



SECURITY INFORMATION SERVICE

Annual report
2025

Security Information Service
Annual Report 2025



TABLE OF CONTENTS

Message from the Director of the Security Information Service	5
Nature and Scope of Intelligence Activities	7
Intelligence Insights	8
Russia – An Ongoing Security Threat	10
Proliferation Networks	16
Cyberattacks	18
China’s Activities in the Czech Republic	20
Energy Security and Protection of Public Finances	22
Terrorism a Radicalization	24
Protection of the Democratic Foundations of the State	27
Cooperation at the National Level	30
Cooperation at the International Level	35
Careers at the BIS	36
Public Relations	38
Budget	40



genpor. Ing. Michal Koudelka
Director General Security Information Service

Dear Readers,

Once again after a year, it is my pleasure to present to you the traditional public annual report on the activities of the Security Information Service, this time for the year 2025. It was a year full of events that undoubtedly had a fundamental impact on the global security situation. The Russian Federation's aggressive war against Ukraine continued, the conflict in the Middle East escalated—resulting this year in an armed clash between the US and Israel on one side and Iran on the other—and China's aggressive rhetoric regarding Taiwan also intensified. This extraordinarily explosive cocktail was further framed by shifts in the long-standing US stance toward Europe and its security. We must therefore mark 2025 as one of the most serious years in the realm of security since the end of the Cold War.

However distant all these mentioned conflicts may seem to the Czech Republic, we have clearly felt their impact and will continue to do so. There are still hundreds of thousands of Ukrainian refugees in the Czech Republic, Russia continues its hybrid operations against EU countries including the Czech Republic, China is intensifying its intelligence activities in cyberspace and elsewhere, the risk of terrorist attacks in Europe is growing, proliferation activities are increasing, and the risk of illegal migration persists. Added to this are the economic impacts of the Middle East conflict, which triggered a prolonged and significant rise in oil prices with all its security and economic consequences, alongside differing views between the US and its European partners on addressing certain pressing issues.

During these times, the BIS bears a far more critical responsibility as a vital component of the state's security architecture than ever before in the past. I consider it good news that, even during this extraordinarily challenging period, the Service succeeded in performing its tasks to an above-standard degree, thereby helping to ensure the safety of our citizens. Just to mention a few key examples of the cases the BIS addressed in 2025: First and foremost, these include extensive Russian hybrid activities, ranging from the dissemination of disinformation and Russian propaganda to the massive recruitment of so-called single-use agents who could carry out sabotage here and across Europe, and extending to conventional intelligence operations and cyberattacks targeting our country. I consider the BIS ability to monitor these activities and thereby prevent potential risks to be absolutely crucial. At the same time, we managed to deal Russia a significant blow by exposing an individual who provided insurance for the so-called Russian shadow fleet used for illegal oil exports, and who was placed on both the national and European sanctions lists this year. These are precisely the clear and confident signals that Russia understands.

Based on a BIS initiative within the European intelligence community, an important measure was successfully implemented to combat cross-border operations by Russian intelligence officers. The objective is to gain oversight of Russian travel into Czech territory and to make it more difficult to use the travel of Russian diplomatic and official personnel as cover for intelligence operations.

The year 2025 brought a number of other challenges for the BIS, which you will read about on the following pages of this annual report. These include Chinese intelligence activities and cyberattacks, online radicalization of minors, the growing activities of left-wing extremists particularly in relation to Palestine, and the issue of proliferation.

This annual report is the tenth and final one issued by the BIS under my leadership. My second term of office will come to an end in February 2027. I would therefore like to thank from the bottom of my heart everyone who supported the BIS and me personally throughout this entire time and helped us with our mission. I am proud to be handing over the BIS as a service that is strong and respected both at home and abroad—a confident, proud, and internally consolidated service. According to independent polls, the BIS enjoys high and stable trust among the citizens of the Czech Republic. One of my goals—to build a bridge of trust between the public and the BIS—has thus been abundantly fulfilled.



| Nature and scope of intelligence activities

The activities, status, and scope of powers of the Security Information Service (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 and Section 5 (1) of Act No. 153/1994 Coll., the BIS is an intelligence service that, within its powers and responsibilities, 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 the consequences of which 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 other 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.

Act No. 153/1994 Coll., in the provision of Section 7, further stipulates that the Government is responsible for and coordinates the activities of Czech intelligence services. Under the provision of Section 8 (4) of this Act, the Government assigns tasks to the BIS within its scope of powers and responsibilities. The President of the Czech Republic also has the authority 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.

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



Intelligence insights

Russia – An Ongoing Security Threat

10

Proliferation Networks

16

Cyberattacks

18

China's Activities in the Czech Republic

20

Energy Security and Protection of Public Finances

22

Terrorism and Radicalization

24

Protection of the Democratic Foundations
of the State

27

RUSSIA

– an ongoing security threat

| The Risk of Sabotage Attacks

The number of uncovered sabotage or other subversive attacks coordinated by Russia, for which „single-use agents“ are hired, decreased in Europe in the first half of 2025; however, since the second half of the year, it has returned to an upward trend. The term „single-use agent“ is derived from the fact that, in the event these individuals are detained, Russia disclaims any responsibility for their actions or for resolving their situation. They are often inexperienced amateurs, as well as individuals with a lower social status or prior criminal history. The predominant motivation is the prospect of financial reward.

Single-use agents usually receive specific instructions from their coordinators only after stating which targets within their reach they are capable of focusing on. Therefore, the risk of a sabotage attack on a specific target depends more on the circumstances of individual agents than on a comprehensive plan by Russian state authorities. This fact is among the factors that make it more difficult to detect the preparation of potential attacks.

The perpetrators of these attacks are often required not only to carry out the attack itself but also to ensure the collection and sharing of visual documentation (photographs, video recordings) showing the preparation, execution, and aftermath of the attack. This documentation subsequently serves as a basis for producing media content that is distributed both within Russia and to European countries. The key message is intended to be that Europe is figuratively and literally „in flames“.

Through these sabotage attacks, in addition to causing nervousness and fear, Russia aims to ensure that the dominant opinion in the public debate of the affected countries becomes that it is not worth providing political support and material aid to attacked Ukraine, from either an economic or a security perspective. It seeks to spread the message that if the countries in question want to avoid trouble, they must get out of Russia's way as

it pursues its geopolitical interests. Regarding the coordination of these attacks, the Russian military intelligence agency (GRU) remains the dominant actor. The involvement of Russian intelligence services was confirmed, among other instances, in the case of a bomb attack on the Polish railway in November 2025.

In none of the security incidents recorded in the Czech Republic in 2025, where investigations were carried out to determine whether they could be a sabotage attack coordinated by Russia or the preparation thereof, has this suspicion been reliably confirmed so far (or it was not confirmed that the investigated activities of the individuals had any real potential to result in a sabotage attack on our territory). The same applies to advertisements offering financial rewards for participating in the preparation or execution of a sabotage attack, which are distributed on the Telegram platform in groups aimed at a Russian- or Ukrainian-speaking audience and simultaneously linked to the Czech environment. The demand for sabotage attacks spread through these groups is enormous, amounting to hundreds of thousands of posts per year, but they predominantly concern targets located in Ukraine or other EU member states rather than the Czech Republic.

The risk of using single-use agents for sabotage attacks directed by Russia clearly persists and primarily concerns entities involved in the production or distribution of aid destined for Ukraine. The highest authorities of the Russian state power adjust the intensity of using sabotage attacks to pressure European states depending on how the situation on the Ukrainian battlefield or the international political constellation develops. Even after the current hot phase of the conflict with Ukraine ends, it cannot be guaranteed that Russia will desist from using single-use agents for sabotage attacks or other subversive activities (such as destabilizing public provocations).

