GEORGIAN EXPERIENCE OF DEVELOPING CYBER CAPABILITIES IN THE DEFENCE FIELD

Akaki SHEKELADZE

Georgian Technical University, Tbilisi, Georgia

Large-scale attacks from 2008 and 2011 against Georgia further emphasized the necessity of implementing law on information security and founding cyber actors in the country. Announcing cyber security as a challenge of collective defence and recognizing the ultimate importance of the providing proper cyber security in the defence field, Georgia started developing its cyber capabilities in the sector in early 2014, through its LEPL Cyber Security Bureau. This article will review 8-year experience of Georgia, describe the deterrent issues in this process and bring information regarding the successful steps, which deserve to be noticed.

Key words: *cyber capabilities, cyber defence, Georgian experience, cyber strategy, cyber security, defence sector*

1. INTRODUCTION

Current Russian-Ukrainian war, along with those others of the late 20th and 21st century proved that conflicts no longer take place only in conventional way and malicious activities are noticed in the cyber space, making protection of information infrastructure inevitable for the states.

Critical infrastructure (CI) protection requires adequate planning and approach. The states usually divide certain categories of CI in order to be able to take steps that are tailored to this part of infrastructure. Usually these are: security, energy, finance, defence, education, etc.

What's more, defence sector is even more significant in this regard, as it is the basis of the national security and warranty for the public order.

The aforementioned was proved back early in 2002 on NATO Prague summit, noting that the alliance should strengthen its capabilities to defend against cyber attacks. This was followed by first cyber attacks in the world directly against the states, specifically against Estonia and Georgia, making this an alarming signal, that in parallel to the military actions, conflict would also move to cyber space in case of any crisis in any part of the world.

The abovementioned was proved by nearly all conflicts that occurred in the world later on.

Georgia started building its cyber capabilities with the Georgian law on Information Security and decided to implement cyber policy based on whole of government approach to provide cyber security in the country. There are overall 6 bodies working in the cyber sphere in Georgia. These are:

document is to strengthen cyber capacity and capability of country. The document addresses wide range of subjects such as: Information sharing. exercises and trainings, Public Private Partnership (PPP) and many more.

2. GEORGIAN CYBER DEFENCE

It does not come as a news that defence field distinguishes from other sectors and requires different

Fig. 1 Georgian Cyber Actors

Among these 6 bodies, the information is being shared constantly and this approach also involves cooperation through joint exercises, trainings and forums, which are held in order to reach success in the cyber sphere in the whole country.

In order to strengthen governing process and to plan strategic cyber directions of the country, the National Cyber Security Strategy 2021-2024 was approved by the Government of Georgia. The aim of this conceptual

approach and management. Due to various reasons, starting with different architecture and finishing with personnel, military institutions are subject to specific cyber threats and it is totally impossible to manage cyber threats in defence via centralized approach and/or governmental CERT. Therefore, for the security of military and non-military infrastructure protection of solely this field, bureau started to take actions.

Based on the law on Information Security, in February 2014, sectorial cyber actor was founded – Cyber Security Bureau of the Ministry of Defence of Georgia.

Cyber Security Bureau (CSB) of the defence Ministry is solidly represented in the above mentioned documents of law and strategy and, side by side, with the other national cyber actors, strengthens cyber resiliency of the state.

More than 8-year period does hold substantial information about the steps that were taken to build cyber capabilities in the defense field through human capital, assistance of partners and technical sustainability development. The main chapter will bring specific information on the steps taken and draw emphasis on the challenges Georgia ran into and currently faces up to.

The aims of CSB are the following:

1. Ensure cyber security in the national defense field;

2. Manage cyber attacks and computer incidents against information security in the defense field;

3. Determine information security policy and facilitating its implementation in the defense field;

4. Draft and perfect legislation regulating cyber sphere.

It should be noted that unlike other issues, cyber security unfortunately cannot be addressed through responsive mechanisms. More emphasis is drawn on proactive steps, as our main goal should be prevention of malicious activities. In case the perpetrator steals our military intelligence data, anybody would agree with us, that reactive mechanisms will not be able to minimize such result. Like in any other part of the developed world, minor cyber incidents do take place from time to time, however, prevention of damaging actions is thanks to the efforts that aim to stay resilient to the threats in the cyber space.

Cyber Security Bureau took various steps, which gained positive feedback both from Georgian and foreign experts and field specialists. I will present several examples for the reader.

