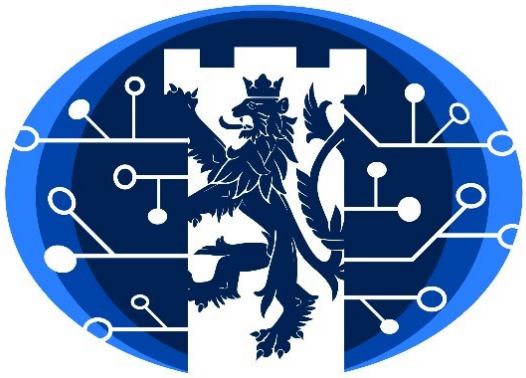

Cyber Defence Strategy of the Czech Republic

2018 – 2022

National Cyber Operations Centre

Introduction

Ensuring security of citizens, protecting sovereignty, territorial integrity, principles of democracy and the rule of law belong to the state's fundamental roles. To sustain these values, the state also needs a complex system of state defence based on a long-term vision.

Substantial social and technological developments have generated the need to change routine forms and methods applied in the field of defence. Current conflicts are increasingly waged by asymmetric warfare methods, with many activities taking place in cyberspace. In this context, also fast development of artificial intelligence and robotic systems must be mentioned.

The Czech Republic considers build-up of defence capacities in cyberspace vital, also with respect to its NATO membership, since NATO acknowledges cyberspace as a planning and operational domain and a cyber attack as a potential activator of Article 5 of the North Atlantic Treaty. Therefore, in accordance with terms of Article 3 of the North Atlantic Treaty, the parties to the Treaty should maintain and develop individual as well as collective capabilities to resist even cyber attacks.

The Czech Republic responds to the above mentioned facts and gradually adopts necessary measures. Yet, handling of cyber attacks has been hampered by system shortcomings. Even though cyber security has reached a high level, a system solution of cyber defence is at the beginning only. Moreover, understanding and definition of these terms differ.

For the explanation it is convenient to say that according to the government's approach, cyber defence is an autonomous and specific branch of a wider cyber security concept. In this context, cyber defence is perceived as part of state defence ensured on the basis of the Act on Ensuring Defence of the Czech Republic. The Act defines state defence as a complex of measures taken to ensure sovereignty, territorial integrity, principles of democracy and the rule of law, and to protect the lives of citizens and their property from an outer attack. This defence includes building-up of an efficient state defence system, preparation and engagement of relevant forces and means and participation in the collective defence system.

Compared with that cyber security is perceived as a complex of tools aimed at ensuring cyberspace protection. These tools can be of varied nature – legal, organizational,

educational, technical, etc. To put it simply, cyber security is supposed to ensure confidentiality, integrity and availability of information and data in the cyberspace.

Cyber defence differs from cyber security mainly in the nature and intensity of attacks, with no possibility to define exact criteria. Therefore, readiness for cyber attacks must be complex and must not focus on the security field only. The state must develop also its capabilities to resist even such attacks that might activate the state defence. Thus, cyber defence would be activated only in case of the most intense attacks. A specific feature of cyber defence will be the fact that it will be active not only in emergencies – mostly in cooperation with other defence bodies of the Czech Republic, but also permanently in non-emergency situations.

A cornerstone of developing an efficient cyber defence system in the Czech Republic was a Government's requirement anchored in the Action Plan for the National Cyber Security Strategy 2015–2020, where a requirement for building-up and strengthening of cyber defence capabilities was set forth. The responsibility for cyber defence has been assigned to the National Cyber Operations Centre (hereinafter NCOC). The concept has been based on conscious understanding of differences between cyber security and cyber defence.

Conceptual conditions of proper state defence in cyberspace are defined by this Cyber Defence Strategy, divided into a public and a non-public part. The public part includes basic visions and, generally, also individual objectives, describing the planned end state of individual areas of the problem concerned. The public part is more general due to the nature of the matter at hand, whereas the non-public part brings a list of specific measures planned to be taken to meet individual objectives. The defined measures stem from defence policy principles of the Czech Republic, reflect current trends of modern defence doctrines and are in full compliance with basic rules of a democratic state. The preparation of these measures respected the premise that the defence is here to maintain and protect basic rights and freedoms of individuals as well as the above mentioned principles and values, since security and freedom do not contradict one another. There is no freedom without security. There is no security without freedom. Thus, the defence measures have been prepared on the proportionality principle to ensure that the Czech Republic is a democratic and safe state with capabilities to protect these values.

