MILITARY INTELLIGENCE ANNUAL REPORT

2020

CONTENT

FOREWORD BY THE DIRECTOR OF THE MILITARY INTELLIGENCE

Dear Readers,

First of all, let me thank you for your interest in the activities of the Military Intelligence, an established institution within the security system of the Slovak Republic and a trusted partner of Allied intelligence services of NATO, the EU and other countries. I am delighted to introduce to you an unclassified version of the Annual Report on the activities of the Military Intelligence for 2020 within the purview of Act No. 198/1994 Coll. on Military Intelligence. With the Annual Report, we provide you with information on current security issues in selected areas of interest and at the same time with a picture of our work.

The mission of the Military Intelligence is to provide objective, timely and unbiased information to authorized users. At the same time, we recognize the need to adequately inform also the general public. In 2020, the Military Intelligence provided hundreds of reports and assessments to authorized users and contributed significantly to the practical provision of national security and the development of the Armed Forces of the Slovak Republic.

The nature of the current security threats confirms the trend of a deteriorating security situation in the world. Intelligence services also face the challenge posed by the growing interconnectivity of different types of threats and the increasingly blurred distinction between military and non-military threats, including higher demands on their staff. Let me therefore take this opportunity to thank all members of the Military Intelligence for their high quality of work, perseverance and responsibility in the performance of their duties.

Brigadier General Ing. Róbert KLEŠTINEC
Director of the Military Intelligence

INTRODUCTION

Within the scope of its responsibilities, the Military Intelligence (hereafter as the "MI") collects, gathers, and evaluates information important for ensuring the defence and defence capabilities of the Slovak Republic (hereafter as the "SR"). The present Annual Report on the activities of the MI for 2020 reflects changes in the internal and external security environment of the SR in 2020.

In the assessed period, the dynamics of the development of the security environment of the SR was significantly influenced by the COVID-19 pandemic. The MI was fast to adapt to the new situation and has fully fulfilled the tasks of intelligence provision for the purposes of ensuring national defence within the scope of the Ministry of Defence (hereafter as the "MoD") of the SR, as stipulated in Act No. 198/1994 Coll. on MI.

In 2020, the MI continued to collect and gather information and evaluate security threats, especially of a military nature. However, an increasing trend within the threat landscape towards information space and cyberspace was noted, accompanied by a growing number and increased intensity of cyber-attacks and influence operations by different actors in order to polarize the society in the SR and weaken the legitimacy of state institutions. In the context of hybrid operations, activities of foreign intelligence services in the SR have been on the rise.

The anti-pandemic measures taken at the state level were exploited by individuals, groups, including groups with the support from foreign powers, to deepen distrust of state institutions and to draw new dividing lines in society. The continued rapid development of information and communication technologies poses not only new political, economic and military opportunities, but also major security threats to the civilian and military sector.

In 2020, the MI paid intensive attention to these internal threats, evaluated their negative impact on the protected values of the SR and their effect on the security environment of the SR. The MI provided information on these threats and their possible ramifications to authorized users in order to support their decision-making process.

The security and defence capabilities of the SR have been influenced by negative trends in the external security environment of the SR of the last decade. During this period, local and regional conflicts have arisen, violations of international law occurred, and new non-state actors with the ability to advance their interests by exploiting hybrid methods of warfare (including cyber as well as information and psychological operations) emerged. These trends will almost certain persist in the coming years with possible implications for the security and defence of the SR.

On June 16, 2021, the MI submitted a detailed description of its activities in 2020 as part of the classified "Report on the Activities of the MI for 2020" to the members of the Military Intelligence Oversight Committee (hereafter as "Committee") of the National Council of the SR and the Committee took note of the report. Subsequently, on December 1, 2021 MI presented its "Report on the fulfilling of tasks of the MI in 2020" to the national deputies of the Slovak parliament.

FULFILLMENT OF TASKS STIPULATED BY LAW

In 2020, the MI fulfilled the tasks of intelligence provision for the purposes of ensuring national defence by providing intelligence within the scope of the MoD of the SR as stipulated in the Act No. 198/1994 Coll. on MI.

The MI performed its statutory tasks taking into account the full spectrum of identified and anticipated security threats that act or may act against the protected values and interests of the SR in the internal and external security environment, including cyberspace.

Ensuring the defence of the SR and military-economic interests of the SR

In the area of defence capabilities of the SR, the MI focused on obtaining and evaluating information related to the construction of modern and interoperable, well-armed and trained Armed Forces (hereafter as the "AF") of the SR capable of defending the territory of the SR, deployable within the framework of national and international crisis management and at the same time fulfilling our commitments to NATO and EU.

In cooperation with the relevant components of the MoD of the SR and the AF of the SR, the MI participated in the defence planning process, which represents a critical element for ensuring security and defence of the SR.

The quality and level of training of the AF of the SR have long been negatively affected by insufficient personnel staffing, retirement of experienced individuals and the high failure rate of morally and technically obsolete armaments. The long-term declining trend in the operability of military equipment is caused by overall obsolescence, insufficient supply of spare parts and uncoordinated and unsystematic provision of repairs by contractors.

The unfavourable technical conditions of the armament and equipment of the AF of the SR and the restrictions on the military training of personnel to be deployed abroad associated with the COVID-19 pandemic affected also the fulfilment of tasks within the framework of international crisis management in NATO, EU and UN operations and missions.

The delay in the build-up of the declared heavy mechanized brigade was again negatively assessed by the NATO Defence Planning Committee.

In the area of implementation of modernization projects, the attention of the MI was mainly focused on the progress and overall effectiveness of the envisaged and ongoing projects from the point of view of achieving a real improvement of the capabilities of the AF of the SR, such as multipurpose fighter aircraft F-16, combat armoured vehicles 8x8, and self-propelled howitzers Zuzana-2.

Special attention was further paid to the possible manifestations of corruption and cronyism, abuse of power by senior employees of the MoD and uneconomic or ineffective performance within the scope of the MoD.

Operation JOINT RESPONSIBILITY

Within the scope of performing assistance tasks on behalf of the Ministry of Interior (hereafter as the "MoI") of the SR, further legislative, personnel and material limits of the AF of the SR were identified, which significantly affected the deployment of the AF of the SR within the framework of domestic crisis management.