2.1. Cyber defence strategy

Sectorial strategy is one of the topics, which gained positive feedback from foreign experts. Georgia had its first defence cyber security strategy back in 2014, when the Bureau was founded. The latest edition of this documents is of 2021-2024. The benefits of such paper is that it gives the unique opportunity to be specific, linked to cyber defence challenges, which compromises action plan, indicators of performance and most importantly, the ability to plan properly and execute in the correct way. Having no sectorial

strategy is the same as sailing in the ocean without compass. The Defence Cyber Security has 3 critical directions:

1. Human Capital Development;
2. Institutionalize processes and increase management efficiency;
3. Ensuring technological sustainability.

The aforementioned document is written in compliance with the national cyber security strategy, is also accompanied with its action plan, giving the sector opportunity to know where we are, what are we lacking, what are our next steps, when do we have certain deadlines and how are we assessing the results. Currently, defence sector is the only one in Georgia that shares this attitude of adopting specific strategic document, while various countries do already have such experience: Belgium that has "Cyber Strategy for Defence", Netherlands with "Defence Cyber Strategy: Investing in digital military capability", the United Kingdom with "Cyber Resilience Strategy for Defence", France with "Cyber Defence Policy" and Luxembourg and Czech Republic with Cyber Defence Strategy.

2.2. Cyber reserve

By 2014, when several countries managed to start implementing such programme, ministry of Defence initiated Cyber Reserve project. The benefits of the programme is well-known for everyone, however, it also acted as an assistance for employing qualified personnel in the defence field, which was one of effective solutions to lack of personnel. This project has long-term benefits of having qualified cyber security specialists, ready to help the state in case of war and crisis. The reserve specialists are involved in projects, training programmes and cyber exercises organized for and by Cyber Security Bureau of MoD. In order to further strengthen the project, it is currently under institutional development.

2.3. Education

Military personnel, as end-point users, are frequently used to attack the defence sector worldwide, which further emphasizes vital importance of cyber security awareness.

Defence sector faces the highest risks of cyber espionage and cyber sabotage. Cyber sabotage can be prevented via technical solutions and preventive mechanisms, while espionage, usually deployed via spyware malicious software, requires high awareness levels from the end-user side.

Due to the high number of military and non-military personnel, trainings cannot work as an only way to raise the awareness. Therefore, multiple methods have been used to address the issue, specifically:

1. Organising cyber hygiene courses tailored to the audience, which covers the topics, including practical advice regarding: malicious software and its types, social engineering, phishing attacks, web and e-mail security, smartphone and social media issues, data protection importance and tools, etc;
2. Developing and simultaneously updating distance course of Cyber Hygiene on MoD e-learning portal. This course was made mandatory for all newly-appointed staff in the defence system;
3. Organising phishing campaigns and training programmes according to their results;
4. Handing out and publishing informative leaflets and handbooks regarding cyber hygiene;
5. Sending information regarding practical measures and current cyber threats (f.e. information about currently spread phishing campaign, two-factor authentication activation instruction on a specific platform, etc.);
6. Issuing monthly "cyber digests" focusing on the latest information regarding the news and major malicious activities in the cyber space.

What's more, cyber security is one of the key components in any military and inter-agency exercises, such as Maple Arch, NATO-GEO and Didgori - the largest-scale exercise in Georgia, taking place once every two years.

2.4. International cooperation

Georgia would not manage to properly secure its defence infrastructure without international cooperation. Cooperation platforms exist as of bilateral and multilateral format, as well as with NATO and EU institutions. Thanks to the international partners, defence cyber actor of Georgia participates in the following international cyber exercises and programmes:

1. NATO OCCE&F;
2. NATO CWIX22;
3. NATO MISP;
4. Regional Cyber Defense Center, as a large-scale OSINT sharing international project, involving the USA, Gorgia, Ukraine and Lithuania;
5. EU Projects: EU4Digital, the Common Security and Defence Policy (CSDP), EU Twinning, EU Safe;
6. Educational courses offered by Romanian Dresmara;
7. Amber Mist organised by Lithuanian Armed Forces;
8. Cyber Dawg hosted by US Georgia state;

9. Locked Shields and Cyber Coalition by NATO;
10. Paintball organized by USA Michigan state National Guard and many more.

Georgia also hosts the annual cyber security event – Intermarium Cyber Security Forum, where key cyber security topics, such as: hybrid challenges, modern trends in cyber space, defence strategies are discussed by local and international invited specialists and experts of this field.

2.5. Challenges and way forward

Specificity of cyber sphere makes infrastructure protection never fully adequate to the current and evolving threats. The states have responsibility to develop cyber capabilities that will battle with various, even unpredicted vectors of compromise.

Defence sector is even more complex due to its large scale and cyber threats existing worldwide. CSB and Mod, in order to provide adequate response to these threats and mitigate the risks, conduct audit and intermittent assessments which give the opportunity to deal with the vulnerabilities, as a matter of prevention, rather than dealing with malicious results post-factum.