Cyber defence key challenges in the Czech Republic

There is a rather huge number of potential attackers able to carry out a cyber attack that would activate cyber defence of the Czech Republic, including both state and non-state actors. Cyber attacks are namely ideal tools for damaging political, business or other targets, and also a strong tool for the attackers to enforce their own will. At the same time, it is often very difficult to identify the attacker, mainly in real time, which decreases the risk of a potential adequate response. These facts along with relative absence of geographic and similar limitations offer a great advantage to the attacker.

Primary targets of these cyber attacks can be especially systems closely interconnecting the computer environment with the real infrastructure, for example in water management, energetics, *etc*. The attacks can even directly target components of the defence infrastructure.

As to cyber defence of the Czech Republic, the most important threat stems from growth of offensive cyber capabilities in potentially hostile states. Other significant threats include a growing threat of cyberterrorism and systematic strengthening of cybercrime structures as well as mutual interconnection of state and non-state attackers.

Priorities in the field of cyber vulnerabilities overlap to a great extent in both cyber security and cyber defence. The most crucial vulnerabilities are low digital literacy and insufficient awareness of individual users of security rules to be observed in cyberspace, mainly in connection with the growing number of the Internet of Things (IoT) appliances. Furthermore, cyber defence sees increasing vulnerability in growing dependence of the state security forces on information and communication technologies.

Most important challenges in detail:

New trends of influence promotion

Recently, the role of non-conventional and unprecedented methods used to achieve political and strategic goals has been growing permanently. The battles have been fought in asymmetric forms. It has become increasingly difficult to distinguish outer attacks from inside ones. Tools of power influence enforcement frequently shift from typical military campaigns to information operations. In this context, the cyberspace plays an important role as part of a broader concept of influence promotion. A real threat stems from engagement of modern robotic military, but also non-military systems or artificial intelligence for these purposes. The threats posed to sovereignty, territorial integrity, principles of democracy and the rule of law have amplified significantly.

State actors

The past decade has repeatedly witnessed cyber attacks worldwide. Given their sophistication and scale, they have been directly or indirectly ascribed to state actors. Individual states have built strong cyber capacities in different forms, from offensive military capabilities to groups covertly working for the states concerned. They focus on industrial espionage, intelligence collection, disinformation spreading, but also on attacks causing casualties and damage to health and property. This threat is a priority of cyber defence, since the attackers get sufficient material and financial backup to carry out the most intensive attacks.

Cyberterrorism

A terrorist attack is mostly perceived as a physical threat. However, various terrorist groups more and more frequently declare to enhance their cyber activities. So far, they have used cyberspace mainly as a recruitment or information platform. Nonetheless, we expect them to master the skills to carry out even relatively sophisticated cyber attacks soon.

Growing number of IoT appliances

In late 2017, about 20 billion appliances were connected to the Internet worldwide. Predictions suggest that the number might grow up to 30 billion by the end of 2020, with subsequent further exponential growth. The direct threat does not stem from the number

of IoT appliances, but from their often weak or none protection, which enables the attackers to gain control over these appliances and use them for cyber attacks.

Low digital literacy and insufficient awareness of users of security rules to be observed in cyberspace

This has been a long-known problem. However, growing dependence of the society on information and communication technologies has made it more visible. With regard to cyber defence of the Czech Republic, it is necessary to mention only poor knowledge of behavior rules in cyberspace and proper operation of the cyberspace among senior state or military officials. The mostly used methods of attackers operating at all cyberspace levels include spear phishing campaigns, malware attacks, compromising of systems through social engineering or manipulation of legitimate user accounts.

