



SECURITY-INTELLIGENCE
AGENCY

PUBLIC REPORT 2025





MISSION

We detect, investigate and understand security threats and challenges by collecting and analysing intelligence significant for national security, thus providing the state leadership and other state bodies with reliable intelligence support in decision-making and act to protect Croatia's national security, interests and the well-being of its citizens.

VISION

A modern, efficient and responsible security and intelligence agency, suitable to requirements, focused on the accomplishment of its mission and achievement of top results, with significant national influence and impact, as well as regional reach, recognised by its developed capabilities, excellent employees and strong partner ties.

CONTENTS

Croatia is a safe and stable democracy in a challenging security environment	1
Global and European security environment is marked by complexity and uncertainty ...	3
Global terrorist organisations exploit complex geopolitical circumstances to rebuild their capacities and reach	6
Extremist ideas are most often promoted among young people and minors.....	8
Foreign intelligence activities targeting EU countries include espionage, sabotage and the instillation of fear	10
Cyber threats are on the rise, and comprehensive protective measures have been initiated	12
Croatia's economic security is influenced by global economic trends	15
SOA is working on locating persons missing from the Homeland War.....	17
The Western Balkans are still burdened by unresolved interethnic and interstate political-security issues	19
Organized crime from the Western Balkans is active in drug trafficking.....	24
Illegal migration remains intense under the influence of unstable global conditions	25
Through cooperation with international partners, SOA participates in safeguarding European security.....	26
SOA is the most significant body in Croatia's security and intelligence system in terms of scope of tasks.....	27
SOA continuously receives job applications and conducts candidate selection procedures.....	34



Croatia is a safe and stable democracy in a challenging security environment

Dear Sir/Madam,

A song by a Croatian punk-blues band reflects: “The world is narrowing; it is increasingly difficult to follow what is happening beyond the hill.” These lyrics may serve as an excellent illustration of the public perception of the security situation: general globalisation has led to a “narrowing of the world”, and every major security disturbance is felt everywhere. At the same time, numerous actors and interwoven processes in such a “narrowed world” contribute to the complexity and speed of developments, making it ever more demanding to recognise and encompass all the factors that influence events. For us in the Security and Intelligence Agency (SOA), the task is to timely identify, monitor, and understand the many processes in this “narrowed world” that affect national security, especially those unfolding away from the public eye, “beyond the hill.”

One of the most frequent asked questions to us is, how safe are we? Seemingly simple, but in fact an extremely complex question, since security is a variable and difficult-to-measure category, and assessments of security are very often the result of personal feeling and perception. Statistical data and surveys on the sense of personal security show that the Republic of Croatia is one of the safest countries in Europe.

In regards to national security that falls under the scope of SOA, there are currently no serious direct threats to national security or to the Croatian democratic constitutional order. However, overall security on the European continent has deteriorated in recent years, with numerous threats, challenges, and risks that may also impact Croatia’s national security. The most significant among them will be addressed in this public report.

Global security conditions are marked by extraordinary dynamics of change, a large number of interwoven processes, and consequent unpredictability. In such an environment of uncertainty and numerous possible scenarios, the role of security and intelligence agencies becomes even more important.

The task of SOA is to understand this complex system of security processes and to enable the state leadership to make decisions essential to the national security and interests. In doing so, SOA does not predict the future but acts as an early warning tool, pointing to trends, probabilities, and possible developments. To achieve this, SOA must have capability for timely collection of reliable data important for national security.

The consequences of the war in Ukraine are felt globally, and the geopolitical changes underway are the greatest since the end of the Cold War. Multilateral global security mechanisms built after the Second World War practically no longer exist. Under such circumstances, the European security architecture is also changing. The European Union (EU) member states are developing ambitious plans for defence cohesion and strengthening European defence capacities, while Sweden and Finland have abandoned their neutrality policy, seeking greater security within the North Atlantic Alliance. The need for significant investment in EU defence capacities is a consequence of decades of European reliance on the defence and security resources and

arrangements of the United States. At the same time, the EU is seeking to strengthen its economic and energy independence, as well as to preserve control over strategic industries and technologies.

There is dynamic shift taking place within the international order in the balance of political, military, and economic influence in various parts of the world, with particular emphasis on developments in the wider European, Middle Eastern, and Indo-Pacific regions.

Parallel to this, other complex political, economic, and technological processes are taking place, influencing the new security architecture being formed, as well as European and national security.

