MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

NATIONAL SECURITY AUDIT

Prague, 2016

SUMMARY

Following a prolonged period of relative safety, Europe is again struggling with a deteriorated security environment. After the dampening of the economic crisis of recent years, which shook Europeans' confidence in some aspects of integration, Europe is facing an extraordinary migration influx, which carries with it a number of pressing social, humanitarian, political, and cultural issues, all linked to important security questions. According to current knowledge, 11 terrorist attacks have taken place in Europe between January and September 2016, claiming 120 victims. After almost two decades, a military conflict has erupted in Europe, and part of the territory of a sovereign state has been annexed. The security environment in Europe's periphery and neighbourhood has deteriorated dramatically in recent years – in all aspects, including the military. Thus, the EU now has to tackle a complicated international situation and a potential military threat not only in remote regions, but also in its immediate vicinity.

So far, the deteriorated security environment in Europe has only marginally affected the CR. Nevertheless, we must face the full spectrum of threats that Europe is currently tackling. Nor should we underestimate a potential military threat. The expert group, comprised of representatives of all members of the security community as well as several other state administration bodies, which was tasked in early 2016 with drafting the outline of this document, decided in spite of this to limit the topics of the Audit to those that have a direct influence on internal security. The context of external security does not solely impact traditional internal security areas such as extremism and radicalisation, or organised crime, where an unprecedented increase in smuggling is currently observed; our internal security is jeopardised by relatively new threats related to information wars or organised cyberattacks. In a globalised world, local issues in remote regions or on other continents can have a major impact on the security environment in our country. At the same time, the CR faces a threat that, although it is not mentioned in the Audit and is not considered to be primarily related to internal security, has an impact on society that is on par with any of the treated topics. This threat is the demographic development of the CR, whose downward curve negatively affects all aspects of society from higher standards of social peace to the inability to ensure a sufficient labour force for a wide range of activities.

Threat assessment must consider not only the direct influence, but also all the secondary effects of the given threat. In case of terrorist attacks, the consequences of the entire scope of attacks committed during one year in the EU do not reach even a fraction of the total number of victims that have been claimed by traffic accidents, for example, although their impact on internal security is much broader. They include the radicalisation of a part of the majority population and the rise of extremist and populist groups and political movements that, not unlike terrorists themselves, disseminate hatred and fear while offering simple and radical solutions. The psychological, economic, and political consequences of terrorist attacks on society can therefore far outweigh material losses.

Threats can be classified according to different criteria (depending on their source – an individual, a state, a *force majeure*, etc.; their object of reference – physical safety, security of facilities, etc.; the area they occur in – economic, military, environmental, political, etc.), however these categories, used in academic texts, fall short of the needs of the National Security Audit conclusions for several reasons. Firstly, the ten topics covered by the Audit do not represent an exhaustive list of all the threats that the CR must face, prevent, and effectively manage in case they occur, but only those that have the greatest potential for seriously damaging the quality of internal national security. Secondly, the topics are interconnected, which is evidenced by cross-references between individual chapters of the Audit – and not just via popular "media shortcuts" linking migration and terrorism. The cross-referencing of five or more topics is not unusual for the Audit, where links between threats – usually based on the unifying motive of their originator – significantly increase their severity rating.

For this reason, the threats in this summary are not classified in any way.

It can be argued, however, that the severity rating of identified threats largely determines their interconnectedness. One group would include the chapter “Energy, Industrial, and Resource Security”, the chapters “Cyberthreats” and “Influence of Foreign Powers”, as well as the chapters “Extremism”, “Terrorism”, and “Security Aspects of Migration”, and especially the overarching chapter “Hybrid Threats and their Impact on the Security of Czech Citizens”. Chapters dealing with threats with a greater potential to be used simultaneously within a single campaign more frequently define systemic deficiencies of national readiness to detect these threats, the absence of firmly anchored strategic solutions, an insufficient or non-existent capacity to perform the tasks of preventing and combating these threats, deficiencies in or the lack of exercising model situations associated with the outbreak of the threats, and, to an extent, legislative shortcomings.

Given the scope of the Audit, the purpose of this summary is not to repeat, in abbreviated form, the solutions outlined in each chapter, but to generally address the range of tasks and recommendations laid forth by the Audit. Throughout the text, several areas can be identified where the chapters have similar conclusions, whether topical or isolated. Given the need to group the recommendations and tasks where this can bring benefits, whether in terms of thematic affinity or the need to efficiently distribute state funds for their implementation, it is useful to group the proposed measures into larger clusters and separately point to those measures whose specificity is justified.

The CR has strategic documents for most individual threats; nevertheless, these documents do not define how to reach the ideal state. On the other hand, the purpose of the Audit is to assess where we stand today in 2016, how the state is prepared to face security threats in selected, serious areas, and what is its resilience when directly confronting danger. The Audit assesses whether the CR has sufficient legislation and how flexibly the security system can respond. It also examines the communication and cooperation abilities between individual bodies and whether relevant institutions, security forces, crisis management bodies and, where relevant, regions, municipalities, and the private sector are adequately involved. It evaluates the capacity that the state has allocated for the prevention and suppression of individual threats. Thus, the recommendations of individual chapters of the Audit can be grouped into the following clusters:

- **Legislative** (recommendations ranging from the general review of legal instruments to very specific amendments to relevant legislation are put forward by all chapters except “Anthropogenic Threats”)

Apart from repeated proposals relating to criminal law, it is worth noting the criticism of the inadequate level to which security aspects are taken into account in the exercise of the right on free access to information, as per Act No. 106/1999 Coll., on free access to information (“Influence of Foreign Powers and Cyberthreats”).

- **HR/staffing** – several chapters signal the need to increase the number of people tackling a given threat, or at least to stabilise the staffing of relevant bodies; the question of specialisation is also addressed. This is the issue of chapters “Anthropogenic Threats”, “Environmental Threats”, “Security Aspects of Migration”, “Organised Crime” and “Cyberthreats. In several cases, these chapters identified a direct lack of employees dealing with an issue (“Influence of Foreign Powers”, “Hybrid Threats”). The requirement for further training of employees responsible for tackling certain threats (migration, influence of foreign powers) is also repeatedly stressed.

In connection with recommendations in the area of HR/staffing, it is interesting to note that two chapters identify **Act No. 234/2014 Coll., on civil service, as problematic**, specifically as a factor reducing the flexibility of the Government in matters of staffing (migration) and negatively impacting the openness of the Government to professionals from the private sector (organised crime).

- The nature of the activities of the security community, not only that intelligence services, lends itself naturally to the trend of classifying its outputs and methodologies. Nevertheless, as regards the Audit, recommendations relating to the **need to strengthen threat assessment coordination** are only a mandatory reminder of a known fact. The inclusion of hybrid threats among the 10 most serious security topics revealed insufficient coordination particularly in the case of an active hybrid campaign led with the intention of damaging not just the CR, but European integration as a whole, of which the CR is a part. The modern aspect of this situation is manifested by the reality that, in order to assess proposals for measures, the system must be able to integrate a wider circle of social, economic, legal, and political aspects of social life outside of the security community in order to interconnect individual low-severity attacks and correctly estimate their cumulative risk. The need for coordination is thus stressed by almost all chapters, although "Hybrid Threats" and "Influence of Foreign Powers" emphasise this particular aspect of the identified deficiency and evaluate it as serious.

- In close connection with the previous remark, the Audit introduces a clearly defined need to support **the long-term development of communication infrastructure and public administration technologies, as well as eGovernment**, for the purpose of securing public order and safety, national security, and crisis management. A safe and sufficiently secure method of transmitting information between relevant Government bodies, whose informational and decision-making potential is crucial in cases where a rapid response is required, is a necessary technical prerequisite for a state resistant to all kinds of threats. This requirement is mentioned in more than half of all chapters and is accompanied by the identified need for training in the use of communication channels during crises.

- One of the fundamental conclusions of the Audit concerns **cooperation with the public and with private entities**, which permeates a number of chapters in the form of a **request for a more active participation of private entities in being responsible for security** when cooperation with the state ("Terrorism", "Anthropogenic Threats", "Environmental Threats"), as well as via **active communication of the state with the public** ("Migration", "Extremism", "Environmental Threats", and "Hybrid Threats"). Chapters "Hybrid Threats" and "Influence of Foreign Powers" identified the need to create a conceptual approach (or to strengthen it) to **strategic communication** of the state both inward and outward.

- Among tasks with long-term effects, a repeated request is made to **add topics within the framework of the educational curriculum**, whether this concerns security education or strengthening of civic or media literacy ("Anthropogenic Threats", "Environmental Threats", "Hybrid Threats", and "Influence of Foreign Powers").

- Several chapters unequivocally **support the further deepening of security research**, which is one of the indirect instruments for the development of security. It allows the systematic employment of capacities of a dynamically evolving research sector for the purposes of the development of the security system. Nevertheless, it should be borne in mind that this is a tool that brings results in the medium and long term, and it's effective functioning is subject to close cooperation with potential end-users of the results of its research activities in developing support instruments, but especially in implementing projects, testing, and evaluation of results and their employment in practice. These aspects of the development of security are referenced in chapters "Environmental Threats", "Anthropogenic Threats", "Security Aspects of Migration", and "Influence of Foreign Powers".

The work associated with the Audit does not end with its submission to the Government. However, it is encouraging that the security community is not currently at the starting line, and does not find itself without experience. The Audit showed that the identified threats are well covered within the system and that the identified issues related to their solution are secondary problems that come up regularly in day-to-day security operations, the solutions to which are proposed, discussed, and implemented continuously. At the same time, the Audit revealed the system's insufficient capacity to evaluate and react to complex interconnected threats. Concrete steps have already been taken with regards to a number of recommendations, where the security community is in agreement. **Following the approval of the Audit by the Government, the MoI, in cooperation with other responsible bodies, will draw up an Action Plan for the implementation of individual tasks and set a schedule for its evaluation. It will inform the Government on the implementation of these tasks as per their deadlines. Specific methods of implementation will be a part of the Action Plan and will be drawn up in cooperation with the bodies responsible for individual tasks.**

CONTENTS

INTRODUCTION

The Audit was drafted by assignment of the Prime Minister. It focuses on ten threats that were selected by an expert group in January 2016.

What is the objective of the Audit?

The Audit verifies two basic abilities of the state: the ability to identify concrete security threats and adopt relevant preventive measures and the ability to respond to an ongoing crisis that needs to be resolved. Therefore, every chapter answers the following questions: Is the current **legislation** sufficient? Does the state have **sufficient capabilities** at its disposal? Does the state have a real ability to adopt appropriate measures and **act when necessary**?

The objective of the Audit is also to look at known threats from a different security perspective: to search for common features and assess the degree of their severity through a new approach that combines the national and international context in which the CR finds itself.

Who is the Audit intended for?

This is a general document. More than one hundred experts were involved in its creation, divided into working groups according to their qualifications. The purpose was not to create a document that would describe every selected topic in detail. On the contrary, the individual groups were tasked with drafting an overview of the issues within the given topic, assess them, and identify those that are most threatening for the further development of the CR.

This is why the resulting document is general, and points in the direction that the Government of the CR should take in facing security challenges. The brevity of the document enables easy orientation within it as well as its presentation to the public, because in addition to charting the direction of the next steps in the field of internal security, the document must also perform its role in informing the public.

The public has a right to know what threats society is facing and what challenges the state is obliged to tackle. For tactical reasons, however, it is impossible to provide detailed information of this nature, which is why most of the work on the final draft was devoted to balancing information so as to offer to the public a good overview of the problems we are facing without providing a guide for potential attackers.

Threat Assessment

A number of chapters used the scale "high – medium – low" to assess the relevance of identified threats. This scale is used only in those chapters where the working groups considered it applicable. It should, however, be noted that the relevance of identified threats cannot be used across chapters. The degree of severity of each threat is assessed in isolation within individual chapters. Furthermore, it should be borne in mind that the degree of severity differs depending on whether the threat is isolated or linked to other threats within a hybrid campaign aimed at negatively affecting the functioning of the state.

Chapter Structure

Each topic consists of four parts: **description and evaluation of the threat** and the associated risks for the CR, a list of the **responsible institutions** within the Czech security system and the **basic tools** (legislative, strategic) for the elimination of these threats and risks, a **SWOT analysis of the given topic** and, in conclusion, a list of **specific recommendations for the Government** intended to strengthen resilience in relation to the given threats and risks.

A standalone chapter “Stability of Currency and Financial Institutions” has been elaborated, and will be presented by the Czech National Bank to the NSC and the Government for approval independently of this document.

TERRORISM

A. Description and Assessment of the Threat and Associated Risks for the CR

1. Introduction

The extensive destabilisation of some Middle Eastern and North African countries, the onset of the so-called Islamic State and other terrorist groups and the phenomenon of foreign fighters, the migration crisis, radicalisation of individuals and groups in various segments of society (e.g. through internet propaganda and social media) – are all mutually interrelated factors that cumulatively increase the risk of a terrorist attack in Europe.

Terrorism can be used to label behaviour that is politically, religiously, or otherwise ideologically motivated and uses violence or the threat thereof particularly in order to induce fear. No country is currently fully immune to the threat of terrorism, including the CR. On the other hand, the relevance and structure of this threat varies in different regions and countries – Western Europe, for example, is threatened by radical Islamism much more than Central Europe because of historical and demographic reasons. This document should evaluate the significance of the risks of terrorism specifically in relation to the CR. While doing so, it is necessary to take into account the current setting and status of the security system and evaluate the sufficiency or identify deficiencies in: a) legislation, b) capacities, and c) the real ability to respond and then take any necessary recommendations for improvement where it is relevant with regard to the factors listed above (all measures must build on a quality risk analysis and the physical and material resources employed must reflect the importance of a specific threat).

Contemporary terrorism has a number of causes, most of which originate outside the CR. The CR is unable to considerably influence some of these causes without the help of other partners. In spite of this, it is important to assess the current preparedness and capability of the CR to prevent terrorist activities (not only) on its territory, to limit the consequences and impacts of possible terrorist attacks, and to actively participate in stabilising the security environment in Europe and the world.

This chapter does not deal with the issue of *cyberterrorism*,[1] because it is addressed in the chapter "Cyberthreats". The chapter "Hybrid Threats" takes a closer look at terrorism *as an instrument of a hybrid war*, while the chapter "Extremism" examines in more detail the phenomenon of radicalisation. During the drafting of this chapter, security research findings have been used, or example those of the "Islam in the CR: Establishment of Muslims in the Public Space" project, which was implemented within the framework of the Security Research Programme of the Czech Republic for the Years 2010 – 2015.

[1] The NSA defines cyberterrorism as follows: "cyberterrorism include aggressive and excessive action, which is carried out with the purpose of inciting fear in society, via which political, religious, or ideological goals are reached. By using cyberspace and ICTs it threatens the functioning of the state, its constitutional establishment, or its capacity to defend itself, *inter alia* by targeting critical information infrastructure and important information systems".

2. Threat Description and Assessment

The terrorism threat as a whole can be divided into several chapters, every one of which deserves an individual relevance assessment for the CR.[2] The following text divides the terrorism threat according to three aspects: 1) in terms of the originator of the threat; 2) in terms of the target of the attack; 3) in terms of the tools of terrorism. When evaluating the relevance of the threat for the CR, the criteria used considered the probability of the threat and the severity of its impact, resulting in a combination that allowed for the relevance to be rated on a scale of low – medium – high.

I) The Terrorism Threat in Terms of the Originator

a) Islamic Radicalism

Threat relevance assessment for the CR: **Low**

In contemporary Europe, Islamic radicalism is most frequently associated with the threat of terrorism (although it is necessary to recall that this has not always been so and that separatist and radical leftist terrorism dominated Europe in the 70s and 80s, for example). Many of the attacks that have recently gained most public attention (because it is precisely that, and not the real impacts or numbers of victims, that is the true measure of the significance of an attack) were committed by persons subscribing to radical Islamist ideology or directly linked to international terrorist organisations (e.g. the so-called Islamic State).

In spite of this fact, risks stemming from Islamic radicalism for the CR can be evaluated as low, although not non-existent. The CR is, in this regard, in a different position than Western European countries. The Muslim community in the CR is significantly less populous than that of Western or Northern European countries, and has shown no extensive radicalisation tendencies as of yet. Until now, the CR has largely been of marginal interest to international terrorist organisations, which have only a minimal foundation for their activities in this country (which is given by the size and character of the Czech Muslim community).

Experience from Western Europe also shows that radicalisation is also often linked to the phenomenon of social exclusion – in this regard, it is positive that the vast majority of members of the Czech Muslim community are economically well integrated and that no socially excluded communities or parallel social structures, which could serve as breeding grounds for terrorist activities, are currently developing in the CR.

While all these factors diminish the threat relevance of Islamic radicalism for the CR, it is not non-existent. The CR is a member of Euro-Atlantic structures and the Global Coalition against the so-called Islamic State, and actively speaks out against Islamic radicalism – this alone makes it a possible target of terrorist attacks. Terrorists may also focus on the CR because of (real or imagined) shortcomings in the security system, or because of the attractiveness of some targets located on Czech territory (e.g. Jewish edifices, Radio Free Europe etc.).

[2] The following chapter divides the terrorism threat into individual parts in accordance with the outline and methodology of the Audit. Individual threats are evaluated according to their relevancy for the CR on a scale of none – low – medium – high, which reflects the probability of the occurrence of the threat in the next two to three years, as well as its possible implications.

While the probability of a high-profile attack by international terrorist organisations is, due to the reasons listed above, rather low, the radicalisation of individuals or small groups inspired by radical Islamist ideology, who may attempt violent actions even without links to established organisations (for details see the section on terrorists acting alone) cannot be excluded.

b) Political Extremism, Other Terrorist Groups

Threat relevance assessment for the CR: **Low**

While the phenomenon of Islamic radicalism affects the CR only to a small extent (as compared to Western European countries), the CR has many years of experience with right-wing (REX) and left-wing (LEX) extremism. This topic is further discussed in the chapter "Extremism", but a brief assessment of a possible terrorist threat stemming from groups or individuals influenced by radical political ideology is relevant here.

Many groups are active in the CR that can be described as extremist; some of these groups have international ties. The members of these groups commit unlawful, in some cases violent, actions. Despite the higher incidence of this phenomenon as compared to Islamic radicalism, it can be stated that the risk of a terrorist act committed by members of REX and LEX groups is no higher than that of ones committed by Islamic radicals. This is mainly because activities on the REX and LEX scene are continuously monitored by security forces and the probability that these groups will now include terrorism in their efforts at systemic change is low. This is largely helped by the internal fragmentation of the Czech extremist scene, and its prevalent effort to gain the sympathies of the wider public, which could be disrupted by the recourse to terrorist methods.

Similarly to what has been said as regards Islamic radicalism, the radicalisation of individuals or small groups inspired by REX and LEX ideologies, who may attempt violent actions even without links to established organisations (for details see the section on terrorists acting alone) cannot be excluded.

The same assessment can be applied to other groups or individuals influenced by ideologies (whether political or religious) other than Islamic radicalism, REX and LEX.

c) Terrorists Acting Alone (Lone Wolves)

Threat relevance assessment for the CR: **Medium**

Although the CR belongs to those few European countries that have not encountered a classical terrorist attack in their modern history, in the past two years at least two incidents have occurred in our country where lone attackers caused tragic consequences. One of these incidents was the shooting in Uherský Brod in February 2015, which claimed eight lives. Even though the attacker was not, according to available information, motivated ideologically, and thus the incident was not a terrorist attack as such, the *modus operandi* was no different from, for example, the shooting at the Charlie Hebdo office in Paris, which was claimed by an international terrorist organisation. Attacks by mentally disturbed individuals or individuals motivated by other than ideological persuasions may have the same course and impacts as terrorist actions. In this regard, similar measures can be applied with regard to both groups, which are therefore not distinguished for the purposes of this chapter.

Based on this experience, it can be assumed that a possible terrorist attack in the CR is more likely to be committed by an individual (or a small group), who would be influenced by the activities of international terrorist groups, but not necessarily directly linked to them. In such a case, it can be a person subscribing to Islamic radicalism or motivated by another radical ideology (an example being the attack of Anders Breivik in Norway, one of the bloodiest incidents in recent years – Breivik was a right-wing extremist, who perceived Islam as a threat).

Persons without closer ties to the surrounding community may also succumb to radicalisation (e.g. converts), inspired by, for example, internet propaganda. Combating the spread of hateful and radical content on the internet and on social media must therefore be a priority. It is equally important to monitor the activities of all extremist groups operating on Czech territory – even if these groups do not attempt violent activities themselves, they may inspire individuals who may try to put their radical programme into practice. In this regard, a considerable risk is posed by the (rather widespread in the CR) activities of islamophobic groups, which enjoy ample media attention (and in some cases political support) and which can:

i) contribute to the feeling of alienation and social exclusion and the consequent radicalisation of individuals from the Muslim minority in the CR,

ii) through their radical "warmongering" rhetoric and the spread of hatred and a feelings of insecurity, provoke individuals or small groups to commit hate crimes targeting members of the Muslim community or immigrants, but also "traitors" from the political or social elite or selected members of civil society (after Breivik's example).

The attack of a terrorist acting alone is very difficult to prevent, which is why, apart from radicalisation prevention, it is necessary to focus on the readiness and capability of the Police CR to promptly react to these situations, to prepare the specified potential targets for these and similar attacks and, not least, to mitigate the consequences of a possible attack. It is therefore very important to continue to strengthen and thoroughly implement measures adopted after the incident in Uherský Brod (e.g. strengthen and equip patrol units of the Police CR, train as many riot police officers as possible to tackle AMOK situations, adjust the process of issuing and withdrawing firearm licences, create a register of offences, etc.).

d) Foreign Fighters[3]

Threat relevance assessment for the CR: **Medium**

The foreign fighters phenomenon concerns foreigners involved in various armed conflicts (e.g. in Ukraine), but is lately particularly relevant with regards to armed conflicts in Syria and Iraq. A number of actors and groups are implicated in this complex and deadly conflict, many of whom enjoy substantial foreign support. Some terrorist organisations have taken advantage of the confusing situation and the power-vacuum in order to take control of a relatively large area of land and to gain new resources for their own activities (e.g. the so-called Islamic State, the al-Nusra Front – renamed Jabhat Fateh al-Sham, etc.). These groups use sophisticated propaganda to recruit new sympathisers who would actively join the conflicts on the side of the terrorist organisations. Foreign fighters are also recruited in EU countries, from where thousands of people have already left in order to fight in conflict zones (not only in Syria and Iraq, but also in Libya and Yemen).

The foreign fighters phenomenon is a serious problem particularly for Western European countries – this is how their citizens are radicalised, and may pose a significant security risk after returning from abroad. During their stay in the conflict zone, they gain combat experience and are subjected to a high degree of ideological indoctrination. Concerns stem mainly from the possibility that these individuals may actively try to organise a terrorist attack in Europe (which is already happening).

[3] Some (especially foreign) materials distinguish between the terms "foreign fighters" and "foreign terrorist fighters", where the former designates persons actively participating in an armed conflict abroad (that is, not as members of their state's armed forces, or without the consent of these) and the latter concerns specifically those foreign fighters that engage on themselves on behalf of terrorist organisations.

However this may be a European problem, the CR is not among those states that are significantly affected by this phenomenon. Foreign fighters (foreign citizens) transiting through the CR do pose a problem, nonetheless, as such cases have been recorded in the past.

If we extend the definition of foreign fighters to other conflicts, we may mention that several Czechs are taking part (or have taken part in the past) in the fighting in Ukraine (on both sides of the conflict). The activities of these persons also pose a certain internal security risk, e.g. with regard to the possibility of these people becoming an instrument of foreign influence.[4] Their riskiness with regards to terrorist activities, however, is currently low.

For the abovementioned reasons, we assess the foreign fighters threat relevance for the CR as medium. In order to prevent its increase in the future, it is particularly important to pay attention to combating radicalisation and recruitment, abuse of the internet and of social media, and the formation of paramilitary groups and the influence of foreign powers.

II) The Terrorist Threat in Terms of the Target

a) Attacks on Critical Infrastructure

Threat relevance assessment for the CR: **Medium**

Protecting its critical infrastructure is one of the key tasks of every state. In the CR, this issue is relatively well established legislatively (see the next section of this chapter describing the security system). This area includes the issue of cyberterrorism, which can, in its narrow sense, include politically, religiously, or ideologically motivated activities in cyberspace, such as intentional and widespread disruption of computer networks and equipment with serious to fatal consequences and implications.[5] For terrorist organisations, critical infrastructure is a secondary target, despite the fact that its disruption may cause severe damage and threaten the lives and health of a large number of people.

This is because terrorism's aim is psychological impact (emotions) rather than objective consequences. The terrorists' main objective is to influence public opinion, to spread fear and panic. Therefore, while the objective fact is that a widespread power outage may ultimately cause far greater damage and result in a higher death toll than an explosion or a shooting in the metro, the traumatising effect on the general population will be significantly higher in the latter case. One need not look too far into the past to find examples.[6]

Despite the statement above, the threat relevance of an attack on critical infrastructure in the CR can be assessed as medium, especially with regards to possible serious effects (which balance out the otherwise rather low probability of such an attack). An attack on critical infrastructure is an opportunity to cause considerable damage with relatively low costs and simple tools and the protection of some critical infrastructure components is moreover very difficult or costly. Another

[4] This topic is further discussed in the chapter on the Influence of Foreign Powers.

[5] In a broader sense, any terrorist activity that combines terrorism and cyberspace can be considered as linked to cyberterrorism. An example could be an effort to obtain funds, recruit new members of terrorist groups and their training. This topic is discussed in more detail in the chapter on Cyberthreats.

[6] The attack at the Boston Marathon in 2013 claimed three victims. For several days, it was the main topic of media outlets around the world, and inspired many reactions. In June 2014, following an intensive storm, a large part of Western Australia was let without electricity, and three people died as a direct result of the blackout (not the storm). With the exception of Australian media, hardly anyone informed of this occurrence, and even in Australia this report was overshadowed by other news (e.g. searching for the missing Malaysian aeroplane).

risk is the issue of so-called insiders – employees (or former employees) of vulnerable facilities, or persons with a good knowledge of security measures and procedures. For this reason, the protection of critical infrastructure should not be underestimated, but perceived as a priority (not only) in the fight against terrorism.

b) Attacks on Soft Targets

Threat relevance assessment for the CR: **Medium**

So-called soft targets are usually places with a high concentration of people (shopping malls, hospitals, schools, public transport, sports, cultural, and social institutions, institutions dedicated to the care for national cultural treasures,[7] etc.) that are not significantly protected. As opposed to well-protected, so-called hard targets (airports, nuclear power plants, etc.) the level of their security is usually lower and an attack on them may potentially have tragic human consequences. It is this combination that makes them ideal potential targets for terrorist attacks.

Recent experience confirms that terrorists currently focus on soft targets, both in Europe and outside it (the attack in Parisian cafés and in a concert hall, the attack at the Boston Marathon, the attack at the university in Garissa and a shopping mall in Nairobi, Kenya, etc.). Such attacks have considerable psychological impact, while at the same time being relatively easy and cheap to implement. In this respect, the most frequent recent attacks were those of suicide attackers in public places, using handheld weapons (as this method is proving to be more efficient – as regards the number of victims – than previously popular explosives or improvised explosive systems, despite their relatively easy construction). Multiple attacks are increasingly frequent, as well, where several perpetrators attack several places at once (e.g. the recent attacks in Paris and Brussels). Such attacks require more manpower and resources, as well as a better coordination of security forces.

Given that soft targets are probably the most likely targets of a possible hypothetical terrorist attack in the CR, it is necessary to assess the relevance of this threat as medium.

c) Particularly Vulnerable Facilities and Persons

Threat relevance assessment for the CR: **Medium**

Apart from so-called soft targets and critical infrastructure, facilities that have a **high symbolic value** for a particular terrorist group (or individual) may also become the likely targets of an attack. This category includes places with religious symbolism, embassies (of countries that are frequent targets of terrorist attacks), magazine and media headquarters or exhibitions (that show controversial works), the seats of public administration bodies and political parties, police and army facilities, etc. In Western Europe and in the USA, several attacks were carried out in recent years that targeted members of the armed forces (police and army officers) who represent the repressive forces of the state and for this reason may be targeted by terrorists.

An increased risk also applies to specific persons who represent attitudes or institutions that can be of interest to terrorists. These include some politicians, foreign diplomats, but also other publicly active persons (writers, journalists, actors, academics, etc.).

Given the diverse motives of individual terrorist groups, it is often difficult to identify in advance the persons or facilities that may be at risk – this is especially true for lone-wolf attackers. On the other hand, in the case of Islamic radicalism and right-wing or left-wing extremism, it is possible to

[7] Act No. 101/2001 Coll., on the return of illegally exported cultural goods: Sec. 2, paragraph 2.

predict to some extent which persons or facilities will be the likely objects of their interest and are therefore particularly vulnerable.

At present, for reasons mentioned above, the following are given special protection (whether by the state or by their owners in cooperation with the state): selected embassies and their diplomats, selected Czech state officials, selected seats of important public institutions, the Radio Free Europe headquarters, some Jewish edifices. The threat relevance for the CR can be assessed as medium.

d) Threats to Czech Citizens and Facilities Abroad

Threat relevance assessment for the CR: **Medium**

While the CR does not have to be the primary target for terrorist attacks, the threat posed to Czech citizens and facilities abroad is, in this respect, much higher.

A particular risk is the abduction of Czech citizens, which has occurred repeatedly in the past (in the last 10 years, Czech citizens have been abducted by radical groups in Iraq, Pakistan, Lebanon, and Libya). In these cases, attackers do not usually focus on Czech citizens; rather, they are randomly selected victims "from the West", who move without sufficient protection in high-risk areas and may therefore become easy targets.

Czech facilities may also be threatened, especially embassies abroad. Czech diplomatic missions stationed in countries where armed conflicts are currently taking place that involve terrorist groups (e.g. Syria, Afghanistan, Iraq, etc.) face an increased risk of attacks.

Despite the low severity of a potential attack, because of the higher probability of an attack on Czech citizens and facilities abroad, the relevance assessment for this threat is medium.

III) The Terrorist Threat in Terms of the Tools

a) Abuse of Weapons of Mass Destruction, Conventional Weapons, Explosives and Dual-Use Technologies

Threat relevance assessment for the CR: **Medium**

The use of **weapons of mass destruction** for terrorist purposes is a widely discussed issue. In reality, there are very few historic examples of their actual use in attacks (one being the 1995 sarin attack in the Tokyo metro perpetrated by the Aum Shinrikyo cult movement). However, their consequences could be widespread and their psychological impact enormous (even in the case of a failed attack).

Some international terrorist organisations actually declared their attempts to acquire weapons of mass destruction. Generally, nevertheless, the focus remains on "conventional" attacks. The use of nuclear, chemical, and biological weapons requires expert knowledge and may be organisationally, financially and logistically challenging, even in the case of constructing a so-called dirty bomb or carrying out toxin attacks (letter bombs or the distribution of anthrax). The level of securing nuclear objects in the CR is relatively high. The use of improvised chemical weapons with the use of toxic materials, or a terrorist attack on storage or transport facilities is somewhat more likely. Such a substance can be any chemical or mixture of chemicals acting quickly and adversely on the human body and causing injury, mutilation, or death. Due to the potentially high devastating effect, it is nevertheless necessary to pay special attention to this issue, especially as reports have surfaced in recent years claiming that terrorists may gain potential access to this type of weapons (illegal trade in nuclear materials, the possibility of acquiring chemical weapons in war-torn countries, potential cooperation of terrorists with authoritarian regimes, etc.). Multilateral cooperation, consistent application of control mechanisms in international trade in dual-use technologies and consistent adherence to principles of safe handling of these materials is necessary in this area.

A great risk also arises from the illegal proliferation of **conventional weapons, explosives, and dual-use technologies**, including the relevant technologies. As was already noted, hand-held weapons are increasingly popular for carrying out terrorist attacks, and this popularity stems primarily from their relatively easy availability. Restricting the availability of conventional weapons for terrorists is one of the key aspects of the fight against terrorism.

The probability of an attack using weapons of mass destruction in the CR is relatively low; what would be significant in such a case would be the effects of such an incident. Conversely, the impact of the abuse of conventional weapons and dual-use technologies is potentially lower, but its probability is higher. The relevance of this threat in the CR is therefore assessed as medium.

b) Financing Terrorism and Other Support Activities

Threat relevance assessment for the CR: **Medium**

Although the CR may not become the direct target of a terrorist attack, it may, through its inaction or inconsistency, inadvertently contribute to increasing the threat of terrorism in other countries. Terrorists may use the CR to acquire or transfer financial resources, Czech territory may serve as a transit zone for persons with links to terrorist organisations, or it may be viewed as a “safe haven” and used to hide from foreign security forces or for preparing a terrorist attack.

In 2015, media reported that some terrorists view Prague as a safe place of transit, where they can easily avoid the attention of security forces. However such a notion may be faulty or unfounded, it cannot be ruled out that terrorists may continue to make use of Czech territory. It is therefore important to focus on these activities and prevent them to the maximum possible extent.

The relevance of this threat for the CR can be assessed as medium.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

Basic Documents

The main document regulating the strategic framework of the fight against terrorism in the CR is the **Strategy of the Czech Republic for Combating Terrorism from 2013** (“Strategy” hereinafter). The Strategy deals with five key areas – cooperation of relevant subjects in the fight against terrorism, public protection and other potential targets, security research and communication with the public, prevention of radicalisation and recruitment by terrorist groups, and the necessary insight into the legislative anchoring of the fight against terrorism. The validity of this document is not limited in time, and any updates therefore arise from current needs. From the point of view of the Audit working group, the Strategy is still valid in its entirety and there is no need to change it at present.

To implement the Strategy, the Government adopted on 31 August 2016 an **action Plan on Combating Terrorism for the Years 2016 – 2018**. This Action Plan consists of three separate documents. These are the **Legislative Proposals in the Field of Internal Security**, and the **Counterterrorism Package**, which both contain specific steps that should lead to reducing the risk of a terrorist attack and the related negative consequences.[8] The third document is the **Proposal of Measures to Improve Security at International Airports in the CR** of the MT, which contains some measures in the field of civil aviation.

Legislation

The CR does not have a special "counterterrorism act"; the issue of criminal responsibility for terrorism is nevertheless fully accounted for in the **Criminal Code** (40/2009, Coll.). Here, the relevant sections are: Sec. 311 (terrorist attack), Sec. 312 (terrorism), Sec. 272 (general danger), Sec. 290 (seizing control of an aircraft, civilian vessel and fixed platform), Sec. 292 (introduction of an aircraft abroad), Sec. 314 (sabotage), Sec. 140 (murder), Sec. 174 (taking hostages), Sec. 175 (blackmail), Sec. 279 (unauthorised possession of firearms), Sec. 280 (development, production, and possession of banned combat means), Sec. 281 (unauthorised production and possession of radioactive materials and highly dangerous materials), Sec. 282 (unauthorised production and possession of nuclear material and special fissionable material), Sec. 357 (spreading alarming information, hoaxes), and some sections pertaining to (verbal) crimes disrupting peaceful coexistence, Sec. 352 – 356 (dangerous threats etc.).

Currently, the **amendment to the Criminal Code**, which further treats, for example, the issue of terrorism financing, support and promotion, or the threat of terrorism, is in the legislative process. The amendment should concern Sec. 311 and Sec. 129 (introducing the term "terrorist group"), Sec. 312 and Sec. 361. The amendment is related to the amendment to Act No. 141/1961 Coll., on criminal proceedings (Criminal Procedure Code). The Audit working group fully supports the adoption of the amendment to the Criminal Code in the wording proposed, as it specifies some of the crimes and clarifies some interpretation issues, therefore allowing a more efficient criminal prosecution of crimes related to terrorism.

Some minor shortcomings in the current legislation that may have an impact on the fight against terrorism (e.g. retention of telecommunications data, use of intelligence in evidence proceedings, or the expansion of cross-border cash transport controls) are discussed in more detail in the already mentioned document Legislative Proposals in the Field of Internal Security. See also the Recommendations section below.

Responsible Bodies

1. 1. **The Government of the CR** – The role of the Government and its place in the Czech security system in relation to the fight against terrorism is defined by the Constitution of the CR; Constitutional Act No. 110/1998 Coll., on the security of the CR; Act No. 2/1969 Coll., on competencies; Act No. 240/2000 Coll., on crisis management and the amendment to certain other acts (crisis management act); Act No. 241/2000 Coll., on economic measures for emergencies and on amendments to certain other related acts, and other laws and regulations. The Government, as a supreme executive authority, is responsible for national security and for the management and the

[8] The document "Legislative Proposals in the Field of Internal Security" was adopted by Government Resolution No. 779 of 31 August 2016. The document "Counterterrorism Package", which was adopted by Government Resolution No. 711 of 27 July 2016, contains non-legislative measures and is classified as per Act No. 412/2005 Coll., on the protection of classified information and on security competencies, as amended.

functioning of the Czech security system. The Government reports to the Chamber of Deputies of the Parliament of the CR.

The Government is authorised to declare a state of emergency; if there is danger of delay, the Prime Minister may do so. There is an important difference between the Government's activities under normal conditions and in emergencies, including a state of war, when it primarily evaluates possible risks and threats in the field of national security and takes necessary measures to reduce or eliminate these risks (for this purpose, it makes use of, *inter alia*, its working and advisory bodies).

The Government is further authorised to, *inter alia*: decide, based on a minister's proposal, on the use of the Czech Army for rescue operations, for securing air transport, on dispatching soldiers, members of the Prison Service and the Customs Administration of the CR to perform the functions of the police, etc.; assign tasks to intelligence services, coordinate and supervise their activities; appoint and dismiss the director of the SIS and the NSA; grant consent to the appointment and dismissal of the director of the OFRI and the director of MInt. The Government decides on the proposal of the Minister of the Interior to announce (recall) a terrorism threat level (or cancels or confirms the minister's preliminary decision to announce a terrorism threat level).

The Prime Minister is the chairman of the NSC.

2. **The National Security Council** – The NSC is a permanent working body of the Government for coordinating national security and preparing measures for its maintenance. The NSC consists of the Prime Minister and other members of the Government, pursuant to the decision of the latter. The NSC prepares Government proposals for measures ensuring internal security. Its basic task is to participate in the creation of a reliable national security system, ensure the coordination and control of measures to ensure national security and international obligations. The NSC has five permanent working bodies, which include the **Committee on Internal Security** (chaired by the Minister of the Interior), the **Committee on the Coordination of Foreign Security Policy** (chaired by the Minister of Foreign Affairs), the **Committee for Defence Planning** (chaired by the Minister of Defence), the **Committee for Intelligence Activities** (chaired by the Prime Minister), and the **Committee for Civil Aviation Planning** (chaired by the Minister of the Interior). Within the Committee for Intelligence Activities, the **Joint Intelligence Group** was established, intended for the exchange of intelligence information and ensuring coordination between intelligence services of the CR, the Police CR, the MoI and the MFA. The **Central Emergency Committee** is included in the NSC system, being the working body of the Government intended to deal with emergency situations.

