**REPUBLIC OF LATVIA**
**MINISTRY OF DEFENCE**

# NATIONAL ARMED FORCES
# CYBER DEFENCE UNIT (CDU)
# CONCEPT

Riga
2013

## Introduction

In accordance with the National Security Concept, information technology threats or actions directed against the interests of national security in electronic information space are among the most topical national security threat factors. Under circumstances when state administration, society and the economy depend on the services ensured and supported by information technologies, illegal use, damage, paralysing or destruction thereof may cause threats to state and public security, public order, as well as may leave a negative impact on state economy.[1]

The state security concept states that in the future, most likely, national threats will be caused by attacks that will vary in the form and character and they will be mutually related and difficult to predict. These attacks will be related both to traditional military operations and non-standard methods of military operations, including terrorist, organised criminal actions, as well as attacks on information technologies, informative war and psychological influence. The enemy will be able to act by using both physical and virtual influence, acting on land, the sea, in the air, as well as cosmic and electronic information space.[2]

Cyber security related issues become more and more topical also in NATO and the EU that develop a single policy for the research, identification and observation of cyber threats, as well as improve cyber defence capabilities. In 2011 NATO approved a Policy on Cyber Defence of the Alliance and elaborated a detailed plan for the development of capabilities. According to international practice, taking into account the presence of information technologies in any sphere and the broad usability, state resources are limited and insufficient to prevent large-scale threat and crises. Both the neighbouring countries of Latvia and other EU and NATO Member States form various state and private or civil-military collaboration forms to ensure the involvement of reserve experts in the security and defence of information technologies.

[1] Article 3.7 of the National Security Concept.
[2] Articles 11-12 of the State Defence Concept.

Information Technology Security Incidents Response Institution CERT.LV has been set up in Latvia that on a daily basis provides support to state and municipal institutions, merchants, and natural persons in terms of incident prevention, and maintains unified portrayal of the activities taking place in the state electronic information space. The Information Technology Security Law sets forth most important requirements for state and municipal institutions and merchants, as well as the obligations and tasks of CERT.LV at peace-time. In case of state threat, the Cabinet of Ministers may adopt a decision regarding transfer of CERT.LV tasks, rights and resources to the National Armed Forces.

State security institutions have identified the critical infrastructure of the cyber space and are currently involved in the creation and supervision of the defence system thereof in accordance with the national regulatory enactments.

Even though institutions, which ensure national cyber security capabilities, have been set up in Latvia, plans for action in the case of increased threat have been elaborated and they are being improved on a regular basis, and involvement of experts is available in collaboration with the private sector; however, the entirety of the present resources and measures is not sufficient and organised enough to ensure efficient and prompt action in the case of serious and extensive cyber incidents or cyber attacks.

Taking into account the security environment, threats existing therein and limited resources at the disposal of the state administration, it is necessary to form an entirety of experts as a reserve unit, which would unite those employed in the private sector and experts having the wish to participate, and which would provide support to the state and private sector in collaboration with CERT.LV in a crisis situation or at the time of war. National Guard service ensures legal basis and serves as a way how to involve high-qualification experts of the private sector in the fulfilment of state defence tasks in an organised manner. Patriotic information technology experts have a chance to become involved voluntarily and, receiving state support, to form collaboration, improve knowledge, participate and organise cyber attack prevention training and, in case of necessity, to provide support to state and private structures. The creation of such unit would both strengthen capabilities of the state to react on

crisis and war situations and enhance collaboration between state administration and private sector in the field of cyber security.

**Goal, functions and tasks**

In order to ensure the formation of reserve cyber defence capabilities in the state, which could be used both for civil and military tasks, there is a **goal** to create a Cyber Defence Unit (CDU), which would be able to attract highly-qualified information technology experts for the fulfilment of state defence tasks during their free time from basic work.

**Basic functions** of the Cyber Defence Unit are as follows:

1. Provision of support to CERT.LV and units of the National Armed Forces in crisis and war situations in terms of the prevention of information technology security incidents and overcoming of consequences occurred in the cyber space if resources at the disposal of CERT.LV are insufficient and the involvement of the unit speeds up the implementation of urgent measures or if special resources for the performance of these activities are at the disposal thereof.
2. Preparation and ensuring of national guards who would form the unit and are able to provide support to CERT.LV and units of the National Armed Forces in crisis and war situations.

In order to achieve the goal and ensure the implementation of functions, the Cyber Defence Unit shall fulfil the following **tasks**:

1. Study and recruitment of information technology experts for participation in the Cyber Defence Unit, elaboration of a development and work plan of the unit.
2. Ensuring initial military and further professional training of the involved national guards.
3. Planning, organisation and ensuring of participation in national and international level trainings. Regular participation in cyber defence training processes in NATO, EU, bilateral, and regional format, including NATO

Cooperative Cyber Defence Centre of Excellence and organisation of regular national level training.