New technologies are changing all aspects of social life, creating unprecedented opportunities for economic growth and development, and we are witnessing technological competition between major global economies. In this competition, protective measures and tariffs are increasingly used, and the technological race is particularly significant in areas such as artificial intelligence and autonomous systems.

As has always been the case throughout history, new technologies demonstrate their impact also in the security and military fields, such as the rapid development and use of unmanned and remotely controlled systems, increasingly highly automated, and in future driven by artificial intelligence.

Threats such as terrorism and extremism are further facilitated by the ability to spread extremist content via the internet, while organised crime exploits global trade flows for its activities. Technological development enables new ways of concealing traces and laundering illicitly obtained money, as with illegal payments.

At the same time and away from the public eye, numerous cyber-attacks are being staged against information and communication systems, where malicious state and non-state actors seek to steal confidential security, economic, technological, and personal data or engage in organised crime. The volume and nature of information present in cyberspace, together with its developmental potential, make this domain strategically important from both a security and defence perspective.

A continuing global challenge is the persistence of destabilising migration, demographic, and social trends, which, together with climate change, form a significant factor in the consideration of security developments.

European open and democratic societies, including Croatia, are the target of disinformation activities and the dissemination of fake news, especially via social media, whereby authoritarian regimes and extremist groups attempt to undermine citizens' trust in democratic values and provoke radicalisation, internal social divisions, and conflict.

In this context, the public needs to have a reliable picture of the security circumstances in which it lives and operates. This public report is therefore SOA's contribution to an objective and well-founded understanding of Croatia's security conditions and perspectives. Naturally, this report does not contain classified information and assessments that SOA provides to the state leadership, but it does represent the basis for understanding the security situation in the Republic of Croatia.

SOA will continue to develop its capabilities, both human and technological, to successfully accomplish its core mission and remain one of the fundamental pillars in safeguarding national security, the democratic constitutional order, and Croatian society.

Deputy Director

Hrvoje Omrčanin

Global and European security environment is marked by complexity and uncertainty

On the global security stage, factors of uncertainty and volatility are strengthening. The European security situation has significantly worsened after Russia's aggression against Ukraine. While the war in Ukraine still shows no sign of an end, conflicts in the Middle East have further undermined the global security situation, particularly the conflict between Israel and Iran, which has global repercussions.

The existing international order is becoming increasingly unstable, international legal and security mechanisms and rules are losing strength and integrity, and as a result, uncertainties and investments in armament and defence systems are growing. At the same time, emergence or form of new international mechanisms for enhancing security and trust is not foreseeable.

China has become the most significant strategic rival of the United States and the West, aiming to achieve its potential as a global power, while at the same time remaining open to investment and trade. Under such circumstances, certain regional powers are balancing between continuing security cooperation with the United States and intensive economic relations with China. The rapprochement between Russia and China, intensified after Russia's invasion of Ukraine, continues, as they seek to promote the creation of an alliance of states as a counterbalance to the West and liberal values. China shares with these states the strategic view that the United States restricts their development and ambitions, and therefore they advocate for the creation of an international order in which they will have a more significant role and zones of interest.

Russia and China are seeking to strengthen their influence in Africa. In certain unstable West African states rich in mineral resources, where several military coups have taken place in recent years, Russian private military companies linked to the Russian state hold significant influence.

The economic sanctions imposed on Russia by Western states have neither prevented the Russian invasion of Ukraine nor decisively reduced Russia's military and combat capacities. Russia is seeking to compensate for the sanctions imposed by Western states through intensified cooperation with BRICS states and the so-called Global South, particularly regarding the export of energy resources and other raw materials.

The new US administration has announced a shift in certain foreign policy and security themes. The US is increasingly emphasising the strengthening of a multipolar world order in which certain world regions gather around different political and economic centres. The new administration has announced a more constructive approach towards Russia, partly due to Russia's rapprochement with China. The US has also begun introducing protectionist trade measures in order to reduce its foreign trade deficit and public debt, as well as revitalise American manufacturing industrial capacities. The new administration has started reassessing US interests and investments in allied arrangements in different parts of the world, including NATO and Europe. In this sense, European states are also intensively considering the construction of a European security architecture in which the US will play a much smaller role. Accordingly, the European Union has announced significant investments in defence capabilities and the European defence industry.

Russia has not abandoned its intention to destroy Ukraine's military power and subject Ukraine to its political control. In doing so, it seeks to portray the war in Ukraine as a defensive reaction to Western actions and counts on having significantly greater chances and resilience than Ukraine in a war of attrition. They expect Western support for Ukraine will weaken with time, particularly with the desired change in US policy. In addition, Russia relies on its long-term quantitative advantage over Ukraine: demographic, military, economic, and military-industrial. The new US administration initially encouraged unconditional negotiations on a peace agreement, but its stance on support for Ukraine changed as Russian offensive activities and missile strikes on Ukrainian cities continued.