3. **The Ministry of the Interior** – The MoI is responsible for internal security and public order, and is thus one of the main coordinators of the fight against terrorism among the central administrative authorities. It is also responsible for related questions of asylum and migration, Schengen cooperation, control mechanisms for arms trade, etc. MoI experts attend working group meetings dealing with terrorism at the supranational level (CODEXTER within the Council of Europe, TWG within the EU, etc.). The Minister of the Interior proposes to the Government the announcement of the terrorist threat level and related measures and in case of danger of a delay announces this level preliminarily.

4. **The Police of the CR** – The scope of authorities of the Police CR is given by Act No. 273/2008 Coll., on the Police CR. The **National Centre against Organised Crime** (NCOC) plays a key role within the police structure in the fight against terrorism. The NCOC, specifically the section on terrorism and extremism, is, by Order of the Police President No. 103/2013, tasked with detecting, screening, and investigating the criminal activity of organised criminal groups (Sec. 361 of the Criminal Code) or especially serious crimes committed by organised criminal groups in the area of terrorism and

extremism and terrorism financing. Within the section, the **National Terrorism Contact Point** (NTCP) functions as one of its units, representing a mechanism that allows for the constant cooperation and exchange of operative information between intelligence services and the police on possible terrorist threats or on suspicious persons or groups. The Rapid Response Unit, regional intervention units, and other units of riot police that can be dispatched to rapidly intervene against armed terrorists and similar (active) attackers have their irreplaceable roles in the fight against terrorism.

5. **The Ministry of Foreign Affairs** – The MFA is the main guarantor of the CR's relations with other states and international organisations; within its sphere of foreign policy, it is responsible for the issue of terrorism, which has a strong international element. The MFA also ensures participation at the COTER (Council Working Party on Terrorism).

6. **The Security Information Service** – The competencies of the SIS are defined by Act No. 153/1994 Coll., on intelligence services of the CR. As per Sec. 5, para. 1 (e) of this act, the SIS provides information relating to organised crime and terrorism. For this purpose, it is authorised to use specific means of obtaining information, defined by Act No. 154/1994 Coll., on the SIS. The SIS provides information to the President, the Prime Minister and member of the Government. The SIS passes information to state and police authorities on findings that fall under their respective competencies. Government Resolution No. 1060 of 13 September 2006 designated the SIS as a place for the collection and assessment of information relevant to combating terrorism. When obtaining information, the SIS cooperates mainly with the OFRI, MInt, and the Police CR, specifically the NCOC. The SIS also cooperates with a number of foreign intelligence services within the framework of international platforms.

7. **The Office for Foreign Relations and Information** – The OFRI is a Czech intelligence service whose primary aim, effort, and mission is to provide state officials and state authorities with timely, objective, and high quality intelligence originating abroad and important for the security and protection of Czech foreign political and economic interests. The purpose of the OFRI's work is to protect the CR against threats originating abroad, including the threat of international terrorism. The competencies of the service are defined by Act No. 153/1994 Coll., on intelligence services of the CR.

8. **Military Intelligence** – MInt participates in carrying out the tasks of the security system relating to terrorism, particularly in the field of detecting threats, i.e. obtaining intelligence that will be helpful in determining whether there is a threat, in the field of threat assessment with regards to the CR and defining the threat level for the CR. The competencies of MInt are defined by Act No. 153/1994 Coll. and Act No. 289/2005 Coll., with a primary orientation towards national defence – only within this scope does MInt contribute to the fulfilment of tasks in the field of terrorism.

9. **The National Security Authority** – The scope of competencies of the NSA in the field of cybersecurity is defined by Act No. 181/2014 Coll., on cybersecurity. Due to current activities of terrorist groups and organisations in cyberspace and given the possible implications of these activities on Czech cybersecurity and its maintenance, the NSA has the authority and obligation to deal with this issue within the scope of its competencies. Within Act No. 181/2014 Coll., this regards those sections of the act that relate to cybersecurity incidents that may take the form of cyberterrorism. Furthermore, the NSA was appointed as responsible for cybersecurity by Government Resolution No. 781 of 19 October 2011. Cybersecurity, as per the National Cybersecurity Strategy of the CR for the Years 2015 – 2020, adopted by Government Resolution No. 105 of 16

February 2015, is understood to be the sum of various measures and instruments designed to ensure a secure, protected, and resilient cyberspace in the CR. As per this document, the NSA further helps to identify, assess, and tackle threats in cyberspace, reduce cybernetic risks, and eliminate the impact of cyberattacks, including cyberterrorism.

10. **The Ministry of Justice** – The MJ is responsible for the field of judicial cooperation, questions of extradition and international legal assistance. The Criminal Code and the Criminal Procedure Code fall within its responsibilities. It is thus the main coordinator of the national criminal policy, including the issue of terrorism prosecution.

11. **The Fire Rescue Service and the Integrated Rescue System** – Dealing with the aftermath of terrorist attacks, as regards impacts on property, lives, health etc., falls within the competencies of the FRS CR, which is responsible for rescue and liquidation works, and the IRS (mainly its primary units – the FRS CR, the Police CR, and the EMS), whose national coordination the FRS CR is in charge of. This corresponds to the main activities of IRS units in the case of, for example, the use of a dirty bomb, the threat of the use of or the detection of a booby-trap, a chemical attack in the metro, an attack by an active shooter, etc. The capacities and abilities of the FRS CR are further discussed in the chapters "Environmental Threats" and "Anthropogenic Threats".

12. **The Ministry of Finance** – The Financial Analytical Unit falls within the MF. This unit ensures for the MF those tasks that stem from special laws to combat the legalisation of proceeds from crime and financing of terrorism, and from special legal provisions regulating the application of international sanctions for the purpose of maintaining and restoring international peace and security, protection of human rights and combating terrorism (hereinafter "international sanctions"), following the measures taken by the UN Security Council and EU institutions. It ensures tasks for the MF that stem from Act No. 104/2013 Coll.

13. **The Ministry of Transport** – In the field of civil aviation protection against illegal actions, the MT is the supreme authority, coordinating the procedures in this area with relevant central government authorities within the Interministerial Committee for Civil Aviation. The system of civil aviation protection against illegal actions is defined by the Civil Aviation Office, which also publishes and updates national security programmes. In emergency situations that directly and seriously endanger civil aviation the MT has the authority to issue orders concerning flight dispatches for the time period necessary. Other emergency measures are defined by Sec. 86 (f) of Act No. 49/1997 Coll., on civil aviation. The physical protection of airports consists of a complex system of concrete security measures that require the cooperation of state authorities, security forces, and airport operators. In the event that civil aviation is in immediate danger from a particularly serious criminal offence, the airport operator is obliged to take emergency measures. In the CR, airport protection is legally covered by Act No. 49/1997 Coll., on civil aviation, as well as by the National Security Programme of Civil Aviation Protection against Illegal Actions in the CR; it is also necessary to mention the provisions of relevant EU regulations, which need to be complied with.

14. **The Ministry of Health** – In terms of responding to a possible terrorist threat, the MH is responsible for health services, the protection of public health, medical research activities, the coordination of health service providers falling under direct management of the MH, and handling addictive substances, mixtures, precursors and auxiliary substances. The primary task of the Czech healthcare system is to minimise the consequences of a terrorist attack impacting the lives and

health of persons; this is ensured by providing urgent pre-hospital and hospital care during incidents that, apart from other security breaches, are brought about by situations with a mass effect on the health of persons or a threat to public health, including threats to use chemical, biological, or nuclear materials. In terms of protecting public health, this concerns the coordination of a series of measures including prevention, setting anti-epidemic measures, and the availability of causal therapy.

15. **The Ministry of Culture** – The MC has no competencies in the field of combating terrorism. However, the task of limiting terrorism-related risks has been included in the Strategy on the Development of Museums in the CR for the Years 2015 – 2020. Pursuant to this task, the MC monitors and evaluates terrorism-related incidents and is currently drafting a series of preventive and protection measures to limit the risk of a terrorist attack in museums in cooperation with the MoI, the Police CR, and the top management of institutions caring for national cultural treasures.

16. **The State Office for Nuclear Safety** – The SONS is the state administrator and supervisor of the use of nuclear energy and ionising radiation, in the field of radiation protection and in the field of nuclear, chemical, and biological protection. Its competencies are defined by Act No. 18/1997 Coll., on the peaceful use of nuclear energy and ionising radiation (Nuclear Act), Act No. 19/1997 Coll., and Act No. 281/2002 Coll.[9] Its competencies do not include physical public protection. Implementation of the abovementioned acts indirectly reduces the possibility of misuse of dangerous chemical materials, biological agents, and nuclear materials for terrorist purposes.

17. **National Terrorism Correspondent** – The National Terrorism Correspondent is active within the Supreme Prosecutor's Office. The function was established by Act No. 104/2013 Coll., on international judicial cooperation in criminal matters. The National Terrorism Correspondent works to ensure easier and faster exchange of information with the national representative to Eurojust.[10]

C. SWOT Analysis

Strengths

- Low attractiveness and a weak basis for the activities of international terrorist groups in the CR (in the sense of organising terrorist attacks in the CR).
- A small and well-integrated Czech Muslim community, which does not show frequent signs of radicalisation; no socially-excluded communities or parallel social structures emerging in the CR that could act as potential breeding grounds for terrorist activities.
- A well-functioning IRS, capable of managing the possible consequences of a terrorist attack.

[9] The new atomic act becomes effective on 1 January 2017, Act No. 263/2016 Coll.

[10] Furthermore, they are active within the entire system of public prosecutors, especially with relation to chief public prosecutors who, as of the entrance into fore of the amendment to Decree No. 23/1994 Coll., on the rules of procedure of the Public Prosecutor's Office, the establishment of branch offices of some public prosecutor's offices, and details on the actions taken by legal probationers, as enforced by Decree No. 226/2016 Coll., perform surveillance in preparatory proceedings in matters of terrorist and related crimes and act as guarantors of interministerial and international cooperation related to exchanging information and training events.

- The impact of the migration wave in the CR is still indirect and does not significantly increase the risk of terrorism in the CR.
- No Czech foreign fighters involved in conflicts in the Middle East and North Africa on behalf of terrorist organisations.
- Satisfactory international cooperation between police and intelligence services.
- The national strategy to fight terrorism and the implementation of the bulk European legislation related to the fight against terrorism.
- A proactive and preventive approach of anti-terrorism forces, where systemic measures to improve response ability are taken even after individual incidents (or incidents outside the CR) – e.g. measures to strengthen resilience after the shooting in Uherský Brod in 2015, the Counterterrorism Package and Legislative Measures after the events in Paris and in Brussels, measures adopted as a result of the attack in Žďár nad Sázavou, continuous adoption of measures aimed at soft target protection.

Weaknesses

- The limited ability of the CR to significantly influence events outside the EU that have a considerable impact on the risk of terrorism (destabilisation in the Middle East and North Africa, the migration wave, the rise of the so-called Islamic State and other terrorist groups, etc.).
- The inability to anticipate attacks of terrorists acting alone.
- The limited experience of the CR with terrorist attacks (in its modern history, the CR has not recorded any terrorist attacks, in the true sense of the word, on its territory).
- The limited ability to suppress, by democratic means, the growing influence of radical, populist, and xenophobic groups that can lead to the radicalisation of individuals and the majority population.
- Limited financial resources available for the prevention and tackling of terrorist threats.
- Some minor legislative shortcomings (in the field of retention of communication data, the inability to use intelligence information in evidence proceedings, issues concerning foreigners, etc.).
- The limited influence of the CR within the EU (terrorism is an issue which must be dealt with at the EU level; in this regard, the CR is not among the leaders of the discussion, which is partially given by the limited significance of this threat in the CR).
- The CR's reputation as an islamohobic country (stoked by the statements of some politicians, widely publicised in the Middle East and North Africa).
- A communication environment inadequate for the use of modern technologies for ensuring internal order and security, national security and crisis management.

Opportunities

- The opportunity to learn from the experiences of Western countries without being directly affected by terrorism at the present moment. Measures can be implemented under conditions of no imminent threat of a terrorist attack in the CR.

- Preventing radicalisation and social exclusion of persons at risk of radicalisation before it occurs (in Western Europe, socially excluded communities with a high potential of terrorist radicalisation already exist; not so in the CR, where it is therefore possible to prevent their future development).
- The favourable development of external factors (which may change over time) – efforts to stabilise Iraq, resolve the conflict in Syria and Libya, ongoing military operation against the so-called Islamic State in Syria and in Iraq, the ceasefire in Syria and efforts to stall the migration wave, the EU agreement with Turkey.
- The opportunity to establish efficient cooperation between the Government and the owners of soft targets, which will mitigate the impact of a possible future attack.
- The opportunity to be a constructive actor within the EU and to contribute to the search for common solutions in the field of fighting terrorism and migration, with regards to their importance and convenience for the CR.
- The opportunity to improve the system of protection of critical infrastructure (physical and cybernetic).
- The opportunity to weaken some terrorist groups via measures aimed at curbing the financing of terrorism.

Threats

- Terrorists acting alone.
- The increase in xenophobic attitudes and of populism as a result of terrorist attacks abroad, the migration wave, and activities of Czech populist and islamophobic groups, which can lead to the radicalisation of individuals or small groups and to violent extremism.
- Attacks on soft targets.
- Threats to Czech citizens and facilities abroad.
- Financing of terrorism and related supporting activities.
- Attacks on particularly vulnerable facilities and persons.
- Attacks on the critical infrastructure.
- The influence of foreign state actors on radicalisation of persons or selected groups (Salafism, creation of paramilitary groups and support of extremist movements, e.g. by the Russian Federation, etc.).
- Foreign fighters.
- The abuse of weapons of mass destruction, conventional firearms, explosives and dual-use technologies.
- Risks arising from the migration crisis.
- Islamic radicalism.
- Political extremism and other terrorist groups.

D. Recommendations to Strengthen Resilience

A series of proposals for measures has already been adopted by the Government in two documents in 2016:

a) The Counterterrorism Package[11]

b) Legislative proposals in the field of internal security

This document sets tasks in the following areas:

1. Retention of communication data
2. Act on OFRI
3. Intelligence as evidence
4. Revocation of a residence permit of a foreign national in the CR
5. Classified information in administrative proceedings
6. Proceedings for granting international protection at the internal border
7. Events attended by large numbers of people (mass events) and police powers
8. General assessment of legislation in the area of prosecution of terrorism and related security threats
9. Expansion of cross-border cash transport controls

Further Measures:

1. Focus on the issue of radicalisation and recruitment. It is necessary that relevant bodies pay attention to signs of radicalisation of individuals or small groups (not only) in the Muslim community – this kind of radicalisation may manifest itself in different ways, e.g. via social networks or other activities in cyberspace. It is important for the state to intervene when persons who may have a wider influence on the given community (e.g. imams) abuse their position in order to disseminate extremist interpretations of Islam, which are incompatible with the principles of a democratic society, or directly encourage violence.
2. In this respect, it is also necessary to monitor the financing and support of similar activities from abroad.
3. Attention should be paid to radicalisation in prisons – experience from Western Europe shows that the criminal environment is a significant factor of radicalisation.
4. Strengthen measures concerning active shooters – in particular, continue training riot police units via so-called AMOK exercises, develop a register of offences, etc.

[11] This document is classified as per Act No. 412/2005 Coll., on the protection of classified information and on security competencies, as amended, and its proposals for measures cannot therefore be included in the present text.

5. Address the issue of protecting soft targets from terrorist attacks. Attacks on soft targets can be prevented (or their consequences mitigated) by strengthening their security (it is however necessary to balance security with costs and efficiency), but also by training their employees. The general problem of soft targets is that they are usually owned by private entities, which makes cooperation of the state with the private sector and the participation of soft targets in ensuring their own protection a key aspect. The Government tasked the MoI with drafting a proposal for the creation of a nationwide system of support of the security of selected soft targets. This activity builds on the long-term experience of cooperation with, for example, owners of Jewish edifices.
6. Concerning the issue of foreign fighters, it is necessary to also dedicate attention to the development of paramilitary groups in the CR as well as to foreign influence.
7. Strengthen the protection of critical infrastructure, both physical and cybernetic.
8. Support the long-term development of the communication infrastructure and public administration technologies, as well as eGovernment, for the purpose of securing internal order and security, national security, and crisis management.
9. Adopt an amendment to the Criminal Code, prepared by the MJ, which amends certain provisions relating to terrorism.
10. Propose a legislative amendment that would, in urgent cases and based on specific information, allow intelligence services and law enforcement authorities to immediately implement measures normally requiring authorisation of another Government authority (typically the court) and to submit the application for authorisation within an additional period (e.g. 48 hours). Typically, this would concern cases where a terrorist attack or its repetition could be prevented, with the consequent clarification and minimisation of the negative consequences of terrorism.
11. Propose a legislative amendment that would, for the purposes of detecting or verifying information on terrorist crimes, grant immediate access to information on owners and holders of bank and similar accounts, on accounts that are connected to an account of interest, on the balance of the account of interest, as well as account statements of financial transactions on an account of interest.
12. The legislative amendment aiming at, *inter alia*, allowing the prosecution of a service of non-state foreign forces is currently being discussed within a working group of the MD. This area needs to be included among those issues that this chapter proposes to resolve.

EXTREMISM

A. Description and Assessment of the Threat and Associated Risks for the CR

1. Introduction

For the purposes of the Audit, extremism[12] denotes clearly identified ideological attitudes that deviate from constitutional norms, carry elements of intolerance, and attack constitutional democratic principles. These principles include, *inter alia*, respect for the rights and freedoms of people and citizens, protection of minorities within decisions of the majority, the freedom and equality of people in dignity and in rights, the inalienability, permanence and irreversibility of fundamental rights and freedoms without distinction of sex, race, skin colour, language, faith and religion, political or other opinions, national and social origin, adherence to a national or ethnic minority, wealth, birth, or other status. These extremist attitudes are capable of manifesting as activities that are destructive to the existing democratic system.

The deeper roots of extremism are social (not only ethnic, but also political, local, family, and/or religious tensions resulting in the search for alternative social ties, the ritualization of behaviour, the creation of myths, etc.), psychological (suggestion, imitation, deprivation, affectation, mob actions), and biological (aggression, territoriality).

Extremism exists at all times and in all societies. It can never be completely eradicated. It is only possible to minimise the threats associated with it that are aimed against the pluralistic democratic system. The level of the threat is related to external factors that are social (the level of social cohesion, coexistence with minorities, migration), political (trustworthiness of mainstream political representatives) and economic (the economic crisis, unemployment), and internal factors that are repressive (the ability to paralyse the extremist core) and preventive (the ability to prevent the radicalisation of majority population, the ability to protect potential victims of extremism). As a rule, when significant negative social, political, or economic changes occur, extremists are among the first to criticise the situation and seek to profit from the criticism. Some causes may be real, while others are artificially contrived through propagandist dissemination of disinformation. Furthermore, it is also true that state and private organisations usually need several years to learn to effectively manage and repress a specific extremist threat.

The hidden danger of extremism lies in the acceptance of extremist ideas in mainstream thought and in their dissemination within society. Thus, though only a specific minority is threatened initially, when extremism starts to interfere, in a totalitarian manner, in the majority's way of life, it is usually too late.

Anti-extremist policy often mistakenly focuses solely on extremist "clients", while forgetting that its primary concern should be the protection of rights and freedoms of the victims of extremism. It is not the role of the state, based on some ritualised perpetuity, to study extremist groups. Its ambition should be to constantly analyse the threats posed by extremists to their real and potential victims and to be able to effectively protect these victims, provide them with a sense of security and with

[12] This definition is based on the general concept used by the MoI.

conditions for a dignified life. This "focus on victims" is already taking place in some Western European countries; the CR is still waiting.

The focus on victims can offer a rationale for why extremist activities take place. The intention to paralyse extremists is not an end in itself. First and foremost, the state protects specific groups of people; after that, it is the right of every citizen to have their view of the world and live by it. What characterises extremists is that they start by picking victims from weak social groups. After acquiring sufficient power, they focus on eliminating all social groups and individuals that disagree with them. Extremism thus ultimately endangers the rights and freedoms of every last citizen of this state.[13]

The chapter "Extremism" assumes cross references with other chapters in the Audit, especially with the chapters "Terrorism" (which takes into account the risks associated with religious extremism), "Cyberthreats", "Security Aspects of Migration", "Influence of Foreign Powers", and "Hybrid Threats and their Impact on the Security of Czech Citizens".

2. The Extremist Threat in terms of the Originator

Because of specific historical experiences, Czech society has developed a certain immunity and mistrust towards right-wing and left-wing extremism. However, this immunity weakens as these specific historical experiences become more remote. New trends are constantly emerging and extremist groups are becoming more internationally interconnected, thus gaining experience and opportunities, and some extremist elements are permeating mainstream politics.

a) Right-Wing Extremism, Anti-Muslim and Anti-Immigrant Extremism[14]

Since the 90s, Czech society perceives right-wing extremism as the more significant threat for democracy. Its most extreme forms are often primitive and its proponents frequently resort to various forms of physical violence. Resistance to traditional right-wing extremism is rooted in the negative image of Nazism that still persists in society.

The right-wing extremist scene is developing dynamically. It is primarily a natural consequence of preventive and repressive measures taken by the state against its manifestations. At the same time, it is influenced by a growing international interconnectedness, which contributes to the sharing of experience and new approaches. From a politological point of view, the current right-wing scene is elusive. Over time, various groups or individuals have changed their attitudes and beliefs, altered their names, and entered new alliances. A coherent system of political views was never a permanent

[13] This way of seeing the problem of extremism is partially transmitted to the public via civil society and international institutions. Such communication with the majority, however, seldom works. Human rights institutions are often viewed as too detached from reality, their messages are often received with scepticism and even antagonism. Therefore, it is important to learn to explain the focus on victims to society as something useful that concerns every citizen. Only then can training of police officers and other civil service employees on how to proceed in relation to victims of extremist crimes really translate into practice.

[14] When evaluating the severity of impact, the vital, strategic, and otherwise important interests of the CR, as defined by the SS 2015, were considered. In the case of extremism, these interests are: maintaining all the attributes of democratic rule of law, including the guarantee and protection of basic human rights and freedoms, security and stability, especially in the Euro-Atlantic area, the prevention and management of local and regional conflicts and mitigating their impacts, the promotion of democracy, basic freedoms and principles of the rule of law, ensuring internal security and public protection, the prevention and suppression of security threats affecting the security of the CR and its allies, reducing crime, creating conditions for a tolerant civil society, suppressing extremism and its causes. As regards the criterion of probability, we considered the historical development of extremism, current trends, experiences from abroad, statistical data on extremist crimes, and sociological surveys. Furthermore, we considered the ability of the state and civil society to effectively counter the individual threats. The final assessment is therefore the result of an expert evaluation and consensus.

factor for the right-wing extremist scene. These policy frameworks constitute merely a vague and changeable backdrop for permanent factors. These are the constant search for enemies and an aggressive identification as their opposite.

It is not essential for most right-wing extremists whether they subscribe to Nazism or aggressive Czech nationalism. In this regard, they may often undergo unconceivable changes of opinion; consistency is an exception. Across all opinion streams, they agree on one thing – hatred towards certain minority groups. In the CR, this hatred is specifically aimed against the Roma, Jews, and other ethnic and national minorities, foreigners, sexual minorities, the homeless and drug addicts. Recently, in connection to terrorism and migration, hatred towards Muslims and immigrants is on the rise. Hostility towards opposing opinions is also intensifying.

It is not only political views that are changeable, but also the groups against which extremists define themselves. Recently, hostility towards the Roma has been entirely subdued and replaced by hostility towards Muslims and immigrants. What is important is to have enemies; who these enemies are is secondary.

Another important permanent factor of right-wing extremism (but also of left-wing extremism) is the entirely different behaviour within and without the community.[15] Inside their communities, right-wing extremists readily voice opinions or carry out activities that are clearly reprehensible or illegal, but deliberately disguise these attitudes when presenting themselves to the majority population. This strategy, aimed at recruiting new members and sympathisers, is often very effective. In the case of some anti-Roma rallies in 2013, for example, it was shown that part of the majority population has adopted some extremist opinions and activities. In extreme cases, the majority population has even obscured the extremists at these rallies. New opinion leaders and organisers replaced traditional extremists.

Since 2015, moreover, the extremist scene is undergoing a qualitative shift. The former right-wing extremist groups are receding into the background. They have exhausted their potential and have become weakened by police repression alongside civil society and media campaigns. Moreover, they have been labelled as “unacceptable in society” for the asocial, primitive, and excessively radical attitudes of their members or sympathisers.

In the context of the migration wave and the terrorist attacks in Europe, anti-immigrant and anti-Muslim entities are becoming more active. These are often unburdened by connections to traditional militants and take care to remain within the law. Their ranks are populated by more educated, more able, and better financially equipped individuals who are able to win over public figures, including political representatives. However, as regards their rhetoric and activities, these new entities have a very similar profile to traditional extremists. Through more sophisticated rhetoric, they are able to reach a broader spectrum of the public.

The unifying element of extremist entities is not a (representative) ideology (e.g. Nazism, fascism, aggressive nationalism), but hatred based on ethnic, religious, or other differences. That is, based on characteristics that the people in question often cannot influence. It has been true in all the stages of modern Czech history that these entities were able to formulate the problem, but not the solution. The solutions they propose are usually very easy and very quick at first sight, but are often at odds with generally accepted democratic principles or with the law. In fact, they increase social tensions and narrow the scope for finding constructive answers. The growing importance of extremist movements signifies increased polarisation and division within society. Any accession to power by extremists would result in limiting freedoms and introducing totalitarian practices.

[15] E.g. squatting.

Fortunately for now, Europe, including the CR, lacks charismatic extremist leaders who would be able to unite the various extremist movements and gain a more significant share of power. Nevertheless, the partial success of some extremist parties in several European countries proves that the emergence of a truly charismatic leader of the pre-war type would be a hard test for democracy.

The activities of extremist subjects are, *inter alia*, a means to undermining pluralistic democracy. For this reason, it is important to bear in mind that they may enjoy the support of a foreign state bent on weakening Czech democracy and ejecting the CR from its alliance with other European democracies.

An integral part of the extremist scene, which always requires special attention, are radicalised militant individuals or groups that do not hesitate to use violence in order to enforce their objectives and to hurt others. They commit violence against people from the ranks of their enemies, especially ideological opponents, but also against the police, which they see as embodying "state power". The radicalism of these people can easily be misused by individual opinion leaders that usually shun direct physical violence, but inspire others to resort to it.

In the internet age, a significant risk is posed by the auto-radicalisation of people who normally do not take part in public extremist activities and who are thus unknown to security forces.

b) Left-Wing Extremism

Decades of communist dictatorship made Czech society mistrustful of utopian ideas of a society organised in accordance with the teachings of Marxism-Leninism. For this reason the left-wing extremist scene has been dominated by anarchist ideas since the 90s.

Anarchists face several problems when promoting their ideas. Firstly, they are unable to agree on cooperation within their own movement. It is formed by several individuals with often differing opinions, who are unwilling to compromise and are unable to subordinate their personal ambitions to those of a team. The anarchist movement is paralysed by diffused debates between various opinion groups that are difficult to understand and often unappealing for the majority population. Secondly, their generally formulated ambitions to change the social order are met with the mistrust of a large part of the population.

Anarchists are aware of their limited influence on the formulation of general social, political, and economic topics, as well as of their disunity. Therefore, they pick a limited range of relatively non-conflictual areas for their presentation to the public. These include antifascist activities, protection of the environment, helping the homeless, promoting alternative ways of life and alternative cultures. Currently, they are focused on assisting refugees.

A closer look at the statements of representatives of radical anarchy, however, divulges their extremist background. It is founded on class hostility, hatred towards opinion opponents, and hatred towards the state and the system. Anarchists usurp the monopoly on the correct way society should be organised and are unwilling to accept any compromises when enforcing it. In no way do they participate in democratic dialogue or respect the pluralistic political system. They have their own ideas about promoting their opinions. Moreover, radical anarchists consider the use of violence legitimate. These radicals want to monopolise violence. In the CR, physical attacks on ideological opponents (especially neo-Nazis) and the destruction of another's property (arson) are quite common.

Similarly to the extreme-right, the Czech anarchist scene is internationalised and Czech anarchists have adopted a number of trends from abroad. In this regard, it should be noted that, in other countries, anarchists are responsible for mass public riots and, in extreme cases, terrorist attacks, murders, and thefts. As in the case of right-wing extremists, left-wing extremists may produce so-called lone wolves, or militant radicals that refrain from public activities while waiting for a suitable opportunity to commit a violent act.

At present, Marxist-Leninist groups can be considered marginal. Young left-wing radicals from this side of the spectrum are facing the disinterest of their peers, personal animosities, and the excessive ambition of some leaders. Their organisations and groups are mostly dysfunctional. More active individuals are therefore joining established left-wing political groups and organisations. Within their framework, they create radical platforms and gradually introduce extreme opinions to the mainstream society. Due to certain similarities of opinion on particular topics (antifascism, the support of radical feminism, etc.), they may cooperate with anarchists.

c) Threat Assessment

Specifics of the Threat	**Right-Wing, anti-Muslim and anti-Immigrant Extremists**	**Left-Wing Extremists**
Rift in society – creating antagonism.	High Risk	Medium Risk
Increased tensions based on ethnicity, religion, or opinion; demonstrations and acts of violence.	Medium Risk	Medium Risk (only the point of view is relevant)
Acceptance of extremist ideas in mainstream politics.	High Risk	Medium Risk
Occurrence of radicalised militant individuals or small groups that may use violence to promote their interests.	Medium Risk	Medium Risk
Emergence of an extremist political entity with a charismatic leader.	Medium Risk	Low Risk
Emergence of extremist militias.	Medium Risk	Low Risk
Abuse of domestic extremist platforms by foreign states.	Medium Risk	Medium Risk

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

Basic Documents

In general terms, extremism is touched upon by the SS 2015. Nevertheless, the documents that, at the state administration level, deal directly and exclusively with extremism are the annual **Report on Extremism in the CR and the Strategy to Combat Extremism**. The Strategy to Combat Extremism is evaluated every year. Both documents are approved by the Government. The Report on Extremism describes significant events and trends of the past year. The documents have been issued since 1997. They include contributions from the MoI, the Police CR, intelligence services, the Supreme Public

Prosecutor's Office, the Supreme Court, the Probation and Mediation Service, the Military Police and the GISF. The Strategy to Combat Extremism is divided into five chapters: Communication to Counter Demagogy; Knowledge to Counter Totalitarianism; A Single Anti-Extremist Platform; Expertise and Immunity; Assisting Victims of Crime.

Legislation

The term extremism is not directly embedded in Czech legislation. In practice, however, several legal norms are useful in its prosecution. The working expression is "crimes with an extremist subtext". Furthermore, the CR is bound by a number of international conventions on extremism. Crimes with an extremist subtext are also reflected in Czech jurisprudence. In terms of legislation, the decisions of international judicial bodies, e.g. the European Court of Human Rights, are essential.

Basic documents on extremism include the Charter of Fundamental Rights and Freedoms and EU norms. Provisions in the administrative and criminal law may be used to combat extremism (restriction of the right to freedom of expression, of association, of assembly, of petition or the labour law – e. g. the impossibility of extremists to exercise certain professions in the security field).

Legal norms offer law enforcement authorities the possibility of issuing strict punishments for violence having an extremist subtext. The chapter "Terrorism" specifies the acts relevant to such actions or their support. Furthermore, Czech and international norms declaratively define democratic principles and condemn historical totalitarian regimes.

The overwhelming sentiment within the security community is that the current legal framework is sufficient. It is necessary, however, to work effectively with the legal instruments available.

Responsible Institutions and Bodies

An efficient anti-extremist policy is among the Government's regular priorities. At the central state administration level, the **MoI** is the coordinator. A key role is played by the **Police CR**. Within the police, several units take part in implementing anti-extremist measures. The police has experts on extremism within its Criminal Police and Investigation Service. The **SIS**, within the scope of its lawful competencies, gathers information on intentions and activities directed against the democratic foundations, sovereignty, and territorial integrity of the CR. The **OFRI** deals with activities of foreign extremists that may impact national security. **MInt** is also involved in combating extremism. Various other tasks that overlap with anti-extremist policy are carried out by **other security forces and security system units**.

Apart from security forces, **other agencies and offices** are involved in anti-extremist activities: **the MJ, the MEYS, the MC, the MLSA, etc.** Particularly in the field of prevention, a number of tasks are carried out by the **Office of the Government** and, at the international level, by the **MFA**.

An irreplaceable role in combating extremism is played by the non-governmental sector. In addition to the activities of **civil society and serious journalists**, it is necessary to highlight the work of some **NGOs** and **specialised academic institutions**.

At the international level, the CR is bound by its **membership** in some **international organisations** or by its **cooperation with them**. Particularly in the area of combating racism and xenophobia, the **Council of Europe and the EU** need to be mentioned (most importantly, the EU Agency for Fundamental Rights), the **Organisation for Security and Cooperation in Europe** (the Office for Democratic Institutions and Human Rights), the **Visegrad Group** (the V4/Austrian Group on Combating Extremism). In general terms, extremism is also tackled by the **UN**. Apart from these institutions, a number of **international platforms** are directly or indirectly involved in the fight against extremism.

Evaluation of Repressive and Preventive Activities

Repression

The dynamics of extremist movements fit into a specific repetitive cycles. These are characterised by an initially rapid rise of a new or modified movement. The movement gradually gains momentum and becomes ever more radicalised. The state apparatus is unable, at first, to respond flexibly. After a thorough assessment of the situation in terms of security risks and breaches of law, and after overcoming a series of lengthy bureaucratic obstacles, it is then able to apply – usually after an appeal or even the urging of civil society – appropriate punitive measures. Repression then causes fear and mistrust among extremists. Their radicalism erodes. Repressive measures are often highly publicised and, in the context of media coverage, some hidden negatives and illegal behaviours of the extremists come to light. This reduces their trustworthiness in the eyes of the public, limiting their support.

In the CR, the most effective approach is a thorough repression of the extremist core. One important rule applies to repression – it must be delivered promptly. Often, it is simply enough that the police clearly declares that a certain type of illegal action will not be tolerated under any circumstances.

The system of the repressive anti-extremist apparatus is relatively well secured. The police has a sufficient number of specialists within the riot and criminal police services. In comparison to other countries, it is also equipped with relatively high quality material and technical equipment. A number of training programmes, methodological tools and relevant internal acts relating to extremism exist. Measures have been set up that aim to prevent extremists from infiltrating security forces.

Nevertheless, the work of the Police CR in the area of extremism is complicated by three factors:

- The lack of flexibility in a large bureaucratic institution.
- Extremism is often understood as a political issue by police officers. They often face direct or indirect pressure of various political representatives in connection with it. Sometimes, they themselves act in a way so as to first and foremost avoid such pressure.
- The perception of certain social issues within the police mirrors the moods of the population. Some police officers, moreover, come into contact with only a certain (usually the negative) segment of reality when performing their daily duties. Therefore, this professional group often faces various prejudicial tendencies.

The ability to react flexibly to new trends in the area of repression stands on the additional activities of a limited number of quality professionals within uniformed and non-uniformed police, who can face the three factors listed above and who can demonstrate the ability to not succumb to political or social pressures.

As regards the justice system, there is a shortage of experts in the CR who understand the area of extremism, have an overview of the current situation and are aware of the associated risks. Ignorance of the real situation may lead to underestimation of extremists and the perception of their crimes as a relatively harmless manifestation of youthful indiscretion or revolt.

The biggest current challenge is to combat illegal and reprehensible content on the internet. In this regard, security forces face three main problems:

- The enormous amount of such content.
- A lack of qualified police specialists.

- The placing of such content on servers located in third countries with different legislation, making it impossible to sanction it.

A traditional and long-term error that can be attributed to the MoI lies in the fact that repressive practices are not justified, explained, or placed within a wider context. The public is informed only about isolated events taken out of context. This enables extremist subjects to formulate an image of martyrs, who – as the “only real opposition” – have become the victims of “state bullying” and “political police”. The police, as a result, is not viewed as a body protecting the interests of the population, but as a kind of natural enemy of the extremists. To give a specific example, a situation where the police protects a group of people from dangerous militants with extremist attitudes may be communicated as the police having clashed with radicals.

Prevention

Prevention of political radicalisation is a European challenge that has not yet found an adequate solution. In the CR, even the basic conditions for its application are vague. The following remains unclear:

- Who should initiate, organise, finance, and evaluate it (government vs. non-governmental sector, which government institution)
- Who it should target in order to be effective (definition of target groups)
- What its message should be (right-wing vs. left-wing extremism, defence of pluralist democracy, focus on extremism vs. focus on related phenomena)
- What channels should be used (media, campaigns, lectures, cultural and sports events, social networks)
- What should be the measurable result (what can be considered a success and how it can be measured).

In the CR, several different anti-extremist prevention projects have been implemented, a little later than in other Western European countries. A number of these projects were very carefully planned and their effects were demonstrably positive. However, at least the same number of projects were created hastily in reaction to certain situations or sudden demand, without clear specifications, without engaging real experts, without defining goals or the method to measure success. This hasty approach resulted in wasted resources and missed chances. In defence of the CR, however, it needs to be said that several Western European countries have had the same experience.

The CR has a large number of experts on extremism (knowledgeable about the scene and its history), but it has no experts on “prevention of extremism” and related phenomena. Extremism prevention is, at least at the state administration level, often understood solely as a repressive measure. Until political representatives realise the importance of extremism prevention, no significant changes can be expected at the central or local level of administration. State administration must formulate a demand, must claim its responsibility, and must create partnerships with other subjects, both governmental and non-governmental. Traditionally, the non-governmental sector is the bearer of new impulses. An enduring problem is the mutual mistrust between state and non-state actors, which may be overcome only through long-term cooperation. In some countries, there are separate institutions or branches dedicated to coordinating and organising preventive activities in the area of political radicalisation (e.g. the German Federal Agency for Political Education).

