Scientific and Practical Cyber Security Journal (SPCSJ) 7(3): 17 – 20 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

HOW TO BUILD THE RESILIENCE AGAINST RUSSIAN CYBER OPERATIONS

Andro Gotsiridze[1]
[1]Business and Technology University, Tbilisi, Georgia

ABSTRACT: In the last two decades, Cyber has become the fifth domain of confrontation. Former US Secretary of State Michael Pompeo mentioned that "Huawei and other Chinese state-backed tech companies are Trojan horses for Chinese intelligence, Russia's disinformation campaigns try to turn our citizens against one another. Iranian cyberattacks plague Middle East computer Networks." Although China, Iran, and North Korea state and non-state actors have offensive cyber capabilities, Georgia remains most concerned about Russia. Cyber threats from Russia and their proxies will remain acute. Additionally, many capable hackers and profit-oriented cybercriminal groups maintain mutually beneficial relationships with the Kremlin that offer them safe haven or benefit from their activity. Cyber diplomacy activities, participation in small alliances for cyber capacity building, creating volunteer-based cyber defense units, and organizing joint governmental cyber exercises are the steps, Georgia can and should take to ensure resilience against cyber threats.

KEYWORDS: Cyber operations, cyber-attacks, resilience, cyber defense

1. INTRODUCTION

What is the geography of destructive Cyberoperations? Former US Secretary of State Michael Pompeo mentioned that "Huawei and other Chinese state-backed tech companies are Trojan horses for Chinese intelligence, Russia's disinformation campaigns try to turn our citizens against one another. Iranian cyberattacks plague Middle east computer Networks."

In the last two decades, Cyber has become the fifth domain of confrontation. The cyber operations today are an important part of any war, conflict, or confrontation. Many states use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure.

Iran's cyber capabilities may be a threat to Georgia insofar as the infrastructure of the states that Iran considers hostile to itself is placed on our territory. Also, it is entirely realistic for the Tehran-backed terrorist organizations to use the Georgian cyber network for recruiting and propaganda purposes. Cyber espionage is another tool for Iran to conducting a terrorist attack. It can be used both for determining real-time geolocation, resulting from surveillance through a cell phone company, as well as for tracking of a potential target to preparing a terrorist act.

China has been advancing its cyber-attack capabilities by integrating its military cyber-attack and espionage resources in the Strategic Support Force, which it established in 2015. Targets of China`s cyber-operations vary from national security related information to sensitive economic data and intellectual property. Furthermore, Georgia should pay significant attention to the cyber security of the national or commercial projects which involves US and other strategic partners, whom Beijing sees as adversaries.

Although China, Iran, and North Korea state and nonstate actors have offensive cyber capabilities, Georgia remains most concerned about Russia. Cyber threats from Russia and their proxies will remain acute. Additionally, many capable hackers and profit oriented cybercriminal group maintain mutually beneficial relationships with Kremlin that offer them safe haven or benefit from their activity.

2. INFORMATION AS A MAIN KEY TOOL OF CYBER OPERATIONS

The Kremlin views the information as a key domain for modern military conflict. Russia is successfully developing its offensive cyber capabilities to achieve political, economic, military goals, as well as geopolitical advantage. The Kremlin considers Georgia to be within its sphere of influence, which is why our country is a target for Russian cyberoperations. Therefore, Georgia's cyber defense policy must be "Russo centric".

How far, with what means and to what extent intentionally or unintentionally can Russia reach into information systems?

From the use of such tools as Not Petya to SolarWinds, or to Yandex and Kaspersky, what are the means of frustration?

Can the Kremlin score an unexpected success in cyber warfare if we are insufficiently prepared? When will we stop defining and start coping with the cyber challenges?

We can see how Russian cyber capabilities are becoming more and more sophisticated. Attack against Estonia, in 2007 was its political message and a punitive operation for the "bronze soldier" - aimed to provoke public unrest and mass disorder. This was the first attempt of using cyber to influence political processes. For the following year, the use of cyberoperations in the Russia-Georgia War was a well-organized complementary process to conventional military actions, aiming at creating an information vacuum, spreading disinformation, and closing the channels of international support for Georgia. Later, In the war with Ukraine in 2014-16 Russia managed to utilize the capabilities of large telecommunication companies to secretly eavesdrop on their clients, determine their locations and use this information to make psychological influence and to determine locations for artillery strikes. In addition, Russian Intelligence services for the first time, disabled part of the Ukrainian energy system by using sophisticated malware [1].

Soon, Russia's destructive cyber activities went beyond the post-Soviet area and Russian government connected hackers targeted elections in Europe and the United States. in recent years, Russian cyber enabled influence operations have been aimed at attacking to state democratic institutions and state sovereignty.

One good example for this was extensive GRU-organized cyberattack in 2019: thousands of Georgian websites—government, courts, media, NGOs —were defaced. Attackers replaced the landing pages with electronic graffiti. Images of former President Mikheil Saakashvili were saying "I'll be back!".

The attack was massive but less sophisticated. This could be an intelligence-by-attack-strategy: testing vulnerabilities, defenses, and resilience of the country; But above all it was to undermine Georgia's state sovereignty, turning citizens one against another. GRU-attack has success in terms of polarization.