The advance of Russian forces in Ukraine over the last two years of war has been limited and very slow. Despite significant losses, Russia has continued to mobilise sufficient numbers of soldiers for the battlefield alongside major investments in the capacities of its military industry, while also receiving political and military support from other authoritarian states, such as North Korea. Ukraine has continued its determined resistance against Russian aggression but remains dependent on Western military and financial aid. A change in US policy could represent a strategic shift in the conduct and outcome of the war for the Ukrainian side.



Russia launched its military invasion of Ukraine in 2022, planning to overthrow the government in Kyiv in a very short time and thus achieve its strategic goal of subjugating the entire country to Russian influence. Having lost the battle for Kyiv, Russia focused on conquering eastern and southern Ukraine, and the war has dragged on for more than three years of exhausting battles with relatively small shifts on the frontlines. This war is also characterised by “information warfare”, primarily carried out on social media, as well as by the massive use of combat and reconnaissance drones, which complement conventional weapon systems. The use of drones also provides excellent real-time battlefield visibility. (Screenshot: Ukrainian Armed Forces)

With Sweden and Finland joining NATO, Russian operations in the Baltic region have been further restricted, while NATO has gained a broader area of operations on its northern flank. Russian political representatives have continued to use threat of nuclear weapons and war escalating into Europe, as a means of intimidating the European and global public in the event of further strengthening of Western aid to Ukraine. To that end, Russia has taken some concrete steps, such as deploying nuclear weapons on Belarusian territory, conducting nuclear military

exercises, and launching new conventional missile systems capable of carrying nuclear warheads.

The terrorist attack by Hamas on 7 October 2023 against Israel triggered a whole series of conflicts in the Middle East (the Israeli military response in Gaza, the conflict with Iran and Hezbollah in Lebanon, Houthi attacks on merchant vessels). The future of Gaza remains uncertain. Israel's military intervention in Gaza also provoked a rise in anti-Semitism worldwide, as well as an increase in Islamist terrorist attacks.

Unlike previously, the June Israeli-Iranian conflict was not fought on territory of third countries. Although brief, it was intense and threatened to spill over into the region if it were not for the fact that Iran's regional allies remained passive, due to exhaustion in their own fight with Israel. The conflict has not been resolved but instead, frozen.

A consequence of geopolitical rearrangements in the Middle East was also the fall of Bashar Al Assad's regime in Syria, which had relied on military support from Hezbollah, as well as Russian and Iranian forces. With their weakening in Syria, Assad's regime quickly collapsed under attacks from rebel forces led by the group Hayat Tahrir al-Sham (HTS). The fall of Assad's regime represents a geopolitical blow to his patrons Iran and Russia.



President of Syria Ahmad al-Sharaa observes rebel HTS forces under his command taking control of the capital, Damascus, in December 2024. HTS emerged from organisations close to Al Qaeda and has been designated a terrorist organisation by many states, although since 2016 al-Sharaa has stressed HTS's departure from terrorist groups. After taking power in Syria, the HTS leadership has sought to gain trust in international relations while at the same time announcing a conciliatory policy towards opposing sides in the Syrian civil war and the reunification of Syria. (Photo: Syrian Presidency)

Prolonged conflicts, political crises, unstable governments with frequent coups, unresolved religious and inter-ethnic relations, the rise of Islamic extremism and terrorism, poor economic conditions, demographic expansion, effects of climate change, transnational criminal networks, and large numbers of refugees/migrants are continuing to generate instability in North African states, the Sahel, and the Middle East. All these factors also reflect on the security of the EU and Croatia.

Global terrorist organisations exploit complex geopolitical circumstances to rebuild their capacities and reach

No terrorist organisations are active on the territory of the Republic of Croatia, and threat from international terrorist organisations in Croatia is again assessed as low.

Nevertheless, as in other European states, we cannot exclude possibility that (self) radicalised individuals inspired by terrorist propaganda could carry out a terrorist attack. In this respect, younger people with psychological difficulties who embrace extreme ideological beliefs and have a propensity for violence are particularly at risk.

The main source of terrorist threat to Europe is Islamic extremism, especially from lone attackers inspired by jihadist propaganda, among whom there is a rising number of young people, minors, and immigrants in the EU from African and Asian countries.