A common shortcoming of anti-extremist measures is their inaccurate targeting. At the state administration level, this concerns large projects such as generally formulated national strategies or national action plans; on a smaller scale, it can be campaigns aimed at “the entire population” or at "young people". These errors are the result of the work of civil servants or activists without sufficient education or professional experience. Valid sociological and psychological data are often lacking for a clear definition of the target group. The security community in Western countries is increasingly talking about prevention targeted directly at extremist "clients". Typical examples of such prevention are so-called exit programmes, which are supposed to help "clients" leave the extremist environment. In terms of security, acquiring a "reformed" individual from the extremist environment carries a multitude of benefits.

The messages of prevention activities are another key unknown. Experience shows that making people fear extremism is an inadequate concept. It is difficult to popularise democratic values in a trustworthy and credible manner. Most projects are directed against extreme right-wing subjects. Prevention campaigns against extreme left-wing subjects, especially anarchists, are practically non-existent. The public relations capabilities of extremists are often incomparably better than those of some projects or campaigns sponsored by the state or non-state actors.

When selecting channels for the transmission of information, one rule is essential – that these channels be managed by experienced professionals. Channels that impact a large number of recipients carry a very high risk that a poorly implemented project may produce the opposite effect from the one intended by its authors.

Over time, increasing demands are being placed on the quality and implementation of prevention projects. As a rule, it is no longer sufficient to declare that "the project was successful" or that it "fulfilled its purpose". It is necessary to set measurable indicators of success, similarly to the way it is done in the commercial sector. Qualitative data may be provided by, for example, sociological surveys. Should prevention be aimed at extremist "clients", it would be necessary to also study psychological factors, for instance amidst people sentenced for crimes with an extremist subtext.

There are even opinions that prevention projects aimed at extremists should not be carried out at all. According to this concept, it is necessary to focus solely on problems that extremists point to, promptly find an alternative solution to populist and often unrealistic extremist proposals, and then introduce this alternative solution to the public and begin enforcing it in practice.

In connection with the neo-Nazi movement focusing on the so-called "Roma question", state authorities dedicated great efforts to combat its proponents. For a certain time, the state focused unilaterally on neo-Nazis, as if they were the sole cause of problems in socially excluded communities and as if these problems were to have been solved by the elimination of neo-Nazis. That this was a faulty strategy was shown by the unrest in Šluknov in 2011, whose main actors had no ties to the extremist scene.

A similar risk of an erroneous understanding of a problem arises in connection with the migration crisis. The state has as yet not managed to respond clearly to fears regarding immigrants. That is, it has been unable to clearly and publicly communicate long-term measures that would limit the risks of terrorism and prevent the emergence of ghettos and the abuse of the social system.

C. SWOT Analysis

Strengths

- A good security system within the repressive apparatus.
- Efficient legislative framework.

- The existence, albeit limited, of a group of professionals who do a great job in the area of repression.

Weaknesses

- A misunderstanding of the basics of the threat of extremism. Society often does not understand the concept of victims, where every citizen may become a victim.
- An outdated and unsustainable concept of right-wing and left-wing political extremism that is still being applied in the area of security policy.
- Low flexibility, the ability of a rapid and adequate response by security forces. The police, in particular, is exposed to frequent and intense political pressure. There are frequent staffing and conceptual changes. These results in the absence of: responsibility for implementing given tasks, strategic direction, expert training, adequate and rapid communication between relevant units, and an appropriate and efficient use of existing powers and instruments, including the communication infrastructure.
- An unclear and dysfunctional concept of prevention. The state relies on repression and only knows how to apply repression. This is unsustainable in the long-term.
- Poor collaboration between the Governmental and non-governmental sector. Poor cooperation between individual entities within the Governmental sector as well as within the non-governmental sector.
- A limited number of sufficiently erudite and professionally experienced experts in the area of prevention of extremism and associated phenomena.

Opportunities

- A functioning, pluralistic democracy. The existence of civil society and independent media.
- Membership of the CR in supranational democratic bodies and the consequence obligation to abide by certain democratic commitments.
- Resentment and distrust towards extreme totalitarian ideologies conditioned by historical experience.
- The disunity of the extremist scene, the absence of charismatic leaders.
- In comparison with other European countries, the CR is ethnically and religiously relatively homogenous.

Threats

- In general, the ability of extremists to split society and weaken the CR by creating antagonisms based on ethnic, religious, class, or other criteria. **High risk**.
- Rising tensions based on the ethnic or religious criteria, including demonstrations and violence. Local triggering events still have the potential to mobilise the public. Even the majority is undergoing polarisation, where animosities emerging among supporters of various opinions. **High risk**.
- The spillover of extremist elements into mainstream politics. **High risk**.

- The possible existence of radicalised militant individuals or small groups that may use violence to promote their interests. **Medium risk**.
- The possible emergence of an extremist political entity with a charismatic leader who will be able to unite the extremist scene and reach out to other potential supporters. **Medium risk**.
- The emergence of extremist militias, which can, often illegally, arm themselves and aim their potential activities against certain groups of individuals based on ethnic or religious criteria. **Medium risk**.
- The abuse of domestic extremist platforms by foreign states with the aim of weakening the functioning of a pluralist democracy in the CR. **Medium risk**.

D. Recommendations to Strengthen Resilience

1. A key requirement is the advocacy and promotion of the concept of victims. This concept may bring the following advantages:
    a. A reduction of the attractiveness of extremist groups.
    b. A reduction of the willingness of public figures, including politicians, to freeride on extremist topics. A reduction of their ability (particularly in the case of politicians) to negatively influence the work of those involved in anti-extremist policies.
    c. An increase in the motivation of those involved in anti-extremist policies.
    d. An improvement in the working conditions of those involved in anti-extremist policies.
    e. A clarification of the concept of prevention and the opening of new possibilities for preventive action.
2. Abandon the concept of extremism in the area of security policy. Redefine threats while emphasising the protection of the state and of pluralistic democracy.
3. Redefine risk groups in the security community, with an emphasis on their ability to undermine the democratic principles of the state. This should enable an efficient division of labour among security forces.
4. Train police and judicial experts on new trends and sanctions as regards extremists. Increase cooperation between the police and public prosecutors' offices, e.g. via joint educational activities and training. Personal encounters between police experts and public prosecutors are essential.
5. Interconnect statistical data of the police, public prosecutors' offices, and courts, enabling the tracing and analysis of individual criminal proceedings.
6. Strengthen the ability of the police to investigate cybercrime, in accordance with the strategic document Development of the Police of the CR 2016 – 2020.
7. Continue implementing measures preventing the infiltration of security forces by extremists.
8. Ensure the innovation of police information systems, prevent duplicity, and enhance capabilities to share necessary and multiple volume data. Develop a communication environment with an emphasis on the use of modern technologies.

9. In order to promote the concept of victims, the state must engage and cooperate with experienced professionals in the area of communication, education, and training. It must explicitly set the expected results and motivate them adequately.
10. The involvement of these professionals should be promoted particularly in the area of prevention. Find inspiration in other Western countries, especially in the UK and in Germany. Learn from the mistakes made in other countries.
11. Deepen cooperation between the state administration, territorial self-Governments, and the non-governmental sector.
12. An open state administration, especially in the area of providing information about the extremist scene and associated phenomena. Ant-extremist policies cannot be implemented in isolation, without informing the public. Anti-extremist measures must be explained and justified to the public. It is also necessary to offer alternative solutions to issues referred to by extremists. It should be borne in mind that, at present, the media and their professionals are much more adept that the state administration at communicating certain messages to the public.

ORGANISED CRIME

A. Description and Assessment of the Threat and Associated Risks for the CR

1. Introduction

Organised crime is repeatedly described as a serious threat to the security of the CR and a priority area for the state administration. There is no doubt as to its presence in the CR. However, questions are raised by the very definition of organised crime, for there is no generally accepted definition of this phenomenon in the CR.[16] Thus, doubts arise as to which activities fall under this concept, which, alongside the high latency of organised crime, contributes to the difficulty of computing the scope of the threat. At the same time, the breadth of the term "organised crime" makes it impossible to provide a detailed description of all its forms in this chapter.

The main motivation of organised criminal groups is financial gain; their secondary motivation is strengthening the opportunities of this gain via increasing influence on the decision-making process of state bodies in relevant areas (in particular the allocation of funds, but also legislation), or strengthening their own defences via infiltration of law enforcement authorities. At the same time, organised criminal groups aim to carry out their activities latently, without attracting the attention of law enforcement authorities or causing displeasure to the public. This is linked to the partial moving away from the use of violent activities (contract killings) towards less conspicuous activities (blackmail, fraud).

Ordinary citizens usually remain untouched by organised crime, since organised criminal groups do not harm them directly. In the area of distribution of certain commodities – e.g. illegal drugs, weapons, and forged documents – organised criminal groups may even be perceived by some citizens as providers of desirable services rather than as criminal entities.

At present, there are different perceptions of the two main areas of organised crime – its traditional and its modern form. Traditional organised crime consists of blatantly illegal activities – e.g. drug trafficking, facilitating illegal migration, forging documents and others – that are currently quite effectively sanctioned by the state.

On the contrary, modern organised crime consists of the undesirable influencing of the decisions of public bodies, the creation of clientelistic and corrupt networks, and the influencing of legislation. All these activities are difficult to prove, many of them can be considered legitimate and legal, and their damaging effects are only manifested as the overall result, which is usually the inefficient use of public funds. As a rule, these activities are very difficult to prove and to prosecute and existing repressive instruments are not adequate for dealing with them. For the purpose of this chapter, activities falling under the concept of organised crime are understood to include both the traditional and the modern variant.

[16] In Act No. 40/2009 Coll., (Criminal Code), Sec. 129 defines an organised criminal group, Sec. 361 defines the offence of participating in an organised criminal group, and Sec. 107 defines an offence to the benefit of an organised criminal group. Nevertheless, none of these definitions fully exhausts the term "organised crime" and does not specify the scope of activities covered by it. Other definitions are given by EU and UN documents.

Organised crime evolves and changes in time. It is absolutely necessary to thoroughly monitor and adequately respond to this development. The currently prevailing trend is that of professionalisation of organised criminal groups, with individual members specialising in specific activities. Professional criminals offer services to various customers and, rather than closely knit groups, operate as loose criminal networks whose members carry out specific activities according to their specialisation. These networks use modern communication devices and encrypted connections, which makes it difficult to identify them. A related phenomenon is the use of professional services offered by lawyers, tax consultants, and accounting firms to disguise illegal activities and money laundering.

Another important trend is the transfer of organised criminal activity into cyberspace.[17] This does not concern merely the communication mentioned above, which is faster, more efficient, and more difficult to intercept in this environment, but also a range of new activities that expand the portfolio of organised criminal groups. It includes, in particular, various types of fraud (e.g. obtaining payments based on fictitious or forged documents or invoices), cybercrime (electronic blackmail, dissemination of malware, identity theft, operation of illicit markets in the darknet etc.), and procedures associated with the legalisation of proceeds from crime (virtual currency transfers). In this global environment, organised criminal groups make use either of their technological advantage over law enforcement authorities, or at least of a higher level of anonymity. Law enforcement authorities must adapt to these groups' activities in a much less flexible environment shaped by legal and organisational limits to their work. For state bodies, it is also much more difficult to adequately remunerate IT experts, while organised criminal groups may, given the profitability of their activities, afford these services easily. In the area of organised crime committed on the internet, we assume a high level of latency due to the difficulty in detecting certain types of criminal activity.

This chapter does not address in detail the current situation in the area of migration and illegal migration, as this topic is the subject of another chapter. Likewise, it does not devote a lot of space to cybercrime, as this topic is the subject of the chapter "Cyberthreats".

2. Threat Description and Assessment

The threats in this chapter are assessed in terms of their impact on financial (tax revenue, efficiency of expenditures) and other state interests,[18] as well as in terms of the estimated range of their occurrence. The criterion of probability of occurrence of these threats is not applicable here, since all these threats are already present to a certain extent in the CR. Given the latency of organised criminal group activities, it is impossible to accurately quantify the scope of these activities. The threat relevance is assessed on a scale low – medium – high based on a combination of the factors mentioned above. Although traditional organised crime (drug trafficking, human trafficking, weapons trafficking, forging of documents, organised property crime – automobile thefts, pick-pocketing, etc.) is considered very serious, due to the limited scope of this chapter, recently published documents addressing these criminal activities are referenced in section B.

At the same time, we consider the situation in these areas to be sufficiently mapped, and prefer to use this chapter to address issues that have not yet received sufficient attention and are thus a greater threat to the state.

[17] This trend is confirmed in the Report of the Public Prosecutor's Office for 2015 (in Czech only, http://www.nsz.cz/images/stories/PDF/Zpravy_o_cinnosti/2015/Zprava_o_cinnosti_SZ_za_rok_2015_-_textova_cast.pdf).

[18] In terms of the SS 2015, the following interests were considered – maintaining all the attributes of democratic rule of law, ensuring internal security and public protection, reducing crime with an emphasis on economic crime, organised crime, cybercrime, and corruption, increase the efficiency and professionalism of state institutions and the judiciary.

I) Penetration of Organised Crime into Public Administration and Law Enforcement Authorities

Threat relevance assessment for the CR: **High**

The infiltration of public administration structures and law enforcement authorities by organised criminal groups has a major negative impact on the functionality and efficiency of public administration and is concomitant to other threats listed below. A permanent problem is the appointment of officials influencing the work of public administration and the allocation of funds from a shortlist of pre-selected individuals who are also loyal to organised criminal groups. Even after persons actively contributing to dysfunctional practices of state authorities are ejected from the central or local public administration body, their influence continues over ordinary employees continues. It is evident in the obstruction of investigations by ordinary employees, some of whom are forced to participate in criminal activities under the threat of loss of employment, but some of whom do not participate in the criminal activities at all.

Some collaborators and members of organised criminal groups that have been removed from lucrative functions are employed in less visible positions with an influence over state or public administration (e.g. publicly owned entities), from where they can continue to carry out activities related to the illegal siphoning of funds from public budgets. At the same time, these people, influencers acting in favour of criminal organisations operating from a position in state or public administration, are remunerated with salaries that are in themselves well above the average. In less important positions in local administrations or in publicly owned entities, salaries are often beefed up by various consulting contracts, bonuses, etc. As regards the transparency of hiring procedures, meetings between members of the hiring board with candidates outside the hiring procedure are problematic, as they can be motivated by a desire to influence the hiring procedure.

Contacts between organised criminal groups and law enforcement authorities and supervisory state administration bodies also exist, as well as infiltration of organised criminal groups into the legislative process not just at the level of local authorities, but even at the governmental and parliamentary level. Organised criminal groups thus obtain access to non-public information. In the area of justice, there are suspicions of outcomes of criminal cases being influenced by circumventing the system of agenda allocation.

The hiring procedure as per Act No. 234/2014 Coll. on civil service, is considered problematic. The new legislation offers very limited possibilities of preventing undesirable persons (unless they have a criminal record) from applying for positions. At the same time, it limits the possibilities for hiring experts from the private sector and thus causes a *de facto* closure of the state administration, often making it problematic to fill vacancies. The situation is not helped by a very low motivation of civil servants, given by low salaries and a non-conceptual approach to human resources (or rather, the absence of any kind of concept) in the field of public administration. This situation benefits organised crime, for it makes it easier to acquire civil servants as collaborators in criminal activities.

II) Abuse of Public Procurement and Public Budgets

Threat relevance assessment for the CR: **High**

A very significant waste of budgetary resources caused by the activities of organised criminal groups is taking place in public procurement and public grants. Complicated systems of procurement, awarding grants, and public procurement associated with the absence of a consistent system of control and individual responsibility for specific decisions results in a situation where a number of projects are being manipulated in favour of organised criminal groups.

Organised criminal groups make attempts at managing public procurement from the very outset, with the purpose of siphoning financial resources into private hands. In practice, this takes place via purposeful division of public contracts into so-called sub-limit contracts, for which there is no need to issue a tender. Firms that are in league with each other repeatedly enrol into tenders, having previously arranged a substantial increase in their price offers. Organised criminal groups resort to the use of various intermediaries and, in exchange for bribes, obtain the desired information and support for their needs. In some cases, firms agree in advance as to which one will win the tender and which one will act as the backer. In order for all parties to be happy, the roles are reversed during the next tender. When another firm enrols in the tender, threatening to disrupt the pre-arranged choice, it is usually eliminated for formal reasons and trivial shortcomings. Proceedings to grant subsidies are similarly rigged.

The issue of individuals participating in a tender procedure for public procurement was repeatedly discussed in the past. The result of these discussions was the introduction of a new type of sensitive activity under Act No. 137/2006 Coll., on public procurement. The requirement for a certain level of integrity of persons contributing to important public procurement is also taken into account in the new Public Procurement Act – No. 134/2016 Coll.

III) Organised Tax Crime

Threat relevance assessment for the CR: **High**

Intensive organised crime activity threatens not only public spending as described in the previous section, but also public revenue, especially in the form of unpaid taxes (VAT and excise duty). Legally operating companies fabricate higher costs based on fictitious invoices gained from illegal entities and thus conceal actual profits. In so doing, they reduce their tax base and thus pay lower taxes than would be appropriate. The problem lies in the vague boundary between legal tax optimisation and tax evasion, which leads to the reality that VAT “cuts” have become a “normal” part of legal business. The very structure of VAT, its calculation and payment, is problematic. This is particularly true for those commodities that will continue to be of interest to organised criminal groups as regards VAT cuts. The gradual introduction of the reverse charge is succeeding in eliminating loopholes, although organised criminal groups are easily reverting to new types of traded goods (e.g. meat products).

One of the major problems in this area is the creation of organised company structures for the purpose of collecting residual VAT cuts (so-called carousel fraud). This phenomenon is sufficiently known and is therefore not detailed further.[19]

Because of this fraud, honest businesses are being destroyed in some areas of trading (fuels, electronics, and others). Due to the massive impact on these segments, honest businesses are unable to compete with their prices and are forced to leave the market. The situation is also complicated by the participation of foreigners as organisers and as straw men. These persons, equipped with false passports, moving easily and freely within Europe, are often used for single operations (founding a limited liability company or opening a bank account) and remain undetectable and untraceable in the context of uncovering criminal activity. Czech entities involved in fraudulent company chains routinely have bank accounts abroad, thus moving the money out of the tax administration’s reach while at the same time complicating consequent clarification in the course of criminal proceedings and ensuring proceeds from crime.

[19] In 2016, there has been an improvement in this area. Textile imports, where this illegal activity was most common, fell significantly. The Customs Administration succeeded in making Chinese customs authorities cooperate. At present, the Chinese have responded to the vast majority of requests for mutual administrative assistance. We cannot yet say that the problem would not continue to exist, but it is also very difficult to estimate its extent. The issue deserves to be analysed again.

Other important types of organised criminal activity include the evasion of customs duties when importing goods from outside the EU (especially from China, where the perpetrators are usually Vietnamese). The intensity of this activity has remained unchanged for the last few years. With the use of forged documents, the value of goods is artificially reduced upon their entering the EU, resulting in significantly lower customs duties (the so-called 4200 customs regime is abused, where the goods are released in another EU member state with a possible determination in the CR). The so-called "Customs Service"[20] remains a key actor in these techniques. The main problem is the absence of the possibility to independently verify the authenticity of the accompanying documents for imported goods, which are presented during customs procedures. The relevant Chinese authorities usually boycott requests for cooperation in verifying the authenticity of accompanying documents for goods exported from China, or only feign cooperation. In some cases, cooperation with relevant authorities in neighbouring countries is also unsatisfactory.

This area also includes the illegal operation of lotteries and other similar gaming facilities, where the aim is primarily to avoid tax obligations imposed on operators legally operating lotteries and other similar games. Notably, the illegal operation of these activities on the internet, the operation of so-called quiz machines and technical gaming devices operated illegally under the auspices of associations or trust funds. Given the scale of these activities, they are usually operated by organised criminal groups. As of 1 July 2016, the Gambling Cobra was established for combating this type of crime, comprised of representatives of the Police CR, the Customs Administration of the CR and the Financial Administration. The successful functioning of the Tax Cobra was the inspiration for its creation.

IV) Legalisation of Proceeds from Crime

Threat relevance assessment for the CR: **Medium**

The activities of organised criminal groups generate huge profits, which their members naturally try to use to their advantage and, if possible, legalise by investing in legitimate assets (corporations or real estate). A major problem in the area is the creation of highly sophisticated corporate structures with the aim of legalising proceeds from crime. It is a crime with a high level of legal erudition. Groups of companies are founded under Czech law, but also under international laws, and reside in many countries, especially in offshore destinations. The common denominator of these foreign destinations is a high degree of privacy protection, or a total lack of cooperation with foreign law enforcement authorities. In some cases, these groups may feign real business activity by creating business contracts, issuing invoices, etc. The purpose of these business relations is, however, entirely fictitious, and it is often difficult to prove that the services have been rendered (advertising, consulting). The purpose of these groups is to carry out a large number of interbank transfers, making it impossible to track the flow of money while at the same time returning the money to the person who inserted it into the system as legitimate income. The payments received in return for laundering money constitute the proceeds from this criminal activity. Law firms are often the perpetrators, and their headquarters are used as company headquarters with the purpose of complicating the work of law enforcement authorities, referring to professional secrecy observed by lawyers.

[20] This illegal service ensures transportation of goods and supplies false documents artificially reducing their value. It also handles all the necessary permits and ensures smooth customs clearance. The companies that are required to fulfil their tax and customs duties are often fictitious or purposefully founded, are seated outside the CR and do not make the mandatory payments.

V) The Misuse of Legitimate Services for the Purposes of Organised Crime

Threat relevance assessment for the CR: **Medium**

Organised criminal groups routinely use various services that are in themselves legal. Their illegal aspect does not stem from the nature of the rendered services, but from the purpose for which they are used (e.g. the transport of drugs via the postal service, the transfer of stolen money to a bank account). In particular, the services of financial institutions, telecommunications service providers, and tax, legal and financial consultants are misused, as well as new technologies and means of payment available to all citizens.

The domination or the establishment of financial institutions (e.g. credit unions) by organised criminal groups can follow two basic objectives – legalise proceeds from crime through legal business on the financial market and tunnel the resources of those saving money, i.e. the credit unions as such. These activities are facilitated by the lower requirements for the establishment and functioning of credit unions and lower levels of supervisions of their activities by the competent authorities. The perpetrators of this crime are usually organised criminal groups that operate in the area of legal business while at the same time navigating the area of the grey economy or of the underworld. The dominated financial institution does not report suspicious activity and does not cooperate with state authorities. Supervision of financial flows is obstructed and the organised criminal group gains control over police requests. International money transfer services are also misused (e.g. Western Union) – illegally obtained financial means are transferred through them in cash to practically untraceable subjects abroad.

Legitimate privileges and instruments making business or the lives of citizens easier are used to the benefit of illegal structures in the following cases, *inter alia*:

- The unlimited creation of companies by one person (organised criminal groups use straw men)
- The high limit for cash payments and withdrawals[21] (prompt transfer of large amounts of illegitimately obtained money)
- The possibility to establish headquarters in Office Houses (remaining unreachable)
- The possibility to use anonymous prepaid payment cards (unidentifiable transactions)
- The use of virtual currency (unidentifiable initiators of a transaction)
- The use of trust funds (siphoning criminal assets)

A case where an organised criminal group purchased a telecommunications services provider for the purpose of creating a closed group of callers was also recorded. The operator provided clients with alerts when there were queries by law enforcement authorities. What is also problematic is the placement of electronic data in data storage facilities outside company headquarters, often on servers abroad, and the use of international telecommunications services based abroad (Facebook, WhatsApp, Gmail, etc.).

Similarly to the previous case, the misuse of legitimate services and privileges does not constitute a new threat, but “merely” helps to successfully commit organised criminal activity.

[21] At present CZK 270 000.

VI) Crime Linked to Insolvency Proceedings

Threat relevance assessment for the CR: **Low**

Since 2014, an increase in fraudulent insolvency proposals has been recorded. These proposals usually combine three factors – the submission of an insolvency proposal at a court not locally relevant, the use of procedural regulations to obstruct the insolvency proceedings, and a dubious debt supported by a service contract, loan, or promissory note. These proposals are abused as part of the competition between businesses and serve as a means for the illegal enrichment of petitioners or their backers. Foreigners (Poles and Hungarians) are often the executives of firms founded specifically for the purpose of submitting insolvency proposals, and these people are usually impossible to track. The insolvency proposals are usually very well handled professionally, suggesting that offenders have good legal services and that the activities are those of organised criminal groups.

Another problem with current insolvency proceedings is the possibility of collusion of an insolvency judge or administrator with some of the parties to the proceedings and the consequent purposeful granting of advantages to these parties, to the disadvantage of others.

Due to the existence of an amendment to the Insolvency Act,[22] which aims to limit manipulative insolvency proposals, introduce greater oversight of insolvency administrators and strengthen the transparency of the entire process, the relevance of this threat is assessed as low.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

As per Act No. 2/1969 Coll., on competencies, organised crime falls within the scope of the MoI, with law enforcement authorities involved in actively combating it. Other ministries, their subsidiary organs, and other state bodies are involved in the fight against organised crime in varying degrees, particularly the MF (Financial Administration of the CR, Customs Administration of the CR, Financial Analytical Unit), the MJ (criminal legislation), and the Office of the Government of the CR (area of drugs and corruption). The Police CR has is the main force fighting organised crime in the CR, particularly the National Centre against Organised Crime and the National Drug Squad of the Criminal Police and Investigation Service. Simpler cases are handled by individual regional police directorates of the Criminal Police and Investigation Service. An important part is also played by intelligence services, which contribute to the issues within their competencies and transmit findings to the Police CR in accordance with Act No. 153/1994 Coll.

In 2014, a specialised team – the Tax Cobra – was created with the participation of the Unit for Combating Corruption and Financial Crime of the Criminal Police and Investigation Service (now the National Centre against Organised Crime), the General Financial Directorate, and the General Customs Directorate. The Tax Cobra deals with complex cases of tax evasion and tax crime, especially in the field of VAT and excise duties. In 2016, the competencies of the Customs Administration CR in criminal proceedings were expanded, with relevant customs authorities now having the power to investigate crimes involving VAT evasion.

Organised criminal groups use legislative loopholes in areas that fall within their scope of interest (public procurement, insolvency proceedings, business corporations, public spending, etc.) to their

[22] Parliamentary Press No. 785, debated at the end of September 2016 during a second reading in the Chamber of Deputies.

advantage. Good laws regulating these processes and their oversight are one of the best weapons against the activities of organised criminal groups.

A generally accepted instrument in the fight against organised crime is criminal and related legislation (Act No. 40/2009 Coll., Criminal Code,[23] Act No. 273/2008 Coll., on Police CR, Act No. 141/1961 Coll., Criminal Procedure Code, Act No. 418/2011 Coll., on criminal liability of legal persons,[24] and other related regulations). This area is stable in the long-term, although minor shortcomings do exist – see proposals for measures below.

The main strategic document in this area is the **Strategy to Fight Organised Crime for the Years 2015 – 2017**,[25] which was approved by Government Resolution No. 919 on 12 November 2014. This strategy contains the evaluation of tasks from the previous strategy, an overview of the situation in the area of organised crime, and 12 specific tasks in the area of monitoring, developing systemic tools, and strengthening international cooperation. Other strategic documents also address the topic (**SS 2015,**[26] **the National Drug Policy Strategy for the Years 2010 – 2018,**[27] **the Government Strategy for Combating corruption for the Years 2015 – 2017,**[28] **the National Strategy against Trafficking in Human Beings in the CR for the Years 2012 – 2015**,[29] and others). We can say, therefore, that from a strategic perspective, the issue is treated sufficiently.

C. SWOT Analysis

All categories are sorted by relevance.

Strengths

- A peaceful security situation in the CR without any serious incidents requiring a significant deployment of security forces.
- A stable state of criminal legislation.
- A good ability of law enforcement authorities to tackle traditional forms of organised crime.
- Membership of the CR in transnational democratic institutions and the associated adoption of measures (especially in the area of legalisation of proceeds from crime).
- International cooperation within the EU (Europol, Joint Investigation Teams, ISs)
- Sufficient long-term strategic oversight of the topic.
- The Tax Cobra is an example of efficient cooperation between authorities that does not require changes in legislation or increase in funding.

[23] See footnote No. 14.

[24] The act was amended in 2016 (No. 183/2016 Coll.), with the former positive list of offenses that may be attributed to a legal person being changed to a negative list, excluding only specific crimes for which a legal person may not be prosecuted. The criminal liability of legal persons has thus been effectively expanded.

[25] http://www.mvcr.cz/soubor/koncepce-boje-proti-organizovanemu-zlocinu-na-obdobi-let-2015-2017.aspx

[26] http://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

[27] http://www.vlada.cz/assets/ppov/protidrogova-politika/strategie_web.pdf

[28] http://www.korupce.cz/assets/protikorupcni-strategie-vlady/na-leta-2015-2017/Vladni-koncepce-boje-s-korupci-na-leta-2015-az-2017.pdf

[29] http://www.mvcr.cz/soubor/material-obchod-s-lidmi-pdf.aspx

Weaknesses

- Insufficient resilience of the state administration against infiltration of criminal subjects in relation to the Act on Civil Service.
- Some minor legislative shortcomings (telecommunications traffic data retention, slow preparation of the new Criminal Procedure Code).
- The high administrative burden of police officers.
- Insufficient staffing, material, and legislative preparedness in the area of cybersecurity (including adequate remuneration of experts).
- A lack of experts in the field of tax investigation and uncovering serious economic crime; inadequate police training in the area.
- Poor international cooperation with geographically and culturally remote countries (Vietnam, China, tax havens).
- The inability to monitor the movement of persons and goods within the Schengen area.
- The absence of a uniform and recognised definition of organised crime.

Opportunities

- New upcoming legislation (Act on Conflict of Interests, Register of Contracts, Electronic Register of Sales, new Act on Public Procurement, Act on Proving Origin of Assets, Central Register of Accounts).
- A significant decline in registered crime makes it possible to dedicate more resources to the fight against organised crime.
- The Strategy on Police Development by 2020 – the development of a strategic framework for the medium term.[30]
- The approved increase in the number of police officers.
- The development of financial investigation as part of the work of the Police CR.
- A wider use of security research.
- The expansion teams modelled on the Tax Cobra into other areas.

Threats

- New upcoming legislation (Act on Conflict of Interests, Register of Contracts, Electronic Register of Sales, new Act on Public Procurement, Act on Proving Origin of Assets, Central Register of Accounts) – particularly its improper implementation.[31]
- The transition of organised crime to more sophisticated criminal activities.
- The risks arising from the current migration crisis (including inappropriate visa liberalisation).

[30] This document has undergone an intraministerial amendment procedure, was discussed by the Committee on Security of the Parliament of the CR and is being prepared to undergo an interministerial amendment procedure.
[31] This point is deliberately listed as both an opportunity and a threat – see below.

- The transition of criminal activities into cyberspace, making detection more difficult.
- The participation of former members of security forces in the activities of organised criminal groups.

D. Recommendations to Strengthen Resilience

The recommendations in this chapter are based on the identified opportunities and aim to limit the impacts of potential threats. It should be noted that a significant number of mainly legislative measures is currently being adopted or proposed (see Opportunities in section C or the documents listed in section B of this chapter). Given that the final wording of some laws is not yet known and their efficiency will depend on the manner of their implementation, it is impossible to assess the contribution of individual new proposals and laws at the moment. New laws can produce either a significant improvement, or a significant deterioration of the *status quo*.

The measures proposed in Legislative Proposals in the Field of Internal Security are highly necessary, especially those on the retention of telecommunications traffic data, the use of intelligence as evidence in criminal proceedings, and expanding controls of transborder cash transfers. Similarly, the adoption and appropriate implementation of the Strategy on the Development of the Police by 2020 will ensure adequate conditions for long-term development and strengthen the capacities in the fight against organised crime of this key security force.

Other Proposed Measures:

1. Improve the capacities (staff, expert, material, and technological) of law enforcement authorities to tackle cybercrime, obtain information from secured electronic communications, forensically investigate modern communication devices, and share necessary data within ISs. Adequate training and sufficiently motivating salaries need to be ensured for experts in the area.
2. Strengthen teams investigating serious economic crime, because this type of criminal activity is the source of the highest financial losses of the state. Investment in this area will provide multiple returns in the form of protected assets. Adequate training and sufficiently motivating salaries need to be ensured for experts in the area. In the area of crime associated with public procurement and granting subsidies, the ability of the Police CR to actively detect such criminal activity needs to be increased.
3. Review criminal legislation; in particular, adopt a comprehensive new Criminal Procedure Code, which will also respond to current developments in the area of modern technologies (ICTs, cybercrime, virtual currency). In addition, evaluate the efficiency and adequacy of measures proposed in the Act on Police CR.
4. Deepen trust, contacts, and possibilities for sharing information between intelligence services and the Police CR, so as to promote more frequent cooperation in the fight against organised crime, including the forwarding of information that may be useful for all parties.
5. Organised joint training sessions for representatives of law enforcement authorities on new trends in organised crime and possibilities for prosecution.
6. Expand the availability and interconnection of statistical data in the area of organised crime.

7. In the area of customs and tax evasions, re-introduce the obligation to collect VAT from taxpayers when goods are released into free circulation. The CR is one of the few countries that do not impose this obligation on importers.
8. Consider an amendment to Act No. 234/2014 Coll., on civil service, allowing greater openness of state administration to experts from the private sector, simplifying tendering, and adding safeguards against the infiltration of organised crime into state administration.

INFLUENCE OF FOREIGN POWERS

A. Description and Assessment of the Threat and Associated Risks for the CR

1. Introduction

The influence of foreign powers is not unknown to any sovereign state; the reasons for foreign powers' efforts to obtain information and exert influence in another state range from economic significance and clout in matters of international relations to historical aspects of defunct and newly established spheres of influence. It is not limited to hostile members of the international community; nevertheless for the purposes of this Audit it is necessary to pay primary attention to those manifestations of foreign powers that may pose a threat to the CR. In accordance with current knowledge arising from information provided by intelligence services as well as other sources, such manifestations would be those exercised by the Russian Federation, the People's Republic of China, and some other non-state actors such as the so-called Islamic State.

A traditional and continuously monitored attempt at influence of a foreign power is observed in the economic field, whether it is gathering information on economic activities of entities outside the state structure or influencing strategic economic decisions at the level of state leadership, as well as all other forms of espionage (in the sense of the gathering of sensitive information by foreign intelligence services) that are not economically motivated.

An old-new manifestation of the influence of foreign powers is the dissemination of propaganda and disinformation as a means of information warfare, via which foreign powers attempt to influence the state in the area of managing and using ICT channels or technologies to influence public opinion. Alongside the risks of the influence of foreign powers in the economic field, where an insufficient response to the activities of a foreign power may lead to consequences of varying severity – from economically disadvantageous situations and the weakening of the economic position of the state, to the creation of an excessive reliance on a specific investor, i.e. the foreign power, to the loss of economic independence of the state for reasons of insufficient diversification of resources, investment structures, or energy independence[32] – exacerbated political propaganda is again gaining ground, which tests the resilience of the public against influence, but also significantly influences the opinions and actions of responsible persons at all levels of the state decision-making process. Current propaganda of foreign powers focuses primarily on **disinformation campaigns** and its methods do not include the promotion of a specific world-view, ideology, or way of life, but rather the relativisation and fractioning of information, disrupting the structure of internal social trust. For this reason, the term propaganda is perceived as outdated, and the term disinformation campaign is used instead to designate this specific manifestation of the influence of foreign powers. Such a campaign, as a manifestation of information warfare, falls within hybrid threats, which are further discussed in the overarching chapter, and thus constitutes one of the most serious threats especially with regards to informational openness of democratic societies and the very limited possibilities of the state, founded on the principle of rule of law, to respond to such a situation.

[32] This topic is addressed in more detail in the chapter "Energy, Raw Material, and Industrial Security".

The topic of disinformation campaigns is closely related to media law, namely the field of regulation of media ownership structures in the state and the possibility of reviewing the lawfulness of media content. A separate chapter is dedicated to the topic of new media (news on the internet, social media etc.).

2. Classification of risks, threats, and their consequences

Factors posing a risk for the CR in the area of influence of foreign powers are classified into **risks coming from the outside (external factors) and internal weaknesses (internal factors).**

External factors include:

- **Targeted efforts of foreign powers to**
    - Influence public opinion in the CR (especially as regards undermining confidence in an independent democratic state ruled by law) contrary to Czech interests

      This effort is carried out by all available means, especially targeted work with information, support of traditional animosities within society, stirring up critical sentiments towards the establishment and integration structures, or the use of negative attitudes of a part of the public towards supranational entities of which the CR is a member, and allies. These methods are used to invoke the idea within society that the state is badly governed, that its focus on Euro-Atlantic integration structures is detrimental, etc.
    - Influence public administration and political representatives

      As per the annual reports of the SIS, both Russian and Chinese intelligence services are building networks of access and influence among representatives of parliamentary political parties, Government officials, and lobbyists.
    - Influence the behaviour of the state via economic instruments

      Strengthening the presence of foreign powers by gradually gaining influence in certain economic sectors.
    - Acquire lawfully classified or otherwise publicly inaccessible information whose acquisition may lead to endangering or damaging state interests

External factors also include the following, whose nature is often **mixed**:

- **Foreign communities** forming the backdrop for activities of foreign powers.[33]

In the CR, the activities of several groups based on membership in a minority, whose official business is conducted as commercial, cultural, scientific, or religious, but which often act as organisers of events in support of opinions that would not stand in a democratic debate, or of visits of cultural and political representatives of non-democratic regimes, are observed; there is also suspicion that these groups may finance or facilitate financing of activities that are contrary to Czech interests.

[33] This topic is partially discussed in the chapter on Terrorism.

- **Concentration of media ownership within foreign subjects and among a limited number of people.**
- **The existence of a relatively large number of media and quasi-media projects in Czech or in Slovak** with a proxy agenda, influencing Czech society.

Internal factors in the area of influence of foreign powers are identified as:

- **Weak resilience of the public against influence and attempts at reducing confidence in democratic rule of law** – inadequate or absent civic and media literacy.
- **Weak resilience of public administration and political representatives against influence and obtention of information, including cybernetic resilience.**
- **Activities of political entities and political representatives openly promoting interests contrary to those of the CR.**
- **Activities of former high political representatives defending interests contrary to those of the CR.**
- **Activities of economic entities defending interests contrary to those of the CR.**
- **The absence of systemic tools of the state enabling it to protect itself against disinformation campaigns.**
- **Insufficient ability to motivate foreign communities in favour of Czech interests.**

Consequently, **these threats** can be classified into **three categories** in an environment where the described factors operate in varying degrees of interconnectedness and in varying intensity. Their **consequences, of which some have already been recorded in the CR**, can also be specified.