Operation SPOLOČNÁ ZODPOVEDNOSŤ (JOINT RESPONSIBILITY) was widely used in the anti-government propaganda by activists, antisystem online groups and alternative media, as well as right-wing extremist entities, leading to increased polarization of society and anti-government sentiment. The deployment of the AF of the SR was also exploited for agitation by various pro-Russian interest groups.

For the most part, negative reactions were not directed against members of the AF of the SR, but focused primarily on the top representatives the AF of the SR and the MoD of the SR. On a regular basis, the President of the SR as the Commander-in-Chief of the AF of the SR was defamed, as was her authority to influence the decisions of the Government of the SR on the deployment the AF of the SR. The AF of the SR were presented as a strong institution that acts on orders and as an instrument of power that is being abused in order to achieve the objective pursued.

Development of the security situation in the close neighbourhood of the SR

Russian Federation

From a geopolitical point of view, the Russian Federation constitutes the greatest military security challenge for both the SR and the interests of NATO

member countries. However, the probability of an open military conflict between NATO and the Russian Federation is assessed as low in the midterm. The Russian Federation continues to strengthen the capabilities of its AF, primarily in the Western and Southern Flank. The AF of the Russian Federation were continuously supplemented with new or modernized equipment, however, the share of such equipment increased only marginally compared to the previous year.

Effects of global warming, coupled with improved access to raw materials and the opening of routes for international trade in the Arctic play into a rise in geopolitical rivalry, to which the Russian Federation is responding by strengthening its military capabilities in the region. In the long term, the Arctic is of fundamental economic importance to the Russian Federation.

The COVID-19 pandemic did not have a significant impact on the combat readiness and training of the AF of the Russian Federation. In 2020, they continued to perform tasks with adjustments for operating under aggravated anti-epidemic conditions.

Under the guise of combating the spread of the pandemic, the Russian Federation took the opportunity to extend its geopolitical reach over the geographical areas of the Middle East, Africa, Asia, Latin America and partially Europe. It also continued its engagement in the crisis areas of the Middle East, Africa, Ukraine and the peacekeeping operation launched by the Russian Federation in Nagorno-Karabakh in 2020. The MI also paid attention to Russian private military companies and their utilisation by the Russian Federation as a grey zone tool for achieving military-political goals and interests without the direct involvement of state security forces.

The Russian Federation also continued exploiting hybrid methods of conducting combat operations. Ukraine, the Baltic States and the so-called Eastern Flank of NATO, were not only areas with the highest level of hybrid activities but also posed an increased potential for endangering the protected values and interests of the SR. NATO's Enhanced Forward Presence in the Baltics is being used by the Russian Federation as a pretext to disseminate disinformation and false information about the activities of NATO military personnel (including accusations of the spread of the COVID-19 pandemic in the region) and for influencing public opinion through negative propaganda. The Russian Federation has actively sought to extend its influence on domestic and foreign policies of individual NATO member

states, including by conducting intelligence activities, exerting influence on politicians, providing support to pro-Russian activists, and through cyber-attacks.

Under the State Armament Programme, the Russian Federation envisaged the start of mass production of a new generation of combat equipment from 2020 onwards. New types of equipment developed by the military-industrial complex (hereafter as "MIC") of the Russian Federation show a high level of combat capabilities. Nevertheless, they will highly likely replace only a small part of the obsolete military equipment over a timeframe of the next five to ten years. The main reasons are high prices, the unfinished state of projects and qualitatively obsolete and quantitatively insufficient production capacities of the MIC companies of the Russian Federation, as well as limited access to some technologies from countries of the so-called West due to the persistence of restrictive measures and economic sanctions.

Republic of Belarus

The security situation in the Republic of Belarus has deteriorated following the controversial presidential elections in August 2020. The current security situation in the Republic of Belarus is relatively stable, but political and civil opposition is being suppressed and no major political changes are expected in the short term. At the same time, the military cooperation between the AF of the Republic of Belarus and the Russian Federation has been further enhanced, while the Russian Federation has further fortified its political and economic influence in the country. In order to stay in power, the Belarussian regime has not many other options left.

By monitoring the MIC of the Republic of Belarus, economic problems were observed. The MIC of the Republic of Belarus is strongly export-oriented, with approximately 70% of its production currently intended for export. The Russian Federation remains the largest importer of MIC production in the Republic of Belarus, however, the share of exports to the Russian Federation is gradually declining.

Ukraine

A ceasefire agreement has resulted in an improved security situation in the eastern part of Ukraine in the second half of 2020. However, international negotiations to resolve the conflict in the format of the Trilateral Contact Group continued without achieving substantial progress.

In September 2020, Ukraine adopted the National Security Strategy, confirming the strategic direction of its foreign policy aimed at NATO and EU membership.

By evaluating the domestic political situation, the consequences of the COVID-19 pandemic have shown that without the help of oligarchs the Ukrainian government is unable to maintain the function of the state apparatus and that oligarchs are likely to continue to have a significant impact on state functioning.

As far as the MIC of Ukraine is concerned, production stagnated in 2020 and even decreased in some areas. This fact affected the fulfilment of the State Defence Contract for 2020, which was implemented only to approximately 45% and also impacted negatively on the development of the AF of Ukraine. The MIC of Ukraine is facing financial problems and several of the associated enterprises are on the verge of bankruptcy.

Other geographical areas

The MI continued to monitor and analyse threats and the security situation in zones of instability and conflict in the Commonwealth of Independent States (hereafter as "CIS"), the Western Balkans, the Middle East and North Africa. The negative development of the security situation in these regions affects the security environment of the Euro-Atlantic area and may also affect possible requirements for the deployment of the AF of the SR to conflict areas within present and prospective commitments of the SR towards NATO and the EU. The MI provided authorized users with relevant information about the development of the security situation in these areas and possible effects on the security of the SR and the Euro-Atlantic area to support their decision-making process.

