Operational Programme
Effective
Public Administration

European Union
European Social Fund

SLOVAK REPUBLIC HYBRID THREATS VULNERABILITY STUDY

Executive Summary

GLOBSEC
IDEAS SHAPING THE WORLD

Supported by the European Social Fund

SLOVAK REPUBLIC HYBRID THREATS VULNERABILITY STUDY
Executive Summary

This text is an Executive Summary of a study mapping the vulnerability of public administration in the Slovak Republic towards hybrid threats. The study has been conducted within a project "Increasing Capacities and Preparedness of Public Administration for Hybrid Threats" led by GLOBSEC. It is a first-of-its-kind study that offers a basic overview of the state of public administration in the Slovak Republic vis-a-vis hybrid threats while identifying key gaps and offering a number of recommendations.

The full text is available in Slovak online at GLOBSEC's website.

AUTHORS

Daniel Milo

Pavol Draxler

Katarína Klingová

Matúš Mišík

Michal Piško

The report has been issued within a project "*Increasing Capacities and Resilience of Public Administration to Hybrid Threats*" realised by Operational Programme Effective Public Administration supported by the European Social Fund.

GLOBSEC, Bratislava, October 2018

GLOBSEC
Vajnorská 100/B
83104 Bratislava
www.globsec.org

Hybrid threats represent a new type of threat to security interests of the Slovak Republic, which surpasses current security frameworks and tools and as such requires a new, coordinated and holistic approach from public administration. The level of awareness and knowledge of hybrid threats within the public administration is not sufficient while a narrow-based approach of various public administration's sections towards different types of threats still dominates. At the same time, central public administration authorities lack capacities to conduct a complex analysis using diversified data and inputs to develop public policies.

To fill in these gaps, GLOBSEC is implementing a project "Increasing capacities and readiness of public administration for hybrid threats," which aims to:

- **Support the development of public policies** linked to prevention and elimination of hybrid threats (processes, experience-sharing, mapping, recommendations, creation of platforms);
- **Support expert and analytical capacities** of public administration in the area of monitoring, evaluation and elimination of hybrid threats;
- **Increase overall awareness of public administration about hybrid threats.**

Hybrid threats represent a *"mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes."*[i]

All countries of the world use various means to pursue their geopolitical, ideological, or political interests - from diplomacy, energy and financial policies to the use of secret service and deployment of armed forces. As it is possible to observe, for example on the development of the security situation in the vicinity of the Slovak Republic, the forms of interstate conflicts have changed, and military warfare has been replaced by a combination of various coordinated efforts and actions with nearly the same impact as an actual military occupation. These types of attacks, which are hidden, subversive and can be directed and coordinated centrally by state or non-state actors in order to achieve specific political objectives are called **hybrid threats.**

The most common tools used therein include:

1. External or internal political pressure on top state officials and state institutions;
2. Economic or energy pressure as part of political influence;
3. Extensive sabotage against key infrastructure;
4. Cyber-attacks with the potential to cause large-scale damage;
5. Information and propaganda operations to undermine confidence in state institutions, trigger social unrest and severely destabilise political and security stability;
6. Influencing ethnic, religious and cultural minorities and manipulating them for political purposes;
7. Threat of using military force;
8. Activities of irregular/paramilitary armed groups disloyal to the government;
9. Espionage and subversive activities of intelligence service;
10. Strategic corruption driven by political motives;
11. Election meddling by foreign actors.

INSTUTIONS AND PUBLIC POLICIES

The issue of hybrid threats has been given a considerable attention in the European Union (EU) and NATO, and several documents have been adopted to this end.[ii] Specialised institutions, such as the European Centre of Excellence for Countering Hybrid Threats, EU Hybrid Fusion Cell within the European Union Intelligence and Situation Centre, NATO Strategic Communications Centre of Excellence, and NATO Cooperative Cyber Defence Centre of Excellence, have been established.

So far, the EU's most prominent and comprehensive public policy on hybrid threats is the *Joint Framework on countering hybrid threats* from April 6, 2016.[iii] The framework was adopted by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy in order to activate a synchronised response at the EU level and to capitalise on the European solidarity, mutual assistance, and the Lisbon Treaty.

The most recent document adopted by the EU in this regard is the *Joint Communication to the European Parliament, the European Council and the Council: Increasing resilience and bolstering capabilities to address hybrid threats*[iv] from June 2018. In its text, the European Commission states that hybrid activities continue to pose a serious and acute threat to the EU and its Member States, with intensifying efforts to destabilise countries.