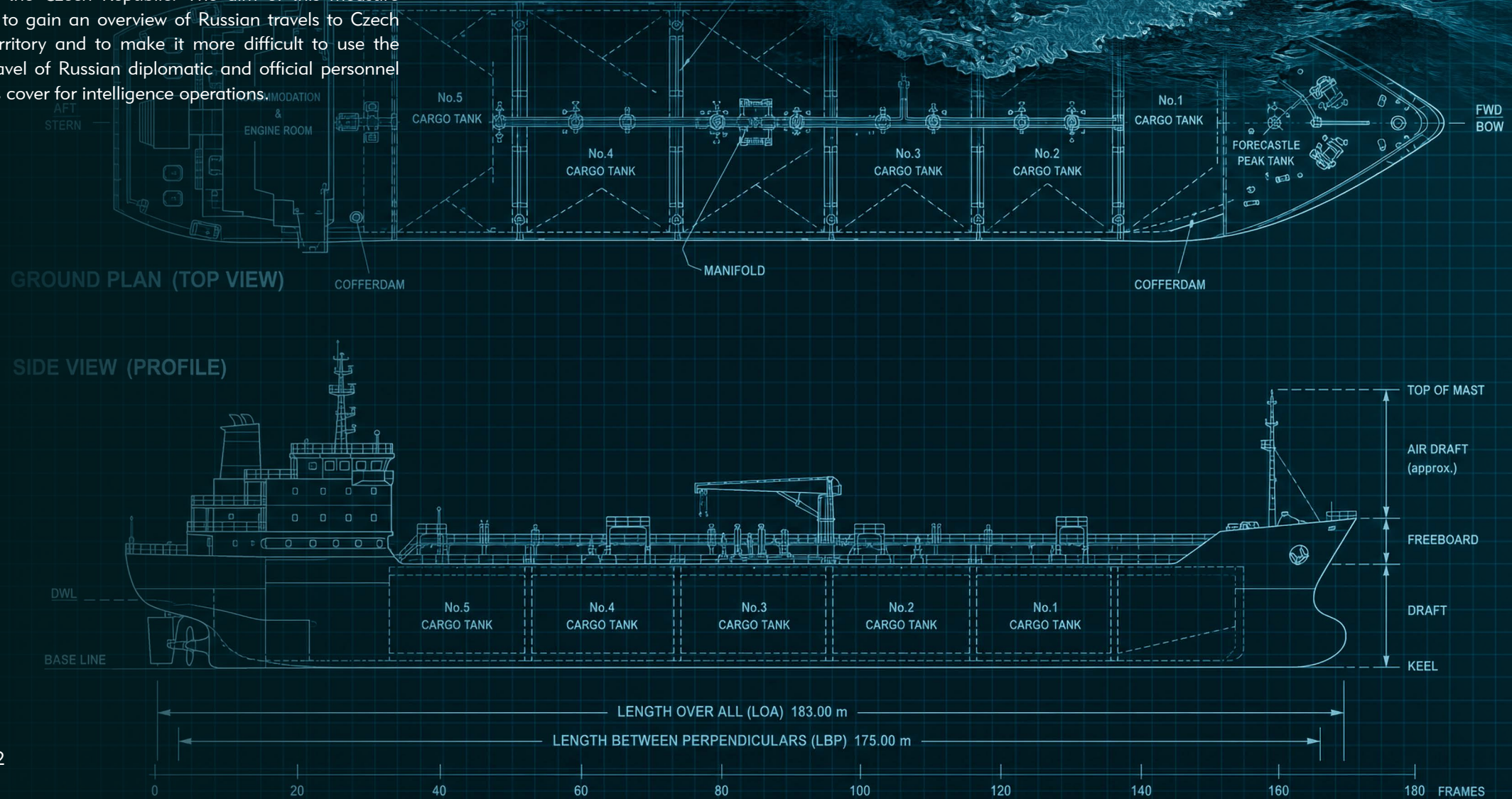




Diplomatic Cover

Diplomatic cover remains among the primary methods by which Russian intelligence services secure their presence in a target country; in the Czech Republic, certain posts at the Embassy of the Russian Federation in Prague are utilized for this purpose. The geographical location and the permeability of borders within the Schengen Area also make the Czech Republic highly vulnerable to Russian intelligence activities conducted from abroad.

An important measure in the fight against cross-border operations by Russian intelligence officers was a regulation adopted in October 2025 (as part of the EU's 19th sanctions package against Russia), which restricted the free movement of Russian diplomatic and administrative-technical personnel within the Schengen Area. Based on this regulation, the Czech Republic decided to introduce a mandatory notification for Russian personnel accredited in the EU – meaning the obligation to notify Czech state authorities of an intent to travel to the Czech Republic. The aim of this measure is to gain an overview of Russian travels to Czech territory and to make it more difficult to use the travel of Russian diplomatic and official personnel as cover for intelligence operations.



The Shadow Fleet

One of the significant sources from which Russia finances its war of aggression against Ukraine is the sale of oil exported from Russia by tankers of the Russian shadow fleet. Its operation is therefore among the factors delaying the conclusion of peace, and it is thus in the interest of the Czech Republic to participate in adopting available measures to neutralize its activities.

The intelligence investigation, which took place throughout 2025, resulted (in March 2026) in the inclusion of Konstantin Rogach on the Czech national sanctions list, specifically in connection with activities supporting the operation of the Russian shadow fleet.

Russian (and Israeli) citizen Konstantin Rogach has long provided commercial services through companies based in Russia, Cyprus, and the Czech Republic to entities operating in international maritime transport. In recent years, he also brokered insurance and provided administrative support for tankers operating within the Russian shadow fleet (tanker insurance is among the key and essential aspects of their operation within international maritime transport). He utilized offshore companies based in Turkey and the Marshall Islands for financial transactions. He also cooperated with insurance companies listed on the sanctions lists of the EU, Great Britain, the USA, and other countries. It is likely that Konstantin Rogach carried out activities in favor of the Russian shadow fleet in fulfillment of a task assigned by one of the bodies of Russian state power.



OIL TANKER
INVESTOR - RUSSIAN FEDERATION

DESIGN OFFICE - DPBK
SHIPYARD CONTRACTOR - PERVAYA VLADIVOSTOCKA VERF

BASIC PARAMETERS
LENGTH WATERLINE 175 M
BEAM 28.26 M
DRAFT 12.6 M
AIR DRAFT 23.7 M
DWT 45 000 - 60 000

| Influence Operations

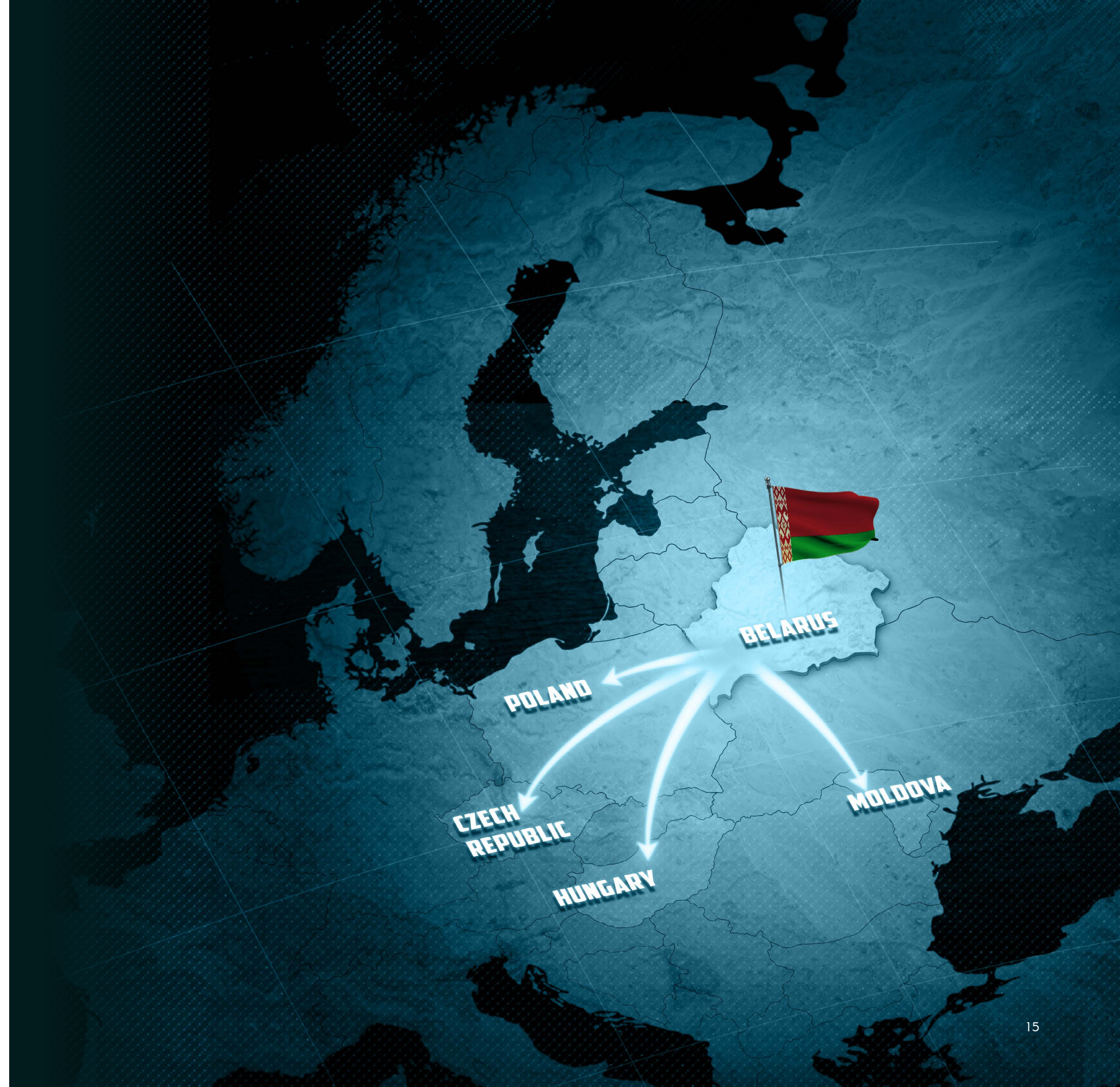
Given that operating directly within the territory of the Czech Republic has not been convenient for Russian influence actors since 2022, they pursued contacts with representatives of Czech politics, as well as the activist and media scenes, in 2025 primarily within the territory of Russia or suitable third countries, both outside and within the EU. Among these individuals were also the organizers of public events commemorating the role of the USSR in the liberation of Czechoslovakia from Nazism, which took place as part of the celebrations for the 80th anniversary of the end of World War II in May 2025.

