CYBER SECURITY BUREAU

Cyber Security Strategy
of the Ministry of Defence of Georgia

2021-2024

Table of Contents

Minister's speech

Activities of the Ministry of Defence of Georgia, that contain components including combat training, operation planning, military exercises, logistics or day-to-day activities, strongly depend on the safe and proper functioning of the information and communication systems. Therefore, ensuring the cyber security of these systems in peacetime, emergency and war situations is one of the strategic goals of the Ministry of Defence of Georgia.

Amid rapid technological advances and an increasingly complex security situation, hybrid threats continue to dominate. From a wide array of hybrid means, the cyber component is actively used for sabotage, espionage and psychological operations. The agenda includes the need for consistent development of cyber security capabilities of the Ministry of Defence, which requires complex planning and proper execution.

The cyber security strategy for the medium term, envisages the strengthening of critically important areas that create a solid precondition for the Ministry of Defence of Georgia to adapt its cyber capabilities to NATO and EU standards.

Juansher Burchuladze

Minister of Defence of Georgia

Introduction

The Cyber Security Strategy and the Action Plan are medium term documents, which define the principles, directions, goals and objectives of cyber security development in the defence field of Georgia.

Strategy is compatible with conceptual documents including The National Security Concept, The Threat Assessment Document, The National Cyber Security Strategy, "Vision of the Ministry of Defence 2030" and "Strategic Defence Review 2021-2025 (SDR) Document". Moreover, Cyber Security Strategy shares international obligations, agreements and treaties undertaken by the Ministry of Defence of Georgia.

Strengthening cyber security in the Ministry of Defence of Georgia and its structural units, as well as creating a safe environment for personnel, requires a systematic approach and proactive implementation of cyber defence policy. Accordingly, Cyber Security Strategy and Action plan, based on years of experience accumulated from encountered challenges and the interdepartmental, national and international level experience, formulates strategic goal achieving activities that ultimately enhance and improve the cyber security posture of the defence system.

Successful implementation of the goals outlined in the document will facilitate wider integration of cyber elements into operations organized by the defence forces and increase cyber potential of the military.

Current situation

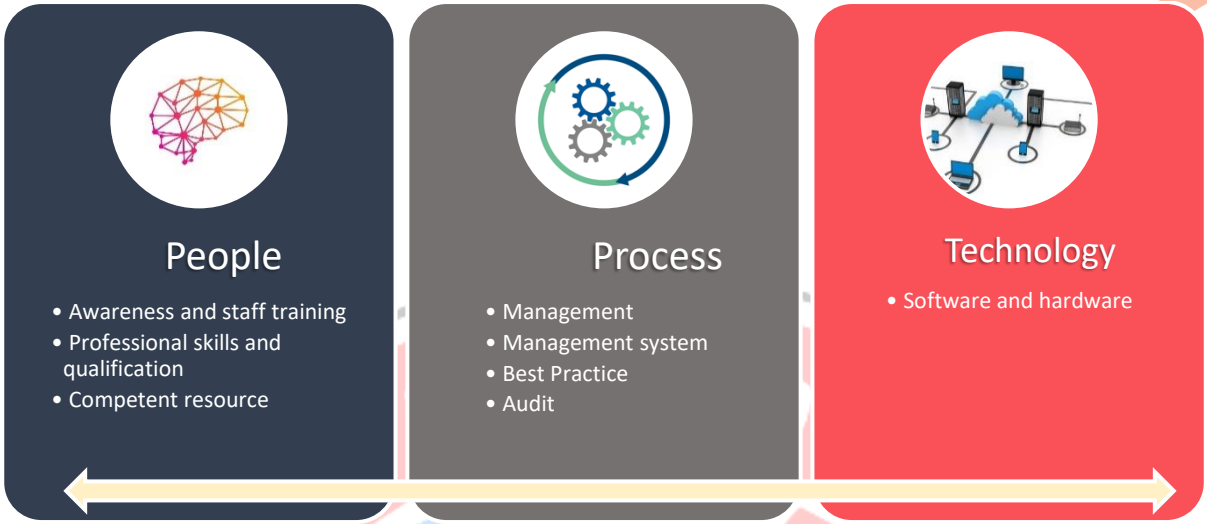
The urgency of creating the document is due to the development of information and communication technologies and the growing dynamics of cyber-attacks. As a result of the ongoing institutional changes in the MoD, activities are being automated, digitized and unified. Centralized management systems are being introduced. This process ensures the development of effective management and communication models, but on the other hand, significantly increases the likelihood of cyber-attacks and the risks of information system compromise.

Based on the understanding of the situational analysis in the Ministry and the best practices in the field of cyber/information security (ISO, NIST, CIS, etc.), the need for changes and improvement of existing approaches has been identified, which should ensure the development of effective and efficient models of process planning, management and monitoring.