Growing dependence of national defence bodies on information and communication technologies

The national defence bodies have become increasingly dependent on information technologies. They use them, for example, for communication, in support of planning and decision-making processes, or as basic part of combat systems. Therefore, development of cyber defence capabilities, but also active operation skills in cyberspace is of growing importance for these defence bodies.

Vision

The Cyber Defence Strategy has been prepared with the prospect that the Czech Republic must become able to handle even the most serious cyber attacks. To meet this vision, the state must fully develop its cyber defence capabilities and engage them both in defence and in support of its military campaigns. Therefore, it is essential to perceive cyber defence as part of complex defence of the Czech Republic. It will be further necessary to establish strong international bonds in the cyber defence field to enhance the capacity to avert and handle potential cyber attacks. We must also get ready to actively aid our international partners within the framework of obligations stemming from our membership in international organizations.

Main strategic vector

The global objective of the Cyber Defence Strategy is to reach a state, in which NCOC becomes able to guarantee cyber defence of the Czech Republic, carry out military operations in cyberspace and play an active role in the international environment.

The global objective will be achieved if following strategic goals are met:

1. Definition of legal framework

2. Building-up and development of NCOC infrastructure

3. Development of defence capabilities in cyberspace

4. Establishment of cooperation and performance of education and training

5. Engagement in ensuring cyber security within the Ministry of Defence

1. Definition of legal framework

Arrangement of cyber defence is at its very beginning in the Czech Republic. In this phase, tools of administrative legal regulation must be used to define basic competence and authorities of individual public authorities involved, mainly the NCOC, as well as rights and obligations of individuals performing the above mentioned powers. It will also be necessary to establish an efficient control system over activities connected with arrangement of cyber defence of the Czech Republic. Subsequently, follow-up legal norms must be adopted to create a complex legal framework. The aim of the adopted legal framework will be support to development of all other spheres and skills needed to ensure cyber defence of the Czech Republic. Fulfilment of this objective will define basic legal aspects of cyber defence. An important step will also be our participation in legal regulation of cyber defence on the international level.

2. Building-up and development of NCOC infrastructure

A crucial step to fulfilment of the global objective will lie in building-up of NCOC. The priority in this field will be to staff NCOC with high-quality personnel, directly followed by measures to train and retain such high-skilled and experienced personnel. Another priority will be acquisition and development of top-class technologies facilitating efficient engagement of human resources. Given cyberspace interconnection, it will be also necessary to use external sources, mainly in personnel and technological spheres. Fulfilment of this strategic goal will help build an adequate background for NCOC activities.

3. Building-up of defence capabilities in cyberspace

To ensure defence of the Czech Republic, it will be vital to develop capabilities enabling to conduct operations in cyberspace. They will be carried out both within cyber defence of the Czech Republic and as part of military operations. It will be also crucial to develop capabilities to predict potential attacks, better localize ongoing attacks, and analyze possible responses to fight them off. Achieved capabilities will be subsequently embedded in a doctrinal framework. It will be also important to develop a “cyber deterrence” strategy within cyber defence of the Czech Republic. Fulfilment of the third strategic goal will help NCOC gain capabilities to actively operate in cyberspace.

4. Establishment of cooperation and performance of education and training

Efficient cyber defence of the Czech Republic can be achieved only in cooperation with state and non-state entities, both on national and international levels. Isolation itself would pose a high security risk, since handling of asymmetric threats and cyber attacks must be complex. Therefore, NCOC will take active part in arrangement of cyber security in the Czech Republic. It will also establish strong alliances in the international environment, mainly within NATO, the EU, and with its neighboring countries. It will develop cooperation with private entities, especially in the field of science and research, to ensure efficient cyber defence of the Czech Republic. Within cooperation efforts, preparation of and participation in various exercises and educational activities will be essential, since they offer an important source of information and experiences regarding the technical and legal consequences for arrangement of cyber defence of the Czech Republic. Fulfilment of the fourth strategic goal will bring significant enhancement of cyber defence of the Czech Republic. At the same time, NCOC capabilities will contribute to improvement of cyberspace security in the Czech Republic and its allied countries.