Activities of foreign intelligence services

The MI paid attention to the long-term presence and activities of foreign intelligence services operating on the territory of the SR against protected values and interests of the SR, NATO and the EU. In 2020, Russian and Chinese intelligence services were at the helm of hostile activities directed against the protected values and interests of the SR both at home and abroad. The MI also kept under scrutiny activities of intelligence services of several CIS countries, whose actions may have a negative impact on the security of the SR, NATO and the EU.

In 2020, the nature of the activities of foreign intelligence services was strongly determined by the global COVID-19 pandemic, which had an impact on the activities of individual intelligence officers as well as the strategic interests of the main geopolitical actors.

The blurring of boundaries between the military and civil domain and the use of non-military tools to achieve military goals were both recorded. Several monitored entities were conducting influence activities aimed at members of the AF of the SR through propaganda or disinformation. The MI also registered an increased interest of foreign intelligence services in Big Data or health information (COVID-19, genetics).

Foreign intelligence services used the territory of the SR also for conducting so-called cross-border operations, i.e. execution of various phases of intelligence operations by the intelligence services of foreign powers in several countries.

Russian Federation

In 2020, the presence and activities of members of the Russian intelligence services posed the highest security threat in terms of foreign intelligence activities on the territory of the SR. Their intelligence interest was directed at acquiring sensitive and classified information relating to the defence of the SR, capabilities, structure and training of the AF of the SR, as well as NATO activities. Moreover, activities of the Russian intelligence services employing means and methods of information warfare and confrontation (hybrid action) with a negative impact on the social and political cohesion of the SR were recorded.

Hybrid activities of the Russian intelligence services aimed at exploiting growing antisystem moods and opposing attitudes within the Slovak society have been constantly on the rise. These activities are either directly controlled by Russian entities operating in the SR, conducted by domestic entities with the support of the Russian Federation, or carried out by autonomous individuals who are sympathetic to such agenda. Together they create an information network with broad-based and subliminal effects on the Slovak society, while the Russian Federation is seeking to progressively increase its influence. Such effects were noticeable in the fields of diplomacy, media, economic support, learning and education sector, history and culture. They were aimed in particular at building a positive image of the Russian Federation and undermining both the confidence in the Slovak political system and the credibility of the EU and NATO.

In the period under review, three members of the Russian diplomatic staff in the SR were declared persona non grata. The reason for their expulsion was the abuse of Slovak visas for conducting a special operation by the Russian intelligence services in Germany coupled with activities of the Russian diplomatic staff in the SR in contradiction to Vienna Convention on Diplomatic Relations. These persons were identified as members of the Russian intelligence services, who carried out intelligence operations on the territory of the SR, or participated in operations directed against the interests of the SR.

People's Republic of China

Chinese intelligence activities in the SR comply with their long-term effort to acquire contacts and penetrate the defence sector of the SR in order to obtain classified information.

The practices of so-called industrial espionage were recorded that are characteristic of the People's Republic of China global reach. Chinese companies with ties to the state are striving to gain research and development products at selected Slovak companies with the likely objective of copying them for subsequent self-production.

Asymmetric threats against values protected in the SR, NATO and the EU

Terrorism, financing and support of terrorism

The MI continuously collects and analyses information regarding possible terrorist threats in the territory of the SR, including possible radicalization of members of the AF of the SR, activities of militant and terrorist groups as well as activities of radicalized individuals within the EU member states. The main focus was directed towards an early identification of so-called lone-wolves and autonomously operating terrorist cells.

In the assessed period, the MI did not observe any indicators that would confirm the direct threat of a terrorist attack or planning of a terrorist attack in the SR. However, religiously motivated terrorism as well as activities of international Islamist terrorist groups and radicalized individuals still pose a real terrorist threat to EU member states, including the SR.

The main terrorist threat in the period under review stemmed from individuals inspired by the jihadist propaganda of global Islamist terrorism groups, namely the so-called ISLAMIC STATE and AL-QAIDA. During the year 2020, the MI recorded 18 terrorist attacks in Europe. An Islamist religious motive was either directly confirmed or highly likely in a substantial number of these attacks.

One terrorist attack was carried out in VIENNA (Austria) on 2 November 2020. The perpetrator, Kujtim FEJZULAJ, holder of North Macedonian citizenship, had visited the SR several months prior to the attack (July 2020). He unsuccessfully attempted to buy ammunition for an assault rifle in BRATISLAVA. His activities in

the SR were detected by the security forces of the SR and the information was shared with Austrian authorities.

In 2020, terrorism related court trials were held in the Czech Republic against two men with ties to the SR. Dominic KOBULNICKÝ (alias Abdul RAHMAN), a Slovak citizen who converted to Islam, was sentenced to five years in prison by the High Court in PRAGUE in July 2020. He was also banned from entering the Czech Republic for ten years. KOBULNICKÝ was found guilty of supporting and promoting terrorism. In May 2020, Samer SHEHADEH, a man of Palestinian origin, who had formerly acted as an imam in PRAGUE and had preached also in a Muslim prayer house in BRATISLAVA, was sentenced to ten years in prison in PRAGUE. He was found guilty of belonging to a terrorist group and financing terrorism.

The Slovak Muslim community continues to be regarded as non-conflicting and opposed to violence. In line with this, the Muslims living in the SR condemned the above mentioned VIENNA terrorist attack.

In 2020, the MI did not detect any indications suggesting an inclination of members of the AF of the SR or MoD employees to a radical interpretation of Islam.

Political and religious extremism affecting the performance of the AF of the SR and extremism in the ranks of professional soldiers

The MI continued to collect and analyse information related to persons and entities with links to the defence sector who support right-wing extremist (hereafter as "RWE") ideologies. In 2020, both the level of action and coordination among RWE supporters have been on the rise. Such activities were detected also among members of the AF of the SR. Several former professional soldiers have been involved in efforts of RWE groups to gain ground on the domestic political scene. The political engagement of RWE entities coupled with the rising radicalization of society pose a security threat to the democratic order in the SR in the long-term.

In order to minimize the risk of spreading extremism within the ranks of the AF of the SR, the main effort was on the initial screening of the applicants to the AF of the SR in coordination with the Personnel selection office of the AF of the SR. The early identification of active soldiers with an inclination to radicalization was also among the top objectives.