We must consider that even low-tech Defacement could result quite high damage to weakly protected infrastructure.

Defacements and destructive wiper malware masquerading as ransomware - several cyber-attacks against Ukraine have made headlines before the Russia's unprovoked full-scale invasion in Ukraine, as military tensions along the Russian/Ukrainian border have escalated. Impacted Websites included the Ukrainian Foreign Ministry, the Ministry of Education and Science, and other state services.

The message "be afraid and expect the worst" was published. Even more additional malware was used to strike Ukrainian government websites and it had some similarities to the NotPetya wiper but was more capable to make additional damage [2-3].

Russia's cyber operations continue to be the serious threat for Georgia. Therefore, securing the cyber space is a priority. Compared to the cyber-attacks of 2008, the level of Russian cyber threats has grown due to several factors:

- First, Russia has not altered its aggressive cyber policy, but increased its offensive cyber capabilities even more.
- Second, Russia has been extending its cyber operations in both directions: Information-Technical and Information-Psychological.
- Third, Georgia's dependence on ICT is much higher now, which increases the scale of the expected damage.

Expected Consequences of Russian destructive cyber operations can be diverse:

- Various Levels of Disruption of Critical Infrastructure including Industry Control Systems (ICS).
- Cyber Espionage
- Cyber Attacks through sophisticated Malware
- Supply Chain Compromising
- Information Psychological Effect

On one hand, Information-technical effect could lead the country to the serious damage and/or casualties. On the second hand, the propaganda spread through cyber channels could cause the alteration of public perceptions in favor of the Kremlin, reduce pro-Western sentiments, and form or strengthen pro-Russian elite; And these might appear as a reason of possible conventional actions [4].

3. KEY STEPS TO ENSURE RESILIENCE TO CYBER THREATS IN GEORGIA

What Georgia as a small country can and should do to ensure resilience against cyber threats?
First, for Georgia it is important to participate in the development of a framework of responsible behavior in the Internet. In 2019 the US and 26 partner states signed a joint statement on the responsible behavior of states in cyberspace. The partners note that, if necessary, they will act jointly against the "irresponsible" countries in accordance with the norms of international law. Russia and China have not signed the document. It is important for Georgia to adhere to this document.
Second, Georgia should not limit itself to statements of attribution. Participation in small alliances for cyber capacity building would be strongly recommended. Annual exercises, organized by the US Department of Defense with the UK, Denmark, Estonia, and France, is based on a conception of a collective defense alliance in cyberspace and acts in accordance with the norms of responsible behavior of states in cyberspace. These Exercises enhance capabilities in terms of detecting malicious actions against critical infrastructure, synchronizing countermeasures and joint responses. Engagement in these events is very important not only for Georgia but for allies as well, as Georgia is a kind of testing ground, polygon for Russian cyber operations. These developments seem real, given the degree of Georgia's cooperation with the West in cyberspace.
Third, it is vital for Georgia to establish volunteer based cyber defense units and organize joint governmental cyber exercises.
Overwhelmed state agencies, unable to provide assistance, resource and talent constraints in the public sector, competitive private-sector salaries that the government cannot compete with, poor cyber habits and lack of awareness among the public – this is the problems landscape of Cyberdefence [5]. Establishing voluntary units similar to the Estonian model would help overcome existing obstacles.
A hypothetical case where volunteer cyber defense units might be involved would be a major cyber incident that involves declaring a state of emergency. This incident might be a disruption of Critical Infrastructure, or a major attack against government networks. In these scenarios, the state agencies may be unable to provide immediate assistance.

4. CONCLUSIONS

The cyber unit’s role is to improve readiness through trainings and exercises, and to be available when called upon for specific situations requiring additional help. Capability building and operations - two broad types of activities of units includes distributing awareness raising information, strengthening cooperation between Cyber security specialists in public and private sectors through the sharing of information, and participating in crisis management by protecting critical infrastructure.

In addition, the cyber unit might represent an opportunity for wounded warriors to reintegrate into the national defense, particularly for those unable provide service in a standard capacity. Georgia has about 1,500 wounded warriors from the 2008 Russo-Georgian War and ISAF and other international missions who cannot serve on active duty due to their health. It also can offer access to duty for those not ready to join the armed forces.

Even though the difference between our adversary and us is enormous in terms of military potential, cyber is a domain where a small country can truly resist a much more powerful aggressor. Cyber can become a successful element of an asymmetric response to destructive actions or a sort of on-going front of resistance. The response need not be devastating but it should at least be painful for Russian intelligence services and kremlin-sponsored criminal groups.

RESOURCES:

1. Janne Hakala, Jazlyn Melnychuk. Russia's strategy in Cyberspace. e NATO StratCom COE. Riga, June 2021. ISBN: 978-9934-564-90-1.
2. Joint Cybersecurity Advisory co-authored by authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. April 20. 2020.
3. Dr Andrew Foxall. Putin's Cyberwar: Russia's Statecraft in the Fifth Domain. Russia Studies Centre Policy Paper No. 9 (2016). The Henry Jackson Society May 2016.
4. Eneken Tikk, Kadri Kaska, Liis Vihun. International Cyber Incidents: Legal Considerations. CCD COE, 2010.
5. Cybersecurity and Infrastructure Security Agency. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. 2022. Alert (AA22-110A).