I) Influencing Public Opinion

Threat relevance assessment for the CR: **High**

- Targeted undermining of confidence in an independent democratic state ruled by law and building sympathies to the interests of foreign powers.
- Disseminating disinformation via media and quasi-media platforms, including social networks, “independent” NGOs, and public figures, including political representatives who are under the influence of or promote interests contrary to those of the CR.
- Using media with concentrated ownership to enforce power interests.
- Encouraging hostile attitudes towards the CR within foreign communities and their engagement in activities contrary to Czech interests.

Consequence – Radicalisation of the Public[34]

- The rise of extremist and anti-system attitudes (threatening Czech interests) within society and among political representatives.

[34] This topic is further discussed in the chapters on Terrorism and on Extremism.

- An increase in support for extremist and anti-system parties and movements, their higher representation in Parliament and representative bodies of local governments.
- A decline in support for the CR's constitutional establishment and its integration in Euro-Atlantic structures, increased support for their revision.
- The decrease in public trust in the ability of the state to ensure vital national interests (SS 2015) (political independence of the CR, maintaining all the prerequisites of democratic rule of law, including the protection of basic human rights and freedoms of citizens) and strategic national interests (ensuring internal security and protection of citizens).
- The radicalisation of minorities contrary to Czech interests.
- Disruption of public order and security as a result of incidents during public gatherings, arming and civil unrest.

II) Influencing Decision-Making at all Levels of Public Administration Contrary to the Interests of the CR

Threat relevance assessment for the CR: **High**

- Influencing public administration officials.
- Influencing political and constitutional representatives, both incumbent and former high representatives of the state via informal channels. Political representatives of the opposition are not overlooked, seen as having future potential.

Consequence – Adoption of Decisions Harming Czech Interests

- A weakening of the credibility and the Czech negotiating position in relation to allies and partners.
- Damage to strategic national interests (SS 2015): enhancing coherence and effectiveness of NATO and EU and maintaining functional and reliable transatlantic ties.
- Potential threats to vital national interests (SS 2015): political independence of the CR.

III) Obtention of Lawfully Classified or Otherwise Publicly Inaccessible Information whose Acquisition May Lead to Endangering or Damaging National Interests

Threat relevance assessment for the CR: **Medium**

Consequence – **Information Leaks** that May Endanger the Security, Political, and Economic Interests of the CR

The following criteria were chosen to evaluate threats, i.e. assess their severity:

- **The severity of threats in relation to the seriousness of the interest of the target of the threat** (classification of interests pursuant to the SS 2015 – vital, strategic, otherwise important)
- **The speed and intensity of the onset of the consequences of the threat** (measurable in some categories based on public opinion polls, phenomena described in the CR based on documented experience from abroad *et al.*)

From the perspective of protected interests listed in the SS 2015 (criterion No. 1), all three of the defined threats target interests defined as vital by the SS 2015. The protection of these interests is perceived by the strategy as a basic obligation of the Government and all public administration bodies. The CR is prepared to employ all legitimate approaches and all available instruments for their security and protection. The threat of **influencing public opinion** targets primarily the following vital interests: ensuring political independence of the CR, maintaining all aspects of democratic rule of law, including the guarantee and protection of basic human rights and freedoms of citizens.

Of course, this threat poses a serious risk for a number of other interests that the SS 2015 defines as strategic. The threat is observed as a serious risk for:

- Enhancing the coherence and efficiency of NATO and EU and maintaining functional and reliable transatlantic ties
- Fulfilling the strategic partnership between NATO and EU, including strengthening their cooperation in the complementary development of defence and security capabilities
- Supporting democracy, basic freedoms, and principles of rule of law
- Ensuring internal security and civil protection
- Ensuring economic security and strengthening economic competitiveness
- Ensuring energy, resource, and food security and an adequate strategic reserves
- Preventing and suppressing security threats affecting the security of the CR and its allies

Influencing decision-making at all levels of public administration contrary to the interests of the CR was assessed as a threat targeted primarily at strategic interests (beyond those enumerated above, these include ensuring cybernetic security and defence of the CR), while after long-term exposure or the outbreak of the threat in a number of high representatives of the state, or in case of the electoral success of a political entity that is perhaps even latently under foreign influence, this threat may also seriously target vital interests. It is, however, possible that even in the case where one political representative of the state – be it a highly placed one – will be influenced, it will be a matter of influencing their individual decisions falling within their specific competencies, and not a matter of influencing strategic decisions taken at the collective level. Nevertheless, it is important to bear in mind that certain individuals are of key importance to national security, in terms of their significant clout e.g. with regards to the armed forces. This threat may, of course, significantly affect the vast majority of interests defined by the SS 2015 as otherwise important.

Within the trio of defined threats, the **obtention of sensitive or lawfully classified information** targets, in the vast majority of cases, interests defined as otherwise important, and to a lesser extent those defined as strategic. It is important to bear in mind that this threat is both a means and a tool enabling the endangering of vital interests, since the constant collection of information from the environment which the foreign power wants to influence constitutes a means of influencing the public as well as political representatives.

Criterion No. 2, relating to the **speed and intensity of the onset of the consequences of the threat**, is difficult to measure. Nevertheless, in a situation where the general criterion for assessing a threat, i.e. the probability of its occurrence, is meaningless, since all three threats are already present in the CR, it is necessary to select another criterion. In the case of influencing public opinion, some guidance could be provided by targeted and repeated public opinion polls, which have however not yet been carried out in the CR in detail.[35] (Opinion polls in the CR[36] regarding undemocratic governance alternatives do not show any major fluctuations of public opinion in recent years, in terms of support for such a development or in its perception as a threat. On the other hand, the first targeted survey showed a high degree of reliance on alternative sources of information and a propensity of the public to consider distorted information to be true.) This criterion can be processed analytically based on research that has already been carried out regarding attempts at influencing in other countries (e.g. the Lisa case in Germany or disinformation disseminated prior to the referendum in the Netherlands, *et al.*). Likewise, in the case of the two other threats, the identification of the speed and intensity of the onset of their consequences would suppose an evaluation of a number of individual attacks and an assessment of whether their unifying purpose is the influence of foreign powers in the form of a so-called hybrid campaign.[37]

In evaluating the threats in this chapter, it is particularly important to remember that, while foreign powers are continuously active in the CR in all three of the defined threat areas, a clear increase in activity is currently observed.

In conclusion, it is necessary to draw attention to the fact that, when facing threats, a democratic society must never use undemocratic means; this is both its weakness and its greatest strength. It does not mean, however, that it must rely solely on existing elements of the security system and cannot consider strengthening its resilience; the current deteriorating security situation is an opportunity for this, providing higher understanding for the security aspect when assessing changes to the system and its overall increased vigilance. Every measure, nevertheless, must undergo a thorough test of proportionality and must be subject to open public debate.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

In the area of prevention and combating threats discussed in this chapter, there is currently no one institution invested with the bulk of responsibility, which is why the list needs to begin with a description of the role of the Government and continue with an analysis of the more or less dispersed tools and competencies of individual institutions.

The Government of the CR

The general and overarching role of the Government in preventing and combating security threats arising from the influence of foreign powers stems from its constitutional position as the supreme executive organ (Sec. 67 (1) of the Constitution). In this respect, the Government manages,

[35] The first targeted survey was conducted in September 2016, when Agentura STEM carried out a survey on a representative sample of 1 061 respondents. It tested the extent to which the public believes disinformation disseminated by pro-Kremlin, so-called “alternative”, media. The survey showed that 25.5% Czechs believe disinformation and 24.5% believe alternative (disinformation) media more than traditional media; 50.2% of Czechs think that the USA are responsible for the hundreds of thousands of Syrian refugees flocking to Europe; 28.3% Czechs think that Russia’s military intervention in Syria is helping solve the European migration crisis; only 31.5% respondents consider EU membership a good thing.
If a referendum on the withdrawal of the CR from the EU were to be help, 40.6% of the population would most probably decide based on a campaign preceding the referendum. http://www.evropskehodnoty.cz/wp-content/uploads/2016/09/Dopady-dezinforma%C4%8Dn%C3%ADch-operac%C3%AD-v-%C4%8Cesk%C3%A9-republice.pdf.

[36] http://cvvm.soc.cas.cz/media/com_form2content/documents/c1/a7529/f3/pd160324.pdf.

[37] The subject of a unifying intention of a campaign is further discussed in the overarching chapter on Hybrid Threats.

controls, and unifies the activities of ministries (Sec. 28 (1) of Act No. 2/1969 Coll., on the establishment of ministries and other public administration bodies), which have specialised competencies defined by the Competencies Act.

The special role of the Government is based on its role as coordinator of intelligence services, for whose activities it is responsible and to whom it assigns tasks within their scope of competencies. The authority to assign tasks to intelligence services is also granted to the President (Sec. 7 and 8 (4) of Act No. 153/1994 Coll., on intelligence services of the CR).

Intelligence Services

Due to the nature of the threats in question, intelligence services play an important role in gathering, collecting, and evaluating information across the wide spectrum of foreign power activities, including, of course, procuring information on the originators of propaganda hostile to Czech interests and on other circumstances and phenomena related to its dissemination and penetration.

The basic method of intelligence services is to gathering and evaluating information, for which purpose relevant legislation defines tools for gathering information; these, with regards to the growing number of and new threats, need to be modified and adapted to a new security environment, as well as the capacities and resources for their implementation.

Strategic documents and legislation:

Act No. 153/1994 Coll., on intelligence services of the CR,

Act No. 154/1994 Coll., on the SIS,

Act No. 289/2005 Coll., on MInt.

The Ministry of the Interior

The role of the MoI is currently fragmented into unconnected segments of internal affairs administration whose influence in the area of foreign power influence is always limited. These segments include: internal order and security, including the analysis of development rends, assembly law, registration of political entities, issues of foreigner and residency policies, granting citizenship, HR issues related to the exercise of civil service, and a number of others. An important role within the ministry is played by the Police CR, especially in the event that one of the manifestations of foreign power influence attains the intensity of a crime.[38]

The set of tools in all relevant areas falling within MoI competency was not, in the past, constructed or systematically assessed for the possibility of averting the threat of foreign power influence as a form of hybrid attack conducted with the unifying aim of a foreign power.[39] The initial assessment, which was elaborated within the scope of this chapter, did not register, save for a few exceptions, significant legislative shortcomings in criminal law (see Recommendations) in relation to available tools; rather, it identified a significant lack of comprehensive assessments of problematic findings and in the coordination of activities leading to their resolution.

[38] These manifestations can fulfil a wide range of constituent elements of a crime, from traditional espionage, to crimes related to the protection of trade secrets, conveyed messages and privacy, to spreading alarming information and various types of crimes disrupting human coexistence and crimes against humanity, peace, and war crimes.

[39] More in the chapter on Hybrid Threats.

Strategic documents and legislation:

The state has conceptual documents for individual areas within MoI competency; however, these documents do not include an evaluation of the topics in terms of threats from foreign powers, nor do they evaluate the efficiency of existing tools in combating the identified threats.

Likewise, existing legislation adequately covers all sectors, including adjustment of sanction and other tools that may be applied when combating threats.

National Security Authority

The role of the NSA in the area of tackling hybrid threats and the influence of foreign powers in the CR is primarily to ensure cybersecurity and to increase the resilience of the Czech IT infrastructure (especially its critical part[40]) against cyberattacks. Apart from cybersecurity, the NSA makes decisions primarily on the issue and revocation of certificates of safety reliability to physical and legal persons and carries out tasks in the area of protection of classified information; these are important activities in combating the influence of foreign powers and hybrid threats.

Strategic and other documents:

The National Cybersecurity Strategy 2015-2020

The Action Plan to the National Cybersecurity Strategy CR 2015-2020

The Memorandum of Understanding in the area of Cybernetic Defence Cooperation between NATO and CR

Legislation:

Act No. 181/2014 Coll., on cybersecurity and the amendment to related acts (cybersecurity act)[41] and Act No. 412/2005 Coll., on the protection of classified information and on security competencies, as amended.

The Ministry of Foreign Affairs

The MFA is the central Government authority responsible for foreign policy; it ensures the CR's relations with other states, international organisations, and integration groups. The MFA issues permanent residency permits to staff members of embassies of foreign states or international Governmental organisations accredited for the CR, or their family members registered with the MFA, and declares these invalid. Through Czech embassies, the MFA grants diplomatic and special visas and has the right to declare these invalid. Pursuant to the Vienna Convention, the receiving state may at any time and without obligation to give reasons for its decision notify the sending state that the head of its mission or any other staff member of the mission is *persona non grata* or that any other member of the mission is not acceptable..

Strategic documents and legislation:

SS 2015

The Foreign Policy Strategy 2015

[40] Critical Information Infrastructure (CII) and Important Information Systems (IIS).

[41] Decree No. 316/2014 Coll., on security measures, cybersecurity incidents, reactive measures and on establishing requirements for submitting cybersecurity incidents (so-called cybersecurity decree). Decree No. 317/2014 Coll., on important information systems and their defining criteria.

Act No. 326/1999 Coll., on the residency of foreigners in the CR and the amendment to some other acts, as amended.

The Vienna Convention on Diplomatic Relations (MFA Decree No. 157/1964 Coll.)

The Ministry of Culture

The MC is responsible for legislation; the tools for regulating the content of radio and television broadcasting are in the hands of an independent authority – the Council for Radio and Television Broadcasting – which carries out legal competencies in relation to audiovisual media upon request. The legislation provides a procedure for granting licences for broadcasting. Within the procedure for awarding licences for the operation of analogue radio broadcasting, it is the Council that is responsible for evaluating the transparency of ownership structures within the applicant company, and may employ a range of other tools. The legislation contained in the press act is based on a liberal approach – based on Article 17 of the Charter of Basic Rights and Freedoms – demanding only evidence of periodical prints, to be submitted to the MC. It states that the content of printed media is the responsibility of its publisher, who is in this regard bound only by general laws.

Legislation:

Act No. 231/2001 Coll., on radio and television broadcasting and on amendments to other acts, as amended.

Act No. 132/2010 Coll., on on-demand audiovisual media services and on amendments to other acts (on-demand audiovisual media services act).

Act No. 46/2000 Coll., on the rights and obligations of publishing periodical press and on amending certain other acts (press act), as amended.

The Ministry of Education, Youth, and Sports

Among the instruments with a significant efficacy in combating foreign power influence, especially as regards the impact of disinformation campaigns and undermining confidence in the democratic rule of law and building sympathies to the interests of foreign powers, is that of education in civic and media literacy. The importance of these tools must be stressed throughout the entire education system. Instruments available to the MEYS should be used for this purpose, in accordance with the education act, in particular when creating curricula.

Legislation:

Act No. 561/2004 Coll., on elementary, primary, secondary, higher, higher professional, and other education.

C. SWOT Analysis

Strengths

- A stable democratic constitutional and political establishment; a functioning state, economic stability; low unemployment and the resultant relative satisfaction of the public with the quality of life.
- The CR’s membership in European and Euro-Atlantic integration structures.

- Long-term monitoring of the situation in the area of influence of foreign powers by the intelligence services.
- Satisfactory international cooperation and exchange of information within the security community.
- Robust public media, institutionally independent of the state power.
- Developed activities of the non-profit, journalistic, and academic sectors in the area of uncovering disinformation of foreign powers.
- The disunity of foreign diasporas in the CR.

Weaknesses

- Underestimation of the threat of the influence of foreign powers to the detriment of other threats.
- The absence of a unified position on the threat across the political spectrum.
- An ambiguous attitude of the public towards the perception of the existence and significance of the threat.
- The necessity to defend guaranteed rights and freedoms (e.g. freedom of speech *et al.*) and democratic principles of applying state power in combating the threat, and the associated limited possibility of a state response.
- Weak public resilience to influence and attempts at reducing confidence in the democratic rule of law via disinformation campaigns.
- An insufficient capability of the state to ensure quality education in the area of civic and media literacy.
- Weak resilience of public administration and political representatives to influence and obtention of information; cases of conscious and unconscious cooperation.
- Inadequate screening of contractors and subcontractors of ICTs and ICT products (software and hardware) in important national security institutions.
- Poorly set cybersecurity policies in important national security institutions and the underestimation of employee education in the area of cybersecurity.
- Limited financial resources of important national security institutions allocated for the prevention and tackling of cyberthreats or for the adequate remuneration of ICT specialists.
- Insufficient ability to motivate foreign communities in favour of Czech interests.
- The amendment to Act No. 106/1999 Coll., on free access to information, allowing for a rather wide publication of information relating to national security.
- Inadequate options of the media regulator to ensure information necessary for the implementation of existing authorisations.
- The absence of strategic communication of the state as a reaction to disinformation and in order to strengthen its own credibility.
- The inability of the state to quickly evaluate the significance of specific cases of disinformation and failure to elaborate a prompt response.

Opportunities

- A relatively clear identification of the intentions of foreign powers, the ability to analyse previous attempts at influence abroad and the responses made by partner countries.
- The increased attention paid to this issue in other EU member states and within European structures (e.g. the EEAS StratCom Team), the possibility to engage in joint initiatives and participate in the search for common solutions.
- The opportunity to benefit from specific experiences of several states that have recently set up new systemic measures against the influence of foreign powers.
- An interest in addressing the threat both by the state and the non-governmental and academic sector – synergies in adopted measures.
- Historical experience of the public with the influence of a foreign power.

Threats

- The influencing of public opinion to the detriment of democratic rule of law or in favour of a foreign power.
- The failure of the system of detection of the activities of a foreign power.
- Severe damage of the credibility of an important democratic institution (Czech TV, Police CR, *et al.*).
- The emergence of a widespread Czech-language media outlet promoting the interests of a foreign power different to those of the CR.
- The growth in importance/the share of power of anti-systemic, extremis, and otherwise radical groups weakening the democratic system.
- The success of political groups promoting interests different from those of the CR in the elections.
- The existence of paramilitary groups enjoying direct or indirect support of a foreign power.
- Influence of decision-making at all levels of public administration contrary to Czech interests.
- Activities of entities with a significant participation in the executive, legislative, and judicial powers.
- Activities of individual representatives with a significant influence on decision-making in the area of security.
- Activities of political entities and political representatives promoting interests contrary to those of the CR.
- A scenario where the political and social development fulfil the objectives of a foreign power.
- The obtention of lawfully classified or otherwise publicly inaccessible information whose acquisition may lead to endangering or damaging state interests.
- Conscious disclosure of information by political representatives or public administration representatives.

- Unconscious disclosure of information by political representatives or public administration representatives.
- The breach of information confidentiality via a breach of cybersecurity.

D. Recommendations to Strengthen Resilience

1. Set up a mechanism for the evaluation of findings on the influence of foreign powers within the framework of mutual cooperation and coordination of proposed measures.
2. Establish departments within relevant Government institutions for the evaluation of disinformation campaigns and other manifestations of foreign power influence.
3. Develop a system of training public administration officials focused on increasing resilience against influence attempts by foreign powers.
4. Create an offer of such training events that could be attended on a voluntary basis by other persons who, in terms of their activities, may be of interest to foreign powers.
5. Review the effectiveness of training relating to principles of safe behaviour on the internet at Government institutions and set a minimal standard for such training.
6. Introduce proposals in the field of substantive and procedural criminal law: possibility of using intelligence in criminal proceedings *et al.*
7. Develop active media strategies of important democratic institutions against the influence of foreign powers.
8. Ensure conditions for the application of HR policies of intelligence services so that these can hire the required number of candidates, train them to become high-quality experts, and retain them in the service.
9. Ensure the speed of exchange of intelligence to lawful recipients and effective feedback.
10. Introduce measures in media law strengthening the ability of the relevant Government authority to obtain information necessary or the exercise of its legal powers, especially in relation to the ownership structure of broadcasters who are legal persons.
11. Analyse the efficiency of existing legal instruments, where necessary, to respond to a significant wave of disinformation.
12. Analyse the exceptions taking into account state security interests when communicating information as per the act on free access to information.
13. Incorporate the topics of research of methods and categories of propaganda, fact-check projects, and other into security research grants.
14. Adjust curricula of primary and secondary schools (enhanced civic literacy and introduction to media literacy).

SECURITY ASPECTS OF MIGRATION

A. Description and Assessment of the Threat and Associated Risks for the CR

1. Introduction

Migration[42] is a natural and constant historical phenomenon and opportunity; for the immigrant, the receiving country, and the country of origin. International trade, foreign investment, study abroad, professional international internships, highly qualified foreign workers, or low-skilled workers, managers of international corporations, but also cultural and scientific international cooperation, all are closely linked to migration. Significant restrictions or even the exclusion of migration could in itself be an economic threat and would lead not only to loss of competitiveness, but would, in the context of reciprocity, affect the freedom of movement of the CR's own citizens.

However, migration is also linked to security aspects. Specific migrants or their large numbers may pose a threat. Such a threat may take the form of terrorism, organised crime, but also the spreading of infectious diseases, cultural practices incompatible with our legal system or a reduced willingness to integrate. Alongside the type of immigration, i.e. immigrants, the volume of migration flows may pose a threat, and security may be compromised by mass uncontrolled immigration that could result in social unrest or radicalism, both within the minority and the majority.

Migration cannot be considered in isolation from international developments in source countries and their immediate vicinity. For this reason, it is necessary to focus primarily on the causes of migration – political solutions to conflicts in source countries, combating terrorism, the fight against smugglers, ensuring conditions for the return of migrants and their involvement in the reconstruction of their countries. In this context, it is also necessary to provide assistance to countries in the immediate vicinity of conflict zones.

While analysing the security aspects of migration, the working group identified, in accordance with SS 2015, the threat of illegal migration as a result of the increased number of local armed conflicts as well as the threat of insufficient integration of legal migrants, which may be a source of social tension. The issue of possible radicalisation[43] of members of immigrant groups or the majority population is discussed in the chapter on Extremism, the issues of terrorism and foreign fighters are discussed in the chapter on Terrorism. In particular, the threat of uncontrolled migration may, under some circumstances, be one of the elements of a hybrid threat, discussed in the eponymous chapter.

[42] Migration is defined as a cross-border phenomenon, closely related to cross-border traffic control, the functioning of border crossing and crossing state borders. In contrast, it is necessary to define the free movement of people, a fundamental principle of European legislation, defined by Directive 2004/38/EC on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States.

[43] For the purposes of this chapter (in accordance with the chapter on Extremism), radicalisation is understood to mean the change in the ideological attitudes of a person towards ones that are extreme, outside constitutional norms, bearing signs of intolerance and attacking basic democratic constitutional principles. These extremist attitudes are capable of developing into actions that are destructive to the current democratic system, including violent actions. Radicalism is the holding of these extreme ideological attitudes; Islamic radicalism is the holding of extreme ideological attitudes that conform to the definition above and that concurrently stem from some radical trends within Islam (or refer to this religion). The present chapter focuses mainly on attitudes calling for various forms of violence.

The long-term goal of immigration policy is to eliminate these threats in the CR through **instruments of controlled migration**, when security risks are reduced via regulatory, especially legislative, instruments and processes. The state-controlled migration process must be safe and balanced. In this respect, the real threat to security within the context of the entire migration process is that of uncontrolled migration. The degree of sovereign influence on controlled migration significantly influences the risk of disrupting the balance of controlled migration.

The process of controlled migration is closely linked to the **process of integration**, since controlled migration may be effective and functional in the long-term only when it is associated with successful integration in the destination country. The ability to integrate and the degree of integration in the majority population define the possibilities and the volume of controlled migration.

In terms of the considerable interconnectedness and the difficulty of separating identified threats, the working group did not use a specific method for their identification. It drew on available strategic documents that were available to it.[44] For both identified threats – the threat of uncontrolled migration and the threat of failed integration – it considered the criterion of the impact severity should these threats occur. Furthermore, the question of vulnerability and system settings in terms of internal factors and the question of motivation in terms of external factors were considered, which influence the success of the entire system.

2. The Security Environment and the Starting Point for the CR – the EU Context

The security environment in which the CR finds itself is the key to correctly identifying threats and analysing risks. This environment is subject to dynamic changes, increasingly complicated predictability, and the reality that the CR is more frequently and more intensely influenced by relatively remote regional or local conflicts. In order to evaluate migration phenomena, defining related policies, and addressing possible threats, it is **essential that the CR participate in the EU and the Schengen area**. The abolition of internal border controls of the Schengen area significantly affects the way in which the territory of the CR is protected, also in relation to fighting illegal migration, and puts increased demands on cooperation of EU member states. Other aspects also stem from the CR's EU membership. Firstly, they relate to the significant influence of EU legislation in the field of border control, migration, asylum and visa and repatriation policy. Thanks to the principle of free movement of people within the EU, EU citizens and their family members are almost outside the reach of state regulation. The mobility of EU citizens accounts for more than 50% of all foreigners residing temporarily or permanently in the CR. Besides EU legislation, the issue of migration is significantly influenced by international obligations of the CR, especially in the field of human rights.

When values and security are shared within a community, the "chain is only as strong as its weakest link". It is a commitment for the CR, therefore, to not become the weakest link and thus an increased security risk for other members. Likewise, this commitment must be accepted by other countries. Experience from the past decade suggests that decisions on the issue of migration made at the national level by one EU member state may have a major impact on real migration in other EU member states.

Since joining the EU and abolishing internal border controls, the CR adopted a number of compensatory measures, which it fulfils within the scope of its assigned competencies. Within its

[44] See section B: Responsible Institutions within the Security System of the CR and Basic Tools for the Elimination of These Threats and Risks.

scope of powers, it reacts to new trends by consistently adhering to accepted standards or by proposing amendments to legislation in accordance with the EU and the Schengen *acquis*.

I) The Threat of Uncontrolled Migration – Uncontrolled Arrivals, Violation of Residency Rules, Inability to Carry Out Repatriation in Case of Such Violation

The threat of losing influence over controlled migration has two factors: internal and external. The **internal factors** are given mainly by the inability or the incapability to adjust the immigration system or process. This system then becomes vulnerable and, when strained, untrustworthy. This vulnerability may be prevented by good legislation and adequate equipment of the system. Higher risks are related to the **external factors**, which influence the occurrence of this threat and which are usually objective facts (conflicts, natural influences and disasters, but also the influence of organised crime in the form of smuggling networks), subjective motivation and psychological factors (e.g. the willingness of migrants to take risks, unrealistic expectations about the opportunities in the destination country, the willingness to spend money on the journey to the destination country and for the services of smugglers, subjective economic motives of migrants, etc.). The capability to mitigate these risks is much more complex and depends on the degree to which the risk can be influenced.

a) The Question of Vulnerability (Internal Factors)

When assessing the vulnerability of the current system, what needs to be taken into account is the security environment, i.e. the non-existence of internal borders between Schengen member states, as well as **the limited opportunity to take advantage of legislative regulations for reasons of an existing EU legal framework**. Visa policy instruments (especially short-term visas) are now almost entirely covered at the EU level, as well as the standards for external border protection. International protection is regulated at the EU level, mostly in the form of regulations and directives. In the field of legal migration, a number of directives have been issued in the past ten years, even though member states still maintain a high degree of discretion and may employ some national regulation mechanisms. The relatively limited possibility for individual states to intervene and shape migration policy both at the EU and at the national level is evident from the high percentage of centrally defined partial policies. The **possibility and ability to legislatively adjust the conditions of entry and residence of foreigners so as to make migration beneficial in the long-term and to minimise its potential negative impacts** is crucial for efficient management of migration.

Alongside the legal framework, in order to reduce risk, it is necessary to ensure **adequate equipment both quantitatively and qualitatively** (technically and materially), the ability to efficiently carry out the visa process, border controls at international airports, detect forged or falsified documents, but also to enforce law – e.g. through combating illegal employment, carrying out residential and employer checks, etc. It is no less important to **share intelligence at the national level** and to interconnect information systems and databases, both at the international and interministerial level within state and local administration bodies, where the administrative burden is reduced on the one hand and the bypassing of legislation is effectively being detected on the other hand. It is imperative, in this day and age, to use modern technologies, which are used in order to ensure internal order and security, national security, and crisis management. This is related to the need to provide a communication environment that will be used by these technologies. It is also crucial to set **anticorruption measures** within state administration, because the area of issuing entry and resident is a risky segment of public administration in terms of corruption.

Procedural and functional rules are crucial for efficient management of migration. The control settings must withstand potential abuse (e.g. fictitious employment, fictitious study, fictitious family ties, etc.) and must provide an adequate tool for controlling migration. This process must be capable, in a relatively short time, to assess whether a specific foreign national is on the territory of the state or not and whether they pose any kind of threat. At the same time, however, the process must not hinder desirable legal migration. If the conditions of entry and residence are set adequately, but the procedural setting is not functioning, a high rate of bypassing the law and of disrupting the process of controlled migration ensues. **Security forces, which must be an integral part of the entire immigration process**, play a key role in reducing individual risks.

What is essential to the credibility of the entire immigration process is the ability of the state to ensure **the effective and efficient repatriation** of foreign nationals who have entered the territory illegally, or no longer hold permission to reside in the territory. The success or failure of repatriation policy depends on the degree of the risk of escalation and the effectiveness of the threat. Here, too, the emphasis is on efficiency and actual feasibility of repatriation of the foreign national to their home country or country of last residence.

b) The Question of Motivation (Push and Pull Factors)

A factor affecting the possible risk of loss or limitation of influence over controlled migration is the motivation of the migrant, often supported by organised or smuggling groups. The motive for uncontrolled migration is mainly affected by push and pull factors.

Push factors include everything that influences people in the country that they are leaving and that encourages them to leave. Most often, these are the security and economic situation (conflicts, threats to specific groups) or natural factors (catastrophes or lack of resources). An important factor is bad governance, corruption, unemployment, prosecution, the loss of perspective. It is necessary to maintain high activity within the EU, both the CR' of regional groupings such as the Visegrad Group.

The socioeconomic situation, security, and standard of living in source and transit countries have a major influence on migration. It is therefore necessary, at the EU and national level, to strengthen the use of instruments to prevent migration from source countries through a variety of specialised assistance programmes. In this respect, the European Commission, in cooperation with the European External Action Service, introduced a new framework or partnership with third countries in June 2016, which should deliver a complex and coordinated approach of the EU targeting the root causes of migration in the long-term. This approach is reflected in the so-called migration compacts – tailored agreements with third countries containing both positive and negative incentives, drawing on the full range of instruments of a complex EU approach. In the short-term, an effective repatriation policy will be a key element of the partnership. The preparation of the compacts with priority countries in Africa and the Middle East has already been launched and the CR is actively involved.

Within the EU, the CR also actively contributes, for example, to the EU Trust Fund for the Middle East and the Western Balkans (MADAD) and the Trust Fund for Africa. Czech financial support is also aimed at the World Food Programme (WFP) and the Office of the United Nations High Commissioner for Refugees (UNHCR). Tools at the national level include foreign development aid, humanitarian assistance, and specialised programmes such as the MoI Programme for Assistance to Refugees in Source Regions and Prevention of Migration Flows in 2015 and the Programme for Humanitarian Evacuation of Medically Disabled People (MEDEVAC).

Pull factors include everything that attracts migrants to destination countries (the availability of a social system, the level of healthcare, the attitude of society to migration, the level of willingness of society to tolerate illegal migration, the size of settled communities, and the ease of abuse of administrative proceedings). It is the size of the diaspora in combination with the potential for economic progress, be it in the grey economy, is an important pull factor for a number of illegal migrants. Penalties for organising illegal migration also play an important role. This crime is motivated by high rewards and minimal punishment. The state of current criminal legislation and the level of social harm caused by organising illegal migration and providing illegal residency, including illegal employment, but also various forms of purposeful declarations of paternity, purposeful marriages, etc., should be considered.

Illegal migration as such is not criminal in the CR. The illegal migrant is affected mainly by being issued an administrative expulsion and entry ban to the entire EU. Individual offences (referred to in the Alien Act) related to illegal migration are not classified in the same category for determining the length of the entry ban. The definition of the length of the entry ban should match the seriousness of the offences.

The threat of uncontrolled migration lies in the insufficient adjustment of the functionality of the system, its limited credibility, and the limited ability to implement set procedures (repatriation) in terms of internal factors. If this legislative framework is not adequately adjusted and adhered to, it may lead to pull factor and other motives to bypass or abuse the system. Here it is necessary to emphasise the importance of prevention and vigilance, which should be ensured by adequate sharing of information and cooperation between relevant Government bodies. It should be noted that the significance of this threat is crucial at the national level, but that the working group nevertheless points out the limited possibility of EU member states to use national legislative regulations because of the existing EU legal framework.

II) The Threat of Failed integration

Integration is a long-term and bilateral process[45] of integrating foreigners into society, with an emphasis on the need to involve both foreigners and the majority population. **The aim of integration policy is a smooth and mutually beneficial coexistence of foreigners and the majority population.** Successful integration is a key factor in eliminating many negative phenomena that may ultimately also lead to security threats.

A non-integrated foreigner poses a threat in relation to the normal coexistence with the majority population and in relation to social peace. Insufficient integration poses the **risk of creating closed foreigner communities**. Their societal isolation or social exclusion lead not only to personal frustration, but breed conflicts between foreigners and the majority population or between different foreigner communities. Insufficient or failed integration poses the risk of increased xenophobia, intolerance, and extremism in society.

Failed integration, however, also poses **a risk for the migrants** – helpless and ignorant migrants may be prone to manipulation, blackmail, and loss of legal residency. The reason for the helplessness of migrants is mostly their limited knowledge of Czech, which does not allow them to navigate society, local customs, and rules of coexistence, and which prevents them from forming relations with the majority.

Successful integration, on the other hand, reduces the risk for immigrants, allowing them to lead dignified and independent lives, enabling their further development and increasing the likelihood of their personal success and their family's prosperity. Successful integration thus contributes to the prosperity of society as a whole. The ability to be independent and not rely on the help of others – intermediaries, interpreters, employers, the state (benefits), etc., plays a key role in integration. The road to independence leads through awareness, the knowledge of duties and obligations, respect of

[45] It is also possible to consider the process of integration as tripartite, as the integration process is to some extent influenced by the source country.

the values of the CR and the EU and their acceptance, but most importantly through the ability to communicate in Czech.

a) The Question of Vulnerability (Internal Factors)

In order to ensure the functionality of the system, the existence of strategic documents that will, alongside sufficient capacities and successful practical implementation, enable the functionality and flexibility of the system, is necessary. From this perspective, the CR has a balanced integration policy that is significantly harmonised by common EU tools and thus maintains a high degree of national discretion.

b) The Question of Motivation (External Factors)

Integration, which is primarily **aimed at migrants** planning permanent residency, can no longer be considered solely as a matter of choice. The subjection of this group of migrants to accepting **to participate at least in basic integration measures** is therefore essential, both in the interest of the migrants and society as a whole. The requirement for a higher level of knowledge of Czech – naturally supported by an expanded choice of classes – is fully justified. Equally, it is reasonable to demand that migrants participate in classes that will introduce them to the value system and rules of coexistence in the CR and the EU, as well as with their rights and obligations. Here, a differentiated approach needs to be applied, based on the cultural regions, but especially the social groups, of the migrants. The factual culmination of the integration process should be the obtention of citizenship, which implies the obtention of and the possibility to exercise political rights.

The **majority population** plays an important role in the integration process. Positive experiences in coexisting with foreigners and non-conflictual relations with them lead the majority society to support coexistence with migrants and to refuse and disagree with radical attitudes of some of its members, whose political and social views are thus suppressed. The willingness or ability of immigrants to integrate themselves, as a result, increases the acceptance of the majority and its willingness to support coexistence with migrants. From the security standpoint, and that of peaceful coexistence of the majority society and migrants, it is the ability of migrants to integrate that directly influences the volume of immigration. The elimination of the threat of non-integrated immigrants thus reduces the risk of creating social unrest and radicalisation of society.

The threat of failed integration lies mainly in external factors, which are difficult to influence. The motivation of migrants to actively take part in the integration process and the willingness of the majority population to allow and support this integration are mutually interrelated and inseparable factors affecting the resulting peaceful manner of coexistence.

Migration policy must, in this regard, minimise the risk of failed integration from the very beginning of the migration process (radical foreigners, the risk of dependency on the social system). It is easier to prevent problems than to **face the consequences of uncontrolled migration and failed integration**.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

International Context and Legislative Framework

Czech migration policy is significantly influenced by international legal obligations and EU membership. EU law has a major impact on Czech migration policy, especially the Treaty on the Functioning of the EU (TFEU), which introduced common policies in the areas of migration, international protection, and borders. Common policies are implemented through EU instruments in the form of specific directives and regulations (e.g. the Schengen Border Code, the Visa Code, the Dublin Regulation, etc.), while practical cooperation at the EU level is implemented, *inter alia*, through EU agencies (EASO, Frontex, Europol). In the area of international law, the UN Refugee Convention can be mentioned.

Migration is a complex phenomenon that, pursuant to Act No. 2/1969 Coll.,[46] on competencies, falls within the competency of the MoI. The CR has a coherent legislative framework in the area of migration policy, covering a wide range of migration issues and subject to minor amendments as necessary. In addition to general standards, some of the most important acts in the area of migration are Act No. 326/1999 Coll., on the residence of foreigners; Act No. 216/2002 Coll., on the protection of state borders; Art. 43 of the Charter of Fundamental Rights and Freedoms;[47] Act No. 325/199 Coll., on asylum; Act No. 221/2003 Coll., on the temporary protection of foreigners.

Basic Documents

The basic strategic framework of migration policy is the **Migration Policy Strategy of the CR**[48] of 2015, which defines seven key areas – integration; illegal and repatriation policy; asylum; the external dimension of migration policy; the free movement of people in the EU and Schengen cooperation; legal migration; international and European obligations of the CR in the area of migration. The updated strategy covers all key aspects of the issue of migration and is an adequate tool governing the Czech migration policy.

Apart from coexistence, security aspects of migration influence the social and economic character of society. In connection to this, the SS 2015[49] was drafted, defining the increased rate of migration and the insufficient integration of legal migrants as security threats. The conclusions of the working group confirm the validity of the threats defined by the SS 2015, and elaborate on them further. The **Threat Analysis for the CR**[50] of 2015 identified a "large-scale migration wave" as a sociogenic threat. For the purpose of tackling this threat, the MoI updated the Crisis Management Model Action Plan – **Large-Scale Migration Wave**, in 2014.[51]

[46] Act of the Czech National Council of 8 January 1969 on the establishment of ministries and other central Government authorities of the Czech Socialist Republic.
[47] Constitutional Act No. 2/1993 Coll., as amended.
[48] Government Resolution No. 621 of 29 July 2015, on the Migration Policy Strategy of the CR and on the Communication Strategy of the CR for Migration.
[49] Government Resolution No. 79 of 4 February 2015, on the SS 2015.
[50] Government Resolution No. 369 of 27 April 2016, on the Threat Analysis for the CR.
[51] The former Crisis Management Model Action plan – Large-Scale Migration Wave, was from 2010.