Another major challenge faces is education. Georgia still lacks the opportunity of cyber security academic education as bachelor and master's programmes. David Aghmashenebeli National Defence Academy of Georgia implemented study discipline of cyber security, which gives the country unique chance to help young people with patriotic spirit, who decided to gain education in the military institution, be trained and become qualified cyber professionals.

Currently, along further deepening all the steps described in the previous parts of the paper, 4 major projects are planned to strengthen defence sector resilience of Georgia:

1. Cyber Security Laboratory - which will increase the digital forensic capabilities, staff will be retrained and qualification upgraded, will be introduced new software solutions that will allow faster and more detailed processing of computer security incidents.
2. Cyber Range – platform which allows, based on various simulation scenarios, to conduct cyber training for different purposes. The platform is widely used by NATO Allies as one of the most effective means to increase and strengthen the capabilities of the cyber defense operations team.
3. Cyber Security Operations Center (CSOC) of modern standards - which will be staffed with information and cyber security analysts, engineers and managers who will monitor the ongoing

processes in the network of the Ministry of Defence from a technically and software-equipped situational room. The main feature of the center is the highest level of confidentiality and on 24/7 basis identification, analysis and response to cyber security incidents. In a close cooperation with strategic partners, a new office of the CSB will be built and CSOC will be stationed there.

4. Cyber Command – while the process is a long-term, various steps have already been taken to consolidate the key elements necessary to provide coordinated and adequate response to cyber threats, including cyber security, network operations and IT services.

Being able to hold an interview with the Director of Cyber Security Bureau, as the lead of cyber defence of the state, Luka Mgeladze points out 3 most successful steps/facts in the Georgian cyber defence, specifically:

1. International cooperation, thanks to which Defence sector improves its networking, gets the opportunity to develop human capital and gains financial resources;
2. Assisting the process of defining cyber security as a priority for defence leadership, giving the opportunity to present relevant solutions, proceed reforms and make structural changes;
3. Current team of CSB – as recruiting and training competent human resources is a key priority for the sector and the field.

Mr. Mgeladze also mentioned that currently defence sector of Georgia faces the following challenges:

1. Human resources outflow – the demand for information security staff rises in both public and private sector, where private organisations have better flexibility and opportunity to offer higher salaries, making this one of the challenges nowadays;
2. Emerging cyber threats, which is a permanent threat especially for Georgia, due to the existence of hostile attitude from the perpetrator, which had malicious actions several times against the country in the past;
3. Cyber security awareness, due to the fact that end-users are always at the front of the line in the cyber space, where even minor mistakes can lead to the terrible consequences, such as data loss, espionage, etc.

2.6. NATO and Georgian Cyber Defence

When developing cyber capabilities in the security and/or defence field in Georgia, as a country striving for Euro-Atlantic integration, NATO attitude should be shared and supported.

Georgia's national security is a constituent part of the global security architecture and change in the latter's security does reflect on our security as well. In the nearest future, there could be epochal change in the global security system under the influence of cyber sphere. This regards to the NATO's Article 5 covering Cyber Attacks.

Article 5 of NATO's charter has existed since 1949, and it is popularly defined as "one for all, all for one". The article reads:

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them.

Article 5 has only been addressed once in the history of the alliance, in response to the terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001.

In 2010, a group of NATO experts, led by the former US Secretary of State, Madeleine Jana Korbel Albright, came to the conclusion that a significant cyber attack on the critical infrastructure of the Alliance countries can be classified as an armed attack and retaliatory actions by military means should be justified. Based on the group's assessments, the 2010 Lisbon summit adopted NATO's first strategic concept of the 21st century, which identified cyber attack as a major threat that could reach such a scale as to threaten Euro-Atlantic security and stability. In 2016, NATO Secretary General Jans Stoltenberg declared cyberspace as a full-fledged operational environment and did not rule out the activation of Article 5 of the Alliance Charter in the event of a devastating cyber attack on any of the member states. According to the General Secretary, paragraph 5 will not be implemented automatically. Everything will depend on the results of the cyber attack and the decision will be made on a case-by-case basis.

Dissatisfaction with Russia's unappealable actions, the victim of which Georgia became multiple times, in the cyber space has also increased in the EU countries. In May 2019, the European Council approved a package of measures to be implemented in response to cyber-attacks, or even attempted cyber-attacks, against member states.

In this direction, the years 2020-2021 were important, when the cyber attacks of an unprecedented scale by Chinese and especially Russian hacking groups against American critical infrastructure facilities created significant challenges for American national security and economic stability. It got to the point that on June 16, 2021, at the Biden-Putin meeting in Geneva, the Russian president was given a list of critical American infrastructure (16 sectors), against which cyber attacks will be considered a red line.