5. Engagement in ensuring cyber security within the Ministry of Defence

Dependence of the national security bodies on information technologies has been permanently growing. Thus, all bodies subordinate to the Ministry of Defence must generally strive to increase the cyber security level. NCOC's priority task will be to ensure cyber security of its own means and networks. NCOC's special skills, however, will be also used to reinforce defence capabilities of other bodies and employees of the Ministry of Defence. Fulfilment of this goal will bring reliability and credibility of NCOC information systems as well as other information systems within the Ministry of Defence.

Objectives of individual strategic spheres

1. Definition of legal framework

1.1. Definition of competence and authorities

First, we must clearly and indisputably define competence and authorities of public bodies engaged, in particular the NCOC, as well as rights and obligations of individuals implementing these powers. It will be also crucial to define conditions, under which the Czech Republic would activate its cyber defence. Only after this basic definition, we can further develop efficient cyber defence, with all regards to constitutional principles and the rule of law. Thus, it will be necessary to prepare required changes to the law to ensure full operational capabilities of NCOC and pass them successfully through the entire legislative procedures.

1.2. Definition of authorities within the decision-making process connected with engagement of cyber defence capabilities of the Czech Republic

Efficient cyber defence of the Czech Republic must be based on unambiguously defined powers, which will influence particularly the decision-making process connected with engagement of cyber defence capabilities of the Czech Republic in the future. Therefore, rules must be set to define these mechanisms. First, we must prepare a plan of cyber defence of the Czech Republic. At the same time, we must approve statutory regulation and conclude cooperation agreements with individual partners. Subsequently, we will approve particular crisis management or cooperation documents to define, among other things, specific conditions of cooperation with our national as well as foreign partners.

1.3. Preparation and revisions of NCOC internal regulations

Also preparation of consequent internal regulations of NCOC will be important. They will specify in details fulfilment of individual tasks, mutual relations, interconnection with internal legal norms of the Ministry of Defence, and responsibilities of individuals engaged in cyber defence of the Czech Republic.

1.4. Participation in preparation and revisions of the law in the field of cyberspace regulation

Knowledge and experiences learnt from NCOC operation will be used for revisions and preparation of statutory amendments connected with cyber security of the Czech Republic and cyberspace in general. It will be important to actively discuss interpretations and meanings of cyber security and cyber defence concepts in the Czech Republic.

1.5. Participation in preparation of cyber defence regulation on the international level

Given the cyberspace characteristics, an important factor influencing cyber defence of the Czech Republic is also the issue of international regulation. Therefore, we will have to actively participate in preparation of legal regulation defining cyber defence on the international level, especially in the fields of jurisdiction, responsibility, and right to self-defence.

2. Building-up and development of NCOC infrastructure

2.1. Achievement of high technological level of NCOC assets

Introduction of first-rate technologies is vital for efficient implementation of cyber defence of the Czech Republic. Thus, one of NCOC priorities will be to monitor new trends in the field of technological development and subsequent fast purchase for advantageous prices and implementation within NCOC's infrastructure. In the fields, in which commercial products cannot sufficiently cover NCOC needs, the emphasis will be put on investments in development and subsequent introduction of own technologies.

2.2. Hiring of sufficient number of well-qualified personnel

NCOC, just like many similar institutions in the Czech Republic, will have to face shortages of qualified personnel. Thus, another NCOC priority will be a more efficient recruitment. The hiring process will also have to meet modern HR trends in the IT field. It will be also further necessary to set and maintain competitive job conditions as regards remuneration and modern benefits. In the long term, NCOC will focus on alternative recruitment methods. Currently, the biggest challenge, mainly in IT field, is to retain and motivate the personnel.

The precondition is to create a system of remuneration and quality systematic education. It will be also important to develop a motivation system of rewards and promotions, based on the staff performance, which will be further connected with application of modern management methods.

2.3. Maintaining infrastructure

A crucial step will be to ensure a suitable infrastructure and necessary logistic support, which will enable to implement efficient performance of cyber defence of the Czech Republic.

2.4. Use of external resources

Exchange of valuable experience between civilian experts and NCOC employees might be very useful to increase qualification of NCOC personnel. Thus, the effort will focus on establishment of various exchange programs with civilian companies. One of the forms how to use external resources will lie in engagement of active reserves and preparation for their potential deployment. NCOC will also strive to use external assets and facilities to develop new technologies or train its personnel.

