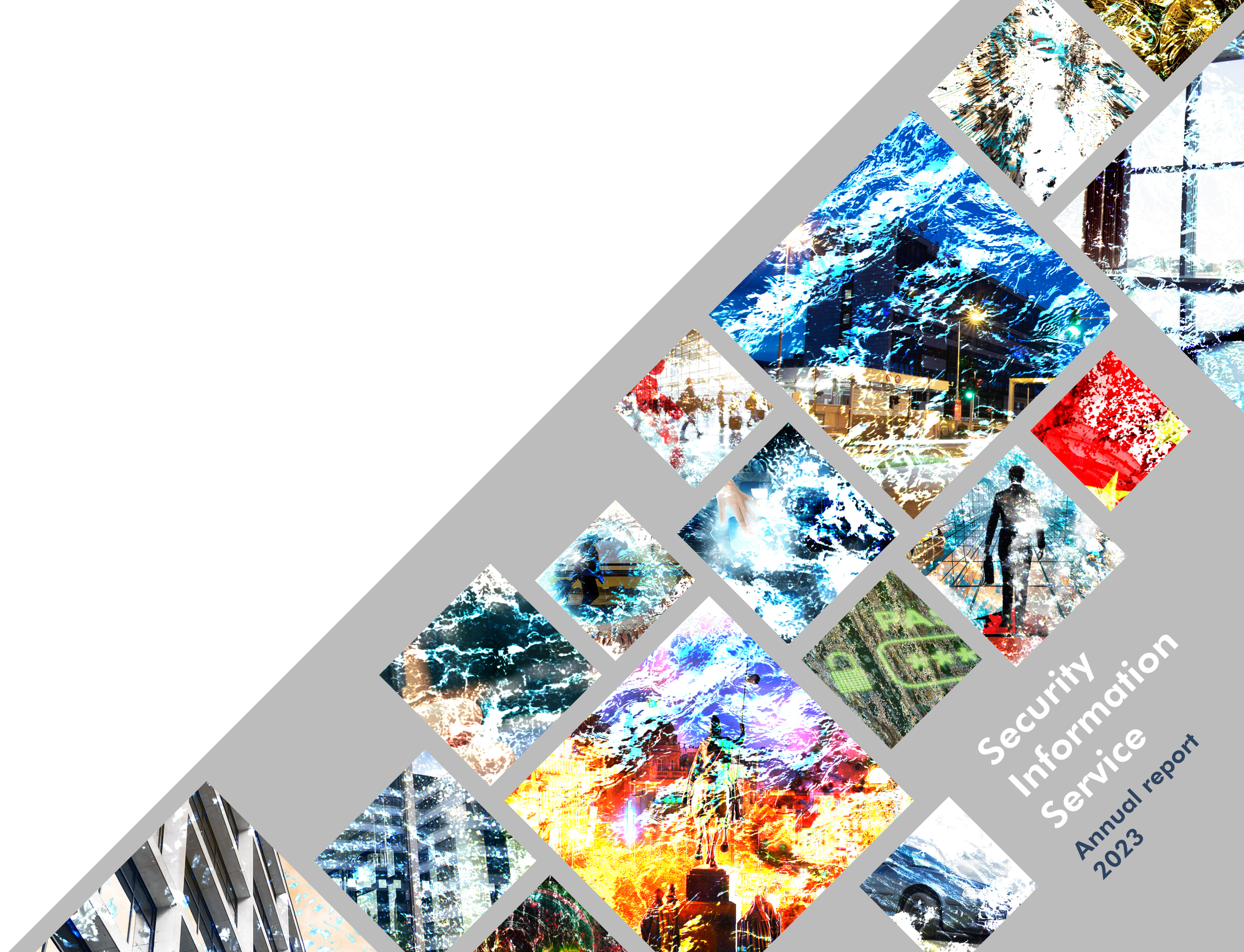
Security Information Service

Annual report 2023



Annual Report
of the Security Information Service
for 2023

Table of contents:

Dear readers,

Once again, I have the privilege of presenting to the public the unclassified annual report on the activities of the Security Information Service (BIS) – this time focusing on the year 2023. It was an extraordinarily challenging and in many respects turbulent year in the security domain. Regretfully, Russia's unacceptable brutal aggression against Ukraine continued, to which the democratic and free part of the world responded by supporting the country under attack. I will always be proud that the Czech Republic has been at the forefront of these efforts throughout, not only as a state but also through dozens of civic initiatives.

As in previous years, Russia remained by far the greatest threat to the security of our country, as well as to all of Europe and the world. Russia's attempt to rewrite the geopolitical map of the world and build a "new world order" is currently the greatest threat and at the same time the greatest challenge for the world community. In addition to the conventional war against its neighboring country, the Russian Federation is conducting permanent hybrid attacks against Western democracies, including the Czech Republic. Russia increasingly uses modern technologies to attack the stability, democracy, and freedom of countries it designates as hostile. The goal of these attacks is to undermine support for Ukraine, weaken citizens' trust in the state, and promote societal division by disseminating hostile propaganda on various platforms – from so-called news websites to massive influence campaigns on social networks and cyberattacks on critical infrastructure.

Modern technology, namely the rapid development of artificial intelligence (AI), presents a huge challenge for today's society as well as security forces. AI can be a good servant but a very bad master. Control over AI by a single state or private entity could have catastrophic consequences, against which today's attacks using deep fake videos or generating disinformation content would seem anecdotal. Russia and China understand this very well and invest enormous financial resources in this area. For the Euro-Atlantic space, it is vital not to lag behind and to keep pace with these non-democratic regimes.

It must be noted that despite the change in strategy caused by the forced downscaling of Russia's diplomatic missions, the Russian intelligence services continued their intelligence operations across Europe. One such operation was uncovered, documented, and stopped by the BIS in cooperation with other European intelligence services. The investigation of the case now known as Voice of Europe began in 2023 and continues to this day. Russia's attempt to influence not only public opinion but also the elections to the European Parliament represent a brutal transgression of the sovereignty of several European countries. The action against this intelligence platform was an extraordinary success for the BIS, but it must be said in the same breath that there is no doubt that the Russian Federation still continues numerous other activities of the same kind on European soil.

This unclassified annual report is, as always, written in general terms for obvious reasons but with the aim of allowing the public to gain insight into our work, to familiarize the reader with the issues the BIS is addressing, and to highlight the threats faced not only by the Czech Republic but by the entire world. It is not always an easy reading, but we believe that an informed society will also be better prepared for what awaits us in the foreseeable future.

I wish you good health, safety, and all the best.

Genmjr. Ing. Michal Koudelka

Nature and Scope of Intelligence Activities

The activities, status, and scope of powers of the BIS are governed by relevant laws, particularly Act No. 153/1994 Coll., on Intelligence Services of the Czech Republic, as amended, and Act No. 154/1994 Coll., on the Security Information Service, as amended. In its activities, the BIS also adheres to the Constitution of the Czech Republic, the Charter of Fundamental Rights and Freedoms, international treaties, and other legal regulations of the Czech Republic.

According to Section 2 (1) of Act No. 153/1994 Coll., intelligence services are public authorities responsible for acquiring, collecting, and evaluating information important for the protection of the constitutional order, major economic interests, security, and defense of the Czech Republic. According to Section 3 of Act No. 153/1994 Coll., the BIS is an intelligence service that, within its powers and responsibilities, as defined in Section 5 (1) of Act No. 153/1994 Coll., secures information on:

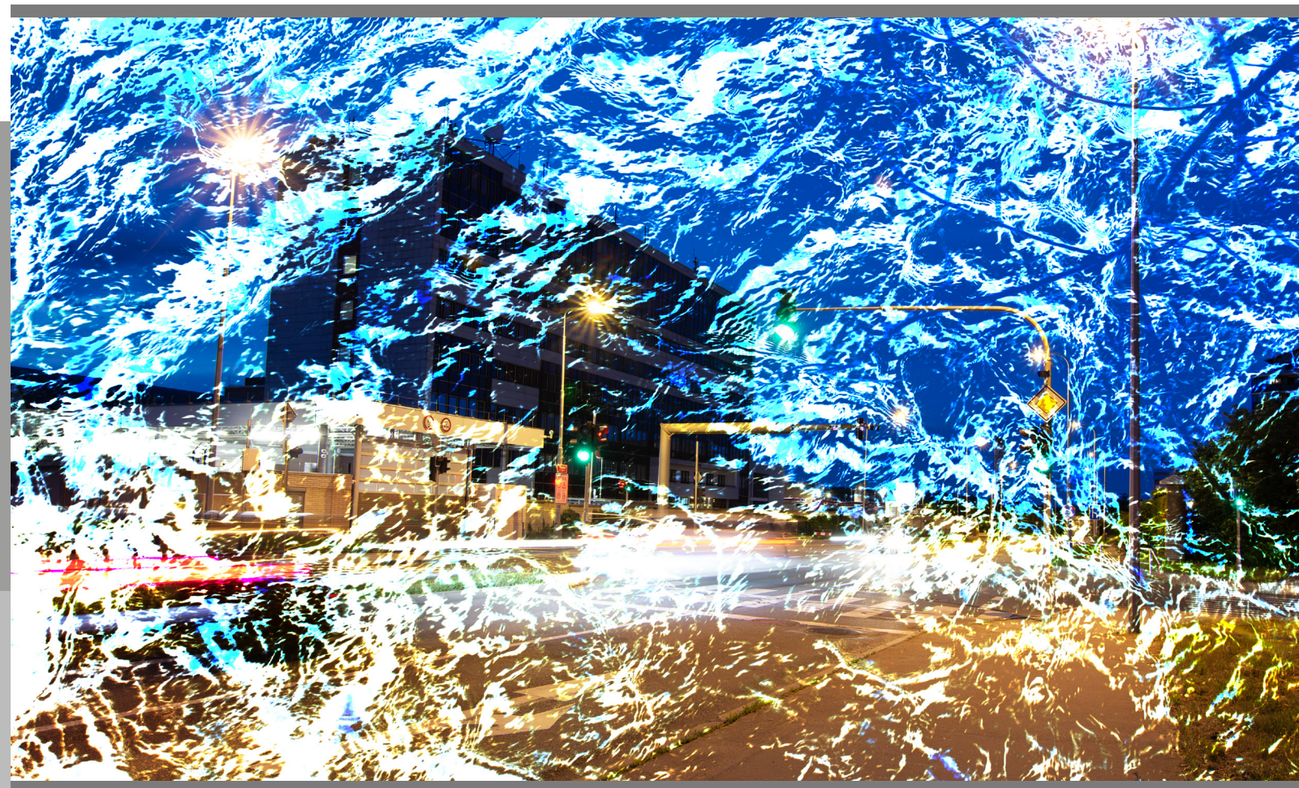
- **Intentions and activities directed against the democratic foundations, sovereignty, and territorial integrity of the Czech Republic,**
- **Intelligence services of foreign powers,**
- **Activities endangering state and service secrets,**
- **Activities whose consequences may put at risk the security or major economic interests of the Czech Republic,**
- **Organized crime and terrorism.**

According to Section 5 (4) of Act No. 153/1994 Coll., the BIS performs additional tasks as specified by specific legislation (e.g., Act No. 412/2005 Coll., on the Protection of Classified Information and Security Eligibility, as amended) or by international treaties binding on the Czech Republic.