The MI also monitored the activities of paramilitary and militia-like groups aimed at creating alternatives to military training and education provided within the

scope and competence of the defence sector (i.e. voluntary military service and active reserves). In this regard, the actions of the 'Slovak Conscripts' (Slovenskí branci) organization were the most visible. The group includes also active duty and former members of the AF of the SR.

In the assessed period, the Slovak Conscripts underwent structural changes aimed at improving their functionality. To make up for a low interest in membership, the group intensified recruitment and succeeded to attract several new members. In order to achieve better public visibility, the group increased collaboration with some conspiracy and disinformation media and exploited both their print and online space for self-propaganda. Their ideological foundation was marked by an inclination towards the so-called antisystem and displayed elements of conservative patriotism and xenophobia. In 2020, the group organized several training activities and public events with the aim to spread propaganda and political marketing. Ongoing efforts to achieve legitimacy through cooperation with public bodies were observed.

The almost non-existent content moderation on social networks plays into the rise of extremist views. Moreover, the legitimization of antisystem and antidemocratic narratives, racist attitudes, hate speech or proven lies by some political players and public personalities helps spreading extremism. The various extremist groups have adapted their strategies with an eye on the legal aspects of the current national legislation on extremism and supplanted their previously aggressive rhetoric by a more sophisticated and cultivated speech.

The media landscape was flooded with misinformation, hoaxes and scaremongering regarding the protective measures taken by the Slovak government to curb the COVID-19 pandemic with potential serious consequences for public health safety and for the whole medical sector. Several individuals and entities attempted to politically capitalize on the increasing trend of society polarization by promoting antisystem, antidemocratic or extremist attitudes. The long neglected and underrated information security combined with an inefficient or absent strategic communication by public authorities only accentuated the worsening polarization of the society.

Within the external security environment of the SR, the strengthening of the RWE scene has been observed in Europe in recent years. Their mutual relations are globally deepening through online platforms and social networks. These communication possibilities also facilitate the overall unification of the RWE scene. In the SR, the RWE community is linked to the antisystem scene, which consists of various extremist or fringe movements. Their common feature is activism on social networks and mass dissemination of disinformation. At the time being, the antisystem does not pose an imminent security threat to the SR. Nevertheless, there is a tendency towards further escalation with the main indicators being the extended level of activism and coordination among supporters of the RWE scene.

Several cases of inclination to RWE ideology have been observed among active duty members of the AF of the SR. Based on the results of a sociological survey carried out in the second half of 2020, the rate of inclination to RWE ideology among members of the AF of the SR is estimated at about 10 – 15%. Following this survey, the MoD adopted measures focused on eliminating such attitudes and preventing the penetration of radicalism and extremism within the defence sector. Several cases of inclination to RWE ideology among members of the AF of the SR were handed over to law enforcement bodies.

During the assessed period, activities of harmful sectarian groups did not pose a security threat to tasks fulfilled by the defence sector.

Illegal migration

The security threat to SR and the EU stems in particular from irregular migration flows originating in risk countries. The 2020 saw a 26% decline in the number of irregular migrants reaching Europe compared to 2019, with approximately 95,100 people coming to Europe. The decreased migratory pressure was likely the result of restrictive measure imposed by transit countries in spring 2020 when addressing the COVID-19 spread. These measures mitigated the migratory dynamics predominantly on the eastern Mediterranean route. As the countries gradually rescinded their protective measures, the migratory pressure from North Africa to the EU begun to rise once again.

The western Mediterranean route saw a 29% increase in the number of new arrivals (altogether 41,861). The numbers on the Atlantic route had risen significantly as well. The 800% increase in the number of arrivals to the Canary Islands in 2020 (23,000) compared to 2019 is likely related to unfavorable socioeconomic conditions in African countries.

Compared to 2019, the central Mediterranean route (towards Italy) recorded a 198% increase in the number of irregular migrants (altogether 34,100). Tunisia and Libya remained the main departure countries, while Sardinia, Sicily and Lampedusa received the majority of irregular migrants.

In 2020, the eastern Mediterranean route (towards Greece) ceased to be the main migratory route. The number of irregular migrants arriving on this route declined by 78% (altogether 15,600) compared to 2019. The route was used by 17% of irregular migrants coming to Europe in 2020.

The migratory dynamics along the Western Balkan route is among others significantly determined by the incapacity of Greece to provide temporary accommodation for migrants and by the domestic situation in Turkey. The dynamics along the Western Balkan route is crucial when assessing the impact of irregular migration on the security in the SR.

In 2020, there was a recorded 40.9% decrease (1,295 persons) in cases of irregular migration in the SR compared to 2019 (2,190 persons). The largest share was comprised of 1,160 cases of illegal stays in the SR (a significant 41% decrease compared to 2019). The aforementioned overall number also includes 135 cases of illegal border crossing to the SR where a 36.6% decrease was observed compared to 2019. The majority of illegal migrants were of Ukrainian (326), Afghan (191) and Syrian (152) origin.

Within the assessed period, the MI also obtained and analysed information regarding individuals and groups involved in the process of transferring illegal migrants into the SR. The MI also focused on cases of pseudo-legal migration in the form of establishing or acquiring companies, employing foreigners or misuse of the visa provided for the purpose of study with the aim to obtain a residence permit in the SR.

Organized crime and crime against the defence of the Slovak Republic and illegal trade in defence industry products

Organized crime against the defence of the Slovak Republic

In the field of organized crime, one of the priority and long-term tasks of the MI is the detection of acts related to illicit armaments and trading in military ammunition that is committed by members of the AF of the SR, drug crime in the environment of the defence sector, corrupt behaviour of employees of the defence sector and members of the AF of the SR and cross-border crime. In order to detect these criminal activities, the MI works closely with law enforcement authorities and other government departments.

The MI actively participated in raising both the level of compliance with generally binding regulations and the level of operational safety with a focus on the storage and handling of hazardous materials in a budgetary organization operating within the scope of the MoD of the SR.

The MI obtained information related to illicit armaments and illegal arms trade committed by individual members of the AF of the SR and of other security authorities as well as by foreign citizens. The majority of cases concerned illegal trade in ammunition, the ownership of illegally held firearms and illegal modification of firearms previously rendered inoperable. In some of the cases, the ammunition came from storage sites belonging to the AF of the SR or the MoI of the SR.

