NATIONAL STRATEGY FOR COUNTERING HYBRID INTERFERENCE

NATIONAL STRATEGY FOR COUNTERING HYBRID INTERFERENCE

Prague 2021

CONTENTS

1. BASIC FRAMEWORK OF THE NATIONAL STRATEGY FOR COUNTERING HYBRID INTERFERENCE

1. The National Strategy for Countering Hybrid Interference (Strategy)[1)] defines objectives and determines instruments essential for the protection of vital, strategic and other important interests of the Czech Republic laid down in the Security Strategy of the Czech Republic (Security Strategy) against hostile hybrid interference. The Strategy is based on the Security Strategy and is also in conformity with other national security policies, particularly with the Defence Strategy of the Czech Republic and the National Cyber Security Strategy of the Czech Republic. The development of the Strategy was tasked by the 2016 National Security Audit. The Strategy complements the existing system of security policy documents by formulating a comprehensive nationwide policy to counter hybrid interference.

2. The security of the Czech Republic is indivisible from the security of the Euro-Atlantic region. The Strategy is thus based on fundamental strategic documents of the North Atlantic Treaty Organisation (NATO) and the European Union (EU). It relies on the principle of solidarity among NATO Allies and EU Member States, and adheres to the member countries' common goals. The Strategy is in conformity with relevant NATO and EU documents.[2)]

1) The Strategy was developed in accordance with the Public Strategy Development Methodology authorised by the Czech Government Resolution No. 71 dated 28 January 2019.

2) For example, the EU Council conclusions on complementary efforts to enhance resilience and counter hybrid threats adopted on 10 December 2019; Commitment to enhance resilience of NATO dated 8 July 2016; NATO Warsaw Summit 2016 Communiqué dated 9 July 2016; NATO's strategy on its role in countering hybrid threats endorsed in December 2015 by NATO Foreign Ministers; Joint Framework on countering hybrid threats dated 7 April 2016; revised European Union Concept for EU-led Military Operations and Missions approved 2 December 2019.

3. Hybrid interference involves both covert and overt actions by state as well as non--state actors (perpetrators of hybrid interference), which target vulnerable elements of democratic states and societies. The perpetrators' aim is to disrupt the working of democratic institutions, rule of law processes, and internal security. They utilize political, diplomatic, information, military, economic, financial, intelligence, and other tools. Hybrid interference also makes use of legal and seemingly legitimate instruments to achieve hostile objectives and undermine the interests of the Czech Republic. The speed, scope, and intensity of hybrid interference have increased, partially as a result of new technology development.

4. In the Czech Republic, the primary executive institution responsible for countering hybrid interference is the Government of the Czech Republic.[3)] The Government itself also takes measures in response to specific manifestations of such threats. The responsibility for countering individual activities and manifestations of hybrid interference lies with relevant public institutions. That includes securing organisational infrastructure and personnel capacity. The State Security Council, an advisory body to the Government, provides platforms for information sharing among public institutions and coordination of countering hybrid interference.

5. In the domain of countering hybrid interference, the Government of the Czech Republic lays down the following strategic objectives:

   - Resilient society, resilient state, resilient critical infrastructure;

   - Systemic and holistic approach of the Czech Republic, and;

   - The capability of adequate and timely reaction.

3) In accordance with the Competence Act (Act No. 2/1969 Coll. of the Czech National Council, on the Establishment of Ministries and other Central Government Authorities of the Czech Socialist Republic (the Competence Act), § 28, paragraph (1)), the responsibility for readiness and response to individual activities and manifestations of hybrid engagement is vested with the Ministries and other Central Government Authorities in the scope of their respective remits.

2. STRATEGIC CONTEXT

6. As the Security Strategy articulates, the security environment of the Czech Republic is undergoing dynamic changes. The environment's predictability has decreased due to a growing interconnectedness of security trends and factors. Although the likelihood of a massive military attack directly threatening the Czech Republic's territory remains low, hostile activities using a broad spectrum of tools of hybrid interference do represent a threat to the security of the Euro-Atlantic region, including the Czech Republic.