Section 7 of Act No. 153/1994 Coll. further stipulates that the responsibility for the activities of Czech intelligence services and for the coordination of their operations lies with the Government. According to Section 8 (4) of this law, the government assigns tasks to the BIS within its scope of powers and responsibilities. The President of the Czech Republic is also entitled to assign tasks to the BIS within its scope of powers and with the Government's knowledge.

To fulfill its duties, the BIS is authorized to cooperate with other intelligence services of the Czech Republic. According to Section 9 of Act No. 153/1994 Coll., this cooperation is conditional upon agreements concluded between the intelligence services with the consent of the Government.

The BIS may cooperate with intelligence services of foreign powers according to Section 10 of Act No. 153/1994 Coll. only with the consent of the Government.



Intelligence Activity and Findings

The primary focus areas for the BIS in 2023 included hostile activities by Russia, cyber threats, and the general risks (and opportunities) associated with the use of new technologies, gaps in the state's readiness to respond to a changing world, and hostile activities by China.

Russia, currently perceived primarily as the aggressor in the war in Ukraine, poses a threat to the Western world, including the Czech Republic, that extends beyond this conflict. Russian efforts to polarize the public, spread disinformation, and conduct sabotage activities represent a serious security issue that the Czech Republic will continue to be dealing with in the foreseeable future.

Today's society is often referred to as an online society – our work, communication with authorities or banks as well as dating are moving into the virtual world. We debate on social networks, our children spend considerable time on mobile phones or other devices... It is not a surprise that with the same intensity and speed, malicious activities – the effort to enrich oneself at the expense of other people, to exploit, deceive, and defraud – are moving into the world of information technology. The area of cyber threats and new technologies will be one of the key security issues of the future.

The past period has highlighted the need to strengthen the state's and society's ability to respond to crises and unexpected events. One of the main factors important for this effort is the reduction of legislative and bureaucratic obstacles that slow down the introduction of new technologies and processes. This also includes increasing the capabilities and capacities of key national authorities. From a security perspective, readiness for changes is crucial, especially when it comes to the domain of energy, sanction mechanisms, large data processing, cybersecurity, and strategic decisions in general.

The People's Republic of China (hereinafter referred to as China) poses a fundamental threat to the Euro-Atlantic civilization, including the Czech Republic. It has long aimed to position itself as the most important economic superpower and create an effective counterbalance to the G7 countries. Unlike its competitors, however, it represents a different socio-economic concept based on communist dictatorship, which is corrosive to the fundamental principles of our civilization, such as democracy and the free market.

The BIS also addressed other threats within its scope of powers, particularly terrorism, disinformation, extremism, energy security, and violations of international sanctions. In the meantime, the Russian invasion of Ukraine continued to fundamentally influence the security landscape.

In 2023, the Czech Republic pursued an ongoing effort to strengthen its energy security by increasing control over key infrastructure, acquiring infrastructure capacities, and reducing dependence on supplies from Russia. Despite these measures, it was not possible to immediately replace all Russian raw materials used as energy commodities. For some alternative supplies, there was a risk that the originally expected delivery timelines would not be met. Measures were planned and prepared to respond to any disruptions in the supply of these commodities from Russia, although in some cases, these would be emergency measures.

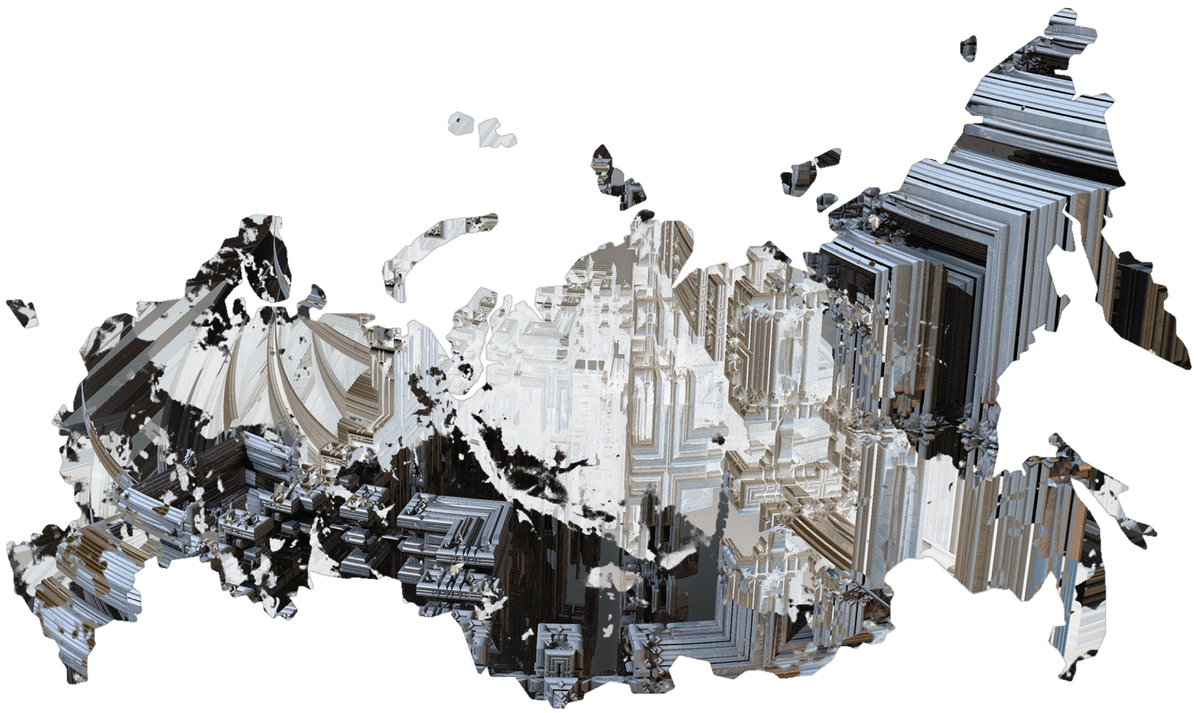
The ongoing Russian invasion of Ukraine continued to significantly influence the overall security situation in the Czech Republic in 2023. Several hundred thousand Ukrainian citizens fleeing the conflict remain on Czech territory. Despite minor issues associated, for example, with the integration of Ukrainian children into the Czech educational system or employment Ukrainian refugees in positions that do not match their qualifications, the handling of the migration wave from Ukraine, unprecedented in the modern history of the Czech Republic, can be considered an extraordinary success of the Czech state and society as a whole.

The Czech security forces have not recorded a significant increase in crime in connection with the arrival of large numbers of refugees from Ukraine. The BIS also does not have information indicating an increase in the activities of organized criminal groups in the Czech Republic related to their arrival. So far, the BIS has not detected the presence of any high-risk individuals with links to Islamist radicalism in connection with the refugee wave from Ukraine.

Throughout 2023, other risks associated with this conflict were also assessed, particularly the danger that some of the weapons supplied to Ukraine could end up on the black market and be smuggled back into the EU. In 2023, the BIS did not find evidence of large-scale organized illegal imports of weapons supplied to Ukraine back into the EU. However, in the medium term, an increase in illegal imports of military material from Ukraine can be expected, which will place greater demands on the relevant national authorities.

Russia – A Persistent Threat to the Czech Republic

Despite being forced to significantly reduce its diplomatic mission in the Czech Republic in 2021 and 2022, Russia continues its efforts to restore broader intelligence capabilities under diplomatic cover by sending new intelligence officers to our territory through long-term diplomatic accreditations or short-term visas.



Security Information Service
Annual Report 2023

Russian intelligence services have responded to the capacity losses caused by the expulsion of their officers or collaborators working in diplomacy in various ways. Espionage and influence operations against certain countries are increasingly directed from Russia or friendly or neutral countires. There is also an increased risk that individuals visiting Russia may become targets of intelligence services, who may attempt to exploit them for espionage against the Czech Republic.

In recent years, Russian intelligence services have increasingly used various online communication platforms to recruit and direct collaborators. Cases from abroad have confirmed the intention of Russian intelligence services to use these platforms (e.g.Telegram) in preparing subversive attacks against NATO or EU entities involved in distributing aid to Ukraine. Czech entities and elements of Czech critical infrastructure are exposed to the same risk.

In 2023, further information was published confirming the involvement of Unit 29155, which is part of the GRU (responsible for preparing the attacks on the ammunition depots in Vrbětice in 2014), in preparing the explosion of ammunition in Lovnidol, Bulgaria in 2011 (after it had been transported there from the Vrbětice depot). The risk of so-called traveling officers or collaborators of Russian intelligence services being sent to Czech territory remains high.

Concerning Russian information campaigns targeting the Czech public, their predominant focus was on the aid provided to Ukraine. This was the subject of an influence operation directed from Russia by Viktor Medvedchuk, a Ukrainian oligarch closely connected to the Kremlin regime. The role of the local coordinator for this operation was held by Artem Marchevsky, who established and led the online medium Voice of Europe in Prague.