The cooperation of the MI with relevant security authorities led to the confirmation of criminal activities consisting of illicit armaments and illegal arms

trade committed by a Czech national. In Jun 2020, the Slovak police initiated criminal proceedings based on information provided by the MI.

In the field of the fight against drug-related crimes, distribution of narcotic drugs and psychotropic substances and anabolic steroids within the defence sector, previous findings on committing organized drug-related crimes were confirmed. The National Criminal Agency (hereafter as "NAKA") launched criminal proceedings against the involved persons based on information provided by the MI.

The MI collaborated with NAKA also in a case of suspicion of corrupt behaviour concerning a military base doctor. In December 2020, NAKA initiated criminal proceedings and the person was detained and charged. At the same time, criminal prosecution was brought against other involved professional soldiers on bribery charges.

During the assessed period, the MI recorded a significant decrease in the airspace infringements of the SR on the Slovak-Ukrainian state border by manned aircraft overflights in comparison with the previous evaluated period. The MI also obtained information about illegal migration and smuggling of goods from Ukraine in the southern part of the Slovak-Ukrainian state border. All interceptions are transmitted by the MI to relevant police authorities to take their own action.

Illicit trade in defence industry products

The security environment of the SR is also significantly affected by trade in defence industry products as well as deactivated or modified weapons. Traders and brokers of defence industry products, weapon systems and weapons perceive the SR as a safe country, suitable for the preparation and subsequent implementation of trades involving the sale of weapons and weapon systems worldwide, including to regions with a disturbed security landscape.

In 2020, the MI within the scope of the Permanent Expert Group of the Ministry of Economy of the SR assessed and verified a total of 840 applications of Slovak companies for foreign trade in defence industry products and 38 applications for permits to trade in defence industry products (for 5 years). In the field of trade in specified products and dual-use goods, more than 640 applications from authorized Slovak trading companies and manufacturers of defence products were assessed.

Several applications of Slovak companies were verified and assessed, the common indicator of which were sensitive final destinations of exported defence military products (weapons, weapon systems, ammunition, production lines for the production of ammunition, or combat vehicles) to countries such as the United Arab Emirates, the Republic of Kazakhstan, the Republic of Rwanda, the Republic of Mali, the Republic of Iraq and others.

In the field of export control, transport, brokering and transit of dual-use goods, several trade operations with the risk of circumventing the relevant legislation were identified. Exports of electronic, telecommunication, signalizing equipment and software to countries such as the Russian federation, the United Arab Emirates, the People's Republic of China, which could pose a risk of potential misuse of the exported goods for purposes other than declared, were verified.

Activities and threats in the cyberspace

Within the scope of the MI, a Centre for Cyber Defence of the SR (hereafter "the Centre") is established, which operates in the cyber domain of national defence. The Centre represents the highest – strategic level of cybersecurity and cyber defence management under the auspices of the MoD of the SR. The Centre's tasks are gathering, centralizing, analysing and evaluating information to ensure cyber defence, inform entities concerned, propose and take adequate measures.

In 2020, the Centre recorded and dealt with numerous cybersecurity incidents involving both state and non-state actors. These incidents involved a wide spectrum of activities ranging from simple hacker attacks launch by individuals to government sponsored sophisticated cyber campaigns. The year 2020 was simultaneously marked by the preparation and approval of a new strategic, doctrinal and legislative framework of cybersecurity and cyber defence in the SR and its consolidation.

On the other hand, the dynamic of the security environment and the complexity of addressed cybersecurity incidents provided opportunities, which in the end contributed to the strengthening of the cyber capabilities of the MI for the

purposes of ensuring defence and defence capabilities of the SR, as well as, for the needs of collective defence.

In the evaluated period, the MI also actively participated in the activities of national top level managing bodies of the SR in the field of cybersecurity and cyber defence as well as expert working groups within the SR and international organizations and associations of which the SR is a member state.

With regards to national defence in the cyber domain, the MI ensured resilience and security of the departmental information and communication infrastructure of the MoD of the SR, as well as, cyber defence of selected parts of critical infrastructure, objects of special importance, and other important objects. The Centre actively participated in solving cyber security incidents within the competence of the defence department, state administration as well as the private sector. It also performed tasks in the field of building security awareness, deepening cooperation with the public, private and academic sector.

In the area of cyber security, the tasks were performed by a special workplace of the Centre – CSIRT.MIL.SK. The departmental internal networks are kept under oversight by monitoring network connections, evaluating security events and detecting targeted attacks on the infrastructure of the MoD of the SR.

Cyber-attacks against the MoD of the SR were a reflection of events happening in the global cyberspace. Attempts to deliver e-mail messages with fraudulent content or malicious attachments to users of the department internal networks were most frequently examined. The information obtained and analysed was further correlated with information from the National Security and Analytical Centre, as the same harmful e-mail messages could be sent to other ministries and central government authorities.

The SR also faces attackers who carry out criminal activity in the cyberspace in order to obtain information from non-public databases. The aim of this activity is financial profit from its sale.

In order to increase the cyber security and defence of information systems in the defence department, the activities of the Centre were mainly focused on detecting vulnerabilities and security deficiencies in various systems. Departmental organizations were regularly informed about the campaigns carried out by the so-called Advanced Persistent Threat (hereafter as "APT") groups supported by various countries around the world, while the Centre tackled identified cyber campaigns directly with the institution concerned, to which it provided the necessary technical assistance and cooperation.

The Centre recorded several advanced cyber campaigns targeting the public and private sectors. An example is the campaign implemented by the APT group KIMSUKY, which had a global character and was aimed at the defence sector of several countries, including the SR. The aim of the campaign was to steal sensitive

information from research and development area of military equipment. The activities of the APT group KIMSUKY are connected with the activities of the military intelligence service of The Democratic People's Republic of Korea.

Due to the COVID-19 pandemic, the main part of the workload of both central government authorities and private sector bodies relocated to the online space in 2020. Attackers moved to exploit this situation in order to compromise their infrastructure. Widespread fishing campaigns as well as targeted attacks were observed.