Improperly protected cyberspace poses significant challenges and serious risks to the defence system. Unauthorized access to information systems by cyber-attackers can cause leakage of confidential information and various types of intelligence-sabotage actions can be carried out, which ultimately aim to reduce Georgia's defence capabilities and represent the country as an inappropriate partner to the international community.

What do we want to achieve by 2024? - People, Process, Technology

People conduct different activities with its own intellectual resources. processes make these activities more efficient and technology allows processes to be automated and optimized. In the context of this provision, the transformation from a narrow technical direction of cyber security to a strategic level system, requires a complex approach. The document discusses cyber security and the accompanying strategic goals in the context of the above interrelated directions. The goals and action plan activities formulated within the framework of the cyber security strategy, serve to increase cyber capabilities in the three areas mentioned.



PEOPLE- Humans are one of the critical components of cyber security. They plan, manage, monitor and evaluate organizational processes. The component integrates the human factor, regardless of their role and responsibilities.

PROCESS - The component includes all types of business processes that serve the strategic goals and objectives set by the organization.

TECHNOLOGY - The technological component consists of hardware and software, which together is the most important element for ensuring cyber security.

Succeeding in the above areas is related to the implementation of specific activities. Accordingly, given the trends in the cyber security dimension and the urgency of the challenges facing the Defence, by the end of 2024, the Ministry will improve cyber security in three areas and focus on achieving the following strategic goals:

1. Human capital development;

2. Institutionalize processes and increase management efficiency;

3. Ensuring technological sustainability.

Methodology and Resources

The Cyber Security Strategy is based on cyber security recommendations prepared by The Global Cyber Security Capacity Center at Oxford University, the US Georgia National Guard and other international partner organizations. The document identifies the problem and sets out clearly formulated goals, objectives and actions for their solution.

The Key Performance Indicator (KPI) is used to measure the performance of specific activities set out in the Action Plan of the document, which provides risk-based planning and effective monitoring.

Both human and financial resources will be used to carry out the activities defined by the cyber security strategy. The activities envisaged by the Cyber Security Strategy, the implementation of which requires material and financial resources, will be done with the budget funds allocated to the LEPL Cyber Security Bureau and with the financial support of partner countries / donor organizations.

Human resources

Implementation of the directions mentioned in the strategy requires properly trained human resources, which will ensure the achievement of the ultimate goal.

Given the high competition in the cyber security market, mobilizing and retaining qualified personnel is a common challenge, however, with the support of the Ministry of Defence, the Cyber Security Bureau has made adequate investment in recruitment/development, bringing the payroll closer to competitive conditions and a successful recruitment policy. In addition, through close and fruitful communication with strategic partners/organizations (US, UK, EST, LITH, NATO), through systematic staff training, the Bureau ensures the growth of organizational competence. At the moment, the competence of the Bureau staff corresponds to ISO, NIST, SANS and other international standards.

The document on human resources refers not only to the qualified staff of the Bureau, but also to the human resources of the Ministry's sub-departments involved in the goals and activities of the strategy, as well as the expertise of the partner countries/organizations needed to accomplish a specific goal or activity.

Financial resource

The Ministry of Defence of Georgia and the Cyber Security Bureau understand, that maintaining the best balance between providing cyber security and the necessary financial support is critical.

Cyber security is a strategic direction in the current institutional development of the Ministry, which is expressed in various actions with the support of the Ministry's leadership. The Ministry realizes the responsibility of fulfilling strategic tasks and comprehensively implements and increases financial and material support to create a strong cyber defence environment.

To achieve the goals and objectives mentioned in the strategy, the financial resources of the Cyber Security Bureau will be used in full, which is subject to growth for the medium term. In addition, where, due to the critical importance of the task, it will be necessary to mobilize additional financial resources, the Ministry of Defence of Georgia will provide funding/co-financing for the direction/activity. At the same time, the involvement of international partners in the process and their financial support is critical in this regard.

The Strategy Action Plan outlines specific activities that require the support of international partners. Without this, the issue of effective implementation of the activity and achievement of goals will be at significant risk.

Strategic Goals

Goal 1: Human Capital Development (People)

Based on the analysis of cyber incidents in the Ministry of Defence, it is clear that the human factor is one of the most vulnerable components in ensuring cyber security. On one hand Inadequately qualified and insufficient technical staff and on the other hand untrained end users are the mixed factor that significantly increases the vulnerability of critical information infrastructure.

Goal 1 is a set of actions that, based on systemic approaches, ensure the development of human capital.

Objective 1.1 Increasing human capacity through engagement in educational activities

For effective functioning of cyber security, personnel with relevant knowledge and skills are critically important. This applies equally to computer security planners and implementers, as well as end users of computer services.

Information security experts agree, that internet users are the most vulnerable in the field of cyber security. Despite the availability of the latest technological tools, a large proportion of the incidents are due to the human factor.