The influence network managed by the former Ukrainian oligarch Viktor Medvedchuk (and following up on the sanctioned media outlet Voice of Europe) continues to focus primarily on building and strengthening connections with selected Members of the European Parliament (including Czech ones).

| Intelligence Services of Belarus

The intelligence operations of the Belarusian intelligence services focus primarily on combating exile opposition forces; however, given the close ties of the local political regime to the Kremlin, they can also be utilized to gather information that is useful for the intelligence work of Russian intelligence services.

In 2025, an operation by the Belarusian intelligence service (KDB) that threatened the security and interests of Poland, the Czech Republic, Hungary, and Moldova was uncovered in cooperation with partner services. A group of KDB officers maintained intelligence contacts with agents operating in Poland and Moldova. In connection with the uncovering of this operation, two individuals were detained on suspicion of espionage, three KDB officers were expelled (including one operating under diplomatic cover in the Czech Republic), and an additional four KDB officers were issued a ban on entering the Schengen Area.





MAIN IMPORTER OF GOODS
TO THE RUSSIAN FEDERATION
FOR 2025

Proliferation networks

The methods by which Russia acquired goods subject to EU restrictive measures in 2025 were similar to those in previous years. Russia attempted to obtain the required goods from the Czech Republic primarily via re-exports through third countries. Most of the cases handled involved Czech manufacturers who had strong business ties to Russia in past years. In the case of trading companies involved in brokering supplies to Russia, these were often entities controlled by Russian citizens, or by citizens of former USSR countries.

A key tool to restrict the supply of items exploitable in the Russian security industry was the utilization of EU restrictive measures (sanctions). Their primary purpose is not to impose repression – on the contrary, they are preventive measures aimed at preventing or stopping the undesirable behavior of individuals or companies. Alongside the ongoing expansion of sanctions and sanctions lists, the enforcement of already adopted sanctions is particularly essential. From this perspective, it was significant that in 2025, Czech institutions involved in the licensing and permitting process succeeded in pushing through specific measures at the EU-wide level to enable more effective compliance with sanctions. Although Russian companies have long been striving to do so, they have not yet rid themselves of their dependence on certain Western technologies. The existence of sanctions makes it more difficult and expensive for Russia to access technologies that it essentially needs to ensure the functionality of its military-industrial complex. As a result of the sanctions, Russian entities were forced to acquire the required goods through increasingly complex routes, with goods from the Czech Republic being supplied via re-exports through multiple intermediaries from third countries. More complex supply chains led to longer delivery times and the involvement of more entities, which can be expected to increase the price for the end users.



Example of the route/re-export of goods through third countries to the Russian Federation:

Even in 2025, Russia was in demand for CNC machine tools, which it needs to increase the production capacities of its armaments factories, including spare parts for the maintenance and servicing of machines supplied in the past. These demands also concerned the Czech Republic, which historically had a significant trade exchange with Russia in the field of engineering, and Czech manufacturers were important suppliers for Russian armaments factories as well. Other high-risk demands recorded in the Czech Republic concerned aircraft spare parts, electronic components, or various types of bearings. Cases of supplies of firearms and ammunition to the civilian markets of the member states of the Eurasian Economic Union, which are in a customs union with the Russian Federation allowing the free movement of goods and services, were also associated with the risk of re-export to Russia.

In 2025, the BIS paid attention not only to cases of supplies for Russian conventional military programs, but also to cases of supplies for entities involved in Russian programs for the development and production of weapons of mass destruction. Specifically, this included, for example, demands or equipment for chemical, biochemical, and molecular biological laboratories.

China continues to play a key role in supporting the Russian military-industrial complex, supplying Russia with components for the production of its weapon systems. Supplies of such goods from the Czech Republic to China were therefore associated with the risk of re-export to Russia.

The risk of supplying technologies of Czech origin to Russia was also associated with the operations of Czech manufacturers in joint ventures with foreign partners in third countries. For example, transfers of manufacturing technologies (including relevant design and manufacturing documentation) from the Czech Republic to these joint ventures in countries that continue commercial cooperation with Russia were recorded.



Cyberattacks

| Russian Actors

Cyber threat actors linked to the Russian state and its intelligence services remained active in the Czech Republic in 2025. Cyberattacks on Czech entities were often part of broader campaigns targeting other countries as well, and they continued to primarily involve the exploitation of technical vulnerabilities (in both hardware and software products or communication protocols), human error (social engineering), or flaws in the design of various authentication mechanisms. Russian cyber actors also continued to utilize domestic information or internet infrastructure to launch attacks on targets outside the Czech Republic.

In May 2025, the U.S. National Security Agency published a Joint Cyber Security Advisory, which the BIS helped prepare. The technical analysis, titled Russian GRU Targeting Western Logistic and Technology Companies, described the techniques and tactics used in previous years by the actor APT28, which is linked to the Russian intelligence service GRU.

Other actors with ties to the Russian state are the so-called hacktivist groups. Their most frequent activity consists of low-sophistication and relatively harmless cyberattacks of the DDoS type. These commonplace attacks on Czech entities have appeared repeatedly since the launch of the Russian invasion of Ukraine in 2022. In recent years, they have been accompanied by opportunistic attacks on unsecured or inadequately secured local technical operations, where the attacker alters system parameters (e.g., pumps, boilers, etc.). Although the compromised systems in domestic cases underwent an automatic safety shutdown, there are foreign cases where equipment damage actually occurred. Another type of targeted devices includes IP cameras, including those located in households.

Russian „hacktivists“ are not organic, loose collectives acting on shared beliefs; rather, they operate as extensions of Russian state power.

Although their role primarily lies in gaining attention for Russia's hybrid operations in the media space, their repeated attacks cause damages that—while small in individual cases along with the inconvenience—amount to a non-negligible total.

Security of Small Industrial Systems

Even the smallest technical operations with remote access or remote management capabilities—such as small hydroelectric power plants, pumps, heating systems, IP cameras, etc.—require adequate cybersecurity. To increase their resilience against cyberattacks, it is sufficient to adhere to standard principles:

- Always change the default password set by the manufacturer
- Use unique and complex passwords
- Enable two-factor authentication for all user accounts
- Secure connectivity – VPN, blocking unused ports, or IP whitelisting
- For remote management, set up user accounts with the lowest necessary privileges (e.g., read-only privileges for monitoring purposes only)
- Regularly update firmware and software
- Regularly check for vulnerabilities
- Consider replacing an obsolete product that is no longer supported by the manufacturer with a current version

| Chinese Actors

The Czech Republic, and particularly the field of Czech diplomacy, are long-standing and regular targets of cyber espionage attacks by Chinese state actors. This remained the case last year, when entities in the Czech Republic faced several cyberattacks by actors linked to China.

However, the year 2025 marked a significant milestone for the Czech Republic in the area of cyber threats, as it saw the first-ever public political attribution of a cyberattack targeting a Czech institution to a state cyber actor of a specific country. On May 28, 2025, the national attribution process concluded with the public attribution of a cyberattack on the Ministry of Foreign Affairs of the Czech Republic (MFA) to the People's Republic of China, specifically to the cyber actor APT31, which is linked to the Chinese intelligence service, the Ministry of State Security.