In Croatia, there are several dozen of Salafi followers who do not advocate violence. In Western Balkans states, there are several thousand Salafi followers and a smaller number of adherents of jihadist Salafism. Followers of jihadist Salafism communicate with each other via social media, but also directly, by gathering in so-called *para-jammats*. In this way, they radicalise young people.

In recent years, younger radicalised individuals have mostly conducted the terrorist attacks in Europe inspired by terrorist propaganda. They have primarily used easily available and improvised means, such as knives or vehicles. In 2024, two individual jihadist terrorist attacks were registered in neighbouring countries: on 29 June 2024, in Belgrade, a radicalised convert to Islam wounded a police officer guarding the Israeli embassy with a crossbow, while in Bosanska Krupa in Bosnia and Herzegovina, on 24 October 2024, a self-radicalised minor killed one police officer and wounded another with a knife.

In the Western Balkans, in recent years hundreds of jihadists, former members of ISIL and other terrorist organisations in Syria and Iraq have returned to their home countries. Upon return sentenced to short prison terms, with most released already. Experience shows that jihadists rarely de-radicalise in prisons, and continue to propagate their radical views both during their imprisonment and after release.

The wives of jihadists returning to their home countries were mostly not subject to criminal prosecution. In many returnee families, radical ideas remain present and are transmitted to their children, representing a long-term security challenge.

A large number of jihadist returnees with military experience represent a security risk not only in their home countries but also in other European states. An additional risk posed is the networking of jihadists from the Western Balkans with the Salafist diaspora in EU states.

Individuals with (dual) Croatian citizenship who joined ISIL are still located in camps under the control of Syrian Kurds, where families of ISIL fighters are situated. They comprise mainly women who were radicalised abroad, from where they went to the territory controlled by terrorist organisations in Syria.

The largest terrorist attack in the world in recent years was carried out by members of Hamas when, on 7 October 2023, they attacked Israeli settlements near Gaza, killing, wounding, and abducting hundreds of people. Shortly after the Hamas attack, European states recorded a wave of terrorist attacks by Islamist extremists, with several also thwarted.

International jihadist terrorist organisations ISIL and Al Qaeda continue to call on their supporters to carry out terrorist attacks in Europe. Lone attackers under influence of their propaganda pose the primary threat, but there is also a risk that these terrorist organisations may transfer their members from terrorist strongholds into Europe.

Terrorist attacks in Moscow and Istanbul at the beginning of 2024, for which ISIL claimed responsibility, confirmed its renewed capacity to conduct external terrorist operations. In these attacks, the perpetrators were mostly from Central Asian states, and the attacks were carried out by ISIL's Afghan branch, known as ISIL-Khorasan (ISIL-K).



A video released by the media platform Amaq showed four terrorists who carried out the attack on the Moscow Crocus City Hall concert venue on 22 March 2024, claiming responsibility for the attack on behalf of ISIL. In the attack, the terrorists killed 145 people and wounded more than 500. ISIL regularly uses Amaq as its communication channel for announcements, including claiming responsibility for terrorist attacks. Thus, in August 2024, ISIL used Amaq to claim responsibility for a knife attack in which the attacker killed three people in the German city of Solingen.

Illegal migration also poses challenge for the EU in regards to terrorism. A significant proportion of terrorist attacks (both executed and prevented) in the EU are connected with individuals who migrated to the EU in recent years. ISIL members used the migration wave to move into Europe, presenting themselves as refugees. As some terrorist attacks in Europe in recent years were carried out by individuals who had or were seeking asylum in the EU, security measures in the context of illegal migration and border controls have been tightened, with some states having temporarily suspended implementation of the Schengen regime.

Extremist ideas are most often promoted among young people and minors

Extremism refers to activities and ideas that oppose the constitutional order of Croatia or advocate for its violent overthrow. Therefore, every form of extremist activity is of interest to SOA, regardless of its ideological, political, religious, or national background.

In Croatian society, there are no pronounced extremist movements or phenomena, and no form of extremism has a large number of followers or significant public support. Nevertheless, there are individuals and small groups who have an extremist worldview or undertake activities that fall under extremist behaviour.

On the extreme right-wing scene, the trend of anti-system extremism remains pronounced, that is, extremism that seeks the abolition of Croatia's existing democratic constitutional order. There are intentions and attempts of paramilitary organisation, conducting military training, and acquiring weapons, with the ultimate goal of changing Croatia's constitutional order.