3. Building-up of defence capabilities in cyberspace

3.1. Building-up of operational capabilities in cyberspace within defence of the Czech Republic

To ensure cyber defence of the Czech Republic, first we must be able to carry out operations that could be launched in case of necessary defence against large-scale cyber attacks. The NCOC will create a set of capabilities offering a broad spectrum of possible responses to various cyber attacks.

3.2. Building-up of operational capabilities in cyberspace in support of military campaigns

Besides cyber defence of the Czech Republic, NCOC will have to develop its capabilities to support military operations. They will cover operational up to tactical levels and will include both combat support in other spheres and operations carried out exclusively in cyberspace.

3.3. Enhancement of cyberspace attacks' prediction and analysis capabilities

To identify an attack in cyberspace, correctly define the enemy, and reveal his motivations, tactics and operational methods is one of the most difficult, but also one of the absolutely crucial tasks. NCOC will strengthen its capabilities of information collection and analysis concerning threats, risks and cyberspace attacks. These capabilities will be based on three main pillars – complex analysis of cyber threats ("Cyber Threat Intelligence"), advanced forensic analysis, and activities of NCOC's Cyber Defence Security Operations Centre. Acquired information will become an indispensable basis for efficient implementation of cyber defence of the Czech Republic. Selected information can be shared with other relevant national as well as international entities.

3.4. Preparation of a doctrinal framework for engagement of cyber defence capabilities of the Czech Republic

Development of operational capabilities must be interconnected with integration of all newly acquired skills in doctrines on strategic, operational as well as tactical levels.

3.5. Development of cyber deterrence strategy

It is also important to discourage potential attackers from conducting of hostile activities. Cyber deterrence embraces a number of factors, such as the ability to reveal an attack and identify its perpetrator, the overall level of cyber defence, or punishments in case of apprehension. However, efficiency of these individual factors if applied independently is much lower than in case of a complex and systematic approach. Since the issue is broad, covering many spheres, it would be suitable to prepare a separate national strategy in this context.

4. Establishment of cooperation and performance of education and training

4.1. Cooperation within the Ministry of Defence

Key cooperation will certainly take place within the Ministry of Defence as part of complex defence of the Czech Republic. Close cooperation will be developed with the Army of the

Czech Republic in support of military operations. It will be also necessary to build secure communication channels in cooperation with other parts of the Ministry of Defence.

4.2. Cooperation on national level

NCOC will participate in development of an efficient system of cooperation among organizations engaged in ensuring cyber security of the Czech Republic, with the core emphasis put on the National Cyber and Information Security Agency (NÚKIB), the Police of the Czech Republic – National Centre for Organized Crime (NCOZ), national CERT and other CERT/CSIRT authorities. Given the fact that cyber threats have been emerging in many forms, compliance of civilian and military approaches to protection of critical activities should be increasing. These efforts must be further fueled by closer cooperation among NCOC, the private sector and the academic sphere. Also cooperation in science and research activities will be of crucial importance. Cooperation on the national level will be backed up also with appropriate strategic communications.

4.3. Cooperation on international level

Given global characteristics of cyberspace, NCOC must build strong and close alliances in the international environment. Main cooperation will focus on NATO and EU structures, within which active involvement of NCOC personnel is expected. Close cooperation will be established mainly with CCD COE. Naturally, the Czech Republic will also enhance partnership cooperation with its neighboring countries. Another crucial aspect will be to develop cooperation on a much broader global scale.

4.4. Exercises

Importantly, the cooperation will also include organization of and participation in exercises. The exercises will help to test and improve our capabilities to deal with real threats. They will focus not only on readiness of technical structures, but also on legal aspects and decision-making processes. These activities must be implemented on national as well as international levels.

4.5. Education

Individuals engaged in cyber defence of the Czech Republic must have access to appropriate education, other individuals involved must be educated by NCOC personnel. Typically, they will attend courses, seminars and conferences. A crucial aspect will be support and

cooperation in establishment of educational programs focusing on cyber defence. Also in this field, the activities must be developed both on national and international levels.