In terms of integration, the CR has the updated **Strategy for the Integration of Foreign Nationals** of 2016[52], which reflects the current situation and the needs within the integration process, including the integration of all foreigners in the CR. Furthermore, the new **State Integration Programme** (SIP), which is aimed at persons under international protection and their integration into society, was adopted in 2015.[53]

Responsible Institutions and Bodies

The multidimensional nature of migration is reflected in the number of departments and state bodies that tackle this phenomenon and that cooperate among themselves. In this context, it is necessary to mention the activities of the interministerial **Coordination Body for Managing Border Protection and Migration**,[54] which was set up on 13 December 2006 under the MoI. Members of the Coordination Body are executives at the level of Deputy Ministers of the MFA, the MIT, the MLSA, the MEYS, the MD, the MRD, the MJ, the MT, and the MH. Furthermore, members include the Police President, the Deputy Minister for Human Rights, Equal Opportunities, and Legislation, the Deputy Prime Minister for Science, Research, and Innovation, and the Secretary of State for European Affairs of the Office of the Government of the CR.

In connection with the adoption of the Migration Policy Strategy of the CR and the Communication Strategy of the CR for Migration on 29 July 2015,[55] and the adoption of Government Resolution No. 824 of 12 October 2015 on the amendment to the previous resolution,[56] the **Coordination Body for Managing Border Protection and Migration meets also at the Governmental level**. The individual competencies are described in the **Situation Report on Migration and Integration of Foreign Nationals in the CR**.[57] The migration policy security framework includes, to varying degrees, individual ministries, and some of their subordinate bodies, whose agenda includes mainly the following competencies:[58] the Office of the Government (coordination of public administration, human rights, European affairs), the MoI (coordination of asylum and migration policy and border protection, coordination of integration, crisis management), the MFA (development cooperation and humanitarian aid, short-term Schengen visas, visa and consular agenda), the MIT (foreign business), the MLSA (employment and social security of foreigners, integration of foreigners in the labour market), the MEYS (education and integration of foreigners within the pre-school, primary, secondary, higher professional and university education system), the MF (financial security, customs, sanctions for illegal employment), the MD (defence of the CR and cooperation with the armed forces of other states), the MJ (criminal legislation, judicial expulsion and extradition), the MT (civil aviation), the MH (safeguarding public health), and the MRD (regional policy).

[52] Government Resolution No. 26 of 18 January 2016, updated Strategy for the Integration of Foreign Nationals "Mutually Respectful".

[53] Government Resolution No. 954 of 8 November 2015, on the State Integration Programme for Persons under International Protection in 2016 and Following Years".

[54] Government Resolution No. 394 of 18 April 2007, on the National Border Protection Management Plan in the CR.

[55] Government Resolution No. 621 of 29 July 2015, on the Migration Policy Strategy of the CR and on the Communication Strategy of the CR for Migration.

[56] Government Resolution No. 824 of 12 October 2015, on the amendment to Government Resolution No. 621 of 29 July 2015, on the Migration Policy Strategy of the CR and on the Communication Strategy of the CR for Migration.

[57] Situation Report on Migration and the Integration of Foreign Nationals in the CR is drafted annually in accordance with Government Resolution No. 467/1993 and Resolution of the Chamber of Deputies of the Parliament of the CR No. 225 of 12 October 1993, and the consequent Resolution of the Chamber of Deputies of the Parliament of the CR No. 716 of 28 June 1995.

[58] The list of competencies for individual ministries and their subordinate bodies is not exhaustive; the competencies are listed with respect to the area of interest.

In terms of safety aspects, a crucial role is played by intelligence services, which participate on the issue within the scope of their competencies, defined by legislation (Sec. 5 of Act No. 153/1994 Coll., on intelligence services of the CR) and in accordance with their annual priorities approved by the Government.

C. SWOT Analysis

Strengths

Systemic

- The existence of the Migration Policy Strategy and migration policy coordination through the Border Protection and Migration Coordination Body, at the Governmental level, since July 2015.
- A stable and consistent Czech position on migration at the national and EU level.
- Significant and long-term experience with migrants, for whom the CR is becoming a destination country (more than 50% of foreign nationals with residence permits obtained permanent residency).
- The existence of a National Schengen Plan and its regular assessment with the purpose of ensuring that the CR fulfils its obligations in the field of Schengen cooperation.
- Regular monitoring and analysis of the migration in the CR and the EU and the ability to take prompt decisions in reaction to current events, including the ability to evaluate individual migration risks during the visa process.
- A long-term and regularly updated Strategy for the Integration of Foreign Nationals, which is built on the ability of targeted integration at the local level and networking at the regional level, as well as on the flexibility of use of instruments.
- The introduction of compulsory integration elements (Czech language exams, exams when applying for citizenship).
- A high level of commitment and targeted security, development and humanitarian intervention in origin, transit, and destination countries, with the aim of preventing large migration flows (the MoI Programme for Assistance to Refugees in Source Regions and Prevention of Migration Flows in 2015, the MEDEVAC Programme).
- The existence of programmes of humanitarian and development assistance, emergency humanitarian programmes (e.g. in Ukraine, Syria, Jordan), active involvement of the CR in EU initiatives – contributions to EU Trust Funds.
- Active involvement in the processes of EU's Common Foreign and Security Policy and operations under the EU's Common Security and Defence Policy.
- The existence of Crisis Management Model Action Plans – Large-Scale Migration Wave and Reintroduction of Internal Border Controls, as well as the existence of Operation Plans of the Police CR, the Army of the CR, and the Customs Administration of the CR.
- The ability to promptly introduce internal border controls in accordance with the Schengen Code.
- The ability to respond to current economic requirements by introducing accelerated and simplified procedures for specific groups of migrants (migration projects).

Legislative

- A comprehensive legal framework.
- Close links between legislation, policy, and practice.

Material, Technical, and Staffing Capacities

- A high level of expertise and proficiency.
- Flexibility within the Police CR.
- Centralised information systems.
- The ability to temporarily use the capacities of other security forces for carrying out tasks of the Police CR, if necessary.
- Financial security of the system and the ability to release financial resources for targeted measures, if necessary.
- The ability to provide material and humanitarian aid abroad.

Weaknesses

Systemic

- The limited ability to effectively enforce law (speed of repatriation operations, efficiency and speed of residence permit withdrawals for security reasons, foreign fighters).
- The vulnerability of the administrative process for legal migration and related areas (reduced ability to effectively identify a migrant without, or with false, documents) – the question of the possibility of excluding individual applications for security reasons.
- The limited ability to ensure integration of foreign nationals residing in the CR (enforcement and monitoring of compulsory school attendance, etc.).
- The abuse and abusability of the asylum system for the purposes of illegal migration into the CR/EU.
- Low political support within the EU for some opinions promoted by the CR.
- The blurring of the boundary between assistance provided abroad through the EU Civil Protection Mechanism designed to address crises, i.e. urgent assistance, and follow-up assistance.
- Fragmented and piecemeal issues of expulsion sentences by courts; inconsistent proposals for the issue of expulsion sentences by public prosecutors.

Legislative

- A legislatively determined low level of social danger of illegal migration and smuggling.
- Vague and inadequate checks and balances in the Criminal Code for evaluating the possibilities of issuing an expulsion sentence.
- An inefficient administrative process for migration management.

- The rapid development of EU legislation implying the necessity of regular amendments to national regulations, which leads to their reduced clarity.
- A reduced ability to influence European legislation in the area of migration.

Material, Technical, and Staffing capacities

- The insufficient ability of state bodies to promptly and efficiently respond to the necessity of increasing staff numbers (hiring new employees, training) and retaining expert staff (financial remuneration).
- Lack of experts with languages who could operate in the field, especially in countries outside of Europe.
- The necessity to continuously renew and develop the material equipment of security forces.
- The inadequate interconnection of state administration information systems.
- An inadequate communication environment for the use of modern technologies in ensuring internal order, national security, and prevention in the area of national security.
- An insufficient ability to efficiently and effectively develop critical information systems.

Opportunities

- Workforce mobility and associated economic development.
- Visa-free regime for Czech citizens as a measure of reciprocity.
- The free movement of people, goods, services, and capital as a fundamental element of the existence of the EU.
- The influx of foreign investors and investments.
- An efficient use of EU financial resources.
- A positive impact on the demographic tally.
- A long-term strategy of security research.
- The use of financial resources from the MADAD Trust Fund and the Trust Fund for Africa not only to prevent migration, but also to strengthen the involvement of Czech entities in the use of these financial resources.

Threats

Uncontrolled Migration

- As a result of conflicts in third countries – migration caused by so-called push factors.
- As a result of natural effects and disasters.
- As a result of the uneven fulfilment of common rules within EU Schengen (external border protection, asylum *acquis*).
- As a result of the so-called foreign fighter phenomenon.

- As a result of organised crime (trafficking in human beings and its proceeds invested back into the illegal system, criminal activity focused on illegal migration – forged documents, smuggling, and illegal border crossing – shelters, purposeful marriages, so-called straw men, illegal employment, etc.)
- As a result of unregulated flows of EU citizens and secondary migration flows (third-country nationals residing in the EU).
- As a result of the abolition of visas for certain countries.

Failed Integration

- As a result of negative attitudes of the majority of society.
- As a result of increased tensions in society.
- Manifestations and strengthening of the influence and activities of extremist groups.
- Due to a lack will of the migrant to integrate into society for reasons of significant cultural differences and traditions different from those of the Czech legal system.
- As a result of the existence of subsequent generations of migrants (naturalised migrants) not integrated into society and not at one with the value system of the CR and the EU.
- As a result of the emergence of ghettoes and the subsequent creation of criminogenic environments.

D. Recommendations to Strengthen Resilience

In summary, it can be stated that the CR has, to the extent determined by the security environment in which it finds itself thanks to its geographical position and its membership in the EU and the Schengen Area, set up a system for managing migration flows. Although the system is set up, it is necessary – due to a high dynamics and low predictability – to continuously assess it, detect partial shortcomings and respond efficiently to new development trends.

Recommendations stemming from the SWOT Analysis (section C above):

Systemic Measures

1. Ensure strategic communication to provide transparent and open information to the public and all other relevant stakeholders.
2. Ensure early identification and assessment of the threat of unregulated migration concerning the CR.
3. Ensure efficient cooperation of security forces at the national and international level as well as timely transfer of information.
4. Exchange relevant information with the Governments of partner countries regarding migration, international protection and the current security situation in regions affected by the crisis (e.g. the Middle East and Northern and Sub-Saharan Africa).
5. Prevent the radicalisation of the majority population and prevent the radicalisation of and recruitment of foreigners through the use of information and awareness campaigns.
6. Optimise the setting of penalties of crimes related to illegal migration. Cooperate in the field of external relations through strengthening capacities in third countries affected by crises.

7. Strengthen humanitarian, development, and reconstruction assistance to source countries of migration.
8. Draft long-term strategies and Government documents.
9. Strengthen assistance to transit and destination countries facing increased migration flows.

Legislative Measures

1. Amendment to Act No. 326/1999 Coll. on the residence of foreigners, in terms of strengthening the security features of the immigration process.
2. Amendment to Act No. 326/1999 Coll., on the residence of foreigners, in terms of strengthening the mandatory elements of integration.
3. Amendment to Act No. 325/1999 Coll., on asylum, with the aim of introducing a possible acceleration of the asylum procedure in specific areas.
4. Amendment to Act No. 150/2002 Coll., on the code of administrative justice, in order to accelerate administrative judiciary.
5. Amendment to Act No. 234/2014 Coll., on civil service, with the aim of ensuring greater flexibility of state administration in matters of staffing and the efficient setting up of a remuneration system with the purpose of retaining expert staff.
6. Make efforts to influence EU legislation and coordination processes in order to streamline administrative processes in areas that are already regulated by EU legislation, with a focus on thorough consideration of subsequent steps with regards to the issue of visa liberalisation.

Material, Technical, and Staffing Capacities

1. Ensure the computerisation of the application procedure as an effective anti-corruption and security aspect of management, which will concurrently improve speed and increase convenience for clients, including the desired interconnection of state administration information systems.
2. Support the setting up of supraministerial principles of long-term development of fixed and mobile communication infrastructures and public administration and eGovernment technologies, for use in ensuring internal order and security, national security, and prevention in the area of national security.
3. Fulfil the concept of development of current critical information, identification, and registration systems (CIS[59], VIS[60]), as well as AFIS[61], in order to introduce new technologies in the area of identification of persons, including a functional and efficient interconnection of these national information systems with the central supranational information systems of the EU.

[59] Alien Information System (*Cizinecký informační system*).
[60] Visa Information System.
[61] Automatic Fingerprint Identification System.

4. Carry out an inventory at border crossings in accordance with the adopted Situation Analysis I the Area of Infrastructure at Border Crossings of the CR. [62]
5. Adopt measures in the area of staffing in order to ensure that all ministries have experts with adequate language skills and training.
6. Regularly renew the material equipment of security forces and consular sections.
7. Ensure institutional support of the long-term strategy for security research.
8. Support the development of the National Centre for Document Verification.
9. Support the development of the National Situation Centre for Border Protection.

[62] NSC Resolution No. 5 of 18 January 2016, on the Situation Analysis in the Area of the Infrastructure at Border Crossings of the CR.

ENVIRONMENTAL THREATS

A. Description and Assessment of the Threat and Associated Risks for the CR

1. Introduction

In the context of climate change, the number of emergencies and crises caused by natural disasters, as well as the severity of their impact, is growing. In most cases, it is impossible to significantly reduce the risk of their occurrence, but they can be monitored and predicted some time in advance, and measures can be taken to ensure preparedness to tackle them. Adapting to climate change is also important, as it will help avoid losses and damages and thus mitigate the economic, social, and other impacts of climate change.

In order to identify and distinguish different threats that can occur in the CR, the Analysis of Threats to the CR was elaborated and approved by Government Resolution No. 369 of 27 April 2016. This analysis identified 72 threats that were further subjected to a multi-criteria analysis,[63] which took into account frequency of occurrence and severity of impact on key interests (lives and health, environment, economy and society). The last step of the analysis was to those assess risks, which were prioritised and clearly defined, that require special attention. In the area of environmental threats, both abiotic (caused by inanimate nature) and biotic (caused by living nature) threats were considered.

The following threats will be considered for the purposes of the Audit:[64]

I) Floods, flash floods, heavy rainfall

II) Prolonged droughts

III) Wildfires

IV) Extremely high temperatures

V) Extreme winds

VI) Epidemics – mass human diseases

VII) Epiphytotics – mass crop diseases

VIII)Epizootics – mass animal diseases

[63] Detailed information on the analysis, including the considered parameters/criteria and the degree of risk for individual threats can be found in the Analysis of Threats to the CR (in Czech only).

[64] These include all environmental threats (identified by the Analysis of Threats) with an unacceptable degree of risk. Furthermore, in accordance with the anticipation of droughts in the upcoming years (and in accordance with the Environmental Security Strategy), the issue of wildfires was also included.

2. Descriptions of Individual Threats:

I) Floods, Flash Floods, Heavy Rainfall

Floods are caused by heavy rain (flash floods) or consistent rain, large areas of melting snow in combination with an unfavourable physical state of the soil and a reduced capacity for water retention. Flash floods are characterised by heavy rainfall and are linked to a rapid rise in water levels in rivers as well as their subsequent rapid decline.

The consequences include losses of lives and damages to health and the environment, especially when the natural territorial limits are not respected. Floods may cause further crises, e.g. soil contamination (soil, water) caused by hazardous material leaks.

The extent and type of contamination (biological, chemical) may result in the impossibility of bringing water to the desired quality for a period of time. Vast areas of damaged crops are an accompanying phenomenon to floods.

Heavy rainfall and its consequences refers to intense rainfall in urban areas where, as a result of exceeding the capacities of the sewer system, the lower parts of edifices and technical infrastructure are flooded by rainwater running off on the surface.

Impact on critical infrastructure could occur particularly in the following sectors: energy, water, food, agriculture, and transport.

II) Prolonged Droughts

From a climatological perspective, drought is a normal, recurring event related to climate fluctuations. Droughts are a result of a prolonged period of low precipitation and are intensified by above-average temperatures and thus increased evaporation. Current methods of farmland management as well as urbanisation with its rapid discharge of water, the infiltration capacities of the landscape are reduced, thus significantly lowering its water retention capacity.

A major problem linked to prolonged droughts is the scarcity of water in reserves catering to the needs of the population, the critical infrastructure, and ecosystems, and the associated restrictions in their ability to provide key ecosystem services. Ultimately, water scarcity can lead to endangering the health and life of the population, a reduction in economic output, contribute to the outbreak and spread of wildfires, and cause damage to forests and farmlands.

III) Wildfires

Fires in nature, i.e. forest fires and grassland fires, fires on farmlands and peatlands, constitute a pressing problem, especially in connection to prolonged droughts. A higher probability of wildfires occurs when the moisture level of organic matter (grassland, forest, leaf litter, etc.) is low, during prolonged droughts, low humidity (air, soil), higher temperatures and a longer duration and higher intensity of sunshine.

Apart from the threat to property, health and lives of the population, wildfires have a highly devastating effect on the environment. Forest fires along the state border crossing into the CR and fires of particularly valuable habitats that threaten their ecological stability or their existence are among the most disastrous. In the case of fires in specially protected areas and in Natura 2000 areas, the potential damage and risk of damaging these areas when extinguishing the fires poses a problem. Extensive fires may also cause significant water and air contamination.

IV) Extremely High Temperatures

Extremely high temperatures (heat waves) threaten the health and lives of the population, but also the functioning of critical infrastructure, especially in sectors such as energy, transport, water, food, and agriculture. The consequences of extremely high temperatures include, most importantly, threats to the health and lives of the population. Other consequences include damage to forests, farmlands, and an increased risk of fires. High temperatures affect evaporation of water from the land and may be one of the causes of droughts. In the area of critical infrastructure, high temperatures are a threat to the energy sector, not only because of the increased energy consumption for air-conditioning, but also because of limited options for refrigeration (e.g. for waste heat, reduction in the level of water used for cooling). Thermal stress may also threaten traffic constructions, e.g. the railway.

V) Extreme Winds

Dangerous wind speeds occur in the CR in the winter, when deep low pressure areas move to eastward and in the summer during intensive storms. Extreme winds with serious consequences usually only affect a specific part of the territory. The impacts of strong winds primarily affect transportation, communication, settlements, and forests that may be seriously damaged or destroyed. The effects on the critical infrastructure are manifested most notably in the energy (compromising the energy grid) and transport sectors.

VI) Epidemics – Mass Human Diseases

An epidemic is the occurrence of an infectious disease that significantly exceeds the expected incidence in a given time and place. In the CR, epidemics can either be caused by commonly occurring infections or an entirely new type of infectious disease (or a disease that has been eradicated). The incidence of infectious diseases (i.e. the frequency of new infections in the population specified by time and place) is influenced mainly by the susceptibility of the population to infections, the virulence of the agent, the toxicity, the efficiency of anti-epidemic measures, and the possibilities of causal treatment.

The impacts of large-scale epidemics cannot be clearly determined, for they will depend on the possibilities of transmission of the infectious disease, the virulence of the agent, the possibilities of causal treatment, the availability of vaccines, etc. (increased illness among the population and the consequent absence from work may have implications across the board on all critical infrastructure sectors).

VII) Epiphytics – Mass Crop Diseases

Epiphytics stand for mass outbreaks of disease in agricultural crops and forest plantations. They depend on developments in climate conditions during vegetation. Their duration deepens on the speed with which phytosanitary measures are implemented, or crops destroyed.

VIII) Epizootics – Mass Animal Diseases

Epizootics are infectious animal diseases affecting large groups (large numbers) of animals over a large area (region, state) at a specific time. The characteristic features of epizootics are a rapid onset, rapid spread, and high morbidity. A panzootic is an extreme form of an epizootic, where the infectious disease spreads to entire continents. Highly virulent (infectious) diseases of viral origin cause epizootics or panzootics. In Europe, the most prevalent are mouth and foot disease, swine fever, or the highly pathogenic form of bird flu – H5N1. These diseases spread very rapidly and may extend to several countries in a matter of days if appropriate veterinary measures are not taken.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

Basic Documents

Population Protection Strategy 2020 with an Outlook for 2030 – the document sets, in a broader perspective, further actions in the development of major areas of population protection, such as education and training, capacities, material resources, the tasks associated with population protection, crisis management, science and research. It also includes basic tasks for implementing the set priorities of population protection for the entire period of its validity, including the outlook for 2030.

Environmental Security Strategy 2016 – 2020 with an Outlook for 2030 – the aim of this document is to limit the occurrence of crises caused by the interaction of the environment and the population, reduce the impacts of occurring crises, and improve environmental security. Achieving these goals stands on the premise of completing the specific legislative, technical, institutional, and information measures. The strategy includes proposals to expand existing measures, which will lead to increased environmental security, both in terms of anthropogenic threats (chemicals, sources of ionising radiation, biological agents) and natural threats (extreme weather conditions, floods, prolonged droughts, slope instability etc.). The **Strategy on Adapting to Climate Change in the CR** is a national adaptation strategy which, apart from assessing the likely impacts of climate change, includes proposals or specific adaptation actions, a legislative and to an extent economic analysis.

Legislation

The basic laws that apply to all types of environmental threats are:

- Act No. 239/2000 Coll., on the integrated rescue system and on amendments to certain acts
- Act No. 240/2000 Coll., on crisis management and on amendments to certain other acts (Crisis Management Act)
- Act No. 241/2000 Coll., on economic measures in crises and on amendments to certain other acts

Legislation and basic planning documents relating to individual threats:

I) Floods, flash floods, heavy rainfall

- Act No. 254/2001 Coll., on water and on amendments to certain other acts (Water Act)
- Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for community action in the field of water policy
- Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks

Related documents: plans for flood risk management, plans for minor waterways, flood plans of municipalities, districts and regions, the Flood Plan of the CR, regional emergency plans, regional contingency plans.

II) Prolonged droughts

- Act No. 254/2001 Coll., on water and on amendments to certain other acts (Water Act)
- **Current legislation in the field of protection against droughts is inadequate.** Within the interministerial working group WATER-DROUGHT, proposals are being drafted for the amendment of specific legislation, with the expected date of completion being 2018.

Related documents: regional emergency plans, regional contingency plans

III) Wildfires

- Act No. 133/1985 Coll., on fire protection
- Decree No. 246/2001 Coll., on determining fire safety conditions and sate fire patrol (Fire Prevention Decree)
- Decree No. 247/2001 Coll., on the organisation and activities of fire protection units
- Regulations of individual regions, establishing the conditions for fire protection in times of increased risk of fire or for securing water sources for extinguishing fires
- Plans for the management of specially protected areas (in accordance with Sec. 38 of Act No. 114/1992 Coll., on the protection of nature and landscape, as amended).

Related documents: fire protection documentation, regional emergency plans

IV) Extremely high temperatures

- Act No. 258/2000 Coll., on public health protection and on amendments to certain related acts
- Act No. 133/1985 Coll., on fire protection

Related documents: fire protection documentations, regional emergency plans

V) Extreme winds

Due to the relatively low incidence of extreme winds in the CR, there are no specific regulations for this threat. However, in the context of climate change, the likelihood is increasing. For this reason, it is necessary to ensure legal regulation of the given area and modify existing legislation relating to warning and forecasting services and the IWSS to meet current needs and ensure the operation and further development of the meteorological services in the CR.

Related documents: regional emergency plans, regional contingency plans

VI) Epidemics – mass human diseases

- International Health Regulations (2005)
- Act No. 258/2000 Coll., on public health protection and on amendments to certain related acts

- Act No. 372/2011 Coll., on health services and conditions of their provision (Health Services Act)
- Act No. 374/2011 Coll., on emergency medical service
- Act No. 378/2007 Coll., on pharmaceuticals and amendments to certain related acts (Pharmaceuticals Act)
- Decision No. 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health
- Decree No. 252/2004 Coll., establishing hygienic requirements for potable and hot water and the frequency and scope of potable water control
- Decree No. 537/2006 Coll., on vaccination against infectious diseases
- Decree No. 306/2012 Coll., on conditions to prevent the emergence and spread of infectious diseases and on hygienic requirements for the operation of medical facilities and social care institutions
- Decree No. 137/2004 Coll., on hygienic requirements for catering services and on principles of personal and operational hygiene in epidemiologically important activities
- Decree No. 473/2008 Coll., on the system of epidemiological vigilance for selected infections

Related documents: pandemic plans, traumatology plans, regional emergency plans, regional contingency plans

VII) Epiphytics – mass crop diseases

- Act No. 326/2004 Coll., on phytosanitary care and amendments to certain related acts
- Decree No. 215/2008 Coll., on measures against the introduction and spread of plant pests and plant-damaging products

Related documents: regional emergency plans, regional contingency plans

VIII) Epizootics – mass animal diseases

- Act No. 166/1999 Coll., on veterinary care and amendments to certain related acts (Veterinary Act)
- Decree No. 290/2003 Coll., on veterinary products and veterinary technical resources
- Decree No. 299/2003 Coll., on measures for the prevention and control of infections and diseases transmittable from animals to humans
- Decree No. 372/2003 Coll., on veterinary controls during trade in animals

Related documents: SVA contingency plans designed for various kinds of diseases, strategy for the redevelopment of areas of mass animal deaths, regional emergency plans, regional contingency plans

Responsible institutions and authorities according to individual threats:

I) Floods, flash floods, heavy rainfall

- flood protection and supervision activities – ME
- population protection – MoI
- activities of watershed companies, including involvement in building flood protection measures – MA
- control activities – flood authorities
- flood forecasting service – CHMI
- contribution to dealing with the consequences of extreme weather conditions – MT, MIT, MH, MA, and SMRA

II) Prolonged droughts

- protection of the environment and of water – ME
- water supply and sanitation, water sources, watershed companies – MA
- population protection – MoI
- regulation of industrial production – MIT
- water transport – MT
- IWSS – CHMI in cooperation with the Department of Hydrometeorology Security of the Military Geographic and Hydrometeorological Institute of the Armed Forces of the CR
- contribution to dealing with the consequences of extreme weather conditions – MT, MIT, MH, MA, and SMRA

III) Wildfires

- fire prevention and protection of life and health of citizens and property against fires – FRS CR
- IWSS – CHMI in cooperation with the Department of Hydrometeorology Security of the Military Geographic and Hydrometeorological Institute of the Armed Forces of the CR

IV) Extremely high temperatures

- IWSS – CHMI in cooperation with the Department of Hydrometeorology Security of the Military Geographic and Hydrometeorological Institute of the Armed Forces of the CR
- contribution to dealing with the consequences of extreme weather conditions – MT, MIT, MH, MA, and SMRA

V) Extreme winds

- IWSS – CHMI in cooperation with the Department of Hydrometeorology Security of the Military Geographic and Hydrometeorological Institute of the Armed Forces of the CR
- contribution to dealing with the consequences of extreme weather conditions – MT, MIT, MH, MA, and SMRA

VI) Epidemics – mass human diseases

- state administration – MH, public health authorities, cooperation with administrative authorities and health service providers

VII) Epiphytics – mass crop diseases

- state administration – MA, Central Control and Testing Institute of Agriculture

VIII) Epizootics – mass animal diseases

- state administration – MA, State Veterinary Administration and regional veterinary administrations

Powers and instruments for tackling environmental threats

Units of the **integrated rescue system** are crucial in dealing with emergencies and crises. The basic IRS units (FRS CR and FPUs ensuring regional coverage, EMS providers and Police CR) ensure a continuous readiness to receive emergency reports, evaluate them, and intervene immediately. For this purpose, their forces are deployed across the CR. Other IRS units provide planned assistance upon request via detached forces and armed forces, armed security forces, other rescue units, public health authorities (e.g. the sanitary service), emergency, expert, and other professional services, civil protection units, non-profit organisations and citizen associations that may be involved in rescue and clean-up operations.

In crises or large-scale emergencies, when standard forces are not sufficient for tackling them, the **system for economic measures in crises** comes into play (particularly the crisis management system, the use of state material reserves and regulatory measures). The aim of an emergency economy is to ensure, during a crisis, the necessary supplies to meet the basic living needs of the population, to support the state administration and the activities of rescue forces, emergency services, the emergency medical service, and the Police CR. For this purpose, plans of necessary supplies are drafted at the regional and central level. Regulatory measures in crises serve to reduce consumption of scarce resources and services, or to regulate consumption of resources and services in accordance with contingency plans in situations where the crisis is so serious that usual economic measures are not effective in providing necessary supplies.

The contribution of legal persons and entrepreneurs that are obliged, in emergencies or crises, to provide material or personal assistance, may ensure the implementation of measures stemming from contingency plans and take part in drafting planning documentation, must not be forgotten.

Evaluation of existing legislation and capacities to tackle environmental threats

Generally, the system for ensuring readiness as well as the actual management of emergencies and crises brought on by natural causes addressed in this chapter is functional – tried and tested in practice. The relevant legislation is sufficiently addresses the identified threats, except for the issue of droughts, which was ignored in the past[65] (the legislation does not provide sufficient support for

[65] It is only in the Environmental Security Strategy 2012 – 2015 with an Outlook for 2020 that prolonged droughts are identified as a priority to be addressed, and in 2014 the interministerial working group WATER-DROUGHT was established.

adopting effective measures to mitigate the effects of a prolonged drought, with the exception of restricting the use of potable water from public water systems and replacement supplies and rations of potable water), and that of meteorological services.

Another legislative shortcoming is the inadequacy of legislation ensuring warning and forecasting services, as well as IWSS and CHMI activities.

Budget cuts to the Aerial Fire Fighting Service, which was an important instrument in identifying and extinguishing fires, may prove to be a threat in the future (as attention is paid only to the issue of firefighting, and not patrolling).

In order to ensure readiness to tackle emergencies and crises, a number of planning documents have been drafted (see individual threats). Their usefulness has been tested in practice when dealing with concrete incidents.

At the central level, and especially at level of local Governments, there is a shortage of staff dealing with crisis management (LGU employees often dedicate only part of their time to the job).

The number of IRS staff dedicated to tackling environmental threats is satisfactory. However, there is a problem with employee fluctuation (a reduction in the number of positions and the consequent layoffs followed by new recruitment is causing senior employees to leave and disrupts the stability of the system).

Material capacities of IRS units are currently at a good level. Nevertheless, it is necessary to ensure the regular renewal and modernisation of material resources, making it possible to effectively manage the increasing number of emergencies and crises.

When tackling emergencies and crises, cooperation with NGOs has proved beneficial. It is, however, necessary to set up an efficient system of their involvement (as well as that of individual volunteers).

The current system of economic measures in crises is a great advantage (especially the emergency economic management system, the use of state material reserves, and regulatory measures), and its usefulness and functionality have been tested during many emergencies and crises. In accordance with new legislation, it is possible to use state material reserves free of charge also for tackling selected emergencies and for eliminating their consequences. What remains problematic is the recurrent disproportion between the approved Plan of Necessary Supplies and the funds allocated to the SMRA for its implementation.

The deployment of modern technologies to deal with emergencies and crises is imperative in current times. This is related to the necessity of providing a communication environment that is employed by these technologies.

The working group drafted a document called “Preparing to implement measures mitigating the negative impacts of drought and water shortages” (approved by Government Resolution No. 620 in 2015). The aim is to prepare a proposal for the implementation of activities and adaptation measures to secure the main goals of the proposed plans for managing droughts and creating an information base for the proposal of a complex strategy addressing the issue of negative impacts of droughts and water shortages. Drought management plans should soon become an integral part of the amendment to the Water Act.

C. SWOT Analysis

Partial SWOT analyses were elaborated for each threat. From these, factors that can be applied cross-sectionally in the area of natural and environmental threat management, were selected and further elaborated in the overall SWOT analysis:

Strengths

- A functional and verified system.
- Existing legislation, methodological guidelines, recommendations.
- Professional knowledge and capabilities.
- International cooperation.
- Blanket coverage.
- Material resources created within the System of Economic Measures for Crisis Situations.

Weaknesses

- Insufficient financial resources.
- Insufficient human resources at both the central and regional level.
- Staff fluctuation in executive bodies.
- Insufficient support for the development of the system.
- A lengthy approval process for strategic documents.

Opportunities

- Compulsory education of the population.
- Security research.
- Sharing experiences at the international level.
- Technological development.
- Broader involvement of NGOs and volunteers.

Threats

- Climate change.
- Staffing restrictions.
- Financial restrictions.
- A population unprepared for self-protection.
- The focus on “current” security topics to the detriment of other topics.

D. Recommendations to Strengthen Resilience

1. Prepare a modification of the population protection system so that it complies with current security trends.[66]
2. Ensure stable staffing of IRS units.
3. Strengthen staffing capacities (professionals in the field of crisis management) at the central and regional levels, so that employees have sufficient capacities to focus on crisis management (to avoid part-time commitment to the issue).
4. Ensure sufficient funds for the preparation and management of emergencies and crises.
5. Increase the co-responsibility of the population for their own safety through compulsory education.
6. Introduce the issue of droughts to legislation.
7. Adjust regulations on ensuring warning, early warning, and forecasting services and on activities of the IWSS of the CHMI to meet current trends.
8. Address the issue of PR, presenting events in the media, communication with the public.
9. Pay particular attention to security research, including a system for sharing information among actors and users of research results.
10. Set up an efficient system of coordination and cooperation with NGOs in the area of population protection.
11. Promote the long-term development of communication infrastructure and technologies to be used to prepare for and manage emergencies and crises.
12. Increase resilience by implementing the Strategy on Adapting to Climate Change in the CR.

[66] In agreement with the current Population Protection Strategy.

ANTHROPOGENIC THREATS

A. Description and Assessment of the Threat and Associated Risks for the CR

1. Introduction

The number of emergencies and crises, as well as the severity of their impact, is steadily growing. Many anthropogenic threats can be prevented with adequate preventive measures, whilst all other cases require an adequate system of measures ensuring preparedness for tackling and the ability to tackle emergencies and crises caused by human activity.

In order to identify and distinguish different threats that an occur in the CR, the Analysis of Threats to the CR was elaborated and approved by Government Resolution No. 369 of 27 April 2016. This analysis identified 72 threats that were further subjected to a multi-criteria analysis,[67] which took into account frequency of occurrence and severity of impact on key interests (lives and health, environment, economy and society). The last step of the analysis was to those assess risks, which were prioritised and clearly defined, that require special attention.

The following threats, for which the assessed risk was evaluated as unacceptable, will be considered for the purposes of the Audit:

I) Special floods

II) Leakage of hazardous chemicals from stationary devices

III) Radiation accidents

IV) Large-scale disruptions of water supply

V) Large-scale disruptions of food supply

2. Description of Individual Threats:

I) Special Floods

Special floods are caused by disorders or accidents of waterworks or water storage facilities, or when waterworks resort to emergency solutions to critical situations (intentional damage, terrorism), causing emergencies near them. For the purpose of supervision, waterworks are included in categories I – V according to the amount of potential damage in the area near the waterworks in case of an accident. The owners (users) or operators of these facilities are obliged to ensure their professional technical supervision, especially in facilities falling within categories I – III. The purpose of this supervision is to continuously survey the technical state of the waterworks in terms of its

[67] Detailed information on the analysis, including the considered parameters/criteria and the degree of risk for individual threats can be found in the Analysis of Threats to the CR (in Czech only).

stability, safety, and possible failures, as well as in terms of proposing appropriate remedial measures.

Special floods may have implications for the population living near the waterworks as well as for all facilities found within the threatened perimeter. The analysis on the possibilities of the occurrence and course of special floods, on determining their effects within the profile of the waterworks and setting benchmarks for flood activity levels in case of a possibility of the occurrence of a special flood, is included in the Plan for Protection of Areas near Waterworks against Special Floods.

II) Leakage of Hazardous Chemicals from Stationary Devices

Hazardous chemicals are currently produced and imported for widespread use. All activities related to the handling of hazardous substances carry a risk to human health as well as the environment. The security risk is related to the occurrence of major accidents caused by technical defects or human error, whether deliberate or inadvertent, with the aim of causing serious harm to human health, the environment, property, or the functioning of society.

One condition for efficient protection of the population from the consequences of major accidents is to establish uniform rules for all activities related to the handling of hazardous substances.

The area of prevention of serious accidents caused by hazardous chemicals and mixtures is based on an approach of escalating duties, depending on the increasing level of risk and the implementation of control mechanisms, as well as law enforcement in the area. Once critical quantities of selected substances and their secure handling have been reached, the responsible entity must meet stricter, more stringent and also more financially taxing obligations.

III) Radiation Accidents

Requirements for the safe handling of sources of ionising radiation, nuclear materials, for nuclear safety and emergency readiness, are defined by the Nuclear Act and its implementing regulations.

The Nuclear Act and international conventions provide, *inter alia*, the conditions for carrying out activities related to the use of nuclear energy and ionising radiation. They also lay down the rules of radiation protection of people and the environment. In July 2016, a new Nuclear Act was approved as Act No. 263/2016 Coll., which will come into effect on 1 January 2017. The new Nuclear Act addresses the area of emergency preparedness (the new “management of radiological emergencies”) much more explicitly. Among other things, it requires the elaboration of a National Monitoring Programme (within 2 years from the entry into force of the new Nuclear Act) and a National Radiation Emergency Plan (within 4 years from the entry into force of the new Nuclear Act).

State administration and supervision in the area of nuclear safety, and radiation protection, emergency preparedness, i.e. management of radiation emergencies and radiation monitoring, is the responsibility of the SONS, which issues relevant permits, approves documentation, and carries out regular inspections at facilities with sources of ionising radiation. The new Nuclear Act also addresses a new area of radiation monitoring in the CR, which is carried out by the SONS and by ministries, other administrative bodies established by the act, and permit holders as defined by the law. The SONS is responsible for managing this monitoring. The data obtained are used for evaluating radiation, for purposes of monitoring and assessing radiation exposure and, in case of a radiation emergency, for deciding on measures to reduce or avert the exposure.

IV) Large-Scale Disruption of Water Supply

The disruption of water supply may affect not only the population, but also the activities of many entities that use potable water e.g. for food production, in agriculture (livestock production) or in health facilities. A disruption in potable water supply may occur as a result of other emergencies or crises. If the cause of the disruption is a common disorder in the water supply network, the situation is addressed by the owner or operator of the water supply and sewage system by providing supplementary supplies. In the event of a large-scale disruption, it is necessary to implement measures ensuring emergency potable water supplies, which are set out in the relevant emergency and contingency plans. Such a situation may also be related to the threat of a deliberate disruption of the water supply system.