The Secretary General of NATO said in a speech at the headquarters of the "Atlantic Council" in Washington, that the alliance should not distinguish a cyber attack from other types of attacks and should determine the threshold value of the consequences of a cyber attack, after which Article 5 will be triggered. The speech of the Secretary General took place before the summit held in Brussels on June 14, 2021 and can be considered as a signal sent to the legislators of the member states - to seriously start discussing the mentioned issue in the legislative bodies.

The dynamics of the development of events show that in the coming years, the amendment to Article 5 of the NATO Charter will be made, which will be a historic event in strengthening global security. It is natural that the mentioned change will affect Georgia as well.

Georgian defence sector puts all the possible efforts to follow the pace of this development and it is highly likely, that even in case of not yet being a NATO-member state, the state will follow the alliance decisions and take all the steps the alliance countries do.

3. CONCLUSION

Georgian experience of developing cyber capabilities should be taken into consideration, as it started with being one of the first states to be attacked and saw multiple attempts of compromise. However, the statistics hardly presents successful attacks solely in the defence field since 2014. Human resources efforts and implemented technical tools through the vast and honest assistance of international partners, did block various potentially malicious activities. Strong international cooperation allows the country to share experience regarding the cyber issues and be part of international cyber community, which is unprecedentedly valuable.

However, the aforementioned solutions may be relevant today. As cyber threats are continuously emerging and cyber offensive capabilities of perpetrators do really rise in fast pace, there is an emphasized necessity to be qualified, flexible and innovative.

Cyber security is a crucial part of collective defense and cyber actor in any country should be representing military sector which will make all the necessary efforts for its proper development. In this process, similar to Georgian example, it is vitally important and ultimately useful to draft sectorial orientation documents, have tight cooperation with Western partners and stay awake to be innovative.

4. ACKNOWLEDGMENT

The views given in the article belong to the author and do not reflect official position, opinion or strategy of the Ministry of Defence of Georgia, nor of CSB.

REFERENCES

[1] Maxmeets (2019): *NATO's Cyber Policy 2002-2019: A very, very brief overview* from http://maxsmeets.com/2019/12/natos-cyber-policy-between-2002-2019-a-very-very-brief-overview/

[2] Georgian law on Information Security (2009) https://matsne.gov.ge/ka/document/view/1679424?publication=5

[3] National Security Council (2021): *National Cybersecurity Strategy of Georgia and its Action Plan have been approved* from https://nsc.gov.ge/en/NEWS/georgia-national-cybersecuri.html

[4] Ministry of Defence: *Cyber Security Bureau* from https://mod.gov.ge/en/page/59/cyber-security-bureau

[5] Agenda (2021): *Defence forces lead inter-agency Didgori 2021 drills for crisis scenarios* from https://agenda.ge/en/news/2021/3452

[6] NATO (2021): *Substantial NATO-Georgia Package (SNGP) and Georgian Ministry of Defence host "Intermarium Cyber Security Forum 2021"* from https://www.nato.int/cps/en/natohq/news_188399.htm?selectedLocale=en

[7] Ministry of Defence: *Cyber Security Strategy of the Ministry of Defence of Georgia* from https://mod.gov.ge/en/page/134/cyber-security-strategy-of-the-ministry-of-defence-of-georgia

[8] NATO (2022): *Collective defence - Article 5* from https://www.nato.int/cps/en/natohq/topics_110496.htm

[9] NATO (2010): *Lisbon Summit Declaration* from https://www.nato.int/cps/en/natolive/official_texts_68828.htm

[10] Sean Lyngaas (2021): *Biden says he gave Putin list of 16 sectors that should be off-limits to hacking,* CyberScoop, from https://www.cyberscoop.com/biden-putin-summit-russia-geneva/

[11] Daniel Malloy (2021): *Secretary General Stoltenberg explains why NATO is getting serious about cyber and China 'is not an adversary'*, Atlantic Council, from https://www.atlanticcouncil.org/blogs/new-atlanticist/secretary-general-stoltenberg-explains-why-nato-is-getting-serious-about-cyber-and-china-is-not-an-adversary/

[12] CCDCOE: Strategy and Governance from https://ccdcoe.org/library/strategy-and-governance/

[13] Council of the EU: *Strengthening EU-wide cybersecurity and resilience – provisional agreement by the Council and the European Parliament* from https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

[14] Robert Gordon & Martyn Bull: *The defence cyber threat landscape in 2022,* Riskaware from https://www.riskaware.co.uk/insight/defence-cyber-threat-landscape/