In January 2025, a Croatian citizen was placed on the US list of specially designated global terrorists. He was designated as a member of the international violent far-right online network Terrorgram Collective (Terrorgram), which was placed on the list of terrorist groups. Terrorgram operates on the social media platform Telegram, promotes violent white supremacism, and encourages racially or ethnically motivated violence, as well as attacks on critical infrastructure and state officials. The US authorities have linked Terrorgram to several terrorist attacks, and since June 2024, it has been on the list of terrorist organisations of the United Kingdom. Terrorgram's emblem depicts the Telegram app logo on a black shield modelled after the insignia of Waffen SS units, the military branch of the Nazi party during the Second World War.

Part of the far right promotes neo-Nazi ideology, with incidences occurring due to animosity towards migrants and foreign workers in Croatia. Although the threat of violence from far-right groups is low, there remains the possibility of individual incidents by self-radicalised individuals, who may or may not have links to extremist groups.

A security challenge in Europe is the trend of radicalisation among children and minors, who increasingly express willingness to engage in violent activities. In recent years, the EU has particularly noted a rise in the radicalisation of minors from both Islamist and far-right ideological spectrums. Internet technologies and social media are the main mediums for radicalisation and mutual communication.

The (self) radicalization of minors is influenced by poor family circumstances (dysfunctional/radicalized family, unfavourable socio-economic conditions, etc.), the social environment (peer violence, isolation), and mental health, including the “search for one’s own identity” among young people.

Left-wing extremists/anarchists do not pose a threat to national security due to their small numbers, lack of organisation, and weak public support. The main drivers of the extreme left are the promotion of anarchism and anti-globalism. Following Israel’s intervention in Gaza, pro-Palestinian and anti-Israeli activism has also increased which sometimes takes on violent forms or spreads anti-Semitism. In recent years, Europe has also seen an increase in extremist violent activities within climate-ecological groups.

Greater Serbian extremism in Croatia still has only a small number of sympathisers not directly connected with extremist Greater Serbian and Chetnik (also pro-Russian) organisations that exist in some neighbouring states. Occasional incidents linked to Greater Serbian extremism are isolated or occur over social media. Hence, they do not pose a threat to national security but may present threat to public safety and inter-ethnic relations at the local level.

Extreme members of football supporter groups occasionally disrupt public safety through violence and riots both domestically and abroad. Despite this, such violent behaviour does not currently pose a threat to national security, but it may be a challenge for public safety. In certain local communities, occasional inter-ethnic clashes have a fan background.

Foreign intelligence activities targeting EU countries include espionage, sabotage, and the instillation of fear

Foreign intelligence interests in Croatia are traced mainly to countries that view Croatia as a security, economic, or political challenge, i.e. a country whose activities may affect their interests. Hence, Croatia is looked upon either individually or as a NATO and EU member state. Foreign intelligence activities in Croatia are conducted through data collection and sometimes by active operations aimed at influencing public opinion, Croatia's international position, or decision-making processes.

Individuals and non-state entities, aiming to gather information on the decision-making process, or to influence it, for the sake of their own economic and financial interests, may also conduct intelligence activities towards Croatia.

After Western states expelled hundreds of Russian intelligence officers operating under diplomatic cover at the beginning of Russia's invasion of Ukraine, Russia lost an important tool of its intelligence activities in the West. As a result, it has turned to other means of intelligence work: using intelligence officers without diplomatic cover (so-called "illegals") and recruiting collaborators in EU and NATO member states.

Some of the activities carried out by Russian intelligence services since the start of the war in Ukraine include diversions, sabotage, and influence operations aimed at preventing the delivery of aid to Ukraine. In this way they spread a sense of tension, fear, and vulnerability in EU and NATO member states due to support for Ukraine, and creating distrust among the public towards the credibility of NATO and the EU.

In most cases, these were ordered low-intensity incidents (e.g. pro-Russian graffiti), but there were also cases of diversions and sabotage involving more serious security risks (industrial plant arson, sending incendiary parcels via postal services and airplanes, attempts to sabotage railways, ports, telecommunications towers, threats of terrorist attacks).

These activities are most frequently recorded in North-Eastern NATO and EU member states. In such cases, Russian intelligence services recruited individuals and groups to carry out the ordered activities for financial reasons. The recruited individuals were mostly younger people (sometimes even minors), most with criminal backgrounds.

Recruitment of agent-perpetrators usually conducted through communication apps and social media, whereby job offers posted for Russian speakers. Recruits receive instructions for carrying out tasks via these apps, while payments mostly made in cryptocurrency.