The attack in question primarily targeted the acquisition of information of interest to China. The incident affected the unclassified network of the MFA, lasted from at least 2022, and ended in July 2024 with the implementation of necessary mitigation countermeasures. Czech security institutions, together with the National Cyber and Information Security Agency, were able to determine responsibility for the attack with a high degree of certainty. The Czech public attribution of the attack on the MFA was supported not only by statements from the EU and NATO, but also by other allied states.

China's activities in the Czech Republic

Members of Chinese intelligence services have long been active within the territory of the Czech Republic, operating primarily under journalistic and diplomatic cover. Their main tasks include conventional intelligence gathering on the ground, creating networks of influence and contact, identifying persons of interest, and monitoring the Chinese diaspora community. Chinese intelligence interests are consistently dominated by the political intelligence line, where the primary objective is to seek out sympathizers (across all political parties) who would support a closer relationship between the Czech Republic and China, provide non-public information (even if unwittingly), promote China's interests, and suppress Czech-Taiwanese cooperation, which is undesirable to Beijing.

A so-called whole-of-society approach is utilized for information gathering, where, in addition to intelligence officers, the diplomatic mission, the Chinese diaspora community, and party organizations are also involved, operating both from within the territory of the Czech Republic and from abroad.

Chinese citizen Yang Yiming, who was identified as a member of a Chinese intelligence service, had been active in the Czech Republic since 2022. He utilized the cover of a journalist for a Chinese periodical, which represents a traditional cover tool used by Chinese intelligence services. During his time in the Czech Republic, Yang Yiming established a diversified network of sources through which he gained access to sensitive and non-public information from the environment of Czech state institutions. Given the topics he was interested in as part of his analyses, his activities were directed against the interests of the Czech Republic.

The academic sphere represents a valuable source of information of interest and contacts for China. China utilizes selected Czech academics to obtain sensitive information and to gain a better understanding of the Czech environment. The process of recruiting Czech citizens usually begins with identifying a suitable candidate who will have access to useful information. Individuals are often approached during their study stays in China, through the professional social network LinkedIn, or directly in the Czech Republic by members or collaborators of Chinese intelligence services. Under the pretext of establishing professional cooperation and with the promise of financial reward, the Chinese side offers cooperation to the contacted academics, most often consisting of writing analyses on assigned topics corresponding to Chinese political interests. These analyses serve as a stepping stone to further cooperation, during which demands for the delivery of

sensitive and non-public information escalate. The goal is, among other things, to obtain compromising information that can be further misused against individuals whom the Chinese side considers undesirable.

China strives to suppress activities associated with the so-called „five poisons,” particularly regarding Taiwan and Tibet, which are among the most important pillars of the political agenda of the Communist Party of China. These topics are perceived as an internal Chinese matter that must be under the control of Chinese authorities at all costs—both within Chinese territory and abroad. Consequently, the attention of the Chinese side is traditionally drawn to various conferences whose focus touches upon the „five poisons,” for example. China seeks to obtain information about the participants or the content of such events in order to prevent damage to its carefully cultivated positive image. Information about Chinese citizens can be further utilized by Chinese repressive bodies, including for forced repatriation or coerced cooperation.

For China, its image before both domestic audiences and foreign partners is important, which is why it continuously and over the long term strives to suppress any news that damages this cultivated image of a hegemon promoting global peace and order. Throughout 2025, we could thus observe the continuation of cooperation between the Czech and Chinese media scenes, involving the distribution of Chinese content primarily to smaller Czech media outlets. The recorded Chinese media contributions serve to influence the perception of China by the Czech public and attempt to depict only the positive side of the communist regime, while negative aspects—such as the trampling of human rights, the oppression of ethnic minorities, or territorial aggression—are deliberately omitted entirely or denied.

Regarding reactions to legislative restrictions both in the Czech Republic and abroad and the subsequent measures, Chinese entities, and by extension the Chinese administration, have been utilizing a more or less uniform system of procedures and tools over the past few years. This primarily involves intensive intelligence gathering concerning the relevant institutions and bodies, reaching out to influential managers, lobbyists, or politicians, and a subsequent pressure strategy directed against individual state authorities of the countries involved, as well as efforts to secure support within the European Commission.



Energy security and protection of public finances

| Energy Lobby

The BIS has long observed lobbying in the area of protecting significant economic interests, particularly in the energy sector, by certain private companies that covertly assert their own interests using contacts within the state administration. Although such conduct did occur in some cases over the past period, the year 2025 was generally characterized by a decline in illegitimate lobbying. However, the reason for this is not a change in the behavior of the entities involved, but rather the fact that as the end of the term of office for the Chamber of Deputies of the Parliament of the Czech Republic approached, the potential to successfully push through any legislative proposals dropped sharply.

Given that the main actors have not changed their intentions, it is highly probable that intensive lobbying will resume in the subsequent period. If the state administration is not adequately prepared to face these challenges—meaning that supervisory and regulatory bodies are not sufficiently supported in terms of capacity, expertise, and finance—it could ultimately have a further negative impact on energy prices. For this reason as well, the BIS has focused in recent years in this area primarily on identifying phenomena that adversely affect the prices of energy commodities.

| Public Procurement

Another area with a significant impact on public finances is public procurement. The BIS has documented a whole range of methods used to influence the public procurement process, based on specific cases across various sectors of the economy (energy, healthcare, transport, agriculture, etc.).

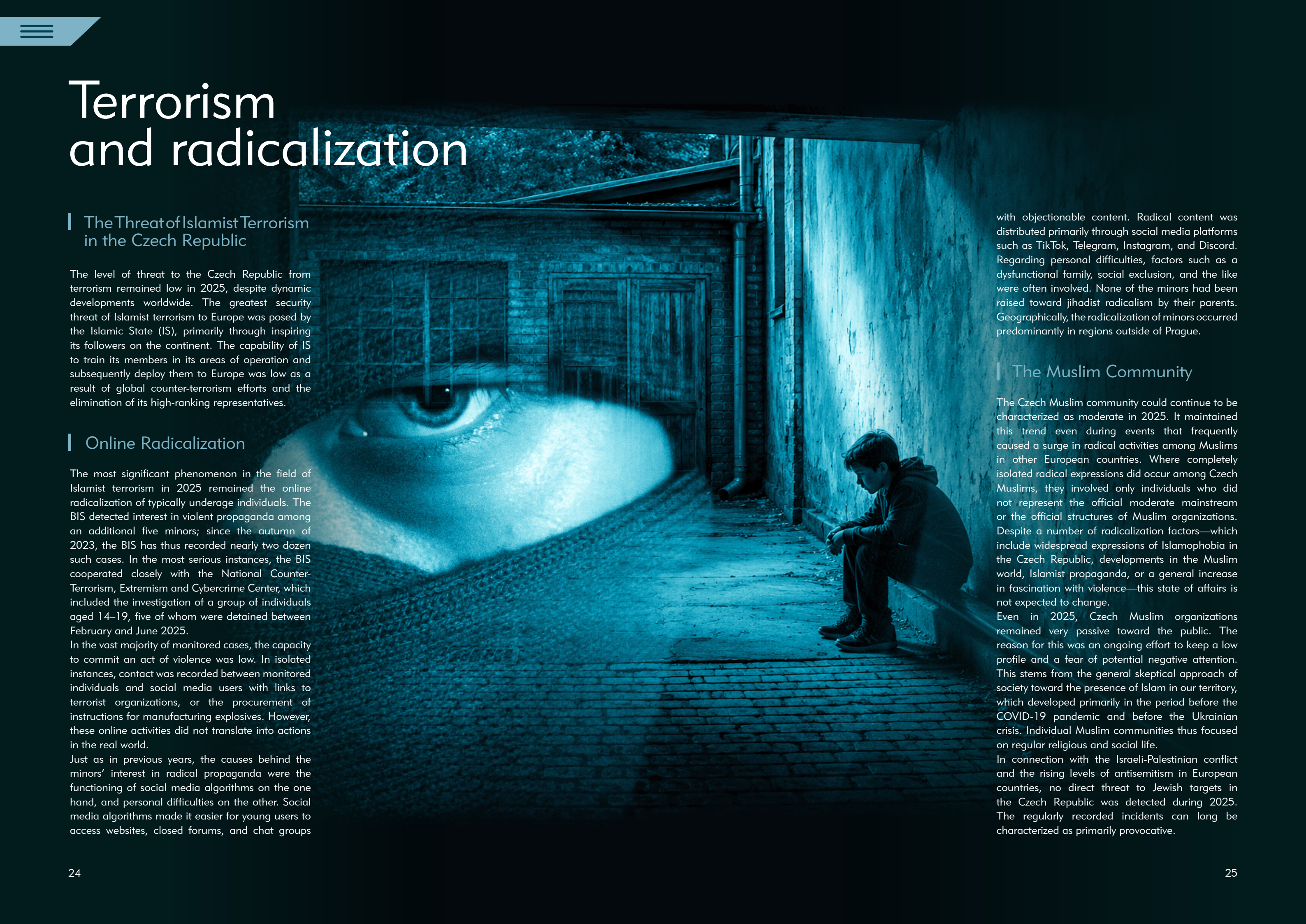
A common element was usually the effort to secure the execution of contracts for preferred suppliers or subcontractors. There were attempts to bypass public bidding, to tailor tender specifications in a way that disadvantaged or directly disqualified other potential suppliers, or to inflate the prices of specific products. The supplier selection process was also accompanied by various forms of conflicts of interest,