In the evaluated period, the Centre reported the exploitation of application vulnerability through which unauthorised access was gained to both the data server of the National Health Information Centre (hereafter as "NHIC") and personal data processed by the application "Moje eZdravie". This involved the activity of a private company which not only alienated personal data in contradiction to the principles of ethical hacking but also disclosed the data for the purpose of self-promotion. This activity combined with other recorded intelligence by the Centre about cyber threats against various bodies processing SARS-CoV-2 testing results data led the Centre to perform an infrastructure vulnerability evaluation of the NHIC, the Public Health Authority of the SR and 36 regional public health authorities. As a result, an examination of security status was conducted followed by implementing measures aimed at strengthening their infrastructure resilience against cyber-attacks.

The main activity in terms of building safety awareness in the field of cyber security consisted of providing specialised trainings with the aim to inform participants about existing security cyber threats, their prevention as well as on how to overcome problems. This awareness building role of the Centre was also aided by the publication of articles and information available on its website www.ckosr.sk.

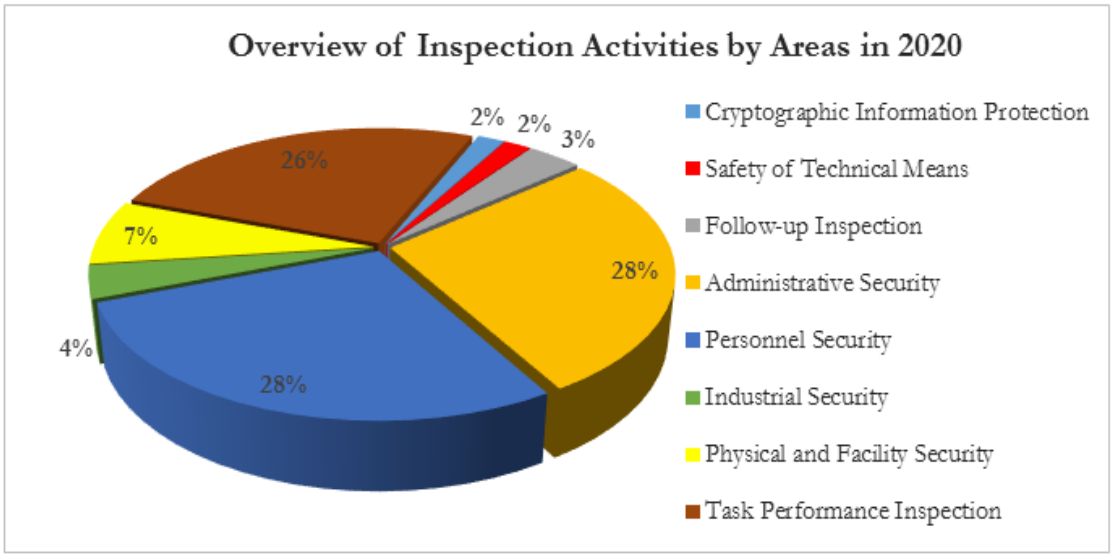
Cyberspace as an operational domain requires close and coordinated cooperation both at domestic and international level. Within the framework of NATO, the MI has a permanent representation in the relevant political and technical committees. The SR is also among the founding states of the NATO Cooperative Cyber Defence Centre of Excellence in TALLIN. At bilateral level, the MI closely cooperates with selected NATO and EU countries in order to strengthen the cyber defence by way of information exchange on recorded cyber incidents.

Protection of classified information and security vetting

The protection of classified information (hereafter as "PCI") within the authority of the MoD is provided by the MI in accordance and within the scope of

Act No. 198/1994 Coll. on MI and Act No. 215/2004 Coll. on Protection of Classified Information and its implementing rules.

In 2020, inspection activities in the area of PCI were carried out in four entities within the competence of the MoD and the findings related to the following areas: personnel, physical, facility, and administrative security. Recorded violations were forwarded to the relevant administrative authority for further proceedings.



The MI also participated in the determination of protection and exchange of classified information between the SR and the USA. In this regard, the MI cooperated on drafting and commenting on a new agreement on security procedures for exchanging and protecting classified information between the governments of the SR and the USA and initiated changes in the area of physical and facility security. Moreover, the MI participated in the implementation of the F-16 project in areas of personnel, industrial, physical and facility as well as administrative security.

In the area of personnel security, the MI received 3,513 applications for Level 2 to 4 security clearances in 2020. Furthermore, the MI cooperated with the National Security Authority of the SR (hereafter as "NSA") on security vetting by providing written reports for 2,115 requests in accordance with Act No. 215/2004. In the process of security vetting, there were more than 42,000 requests sent out by the MI to other governmental institutions, local authorities and legal persons.

In the area of industrial security, the MI drew up expertise on 54 contracts and 37 contract addendums on sharing classified information. In the process of performing security checks of entrepreneurs, the MI provided the NSA with 198 written reports in response to requests in accordance with Act No. 215/2004. In connection with the provision of information on security reliability of proposed persons, the MI processed 5,072 requests and statements.

USE OF INFOMATION AND TECHNICAL MEANS

In 2020, the MI used information and technical means (hereafter as "ITM") in accordance with provisions of Act No. 166/2003 Coll. on protection of privacy against unauthorised use of ITM and amendments to certain laws (hereafter as "Protection against Eavesdropping Act"), as last amended, and Act No. 198/1994, while each use of ITM was in accordance with Section 4 of the Protection against Eavesdropping Act and based on prior written consent of a lawful judge. There was no unauthorized use of ITM in either cases.

The MI submitted a total of 36 requests for the use of ITM in 2020. 35 requests for consent were approved and 1 was rejected by a lawful judge. 17 extension requests were submitted for ITM use and all of them were granted judicial approval. The purpose and objective of ITM use as required by law were met in all concluded authorized cases in 2020.

IMINT CAPABILITIES DEVELOPMENTS

The MI successfully implemented measures in both personnel and technical area of Imagery Intelligence (hereafter as "IMINT") capability development. By signing agreements with satellite imagery providers in the assessed period, full operational capability of IMINT was achieved in 2020.