Through the covert financing and management of Voice of Europe, Medvedchuk aimed to influence public opinion in Europe and create conditions for gaining leverage over candidates in the 2024 European Parliament elections. His goal was to advance Russian foreign policy interests, particularly those directly opposed to Ukraine's interests. The influence network also included collaborating journalists and politicians from EU countries.

On top of that, Russian state-controlled media, including Sputnik, have long been involved in influencing the Czech public. Despite being unable to operate as a regular news outlet in the EU due to sanctions, it continued its activities in the Czech Republic throughout 2023 via several websites and platforms. The individuals behind these operations managed to obtain statements from Czech politicians or pro-Russian activists, which were then used in published content to support arguments favorable to Russian propaganda.

The trips of pro-Russian activists to Russia were infrequent, and the number of politicians participating in them significantly decreased. However, certain activists repeatedly attended commemorative events in Russia related to World War II in 2023. An individual associated with the Russian intelligence service was also involved in organizing a trip to Moscow in May 2023.

Russian intelligence services continue to pay increased attention to international events where politicians and activists travel to non-NATO or non-EU countries, especially Serbia. Individuals operating in Serbia (linked to Russian intelligence services) repeatedly attempted to establish contacts with Czech disinformers.

Furthermore, the continuous tightening of EU restrictive measures against Russia has curtailed access to goods in demand by its military-industrial complex. Nevertheless, demand continues, as do attempts to facilitate deliveries through re-exports, especially via member countries of the Eurasian Economic Union. In 2023, several high-risk demands involved machine tools from Czech manufacturers. The ongoing war in Ukraine has demonstrated

Security Information Service
Annual Report 2023

the crucial role of unmanned aerial vehicles (UAVs) in combat operations. Components from Western manufacturers are extensively used in the production of UAVs and other weapon systems utilized by the Russian military. In 2023, Czech companies were repeatedly approached with requests for aircraft spare parts by high-risk entities that had previously been involved in non-transparent exports to Russia.

At the beginning of 2023, several machine tools potentially usable in the military industry were exported. Their declared destination was Kyrgyzstan. However, instead of being delivered to that country, the machines were diverted to Turkey and subsequently to Russia.

The numerous restrictive measures place significant demands on regulatory authorities, whose capacities are limited. Many components crucial for the production of Russian weapon systems, which are subject to sanctions, do not fall under controlled items. This fact complicates the identification of routes through which Czech components reach Russia.

After a partial decline in the activities of state-supported Russian cyber actors in 2022, there was a resurgence in activity, likely due to Russia's

intelligence needs. The ongoing isolation of Russia is reflected in a significant reduction of the traditional operational capabilities of Russian intelligence services, making cyber espionage an important tool for gathering information.

As in previous years, a state-supported Russian actor was active in the Czech Republic, focusing primarily on obtaining information from the field of international politics, with an emphasis on EU and NATO countries and international organizations. It conducts initial penetration into computer networks by mass sending of phishing emails. These emails typically take the form of standard diplomatic correspondence. The Czech Ministry of Foreign Affairs was the target of some campaigns, but it also appeared as a spoofed sender of malicious messages in some instances when attacks aimed at other countries.

In 2023, investigations were conducted also into the activities of another Russian cyber actor responsible for numerous attacks against Ukraine, NATO countries, and European government and energy organizations. Since the second half of 2022, this actor had been scanning the computer networks and information systems of various entities within the Czech railway infrastructure. The attacker also scanned for vulnerabilities in the computer infrastructure of railway transport entities and, in several cases, managed to exploit found vulnerabilities for short-term access to less significant information systems.

In the first quarter of 2023, the same actor expanded its scope and scanned other computer networks, including those of critical infrastructure entities. It was retrospectively discovered that some attempts to connect had already occurred in 2022. However, no successful intrusions were detected, partly because the security solutions of some affected entities automatically blocked connection attempts from the attacker's infrastructure. A similar campaign was observed in other EU and NATO countries. With the assistance of the BIS and Military Intelligence, it was possible to mitigate the potential negative impacts of the attacker's activities.

Since the start of the war in Ukraine, the information infrastructure of various Czech institutions and organizations has repeatedly become the target of so-called pro-Russian patriotic hacktivist groups. Their attacks are short-term, unsophisticated, and do not impact the confidentiality or integrity of information systems. Besides propaganda purposes, these attacks can create a sense of threat among the population of the affected countries and reduce confidence in the state's ability to prevent them. The media coverage of such DDoS attacks is likely their main goal since they are conducted as part of information-psychological operations. Therefore, they often appear in connection with elections and particularly as "retaliation" during events aimed at supporting Ukraine. Examples include DDoS attacks on the websites of Czech Radio in June 2023 during the Media and Ukraine conference, or the October wave of DDoS attacks that coincided with the second summit of the International Crimea Platform, organized by the Chamber of Deputies of the Parliament of the Czech Republic.

Cybersecurity and New Technologies

Using devices that are not sufficiently secured or updated poses a risk, particularly for the user, who loses full control over them. This can lead to the leakage of private data (including voice or audiovisual recordings) and its misuse. An attacker who gains control of a sufficient number of vulnerable devices can use them to conduct reconnaissance or directly harmful activities on the internet. Vulnerable devices, therefore, pose a risk to all networks connected to the internet. An example is so-called botnets, which are various devices grouped into a network controlled by an attacker. The BIS has repeatedly observed that the tactic of controlling vulnerable devices is used in various forms by state cyber-espionage groups, in some cases even on a large scale. Their goal is to conceal their identity, mask illegitimate access, conduct espionage, and exfiltrate data from other victims.

Security Information Service
Annual Report 2023

In 2023, there was no legislation in the Czech Republic regulating the security of various consumer products capable of communicating over the internet (IoT). At the EU level, this legislation is still being prepared (Cyber Resilience Act), but for example, the USA and the UK have already introduced such requirements into their legislation. Minimum security standards have been set for smart devices connected to the internet, such as the prohibition of supplying devices with uniform and weak default passwords. Although some reputable manufacturers already do this today, the responsibility is currently primarily transferred to each user. Users should ensure that all their internet-connected devices are updated and secured, thereby reducing the risk of unauthorized access.

Furthermore, there is the issue of highly complex personal devices such as smart phones, watches, and electric vehicles and their software (applications), through which data collection on location, data and voice communication, and audiovisual recordings can be conducted. The vulnerability of such devices does not primarily lie in the installation of highly sophisticated spyware but in the collection of data through mobile applications or firmware (non-removable applications provided with the device). Users should, therefore, pay increased attention to whether the devices—from smart watches to cars—do not originate from countries whose political regime and legislation increase the possibility of data misuse by public authorities. The same applies to the use of cloud services or various AI assistants.

Most countries, including the Czech Republic, do not have sufficient means and capacities to regularly verify and certify the security of technological products, especially when manufacturers are allowed remote management, for example, to deliver security updates. As a result, individual states typically do not control the entire supply chain and must rely on the trustworthiness of the product manufacturers. In such cases, it is crucial (especially for elements of critical infrastructure) to rely on manufacturers from countries with the same or at least similar political, legal, or business environment. This is even more pertinent now, given the global trend of moving the operation of software products, including their data, to the cloud environment instead of maintaining them within the infrastructure of the respective entity.

Basic Security Guidelines

- When purchasing devices and applications, pay attention to the manufacturer's trustworthiness and the country of origin, keeping in mind the data collected by the device. For IoT devices, also consider that they often require their own service application installed on mobile devices.
- Regularly update internet-connected devices—network elements (routers, switches), phones, cameras, televisions, smart home appliances, and other IoT products. Many of them can be set to update automatically, for example, overnight.
- Always change the default login credentials set by the manufacturer. Use two-factor authentication, unique and complex passwords, or secure passwordless login.
- When selecting applications, especially for mobile devices, pay attention to the permissions the application requests for its operation, whether they are absolutely necessary for the desired functionality, and regularly review these settings.
- Uninstall unused or rarely used applications.
- If there are doubts about security, dedicate one device (which should not be your personal mobile phone) for the installation of service applications for IoT devices in the household.
- Segregate IoT devices into a separate WiFi network or a separate segment. Many home routers have the option to create a so-called guest network, where devices have internet access but are isolated from other devices on the same network.

The high degree of global interconnectivity is also reflected in cybersecurity and can have unexpected and unintended impacts through the so-called spillover effect. Historically, perhaps the most well-known example is the damage caused by the Russian computer virus NotPetya in 2017, which was created to cause destruction in Ukraine but resulted in global-scale damage. Another example is the disabling of ground stations of the VIASAT/KA-SAT satellite system on the day of the Russian invasion of Ukraine in 2022, and more recently, the spillover of the Israeli-Palestinian conflict into the Czech cyber space.

This occurred in November 2023 during a global campaign by the pro-Palestinian actor CyberAv3ngers. In response to the ongoing conflict, they exploited a critical vulnerability in devices from the Israeli manufacturer UNITRONICS used for industrial automation. As a result of the attack, the device display showed the attacker's message instead of status information. In the Czech Republic, this affected several devices in the water sector and energy industry. Although it was one of the few successful recorded attacks against industrial systems (ISCS/SCADA) in sectors classified as critical infrastructure, it did not have a significant impact. This was partly because the attacked systems were directly connected to the internet, whereas industrial control systems in the critical infrastructure's production domain generally do not have such direct and unsecured connectivity.

The year 2023 was groundbreaking for artificial intelligence. Technological advancements, particularly in the field of generative AI, combined with greater user-friendliness, enabled the proliferation of synthetic media (deepfakes) into the mainstream information space.

The BIS experimentally verified the possibilities of creating synthetic content tailored to the Czech environment. Improvements in large language models confirmed that there is no longer anything that would prevent mass-scale creation of synthetic text. At the same time, synthetic text is almost impossible to detect. While forensic analysis can still reveal artifacts of automated manipulation in visual content, text produced by a large language model is indistinguishable from human output. Due to the absence of entry barriers and low detectability, the BIS currently considers this type of synthetic media to represent the highest risk.