5. Engagement in ensuring cyber security within the Ministry of Defence

5.1. Ensuring NCOC cyber security

NCOC will very probably become a target of differently motivated cyber attacks, which will try to acquire information, and to discredit or directly eliminate NCOC to weaken the general defence capabilities of the Czech Republic. Therefore, NCOC must take all measures available to ensure maximum level of its own cyber security.

5.2. Participation in detection of threats and vulnerabilities of the Ministry of Defence networks

NCOC will possess detailed information on cyberspace threats, based on which it will issue recommendations concerning measures to be adopted in order to ensure cyber security of the Ministry of Defence. NCOC's operational capabilities will be also used as one of the means to detect cyber vulnerabilities within the Ministry of Defence. For this purpose, the Ministry of Defence can also apply modern methods based on cooperation with the general public.

5.3. Participation in ensuring cyber security of the Ministry of Defence networks and personnel

NCOC's Cyber Defence Security Operations Centre must establish close cooperation with similar offices within the Ministry of Defence, mainly with the CIRC Centre of the Ministry of Defence. This cooperation must include active information exchange and coordination of activities of its individual participants. NCOC must also take active part in definition of cyber security standards planned to be introduced. Another measure would be participation in protection of the Ministry of Defence personnel, who might become a target of cyber attacks carried out in different forms and with various motivations. This effort might focus, for example, on training, but also on active aid to individuals directly threatened by cyber attacks.

5.4. Participation in training of ICT experts within the Ministry of Defence

NCOC members will get above-standard training and will also learn exclusive experience during their activities. Subsequently, they will pass their acquired knowledge and experiences via training to relevant employees of the Ministry of Defence to generally increase digital literacy of the personnel.

Implementation

The Strategy has been developed up to the level of specific goals, described in a way enabling their release to the expert and general public. The above mentioned goals serve as a basis for development of a non-public Action plan, which specifies measures aimed at fulfilment of individual goals, responsibilities, implementation time limits, and evaluation methods.

Implementation of the Strategy will be continuously reviewed and evaluated. Given the dynamics of modern technologies development, it will be necessary to permanently monitor whether the Strategy reflects the latest situation developments. Also public discussion will be of concern. For this purpose, a publicly available contact point in form of an e-mail address will be established. Thus, the Strategy is expected to be reviewed, if necessary.

The implementation will be continuously evaluated in form of annual reports submitted by the Director of Military Intelligence to responsible authorities.

Conclusion

The nature of the prepared Strategy is rather organizational. It will help establish an efficient cyber defence system of the Czech Republic. Information and experience learnt from ensuring cyber defence of the Czech Republic will become a cornerstone of plans of future development and strategic orientation. Subsequently, a follow-up Strategy might be more ambitious, potentially even with the Czech Republic's focus on a potential effort to become one of the most important actors in the field of global cyber defence.

List of abbreviations

AČR – Army of the Czech Republic

CCD COE – NATO Cooperative Cyber Defence Centre of Excellence

CERT – Computer Emergency Response Team

CIRC – Computer Incident Response Capability

EU – European Union

NATO – North Atlantic Treaty Organization

NCOC – National Cyber Operations Centre

NÚKIB – National Cyber and Information Security Agency

Annex

Objectives of the Cyber Defence Strategy of the Czech Republic 2018–2022.

Cyber Defence Strategy of the Czech republic 2018 - 2022

1 Definition of Legal Framework

- competence and authorities
- decision-making process
- internal guidelines
- international law
- legal aspects of cyberspace

2 Infrastructure

- technical background
- personnel
- infrastructure
- external sources

3 Cyber Defence Capabilities

- operations in cyberspace
- support of military operations
- prediction and analysis
- doctrines
- cyber deterrence

4 Cooperation, Education and Training

- at department, national and international levels
- exercises
- education

5 Department Cyber security

- cyber security of NCOC
- participation in
- detection of threats and vulnerabilities
- security arrangements
- schooling

Cyber Defence Strategy of the Czech republic 2018 - 2022

objectives

NCOC 2018