Given the scale and complexity of the defence system, great attention is paid to the appropriate training of personnel. Therefore, to ensure adequate level of knowledge of internet users, permanent awareness raising activities are critically important, which helps to minimize cyber risks facing the system.

The Ministry of Defence believes, that in the changing cyber security environment, highly qualified and knowledgeable cyber specialists are needed. Internationally qualified cyber specialists based on relevant knowledge will plan and conduct various security-oriented tasks.

Objective 1.2 Strengthening technical skills of specialists in the field of cyber security by participating in various types of cyber exercises and projects

Asymmetrical growth of cyber-attacks is in parallel with the rapid development of information technology. In changing cyber environment, adversary is permanently changing tactics, techniques and procedures (TTP) of cyber-attacks. Therefore, it is important that cyber specialists regularly participate in a variety of activities, which aim to develop practical cyber skills, as well as to introduce current best practices in the operating environment.

Involvement in the high-level cyber exercises is needed to strengthen the practical skills of the cyber security technical team. These activities are the best way to increase competence, which by simulating real-time cyber crisis scenarios, contributes to the capacity building.

It is important to focus on different types of projects concentrating on cyber security issues. Active participation in projects, on the one hand, facilitates sharing of best practices and allows the knowledge and experience gained to be used on an everyday basis.

Goal 2: Institutionalize processes and increase governance efficiency (Process)

Some of the ongoing processes within the Ministry need improvement and institutional refinement. Fragmentary planning and management mismanage processes, which in turn affects the effectiveness of a particular goal or task.

Goal 2 ensures improvement and adequate updating, planning and execution of processes based on risk analysis.

Objective 2.1. Optimizing governance via risk-based planning

Proactive planning of processes is critically important in order to strengthen country's defense capabilities. Therefore, it is important to have clear and distinct cyber-operational plans or scenarios, which will create a proper precondition for the active and effective use of cyber elements in a war or crisis situation.

The Ministry of Defence of Georgia considers the introduction of information security standards as one of the most important areas of cyber and information security in the field of defence. Internationally recognized standards, enhance the security of information assets and give opportunity to manage risks and incidents.

Information assets, risk management and methodology, as well as, development and implementation of other important rules and policies, will further enhance the degree of infrastructure protection of defence system. In addition, introduction of an information security systems in the critical information system subjects of defence sphere, represents an important factor for strengthening cyber security.

Periodic assessment/audit of information and communication systems is equally important. In case of timely detection of vulnerable areas and adequate response to them, it is possible to avoid disruption of network infrastructure and disruption of system integrity.

Objective 2.2 Research and Analysis

Depending on the pace of development and effective provision of cyber security, it is advisable to conduct research and analysis of different types and purposes in the Ministry of Defence of Georgia.

Additionally, in order to assess the cyber security environment in the defence field, periodic research and analysis should be conducted to identify weaknesses and raise the issue of initiating necessary changes. Moreover, such assessments should be based on international standards and questionnaires and research methods should be developed based on them.

Regular research and analysis of existing and potential risks in cyberspace is needed. Understanding the threats and assessing their potential impact, will help strengthen security measures. Based on the threat assessment and risk analysis, preventive measures should be developed in order to overcome challenges. In this regard, research and analysis of innovations in the field will contribute to the development of cyber capabilities of the Ministry of Defence of Georgia and introduction of best practices in this area.

In this contexts, assessment of the existing legal basis in order to alighn our reality to international standard is of the utmost importance.

Goal 3: Ensuring Technological Sustainability (Technology)

The Ministry of Defence, as well as the whole country, is facing the inevitable digitization process, which significantly simplifies the case management and takes the processes to another level of efficiency. On the other hand, due to the specifics of the work of the Ministry, various command systems are under the influence of cyberspace, which requires adequate protection by using advanced technologies.

Goal 3 By integrating modern cyber defence infrastructure and accompanying processes into the system, it is possible to provide security and proactive cyber defence mechanisms.

Objective 3.1 Strengthening cyber capabilities through high level technical support

For ensuring an adequate level of cyber security in the field of defence, permanent development of technological capabilities is necessary. With the integration of latest technologies in the field, the Ministry will be able to effectively and timely implement set priorities.

Introduction of new technologies is the main pillar for the development of cyber defence capabilities, for which appropriate resources should be allocated and staff properly trained. Introduction of innovative approaches and the latest technical capabilities in the cyber security architecture of the Ministry, enables prevention of malicious actions.

The Cyber Security Bureau should take proactive measures to ensure the security of critical information systems of the Ministry of Defence. This way, in the properly equipped environment, through infrastructure monitoring and effective response the resilience of the system will be increased.

In order to ensure proactive cyber security, it is critically important to exchange information on national and international level. Cyber Security Bureau should continue such involvement in similar platforms.