4. Formation of expert examinations in collaboration with military CERT experts of the National Armed Forces and CERT.LV, participation in new security solution testing and evaluation, and provision of proposals for the improvement of cyber defence.
5. Preparation and participation in NATO, EU or regional cyber defence units or reserve.
6. Promotion of civil-military collaboration or public and private partnership in the field of cyber defence.
7. Promotion of the understanding and knowledge about cyber threats among information technology experts and the society. Involvement of the Young Guard, promoting education of youth and further interest in becoming involved in the field of information technology security and defence.

**Formation of the unit**

Taking into account the normative basis, from the point of view of administration it would be most appropriate to form the unit within the scope of the National Guard, whereas to organise the operational subordination and activity in conformity with consolidated and efficient use of resources, including maximum promotion of the use and collaboration of the available experts.

IT experts, who correspond to the following criteria, shall be involved in the formation of the unit:

- Knowledge and skills required to fulfil the tasks of the unit;
- Patriotism and desire to provide contribution towards strengthening state security;
- Compliance to work with state secret (including NATO, EU);
- Innovative manner of thinking, ability to rapidly become adjusted to the changing information technology environment; and
- Ability to devote 1-3 days per month for training and fulfilment of service tasks at the place of service or in virtual space.

Involvement of IT experts in the unit is motivated by:

1) participation in international training and measures within the scope of NATO, EU, bilateral and regional format and broadening of their professional knowledge;
2) acquiring knowledge and practising abilities in the information technology environment of defence department in collaboration with military CERT experts of the National Armed Forces and participation in cyber operations; and
3) becoming acquainted and collaborating with international experts in the field of defence and security in cyber space.

Thereby not only cyber security capabilities of state structures will be promoted, but also the private sector will have a chance to improve the qualification of its experts and to strengthen cyber security of companies.

Further steps to launch the formation of the unit:

1. Creation of a project group of the unit that is formed by 2-3 experts, who elaborate operational capabilities of the unit and the implementation action plan thereof.

2. On the basis of the recommendations of the selected experts and the environment evaluation of IT professionals, an entirety consisting of at least 5 highly-qualified information technology experts shall be set up that in addition to the basic work has agreed to provide consultations and comments on the formation action plan of the unit and planned measures.

3. Organisation of meetings and presentations at higher education establishments and large companies focused on IT specialisation or significant IT activity maintenance sector, informing about the formation of the unit, its tasks and potential benefits to the employees of the unit.

4. Formation of direct and continuous contact or regular collaboration with large companies whose networks and systems traditionally are exposed to high threats and therefore recruiting higher-qualification experts (banks, electronic communication service providers, transport companies, etc.), encouraging to

participate in the operation of the unit and offering to include risk factors related to the sphere of activity of the relevant company in training scenarios.

5. Gathering of information about and involvement of ex-service experts of professional military service, offering a chance to retain a link with military environment, which is related to their basic profession.

6. Involvement of the students of IT study programmes at Latvian higher education establishments in the activity of the unit, offering military cyber training thereby preparing potential IT experts of the unit.

Formation of the unit and attraction of participants are organised in collaboration with CERT.LV and the IT/IS Security Expert Group formed within the scope thereof.

**Operation of the unit**

Work of the unit is organised both in virtual space and by organising regular meetings, as well as organising and participating in national or international trainings.

Depending on the operational necessity or specialisation, experts of the unit will be divided in groups, for instance, fulfilling the obligations of fast response group, cyber laboratory personnel or leaders of groups. Taking into account the planned number of (full time) professional service soldiers in the unit, its internal structure and division of obligations must be based on experts who are leaders in terms of opinions and expert examinations in their particular field, and are capable of gathering IT professionals with a similar specialisation around them. Application of such concept has proved itself in the units of other states when a group not related to the formal structure, which includes all necessary expert examinations and support, is being formed for the fulfilment of a specific task.

Even though most significant location of IT experts is Riga, it is planned to develop elements of the unit also in regional centres, considering the possibility to use higher education establishments, which offer IT speciality study programmes, as the basis.

Formation of CDU capabilities is planned over a period of five years:

- at the beginning of 2015, the unit will reach initial operational capabilities;
- at the beginning of 2018, the unit will reach full operational capabilities;

Further action:

1. Commencement of the implementation of steps described in the document for the formation of the unit.

2. Study and use of international and national experience to elaborate in detail during the formation of the unit and develop further the idea of cyber defence unit reservists.