V) Large-Scale Disruption of Food Supply

Given the number of producers, manufacturers, and storage facilities, a large-scale disruption of food supply is not very likely. However, it may occur as a secondary consequence of other incidents.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

Basic Documents:

Population Protection Strategy 2020 with an Outlook for 2030 – the document sets, in a broader perspective, further actions in the development of major areas of population protection, such as education and training, capacities, material resources, the tasks associated with population protection, crisis management, science and research. It also includes basic tasks for implementing the set priorities of population protection for the entire period of its validity, including the outlook for 2030.

Environmental Security Strategy 2016 – 2020, with an Outlook for 2030 – the aim of this document is to propose the expansion of existing measures that will lead to limiting the occurrence of crises caused by the interaction of the environment and society (especially serious accidents, natural disasters, and terrorist acts).

Legislation:

The basic laws that apply to all types of anthropogenic threats are:

- Act No. 239/2000 Coll., on the integrated rescue system and on amendments to certain acts
- Act No. 240/2000 Coll., on crisis management and on amendments to certain other acts (Crisis Management Act)
- Act No. 241/2000 Coll., on economic measures in crises and on amendments to certain other acts

Legislation and basic planning documents relating to individual threats:

I) Special floods

- Act No. 254/2001 Coll., on water and on amendments to certain other acts (Water Act)
- Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for community action in the field of water policy
- Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks
- MA Decree No. 471/2001 Coll., on the technical and safety supervision of waterworks
- MA Decree No. 236/2002 Coll., on the method and scope of drafting and determining flood plain areas
- MA Decree No. 24/2011 Coll., on river basin management pans and flood risk management plans

Related documents – the Plan for Protection of Areas near Waterworks against Special Floods, flood risk management plans, regional emergency plans, regional contingency plans

II) Leakage of hazardous chemicals from a stationary device

- Act No. 224/2015 Coll., on prevention of major accidents caused by hazardous chemicals or mixtures and on amending Act No. 634/2004 Coll., on administrative fees, as amended (Act on Prevention of Major Accidents)
- Decree No. 226/2015 Coll., on principles defining emergency planning zones and procedures for their definition, and on particulars of the content of the external emergency plan and its structure
- Decree No. 228/2015 Coll., on the level of processing information to the public, reporting serious accidents, and giving final reports on the occurrence and the impacts of a major accident

Related documents – security programmes, security reports, internal emergency plans, external emergency plans, regional emergency plans, regional contingency plans

III) Radiation accidents

Legislation applicable until 31 December 2016

- Act No. 18/1997 Coll., on peaceful utilisation of nuclear energy and ionising radiation (Nuclear Act) and on amending and supplementing certain acts, as amended
- Government Regulation No. 11/1999 Coll.**,** on emergency planning zones
- Decree No. 146/1997 Coll., specifying activities that directly affect nuclear safety and activities especially important for radiation protection, qualification and training requirements, the method of verification of special professional competencies and authorising selected employees, and on the method of implementing approved documentation for licensing to train selected employees
- Decree No. 106/1998 Coll., on ensuring nuclear safety and radiation protection of nuclear installations during their commissioning and operation
- Decree No. 195/1999 Coll., on requirements for nuclear installations to ensure nuclear safety, radiation protection, and emergency preparedness

- Decree No. 307/2002 Coll., on radiation protection
- Decree No. 318/2002 Coll., on details ensuring emergency preparedness of nuclear installations and workplaces with ionising radiation and on requirements for the content of the internal emergency plan and emergency rulebook
- Decree No. 319/2002 Coll., on the function and organisation of a nationwide radiation monitoring network

Legislation effective from 1 January 2017

- Act No. 263/2016 Coll., Nuclear Act and its implementing regulations (on specifics related to ensuring the tackling of radiation emergencies, on radiation monitoring, on radiation protection, and on ensuring radionuclide sources)

Related documents – internal emergency plans, external emergency plans, regional emergency plans, regional contingency plans

IV) Large-scale disruption of water supply

- Act No. 274/2001 Coll., on water supply and sewer systems for public use and on the amendment to certain acts (Water and Sewage act), as amended
- Act No. 254/2001 Coll., on waters and on the amendment to certain acts (Water Act), as amended
- Plan for development of the water supply and sewage systems in the CR
- Plan for the development of the water supply and sewage systems in the regions
- Methodological instruction of the MA to ensure uniform procedures of regional authorities and authorities in Prague, municipality bodies and boroughs in Prague in ensuring emergency supply of potable water to the population in emergencies and crises by the Emergency Water Supply Service

Related documents – regional emergency plans, regional contingency plans

V) Large-scale disruption of food supply

- Act No. 110/1997 Coll., on food and tobacco products and on amending and supplementing related acts

Related documents – regional emergency plans, regional contingency plans

Responsible institutions and authorities according to individual threats:

I) Special floods

- state administration – MA in cooperation with MoI and ME
- technical and safety supervision

II) Leakage of hazardous chemicals from stationary devices

- chemical substances and mixtures and the prevention of major accidents – ME
- impact of hazardous chemicals on human health – MH

- impact of hazardous chemicals on agriculture – MA
- emergency planning – MoI

III) Radiation accidents

- nuclear safety, radiation protection, emergency preparedness – SONS
- radiation monitoring in the CR – RMN (SONS, MF, MD, MoI, MA, and ME)
- emergency planning – MoI, SONS

IV) Large-scale disruption of water supply

- water management – MA

V) Large-scale disruption of food supply

- state administration – MA

Powers and instruments for tackling anthropogenic threats

Units of the **integrated rescue system** are crucial in dealing with emergencies and crises. The basic IRS units (FRS CR and FPUs ensuring regional coverage, EMS providers and Police CR) ensure a continuous readiness to receive emergency reports, evaluate them, and intervene immediately. For this purpose, their forces are deployed across the CR. Other IRS units provide planned assistance upon request via detached forces and armed forces, armed security forces, other rescue units, public health authorities (e.g. the sanitary service), emergency, expert, and other professional services, civil protection units, non-profit organisations and citizen associations that may be involved in rescue and clean-up operations.

In the area of anthropogenic threats, the Radiation Monitoring Network should also be mentioned. The data obtained are used for evaluating radiation, for purposes of monitoring and assessing radiation exposure and, in case of a radiation emergency, for deciding on measures to reduce or avert the exposure.

In crises or large-scale emergencies, when standard forces are not sufficient for tackling them, the **system for economic measures in crises** comes into play (particularly the crisis management system, the use of state material reserves and regulatory measures). The aim of an emergency economy is to ensure, during a crisis, the necessary supplies to meet the basic living needs of the population, to support the state administration and the activities of rescue forces, emergency services, the emergency medical service, and the Police CR. For this purpose, plans of necessary supplies are drafted at the regional and central level. Regulatory measures in crises serve to reduce consumption of scarce resources and services, or to regulate consumption of resources and services in accordance with contingency plans in situations where the crisis is so serious that usual economic measures are not effective in providing necessary supplies.

Legal persons and entrepreneurs are, of course, also involved in tackling anthropogenic threats. They include particularly those entities that may pose a threat for their surroundings. However, all legal persons and entrepreneurs are obliged, in emergencies or crises, to provide material or personal assistance, and may ensure the implementation of measures stemming from contingency plans and take part in drafting planning documentation.

In the area of management of anthropogenic threats, it is necessary to mention the Transport Information and Emergency System (TIES), which provides – via its centres – nonstop assistance in emergencies linked to transportation and/or storage of hazardous materials.

Evaluation of existing legislation and capacities to tackle anthropogenic threats

Generally, the system for ensuring readiness as well as the actual management of emergencies and crises brought on by anthropogenic threats addressed in this chapter is functional – tried and tested in practice. The relevant legislation is sufficiently addresses the identified threats (the Act on Preventing Major Accidents was updated in 2015 and the new Nuclear Act comes into effect on 1 January 2017).

In order to ensure readiness to tackle emergencies and crises, a number of planning documents have been drafted (see individual threats). Their usefulness has been tested in practice when dealing with concrete incidents.

At the central level, and especially at level of local Governments, there is a shortage of staff dealing with crisis management (LGU employees often dedicate only part of their time to the job).

The number of IRS staff dedicated to tackling anthropogenic threats is satisfactory. However, there is a problem with employee fluctuation (a reduction in the number of positions and the consequent layoffs followed by new recruitment is causing senior employees to leave and disrupts the stability of the system).

Material capacities of IRS units are currently at a good level. Nevertheless, it is necessary to ensure the regular renewal and modernisation of material resources, making it possible to effectively manage the increasing number of emergencies and crises.

The current system of economic measures in crises is a great advantage (especially the emergency economic management system, the use of state material reserves, and regulatory measures), and its usefulness and functionality have been tested during many emergencies and crises. In accordance with new legislation, it is possible to use state material reserves free of charge also for tackling selected emergencies and for eliminating their consequences. What remains problematic is the recurrent disproportion between the approved Plan of Necessary Supplies and the funds allocated to the SMRA for its implementation.

On the other hand, the involvement by legal persons and entrepreneurs (especially those that pose an increased risk to their surroundings) in preparing for emergencies and crises and their tackling, is insufficient.

The deployment of modern technologies to deal with emergencies and crises is imperative in current times. This is related to the necessity of providing a communication environment that is employed by these technologies.

C. SWOT Analysis

Partial SWOT analyses were elaborated for each threat. From these, factors that can be applied cross-sectionally in the area of natural and environmental threat management, were selected and further elaborated in the overall SWOT analysis:

Strengths

- A functional and verified system.
- Existing legislation, methodological guidelines, recommendations at the national and European level.
- Existing planning documentation.
- Professional knowledge and capabilities.
- Material resources created within the System of Economic Measures for Crisis Situations.

Weaknesses

- Insufficient financial resources.
- Staff fluctuation and insufficient human resources at both the central and regional level.
- Lengthy administrative and legal procedures in the implementation of some preventive measures (e.g. building polders).
- Insufficient linkage to territorial planning and construction management.
- Fragmentation of responsibilities in the area of CBRN.

Opportunities

- Compulsory education of the population.
- Security research.
- Technological development.
- Sharing of experiences and conclusions from specific incidents abroad.

Threats

- Staffing restrictions.
- Financial restrictions.
- The insufficient involvement of selected legal persons and entrepreneurs.
- The emergence of large agglomerations involving industrial zones with dangerous facilities.
- The possibility of terrorist attacks.

D. Final Recommendations

1. Ensure an update of the system of population protection as regards anthropogenic threats.[68]
2. Ensure stable staffing of IRS units.
3. Strengthen staffing capacities (professionals in the field of crisis management) at the central and regional levels, so that employees have sufficient capacities to focus on crisis management (to avoid part-time commitment to the issue).
4. Ensure sufficient funds for the preparation and management of emergencies and crises.
5. Increase the responsibility of selected legal persons and entrepreneurs operating facilities that may pose an increased risk for their surroundings (e.g. operators of category IV facilities under the Nuclear Act, operators included in category B under the Act on Prevention of Major Accidents and operators of category I waterworks under the Water Act). Ensure their wider involvement in the preparation for emergencies and crises and their solutions through closer cooperation with relevant public administration authorities and increased participation in the implementation of specific tasks.
6. Increase the co-responsibility of the population for their own safety through compulsory education.
7. Pay particular attention to security research, including a system for sharing information among actors and users of research results.
8. Ensure the consistency of population protection needs with the processes of territorial planning and construction management.
9. Promote the long-term development of communication infrastructure and technologies to be used to prepare for emergencies and crises.

[68] In agreement with the current Population Protection Strategy.

CYBERTHREATS

A. Description and Assessment of the Threat and Associated Risks for the CR

1. Introduction

No state is currently fully immune to cyberthreats, including the CR. The deteriorating security situation not only in the immediate vicinity of the EU and NATO member states exacerbates the increasing demands on the CR's capability to independently react to cyberthreats. There are increasing efforts of state and non-state actors to build and use offensive cybernetic means targeting, in particular, critical infrastructure (CI), i.e. that portion of it which is exposed in cyberspace – critical information infrastructure (CII)[69] and important information systems (IISs)[70]. The latter constitute a key system of elements in the CR whose disruption or dysfunction would have a serious impact on Czech security, the provision of basic living needs of the population, or economics.

This section divides the chapter on Cyberthreats into five specific threats that are of significant importance to national security:[71]

I) Cyberespionage

II) Disruption or the lowering of resilience of IT infrastructure

III) Hostile campaigns

IV) Disruption or the lowering of security of eGovernment

V) Cyberterrorism

Cyberespionage or hostile campaigns in cyberspace are increasingly the work of foreign states or their security structure. Furthermore, the cyberspace activities of criminal, terrorist, and other extremist groups and individuals, that may eventually escalate to cyberterrorism having implications on the lives and health of large numbers of people, are gaining importance.

The CR must, therefore, strive to strengthen the resilience of IT infrastructure in order to minimise the impacts of cyberattacks and to promptly return the infrastructure back to its functional state. Simultaneously, the CR must enforce strict adherence to safety standards for information and communication systems (IS and CS) managed by public authorities and managers of CII and IIS, and to focus, within this effort, on the computerisation of public administration – eGovernment. Severe disruption of its security could halt the digitalisation of public administration, lead to citizens' distrust of this concept, and thus even disrupt or slow down the functioning of the state.

[69] CII is an element or elements of the critical infrastructure (as per Sec. 2(g) and (i) of Act No. 240/2000 Coll.) in the communication and information systems sector of cybersecurity (Sec. 2(b) of Act No. 181/2014 Coll., on cybersecurity and amendments to related acts).

[70] IISs are information systems managed by a public administration body, which are not CII and where breaches of information security may limit or significantly compromise the performance of public authority.

[71] These five threats were assigned along with the Audit.

The abovementioned threats to national security are exacerbated primarily by the phenomenon of cybercrime. Increasingly, perpetrators use the anonymity and special effervescence of cyberspace, which brings fast results at a considerably reduced risk of prosecution.

Links to other chapters in the Audit: this chapter is linked to the chapter on Hybrid Threats and Influence of Foreign Powers as regards parts on cyberespionage and hostile campaigns. Also, it is linked to the chapter on Energy, Raw Material, and Industry Security and includes the threat of cyberterrorism, which complements the chapter on Terrorism.

When assessing the relevance of the threat for the CR in this text, probability and severity of impact criteria were used, whose combination led to the assessment of the threat relevance on a scale of low – medium – high.[72]

2. Classifying Threats

This section is divided into several parts. Because of the complexity and heterogeneity of factors and variables for each specific threat, each threat is firstly described in general terms, followed by a list of the most important risks and problems associated with it, in Part A. The description of the threat and the individual risks and challenges is based on an expert evaluation and consensus at the working group level.[73] Consequently, Part B includes a non-exhaustive list of responsible institutions and basic instruments for eliminating cyberthreats. Part C includes the SWOT analysis with integrated bullet points detailing the main strengths, weaknesses, opportunities, and threats. Finally, Part D includes key recommendations for enhancing national security and resilience against cyberthreats.

I) Cyberespionage

Threat relevance assessment for the CR: **High**

Cyberespionage, as an effort to gain strategically sensitive or important information and personal, sensitive, or classified data without the consent of their holders, is a manifestation of hostility. The attackers target individuals, groups, or organisations working in both the private and the public sector. It is their aim to obtain personal, economic, political, or military advantages through cyberspace, i.e. the internet, social networks and ICTs in general. Individuals, groups, and organisations stand behind cyberespionage. In certain cases, the attacks are directly organised,

[72] When evaluating the severity of impact, the vital, strategic, and otherwise important interests of the CR, as defined by the SS 2015, were considered. In the case of cyberthreats, these interests are: ensuring the sovereignty, territorial integrity, and political independence of the CR, maintaining all the attributes of democratic rule of law, including the guarantee and protection of basic human rights and freedoms. Furthermore, they include ensuring internal security and public protection, ensuring economic security of the CR and strengthening economic competitiveness via a secure cyberspace, and primarily via ensuring cybernetic defence of the CR, along with the prevention and suppression of security threats in cyberspace affecting the security of the CR and its allies. As regards the criterion of probability, we considered experience from abroad, as well as the analysis and experience of the activities of national subjects in cyberspace, alongside experience with the frequency and method of cyberattacks, their causes and motives. Furthermore, we considered vulnerability of certain targets and the ease of carrying out an attack on them. The working group agreed that these factors cannot be quantified mathematically, and the final assessment is therefore the result of an expert evaluation and consensus at the working group level.

[73] There is some overlapping and partial duplicity of some risks and challenges among the threats, which is given by the complexity of the cybersecurity topic, where individual challenges and risks inevitably simultaneously affect several assessed threats.

supported, used, or at least tolerated by some state actors. The boundaries between attackers who commit cybercrime and cyberespionage are often very vague or non-existent.

Cyberespionage is associated with the “advanced persistent threat” (APT), which is much more sophisticated than traditional cyberattacks. The ATP uses such techniques and attacks those vulnerabilities that are difficult to discern for commonly used detection methods and tools. These activities remain undetected for long periods of time and in specific cases it is very difficult to trace and identify the real perpetrators. The exfiltration of information and data may therefore take place continuously over several years, i.e. until the threat is detected and eliminated.

The significance of the threat of cyberespionage is reflected in the number of cases and the increase in the risk of the use of cybernetic tools for attacks on the public and private sector. The growth in this trend is due to easier access to sophisticated cyberespionage tools, the professionalisation of attackers, the building of offensive capabilities by both state and non-state actors in the field of cybersecurity, the computerisation of many everyday activities as well as the global political climate.

Cyberespionage may be one of the early signs of preparation for a cyber or kinetic attack or conflict, or be part of a hostile campaign where, apart from gathering strategic and sensitive information, key infrastructure, which may be the target of a later attack, is mapped. The response to cyberespionage requires the deployment of special resources and procedures in order to minimise existing and potential damages. Tackling these kinds of incidents requires cooperation across ministries dealing with cybersecurity, as well as the support and cooperation of individual actors.

The CR and its institutions have repeatedly been the targets of cyberespionage, and we may assume that undetected advanced persistent threats are currently underway in the CR, which are harmful to national interests. Due to the frequency of cyberespionage and its potentially serious consequences for national security, the relevance of this threat can therefore be assessed as high. The victims are usually state authorities and their representatives, but also institutions dealing with education, research and development, operators of ISs and CS CIIs, administrators of IISs, security forces, as well as a number of other organisations. Similarly, cyberespionage relates to the private sector, where it serves primarily as a means of competition and is the means to serious theft of intellectual property and industrial espionage.

Specific Risks and Challenges:

- In many organisations, insufficient financial resources are allocated for cybersecurity, and cyberthreats are underestimated.
- Some ICT manufacturers or distributors who have ties to the Government and security forces of other states participate directly or indirectly in cyberespionage.
- In many organisations, solutions to cybersecurity are outsources, which expands the circle of potential risk carriers.
- In many organisations, cybersecurity is only addressed at the operational level, i.e. not comprehensively and systematically.
- With the advancement of the Internet of Things, the cybersecurity of non-traditional devices newly connected to cyberspace is insufficiently addressed.
- Many organisations have not created or adequately set up a realistically applicable cybersecurity policy.
- Organisations may be infiltrated and sensitive data may be compromised via insufficiently screened or qualified staff or experts, acting consciously or unconsciously in favour of third parties.

- Many organisations do not pay enough attention to education and awareness of staff in the field of cybersecurity, i.e. relevant employees are lacking in IT literacy.
- The purchase of ICTs takes place via insufficiently screened intermediaries and without knowledge of the product chain, which may contain backdoors (both in software and hardware) allowing the exfiltration of information.
- Sensitive information is at risk of unauthorised use due to the use of private means (PCs, mobile devices, email) for work purposes or the inappropriate and inadvertent handling of work resources (data carriers and mobile devices).

II) Disruption or the Lowering of Resilience of IT Infrastructure

Threat relevance assessment for the CR: **High**

In an environment of ever-changing cyberthreats that can emerge from a dynamically developing cyberspace, the CR must create a secure and trustworthy cyberspace and a resilient IT infrastructure. For this purpose, the state must constantly build and increase national capacities in this area, bearing in mind that the necessary efficiency of these activities cannot be achieved without cooperation with the private and academic sectors, without intensive international cooperation and especially not without the involvement of the population.

The resilience of IT infrastructure means the capability of the entity to maintain an acceptable level of services and to quickly adapt and respond without regard to arising problems and complications. Due to the high number of eventualities and factors that may cause the disruption of the IT infrastructure (technical failures, human errors, natural disasters, cyberattacks, etc.); it is important to create an efficient system of recovery for the IT infrastructure following a disaster or attack.

Due to the increasing frequency and sophistication of cyberattacks, it is necessary to continually increase the resilience of Czech IT infrastructure, especially that of CI and IISs. Because of the high number and frequency of eventualities and factors that may cause the disruption not only of the critical part of the IT infrastructure, and because of the increasing robustness and complexity of the entire IT infrastructure, the relevance of the threat of disruption of the resilience of the IT infrastructure must be assessed as high. It is thus necessary to continually increase both the organisational and the procedural and technical capabilities and capacities, and thus strengthen the overall resilience of the IT infrastructure in the CR.

Specific Risks and Challenges:

- The risk of an attack on the CII and IISs via cyberespionage, cyberterrorism, criminal organisations, hacktivists, and others.
- Insufficient financial resources for ensuring the necessary technical courses and for hiring security screened ICT and cybersecurity experts.
- The chemical industry and other strategic branches are not included in the critical infrastructure and their selected ISs and CSs cannot be included in the CII. For healthcare facilities, there is no criterion in the relevant Government resolution allowing for the inclusion of some of their ISs and CSs.
- State and public administration employees are not sufficiently aware of cybersecurity; they lack education and do not respect the basics of digital hygiene.
- Unsystematic security testing.

- Attacks on the IT infrastructure via production, supply, and subcontractor chains. In terms of the acquisition process, there are limited possibilities of awarding IT and security solutions tenders to screened suppliers and subcontractors or the impossibility of refusing suspicious suppliers and subcontractors.
- Poor prioritisation of some ministries and institutions when planning investment in security technologies and other ICTs.
- Insufficient legislative regulation of cybercrime, i.e. the problem of detecting perpetrators and consequently providing evidence related to inadequate legislative means for the collection, filing, and use (in court) of electronic evidence.
- Healthcare facilities, the chemical industry, and other strategic branches are not included in the critical infrastructure, and their selected ISs and CSs cannot thus be included in the CII.
- In many cases, dated systems are maintained, whilst the costs incurred by their operation and maintenance often exceed investments in new, more secure technologies.
- Cybersecurity solutions, i.e. the securitisation and overall maintenance of ICTs, are outsourced, and the "locked-in" model without an "exit" plan and a related replacement plan is prevalent, which is related to the problem of managers and operators being ignorant of security levels.
- Fragmented systems of means of communication within the Government, hindering adequate, efficient, and timely maintenance, security and control.
- The non-existence of central methodologies for the use of ICT instruments, especially mobile devices, which currently pose an ever-increasing risk.
- The absence of an obligation to use secure (commercially encrypted) email and other electronic communication between Government institutions and civil servants.
- Current legislation (Act No. 234/2014 Coll., on civil service) makes it difficult for some institutions to hire IT specialists.

III) Hostile Campaigns

Threat relevance assessment for the CR: **High**

A hostile cyber campaign poses a number of various interconnected operations aimed at a specific strategic objective or outcome. It is a period when a series of planned and coordinated (cyber) attacks or other operations in cyberspace take place. These campaigns can be carried out by individuals, or they can be the result of a concerted effort by several actors (most often state or state-sponsored or organised). A hostile cyber campaign can be defined and framed according to its purpose, i.e. achieving a certain predetermined objective in cyberspace; according to its defined resources (technologies, actors, location); or according to its course through time. In real conditions, campaigns or their parts are often "recycled", because the development of ever-new tools and procedures for attacks and other actions in cyberspace is a relatively costly and time-consuming process.

Cyberspace and ICTs play a significant role in hostile campaigns. We can already observe the systematic influence of foreign powers, i.e. hostile campaigns in cyberspace, in the CR. The means and methods of combating them are currently not adequately efficient. Due to real risks, and potential impacts, the relevance of this threat can be assessed as high.

Specific Risks and Challenges:

- Influence and disinformation media campaigns on the internet may have a major impact on public mood, which poses a high risk of causing social unrest.
- Influence and disinformation media campaigns on the internet organised by interest groups, organised criminal groups, or foreign intelligence services. In the CR, such information is disseminated by both established and new internet media outlets.
- The environment of social media is frequently used, due to their international aspect and a different approach to freedom of speech. For this reason, it is possible to make ample use of them for the purpose of disseminating hate and disinformation campaigns against certain population groups as well as against Government bodies or Czech foreign policy, for the purpose of achieving military, political, or economic goals.
- Problematic factors include the ownership of structure of specific Czech internet media outlets that may follow different private interests, or the interests of other states, in their reporting.
- Organised crime makes use of the possibilities of cyberspace named above in order to undermine the credibility of security forces.
- Insufficiently screened staff or experts working (albeit unconsciously) in favour of third parties, who have access to strategic assets, may, via exfiltration of sensitive and otherwise important information and data, seriously threaten national security.
- Current legislation on free access to information (Act No. 106/1999 Coll.) may threaten Czech cybersecurity, i.e. it may be abused in the context of hostile campaigns. Specifically, this legislation makes possible requests for information regarding elements of the CII or the communication between the NSA and relevant bodies discussing aspects affecting the security of the systems in question.

IV) Disruption or the Lowering of Security of eGovernment

Threat relevance assessment for the CR: **Medium**

The idea of eGovernment is the use of modern electronic tools for the purpose of public administration, making it more accessible to citizens, more efficient, faster, and cheaper. A key project of the Czech eGovernment is a network of public administration contact points – Czech POINT – which are now almost in every village. Thanks to them, citizens may obtain a number of documents and use the services of several different offices in one place. Furthermore, a data exchange system has been set up as a tool for guaranteed electronic communication with the Government. Finally, a system of basic registers containing current data that offices no longer need to request from citizens has been set up.

The use of eGovernment is becoming increasingly important. For such complex and demanding systems to operate, it is necessary to create a robust and particularly secure infrastructure. The continuing digitalisation of public administration in the CR serves to improve the functioning of public administration and its rapport with the public. However, services and applications provided to citizens and private enterprises via eGovernment carry certain cybersecurity risks. The individual eGovernment systems work with enormous amounts of managed and processed important data.[74]

[74] Czech Point, data boxes, EiDAS, SIS, VIS, ISZR, STC, and eSbírka (electronic acts) and eLegislativa (electronic legislation).

The security of eGovernment may be compromised not only by inadequate handling of information and data, but also by an external threat, i.e. cyberattacks. An extensive disruption of the cybersecurity of individual eGovernment projects, i.e. their data and information, could lead to the distrust of citizens in the entire eGovernment concept and halt the use of its services by the public. A failure of the eGovernment system would therefore be critical.

Despite the attractiveness of this objective, and the possible serious consequences of the failure of any eGovernment system or the disruption of its data and information, most cyberattacks linked to this concept are not severe, and a change in the near future cannot be predicted with certainty. Therefore, the relevance of the threat, especially as regards the serious consequences of a failure of the eGovernment system, can be assessed as medium.

Specific Risks and Challenges:

- Insufficient funding of cybersecurity, insufficient financial remuneration of staff and number of staff in the field of cybersecurity, as well as the underestimation of cyberthreats in the state administration.
- Inadequate security of state administration ISs and CSs used for communication between the citizens and the state. This concerns systems that ensure the performance of state administration for Czech and EU citizens.
- Poorly set cybersecurity policies and inadequate of employees in state administration as regards cybersecurity.
- Insufficient awareness and education of the public regarding cybersecurity and eGovernment as such.

V) Cyberterrorism

Threat relevance assessment for the CR: **Medium**

The NSA defines cyberterrorism as follows: *"Cyberterrorism incorporates aggressive and excessive behaviour, which is done with the intention of causing fear in society, and which aims to achieve political, religious, or ideological goals. Through the use of cyberspace and ICTs, it threatens the functioning of the state, its constitutional order, or its defence capabilities,* inter alia *by targeting critical information infrastructure and important information systems."*[75]

In a narrower sense, only those terrorist activities in cyberspace that cause widespread disruption of computer networks or devices with severe or fatal consequences can be considered as acts of cyberterrorism. These attacks may cause deaths or, when the economy is compromised, very serious economic losses with unpredictable consequences. However, the state must also defend itself against other terrorist activities that take place in cyberspace, such as incitement to hatred or the creation and dissemination of propaganda. So-called new media play an important role in this regard.

Cyberterrorism can no longer be considered a hypothetical phenomenon and it is likely that cyberterrorist attacks will take place in the near future. Currently, a considerable number of cyberattacks and incidents, often widely covered by the media and described as cyberterrorism, can be more precisely described as the use of cyberspace, i.e. the internet, by terrorists.

[75] In the absence of a definition of cyberterrorism in the CR, the NSA created an entirely new one for the purposes of the Audit.

For now, terrorist organisations do not have sufficient capacities and capabilities to carry out cyberattacks with serious or fatal consequences. On the other hand, it is not difficult to purchase these capabilities as a service, which is substantiated by the heightened activity and interest in this form of terrorism, especially of the so-called Islamic State. Recently, this organisation managed to carry out cyberattacks (however unsophisticated) that other terrorist organisations have been unable to carry out at all for a very long time.

As regards the CR, the relevance of the threat of cyberterrorism can be assessed as medium, not low. The CR is in a different position from that of Western European countries and the USA, similarly to its position with regards to terrorism stemming from Islamic fundamentalism and radicalism. On the other hand, the so-called darknet is used in the CR for illegal activities aimed at high political representatives and for using stolen email communication in order to discredit certain other representatives, in an attempt to influence public opinion. Furthermore, some partially successful attempts at Denial of Access to websites or services, or even the social profiles of political entities or media outlets, were recorded. Such situations will most likely occur repeatedly in the future, and the level of their severity may escalate.

Specific Risks and Challenges:

- The possibility of a coordinated cyberattack:
    - In order to blackmail state authorities, business corporations, or frightening society;
    - On IRS units and communication systems of operators;
    - In order to destroy specific technologies/systems (usually in connection with CII and ICS or SCADA[76] systems);
    - On energy distributors or service providers, with the aim of discontinuing the service (usually an energy blackout) and others.
- Cyberattacks aimed at gathering sensitive intelligence for the purpose of using it during a kinetic terrorist attack, e.g. information regarding the selection of targets or the preparation of an attack, or the support for the disorientation or destruction of an enemy entity, which can be directly related to planned military or terrorist kinetic activities.
- Terrorists make ample use of ICTs to disseminate propaganda as well as documents supporting the radicalisation of followers and their recruitment. They mainly use various social networks and communication platforms (including those that are protected by encryption) as strategic information platforms.
- Terrorists use cyberspace to manage sympathisers, especially as regards calls to action against possible targets, planning operations, providing feedback, and learning from past activities or attributing merit for past operations.
- Terrorists publish the private information (obtained by online searching or theft) of persons of interest (for terrorist and extremist organisations) on the internet and incite hatred against them so as to make them the targets of attacks perpetrated by so-called lone wolves and others.
- The low readiness of security forces for the specifics of a digital environment and operations within it. There are not enough ICT experts in security forces, and in many cases there is also a language barrier.

[76] ICS – Industrial Control Systems; SCADA – Supervisory Control and Data Acquisition systems.

- The low readiness of security forces for the so-called darknet (or deep web, i.e. the hidden internet), which is increasingly being used by organised criminal groups and terrorists.
- A low rate of obtaining experience from foreign partners, who have long-term practical experience, especially in the area of education.
- Insufficiently screened staff or experts working in favour of third parties, who have access to strategic assess, may, via exfiltration of sensitive and otherwise important information and data, seriously threaten national security.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

Basic Documents

The basic document for cybersecurity in the CR is the SS 2015, which serves as a basis for the National Cybersecurity Strategy 2015 – 2020 – a fundamental document regulating the strategic framework of cybersecurity in the CR. The Strategy, in turn, serves as a basis or the Cybersecurity Action Plan 2015 – 2020, which defines specific tasks and determines responsibilities, deadlines, and oversight. The NSA regularly monitors, discusses, and evaluates the implementation of the Strategy and the Action Plan in cooperation with all relevant stakeholders. Within the annual Report on Cybersecurity in the CR, which informs the Government on the state of ensuring cybersecurity, the NSA drafts a report on the progress in implementing the Action Plan, which is attached to the Report.

In the area of cybercrime, tasks are gradually being completed that stem not only from the Strategy and the Action Plan, but also the Strategy for Developing Capabilities of the Police CR in Investigating Computer Crime by 2020.

Based on the Strategy and the Action Plan, new capacities are also being developed in cyberdefence within the MInt. Finally, with regard to the issue of eGovernment, the Strategy for Developing ICT Services within Public Administration and the measures it proposes to streamline ICT services should also be mentioned.

Legislation

In the area of cybersecurity, the CR has unique legislation in the form of Act No. 181/2014 Coll., on cybersecurity and the amendment to related acts and its implementing legislation – Decree No. 317/2014 Coll., on important information systems and their defining criteria and Decree No. 316/2014 Coll., on security measures, cybersecurity incidents, response measures and the determination of requirements for reporting cybersecurity incidents (the so-called Cybersecurity Decree). Furthermore, Government Regulation No. 432/2010 Coll., on criteria for defining an element of critical infrastructure (the amendment was published in the Collection of Acts under No. 315/2014 Coll.).

All crimes, including those committed in the cybernetic realm, are regulated by Act No. 40/2009 Coll., the Criminal Code, as amended. The majority of cybercrimes relate to crimes against the confidentiality, integrity, and availability of computer data and systems, as defined in Chapter V on crimes against property. Crimes committed in relation to data (stored information) are mainly the following:

- Unauthorised access to a computer system and data carrier (Sec. 230),
- Obtaining and storing access and password to a computer system and other such data (Sec. 231),
- Damage to a record in a computer system and data carrier and interference with a computer due to negligence (Sec. 232).

Interception of data is regulated by Sec. 182 among crimes against the rights to protection of a person, privacy, and secrecy of correspondence.

As regards cyberdefence, the interministerial comment procedure is currently underway relating to a proposal for legislative changes that are necessary in order for the MInt to carry out cyberdefence. Until these legislative changes are approved, the MInt performs its tasks in accordance with its established powers and priorities set by the Government, and consisting solely in providing relevant information important for national defence and security.

Responsible Bodies

National Security Authority

In the CR, the Government body responsible for cybersecurity is the NSA. As of 2011, it is responsible for cybersecurity and is the national authority in this field (as per Government resolution No. 781/2011). In 2014, the Cybersecurity Act charged the NSA with carrying out state administration in the field of cybersecurity. Based on the adopted resolution, the National Cybersecurity Centre (NCKB) was established within the structure of the NSA, with its headquarters in Brno. The role of the NCKB is primarily to coordinate cooperation at the national and international level in preventing cyberattacks and to propose and adopt measures to tackle incidents and ongoing attacks. The Government CERT (GovCERT.CZ), which plays a key role in protecting CII and IISs as per the Cybersecurity Act, operates within the NCKB. The act in question also introduced the national CERT[77], which is currently operated by CZ.NIC based on a public contract with the NSA.

Ministry of the Interior

The MoI is responsible for internal security and public order. In terms of cybersecurity, it plays a key role as the main guarantor of the computerisation of public administration (eGovernment) and is responsible for the operation of a wide range of important information and communication systems that are important for the functioning of state administration (basic registers, data boxes, Czech POINT system, CMS, etc.), as well as for the IRS (e.g. the 112 hotline, the PEGAS system). In the future, all these systems will gradually be connected to the eGovernment monitoring centre (DCeGOV), which is currently already monitoring some IISs and the CII.

Police CR

The Police CR, as the largest security force, forms one of the basic pillars of Czech internal security. In combating threats in cyberspace, an irreplaceable role belongs to the law enforcement

[77] Bodies and persons listed in Sec. 3 (a) and (b) of the Cybersecurity Act are responsible to the national CERT.

authority whose task it is to search, detect, and investigate cybercrime. The essential prerequisites for achieving this goal include adequate staffing and material equipment, a targeted system of education and professional training, as well as a legislative framework allowing a prompt and efficient response to cybercrime, including securing evidence from information stored in cyberspace. The department responsible for investigating cybercrime within the Police CR is the National Centre against Organised Crime of the Criminal and Investigation Police Service, as well as regional police directorates of the Police CR.

Ministry of Defence

The MD ensures cybersecurity of ministerial communication and information systems, as well as military networks.

The MD is responsible for minimising the impacts of cyberthreats in cases where these threats may threaten the functioning of the Czech Armed Forces:

- The use of cyberattacks as part of military or hybrid campaigns;
- Cyberespionage aimed at obtaining military information;
- Hostile campaigns and influence of foreign powers in cyberspace for the purpose of achieving military objectives.

The MD is also responsible for the fulfilment of commitments in the area of Cyber Defence, stemming from membership in NATO and the EU, in the planning, development, and capacity-building of the Czech Armed Forces.

Ministry of Foreign Affairs

The MFA, in cooperation with the NSA and some other ministries, is involved in the successful implementation of specific tasks set by the Action Plan of the Strategy, particularly in relation to international organisations and selected states. The MFA also considers cyber issues as a topic of Czech foreign policy.

Intelligence Services

The basic mission of the SIS, OFRI, and MInt is gathering and evaluating information with the purpose of detecting threats to the interests and security of the state and its inhabitants. Intelligence services thus also collect and analyse information on threats and risks in cyberspace. They participate in ensuring cybersecurity of the CR particularly by providing intelligence to competent state authorities.

The MInt, as part of the MD, is also responsible for cyberdefence of the CR based on the approved Strategy and Action Plan, and is currently developing a National Cyberforces Centre (NCKS), which will, in the future, perform a wide scope of operations in cyberspace and other activities necessary for ensuring cyberdefence of the CR.

C. SWOT Analysis

Strengths

- A functioning fundamental legal and legislative framework for managing cybersecurity.
- Adequate capacities of the NCSC, i.e. the Government CERT (Gov.CERT.CZ).
- Excellent international cooperation in the area of cybersecurity, especially among CERT/CSIRT teams.
- A large number of CSIRT/CERT teams in the CR and efficient cooperation within the community.
- Development of the National Centre for Cybernetic Forces for the management and resolution of major cyberattacks within the concept of cyberdefence.
- An updated and supported strategic national cybersecurity framework.
- Efficient implementation and annual evaluation of the Strategy, i.e. its Action Plan.
- An effective model of cooperation in cybersecurity among security authorities, intelligence services, and other key national stakeholders.