close ties between state institution officials and supplier representatives, procurement of redundant services, mutual coordination among bidders, or the involvement of additional subcontractors whose actual contribution to the performance of the public contract was under serious doubt. The circumstances surrounding some contracts also pointed to efforts to siphon off financial resources on a large scale.

| Clientelism

The system of favoring selected business partners is often closely linked to above-standard relationships with representatives of state-controlled entities. In some institutions, it has long been firmly embedded and built on mutual benefit. This benefit does not necessarily have to consist of financial compensation, but rather serves to build a network of contacts and ties of influence that help the state representatives involved remain in their positions or secure future employment. Such individuals then remain in their positions for multiple terms, further strengthening the established system. These officials often act within their organizations as completely autonomous rulers, leading to the suppression of the control functions of supervisory bodies. The latter are often inadequately and deceptively informed about developments in state-owned companies, and not infrequently the roles of the supervisors and the supervised are reversed, with the latter effectively forcing compliance from members of the supervisory boards.

The inadequate flow of information to supervisory bodies in certain state-controlled entities even extended to matters as fundamental as the actual state of financial management. For instance, representatives of a specific entity had long artificially inflated economic results, meaning the actual situation did not correspond to the data presented to members of the supervisory board. In another case, officials of a state institution failed to report the consequences of an ongoing financial situation which, among other things, posed a risk of restricting options to secure further sources of financing.



Terrorism and radicalization

| The Threat of Islamist Terrorism in the Czech Republic

The level of threat to the Czech Republic from terrorism remained low in 2025, despite dynamic developments worldwide. The greatest security threat of Islamist terrorism to Europe was posed by the Islamic State (IS), primarily through inspiring its followers on the continent. The capability of IS to train its members in its areas of operation and subsequently deploy them to Europe was low as a result of global counter-terrorism efforts and the elimination of its high-ranking representatives.

| Online Radicalization

The most significant phenomenon in the field of Islamist terrorism in 2025 remained the online radicalization of typically underage individuals. The BIS detected interest in violent propaganda among an additional five minors; since the autumn of 2023, the BIS has thus recorded nearly two dozen such cases. In the most serious instances, the BIS cooperated closely with the National Counter-Terrorism, Extremism and Cybercrime Center, which included the investigation of a group of individuals aged 14–19, five of whom were detained between February and June 2025.

In the vast majority of monitored cases, the capacity to commit an act of violence was low. In isolated instances, contact was recorded between monitored individuals and social media users with links to terrorist organizations, or the procurement of instructions for manufacturing explosives. However, these online activities did not translate into actions in the real world.

Just as in previous years, the causes behind the minors' interest in radical propaganda were the functioning of social media algorithms on the one hand, and personal difficulties on the other. Social media algorithms made it easier for young users to access websites, closed forums, and chat groups

with objectionable content. Radical content was distributed primarily through social media platforms such as TikTok, Telegram, Instagram, and Discord. Regarding personal difficulties, factors such as a dysfunctional family, social exclusion, and the like were often involved. None of the minors had been raised toward jihadist radicalism by their parents. Geographically, the radicalization of minors occurred predominantly in regions outside of Prague.

| The Muslim Community

The Czech Muslim community could continue to be characterized as moderate in 2025. It maintained this trend even during events that frequently caused a surge in radical activities among Muslims in other European countries. Where completely isolated radical expressions did occur among Czech Muslims, they involved only individuals who did not represent the official moderate mainstream or the official structures of Muslim organizations. Despite a number of radicalization factors—which include widespread expressions of Islamophobia in the Czech Republic, developments in the Muslim world, Islamist propaganda, or a general increase in fascination with violence—this state of affairs is not expected to change.

Even in 2025, Czech Muslim organizations remained very passive toward the public. The reason for this was an ongoing effort to keep a low profile and a fear of potential negative attention. This stems from the general skeptical approach of society toward the presence of Islam in our territory, which developed primarily in the period before the COVID-19 pandemic and before the Ukrainian crisis. Individual Muslim communities thus focused on regular religious and social life.

In connection with the Israeli-Palestinian conflict and the rising levels of antisemitism in European countries, no direct threat to Jewish targets in the Czech Republic was detected during 2025. The regularly recorded incidents can long be characterized as primarily provocative.

| Iran and its Allies

In 2025, Iran continued its strategy of cooperation with European criminal networks, utilizing their members to carry out individual attacks against alleged enemies of the country living in Europe—specifically from the ranks of Iranian opposition, Israeli, or Jewish entities. Threats from Iran, further amplified by the armed conflict between Iran and the State of Israel with US involvement in June 2025, were directed to varying degrees against most European states, and marginally also against the Czech Republic.

Among the sought-after targets of the Iranian regime in Europe are also Iranian opposition journalists. In this context, cases were recorded in the Czech Republic of individuals who were intimidated by Iran due to their opposition journalistic activities.

In general (in relation to the Czech Republic), the activities of Iran and its proxy groups in 2025 can be described as low-profile. The Shia community in the Czech Republic remained moderate in 2025 as well, with some Iranians even demonstrating public criticism of the regime in their country of origin.



Protection of the democratic foundations of the state

| Foreign Power Information Operations

The information isolation continues for that segment of Czech society which has accepted channels producing disinformation and conspiracies as their regular source of information on public affairs. This not only leaves them vulnerable to foreign power influence operations, but also increases the risk of sporadic radicalization among their individual members.

Within this isolation, websites spreading disinformation, conspiracies, and hateful content continue to play a significant role. They form an interconnected ecosystem and cross-reference one another, which, among other things, creates a false impression of mutual validation for the published stories and locks their readers into an alternative version of reality. In many cases, these websites consistently conceal their operational and creative backgrounds (an absence of sources under published articles, the use of fake author names, and non-public editorial teams and management). The non-transparent nature of how some of these websites operate is further heightened by the use of cryptocurrencies or otherwise concealed forms of financing or ownership structures based on a system of „straw men” (nominees). The typology of these web portals varies—some function as aggregators of texts published elsewhere (including adopting content directly from Russian sources that are subject to sanctions within the EU), while others serve as sources for the rest and fabricate selected disinformation themselves, primarily for financial profit.

Although the spread of disinformation in the Czech environment can still be perceived as predominantly the activity of domestic actors—whose motivation is primarily financial, ideological, or driven by their political ambition—the interest of foreign powers, namely Russia and China, in individual actors on the disinformation scene persisted in 2025 and, in some cases, escalated into support or even direct

cooperation. A foreign power considers it a success if it manages to get its influenced output or its proffered narrative into the mainstream, whether through the media or selected opinion makers (politicians, journalists, influencers).

For instance, in the past, Chinese state media companies provided a selected disinformation producer with a regular monthly income in this manner (ranging from low tens of thousands to low hundreds of thousands of CZK). The purpose of such support may not only be to commission specific content, but also to financially stabilize the disinformation project or to provide general support for aggressive stances that attack the Czech Republic as part of the collective West, the EU, and NATO.