7. The perpetrators of hybrid interference can be both state and non-state actors. Hybrid interference is comprehensive and can therefore only be countered through a whole--of-society approach. It must include not only security services and government authorities, but also relevant elements of commercial, media, educational, and non-profit sectors. The perpetrators target key elements of the functioning of the state and society, and use a flexible combination of diplomatic, informational, military, economic, financial, intelligence, and legal tools. The state actors targeting the Czech Republic through hybrid interference on a sustained and systemic basis are mostly authoritarian and revisionist powers with regional or global power ambitions.

8. Hybrid interference seeks to blur the boundaries between peace, crisis, and conflict. It intentionally strives to be covert, ambiguous, and difficult to attribute to its perpetrator. Hybrid interference makes use of already-existing vulnerabilities and inner divides within the society, aiming to deepen them further. Its goals may include delaying or paralysing political decision-making process (including decision-making in defence and security) or weakening of the citizens' trust in the constitutional system, democratic institutions, and mechanisms. Moreover, it attempts to disrupt economic processes, gain influence in key economic sectors and strategic enterprises, manipulate or take control of the information environment, and weaken or affect the operation of critical infrastructure.[4)] To achieve that, the perpetrators of hybrid interference employ a variety of tools, including malicious activities in cyberspace.

4) In accordance with the Ordinance of the Government of the Czech Republic No. 432/2010 Coll., the critical infrastructure comprises power industry, water management, food industry and agriculture, health system, transportation, communication and information systems, financial market and currency, emergency services and government.

9. Many specific tools and methods of hybrid engagement have already been used in the past. Nevertheless, their scope, complexity, technical sophistication, and the level of organisation has grown. That was enabled by the development and availability of new technologies. The expanding use of modern technologies, such as social networks and other internet applications, creates a range of new vulnerabilities that need to be addressed and reduced.

10. The Czech Republic is exposed to hybrid activities mainly in the following areas:

    a. Ideology and values foundation of the society and the constitutional system of the state;
    b. Economy;
    c. Security and defence.

Ad a: Hybrid interference can include overt or covert influencing of political structures (including political parties) and political decision-making process, courts, police, armed forces, media, and public opinion. The goal is to destabilize or divide the society and undermine the citizens' confidence in values and ideological orientation of the country. It also targets the constitutional system, including the constitutional institutions and the democratic process.

Ad b: Hybrid interference can negatively affect economic interests of the state. It can leverage the Czech Republic's dependency on strategic material supplies from foreign countries such as oil, natural gas, or nuclear fuel. It can take an advantage of the Czech economy's openness and its orientation on export, foreign investment, and loans that are in strategic sectors of the economy or that lead to strategic dependency on their providers. Perpetrators of hybrid interference may seek to take control of strategic economy sectors and individual key enterprises including those forming the Czech Republic's critical infrastructure. Hybrid interference can also manifest itself through the use of modern technologies and technology solutions, such as 5G networks and artificial intelligence, that originate from countries with different ideological and values systems. (These technologies are mainly used by the private sector.) Further risks stem from corruption, links between diplomacy, business, and espionage, or from acting in the interest of foreign powers.

Ad c: The Czech Republic's security can be threatened by overt or covert use of armed violence. That includes violence targeted at the Czech Republic's military engagement in NATO and EU missions, operations, and other activities, as well as aggressive deployment of foreign intelligence services or special forces on Czech territory. Hybrid interference can

include mobilisation of interest groups (defined by religion, ethnicity, nationality, or language) or criminal groups acting against the Czech Republic's security interests and violating public order. Hybrid interference seeking to delay or paralyse decision-making processes in the domain of defence and security also presents a risk. That includes NATO's collective defence and political and military cooperation of the EU.

3. STRATEGIC OBJECTIVES

Resilient society, resilient state, resilient critical infrastructure

11. Resilience is understood as the ability of a state and society to cope with a sustained and intensive hybrid interference without a significant negative impact, and to redress immediately and restore a full functionality in case damage occurs.

12. As part of the national security system, the Czech Republic will strengthen its capability of hostile hybrid activities early detection and their attribution to specific attackers, and its early response capability. The Czech Republic will be able to identify hybrid interference early and will be able to react to it adequately. A public attribution of the hybrid interference perpetrators is a political decision made by the Government.

13. The Czech Republic will continue to strengthen the resilience of the state and the society on the basis of a comprehensive, whole-of-society approach to security. Such resilience will be strengthened to the effect of reducing vulnerabilities exploited by perpetrators of hybrid interference.