In the context of the Slovak Republic (SR), the concept of hybrid threats appeared for the first time in public policies in 2016 in the *White Paper on the Defence of the Slovak Republic*[v] and was subsequently considered during the drafting of *Security Strategy of the Slovak Republic*. In terms of complexity and relevance, the most important nation-wide document focusing solely this topic is the *Framework of the Slovak Republic on Countering Hybrid Threats*[vi], which was adopted by the Government of the Slovak Republic on July 11, 2018 by the Resolution no. 345/2018. The Framework has three main sections. The first section describes the change of the security environment and the reasons why hybrid attacks are increasing in frequency. The second section describes the situation in the Slovak Republic and draws attention to several key vulnerabilities. The final section describes the institutional framework and lists the indicators of hybrid attacks and practical methods of their identification.

An equally important part of the Framework is the definition of monitoring and response competences and duties of individual authorities and institutions. In line with the Framework´s definitions, the Situational Centre (SITCEN) established at the Government Office of the Slovak Republic, acting as a national contact point for hybrid threats, and the National Security Analytical Centre (NBAC) established in the Slovak Information Service, acting as a national hybrid threat cooperation centre, play the primary role in this regard.

GAPS AND VULNERABILITIES IDENTIFIED IN THE STUDY

During the initial mapping process of hybrid threats in the Slovak Republic, the authors of this study identified a number of gaps and vulnerabilities.[vii] The following aspects are of the highest importance:

1. Insufficient strategic communication capacities of the state institutions.
2. Insufficient analytical capabilities in cyber security and the absence of specific actions with clear feasibility criteria aimed at improving the current status.
3. Insufficient attention of the energy infrastructure on the possibility of hybrid threats and impact of potential attacks on the infrastructure, which can be more far reaching than power blackouts.
4. No legal regulation of paramilitary groups.
5. Insufficient consideration of the impact of foreign subversive efforts on security and stability of the Slovak Republic.
6. Absence of consideration of non-financial motivation in anti-corruption legislation - strategic corruption with political intents and involvement of foreign actors.
7. Current legislation on the funding of political parties and electoral campaigns does not contain provisions to identify real contributors/donors acting on behalf of third parties.
8. Non-existence of specific legislation on electoral campaigns on the Internet and social media.

RECOMMENDATIONS

The most important recommendations to address the above-mentioned vulnerabilities are the following:

1. Adopt a comprehensive whole-of-government approach in the area of strategic communication covering all relevant bodies of public administration.
2. Establish specialised national units focusing on strategic communication across all relevant sectors.
3. Create cyber security analytical units dealing with the preparation of public policies.
4. Adopt an action plan on cyber security with clear measurable criteria.
5. Systematically deal with the issue of hybrid/cyber threats in strategic documents regarding energy policy and/or energy security.
6. Pay more attention to the specifics of the energy sector, which differs from other areas of critical infrastructure, since hybrid threats in this area have far reaching consequences not only on the energy security but also on the so-called “hard security”.
7. Identify hybrid threats and solutions not only at public/state administration but also within the (semi) private energy sector, which is essential for maintaining energy security.
8. Consider “smart” technologies when assessing hybrid threats to energy security.
9. Amend legislation on arms and ammunition and adopt legislation regulating the operation of paramilitary groups and their support by foreign actors.
10. Create easy-to-access, low-threshold alternatives for youth interested in military and history under the state supervision and with the involvement of the Slovak Armed Forces.
11. Apply consistently the provisions of the Criminal Code regarding participation in combat activities of an organised armed group in the territory of another state and its support.
12. Strengthen international and domestic tools to detect suspicious financial flows through shell companies and tax havens with regard to politically motivated strategic corruption.
13. Analyse non-financial aspects of corruption and embed the concept of strategic corruption into public policies and legislation.
14. Adopt legislation regulating transparent funding of political parties throughout the electoral mandate, not only during election campaigns.
15. Change the list of subjects eligible to finance election campaigns during the elections to the National Council of the Slovak Republic and to the European Parliament to be on par with the presidential elections.
16. Introduce the duty to disclose the information on the buyers of political ads even outside of the campaign period.

REFERENCES

[i] European Commission, *Joint Framework on countering hybrid threats: A European Union response*, June, April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en

[ii] European Commission, *Joint Framework on countering hybrid threats: A European Union response*, June, April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en, European Parliament, Countering hybrid threats: EU-NATO cooperation, Briefing March 2017, http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf

[iii] European Commission, *Joint Framework on countering hybrid threats: A European Union response*, April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en

[iv] European Commission, *Joint Communication to the European Parliament, the European Council and the Council: Increasing resilience and bolstering capabilities to address hybrid threats,* June 2018, https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf

[v] Ministry of Defence of the Slovak Republic, *White Paper on the Defence of the Slovak Republic,* September 2016, https://www.mod.gov.sk/data/BKO2016_LQ.pdf

[vi] Government of the Slovak Republic, *Framework of the Slovak Republic on Countering Hybrid Threats,* July 2018, http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=27668

[vii] The information in this publication is current as of October 1, 2018.