The BIS ranks synthetic voice as the second synthetic media in terms of security concerns. It is expected that freely available tools will soon be capable of creating a credible voice clone in the Czech language.

Despite the advanced and currently available technologies, the use of synthetic multimedia in influence campaigns in the Czech Republic has not yet been recorded. However, in countries where this has already occurred, the impact of their use has been very small.

Challenges for State Preparedness in Responding to a Changing World

The Czech Republic and the entire Western world are undergoing significant technological, economic, and societal changes that have a substantial impact on security and the work of intelligence services. In order to respond to and potentially leverage these changes, states must be adaptable and prepared for a rapidly changing environment, which applies to their national authorities as well.

The war in Ukraine has been a catalyst for systemic changes in many aspects of the public administration's work. It has had a significant impact on economic interests, particularly in the energy sector. The necessity for a quick response to rapid developments in the economy highlighted the state's uneven preparedness for these changes. While private entities quickly adapted to the situation and promptly sought to exploit new conditions (e.g. subsidies in the energy sector) to maximize their own benefit, the public sector faced numerous problems stemming mainly from a lack of expertise and staff. Regulatory authorities are often unwilling to confront regulated entities, due to their indifference, sluggishness, or a lack of personnel. Such behavior had visible impacts in the area of regulation, where, in some cases, oversight activities were conducted only formally, without detailed analysis or proper verification of data reported by regulated entities.

Efficiency of Public Administration

The aforementioned lack of expert staff has fully come to light following the dynamic changes in recent years. However, this is a long-term issue that a large part of the public administration has been struggling with. This problem is most poignant in the IT sector, but it affects many other areas in which the state loses the battle for experts to the private sector. This often leads to the outsourcing of important state roles to third parties. Such entities are then usually in a conflict of interest, as they participate in the preparation of supporting documents for legislation drafts while being those regulated by the legislation in question.

In 2023, the BIS recorded several cases of blatant conflicts of interest stemming from the state's inability to sufficiently compete with private employers. Representatives of some state institutions received financial compensation from third parties to supplement their low salaries in the public sector. These entities were seeking public contracts from the institution where the individual in question was employed or were subject to legislative proposals from that institution.

The BIS, in connection with attempts to influence legislation or public administration officials, also noted an increasing trend of private entities using various associations or organizations for such purposes. These entities, although presenting themselves as independent (at least by their names or declared general beneficial goals), are in reality influenced by said private entities and act in line with their particular interests.

In some cases, representatives of state-controlled entities repeatedly took advantage of the inadequate ability of state representatives to exercise proper oversight. They continued in 2023 to deliberately adjust the content of background or strategic materials, which are used, among other things, to decide on the future and further development of these entities.

Another example of promoting private interests at the expense of the state is clientelism, the provision of unauthorized advantages to selected individuals or companies. Such phenomena occurred in public procurement, selection processes, or the redistribution of public funds managed by state institutions. In the past, such actions were often accompanied by the provision of direct compensation (corruption), which was more easily detectable and punishable by the responsible authorities. This can be considered outdated today. In recent years, representatives of state institutions often promote particular interests of various groups primarily to strengthen their own position and especially to secure their future employment with such entities. Their motivation lies mainly in the expectation of future benefits, which is, however, very difficult to prove. Paradoxically, the BIS has noted tendencies towards such behavior particularly in cases where strong personalities occupy leading positions in state bodies or when the leadership of the institution is based on a monocratic principle.

The necessary expansion of restrictive measures against Russia brings an unprecedented increase in the agenda for the Czech export control system without it being compensated by the allocation of corresponding human and financial resources. Institutions dealing with export permits in some developed countries employ technical experts on controlled items (their identification, classification) or have separate departments

focused solely on the issue of export permits for know-how and the provision of expert knowledge in studies and scientific research (so-called intangible technology transfer). The Czech public administration lacks similar capacities. Some public authorities also face a shortage of workers with adequate security clearance, which limits the exchange of information with intelligence services. The rising costs associated with the screening of entities, but especially with managing and securing classified data, will inevitably lead to a debate on what information really needs to be classified and at what level.

In recent years, there has been quite a shortage of quality employees in many key areas of public administration, which are absolutely essential for the proper functioning of the state. Insufficient financial remuneration makes it impossible to recruit qualified workers, further hampering the state's ability to respond to the changing global environment. However, there are also departments and official positions whose activities are unnecessary for the functioning of a modern state. A functional public administration is a necessary prerequisite for a functional state. And a functional state is the only form of state that ensures security and personal freedom for its citizens. Without a systemic change in the approach to the Czech public administration, these capabilities will decrease in the future.

Managing Migration

The BIS has long been monitoring the migration situation in the Czech Republic and Europe, evaluating information obtained from its own activities, foreign partners, and interdepartmental cooperation. The information about illegal migration that the BIS has acquired in the past period does not meet the parameters of a security threat. However, migration trends are leading to an increase in the number of immigrants coming to Europe. The Czech Republic, like other EU countries, faces the influence of long-term push factors in the source countries of migration (low level and instability of living standards, war, religious and ethnic conflicts, political pressures) and pull factors in the destination countries (political stability, economic prosperity, quality of life, social and personal freedom, internal security) that bring immigrants to our territory. The realistic possibilities of weakening the push factors are limited, and changes to the pull factors are undesirable.

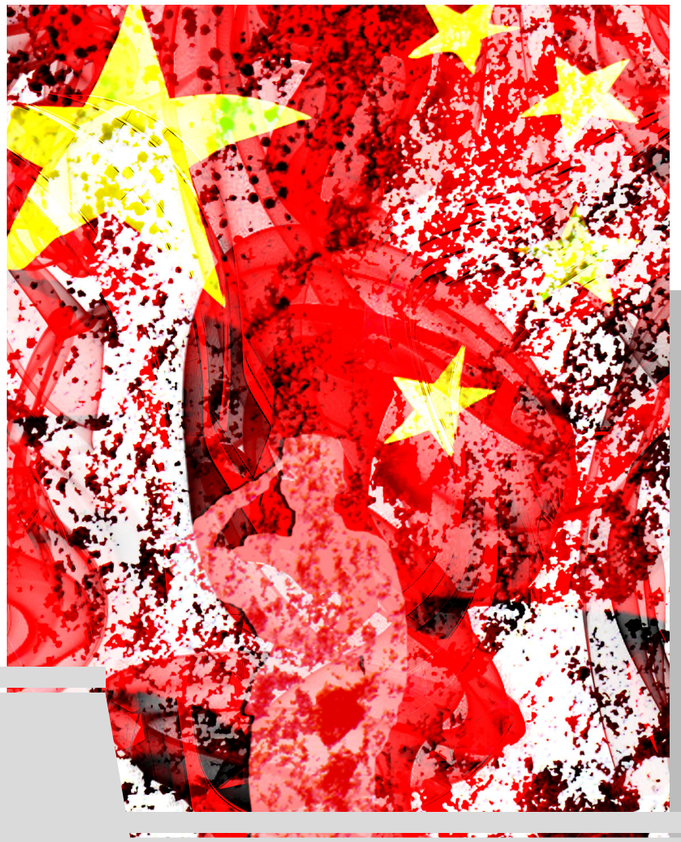
Administrative solutions for migration, involving the restriction of legal options for migrants to enter and stay in the Czech Republic, will therefore have only a short-term effect and will lead to the transfer of the immigration agenda from the state's jurisdiction to the sphere of irregular or outright illegal activities of various intermediaries, agencies, and companies exploiting migrants. In the event of an increased influx of people, the state is also unable to obtain sufficient information about applicants for residence permits, which is partly due to the limited capacity of the relevant authorities. The ability of the public sector to create conditions for the active integration of migrants is crucial, as it acts not only as an important element of prevention against radicalization but also contributes to overall social cohesion. The successful integration of Ukrainians into Czech society serves as a documented example of a well-managed integration process.

Protection of Critical Infrastructure

The Czech Republic is still working on building and strengthening its framework for the protection of critical infrastructure, which will prevent information gathering by hostile states and reduce the risk of sabotage. The goal is to systematically collect and analyze insights about potential security incidents. Experiences from various Western countries, and indeed the case of Vrbětice in the Czech Republic, confirm the BIS's concerns about the capabilities and willingness of some hostile countries to carry out sabotage on our territory in various forms. The state's ability to respond quickly and effectively to such threats will be crucial for its security in the future.

China – A Major Security Issue of Today

The expression ”Chinese threat“ resonates throughout the democratic world. While other actors, led by Russia, openly define how they threaten us, particularly through crimes committed in plain sight and openly declared hostile intentions, understanding the necessity to defend against China‘s (i.e. the PRC) influence is more challenging. The fact that we do not currently perceive a direct Chinese military threat aimed at us, do not record a terrorism threat from China, and are not concerned about massive illegal migration from this territory does not mean that China does not pose an imminent and significant threat to us.



China is distant from the democratic world, not just geographically (with regard to the Euro-Atlantic space) but first and foremost intellectually. Therefore, we must exert more effort to understand its intentions and goals, modus operandi, and the tools it uses to build its desired position as a world leader. Just as China never makes decisions without linking economic interests with politics – a fundamental axiom of the Communist Party of China – so too must we remember the global context of which we are a part. This is all the more challenging because we will need to engage in dialogue with China and cannot avoid cooperating with it.

The threat does not come from the Chinese people, although their gradual increasing indoctrination through information isolation is a factor of high concern, nor from Chinese culture and tradition. However, our technological and strategic raw material dependence on this autocratic regime, which has global ambitions to create an effective counterbalance to the G7 countries, is a situation that requires active response. Falling into China‘s sphere of influence means gradually surrendering technological and strategic know-how to a system representing a different socio-economic concept based on communist dictatorship, which is corrosive to the

fundamental principles of our civilization, namely democracy and the free market.

China expands its geopolitical influence through aggressive lending and trading practices used globally, development initiatives aimed at politically binding poor countries of the Global South, and economic dominance in uncompromising control of the global strategic mineral market. The Czech Republic—a member of the EU, NATO, and numerous other international platforms—does not stand aside in this global competition. Our stance or support, not only towards China but also towards Taiwan, which Beijing considers a vitally neuralgic point and regards as its territory, is of considerable importance to China.