Weaknesses

- Limited financial resources of individual organisations that could be used for the prevention and management of cyberthreats.
- A lack of qualified ICT and cybersecurity specialists and the inability to provide these specialists with adequate financial remuneration.
- Poorly set cybersecurity policies, the neglection and underestimation of cyberthreats in state administration. Long-term underestimation of staff education in the area of cybernetic security and insufficient IT literacy of relevant state administration employees.
- Some strategic industries are not and cannot, under existing legislation, be included in the CII system.
- Legislation on the issue of public procurement does not reflect cybersecurity requirements, and may, in fact, create or strengthen cybersecurity risks.
- Legislation providing free access to information to Czech citizens does not reflect cybersecurity requirements and may, in fact, create or strengthen cybersecurity risks.
- Legislative shortcoming in the issue of investigating cybercrime.
- The absence of a mechanism for systematic complex evaluation of incidents and activities that would lead to the detection of a potential hybrid campaign.[78]

[78] This topic is further discussed in the chapter on Hybrid Threats.

- A low level of preparedness of security forces for the phenomenon of cyberterrorism and other terrorist activities in cyberspace.
- Insufficient regulation of relations between CII and IIS administrators on the one hand and contractors and subcontractors of ICT services on the other hand.
- Insufficient participation of members of security forces in the darknet, as well as their inadequate knowledge of this environment.
- A weak security awareness of the population of e-Government services, which can be exploited by perpetrators of cyberattacks.
- Varying staffing policies with regards to the cybersecurity agenda in state and public administration, where ICT employees work under three different legal provisions – Act No. 234/2014 Coll., on civil service, Act No. 262/2006 Coll., Labour Code, and Act No. 361/2003 Coll., on the service of members of security forces.

Opportunities

- Motivate ICT and cybersecurity experts to work in state administration by providing adequate conditions – not only financial.
- Deepen and expand existing international cooperation in the area of cybersecurity based on the above standard reputation of the CR and its expertise in this field.
- Participate more actively in international projects and activities in the field of cybersecurity, cybercrime, and cyberdefence.
- Standardise staff training in the field of cybersecurity and digital hygiene at all levels of state authorities.
- Create a central training facility for high quality technical training of ICT and cybersecurity experts.
- The opportunity to learn from the experiences of Western countries as regards preparations for the era of cyberterrorism, without currently facing the imminent danger of cyberterrorism in the CR.
- Address the security of the supply chain with regard to manufacturers and suppliers that supply unsecured hardware and software.
- Amend relevant laws relating to cybersecurity, cybercrime, and cyberdefence.
- Build an overarching mechanism for the evaluation of potential hybrid campaigns (coordinated by the Office of the Government).[79]
- Identify the bodies that will fulfil the role of national partners to the "Hybrid Fusion Cell" of the European External Action Service (EEAS) for effective cooperation not only in the field of cybersecurity.[80]

[79] A concrete solution will be formulated on the basis of the conclusions of the working group created within the NSC system by the Office of the Government to implement the conclusions of the Audit in the field of hybrid threats; the purpose of this group will be to find consensus on the specific form of the supraministerial platform for the exchange of information relating to hybrid threats and for the coordination of communication between relevant bodies.

[80] This issue is further discussed in the chapter on Hybrid Threats.

- Strengthen the NCSC in terms of staff and technologies and thus more frequently perform cybersecurity audits, IS and CS testing (i.e. IT infrastructure resilience testing) at relevant facilities, and provide methodological and other support to all (also non-critical) entities in the CR.
- Create a platform bringing together top ICT and cybersecurity experts from the public, academic, and private sector in order to support the resilience of CR's IT infrastructure.
- Strengthen security forces (in terms of staff and finances) by hiring specialists dedicated specifically to the issue of cybersecurity, cybercrime, and cyberdefence, and continuously train them with regards to the specifics of phenomena associated with these areas.
- Develop a secured communication platform for the public and state administration.

Threats

- An exponential increase in the number of cyberattacks and their potential targets, including vectors of attacks and security vulnerabilities.
- The influence of foreign powers in the CR via cyberspace and cyberattacks as a method of hybrid warfare.
- Easier access to sophisticated tools for carrying out cyberespionage, the professionalization of attackers and the building of offensive capacities by state and non-state actors in the field of cybersecurity.
- A lack of qualified personnel in the area of cybersecurity and ICT as a *sui generis* threat.
- Outsourcing cybersecurity solutions, i.e. the security and overall management of ICT, thus widening the circle of potential culprits.
- Insufficient screening of personnel and qualified ICT personnel working for the benefit of third parties (insider threat) and insufficient screening of contractors and subcontractors of ICT products.
- Hostile campaigns sponsored by state actors through lobbies and disinformation media campaigns carried out in cyberspace.
- The abuse of cyberspace by interest groups and terrorists for their own benefits, advantages, propaganda, incitement of discontent or hatred in society or radicalisation.
- Back doors (implemented in software and hardware) used for exfiltrating information and data.
- The threat of a serious breach of security within the eGovernment project.

D. Recommendations to Strengthen Resilience

1. Strengthen security forces in terms of staffing by hiring more specialists dedicated specifically to the issue of cybersecurity, cybercrime, and cyberdefence.
2. Strengthen security forces in terms of financing by supporting new security projects, technological development, and deepening or expanding current skills and capacities, ad by supporting and developing awareness-raising events and other educational projects.
3. Carry out certain amendments to current legislation in the field of combating cybercrime. In particular, focus on the question of internet user anonymity and the associated search

for perpetrators of illegal activities through the possible addition of further instruments to the Act on the Police CR.

4. Prevent the shortage of qualified personnel in the area of cybersecurity via:
    a. The elaboration of measures to increase the number of cybersecurity experts in the CR. These should be followed by the improvement of remuneration of key employees and by the creation of working conditions enabling the state to bring in and retain candidates.
    b. An amendment to Act No. 234/2014 Coll., on civil service, so as to simplify the hiring of high-quality ICT and cybersecurity experts in state administration.
    c. The expansion of cybersecurity education at secondary schools and especially at universities.
5. Incorporate important sectors such as the chemical industry, medical facilities, and other strategic industries into the CII system via:
    a. An amendment to the crisis management act and Government Order No. 432/2010 Coll., on criteria for determining elements of critical infrastructure that would allow the incorporation of important sectors among CI sectors, through which the CII system is determined.
6. Adequately regulate relations between CII and IIS administrators on the one hand and ICT service contractors and subcontractors on the other hand.
    a. The NSA has already proposed a solution to this issue within the interministerial comment procedure on the draft of a legislative proposal amending Act No. 365/2000 Coll., on state administration information systems and other acts, as amended, which has been submitted by the MoI (MV-165721/LG-2015) for further legislative comments to the Government Legislative Council; the NSA proposed a change in this field as well as an amendment to Act No. 181/2014 Coll.
7. Regulate the issue of the Act on Free Access to Information (No. 106/1999 Coll.) in relation to cybersecurity by either:
    a. amending the scope of Act No. 106/1999 Coll., or
    b. extending the obligation to maintain confidentiality, as regulated by the CYSA, to selected aspects of security measures, and extend this obligation to IS and networks operators and administrators falling within the substantive scope of this act (at the moment, the obligation to maintain confidentiality applies only to records of incidents kept by GovCERT.CZ). This would result in security-related information being exempted from the scope of Act No. 106/1999 Coll., without the need of interfering in its structure.
8. Reduce cybersecurity risks associated with the Act on Public Procurement (Act No. 134/2016 Coll.), i.e. prevent the disclosure of tender documentation to third parties and allow, in some specific cases, to exclude candidates due to security risks on their part.
    a. Tenders for the supply of ICTs cannot *a priori* be exempted from the competence of the act. However, it is necessary to legislatively provide for situations where cybersecurity of individual CII and IIS should be superior to open competition so that CII and IIS administrators may have the opportunity to manage risks in the manner dictated by CYSA. It is also necessary to reach an agreement with the MRD and the Office for the Protection of Competition on the issue of guaranteeing the requirements posed by CYSA with those of open competition.

ENERGY, RAW MATERIAL, AND INDUSTRY SECURITY

ENERGY SECURITY

I) A Large-Scale Disruption of Electricity Supply

A. Description and Assessment of the Threat and Associated Risks for the CR

The most likely cause of a large-scale disruption of electricity supply is an unpredictable and uncontrollable excess of electricity, a technical failure, a natural disaster, a cyber- or terrorist attack, most notably at the level of the transmission system. Recent studies and continuous monitoring indicate that the probability of a large-scale disruption of electricity supply is quite low. Nevertheless, outages lasting several hours have occurred in the past, e.g. in Prague. In this regard, it is necessary to note that, in the event of a large-scale outage in the entire country, it is very probable that the entire region of Central Europe would be affected, as well as parts of Western Europe. Conversely, the interconnectedness of electricity grids of individual states and their synchronised operation enables the spill-over of crises into the CR from neighbouring or from other European countries. If the cause of the outage was “simply” a disproportion between electricity production and consumption, it would most probably be possible to renew the functioning of the electricity grid in a matter of hours. However if, for instance weather conditions caused the mast of a transmission system to fall, or if a terrorist attack seriously damaged or destroyed power lines, a significantly longer period would most likely be needed to restore service. In this regard, it would probably be necessary to find alternative routes of providing electricity as quickly as possible. Entities that are important for the functioning of the state and for ensuring basic vital needs of the population and entities of critical infrastructure should have replacement power supplies installed in their facilities. It should however be noted that not all of these entities have them and those that do will only be able to use them for a limited time (around 6 – 8 hours). Although diesel generators are ready to deliver electricity within several seconds, fuel supplies usually last – depending on consumption – at most 8 hours. This means that if an outage lasted for 4 – 5 hours, everything should be alright, but if it lasted for several days, a huge logistical problem would arise in relation to the supply of fuel. It follows that, after approx. 8 hours, most diesel generators would be inoperative. A solution would be to have legislation impose having alternative power sources and maintaining sufficient fuel reserves (e.g. in Austria it is 72 hours).

Cyberattacks on the energy sector are ever more frequent. The nature of this threat is also changing, and energy companies across the world are faced with much more intelligent and complex cyberattacks. Given the trend of openness and interconnectedness of critical industrial control systems (ICS) and SCADA with other IT systems in order to ensure greater efficiency and lower costs, the risk is growing. Moreover, it is not only the energy sector that uses ICS/SCADA systems with a long service life, which eventually cease to meet the cybersecurity requirements. The consequences of attacks on the energy sector can be disastrous. Coordinated cyberattacks on the electricity network in Ukraine in December 2015, which caused an outage lasting several hours in tens of thousands of households, clearly demonstrate the threat.

Should the power system be physically attacked, serious problems could ensue, but only in the case of, for example, multiple terrorist attacks. For this reason, an analysis of the impact of multiple terrorist attacks on the power system, thereby causing a large-scale disruption or discontinuation of its functioning as a result of intentional human activity, was elaborated. Several sensitive places were identified that, if attacked simultaneously on a critical day when the power lines are fully used, and in combination with shutdowns in the implementation of the planned investment programme, could cause large-scale outages of electricity supply. The elaboration of the analysis enabled the assessment of existing security documents with the aim of improving conditions for a rapid and efficient intervention of IRS units (minimise arrival time and responses to “distress” calls; improve emergency communication; standardise security practices and procedures).

1. At present, the most likely possible cause of an outage would be the unexpected spill-over of a large amount of electricity, particularly from northern Germany, where intermittent sources of great power are situated. Electricity from these sources is transmitted to points of consumption in southern Germany and in Austria, partly through the Czech transmission system (see, for example, the emergency in the Czech transmission system caused by an oversupply by wind parks in Germany at the turn of 2014-2015). Another cause of unplanned power flows that may threaten the security of the Czech transmission system is the non-existence of a coordinated mechanism for the allocation of transborder capacities at the German-Austrian border. The joint German-Austrian commercial zone allows *de facto* unrestricted business exchanges that exceed the physical capabilities of the interconnected systems of Germany and Austria. Such an outage of electrical power would be manageable in a matter of hours, due to the activation of electrical protection, thus leaving transmission system devices intact.

In the case of an accumulation of failures or attacks at multiple locations and the subsequent disintegration of the transmission network, the timely recovery of electricity supply for all big agglomerations must be guaranteed. One of the tools defined in the National Energy Policy therefore requires the elaboration of a national programme aimed at improving energy resilience and the ability of large agglomerations to operate as islands. Priorities set by the National Energy Policy also include the addition, to regional energy policies, of ensuring the security of island operations in emergencies, which are currently being implemented as per the Energy Management Act.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

Responsible institutions: MIT, ERA, SEI, NSA

Basic tools (legislation): Act No. 458/2000 Coll., on business conditions and public administration in energy sectors (Energy Act); Decree No. 79/2010 Coll., on the dispatch power system management and data transmission for dispatch management; Decree No. 80/2010, Coll., on emergencies in electricity industry and the required content of an emergency plan; Decree No. 401/2010 Coll., on the required content of the Rules for the Operation of the Transmission System and Rules for the Operation of the Distribution System; Act No. 181/2014 Coll., on cybersecurity and the amendment of related acts; Decree No. 316/2014 Coll., on security measures, cybersecurity incidents, response measures, and establishing requirements in the field of cybercrime reporting.

Basic tools (EU strategies): Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investment and Regulation (EU) No. 347/2013 of the European Parliament and of the Council of 17 April 2013 on guidelines for trans-European energy infrastructure and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank – A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy (2015).

Basic tools (Czech strategies): National Energy Strategy, Standard Plan for a Large-Scale Disruption of Electricity, National Cybersecurity Strategy 2015-2020, Action Plan to the National Cybersecurity Strategy 2015-2020.

C. SWOT Analysis

Strengths

- High quality and reliability of electricity supply.
- A relatively favourable indicator of dependency on energy import.
- Full self-sufficiency in the production of electricity and heat.
- Legal regulation of cybersecurity ICS/SCADA[81] in the energy sector.
- Production of electricity/heat that is a primarily/significantly based on domestic reserves.

Weaknesses

- An ageing resource base and network infrastructure.
- A high standard and quality and reliability of supply that is taken for granted.
- The use of outdated ICS/SCADA systems that do not satisfy cybersecurity requirements.
- Insufficiently developed legislative coverage, technical and technological regulations ensuring cybersecurity in the area of smart grids.

Opportunities

- The continuing interconnection of European electricity markets.
- The introduction of phase regulation transformers in the CR in order to prevent crises at the level of the transmission system.
- The development of modern legislation ensuring cybersecurity in the area of smart grids.
- Participation in international cooperation when standardising and creating technical regulations and technological manuals for ensuring cybersecurity in the area of smart grids.
- The introduction of a coordinated allocation mechanism of cross-border capacities at the German-Austrian border, i.e. splitting the joint German-Austrian commercial zone.

[81] ICS – Information and Communication Systems, SCADA – Supervisory Control and Data Acquisition system (software that monitors industrial and other technical equipment and processes from a central workplace and enables their management).

Threats

- A forced decommissioning of the nuclear power plant in Dukovany for technical or political reasons.
- The continued development of electricity production from intermittent sources in northern Germany, with a continuing trend of declining stable resources in areas of high consumption in southern Germany, while the adequate connection between these two areas is at the same time being delayed.
- A threat to the function of smart grids, and this the energy infrastructure.

D. Recommendations to Strengthen Resilience

1. Define, when elaborating the National Program for Energy Resilience, socio-technological standards (levels of security of electricity supply) for both the normal and emergency state in electric power engineering.
2. Examine the readiness of the electric power engineering sector to deal with potential emergencies through regular exercises both at the level of the transmission system as well as at the level of distribution networks, with the participation of regional crisis management authorities and IRS units.
3. Update crisis readiness plans of critical infrastructure operators to ensure physical protection of elements of critical infrastructure.
4. Update territorial energy concepts with a focus on energy resilience and capacity of island plants to supply energy.
5. Set an obligation to have an alternative source of electricity and maintain sufficient reserves of fuel in case of a prolonged outage.
6. Provide a secure and affordable communication environment for tackling crises caused by extensive power failures and apply it in the area of preventive monitoring.
7. Prepare a study of the most suitable procedure for ensuring supplies of nuclear fuel to the extent specified in order to cover one fuel cycle of all nuclear power plants.

II) Large-Scale Disruption of Gas Supply

A. Description and Assessment of the Threat and Associated Risks for the CR

The most likely causes of a gas supply failure are natural disasters, technological accidents, terrorism, or trade and political disputes. Depending on the territorial extent and intensity of natural disasters, international gas transit may be disrupted. This concerns the threatening, in particular, of courses over waterways by floods in places where soil is prone to washing away or slipping. Thoroughly providing for these critical places significantly reduces the risk. Technological accidents may also be the cause of major changes in the operating mode of the gas network. During normal operation, these risks can be eliminated by consistent adherence to maintenance and repair tasks, as set by the maintenance schedule, and to technological procedures, safety regulations, inspections, controls, revisions, and testing of gas equipment, including regular training of operators and assembly workers. The destruction of operational facilities of the gas network as a result of a terrorist attack would directly impact the reliability of the supply of gas to the CR. The higher the degree of pressure of the gas pipelines, the greater the surface impacts of the accident should they be hit. An accident at gas storage facilities would have a significant impact on the supply of gas to customers, especially in winter months. The threat posed by a long-term disruption of gas supply from one foreign supplier is significant, from the point of view of practically full dependency on import. It can be lowered by ensuring the diversification of resources and negotiating long-term contracts with gas producers. Securing gas supplies from multiple sources and ensuring more than one transport route, as well as the option of reverse flows will result in defence against potential political abuse and present a solution in case of emergencies. The European system of long-distance gas transport has, in recent decades, developed into a fully interconnected form, which is an important prerequisite for ensuring the reliability and security of gas supply.

The CR has a robust, high-quality, and carefully maintained transportation system, which ensures a high standard of fulfilment of criterion N-1. This standard is actually substantially higher than the requirement of Regulation 994/2010 of the European Parliament and of the Council of 20 October 2010 concerning measures to safeguard the security of gas supply and repealing Council Directive 2004/67/EC.

Gas storage, which accounts for approx. 37% of the annual consumption, significantly helps to ensure gas supply to end customers. Storage capacities are currently being expanded; at the end of the process the total storage capacity will be equivalent to 40% of annual consumption.

The CR uses diversified supplies. Approx. 64.44% of gas comes from Russia, 2.95% from Norway, and 33.59% from the EU.

The diversification of a new route was completed – commissioning the Nord Stream pipeline, the connected OPAL pipeline and the Gazelle pipeline (BTS Brandov) will make it possible to supply gas to CR via a new route, which is primarily intended for transporting gas to Germany (i.e. from BTS Brandov and BTS Waidhaus). Investments were also made to enable the reverse flow of gas West – East and partially North – South (STORK I), although not fully. Risk analysis shows that the accumulation of failures, such as a simultaneous outage of gas supply at two border transfer stations or that of several underground gas storage facilities, is highly unlikely.

The disruption of gas supply does not compromise the production of electricity, since only 2.5% of total electricity is produced in gas-powered plants. However, it cannot be ruled out that this proportion will reach significantly higher levels in the future, depending on developments in the construction of new electricity sources. Natural gas is, nevertheless, an important source of heating and hot water in households, when in 2015 a total of 2 636 189 household subscribers were registered by the ERA. Natural gas also plays a significant role in the industrial sector.

The identified risks, should only one of them occur at any time, will not cause a threat or a reduction of gas supplies to the CR. In order for these risks to impact supply to customers, at least two of them would have to occur simultaneously, which is highly unlikely, especially as regards BTS Lanžhot and BTS Hora Svaté Kateřiny. Risk analysis shows that at least three adverse circumstances would have to occur simultaneously, i.e. a failure of infrastructure, a substantial decrease in extraction from gas storage facilities, and long-lasting adverse weather conditions.

The most serious unexpected failure to supply gas by the Gazprom Export company was registered with regards to Russian-Ukrainian disputes in January – February 2006 and especially in January 2009. During this period, supply deficiencies were compensated by supplies from underground storage facilities and via alternative transport routes, so that no customer in the CR was shorthanded in their demand for gas supply. No such cases were recorded with Norwegian gas suppliers, since emergencies (e.g. for maintenance purposes) are reported well in advance, allowing for the purchase of gas on the market and thereby avoiding shortages.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

Responsible institutions: MIT, ERA

Basic tools (legislation): Act No. 458/2000 Coll., on business conditions and public administration in energy sectors (Energy Act); Decree No. 344/2012, on emergencies in the gas industry and on the method of ensuring security of supply standards, as amended; Decree No. 401/2010 Coll., on the required content of the Rules for the Operation of the Transmission System and Rules for the Operation of the Distribution System.

Basic tools (EU strategies): Regulation No. 994/2010 of the European Parliament and of the Council of 20 October 2010 concerning measures to safeguard security of gas supply and repealing Council Directive 2004/67/EC and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank – A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy (2015).

Basic tools (Czech strategies): National Energy Strategy, the annually updated Czech Gas Network Emergency Response Plan, the Plan for Emergency Measures to Mitigate and Eliminate the Impact of a Disruption of Gas Supply in the CR, the Plan for Preventive Measures Necessary to Eliminate or Mitigate Identified Risks to Ensure the Supply of Natural Gas in the CR, and the Plan to Assess Risks Affecting the Security of Gas Supply in the CR.

C. SWOT Analysis

Strengths

- A robust, high quality and carefully maintained transportation system.
- Diversified transport routes.
- A high standard of fulfilment of criterion N-1.
- The possibility of a reverse flow in the transit transport system.
- A high capacity for gas storage due to natural gas consumption as well as a high parameter of the maximum daily withdrawal capacity.

Weaknesses

- A relatively low diversification of natural gas resources.
- Commercial operation of gas storage facilities – injections influenced by the trend in spot prices on the European stock exchanges.
- A private for-profit company supervising the GTS.
- The application of the rules of European legislation and consistent unbundling.
- A total lack of domestic natural gas resources.
- Insufficient interconnection of North-South natural gas transmission routes.
- No state control over gas transmission.

Opportunities

- The construction of new gas storage facilities in areas with terminated hydrocarbon extraction or underground extraction of uranium.
- The further development of plans to strengthen infrastructure.
- The possibility to access sources of liquefied gas.
- The construction and reinforcement of North-South gas pipelines (connecting CZ-AT and CZ-PL).

Threats

- The rise in the proportion of natural gas in electricity production due to unfavourable development in the area of nuclear power plant construction.
- Private entities in the gas industry will implement their development investments only when these are guaranteed by a relatively quick economic return.

D. Recommendations to Strengthen Resilience

1. Increase the operational and mining capacity of underground gas storage facilities in the CR.
2. Strengthen the North-South connection (Stork II, BACI).
3. Construct the "Moravia" gas pipeline, leading to North Moravia, in case of a simultaneous outage of underground gas storage facilities in Lobodice, Štramberk and Třenovice.

III) Large-Scale Disruption of Oil Supply

A. Description and Assessment of the Threat and Associated Risks for the CR

The CR is dependent on oil supplied by the Družba and IKL (Ingolstadt – Kralupy nad Vltavou – Litvínov) oil pipelines. The production of fuels and other petroleum products in Czech refineries is thus directly related to the supply of oil by pipelines from abroad, both in terms of the quantity and quality of oil.

In this regard, it is important to note that the oil transported to the CR from various regions has somewhat different characteristics. So-called medium heavy, relatively sulphurous oil is imported via the Družba pipeline from Russia. Oil from Azerbaijan and Kazakhstan is imported via the IKL pipeline; these countries produce oil that is so-called light and sweet, i.e. with a higher proportion of less complex hydrocarbons and lower sulphur content. While the refinery in Litvínov is set to process Russian oil, the refinery in Kralupy nad Vltavou is set to process oil from the Caspian Sea region.

This dependency creates the risk of a situation where there is an interruption of oil supplies to the CR. The interruption can be short or long term. A short-term interruption will most likely not cause a significant decrease in the production of petroleum products. Such a deficiency of oil needed for the production of petroleum products would be covered by reserves of refineries and other petrochemical companies as well as fuel distributors, or state material reserves. In the event of a prolonged shortage of oil, these reserves could be depleted. A long-term shortage, especially of fuel, on the market and the assumption of a further escalation would create a situation which it would not be possible to solve without the intervention of the state and its administrative offices, or possibly territorial Governments. At this point, the situation could be classified as an emergency, which is defined by the law on emergency oil stocks as a situation where the threatening of supply of oil or petroleum products to the market in the CR or in other EU member states or in member states of the International Energy Agency has occurred or is likely to occur.

In the event of a further escalation of the shortage of oil and petroleum products, especially fuel, the Government could declare a state of oil emergency. In that context, the Government may establish measures to limit the consumption of oil and petroleum products. If the consequences of the shortage of fuel on the market reached such an extent that it should influence the functioning of further infrastructure, the declaration of a state of oil emergency could be accompanied by the declaration of a state of crisis.

The most likely cause of a large-scale disruption in the supply of oil and petroleum products could be the deterioration of the international political situation, a long-term outage of extraction and processing of petroleum products and their distribution to consumers, and an interruption in the operation of the Družba and/or IKL pipelines.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

Responsible institutions: MIT, SMRA, NOCACOS

Basic tools (legislation): Act No. 189/1999 Coll., on emergency oil supplies, on the resolution of states of oil emergency (Act on Emergency Oil Supplies); Act No. 97/1993 Coll., on the competence of the State Material Reserve Administration; Decree No. 165/2013 Coll., on types of oil and composition of petroleum products for storage in emergency oil reserves, the calculation of emergency oil reserves, on storage facilities and reporting of emergency oil reserves.

Basic tools (EU strategies): Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products; Regulation (EC) No. 1099/2008 of the European Parliament and of the Council of 22 October 2008 on energy statistics; Communication of the Commission to the European Parliament – European Energy Security Strategy (2014); Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank – A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy (2015).

Basic tools (Czech strategies): National Energy Strategy, Standard Plan for a Large-Scale Disruption of the Supply of Oil and Petroleum Products, Plan of Action in an Oil Emergency, Measures to Introduce Rationing in an Oil Emergency.

C. SWOT Analysis

Strengths

- Diversified suppliers and oil transport routes.
- Sufficient emergency oil and petroleum product supplies.

- Adequate petroleum security legislation and emergency response system.
- Active involvement of the CR in the international petroleum security system (IEA, EU).
- A dense domestic network of product pipelines.
- The protection of emergency reserves by state-controlled entities.
- State supervised storage and distribution of fuels in significant volumes.

Weaknesses

- The absence of domestic oil sources.
- Limited state influence on refineries and their uncertain future.
- No low-sulphur, non-Russian, so-called sweet crude oil in state reserves.
- The need for substantial investments in refineries, with the risk that financial resources will not be allocated due to other investment priorities of the private entity in charge.

Opportunities

- The possibility to increase emergency reserves at relatively low oil prices.
- The construction of additional storage capacities for oil or fuel.

Threats

- A decrease in state-held emergency reserves of oil and petroleum products to the mandatory limit of 90 days, due to the growth of domestic consumption.
- Long-term outages in the production of petroleum products in refineries.

D. Recommendations to Strengthen Resilience

1. The gradual increase of emergency reserves up to 120 days of average daily net import in the reference year.
2. The inclusion of light crude oil in emergency reserves.
3. The further diversification of transport routes (e.g. a project of common EU interest Litvínov – Leuna).
4. Strengthening the role of the state in the Czech refinery industry (support for domestic oil processing).
5. Regular reviews of plans and measures for oil emergencies.
6. Ensuring the accessibility of emergency reserves by storing them in the CR.

RAW MATERIAL SECURITY

A. Description and Assessment of the Threat and Associated Risks for the CR

Minerals represent crucial input for the vast majority of industries and therefore for the entire economy, and their uninterrupted supply is the key to keeping the economy going. Ensuring non-discriminatory access to raw materials, whether domestic or imported, is an essential parameter of national raw material security. Global players are well aware of this fact and states that think strategically put great emphasis on ensuring sufficient input of raw materials into their economies.

In the first decade of the 21st century, due to the vast modernisation of a part of formerly developing and very populous countries, the principles on which the world market in raw materials had previously functioned for decades were been overturned. As a result, typical producers and exporters of raw materials gradually became their consumers, and even importers. This fact added a new quality and dynamic to the traditional rivalry for raw materials among global player. Traditionally, Asian states (Japan, South Korea, lately also China) devote special attention to providing their national economies with raw materials. The European continent finds itself in a very unusual position – it is one of the world's biggest consumers of raw materials while at the same time being a negligible producer, hence it is unable to influence world trends in the raw material industry. The mining industry in Europe was subdued much too rapidly in the 70s, 80s, and 90s and, after the major changes on the world market following 2003, proved to be a strategically unwise decision. At present, EU member states are highly dependent on imports of a range of raw materials (including strategic commodities) from abroad, which makes the EU vulnerable to blackmail in this field. The UE is thus not, as an entity, capable of guaranteeing its members the ensuring of adequate raw material and energy security. In such a situation, at the end of 2008, the integrated Raw Materials Initiative was introduced, seeking to address the situation. It is build three interrelated pillars:

a) Greater use of domestic (European) raw materials;

b) Promotion of mutually beneficial economic relations with third countries that have broad raw material potential (raw material diplomacy);

c) Promotion of raw material efficient technologies, i.e. smart recycling.

The years that followed, the EU identified a list of so-called critical (super-strategic) commodities on whose imports the EU is extremely dependent and that are produced by a monopoly of one or several states or that are imported into the EU from politically unstable regions – in 2011, the list contained 14 commodities; in 2014, it was updated and expanded to contain 21 commodities. They are the following commodities: *antimony, beryllium, borates, chromium, cobalt, coking coal, fluorite, gallium, germanium, heavy rare earth metals, indium, light rare earth metals, lithium, magnesite, magnesium, natural graphite, niobium, phosphates, platinum group metals, silicon, and tungsten.*

A disruption in the supply of some strategic raw materials would lead to the threatening of certain strategic production or the damaging of the competitiveness of the Czech economy.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

Responsible institutions: MIR, SMRA

Basic tools (legislation): Act No. 241/2000 Coll., on economic measures for emergencies and on amendments to certain other related acts, as amended.

Basic tools (EU strategies): Raw Materials Initiative (2008), Critical Raw Materials (2011; 2014).

Basic tools (Czech strategies): Raw Energy Policy of the CR in the Area of Raw Materials and Their Sources (2016), National Energy Strategy (2015), Background to the Raw Material and Energy Security Strategy (2011).

C. SWOT Analysis

Strengths

- A relatively good level of exploration of the territory of the CR by traditional methods for traditional raw materials.
- Sufficient reserves and production of certain non-metallic resources.
- Sufficient reserves of building materials.
- The good reputation of Czech/Czechoslovak geology in the world.
- Sufficient domestic reserves of uranium ore, as compared to European standards.
- Domestic reserves of brown coal, albeit limited by time or administration.

Weaknesses

- The results of exploratory activities are 30 to 50 year old; their quality, focus, predictive ability, and therefore their use is problematic in many cases, particularly with respect to modern, previously unavailable mining and processing technologies.
- Minimal knowledge about the potential of the CR in the area of new modern high-tech raw materials.
- A total lack of domestic economically exploitable ore and specific non-metallic resources.
- Underdeveloped raw material diplomacy as an integral part of Czech economic diplomacy.
- The preference of some companies and authorities as regards the environmental pillar of sustainable development.

Opportunities

- Using modern methods of exploration for the search for new raw materials in the CR (e.g. high-tech raw materials), including the use of modern mining and processing methods.
- Eliminating part of the ecological burden of the past by re-using them as secondary deposits of valuable commodities.
- Identifying the potential of the CR in the area of modern high-tech raw materials, e.g. strategic metals.
- Maintaining valuable know-how in the area of mining and processing of uranium ores and the possibility of their use in raw material diplomacy.

- Restructuring existing strategic reserves of raw material commodities in state material reserves without the need for considerable funding from the state budget.
- Anticipatory construction of a transport infrastructure for the import of raw materials into the CR – in advance, with a sufficient transport capacity, and with ample room for expansion.

Threats

- The loss of mining capabilities of certain specific mineral commodities – a narrowing of the spectrum of raw materials produced in the CR – increased imports and dependency of the state.
- An insufficient continuous replacement of terminated mining deposits by new venues.
- The loss of necessary know-how in the field of technical sciences.
- A reduction in the diversification of strategic raw material supplies to the CR.
- Loss of control over critical infrastructure hitherto belonging to the state.
- Restriction or liquidation of strategic processing capacities.
- The duration of the unfavourable situation on the world market for black coal, which threatens the European black coal industry.
- A decline in state-held emergency oil and petroleum product reserves to the mandatory limit of 90 days due to the growth in domestic consumption.

D. Recommendations to Strengthen Resilience

1. Restructure/modernise the structure of state material reserves in the area of non-energy commodities.

2. Explore the true potential of the CR in the area of modern high-tech raw materials that are used in industries with a high added value.

INDUSTRY SECURITY

A. Description and Assessment of the Threat and Associated Risks for the CR

In the CR, industry accounts for an important sector of the economy. It represents 35% of the national economy and employs over 40% of the economically active population. The main pillars of Czech industry are engineering, metallurgy, chemistry, and food. Other important industries are energy, construction, and consumer. The construction industry is one of the most traditional in the CR. The automobile industry is its most important component, which significantly contributes to national exports. Export performance is mainly driven by the automobile, electronic, engineering, and electrical industries. Their combined export share exceeds 60%.

The dependency of the Czech economy on exports to EU countries is still high. More than 80% of domestic exports are intended for the EU. The economy is thriving in the central and northern part of the EU and demand for Czech goods is growing. The CR's biggest trade partners, Germany and

Slovakia, are continuously importing more Czech products. Meanwhile, the state supports an opposite trend – the Export Strategy of the CR 2012 – 2020 sets 12 priority countries for exports, which are all outside the EU. However, exporters understand the EU market well. Here, they do not encounter cultural differences and the administration relating to the export of goods and services is relatively simple. Maintaining foreign business networks is not as time-consuming and financially taxing in comparison to more distant markets.

Economic development in the CR and in Germany is parallel. If the annual GDP is rising in Germany, it is also rising in the CR. The CR also follows Germany in the opposite direction – the decrease in gains or an absolute decline as compared to the previous year is also recorded in the CR in the same year. However, to draw the conclusion that the Czech economy is so closely linked to the German one that growth in Germany is a guarantee of growth in the CR would be a dangerous simplification. The relationship is mainly linked to the fact that several hundred German companies are active in the CR, which are directly connected to the mother economy and develop almost simultaneously with it. It is true for a substantial part of Czech exports to Germany that their main actors are foreign companies based in the CR. The activities of these companies contribute significantly to Germany's high share in Czech exports. As regards the opinion that it is necessary to decrease dependency on Germany, it is important to note that exports of foreign companies are – as regards the Czech economy – the easiest and cheapest way to penetrate the German market. The importance of these companies in Czech foreign trade, however, also increases the risk of a negative influence should these companies leave the CR, which can be done quite easily. For Czech exporters, it is important to know what position they find themselves in in Germany. Alongside companies that have established themselves via competitive final products, there are a number of businesses that are integrated into the production processes as subcontractors. A good subcontractor may have a very strong position. An example can be that of exporters of automobile parts, who are an indispensable component of production structures. The value of their exports exceeds the volume of exports of automobiles. The stabilisation of their position on the German market should be one of the goals of export promotion. Statistical data on the development of exports during the crisis show that the robust German economy stabilised Czech exports during the global economic downturn, and this much more efficiently than was the case of priority or interest countries. We cannot expect the economic turbulences not to occur again. If foreign companies decide to leave the country, the volume of Czech exports to Germany would decrease. Without foreign companies, only one tenth of total exports is intended for Germany.

The automobile industry accounts for almost a quarter of Czech exports and 7% of GDP. The industry employs some 150 000 people. A significant dependency on one sector may pose a serious threat to the Czech economy. The automobile industry could, according to experts, find itself in dire straits in case demand falls. Should demand fall during an economic downturn, the Czech economy will slow down. Not only production and employment would fall, but consequently household consumption, which will be felt by companies from other industries. Concerns relate mainly to the saturated demand for automobiles in Europe. Analysts predict that, sooner or later, demand will undoubtedly fall, which could be a cyclical phenomenon or one caused by another economic downturn. Czech automobile manufacturers, however, are currently not threatened, due to low labour costs, highly qualified employees, modern production plants, leading development institutions, and a favourable geographic location. Likewise, no shock is likely to occur overnight. It should be noted that, when talking about reducing dependency on the automobile industry, other alternatives have to be presented. Currently, no such alternative that could offset the clout of the automobile industry exists. In the future, it could be engineering – from energy to manufacturing medical devices.

Approximately 98% of industrial enterprises are domestically owned. It should be noted, however, that the total number includes a multitude of small companies, including entrepreneurs – physical persons. Foreign investors are important primarily in larger companies, whose economic significance goes beyond their number. According to the Czech Statistical Office, foreign-owned companies in the industry sector account for 60% of total sales. The added value created by these companies, which indicates their importance in terms of economic performance, amounts to CZK 500 billion, or roughly half of the total for the entire industry sector. Foreign-owned companies play the most important role in the automobile industry. The foreign ownership of some key industry companies, however, can pose a security risk should these persons act in the interests of a foreign power.

Influence and infiltration operations of foreign intelligence services aimed against strategic industrial interests of the CR, industrial, scientific and technical espionage, can pose a significant risk for the Czech industry. In the case of Government owned or co-owned companies, the defence against such activities is subject to the proper exercise of ownership rights. In the case of joint stock companies with private participation, however, it is often difficult – with regards to the legal framework – to adequately take into account national security interests in their decision-making processes. Significant opportunities and challenges associated with finding professional opportunities in sales of industrial commodities will, in the following years, include the implementation of processes linked to the development of digital markets, including Industry 4.0, the fourth industrial revolution, based on a complex system of changes in a number of activities, not only in industrial production. Industry 4.0 transforms the production of separate automated parts into a fully automated and continuously optimised production environment. Vertical production processes will be horizontally integrated within corporate systems that will respond in real time to immediate and changing demand for products. One opportunity is the creation of conditions for the dual role of Industry 4.0, i.e. the support of modern industrial production in the CR, but also of export of solutions or research results to global markets. This also applies to the use of digital technologies in other sectors of the economy.

A competitive defence and security industry is one of the prerequisites for ensuring the fundamental security interests of the CR and the development and maintenance of national defence capabilities.