14. The Czech Republic will strengthen the capabilities of the critical infrastructure elements to maintain their sufficient functionality for instances of being targeted by hybrid interference.

15. The Czech Republic will employ a robust and transparent screening system for foreign investments into strategic sectors of the economy and key enterprises, especially those comprising the critical or other important state infrastructure.

16. The Czech Republic will reduce its strategic dependency on countries with different ideological and value systems. Such dependency could be used against the interests of the Czech Republic.

17. The Czech Republic will consistently and coherently increase the awareness of its key social groups and the society as a whole of hybrid interference existence and its nature. Countering hybrid interference will also be a part of relevant educational programs and outreach events. To that effect, cooperation will be enhanced among the government, commercial sector, education system, non-profit sector, and civil society.

18. The Czech Republic will continue to strengthen the ability to identify its vulnerabilities and to perform stress tests simulating effects of hybrid interference across the government and critical infrastructure. In this domain, the Government of the Czech Republic will seek to enhance cooperation with the commercial, media, non-profit, and education sectors.

19. The Czech Republic will build a system of strategic communication which will be able to effectively, coherently, credibly, and timely share information with the public and other types of target audience. Which must be done both continuously and preventively, as well as in response to specific emergencies and crises. The system will be based on coordination and synchronisation of communication activities among all relevant Ministries and public institutions.

Systemic and holistic approach by the Czech Republic

20. In order to effectively counter hybrid interference, inter-ministerial cooperation and supra-ministerial coordination will be strengthened. The Czech Republic will increase its capability of coordination and information-sharing among all relevant domestic actors. That will be done with the aim of covering the whole spectrum of tools utilized by hybrid interference and providing a sustained situational awareness in adequate quality. For the purpose of a more efficient information sharing, the State Security Council platforms will be optimised, and the position of Coordinator of Countering Hybrid Interference will be created. Lessons learned from hybrid interference and related issues will be shared within an expert group on a regular basis.

21. The Czech Republic will regularly verify the readiness of its security system to counter hybrid interference through both national and international exercises. The outcomes of such exercises will be used in further efforts to make the Czech Republic's security system more efficient.

The capability of adequate and timely reaction

22. The Czech membership in NATO and the EU is the key instrument to deter perpetrators of hybrid interference. Therefore, the Czech Republic will continue to actively participate in activities and initiatives of NATO and the EU in countering hybrid interference. The Czech Republic will seek to use NATO's and EU's counter hybrid capabilities as well as to contribute to those capabilities tangibly.

23. Solidarity and mutual support of NATO Allies and EU Member States represents an effective instrument of both preventing hybrid interference and responding to its specific manifestations. Therefore, the Czech Republic will actively support unity and solidarity of NATO Allies and EU Members States, including possible collective identification of hostile hybrid activities, which may deter the perpetrators from continuing the activity.

24. The Czech Republic will also support further development of cooperation between NATO and the EU, which is essential to cover the whole spectrum of the used hybrid instruments. In that sense, the Czech Republic will contribute to the activities of other international initiatives, including the European Centre of Excellence for Countering Hybrid Threats in Helsinki, Finland.

25. In order to deter the actors using methods of hybrid interference, the Czech Republic will seek to develop response capabilities designed to increase the cost and reduce the benefit of employing hybrid interference against interests of the Czech Republic. The Czech Republic will define response options to hybrid interference and will regularly exercise those responses.

26. The Czech Republic will continue to work on indicators of hybrid interference enabling an effective and timely response.

27. In response to hybrid interference, the Czech Republic will use its strategic communication system when communicating coordinated national positions. Such communication will target domestic as well as international audiences, including the perpetrators of hybrid interference.

28. The Czech Republic will evaluate and develop options for public attribution of hybrid interference to its perpetrators.

29. The Czech Republic is ready to respond to hostile hybrid activities with retaliatory measures (including sanctions) and other instruments, including instruments by international organisations the Czech Republic is a member of. An adequate response will also involve the development of a capability to evaluate its effectiveness, which will feed back to inform the future course of action.

4. IMPLEMENTATION

30. The Strategy will be updated on a regular basis, following developments in international security environment. The Strategy will be followed by an Action Plan defining specific tasks and steps. The fulfilment of tasks included in the Action Plan will be reviewed annually and the plan will be updated as needed.