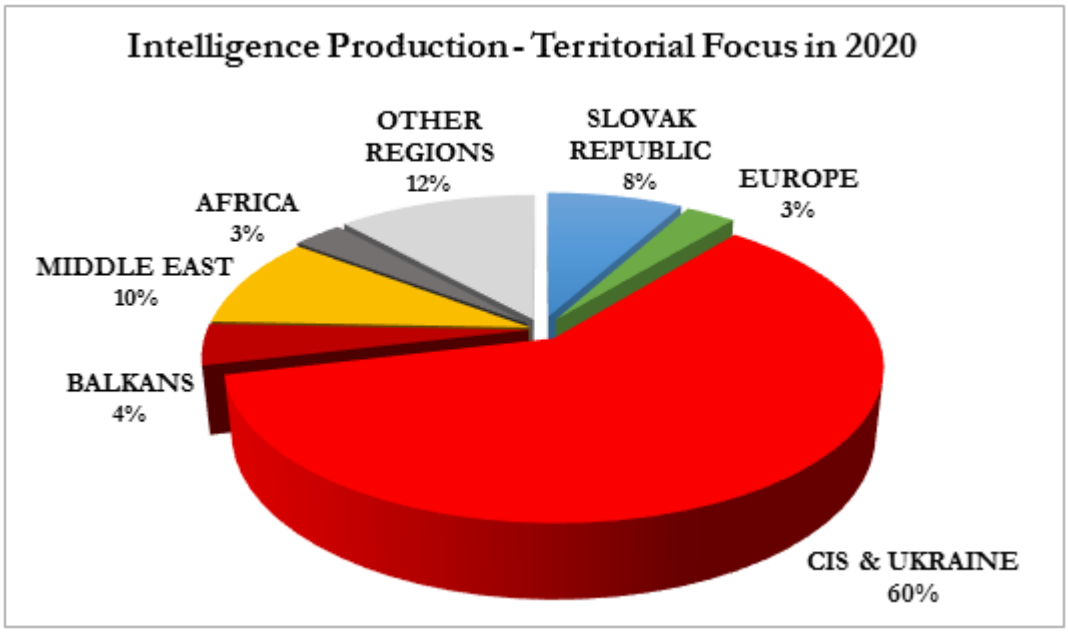
The provision of IMINT reports to decision makers of the MoD and other authorized users significantly contributed to threat analysis assessment against SR and security situation assessment in the areas of intelligence responsibility and intelligence interest. The IMINT reports were also highly appreciated within the intelligence community of NATO and the EU.

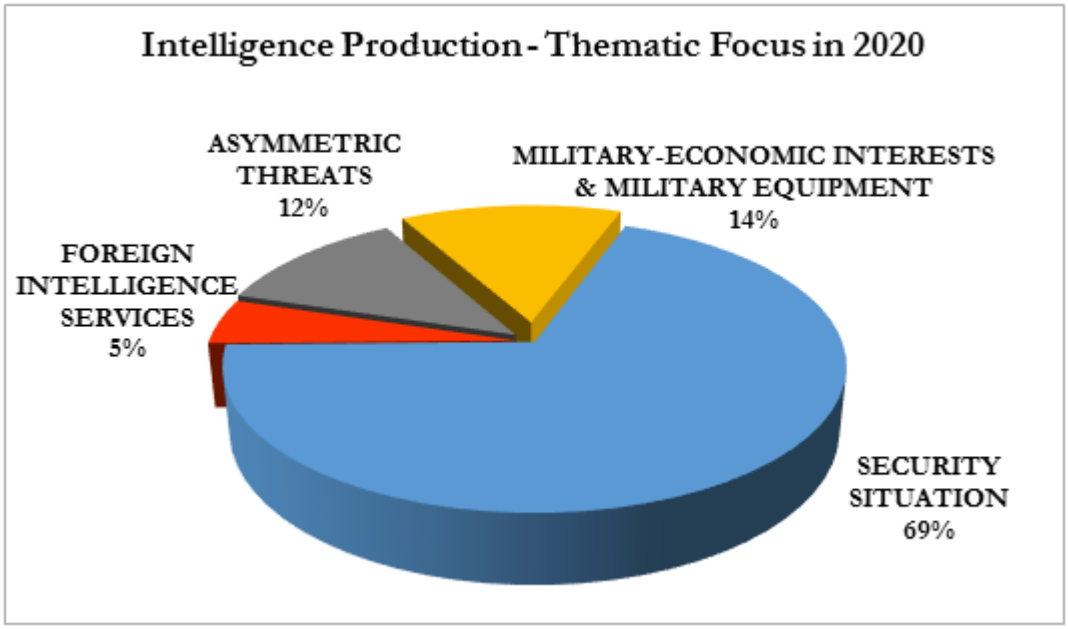
INTERNATIONAL COOPERATION AND INFORMATION EXCHANGE

International cooperation activities of the MI were influenced by the global pandemic situation, and any personal, expert, bilateral and conference meetings were primarily held via secured video-teleconferencing (hereafter as "VTC"). The initial meetings of our new director with his counterparts from the V4 countries were also facilitated by the secured VTC capabilities, which is a proof of effectiveness in utilizing this technology. The most intense cooperation took place with long term partner services from the V4 countries, the USA, the United Kingdom, Germany and Austria.

There was a demand for swift and efficient countermeasures to be taken by the MI due to the dynamics of the development of the global security environment coupled with new threats and the COVID-19 pandemic. One of the key determinants influencing proper reaction time to current threats was cooperation and active intelligence sharing on bilateral and multilateral levels.

In 2020, the MI processed and provided 628 intelligence products to authorized users and contracted entities. Of these, 190 were intelligence reports, 4 summary intelligence reports and 434 exchange intelligence products.





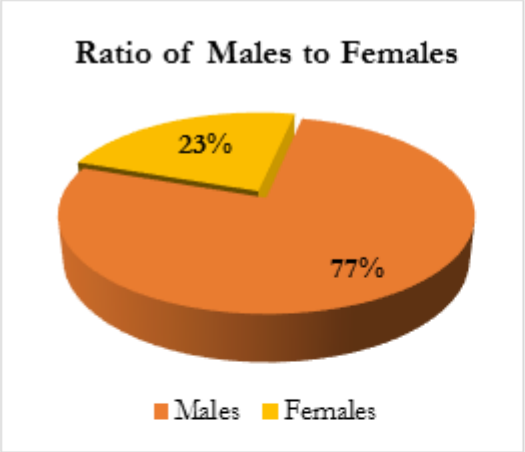
The cooperation with partners has a substantial effect on expanding the information databases of the MI, especially in the fields of global and regional security assessments, terrorism, cyber threats, as well as, foreign intelligence services.