An important factor for maintaining, or increasing the competitiveness of the defence and security industry is a predictable source framework for the area of defence, which is essential not only for the efficient functioning of the armed forces of the CR, but is also a very important factor in relation to the Czech defence and security industry. A stable financial environment enable medium- and long-term planning by the Army of the CR, and thus gives the defence and security industry the possibility to adequately respond to set goals and to prepare for their implementation in the field of research and development well in advance. Ties between the Czech defence and security industry and the army, as well as the reference customer, are thus strengthened. The decision to gradually increase the budget of the MD in the medium term so that it reaches 1.4 GDP in 2020 (SS 2015) thus gives the defence and security industry a certain degree of perspective.

Another important factor is the diversification of production. The consequences of economic crises are delayed in the defence and security industry as compared to civilian sectors. The reason is that buyers of military equipment are mostly Government bodies, thus the funds for arms purchases come from Government budgets, which are drafted every year and thus do not react to the crisis immediately (by reducing budgets for arms purchases). Companies operating in the defence and security industry mitigate or eliminate the negative consequences of crises by a counter-cyclical diversification of their production portfolio to include industrial, dual, and civil production as well as by regional diversification of sales.

Currently, the most pressing problem for Czech producers/exporters is the shortage of employees with technical education. Because of this, exports are likely to grow more slowly this year, which can lead to a slowdown in the Czech economy. The lack of qualified employees may dissuade foreign investors. Employers in the industry are experiencing a shortage of qualified workers in certain technical fields. Apart from new investors, the CR may be losing current ones. For new investors, or when considering expanding production of existing companies, the search for new employees is an obstacle that may direct them to another country. The disproportion between the number of professionals retiring in the next few years and the number of graduates of secondary schools and universities in key fields could cause problems both with the influx of foreign investments and with the operation of established firms. For this reason, the issue of technical education should be addressed jointly by all relevant parties.

The Confederation of Industry and Transport notes that the Czech industry lacks at least 100 000 technically educated workers. At the same time, around 60 000 technically educated workers will retire from the engineering and automobile sectors before 2020. Foreigners could be a partial solution to the shortage of skilled workers. Cooperation could be developed especially with Eastern European countries. Hiring third country employees, however, poses an administrative burden for businesses and takes one year on average.

An essential step to improve the quality and attractiveness of technical fields is the cooperation of schools and businesses, particularly in providing as much practical training as possible in the real business environment. For this reason, changes were made in 2013 to the Act on income taxes, and employers cooperating with schools may, as of 1 January 2014, apply tax breaks for investment in educational equipment and on-site student training.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

Responsible institutions: MIT, CzechTrade, CzechInvest, MFA

Basic tools (EU strategies): Free Trade agreements between the EU and its member states on the one hand and other states on the other hand.

Basic tools (Czech strategies): Export Strategy of the CR 2012 – 2020, National Innovation Strategy, Foreign Policy Strategy, Strategic Framework for Sustainable Development of the CR, Strategy for International Competitiveness of the CR 2012 – 2020, Action Plan to Support Economic Growth and Employment, Action Plan for the Development of the Digital Market, Global Sectoral Opportunities Map.

C. SWOT Analysis

Strengths

- The CR is the most industrialised country in the EU.
- Modern production facilities.
- State-of-the-art research and development facilities.
- High qualification of some employees.
- A favourable geographical location.

Weaknesses

- A lack of qualified staff in some technical fields.

Opportunities

- Maintaining the position of the CR in traditional industries.
- Gaining a leading position in new industrial sectors.
- Ensuring the diversification of foreign outlets for Czech industrial production.
- Ensuring the source framework for the area of defence as 1.4% GDP.

Threats

- A significant dependency on one industry – the risk of decline in the demand for products of the automotive industry.
- Insufficient diversification of industrial production exports.
- The significant role of foreign investors in large companies.
- The outflow of foreign investments as a result of shortages of qualified workers in technical fields.

D. Recommendations to Strengthen Resilience

1. Implement incentives to industries with a high added value and to regions with high unemployment.
2. Create new jobs and support the growth of companies by increasing trade and internationalisation of business, strengthening the prestige of the CR in the world and in international organisations, and using global trade opportunities for the growth of prosperity of the CR.
3. Cooperate with trade association, the Exhibition Committee of the Confederation of Industry, Czech embassies and their economic sections abroad, the CzechTrade and CzechInvest agencies, including their foreign offices, to ensure official Czech participation in trade fairs and exhibitions abroad.
4. Implement measures for the improvement of the quality and attractiveness of technical disciplines at secondary schools and universities and increase investments in the education system.
5. Create conditions for the hiring of foreign personnel educated technically in secondary schools and universities.

HYBRID THREATS AND THEIR IMPACT ON THE SECURITY OF CZECH CITIZENS

A. Description and Assessment of the Threat and Associated Risks for the CR

1. Introduction

International politics of the 21st century reveal the extent to which instruments from the entire range of power dimensions known as DIMEFIL[82] are applied in conflicts. A number of state and non-state actors are trying to achieve their political goals through overt and covert activities coordinated within the entire range power instruments, without regard to any possible collision with the international order founded on rules. It is in this context that the term hybrid threats, or hybrid warfare, emerges. This chapter covers a range of threats from other chapters, especially Influence of Foreign Powers, Cyberthreats, Energy, Resource and Industry Security, Terrorism, and partly Security Aspects of Migration and Extremism. The threats mentioned in these chapters may or may not be part of a coordinated campaign. For this reason, the topics discussed in these previous chapters overlap to varying degrees with the present chapter, which has the ambition to coordinate the overlay.

The elementary definition of "hybrid threats" already points to the fact that these cannot be understood in sense similar to that of most other threats, where each one represents a threat in more or less one dimension. What we mean by hybrid threats is primarily a method, a way to wage a confrontation or a conflict. This manner of waging a conflict represents a wide, complex, adaptable, and integrated combination of conventional and unconventional means, overt and covert activities, characterised primarily by coercion and subversion, that are executed by military, paramilitary, and various civilian actors.[83]

The aim of a hybrid campaign is to exploit the weaknesses of the adversary; mask oneself by pursuing legitimate targets; prevent a clear interpretation of events and the discovery of their interconnectedness; complicate or prevent the identification of the originator and disguise their intentions; complicate, destabilise, or paralyse the decision-making process and thus prevent a timely and effective response from the attacked. A hybrid attacker plots and carries out activities damaging the vital, strategic, or general security interests of the attacked while striving to create an environment where responsibility for these activities cannot (at least formally) be attributed to them, or at least only speculatively and with great difficulty (see the concept of "plausible deniability"). A hybrid attacker will try to keep their activities below the threshold that would be considered by the international community as armed aggression. They will most likely try to avoid direct military

[82] Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal.

[83] The concepts of hybrid warfare, method of hybrid conflict, or hybrid strategy can basically be understood as synonyms. In the interest of a most concise expression for these concepts, the term "hybrid campaign" will be primarily used in the following text. The definition of "hybrid campaign" used in the present chapter is based on the "Strategy on NATO's Role in Countering Hybrid Warfare" (2015).

confrontation, although it must be assumed that military means in one form or another may be incorporated into a hybrid campaign at some point.

Hybrid strategies can be applied by both state and non-state actors, via various modes of attack that may significantly vary in their degree of development and integration.

A hybrid campaign may connect a number of classic instruments of the aforementioned range of spheres of influence, i.e. power dimensions – DIMEFIL:

D) Diplomatic/Political – exerting influence and coercion through words and actions of official political representatives;

I) Information – media, social networks and other means of disseminating information, their manipulative use, disinformation campaigns and propaganda;

M) Military – the overt use of military means as a threat (demonstration of military presence and readiness), or direct combat, or various forms of covert deployment of individuals and small groups for the purpose of infiltrating the attacked state;

E) Economic – various forms of economic coercion (imposing duties and embargoes, denial of supply of resources or energy, banning transport or limiting transport routes, destabilising key industries, businesses etc.);

F) Financial – destabilisation of currency, the share and the bond market, the banking sector, influencing key financial institutions;

I) Intelligence – activities of intelligence services, espionage, acquiring collaborators (especially state or Government officials) for subversive activities;

L) Legal – various subversive activities targeting the value, legal, and other aspects of social organisation, e.g. fomenting unrest in the attacked state through the exploitation of ethnic, religious, or social rifts in society, or the use of a wide scale of terrorist attacks and other typically criminal methods (e.g. abduction, blackmail, intimidation).

Cyberspace holds a specific place in relation to the abovementioned instruments – it represents an environment where the individual power dimensions overlap, and its significance for the functioning of states and economies is critical. Cyberattacks may target and threaten public administration, critical infrastructure (electricity supply etc.), the financial sector, they may threaten the security of important facilities, they may be used for purposes of espionage, disinformation campaigns, etc.

Historically, individual hybrid conflict instruments are nothing new. The novelty lies in the range and the methods in which the instruments are combined and coherently applied to achieve strategic goals.

The individual elements of a hybrid campaign do not necessarily have to be illegal or pose a threat in themselves; the danger lies in their sophisticated combination, which simultaneously seeks to disguise their true purpose.

A sophisticated hybrid campaign model was showcased by Russia during its conflict with Ukraine; its highlight was the annexation of Crimea in 2014 and its outcrop is the attempt to freeze the conflict in Eastern Ukraine. Russia wages its campaign using all available methods and forms of coercion and with a very high degree of coordination, as well as with a long-term view. One fact that cannot be overlooked is that Russia is a nuclear power. The methods of the so-called Islamic State terrorist organisation also bear characteristics of hybrid warfare, although the spectrum of instruments employed is not so wide. The main ones include propaganda via social media, manipulation of facts and disinformation, the manifestation of armed power in combination with the use of underground networks of supporters and followers, asymmetrical fighting, cyberattacks, intimidation through terrorist attacks, etc. The manipulative use of information and multimedia activities are, in the case of the so-called Islamic State, used in a much more sophisticated way than conventional military weapons. Nevertheless, it is true even of hybrid warfare that, in certain conflicts, various hybrid campaigns will be waged, adapted to their specific targets.

2. Identification of Risks

The principal risk to which a subject attacked by a hybrid campaign is exposed lies in the fact that they will not be able to identify the hybrid campaign – in time, in its full scale, or at all. If the originator of the hybrid campaign, the extent of their methods, as well as their targets, is not identified in time, the response will not be adequate, which will reflect on the degree of its success. This is why the basic instrument of any security system for combating hybrid campaigns is the ability to collect information and evaluate it in order to identify the hybrid campaign and its originator.

Other risks can be identified based on the specific combinations of instruments and methods that may be employed during a hybrid campaign, as well as their specific targets. In this regard, the CR may face hostile activities that will target its three basic interests, i.e. the pillars of the state:

a) A Cohesive Society and its Identification with the Ideological and Value Foundations of the State

Influencing political structures and the political decision-making process, the judiciary, the police, the armed forces, the media and public opinion may be part of a hybrid campaign seeking, ultimately, to destabilise or divide society and undermine public confidence in its ideological-political organisation (democracy, rule of law, guarantee of basic human rights and freedoms, guarantee of political and social rights – in other words, constitutional liberalism and a corresponding foreign policy orientation of the CR, expressed, for example, by its membership in the EU, NATO, and other organisations). The will of political representatives and the public to meet allied commitments of the CR to collective defence in favour of another NATO member state facing an apparent threat, or to provide similar mutual assistance to EU member states may be a specific target of a hybrid campaign.

These kinds of activities are directed especially against the following interests of the CR, enumerated in the SS 2015:

- Strengthening the coherence and efficiency of NATO and the EU and maintaining functional and reliable transatlantic ties;
- Supporting democracy, basic freedoms and the principles of rule of law;
- Creating conditions for a tolerant civil society, suppressing extremism and its causes;
- Enhancing public awareness and active participation of the public in ensuring security.

The probability of confrontation with these types of activities is relatively high in comparison to other hybrid campaign instruments that hypothetically come into consideration. Czech society is, however, homogenous ethnically, socially and it terms of its basic value orientation. Part of this orientation is a generally low level of interest in politics and a low level of involvement in public affairs. Overall, the relevance of the threat stemming from a potential hybrid campaign seeking to destabilise society by exploiting its internal divisions is assessed as **medium**.

b) A Functioning Economy

The damage and destabilisation of the economic foundation of the state, e.g. by disrupting the supply of strategic resources and energies, boycotting Czech exports, etc., may be part of a hybrid campaign. Often, the vague structure of ownership relations in a number of key sectors represents a specific problem that reduces the economy's resilience against efforts at its destabilisation.

Such activities would damage, in particular, the following two strategic interests of the CR:

- Ensuring economic security of the CR and strengthening the economic competitiveness;
- Ensuring energy, resource, and food security of the CR and an adequate supply of strategic reserves.

The probability of the adversary's focus on damaging the economy is relatively high, as Czech economy is very open and therefore highly likely to respond to (negative) prompts from abroad. A higher risk is identified in ensuring the state's energy needs, since the CR's own energy resources are limited and the economy is to a large extent dependent on their import. At the same time, supply sources are not sufficiently diversified. The probability that an attempt at damaging the economy will take advantage of owners of major economic entities affiliated with the hybrid attacker is relatively low. The short-term consequences of such interventions would likely be serious, but the strong integration of the Czech economy within the EU offers possibilities of a quick recovery. In this case, therefore, the threat relevance is assessed as **low**.

c) Security and Defence

The mobilisation of interest – religious, ethnic, national, or linguistic – and criminal groups in order to perform subversive activities and disrupt public order may be the instrument of a hybrid campaign. In this context, the term "fifth column" or the so-called Karaganov Doctrine (the use of ethnic minorities abroad as a pretext for interference under the guise of protecting their rights) may be used as an illustration. The attempt to directly influence members of the armed forces, the police, and other security forces with the goal of exploiting their potential/latent extremist tendencies and thus weakening their responsiveness may be a variant of this approach. In the past, some members of security forces have shown extremist tendencies. This is related to the involvement of former professional soldiers and police officers in non-state paramilitary groups. It is a phenomenon that requires attention.

The security of the CR may also be threatened by the overt or covert use of military forces directed, for example, against the military involvement of the CR in operations and other activities of NATO and the EU or by the aggressive deployment of foreign intelligence services or special forces in the CR.

At a certain stage of escalation, these activities could directly threaten the vital interests of the CR. They are also directed, in particular, against the following strategic and otherwise important interests of the CR:

- Security and stability, especially in the Euro-Atlantic area;
- Ensuring internal security and public protection;
- Ensuring cybernetic security and defence of the CR;
- Reducing crime, with an emphasis on economic, organised, cybernetic crime, and corruption;
- Creating conditions for a tolerant civil society, suppressing extremism and its causes.

The likelihood of a massive military threat to the CR is very low. However, it is necessary to consider the fact that some NATO member states face a more palpable threat than the CR, and this may create demands for solidarity participation of the CR in the interest of ensuring their security. The possibility of a threat to Czech armed forces operating outside the CR is high, and directly corresponds with the nature of each particular deployment. When engaging in low-intensity stabilisation operations (that were the dominant type of engagement of Czech armed forces in the last 20 years), Czech armed forces have sufficient capabilities and capacities to avoid undue risk.

A medium risk would stem from the actual state of the Czech armed forces in terms of personnel and material equipment and readiness in case of necessity in more demanding scenarios, such as, for example, collective deterrence or collective defence within NATO against a conventionally strong opponent or a widespread reinforcement of security forces in the CR for the purpose of maintaining public order and security.

B. Responsible Institutions within the Czech Security System and Basic Tools (Legislative, Strategic) for the Elimination of These Threats and Risks

The following text reflects the fact that the various tools and methods useable in hybrid campaigns and the measures against them are primarily the object of almost all the other chapters of the Audit. Therefore, the present chapter focuses on the essence of hybrid campaigns, i.e. complicating the decision-making process to the extent that it is incapable of taking effective countermeasures. Such a situation may occur if the individual components of a hybrid campaign are tackled individually, with no awareness of their mutual interconnectedness.

It is highly improbable that the CR would face a widespread hybrid campaign on its own. The threat is perceived similarly within NATO and the EU, which are developing their own abilities to counter a hybrid campaign. Both organisations recognize the primary responsibility of member states as the guiding principle, and view their role as supportive. NATO defined its approach in the “Strategy on NATO’s Role in Countering Hybrid Warfare”[84] and in supplementary documents in the field of civil preparedness.[85] The approach of the EU is expressed in the joint declaration of the European Commission and the High Representative for Foreign and Security Policy, “Joint Framework on countering hybrid threats: a European Union response”.[86] The approach, role, and capabilities of both organisations are largely complementary, which is why it is desirable to align their efforts and thus increase their efficiency. Both organisations drafted their “manuals” for mutual cooperation and coordination of responses to hybrid attacks.[87] The CR should actively contribute to shaping the approach of NATO and the EU, take their relevant outputs into account in its own national approach, and be prepared to assist NATO and EU member states in case of an attack, and be prepared to accept assistance if it should itself become the target of a hybrid campaign.

The responsible institutions are identified against the backdrop of three basic interests, i.e. the pillars of the state, against which hybrid campaigns can be aimed.

[84] PO (2015)0673, 1 December 2015

[85] Report on the State of Civil Preparedness, PO (2016)0057, 5. 2. 2016 *et al.*

[86] Joint Communication to the European Parliament and the Council, JOIN (2016) 18 FINAL, 6 April 2016.

[87] NATO-EU Staff to Staff Hybrid Cooperation Playbook, DPRC-N (2016)0045, 11 May 2016; Joint Staff Working Document – EU operational protocol for countering hybrid threats – 'EU Playbook', SWD (2016) 227 FINAL, 7 July 2016.

Action against the Cohesion and Ideological-Value Foundation of Society

In reaction to this kind of action from the adversary, the entire political representation (parliament) and the self-organising civil society play an important role. However, when discussing the narrower sense of the Czech security system, it is the Government is the responsible institution.

The core reaction against this segment of a hybrid campaign is a credibly developed and implemented state (Government) strategic communication system in relation to its own population and as well as in relation to its adversary. Its role in relation to its own population is to strengthen its resilience and assure it of the readiness of the state to ensure its security. The resilience of the population is founded on the sharing of (basic) values and the willingness to protect them, on civic awareness and solidarity; developing good governance and removing internal tensions increases the population's resilience. The strengthening of this resilience is the subject of long-term social and political discussion and practical implementation, as well as education. Due to this, it is difficult to try to find space here for implementing specific instruments for ensuring security. In relation to the adversary, the role of Government strategic communication is to demonstrate readiness, ability and resolve to defend oneself and one's allies, and thus to deter the adversary from their aggressive intentions. Government strategic communication must be supported by other relevant bodies/authorities depending on the nature of the threat – the MFA, MoI, MD, MIT, etc. The use of propaganda and disinformation as part of a hybrid campaign should be seen in the context of other events that – potentially or currently – damage state and public security, and their potential links should be studied. The channels, or more broadly the information space, that are being used by propaganda and disinformation campaigns, need to be monitored and evaluated continuously. The fight against hostile propaganda is further discussed in the chapter on Influence of Foreign Powers.

This area of a hybrid campaign needs to include activities aimed at influencing political structures and the political decision-making process, the judiciary, the police, the armed forces, and other state/public institutions – in other words, an attack against the functioning of the state. Institutions that may effectively face these activities are generally authorities investigating (serious) crime, typically corruption, as well as intelligence services.

Action against a Functioning Economy

In this area, as well, it is more expedient to refer to the identification of risks and the list of institutions and their instruments included in chapters on Energy, Resource, and Industry Security or Stability of Currency and Financial Institutions. Should some forms of economic coercion or undermining of the economy be used as part of a hybrid campaign, it is very likely that methods to counter them will be of a regulatory nature, involving restrictive and prescriptive measures affecting the functioning of markets, trade, ensuring the supply of goods and the running of industries. The security system must, however, be capable of detecting the potential correlation of events damaging the economy with other activities aimed against Czech interests.

Action against State and Public Security

Among institutions responsible for tackling this area of a hybrid campaign, the primary role is played by institutions collecting information (also "intelligence services"):

- SIS,
- OFRI,
- MInt.

A specific, cross-cutting role is played by cybersecurity authorities:

- NSA and its subordinate elements,
- the network of CERT (Computer Emergency Response Team) office,
- the National Centre of Cybernetic Forces generated by MInt.

Institutions that have the main executive powers and instruments include:

- the MoI,
- internal security and public protection authorities,
- the Armed Forces of the CR.

Undoubtedly, other institutions may contribute to defence and security, especially by collecting information, e.g. the MFA. The overall responsibility and coordination role lies with the Government. The most important decisions in matters of national defence are granted by the Constitution to the Parliament.

Responsible Institutions, their Tools and Capacities

Intelligence Services

The basic mission of the SIS, OFRI, and MInt is gathering information and its evaluation in order to detect threats to the interests and security of the state and its population. These activities are constant. In case of the need to intensify intelligence activities in identifying increased activity against the security of the state and its population, the Government may strengthen the capacities of intelligence services. The powers of intelligence services are currently defined by Act No. 153/1994 Coll., on intelligence services of the CR, Act No. 154/1994 Coll., on the Security Information Service, and Act No. 289/2005 Coll., on Military Intelligence.

A key contribution to unveiling a hybrid campaign is the continuous gathering and sharing of information by intelligence services within their legal powers. This enables mutual consideration of information and the detection of a possible correlation between different activities that are part of one hybrid campaign. The spectrum of relevant information is very wide – it includes events with a negative impact on the state economy and the functioning of key industries or enterprises, the activities of groups defined by ideology or interest, the character of cybersecurity incidents, etc. The activities of intelligence services involve, in particular, the understanding of the context of a situation. The current legal framework does not allow them to actively participate in preventive and reactive measures to ensure state security.

Cybersecurity Authorities

As of 2011, the NSA is responsible for cybersecurity. Act No. 181/2014 Coll., on cybersecurity, made it officially responsible for public administration in the field of cybersecurity. The current National Cybersecurity Strategy of the CR defines the basic approaches, tools, and tasks of relevant institutions, taking into account the international dimension of cyberthreats. The role of the NSA in relation to a hybrid campaign is that of ensuring cybersecurity, preventing specific cyberattacks, and increasing the resilience of the Czech information infrastructure. For this purpose, a high-end CERT-type office operates under the NSA – Government CERT, or GovCERT.CZ. Similar activities are carried out by other CERT teams in other institutions.

The National Centre for Cybernetic Forces is currently being developed so as to be able to perform a wide range of operations in cyberspace necessary for ensuring cyberdefence of the CR.

The NSA may use its capacities to assist, in particular, the Police CR in detecting and investigating cyberattacks. The NSA may also, owing to good cooperation with the intelligence services, the Police CR, and other institutions, aid in identifying the originators of serious cyberattacks. However, the NSA has limited staff for these activities. It is very difficult to evaluate in more detail the sufficiency of existing resources for a complex response to large-scale cyberattacks that would be part of an intensive hybrid campaign, since this depends on the possibilities of coordinating the activities of individual CERT teams; generally, however, it is recommended to strengthen them. This issue is further discussed in the chapter on Cyberthreats.

The MoI, Internal Security and Public Protection Authorities

As per Act No. 2/1969 Coll., the Competencies Act, the MoI has a number of responsibilities that make it the central public administration office responsible for dealing with primarily non-military instruments of a hybrid campaign. Its scope of responsibilities includes ensuring public order, internal security, public protection, and other issues of internal governance.

The tools of the MoI and the Police CR are further discussed in the chapters on Terrorism, Extremism, Security Aspects of Migration, Organised Crime, and Influence of Foreign Powers. These chapters also describe the contribution of the MoI and the Police CR to the response to a hybrid campaign, should it include, for example, terrorist and extremist acts, uncontrolled migration, or organised criminal groups.

The inclusion of basic and other IRS units in crisis management would take place through the IRS, which is coordinated by the FRS CR. The situations which IRS units are prepared to tackle include, for example, the use of a dirty bomb, the threat of use or discovery of a booby trap, a chemical attack in the metro, an active shooter attack, etc. The capacities and abilities of the FRS CR and the IRS are further discussed in chapters on Environmental Threats and Anthropogenic Threats.

In case of a hybrid campaign focused specifically against the CR, the security system must be prepared to act against dispersed, latent, or unidentifiable groups of armed persons using tactics of asymmetrical fighting or terrorism with the purpose of disrupting public order, threatening public security and destabilising the state.

The responsibility for tackling internal security threats lies with the Police CR. Should its capacities not suffice to ensure internal order and security, it may be strengthened by selected components of the armed forces and other security forces.

The Armed Forces of the CR

The purpose of the armed forces is mainly to deter, repel, and eliminate external attacks against state and public security. The possible deployment, tasks, and tools of the armed forces are defined in particular by the following acts: Constitutional Act No. 110/1998 Coll., on the security of the CR; Act No. 222/1999 Coll., on ensuring the defence of the CR; Act No. 219/1999 Coll., on the Armed Forces of the CR; Act No. 585/2004 Coll., on conscription and its management (Conscription Act), and the Security Strategy of the CR and the Defence Strategy of the CR. The required skills and capacities of the armed forces are defined in particular by the Long-Term Defence Outlook 2030, the Strategy for Development of the Czech Army before 2025 and a number of other lower-level strategies focused on specific areas of skills or on particular tools and mechanisms – the use of active reserves, preparing the population for defence, etc.

In an extreme case, a hybrid campaign could lead to the outbreak of a conflict with the extensive use of the armed forces. The CR ensures its defence on the principle of collective defence within NATO. The CR is surrounded by allies and is not a NATO border state.

Therefore, the armed forces are not designed to fully ensure the defence of the CR, but to provide a proportional contribution to collective defence with the participation of all NATO member states. In case of a hybrid campaign using military means, the role of Czech armed forces resides mainly in contributing to the deterrence or the repelling of an attack on the CR or another NATO member. The minimal contribution of the CR to collective defence expected by NATO (which includes deterrence) is a brigade task force of ground troops adequately equipped with all necessary support and security (including air forces) that will enable it to independently and fully perform combat missions. Therefore, the armed forces have only minimal spare capacities in peacekeeping structures, which would allow for a more extensive deployment, than in a contribution thus conceived. In order to repel a military attack that would take place in close proximity to or on Czech territory, all armed force capacities would naturally be deployed, including active reserves and other means of mobilisation. In emergencies, the armed forces may deploy soldiers to strengthen the Police CR in performing tasks to ensure internal order and security. According to the needs evaluated *ad hoc* based on a specific situation, the armed forces may in principle set aside an entire spectrum of their skills and capacities.

The detection of a possible disruptive influence on soldiers (e.g. incitement to extremism) is primarily the task of the Military Police.

The Government of the CR

The Government has the overall responsibility for ensuring the security and defence of the state and the population. It has at its disposal the entire security system and relevant working bodies such as the NSC and the Central Emergency Team to deal with crises.

The duties and powers of the Government are defined mainly by Constitutional Act No. 1/1999 Coll., Constitution of the CR; Constitutional Act No. 110/1998 Coll., on the security of the CR; Act No. 222/1999 Coll., on ensuring the defence of the CR; Act No. 219/1999 Coll., on the Armed Forces of the CR.

A key role of the Government is to take decisions on specific measures to ensure security and defence, in other words, to manage crises. For this purpose, it is necessary to ensure several basic and interrelated conditions – the quorum of the Government, a secure workplace and a secure communication channel enabling the management of the security system and its elements.

In case of a hybrid campaign waged against the CR or a group of states of which the CR is a member (e.g. NATO or the EU), the Government needs, first and foremost, reliable and timely evaluation of information to make necessary decisions. The tempo of a hybrid campaign may vary, from a log-term and gradual to an intense and very dynamic unfolding of events. The Government may face the necessity to make decisions in an extremely short time. Crisis decision-making by the Government must therefore be resolved in a manner that will, under all conditions, guarantee the quorum of the Government, especially in time-constrained situations.[88]

A key factor for detecting a hybrid campaign waged against the CR or its allies is the continuous collection and evaluation of information. The sharing of information should occur in one place. The Government needs just such a mechanism within the structure of the security system.

[88] This issue is covered in the document "Optimising the Current Security System of the CR" – see task assigned by Government Resolution No. 980 of 2 December 2015.

The President of the CR

The powers of the president in relation to state defence are defined by Constitutional Act No. 1/1999 Coll., on the Armed Forces of the CR and by Act No. 585/2004 Coll., on conscription and its management (Conscription Act).

The president is the supreme commander of the armed forces. Their role is mainly symbolic and ceremonial – they nominate and promote generals, appoint soldiers to the highest military functions and approve basic military orders. Decisions issued by the president as supreme commander of the armed forces require the co-signature of the prime minister or a member of Government delegated by them. The Government is responsible for decisions of the president thus co-signed.

The Parliament of the CR

The powers of the parliament are enshrined in Constitutional Act No. 1/1999 Coll., Constitution of the CR and in Constitutional Act No. 110/1998 Coll., on the security of the CR.

The parliament decides on the declaration of a state of emergency or a state of war if the CR is attacked or if it is necessary to fulfil international treaty obligations concerning collective defence against an attack and the participation of the CR in defence systems of international organisations of which the CR is a member. Furthermore, the parliament approves the deployment of armed forces outside Czech territory and the presence of foreign armed forces in the CR, unless such decisions are reserved for the Government.

If the chamber of deputies is dissolved, these decisions are made by the senate. Furthermore, the parliament, i.e. the senate, may also face the necessity to make decisions in an extremely short time. For this purpose, it is necessary to ensure conditions in practice that would, under all circumstances, guarantee the quorum of the parliament.[89]

C. SWOT Analysis

Given that hybrid warfare is a complex approach combining a variety of instruments, the ambition of this SWOT analysis is to assess the resilience and the possibilities of the Czech security system as a whole.

Strengths

- A solid structural integration of the CR into NATO and EU. Both organisations currently provide the highest possible guarantees of security and collective defence.
- A developed national security system with a reasonable structure of working coordination bodies based on a comprehensive approach to crisis management.
- Experience with the functioning of purposefully established platforms for sharing information and coordinating activities – e.g. the Joint Intelligence Group, established primarily for tackling terrorist threats.

[89] This issue is continuously addressed in the document "Optimisation of the Current Security System in the CR"- see task assigned by the Government on 2 December 2015, No. 980.

- The existence of an IRS, which can effectively deal with a wide range of consequences brought about by emergencies and crises endangering the lives, health, and property of inhabitants, as well as the environment.
- A relatively high degree of homogeneity of Czech society; a relatively well-developed civil society with the potential to mobilise itself in order to protect national interests.

Weaknesses

- A limited ability to identify a hybrid attack conducted against the CR due to the absence of a mechanism for systematic and comprehensive evaluation of events and activities that would lead to the recognition of a hybrid campaign.
- The insufficient addressing of situations, within crisis management exercises, that would test infrastructure and procedures to preserve the functioning, including the decision-making process, of the Government, especially in situations where the adversary is seeking to disrupt the decision-making process. Crisis management exercise scenarios do not address the need to ensure the quorum of the Parliament.
- The overall peacekeeping capacity of the Czech armed forces, when carrying out regular tasks, does not enable it to significantly strengthen the Police CR, especially over longer periods of time. There is no mechanism for a rapid increase in the number of armed forces staff, either through hiring volunteers or through mobilising reserves. The Czech Army has a relatively small Special Forces component.
- There is no requirement for the capability of Czech armed force to respond to prompts in an extremely short time frame. There is no mechanism for a rapid request or forces and equipment for Czech armed to strengthen the Police CR for the purposes of carrying out tasks related to ensuring security in the CR.
- The lengthy process of acquiring weapons, equipment, and other material by way of public procurement in case of a need for a rapid response.
- The absence of a mechanism for the preparation and involvement of the public in case of a widespread threat to national internal security or for ensuring the functioning of the state in emergencies.
- Inadequate capacities of professional staff that can ensure cybersecurity monitor and analyse cyberattacks and eliminate them.
- Inadequate screening of providers of ICTs ad ICT products (software and hardware) in important national security institutions. Poorly set cybersecurity policies in these institutions and the underestimation of employee education in the area of cybersecurity.
- The absence of a systematic approach and efficient tools for the implementation of strategic communication by the Government and other public administration institutions.
- The propensity of a part of the population to be influenced by propaganda and disinformation campaigns and the doubting/underestimation of the existence of such propaganda by some public figures.
- Insufficient material and technical conditions in a number of state institutions, which hinders the creation of a safe communication environment and the use of modern ICTs for the purposes of ensuring national defence and security and crisis management.

Opportunities

- Extensive information sharing and experience within NATO and EU concerning efficient methods and tools to face hybrid campaigns and strengthen the overall resilience of society against an attack.
- NATO and EU are currently working on defining their approach to hybrid campaigns led against them (or against their member states) and are simultaneously working intensively on setting up mechanisms of mutual cooperation and assist their member states in the event of a hybrid attack. The CR can actively participate in these processes, influence their results and use the experience to adapt its own security system accordingly.
- The possibility to use NATO and EU crisis management exercises focused specifically on scenarios of hybrid attacks in order to test the overall readiness of the Czech security system.
- The fact that political parties represented in the Chamber of Deputies of the Parliament (with the exception of the Communist Party of Bohemia and Moravia) declared their responsibility for the safety of Czech citizens and their determination to push through the steps necessary for ensuring the defence of the country in March 2014.

Threats

- A number of partial adverse factors that are also relevant in the context of a hybrid threat have been identified in other chapters, in particular in the chapters on Influence of Foreign Powers and Cyberthreats. These may be complemented by more general threats relating to the entire security sector.
- An unexpected turn of events that would lead to the prioritisation of public expenditure of the CR in favour of sectors other than security and defence.
- The tendency of some states, NATO and EU members, to show restraint in sharing sensitive intelligence.
- The stagnation in strengthening and deepening mutual cooperation between NATO and EU.

D. Recommendations to Strengthen Resilience

The assessment of the possible threat posed to the CR by a hybrid campaign, in light of current instruments and institutional capacities of the security system, does not lead to any alarming conclusions. The legislative and operative tools of individual institutions are generally adequate. Nevertheless, the CR has certain deficiencies when it comes to its abilities to face a hybrid campaign in the most efficient way. In order to remove these deficiencies, the following measures are recommended:

1. Create, within the Czech security system, a platform for sharing information that will converge information and knowledge based on which it will be able to identify a potential hybrid campaign. It is not necessary to establish a new institution; merely to create a specific capacity of people with the required expertise within existing institutions, retaining their powers, under valid legislation.

2. Create a system of warning indicators that would help institutions other than intelligence services to capture information that may contribute to identifying an ongoing hybrid campaign.
3. Define a strategic approach of the CR to counter hybrid campaigns conducted against it or against another NATO or EU member state (as part of the Security Strategy of the CR or as a separate strategic document). In doing so, build on the analysis of benefits of international cooperation, primarily within EU and NATO.
4. Focus, within specified crisis management exercises, on testing the infrastructure and the procedures ensuring the functioning, including the decision-making process, of the state in demanding situations.
5. Alter the structure of Czech armed forces and their readiness to respond to the new objectives of NATO defence planning. These objectives express the contribution that the CR is expected to fulfil within its commitment to joint defence and reflect also the requirements for the adaptation of NATO to a new security environment. The ministers of defence will approve these objectives in June 2017.
6. Simplify the process of acquisition of equipment and services for armed forces through public procurement so as to enable their purchase in a very short time, especially in protecting important security interests of the CR.
7. Adapt the legislative framework so as to facilitate the active involvement of intelligence services in the implementation of measures to counter a hybrid campaign conducted against the CR or NATO and EU states.
8. Assess whether the existing configuration of options for using Czech armed forces (individuals and units) to ensure national security is also adequate in the context of hybrid threats.
9. Explore the possibility of creating a mechanism for the preparation and participation of the public in case of a widespread threat to internal security or the functioning of the state in emergencies, as part of the implementation of the strategy to protect the population and preparation of citizens to defend the state.
10. Create conditions for efficient and credible Government strategic communication, i.e. establish a conceptual approach and set up a mechanism for the systematic coordination of all relevant public administration actors.
11. Strengthen civic education in schools (basic values, media literacy, and action during emergencies).
12. Within exercises and testing related to security and resilience of key cybernetic infrastructure, regularly apply the scenario of a hybrid attack (focus on the energy distribution system, state administration information systems, etc.).
13. Using modern ICTs, ensure a safe communication environment for the purposes of all kinds of crisis management.

ABBREVIATIONS

CAO	central administration office
CBRN	chemical, biological, radiological, and nuclear substances and materials
CEI	Czech Environmental Inspectorate (*Česká inspekce životního prostředí*)
CHMI	Czech Hydro-Meteorological Institute (*Český hydrometeorologický ústav*)
CR	Czech Republic
CYSA	Cybersecurity Act (*zákon o kybernetické bezpečnosti*)
EMCS	economic measures for crisis situations
EMS	Emergency Medical Service
ERA	Energy Regulatory Authority (*Energetický regulační úřad*)
EU	European Union
FPU	fire protection unit (*jednotka požární ochrany*)
FRS	Fire Rescue Service of the Czech Republic (*Hasičský záchranný sbor ČR*)
IRS	integrated rescue system
IWSS	Integrated Warning Service System
LGU	local Government unit
MA	Ministry of Agriculture
MC	Ministry of Culture
MD	Ministry of Defence
ME	Ministry of Environment
MEYS	Ministry of Education, Youth, and Sports
MH	Ministry of Health
MInt	Military Intelligence
MIT	Ministry of Industry and Trade
MoI	Ministry of the Interior
MJ	Ministry of Justice
MRD	Ministry of Regional Development
MT	Ministry of Transport
NATO	North Atlantic Treaty Organisation
NOCACOS	National Organisation for Coordinated Action in Case of Oil Shortage
NSA	National Security Authority (*Národní bezpečnostní úřad*)
NSC	National Security Council (*Bezpečnostní rada státu*)

OFRI	Office for Foreign Relations and Information (*Úřad pro zahraniční styky a informace*)
Police CR	Police of the Czech Republic (*Policie České republiky*)
PR	Public Relations
RMN	radiation monitoring network
SEI	State Energy Inspectorate (*Státní energetická inspekce*)
SIS	Security Information Service (*Bezpečnostní informační služba*)
SMRA	State Material Reserves Administration (*Státní správa hmotných rezerv*)
SONS	State Office for Nuclear Safety (*Státní úřad pro jadernou bezpečnost*)
SS 2015	Security Strategy of the Czech Republic 2015 (*Bezpečnostní strategie ČR 2015*)
SVA	State Veterinary Administration (*Státní veterinární správa*)
UNO	United Nations Organisation

NATIONAL SECURITY AUDIT

Issued by the
Ministry of the Interior of the Czech Republic, Security Policy and Crime Prevention Department
Nad Štolou 3, 170 34 Praha 7, Czech Republic

Prague, 2016
This text has not been proofread.