The Czech Republic is not immune to Chinese attacks on the post-pandemic attempts of the Western world to diversify supply chains, which have a direct impact on our economy, cyber espionage aimed at extracting strategic data, and ultimately even escalating military threats in the Indo-Pacific region. In a globalized world, the potential annexation of Taiwan would have direct consequences for the Czech Republic—the shutdown of the dominant global production of

semiconductors would result in drastic inflation and shortages of some products. The Chinese threat is also growing in the context of the war in Ukraine, which is crucial for our security. The North Korea-China axis continuously cultivates relations with Russia, providing it with significant support.

The Chinese diplomatic mission in our territory unsurprisingly focuses on gathering information about the Czech political scene. Members of the Chinese intelligence services have cultivated relationships with influential individuals, and the BIS has recorded China's interest in suppressing activities associated with the so-called five poisons, which it perceives as a threat to the stability of the Communist Party's rule. Whenever the Chinese learn of an event in the Czech Republic where negative comments about China might appear, it begins to take systematic steps to obtain sensitive information about the location, content, and participants of the event.

The Chinese community plays a significant role as it can be utilized at any time, among other things, to support covert operations. Such operations are also conducted in the Czech Republic, where they are carried out by Chinese intelligence services as well as members of Chinese party organizations such as the International Department of the Central Committee of the Communist Party of China (IDCPC) and the United Front Work Department (UFWD).

The academic sphere also represents a valuable source of relevant information and contacts. China uses Czech academics to gather non-public information and to better understand the Czech environment. For identifying and initially approaching academics, China most often uses the professional social network LinkedIn. To establish contact, Chinese intelligence services use cover profiles of employees from fictitious consulting or headhunting companies, most commonly based in Singapore or Hong Kong. Under the pretext of establishing

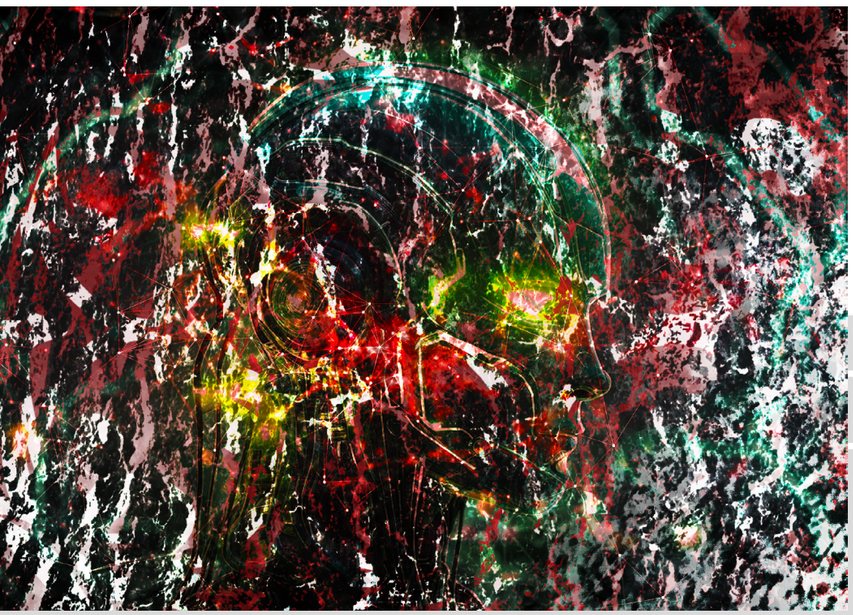
professional cooperation and with the promise of financial reward, they request the creation of reports and studies in areas corresponding to China's political interests. These studies generally serve as a preliminary step towards further cooperation, involving the provision of specific information. Further cultivation includes, among other things, invitations to China, with the Chinese side covering all expenses.

Official invitations to visit China are traditionally used to create a network of contacts who feel indebted and may be inclined to support Chinese interests in

the Czech Republic in the future. Invitations target former and current politicians, representatives of national and local government, prominent academics, and influential businesspeople. Participants may be approached by Chinese intelligence services or their presence may be used for propaganda purposes, not to mention that there can be also a certain sense of obligation created by the hospitality of the Chinese which they would be willing to exploit at a later date.

For China, its image in the eyes of the domestic audience and foreign partners is highly important, which is why it has long been trying to suppress any information that damages the image of a hegemon promoting global peace and order. Throughout 2023, the BIS monitored the ongoing cooperation between Czech and Chinese media scenes, during which Chinese content is distributed mainly to smaller Czech television channels. Chinese content is used to influence the perception of China by the Czech public, showing only the positive aspects of the communist regime while completely omitting or denying any trampling of human rights, oppression of ethnic minorities, and territorial aggression.

China continues its efforts to acquire advanced technologies and know-how possessed by Western countries, using all means, including espionage. There is interest and support from China for joint venture projects, where the manufacturing process is moved to Chinese territory, making it easier to steal Western technology. Another traditional way to gain access to Western technologies and know-how is by sending Chinese students to foreign universities, where they participate in development and research.



In response, the EU and NATO continue efforts to prevent China from obtaining technology in the field of Emerging Disruptive Technologies (EDTs), which includes advanced semiconductor technologies, artificial intelligence, quantum technologies, biotechnology, space technologies, autonomous systems, advanced materials – nanotechnology, etc. The risk of losing control over the further use of proliferable goods in the event of export to China is high. Besides the control regime related to nuclear technologies, China is not a member of any other international control regime governing trade in dual-use items or military material. The strategy of the Chinese government to integrate the civilian and military sectors amplifies the risk that exported technologies will be used to increase the capacities of armed forces. Exports to Chinese entities involved in re-exports also lead to increased production capacities in countries such as Iran or Russia.

In cyberspace in 2023, there was a significant decrease in spear-phishing attacks attributed to a specific Chinese cyber-espionage group that targeted Czech public administration after the start of the Russian invasion of Ukraine. This decline likely occurred due to changes in the targeting of this group, which began focusing on targets in another region. However, this decrease did not mean a reduction in other sophisticated espionage-motivated cyberattacks against Czech public administration.

Cyberattacks attributed to Chinese actors are typically highly sophisticated. They often involve the exploitation of vulnerabilities in software products, and in some cases, these are so-called zero-day vulnerabilities, for which effective patches do not exist at the time of the attack. By exploiting such a vulnerability, the attackers manage to gain initial access to the victim's network, which they can then effectively use to their advantage. The attackers begin to move stealthily within the network, exploring the internal environment and its settings. In the later stages of the attack, they usually ensure persistence in the network by installing additional malicious tools or erasing traces. In the final phase, the attackers exfiltrate targeted data to servers they control, which they can successfully do repeatedly if the victim's detection capability is insufficient or delayed. One such exploited vulnerability can affect not only the organization that becomes the victim of the cyberattack but also other entities that are in a professional, business, or other relationship with it.

Other Important Intelligence Topics

Throughout 2023, the BIS did not detect any immediate threat of Islamist terrorism on Czech territory. Only a few individuals were investigated due to signs of Islamist radicalistation, which is in accordance with the positive trend of recent years. In Europe, however, the level of threat from Islamist terrorism began to increase in the second half of 2023. This was not a random fluctuation but a result of the resurgence of traditional mobilizing influences, specifically numerous instances of desecration of the Quran and the escalation of the Israeli-Palestinian conflict. Another factor influencing the threat level was the effort of the Afghan branch of the so-called Islamic State (IS) to motivate attacks in Europe. Due to its inability to send trained terrorists to Europe, IS tried to incite attacks through online communication, targeting primarily individuals from Russian-speaking diasporas in Europe, often originating from Central Asia.

In May 2023, a Kyrgyz individual transiting through the Czech Republic, who was under investigation by European intelligence services for contacts with individuals associated with IS, spent one night in Prague. One of his contacts was a Tajik, who was arrested in June 2023 in the Netherlands for preparing acts of terrorism. No activity of concern related to this journey, or the journeys of other investigated Central Asians through the Czech Republic, was detected on our territory. The transit of high-risk individuals through the Czech Republic is not a new phenomenon, but such cases increased in 2023.

From the perspective of ideological orientation, 2023 did not bring any changes to the Czech Muslim community. It maintained its moderate character, disrupted only by a few individual expressions of radical tendencies, which were not representative of the views of the majority of Czech Muslims. The conflict between Israel and the terrorist organization Hamas had the most significant influence on the community regarding one-sided support for Israel. Palestinians living in the Czech Republic focused on providing aid to their relatives affected by the situation in Gaza, which allowed mainly leftist-oriented entities and activists to take over the dominant role in pro-Palestinian and anti-Israeli events from the early beginning. They accused Israel of long-term oppression of Palestinians in Gaza, colonialism, and genocide. Compared to similar demonstrations worldwide, the events in the Czech Republic were peaceful.

One significant trend affecting the threat of Islamist terrorism is self-radicalization via the internet. The age of radicalized individuals has been gradually decreasing, including not only adolescents but also children around 13 years potential radicalization in 2023. While the Arab and Muslim communities of interest mostly supported the Palestinians, only a few individuals expressed support for Hamas during the conflict, and this opinion did not prevail in the community.