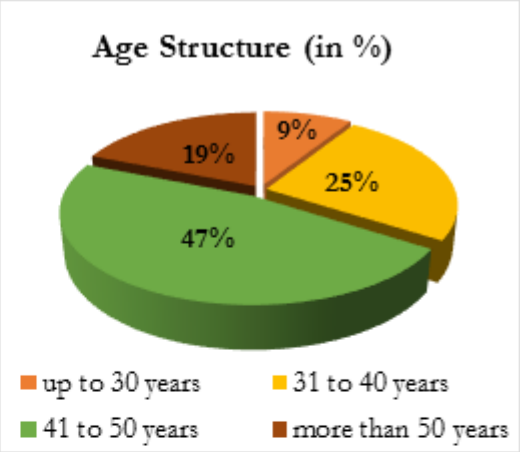
The MI also pays special attention to the ongoing evaluation of activities related to international terrorism groups that may pose a threat to protected values and interests of the SR, EU and NATO member states.

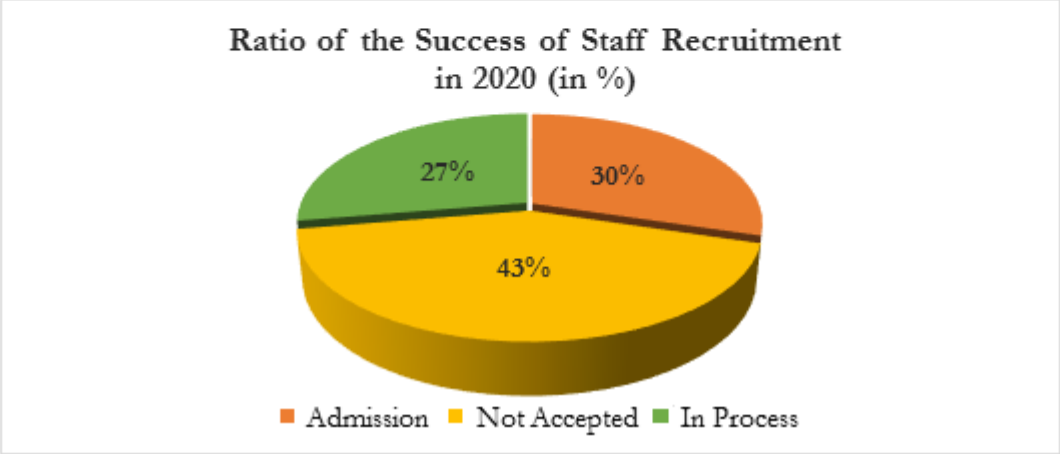
HUMAN RESOURCES

As of 31 December 2020, the staffing level stood at 63.62% out of the planned staff structure. This figure represents an increase in the number of personnel by 2.73% compared to 2019. The average age of the MI personnel was 44 years. The staff structure, as defined by standard demographics, remains unchanged compared to the previous year.

78% of the MI employees are professional soldiers and 22% are public service employees. The higher education attainment rate (including first level higher education) among the MI personnel stands at 73%.







There were several hundred job applications submitted to the MI consisting of admissions into the state service of professional soldiers, temporary assignation for the fulfilment of tasks of the MI and public service employment applications. The admission rates were as follows: 30% successful admissions, 43% unsuccessful admissions and 27% of the applications are still pending.

BUDGET

The budget administrator of the MoD chapter set the biding indicators for the MI for 2020 in the area of revenues to the amount of 64,400 EUR, and in the area of expenditures to the amount of 105,591,951 EUR.

As of 31 December 2020, the binding indicator in the area of expenditures was decreased by 14,641,603 EUR, representing a 13.87% reduction, to the total amount of 90,950,348 EUR.

CONCLUSION

The activity of the MI in 2020 was influenced by the development of the COVID-19 pandemic in the SR and in the world, to which the MI promptly responded and part of its resources was earmarked for monitoring the spread of the disease and adopted measures in the regions of the SR and in the world.

The recorded shifting trend of threats towards the information and cyber space will continue with high probability into the future. We also expect that the number of cyber-attacks and influence operations will continue to grow in order to polarize the Slovak society and weaken the legitimacy of state institutions, also owning to the fact that this type of attacks is likely perceived as effective by their perpetrators.

The continuation of the pandemic and the measures taken at state level to prevent its spread can be exploited by both state and non-state actors for fuelling divisions within society, creating new dividing lines and an overall radicalization of society. This creates a breeding ground for extremism reaching all spheres of society, including members of the AF of the SR and the defence sector.

Regarding terrorism, the dissemination of radical propaganda by global Islamist terrorist groups is likely to continue. In combination with anti-pandemic measures, it can lead to self-radicalization of individuals in the online space and act as catalyst for the formation of so-called lone wolves.

Ongoing conflicts, the poor socioeconomic situation of the population and climate changes in the crisis regions of Africa, the Middle East and South and Southeast Asia will be significant factors with influence on the ongoing migration waves to Europe, including the SR. The withdrawal of coalition troops from the Islamic Republic of Afghanistan will with high probability lead to deterioration of the security situation in the country in the short to medium term and the subsequent increase in migration to the EU.

The dynamics, sophistication, complexity and quantity of identified cyber threats against both the state and private sector of the SR will highly likely persist in short term. We assume that the nature of cyber campaigns in the short term, focused against the state sector, will not change fundamentally. They are considered the

greatest threat to vulnerability of industrial management systems across multiple sectors, which are intended for management and in some cases visualization of industrial processes.

All the tasks of the MI, as defined in Act No. 198/1994 Coll. on MI, and stipulated in the Intelligence Objectives of the MI for 2020, were completed despite pandemic-related measures and restrictions. The fulfilment of these tasks creates favourable conditions for future activities and further capability development of the MI.