The Russian side required its cooperating producers to report their reach (how many articles were placed on how many websites per month) or, as the case may be, instructed them to share specific pieces of disinformation. Anti-system political communication and pro-Russian propaganda often blend together. In 2025, information channels directly linked to the Russian state apparatus remained active, most notably the successors to the Sputnik media outlet (namely the website 42tcen.com and the Telegram channel neČT24, which share personnel ties with Sputnik). Components of the Russian apparatus responsible for information and influence operations, or their collaborators, always look to secure contacts and interviews with domestic politicians from the target country who support pro-Kremlin stances and contextualize them for the local audience; in this regard, Russia was partially successful with marginal segments of the Czech political spectrum. As demonstrated by the Voice of Europe case, collaboration on propaganda efforts can serve as a stepping stone for more complex intelligence operations, and the initial utilization of interview offers or participation in discussions is typical of Russian influence operations.



| 2025 Elections

The BIS did not record any serious disruption to the course of the elections or any threat to their legitimacy. Particularly at the beginning of the election campaign, various narratives associated with new voting elements, most notably postal voting, resonated significantly. However, these gradually subsided in connection with information showing that the numbers of voters abroad intending to use this option were substantially lower than originally anticipated.

As part of its election protection efforts, the BIS also monitored, for example, the activity of an inauthentic network on the TikTok platform that was spreading anti-system and pro-Russian narratives aimed at the Czech audience. This network had been built up over the long term, and its individual accounts, most of which could be characterized as fake, were interconnected both through mutual following and through the sharing (reposting) of objectionable content. The goal of this interconnection was likely to increase the reach of the published and shared topics. The BIS evaluates the intensity of the interconnection as artificially created, which supports the hypothesis that the network's goal was to manipulate the algorithm to increase the impact of the disseminated content and secure its breakthrough to a real audience.

Content consisting of pro-Russian and socially polarizing narratives that is spread and artificially boosted by inauthentic profiles corresponds to the Russian *modus operandi* and serves to advance Russian interests in the Czech Republic. According to the assessment of the BIS, the recorded case on the TikTok platform had no relevant impact on the results of the parliamentary elections in the Czech Republic.

Interconnection within a representative sample of analyzed TikTok accounts (the size of the node signifies importance, i.e., the number of connections of individual accounts within the monitored sample):

| Left-Wing Extremism

The dominant theme of the generally moderate left-wing activist scene throughout 2025 remained the Israeli-Palestinian conflict and its global repercussions, which completely overshadowed the traditional climate issue.

In previous years, the topic of the Israeli-Palestinian conflict had already been entirely dominated in the public space by left-wing activists. A new phenomenon in 2025, however, was the unsolicited and often poorly received injection of the anti-Israeli theme into events not directly related to the Palestinian question, such as Prague Pride or the election campaign ahead of the parliamentary elections.

The core of anti-Israeli activities was maintained primarily within the academic environment and on social networks. Here, as the conflict continued, an increase in anti-Israeli verbal aggression occurred. Most notably on social networks, the flying of Palestinian flags at many faculties of Czech universities resonated significantly, particularly as it was deliberately and insensitively timed to coincide with the anniversary of the Hamas attack on the Israeli festival on October 7, 2023.

| Right-Wing Extremism

The Czech right-wing extremist scene as a whole does not currently pose a direct risk to state security. Although right-wing extremist ideas continue to resonate among certain small groups or individuals, their approach lacks systemic organization and is rather superficial and selective.

Over the years, the scene has split into two primary groups. The first, and currently more dangerous group, consists of very young individuals, with social networks (Discord, Telegram, etc.) serving as the dominant space for their activities. Here, they gradually gather various, often highly expressive extremist materials, particularly of a violent nature, whether purposefully or through algorithms. They then disseminate these materials further, while simultaneously using them to establish contacts with like-minded individuals. They often maintain only online communication with them, while real-world encounters occur rather infrequently.

The second group consists of individuals who are influenced by „traditional” right-wing extremism. This primarily involves older individuals who have pre-existing social ties with other extremists. These individuals have practically ceased political activism and focus mainly on various recreational activities, such as boxing or MMA tournaments, or right-wing extremist music events both in the Czech Republic and abroad.

| Paramilitaries

Only a few dozen people, mostly of older age, were actively involved in the Czech paramilitary environment in 2025, focusing primarily on paramilitary training (marksmanship, first aid, etc.). Practically all of their activities were relatively stereotypical in nature, lacking new impulses or innovations.

It can be assumed that the paramilitary movement in the Czech Republic has already passed its zenith, and its mobilization potential will gradually decrease significantly. Consequently, the primary danger associated with the existence of the paramilitary scene will not stem from the activities of paramilitaries as a whole, but rather from the individual actions of certain, most radicalized individuals from this environment.



Cooperation at the national level

| Czech Intelligence Services

Alongside the standard exchange of intelligence, cooperation with the Office for Foreign Relations and Information (ÚZSI) and Military Intelligence consisted primarily of vetting applicants for short-term Schengen visas. In this process, the BIS serves as the guarantor for the Czech intelligence services and subsequently passes the final standpoint to the Police of the Czech Republic.

Another form of cooperation with the ÚZSI involved vetting individuals applying for accreditation as a diplomatic representative or a member of a diplomatic mission operating within the territory of the Czech Republic. The number of vetted diplomats in 2025 was nearly identical to the previous year, with 114 diplomats and 40 family members vetted.

| National Security Authority

The BIS cooperates very closely with the National Security Authority (NBÚ) – specifically, it acquires, gathers, and evaluates information within its competence required for the NBÚ's decision-making in security clearance proceedings conducted under Act No. 412/2005 Coll. This involves relevant intelligence concerning holders of a clearance or certificate, or applicants for the issuance of a clearance or certificate. The scope of the procedures performed varies depending on the type of certificate the participant is applying for (a security clearance allowing access to classified information or a certificate of security competence) and the level of classified information to which the participant in the proceedings is to be granted access.





| The Police of the Czech Republic | Ministry of the Interior

Highly successful cooperation and a regular exchange of information took place with a number of units of the Police of the Czech Republic – in particular with the National Organized Crime Agency and the National Center Against Terrorism, Extremism, and Cybercrime.

In 2025, the BIS also cooperated intensively with the Directorate of the Foreign Police Service (ŘSCP), primarily on vetting applicants for short-term Schengen visas. Approximately two million visa applications were vetted, which is nearly the same number as in the previous year.

Furthermore, in cooperation with the ŘSCP, the BIS participated in vetting applicants for a reliability certificate under the Civil Aviation Act. Holders of this certificate are permitted to enter restricted security areas at airports. The BIS, in cooperation with the ŘSCP, assesses the so-called trustworthiness of the individual. In 2025, nearly 24,000 individuals were vetted, representing an increase of approximately 4,000 people compared to 2024.

The cooperation between the BIS and the Ministry of the Interior of the Czech Republic continued in assessing the security risks of foreigners applying for international protection, residence permits, and the granting of Czech citizenship. In connection with applications for the granting or extension of international protection, the BIS vetted nearly 800 applicants in 2025. Vetting also continued for legal and physical entities applying for employment brokerage permits, as well as for individuals requesting permission to join the Armed Forces of Ukraine.

In 2025, the BIS vetted nearly 158,000 individuals over the age of 15 applying for residence permits under the Act on the Residence of Foreigners. In terms of the requested types of residence, a long-term residence permit for the purpose of employment remains the most requested by default (accounting for 40% of the total number of vetted individuals). During the vetting of residence permit applicants, the BIS submitted information regarding a few dozen individuals to the proceedings. In terms of specific security areas, this primarily involved information from the fields of countering scientific and technological espionage, cooperation with a foreign power, or supporting Russian influence within our territory, and in two cases, the area of terrorism. The granting and extension of temporary protection also continued in 2025. The number of temporary protection applicants vetted by the BIS in 2025 was approximately 350,000 (individuals over the age of 15). Compared to previous years (2023 – 303,000; 2024 – 327,000), this represents another increase, confirming the sustained interest in temporary protection granted in the Czech Republic.

In 2025, within the framework of vetting individuals applying for Czech citizenship, the BIS issued assessments for more than 6,800 applicants. The slight increase in the number of applicants compared to the previous year is likely a result of the long-term trend of an increasing number of applicants for Czech citizenship.

| Ministry of Foreign Affairs

In 2025, the BIS vetted nearly 700 entities (both physical individuals and legal entities) applying for cooperation with the Ministry of Foreign Affairs (MZV). In the majority of cases, these were physical individuals, such as applicants for internships, local staff at embassies, and applicants for journalist accreditation granted by the MZV.