An example of third-party engagement by Russian intelligence services is a group of six Bulgarian nationals convicted for espionage in the United Kingdom in 2025. The group was engaged by Russia's GRU military intelligence service for tasks in several European states, ranging from data collection to monitoring European journalists investigating assassinations and other GRU activities (e.g. the Skripal case), and they even considered their abductions. British prosecutors

revealed that the Austrian national led and financed espionage group. Namely, a GRU agent long on the run from prosecution in the EU.

In February 2025, a Russian national suspected of coordinating sabotage operations against Poland, the US, and other allies was extradited from Bosnia and Herzegovina to Poland. The suspected group, under the orders of a person who had recruited them via the Telegram app, sent explosive devices in postal parcels, which detonated in Poland, Germany, and the United Kingdom.

Foreign intelligence activity towards European states also includes cyber-attacks aimed at sabotage or data theft, carried out by state-sponsored cyber groups. All NATO and EU member states, including Croatia, are recording an increase in this type of threat in their national cyberspace.



In recent years, several cases of Russian “illegals” have been uncovered, i.e. individuals who covertly, under the guise of third-country nationals, operated as intelligence agents for Russia. “Illegals” as actors of intelligence work are a long-standing Soviet, now Russian, practice, intensified with the start of the Russian-Ukrainian conflict as a response to reduced Russian intelligence capacities in Europe caused by the expulsion of Russian diplomats. Western services uncovered several cases of “illegals” operating individually or in groups across the EU. One case was uncovered in Slovenia, where Russian “illegals” had settled in 2017, posing as a married couple, Maria Rosa Mayer Munos and Ludwig Gisch from Argentina, with two children. These were false identities, as they were in fact agents of Russia’s SVR intelligence service, arrested by Slovenian authorities in December 2022. Their real names were Anna and Artem Dultsev. The couple were deported to Russia in a major prisoner exchange on 1 August 2024 in Turkey. Upon their return, they were personally greeted by Russian President Vladimir Putin. (Screenshot: YouTube)

Cyber threats are on the rise, and comprehensive protective measures have been initiated

With the adoption of the Cyber Security Act at the start of 2024, SOA became the central state body for cyber security, and the SOA Centre for Cyber Security became the National Cyber Security Centre as the national coordination point for the implementation of the Act and further regulatory arrangements for the protection of cyberspace.

The National Cyber Security Centre continuously monitors the security situation in cyberspace and enhances national capacities for detection, early warning, and protection against state-sponsored cyber-attacks, Advanced Persistent Threat (APT) campaigns, and other cyber threats directed against Croatia.

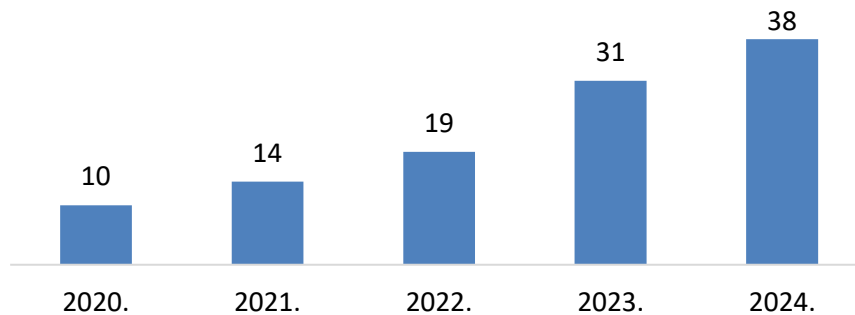


Visual identity of the National Cyber Security Centre. The National Cyber Security Centre also has its own website (www.ncsc.hr), which contains information on the implementation of the Cybersecurity Act and EU legislation in the field of cybersecurity.

In recent years, there has been a continuous increase in state-sponsored APT cyber-attacks against targets in Croatia. In 2024 alone, 38 such attacks were detected, seven more than the previous year. These are organised cyber-attacks primarily aimed at espionage against state bodies, i.e. stealing data of importance to national security. The targets of APT attacks are state institutions and, increasingly, critical national infrastructure. Alongside the rise in the number of attacks, the number of targeted institutions is also increasing.

Russian state-sponsored APT groups carried out two-thirds of significant attacks on targets in Croatia. In addition to already known APT groups, new attackers are emerging.

Alongside state-sponsored APT cyber-attacks, ransomware attacks are becoming more frequent, carried out by advanced cybercriminal groups, mostly Russian.



Number of state-sponsored attacks detected against Croatian targets by year

In their attacks, these criminal groups use tools and tactics similar to those of state-sponsored cyber groups. An example is the Lockbit criminal group's attacks, recorded in Croatia as well, including a ransomware attack on the information system of Zagreb University Hospital Centre (KBC Zagreb) in June 2024.

