (MFA OF Georgia, 2019)/ The Cyber attack was condemned by US, UK and many other EU and Nato countries The United States called on Russia to cease this behavior not only in Georgia but elsewhere. The government of US made special announcement on the US Department of State saying that: “On October 28, 2019, the Russian General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST, also known as Unit 74455 and Sandworm) carried out a widespread disruptive cyber attack against the country of Georgia. The incident, which directly affected the Georgian population, disrupted operations of several thousand Georgian government and privately-run websites and interrupted the broadcast of at least two major television stations. This action contradicts Russia’s attempts to claim it is a responsible actor in cyberspace and demonstrates a continuing pattern of reckless Russian GRU cyber operations against a number of countries. These operations aim to sow division, create insecurity, and undermine democratic institutions. The United States calls on Russia to cease this behavior in Georgia and elsewhere. The stability of cyberspace depends on the responsible behavior of nations. We, together with the international community, will continue our efforts to uphold an international framework of responsible state behavior in cyberspace. We also pledge our support to Georgia and its people in enhancing their cybersecurity and countering malicious cyber actors. We will offer additional capacity building and technical assistance to help strengthen Georgia’s public institutions and improve its ability to protect itself from these kinds of activities.”

(Michael. R. Pompeo, The US condemns Russian Cyber attack against the country of Georgia, feb, 2020). Russia's reaction was feasible. Russia Duma representatives have denied the allegations and spoke about the political goals of US in the region.

Finally, it can be concluded that the recent cyber security activities in the Caucasus region suggest that we are dealing with a completely new precedent related to the deployment of forces in the cyber security field. This process was first revealed during the Azerbaijani-Armenian military confrontation in April 2016, when concurrent with the military action, there was also a more intense confrontation in cyberspace. In particular, in this case, the main players in the Caucasus region - Turkey and Russia - also engaged in a confrontation between the two countries [7]. The former supported Azerbaijan, the latter sided with the Armenia, and both countries are actively involved in the cyberspace confrontation. Of particular interest was the position of Iran, which preferred neutrality due to the fact that Iran has very good relations with both opposing countries in terms of politics, economics and trade.

In fact, this case has clearly demonstrated the increasingly active use of cyber security elements in international relations, and primarily in terms of distribution of power.

REFERENCES

1. L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi
2. FireEye, APT28: A Window into Russia’s Cyber Epionage Operations
3. საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდი:რუსეთ-საქართველოს 2008 წლის ომის კიბერგანზომილება, 2019, ა. გოცირიძე
4. CYBER ESPIONAGE Against Georgian Government (Georbot Botnet) LEPL Data Exchange Agency Ministry of Justice of Georgia
5. Cyberwar: How Russian Hackers and Trolls Helped Elect a President by Kathleen Hall Jamieson
6. Johnson P.A. (2002). M.N. Schmitt, B.T. O’Donnell (Eds.). Is It Time for a Treaty on Information Warfare?.
7. Michael. R. Pompeo, The US condemns Russian Cyber attack against the country of Georgia, feb, 2020