As the conflict continued and the number of Palestinian casualties increased, there began to be criticism of the Czech government representatives and media, accusing them of

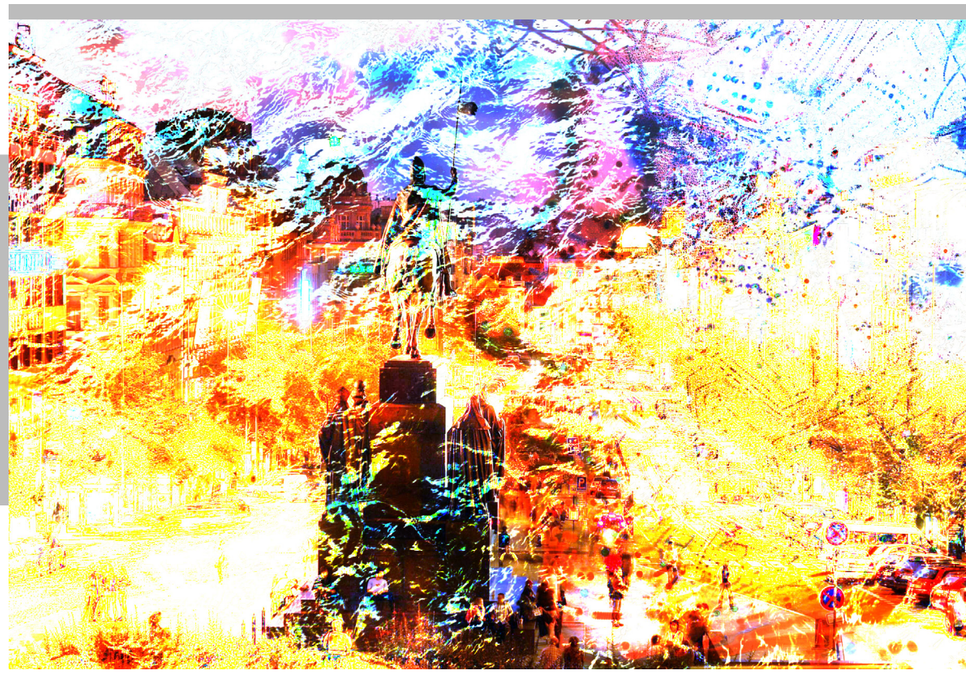
of age. Another phenomenon is the relatively rapid radicalization (within weeks to months) under the influence of foreign events and their biased or purposeful interpretation, such as the desecration of religious symbols or the situation in the Gaza Strip. An important factor is that some radicalized individuals suffer from mental disorders. In response to this development, international and especially interdepartmental cooperation in the area of risk analysis of radical expressions on the internet is being intensified.

Disinformation narratives spread throughout 2023 focused on the war in Ukraine and the related economic and social issues. As in previous years, one of the main channels for spreading disinformation were websites and social networks. However, an important trend was the increased popularity of sharing content in the form of videos, which amplified the influence of platforms like YouTube and TikTok.

The activities of the Czech disinformation scene remained largely autonomous, without coordination or direction by a foreign actor. Nevertheless, the BIS identified several cases of domestic alternative media or disinformation activists being exploited to disseminate pro-Russian narratives in the Czech information space. For example, as early as 2022, a Russian influence agent operating long-term in the Czech Republic ensured the dissemination of Russian propaganda at the request of one of the top-ranking institutions of the Russian state. An information campaign with a budget of several thousand euros questioned the meaningfulness of providing aid to Ukraine or the EU sanctions and involved some publicly known figures.

Platforms directly connected to Russia also operated in this environment, spreading pro-Russian disinformation through altered and deceitful videos. One of the videos was introduced into the Czech information space during the presidential elections in January 2023 via the Telegram channel „neČT24“ in order to discredit one of the presidential candidates.

The extremist scene as a whole did not represent a significant security risk. The number of individuals inclined towards violence was marginal. Socially vulnerable individuals, whose primary motive for hateful expressions is not ideology but rather a fascination with violence, have remained potentially dangerous. In this context, Siege culture (an extreme form of neo-Nazism) is particularly popular. Except for a few exceptions, these individuals are active only on the internet. The Czech militia and paramilitary scene struggled with a lack of members, whose number continued to decrease. The persistent and most dangerous activity associated with militia activities was the effort to produce illegal firearms and explosives.



In December 2023, an active shooter attack occurred at the Faculty of Arts at Charles University in Prague, during which the perpetrator killed 14 people and injured dozens of others. This act was the most tragic event of its kind in modern Czech history. The attack ended with the suicide of the perpetrator. Shortly before the attack, the shooter also killed his father and earlier had shot a 32-year-old man and his two-month-old daughter in Klánovice, Prague. They were random victims with no relation to the perpetrator.

According to the information obtained, it was an individual attack by a lone shooter. The act was not terrorist or extremist in its nature but a criminal act by an individual. The killer was not connected to any extremist or terrorist group, which made timely identification very difficult. This tragedy demonstrated that such crimes can also occur in the Czech Republic. Although they cannot be prevented in all cases, their potential consequences can at least be minimized through systemic measures (protection of soft targets, training for potential victims, early warning systems, appropriate weapons legislation, etc.). Close cooperation between public administration bodies and security forces, including the BIS, is essential.

Cooperation with Czech Intelligence Services and Other Authorities

Cooperation with Czech Intelligence Services

In 2023, the BIS sent more than 100 reports to the Office for Foreign Relations and Information and more than 40 reports to Military Intelligence. Cooperation with both services also takes place in other operational, analytical, or support activities.

The BIS's collaboration with the Office for Foreign Relations and Information in screening applicants for diplomatic accreditation aims to reduce the security risk from hostile activities of individuals operating in diplomatic services on our territory. This close cooperation continued in 2023, during which 199 diplomats, members of diplomatic staff, and their family members were vetted, representing a slight increase in comparison to 2022.

There was also cooperation with the Ministry of Defense, specifically Military Intelligence, in the development of the integrated public register system for the needs of intelligence services.

Furthermore, the BIS, Military Intelligence and the Office for Foreign Relations and Information took part in EU or NATO crisis management exercises.

Cooperation with the Police of the Czech Republic

The Police of the Czech Republic is, after the President, the Prime Minister, and the ministers, another recipient of certain intelligence information from the BIS, in accordance with Section 8 (3) of Act No. 153/1994 Coll. Information relevant to its scope of powers is provided to the Police in cases where the transfer does not jeopardize an important interest of the BIS. Cooperation between the BIS and the Police takes place mainly with regard to the information provided. Information exchange also occurs in response to requests from the Police or the public prosecutor's office concerning specific criminal proceedings.

As in previous years, the BIS collaborated with the Directorate of the Alien and Border Police to screen applicants for short-term and long-term Schengen visas. In 2023, the BIS screened almost 1,700,000 applicants. One factor influencing the number of screened visa applications was the new restrictive visa policy towards Russia, which the EU adopted following the outbreak of war in Ukraine. Strict rules were adopted in the Czech Republic regarding visa applications from Russian and Belarusian citizens, resulting not only in a reduction in their number but also in limiting the possibility of visa misuse by individuals collaborating with foreign powers. The tightening of rules included a measure allowing the BIS to comment on visa applications from Russian citizens submitted at the consular offices of all EU member states. In 2023, more than 4% of the total number of visas submitted by Russian citizens were denied, compared to only a fraction of a percent in 2020. Czech measures are among the strictest in Europe and significantly contribute to reducing the security threat posed by the activities of Russian intelligence officers.

In 2023, the BIS continued its cooperation with the Directorate of the Alien Police Service on the screening of individuals required by the Civil Aviation Act, who are applying for a certificate of reliability. The screening's purpose is to prevent any security risks posed by individuals applying for permission to enter restricted security areas at airports.

The cooperation between the BIS and the Directorate of the Alien Police Service includes also the inclusion of foreigners in the register of undesirable persons, which serves to prevent the entry of foreigners who might pose a threat to national security while staying in the Czech Republic.

Cooperation with the National Center for Combating Organized Crime and the National Center against Terrorism, Extremism, and Cybercrime (NCTEKK) involved the exchange of information primarily on issues related to significant major interests, terrorism, organized crime, proliferation, and cyber security.

Cooperation with Other Public Authorities and Institutions

The BIS provides information and assessments to selected public administration bodies regarding the security screening of individuals and companies, either based on legal provisions or interdepartmental cooperation agreements. The main recipients of such information include the National Security Authority, the Ministry of the Interior, and the Ministry of Foreign Affairs.

Concerning personnel and industrial security screenings, the BIS cooperates with the National Security Authority, in accordance with Section 107 (1), Section 108 (1), and Section 109 (1) of Act No. 412/2005 Coll., by conducting so-called administrative screenings or by gathering information in the field when required by the NBÚ in accordance with Section 107 (2–3), Section 108 (2–4), and Section 109 (2) of Act No. 412/2005 Coll. During field investigations, standard intelligence activities are conducted and specialized intelligence-gathering means may be used.

Within its scope of powers, the BIS also gathers – even without a request from the National Security Authority – information indicating that holders of security eligibility certificates no longer meet the legal requirements. Any relevant findings are promptly forwarded to the National Security Authority, provided this does not compromise an important interest pursued by the BIS. In 2023, the BIS conducted more than 22,000 administrative screenings based on requests from the National Security Authority.

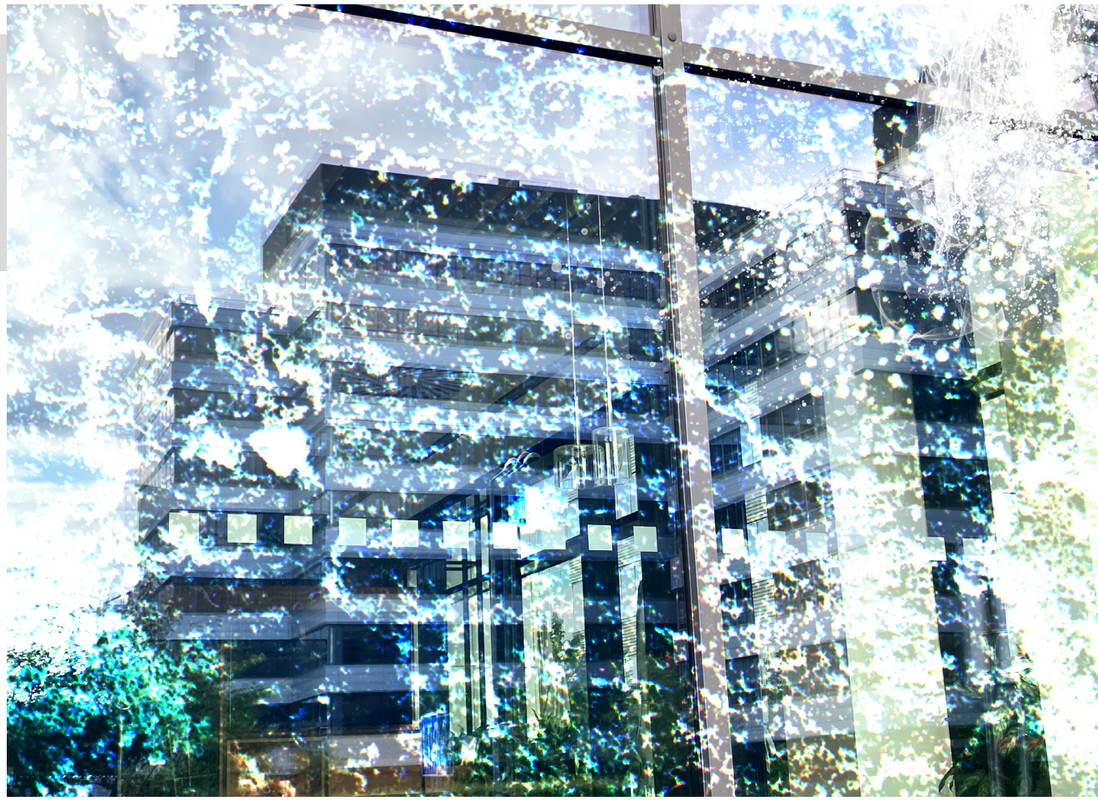
Within the interdepartmental working group „Impacts of Public Administration Digitization on the Activities of the Security Forces of the Czech Republic," there continued to be close cooperation with the Ministry of the Interior and other involved security forces on measures related to the digitization of public administration.