A significant segment of cooperation with the MZV was also the area of international sanctions, particularly in connection with EU restrictive measures and the listing of entities on the national sanctions list.

| Ministry of Industry and Trade

In 2025, the cooperation between the BIS and the Ministry of Industry and Trade of the Czech Republic on screening foreign investments continued. In this year, the BIS participated in screening the largest volume of foreign investment cases since the Act on Foreign Investment Screening came into effect, i.e., since 2021. However, 2025 was exceptional in the field of foreign investment screening not only due to the number of cases, but also because of the first issued prohibition. In 2025, the continued existence of an investment by a Chinese company into a ground satellite station was prohibited.

| Digital and Information Agency

The BIS cooperates with the Digital and Information Agency (DIA) on vetting cloud computing providers for public administration bodies. In 2025, the BIS received a total of 40 requests to vet applicants for entry into the cloud computing catalog maintained by the DIA. Another form of cooperation with the DIA involves vetting applicants for the issuance of accreditation to manage a qualified electronic identification system. In 2025, the BIS received no requests for this type of vetting.



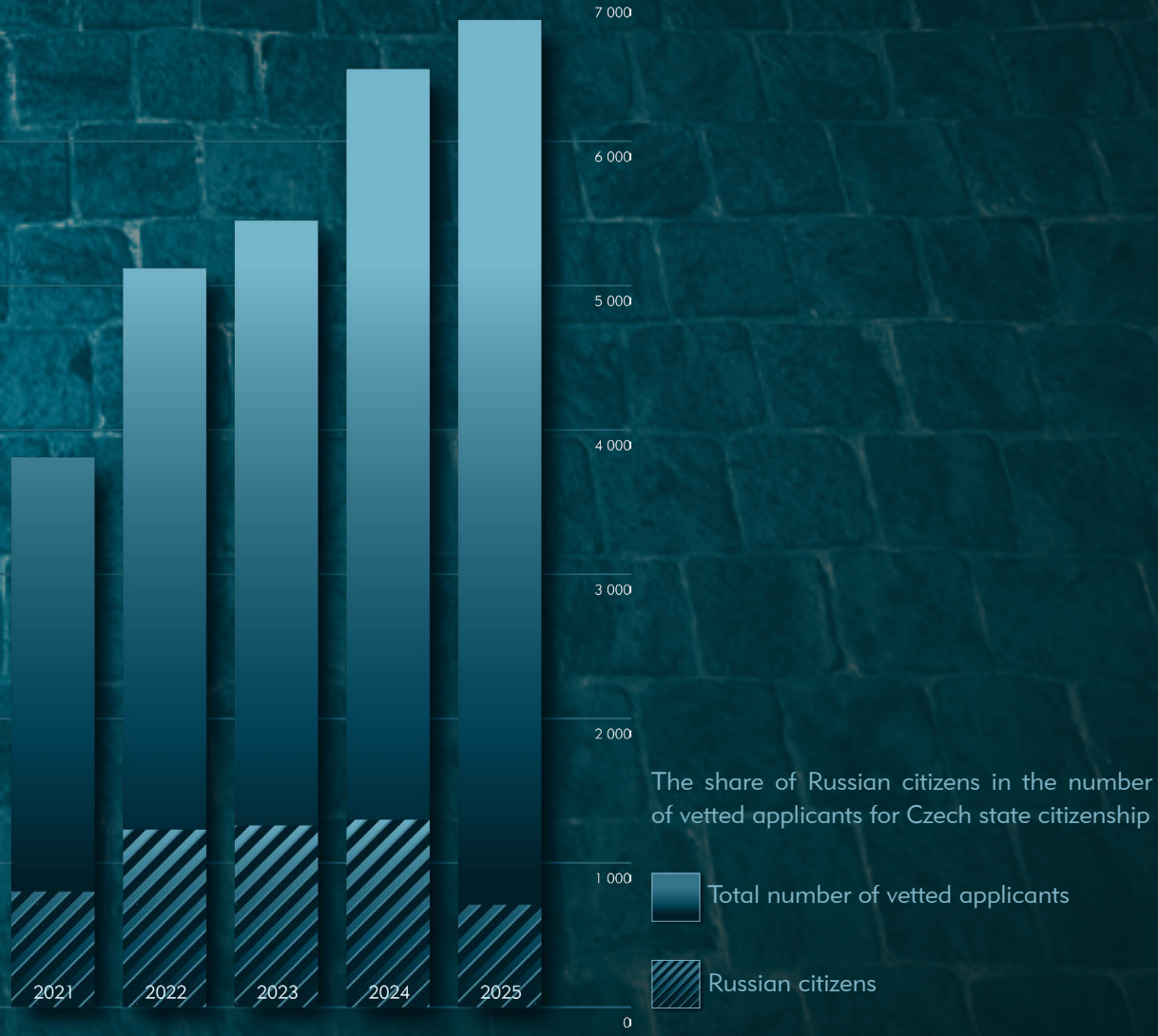
Measures Restricting Russian Influence

In the area of visa policy, a significant element leading to the restriction of Russian influence in the Czech Republic in 2025 remained the opportunity to provide assessments on visa applications submitted by citizens of the Russian Federation at the embassies of other Schengen Area states. This measure fundamentally reduces the security threat posed by the movement of Russian intelligence officers within Schengen Area countries. In 2025, the BIS vetted approximately 630,000 applications from Russian nationals, including both applications submitted at Czech embassies and those submitted at the embassies of other member states.

The Czech Republic has applied a strict visa policy toward Russia since the beginning of the conflict; the number of applications submitted by Russian citizens at Czech embassies has been very low for several years and decreases slightly each year. In 2025, over 200 applications for short-term Schengen

visas submitted by Russian nationals at Czech embassies were vetted. However, the total number of applications submitted by this group of individuals across the entire Schengen Area shows an increasing trend. This is due to the inconsistent approach of member states toward applicants of Russian nationality, as some states have not tightened their visa policy toward Russia even after the outbreak of the conflict and continue to issue Schengen visas to Russian nationals without major restrictions.

In 2025, a decline was also observed in the number of citizens of the Russian Federation (RF) among applicants for Czech citizenship, caused by an amendment to Act No. 65/2022 Coll., which significantly restricted this group of individuals from acquiring Czech citizenship. The law was adopted as a consequence of the ongoing military conflict in Ukraine and the growing security risk posed by Russia.



Cooperation at the international level

COOPERATION AT THE INTERNATIONAL LEVEL

Cooperation with foreign intelligence services continued to play an irreplaceable role across numerous areas of the BIS's competence in 2025, fundamentally contributing to ensuring the security of the Czech Republic. Based on approval from the Czech Government, the BIS is authorized to cooperate with more than one hundred intelligence services from around the world. It develops information exchange and active contacts primarily with the intelligence services of EU and NATO member states.

The BIS also actively participated in the activities of a number of multilateral groupings. Cooperation with EU institutions also continued. A key outcome of the joint strategy with foreign partners from Schengen Area countries in 2025 was, for example, the tightening of visa rules for Russian diplomats.

The main areas of cooperation between the BIS and foreign intelligence services remain the fight against terrorism, counterintelligence, the proliferation of weapons of mass destruction and their delivery systems, cybersecurity, the protection of classified information, and the field of security competence.

Within the framework of international cooperation in 2025, the BIS received nearly 14,000 intelligence reports and forwarded over 2,400 documents. At the strategic and expert levels, BIS representatives participated in more than 1,000 international meetings.



Careers at the BIS

The BIS fulfills tasks and duties stipulated by law, but its true strength relies on specific people of various professions, expertise, and backgrounds. They all have one thing in common –

they have tied their professional careers to protecting the security interests of our republic.

At the BIS, we function as a complex and self-sufficient entity that manages most of its services internally. Intelligence activity is built primarily on the cooperation of case officers (operatives) and analysts. Case officers operate directly in environments of interest, establishing contacts and relationships to gather knowledge and information. Analysts then evaluate the acquired information, connect the dots, and create a comprehensive picture of the situation. Their colleagues, who secure the surveillance of targets and perform other necessary operations, also step into this entire process of gathering and linking information.

Within the BIS buildings themselves, operation is supported by a range of specialists whose work is essential for the intelligence service to fulfill its goals. This includes not only IT professionals, technicians, lawyers, security guards, and HR staff, but also psychologists, doctors, and other medical personnel. Due to the self-sufficiency of the BIS, you would also find a number of positions here that you might not expect, but which are vital for the smooth and stable running of the organization. These include colleagues working in facilities management, construction, and maintenance. Furthermore, colleagues from catering and cleaning services also contribute to a well-functioning and pleasant environment.

Without intelligence, specialized, and support professions, the intelligence service could not operate long-term and with good results. It is precisely from this mosaic that an effectively functioning whole is created, within which no expertise is left without a suitable application.