Ways & Means to achieve strategic goals

Given the rapid development of cyber security and the limitations that do not exist in this dimension, it is difficult to fully respond to challenges on an individual basis. Consequently, close cooperation and exchange of information on cyber incidents is of immeasurable importance.

The Cyber Security Strategy of the Ministry of Defence of Georgia considers cooperation at different levels not as a goal, but as a means/way to achieve strategic goals.

Intra-agency, national and international cooperation are the main means by which strategic goals and activities set out in the document will be actively and effectively used. In general, this will increase cyber capabilities of the Ministry of Defence of Georgia and approach to the western standards.

Intra-Agency (MoD) cooperation

One of the critically important methods of achieving strategic goals is cooperation at the intra-departmental level. This component acquires special character, when management requires complex approach and active participation of various sub-departments.

The structural units of the Ministry of Defence of Georgia are formed in the unified system, which are closely connected by information technology and communication systems.

Cyber security of the critical infrastructure of the Ministry of Defence is provided by the LEPL – Cyber Security Bureau (CSB), which is in close cooperation with the J-6 communications and Information Systems department of the General Staff and Information Technology department of the Ministry of Defence. Cooperation includes providing cyber security not for only network infrastructure, but also securing different applications of the Ministry.

Close communication and cooperation with other relevant structural units of the Ministry and legal entities of public law (LEPL) are of vital importance, because they are all a part of the unified system and cyber-attacks against them are directly related to the breach of the

confidentiality, integrity and accessibility of the unified information and communication system of the Ministry.

Hence in case of inadequate level of cooperation, the Ministry of Defence faces significant challenges, because despite the effective operation of individual structural units, if the processes are not planned and implemented with the unified approach, it will be difficult to provide a complex defence system with cyber security.

National level cooperation

The existing format of cooperation at the national level ensures cyber threat response and information sharing. Cyber actors of different state levels are involved in this process and functions are not duplicated. These agencies are: National Security Council (The deliberative body of the Prime Minister on national security issues), LEPL Digital Governance Agency DGA (Ministry of Justice of Georgia), LEPL Operative Technical Agency (State Security Service of Georgia), LEPL Cyber Security Bureau (Ministry of Defence of Georgia) and Cyber Crime Division (Ministry of Internal Affairs).

The need for inter-agency cooperation was identified in order to adequately respond to the challenges in cyberspace and to ensure national cyber security at an appropriate level. The national security mechanism should function as a unified system and not as a mechanical unit of separate component. A unified governmental approach to planning and implementing national cyber security ensures usage of the existing resources with coordinated efforts.

The Ministry of Defence shares unified state approach, that includes involvement of the national level critical information system subjects, business sector, academia and information society (PPP) in the development of cyber security in Georgia.

With enhanced cooperation at the national level and unified governmental approach, the Ministry of Defence will be able to take into account the scenarios of cyber security developments in the plan of crisis management during peace, emergency and war times. Organizing such a unified state effort in the field of cyber security will also help to prevent threats in cyber space and reduce the damage caused by incidents.

International level cooperation

In the modern world cyberspace is actively used for political, military, economic and other purposes. As technology evolves, it becomes more and more difficult to prevent risks and threats in cyberspace, especially when the cyberspace has no defined boundaries.

To strengthen national cyber security and contribute to global security, one of the critically important components is to strengthen cooperation at the international level and share best practices.

Enhancing cooperation with technologically advanced strategic partners in bilateral and multilateral formats contributes to the growth of the Ministry's cyber capabilities. The close alliance with NATO and the EU ensures the involvement of the Ministry's cyber specialists in various educational programs, cyber exercises, seminars or conferences, which in total increases the compatibility of the Ministry with Western standards and doubles Geo MoDs contribution to partner's initiatives.

Conclusion

Existed document is a strategically important statement, implementation of which will allow the Ministry of Defence of Georgia to be properly and effectively ready to deal with cyber challenges in today's world.

Considering identified priorities and achieving targeted indicators, makes it possible in the coming years to have an even more sustainable information and communication infrastructure.

The classification of the objectives and action plan activities in to three directions (people, process, technology) makes the relationship and integration of its components clearer. By strengthening the relevant elements, we will achieve all the strategic goals, that are vital for the Ministry of Defence in combating cyber threats.

Fulfilling obligations set out in the strategy will make a significant contribution to the Ministry's compliance with NATO and EU standards and increase the quality of international cooperation at the strategic, tactical and operational levels, which will have a positive impact on the national security agenda.

Thus, the Ministry of Defence of Georgia recognizes the importance of coordinated actions to deal with cyber security in the context of global strategic security, the urgency of cyber security issues and the importance of coordinated action. Accordingly, it identifies the strategic directions and priorities of development that we should rely in the coming years.