The Ministry of the Interior and other entities under its budget chapter have long provided the BIS with a number of services based on agreements in the areas of electronic communications, fire protection activities, occupational health and safety, energy, water management, environment protection, and also in the area of catering.

In 2023, cooperation with the Ministry of the Interior continued namely with regard to preventing security risks from foreigners applying for international protection, residence permits, and citizenship. The BIS also participated in the screening of legal and natural persons applying for employment agency certification and continued to screen individuals applying for authorization to enter the services of the armed forces of Ukraine. Cooperation continued also on matters regarding the Electronic Identification Act and, newly, in assessing applicants for inclusion in the national cloud computing catalog.

Furthermore, the BIS continued its cooperation with the Department of Security Policy of the Ministry of the Interior in screening individuals and legal entities applying for employment agency certification according to the Employment Act. Due to the ongoing war conflict, the screening of individuals applying for authorization to join the armed forces of Ukraine under the Conscription Act also continued in 2023 in cooperation with the Department.

Cooperation with the Ministry of the Interior continued on screening individuals applying for international protection and residence permits in the Czech Republic. As in 2022, the war in Ukraine impacted the structure of applicants. In 2023, the BIS screened 789 applicants for international protection, with the largest number of applicants coming from Ukraine, followed by applicants from Syria, Afghanistan, Russia, and Belarus. The BIS also screened 157,000 applicants for residence permits and 303,000 applicants for temporary protection.



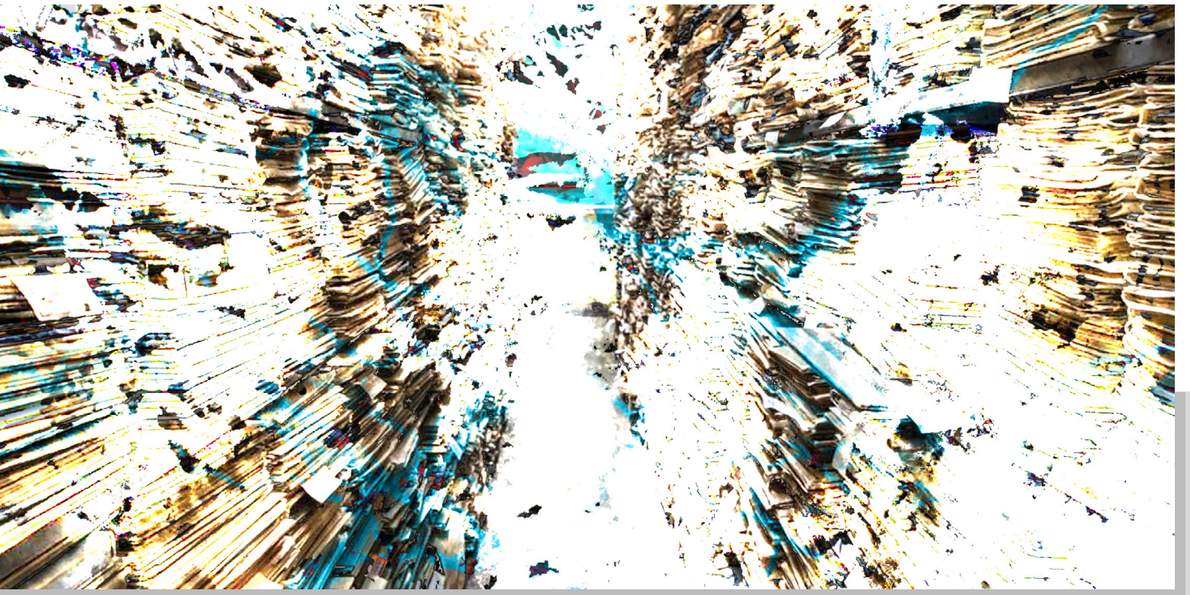
In connection with the war in Ukraine triggered by the Russian invasion in 2022 and considering the change in the security landscape, the presence of some individuals in the Czech Republic was assessed as a potential security risk. In a number of cases, residence permits were revoked and individuals were required to leave the territory.

During the vetting of individuals under the MEDEVAC medical and humanitarian project and the Humanitarian, Stabilization, Reconstruction, and Economic Assistance Program for Ukraine, a total of 57 individuals were screened. In all cases, these were medical personnel participating in professional internships in the Czech Republic.

In 2023, the BIS screened 5,500 applicants over the age of 15 who were applying for Czech citizenship. This figure aligns with the long-term trend of increasing numbers of applicants. In 2023, the BIS completed the re-vetting process regarding applicants of Russian nationality whose applications were still pending at the time of the outbreak of war in Ukraine.

The significant increase in negative the BIS assessments regarding citizenship applicants from Russia in 2023 was given by the recent developments in the security landscape following the start of the armed conflict.

Throughout 2023, the BIS received 50 applications for inclusion in the national cloud computing catalog (which involves storing data, applications, and programs on provider servers, with user access ensured remotely) according to the Act on Information Systems of



Public Administration, meaning that 85 legal entities and 182 individuals were screened. The BIS did not receive any applications in 2023 for accreditation for the management of a certified electronic identification system, granted according to the Electronic Identification Act.

Cooperation with the Ministry of Foreign Affairs focused mainly on the screening of prospective employees or collaborators of the ministry. The number of vetted individuals was similar to the previous year, with a total of 555 individuals and 19 legal entities.

For the third year, the BIS participated in the screening of foreign investments. In 2023, there was a resurgence in investments, and twice as many cases were investigated as in the previous year. The BIS screened 15 investment projects as part of the consultation process and six projects as part of formal proceedings. The European notification system also saw a 14% increase in the number of screened investments. In 2023, the BIS paid increased attention to identifying investments which the investor did not submit for screening in due time, although prior approval from the Ministry of Industry and Trade was required by the law. Most priority was placed on monitoring ownership changes in legal entities whose ultimate owners were on the EU sanctions list. Specific cases were then addressed by the BIS in close cooperation with the Ministry.

The BIS regularly shared intelligence insights within the Joint Intelligence Group and contributed information for assessing the security situation in terms of potential threats to the Czech Republic. The BIS also continuously shared information within the NKBT platform, which operates as one of the departments of the NCTEKK. The main focus of this cooperation was on the screening of

identities investigated in connection to terrorist attacks on EU territory.

Representatives of the BIS participated in meetings of working bodies of the National Security Council, including the Intelligence Committee, Internal Security Committee, Committee for Coordination of Foreign Security Policy, Defense Planning Committee, Cyber Security Committee, and Civil Emergency Planning Committee. The BIS expert departments prepared assessments and reviewed materials in collaboration with the committees as well as the National Security Council.

In addition to the above, the BIS also cooperated with the General Inspection of Security Forces, the Financial Analytical Office, the Customs Administration of the Czech Republic, the General Directorate of Customs, the Prison Service of the Czech Republic, the General Financial Directorate, and with courts and public prosecutors.

The cooperation with other public administration bodies also involved addressing specific cases related to the proliferation of weapons of mass destruction and related delivery systems, and the trade in military material. This cooperation was particularly close with customs authorities, both at the level of the General Directorate of Customs and individual customs offices. There was ongoing collaboration with customs authorities concerning the risks of potential transports of controlled items, especially military material and dual-use items, to sanctioned countries. In specific cases, cooperation also took place with the Ministry of the Interior, the Ministry of Defense, the Ministry of Foreign Affairs, the Licensing Authority of the Ministry of Industry and Trade, the State Office for Nuclear Safety, and other organizations. The cooperation regarded ongoing licensing proceedings as well as reports on compliance with licensing conditions and international control regimes.

The BIS continued to coordinate the work of the Intelligence Activities Committee regarding the export of equipment which is not listed in international control regimes but can be regarded as dual-use material if exported to high-risk areas. Representatives of the Ministry of the Interior, Ministry of Foreign Affairs, Ministry of Industry and Trade, State Office for Nuclear Safety, General Directorate of Customs, Financial Analytical Office, Office for Foreign Relations and Information, and Military Intelligence were involved in fulfilling this task.

In securing information on activities threatening major economic interests, the BIS collaborated with other public administration bodies. Communication with the General Financial Directorate concerned primarily information from tax proceedings, which the BIS is authorized to obtain. Information relevant to their scope was provided to law enforcement agencies, State Office for Nuclear Safety, and the Office for the Protection of Competition.

Active cooperation continued within the interdepartmental body for combating illegal employment. The activities of this body focus, among other things, on inspection activities related to the operations of employment agencies and, last but not least, on activities referred to as undeclared work.

Cooperation with the National Security Authority involves consultations on securing classified information within the framework of physical security.