LOCKBIT 3.0 **LEAKED DATA** [TWITTER](#) [HOW TO BUY BITCOIN](#) [CONTACT US](#) [PRESS ABOUT US](#) [AFFILIATE RULES](#) [MIRRORS](#)

Deadline: 18 Jul, 2024 04:52:16 UTC

kbc-zagreb.hr
 KBC Zagreb is a company that operates in the Hospital & Health Care industry. It employs 2,001-5,000 people and has \$500M-\$1B of revenue.

we have:
 Medical records, patient exams and studies; doctors' research papers; surgery, organ and donor data; organ and tissue banks; employee data, addresses phone numbers etc; employee legal documents; data on donations and relationships with private companies; donation book; medication reserve data; personal data breach reports and much more

UPLOADED: 01 JUL 2024 11:52 UTC UPDATED: 01 JUL 2024 11:53 UTC

1-4 of 12

In recent years, advanced ransomware cyber-attacks on critical infrastructure have become more common. In June 2024, a ransomware cyber-attack was conducted against KBC Zagreb. The attackers managed to steal and lock a large quantity of the hospital's medical documentation. In response to this cyber-attack, the SOA Cyber Security Centre conducted a forensic investigation and issued security recommendations that prevented a greater escalation of the attack. The exfiltrated (stolen) data was successfully recovered and returned to KBC. The screenshot shows a post in which the attackers announced the executed attack, along with several documents proving that they were in possession of medical and other records from KBC Zagreb. The attackers threatened to publish a larger amount of stolen data, but ultimately did not carry out that threat

Cyberspace is continuously used for political propaganda, incitement of social unrest and polarisation, spreading fake news and conspiracy theories, particularly in the context of Russia's aggression against Ukraine.

Large quantities of data, including user personal data, is collected not only by internet companies but also by states, and by malicious individuals and groups.

[SK@UT]

As part of the National Cyber Security Centre, SOA continued the development of SK@UT, the national system for detecting cyber threats and protecting cyberspace. SK@UT currently covers more than 90 state bodies and legal entities in Croatia. In this way, greater visibility of Croatian cyberspace is ensured, the overall capacity and resilience of Croatia to large-scale cyber-attacks and cyber crises is increased, and better conditions are created for attributing cyber-attacks. By law, SK@UT is also defined as a voluntary additional mechanism of cyber protection. To raise cyber security awareness, SOA organised annual conferences in 2023 and 2024 for SK@UT community representatives, where best practices in cyber protection were discussed, solutions for system security proposed, and cases of cyber-attacks analysed.

The availability of large quantities of data on internet-connected servers and in cloud computing environments is leading towards increasing frequency of mass data theft. The EU has therefore launched the drafting of a series of regulatory acts to increase cyber resilience, such as the NIS2 Directive and the Cyber Resilience Act. In recent years, the EU has also conducted several public attributions of cyber-attacks as a method of deterring states sponsoring cyber APT attacks.

In the field of cyber security, SOA is active in international forums and platforms, especially those related to NATO and the EU. The National Cyber Security Centre represents Croatia within the CyCLONE network for cyber crisis management at the EU level.

SOA, i.e. Croatia, also participates in global efforts to combat ransomware attacks through the Counter Ransomware Initiative (CRI), launched by the US with more than 70 partner countries worldwide.

Croatia's economic security is influenced by global economic trends

In order to safeguard Croatia's economic system, SOA collects and analyses information on risks and threats within economic developments that adversely affect the Croatian economy, reporting to the state leadership and competent authorities. In the course of such task, SOA may also obtain indications of potential criminal offences that are then reported to law-enforcement bodies.

Croatia's entry into Euro and Schengen zones has made it even more attractive for attempts at non-transparent investment — notably in the form of money-laundering or evasion of international restrictive measures (sanctions). Following the EU's comprehensive packages of measures aimed at constraining Russia's ability to finance the war against Ukraine, special attention is required for attempts at covert investments of Russian capital in the EU, transferring funds out of Russia, and circumventing sanctions.

Sanctions circumvention is sometimes attempted through private companies registered in third countries, which presents a particular challenge.

The condition of the Euro-zone economies — especially the largest EU members, which are also Croatia's main trading partners — significantly affects industrial trends in Croatia and the performance of the tourism sector. Despite difficulties in parts of the EU, Croatia's economy has continued to grow above the EU average, accompanied by rising employment.