We recruit new colleagues throughout the entire year,

aiming to guide every job applicant precisely to where they can apply not only their education or past experience, but also their personality traits, abilities, and skills. Applicants without a specific expertise (or from fields entirely different from those mentioned) may also apply, provided they are interested in learning new things and care deeply about the security of our country. The selection of new colleagues is carried out with high diligence, allowing you to become part of an even more high-quality team.

Applicants interested in employment can send their CVs and cover letters to personal@bis.cz.



Public relations

The BIS views communication with the public as a component of the oversight of its activities, as well as a source of feedback and information. The primary goals of BIS communication are education and the managed building of trust between citizens and the intelligence service as one of the fundamental pillars of state security.

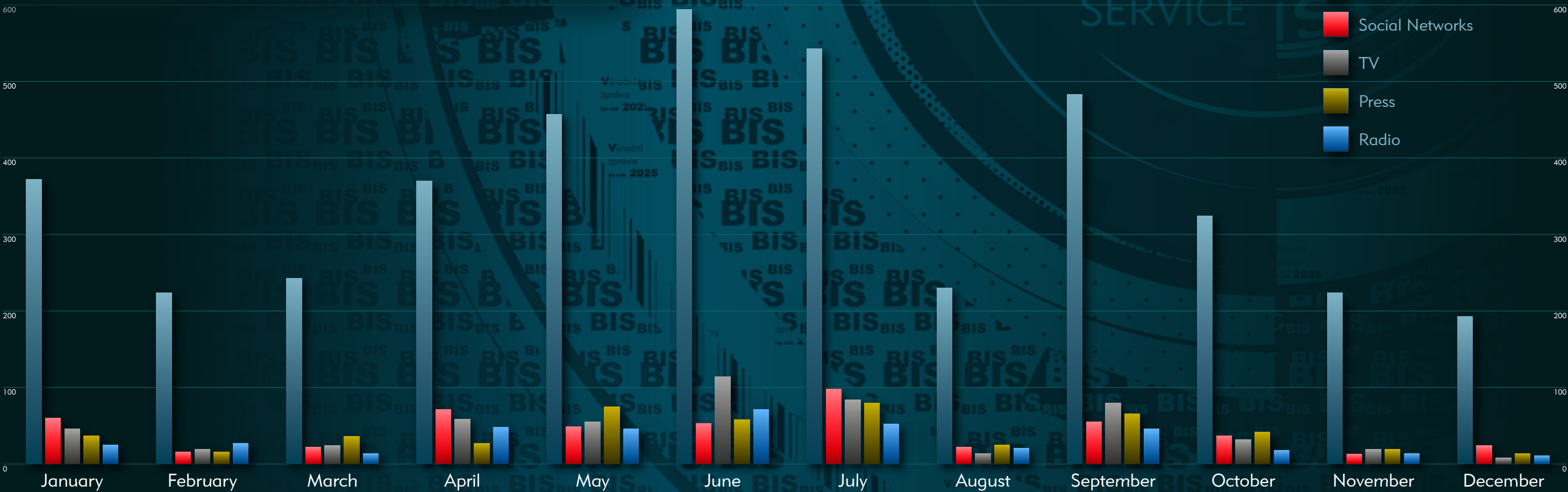
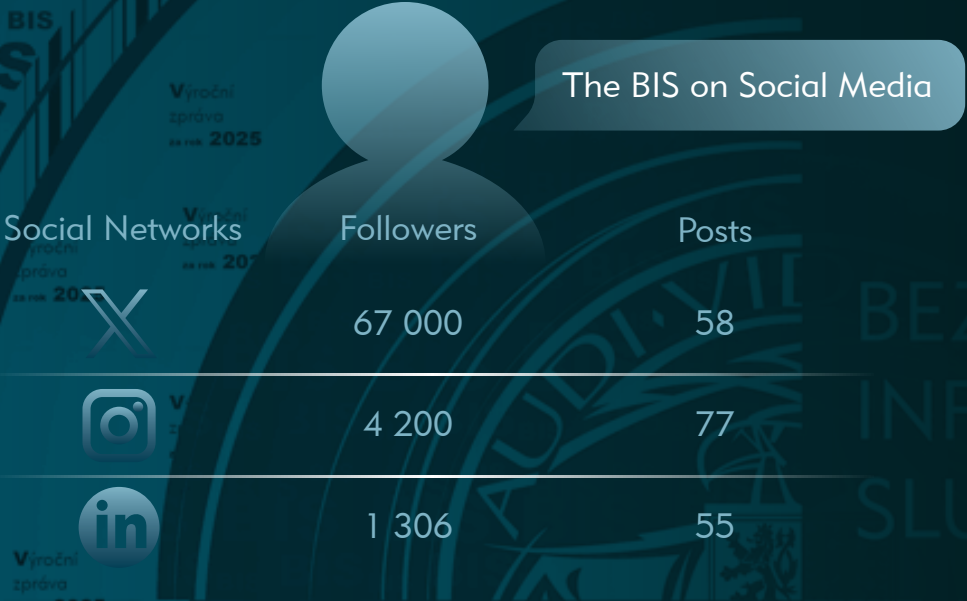
The main tools include direct communication with mass media representatives and providing information via the website www.bis.cz and the social networks Instagram, X, and LinkedIn. According to an analysis by the company Toxin, the BIS recorded a total of 6,219 media outputs across all media types in 2025.

The BIS also communicates directly with the public through its press spokesperson. This involves responding to incoming inquiries sent both electronically and by traditional mail. In 2025, a total of 1,137 inquiries from journalists, institutions, and citizens were handled in this manner.

Every year, there is a growing number of requests from educational institutions—ranging from secondary schools and grammar schools to

universities—for lectures on topics related to security and the actual activities of intelligence services. Through these lecture activities, the BIS successfully fulfills the educational component of its communication efforts, while these meetings with students can also lead some of them to consider connecting their future professional careers with the BIS. This high demand for lectures confirms the rising interest of the younger generation in security issues and shows that young people approach state defense topics very actively and responsibly. The internship program at the BIS for university students also continued in 2025.

The BIS also plays a significant role in training public administration officials, focusing on increasing their resilience to attempts at influence by foreign powers. The aim of this training is to raise the security awareness and capacity of state officials (beyond the scope of basic and periodic security training) so that graduates are able to identify security anomalies (i.e., increased interest in their person or work activities) in both their professional and personal lives, and know how to proceed in such cases.





Budget

The BIS budget for 2025 was established by Act No. 434/2024 Coll., on the State Budget of the Czech Republic for 2025. Revenues set by the budget chapter at CZK 290,000 thousand were fulfilled in the amount of CZK 309,011 thousand. Expenditures determined by the budget in the amount of CZK 2,368,430 thousand were executed in the amount of CZK 2,476,729 thousand, also with the contribution of the remaining claims from unspent expenditures that the BIS still had at its disposal.



BIS expenditures over the last five years (in thousands of CZK)

For capital expenditures, a significant discrepancy between identified needs and realistically available funds persisted in 2025 as well, which was the main limiting factor for progress in implementing certain key infrastructure and development projects. Consequently, as in previous years, investments regarding intelligence, information, and communication technology were postponed, as were investments in the construction sector, which were restricted to minor actions of a technical appreciation nature.

In 2025, capital expenditures were primarily directed towards the acquisition of software and licenses, software upgrades, the purchase of hardware and encryption devices, and intelligence data backup software. Expenditures in the construction sector focused mainly on modifications to low-voltage wiring, the installation of security system cabling, and similar projects. Furthermore, the renovation of offices and technical rooms continued.

Within the executed current expenditures, the most significant item consisted of personnel expenditures, i.e., expenditures on the service income of members including the stabilization allowance, which had not yet been applied in the BIS due to limited funds, and expenditures on the salaries of employees under employment contracts and their accessories. Another significant group of mandatory expenditures consists of social benefits, especially service pensions and severance pay, the provision of which is guaranteed to members by Act No. 361/2003 Coll., on the Service of Officers of the Security Forces.

The basic operational needs of the BIS were covered in 2025, even with the utilization of all claims from unspent expenditures. Priority was given to securing mandatory and quasi-mandatory expenditures; however, a number of strategic projects, particularly in the area of intelligence, information, and communication systems, were postponed. This strategy is not sustainable in the long term, as the BIS must not only renew and modernize its technical equipment at regular intervals, but also accelerate the development of its capabilities in response to the advancement of artificial intelligence and technological evolution.



Security Information Service
Annual Report 2025

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