With the National Cyber and Information Security Agency, the BIS collaborates primarily on topics related to the protection of classified information in ICT, including the certification of such systems, as well as in the area of compromising emissions and cryptographic protection of classified information.

The BIS also actively participated in the activities of the National Group for Combating Proliferation, which focused primarily on operational cooperation.

Cooperation with Foreign Intelligence Services

Cooperation with foreign intelligence services is a key factor in several areas of the BIS's operations, enabling it to provide its statutory recipients with crucial information regarding the security of the Czech Republic. With the approval of the Czech Government, the BIS is authorized to cooperate with more than a hundred intelligence services from around the world. The BIS primarily develops information exchange and active contacts with services from EU, NATO, and certain other countries. At the multilateral level, the BIS took active part in the activities of all working bodies of which it is a member (e.g., the Counter-Terrorism Group and NATO Civilian Intelligence Committee) throughout 2023.

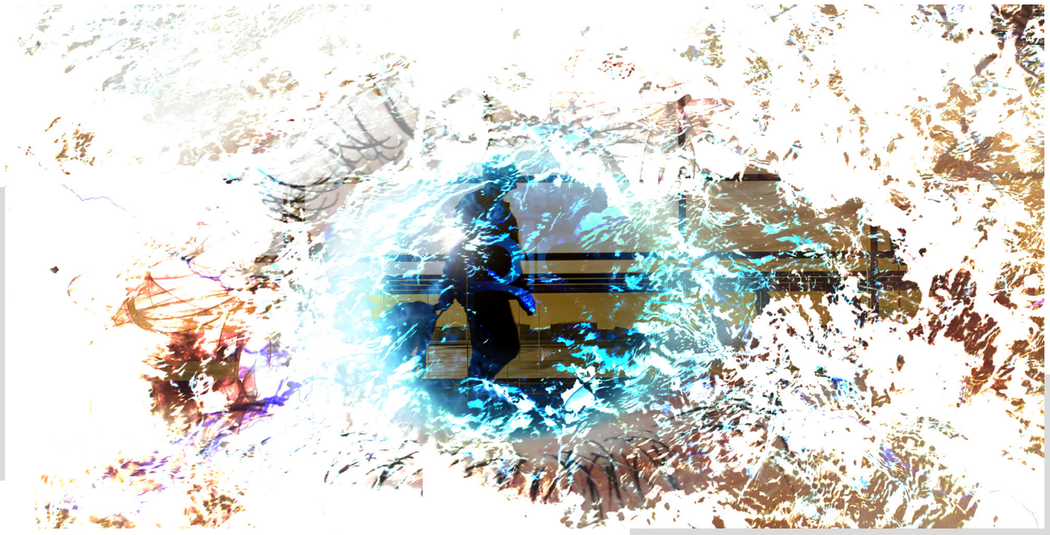
The main areas of the cooperation between the BIS and foreign intelligence services are counter-terrorism, counter-espionage, proliferation, cyber security, and the protection of classified information. As part of international cooperation, the BIS received more than 14,000 reports and forwarded more than 2,500 documents in 2023. At the strategic and expert levels, BIS representatives participated in more than 900 international meetings.

Oversight

The legal basis for the oversight of BIS activities is anchored in Section 12 (1) of Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, which stipulates that BIS activities are subject to oversight by the Government, the Chamber of Deputies, and the Independent Intelligence Oversight Body of the Czech Republic.

Although the law does not specify the exact scope or method of oversight by the Government, its oversight powers with regard to the BIS are based on its authority to assign tasks to the BIS and evaluate their fulfillment. The Government is responsible for the work of the BIS, it coordinates it, and appoints and dismisses its director general. The BIS is also obliged to submit annual reports on its activities to the President of the Republic and the Government as well as to report on its activities whenever requested. This provision indicates that government oversight covers all areas of BIS activities.

The Chamber of Deputies is informed about the activities of intelligence services by the Government through its intelligence oversight body. In relation to the BIS, the relevant body is the Permanent Commission for the Oversight of the BIS. Members of this commission are, for example, authorized to enter BIS premises accompanied by the BIS director general or a designated officer. The oversight body can also request necessary explanations from the BIS director general if it suspects that BIS activities unlawfully restrict or harm citizens' rights and freedoms. Additionally, the BIS director general is obliged to submit information and documents specified by the law to the oversight body.



Act No. 325/2017 Coll., which amends Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, and other related laws, envisages the establishment of a five-member Independent Intelligence Oversight Body of the Czech Republic, appointed by the Chamber of Deputies for a five-year term based on a proposal by the Government. This body is expected to review the activities of the BIS when requested by one of the special oversight bodies. This body, which will be authorized to request from the intelligence service, with a few exceptions, all necessary information about its activities related to the issue under review, has not yet been appointed in 2023.

The fulfillment of the BIS's tasks in the area of public property management and national budget compliance is overseen by relevant public authorities, for example, under Act No. 320/2001 Coll., on Financial Control in Public Administration, Decree No. 416/2004 Coll., implementing this act, and Act No. 166/1993 Coll., on the Supreme Audit Office, as amended.

The protection of the secrecy of intelligence services' activities is ensured by special methods by which oversight is conducted. For instance, in the facilities of the intelligence service, oversight can only be performed with the consent of its director general.

In cases of using intelligence technology according to Act No. 154/1994 Coll., BIS activities are also subject to judicial oversight. The authorization to use intelligence technology is decided by the president of the panel of judges of the High Court in Prague, who also oversees the process of its use. The chairman of the panel of judges of the High Court in Prague additionally decides on BIS's requests for reports on matters concerning clients that are subject to banking secrecy. The court not only issues prior authorization based on the BIS's written request but also monitors whether the reasons for the request persist. If not, the authorization is revoked or withdrawn.

The public monitors BIS activities mainly through mass media or via the BIS's website, where, for example, annual reports and current communications regarding the security situation are freely accessible.

Compliance, Handling Requests and Notifications

The scope of responsibilities of the Inspection Department involves handling requests from law enforcement authorities or other public administration bodies and investigating reports, suggestions, and complaints directed at BIS officers. The Inspection Department investigates cases of suspected misconduct that bear the characteristics of disciplinary infractions and misdemeanor, including the investigation of emergency events. Additionally, the Inspection Department, within its scope, acts as a law enforcement body in cases of suspected criminal offenses committed by BIS officers, as defined in Section 12 (2f) of the Criminal Procedure Code.

The vast majority of investigations into suspected disciplinary infractions or acts bearing the characteristics of misdemeanor in 2023 were related to transportation, such as traffic accidents involving service or private vehicles, damage to service vehicles, and suspicions of other violations of traffic laws. Cases where a suspicion of a disciplinary infraction or an act bearing the characteristics of misdemeanor by a BIS officer was found were referred for disciplinary proceedings.

Out of a total of 93 submissions, none were evaluated as complaints about the conduct of BIS officers. The content of all submissions was reviewed and evaluated. Some submissions were forwarded to BIS intelligence units for further action. Other submissions were forwarded to relevant public administration bodies or the Police of the Czech Republic. The content of citizen reports reflects societal events, mirroring the situation surrounding the war conflict in Ukraine and Israel.

The Inspection Department collaborates with other public administration bodies primarily in the form of requests, most frequently sent by Police authorities involved in criminal or administrative proceedings.

As a law enforcement body, the Inspection Department fulfills tasks arising from the Criminal Procedure Code and is overseen by the competent and locally relevant public prosecutor's office in the course of its activities.

Security Information Service
Annual Report 2023

Budget

The budget for the BIS for the year 2023 was set by Act No. 449/2022 Coll., on the State Budget of the Czech Republic for 2023. Revenues for the chapter were set at CZK 250,000 thousand and expenditures at CZK 2,227,190 thousand.

In addition to budgetary funds, the BIS had claims from unused expenditures in 2023. The final expenditure budget, representing the total available resources including the engaged and consumed unused expenditures amounted to CZK 2,568,530 thousand by the end of the reporting period.

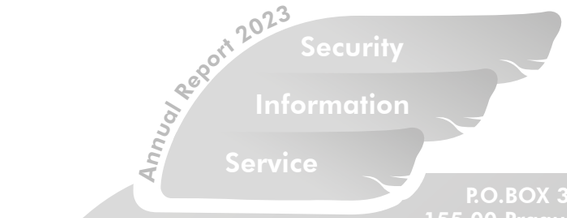
The total actual expenditures in 2023 reached CZK 2,375,501 thousand, which represents 107% of the adjusted budget or 92.5% of the final budget for the chapter.

Capital expenditures approved for 2023 were utilized to maintain the operational capability of the material and technical base and its necessary development. In 2023, the most significant project in this program was the construction of a technical-administrative building, which was successfully completed in the second quarter of 2023 after nearly five years of construction. Alongside this major investment, work began on another crucial multi-year investment project, the development of a new intelligence information system. Other investment actions primarily involved the simple reproduction and necessary development of the BIS's long-term assets. A significant portion of the investments was also directed towards acquiring and modernizing intelligence technology and information and communication technologies. It is also worth noting the expenditures on the necessary renewal of transportation vehicles.

The largest portion of current expenditures was payroll expenses, including salaries and related costs, whose year-on-year growth was due to the increase in basic tariffs for service income of officers as of January 1, 2023. Expenditures on retirement benefits, which are due to former officers who have met the required length of service, remained at the same level as in the previous year.

Another significant group of current expenditures, in line with the special financial management procedures of the BIS, includes expenses for specialized equipment specific to the intelligence service's activities and special financial resources allocated for direct intelligence activities.

Current expenditures also include operational expenses, which primarily cover services ensuring daily operations and contractor-provided repairs and maintenance of BIS assets and facilities. In 2023, the level of these operational expenses was influenced by the rise in prices of various commodities and services essential for BIS operations and its scope of activities. The year 2023 was marked by high energy and fuel prices. However, for the BIS, the market price developments of these commodities did not pose a significant issue in terms of budget management, as fixed prices for most supply points had been contractually secured at pre-energy crisis levels.



P.O.BOX 31
155 00 Prague 515
Czech Republic
Phone: +420 235 521 400
Fax: +420 235 521 715
E-mail: info@bis.cz
Data box: cx2aize