The floating liquefied natural gas (LNG) terminal is located on the island of Krk. The terminal has a geopolitical and strategic dimension within the framework of strengthening the European energy market and increasing the security of gas supply to the EU, particularly for Central and Southeast European countries seeking to secure a reliable supply route. This is a project of strategic importance for both the EU and the Republic of Croatia. The terminal is included on the EU list of Projects of Common Interest and awarded a grant of 101.4 million EUR. The terminal's technical capacity is 2.9 billion cubic meters per year. It consists of an FSRU vessel and the onshore terminal facilities (Photo: LNG Croatia)

Croatia's geographical transport position is important for the European economy and security, with particular emphasis on the importance of Croatian Adriatic ports and their connection to European transport corridors.

Croatia's energy infrastructure, especially the LNG terminal on Krk, makes a substantial contribution to strengthening European energy independence.

EU–China relations continue to be marked by intensive trade ties, but also by systemic rivalry in terms of value-based and societal models. China promotes its model of governance as an alternative to liberal democracy.

The new U.S. administration is seeking to balance its foreign trade by announcing the introduction of trade restrictions and tariffs on countries with which it has a trade deficit, as well as to bring industrial production back to the United States.

Russia has redirected a significant part of its industrial capacity toward military production, while attempting to divert its energy exports to third countries due to reduced opportunities for placing energy products on the European market. In the production of its military systems, Russia relies on Western technology and components.

An ongoing risk is Western technology diverted for military needs of authoritarian regimes under sanctions. Such regimes employ various schemes to circumvent sanctions and procure restricted Western technologies; they also seek to market their own products, including energy, by concealing their true origin. In parallel, co-operation between authoritarian states attempts to substitute restricted Western components with indigenous solutions.

Economic Crime and Corruption

Where SOA, in the course of its operative work, obtains information possibly indicating economic crime or corruption, it is obliged to inform the State Attorney's Office (DORH) and where necessary, other state bodies such as the Ministry of the Interior (MUP).

In accordance with its statutory powers, SOA may, in exceptional cases and at DORH's request, support such proceedings with information and operational-analytical capabilities.

Following the establishment of the European Public Prosecutor's Office (EPPO) in Croatia, SOA can also support EPPO under the same principles and legal provisions as apply to DORH.

SOA participates in the national system for combating money-laundering and terrorist financing, which comprises numerous state bodies — including the Anti-Money Laundering Office, DORH, USKOK, MUP, the Croatian National Bank (HNB), HANFA, and the Ministry of Finance — and co-operates internationally with foreign financial-intelligence units. SOA engages where its jurisdiction and capabilities allow for the requirements of competent authorities, being especially important in cases involving terrorist financing.

SOA is working on locating persons missing from the Homeland War

By mid-2025, the fate of 1,363 persons who disappeared during the Homeland War was still unknown, and the burial sites of the remains of 385 persons killed in the war remained to be located — a total of 1,748 unresolved cases.

One of the priority tasks for SOA is to collect information that can help clarify the fate and burial locations of persons missing from the Homeland War. In addition to the search for the missing and their burial sites, SOA — independently and with other state bodies — gathers information on the circumstances of war crimes, reporting to the competent authorities.

SOA works continuously with the Ministry of Croatian Veterans, MUP, VSOA, DORH, and others.

One of the most significant locations identified in the period under review — for which SOA also collected relevant information — is a mass grave discovered at the remediated Petrovačka dola landfill near Vukovar, where excavations uncovered the remains of at least ten persons who went missing in the Vukovar area after the 1991 occupation.



The Petrovačka dola site has been the most challenging and longest-running investigation of a mass-grave location with the remains of missing persons. Searches began in April 2022, and the first remains were found in May 2024. Over the course of the investigation, more than 110,000 m³ of waste were excavated, examined, and transported to a temporary disposal site. There are indications that additional remains lie beneath the asbestos mound, and the investigation continues. During 2024, the remains of seven missing persons were also found in Negoslavci, and in January 2025, the remains of three persons were discovered in the Berak and Bobota areas. (Screenshot: Ministry of Croatian Veterans)

The issue of tracing the missing is highly sensitive — with a profound personal and humanitarian dimension — also significantly affecting inter-ethnic and inter-state relations.

In this context, institutions in Serbia hold documentation from the time of the Croatian Homeland War — especially relating to the period of occupation of Croatian Danube region — that could help clarify the fate of the missing. Many of the individuals who possess relevant information are also located in Serbia. In addition, during their aggression against Croatia, there were prison camps on Serbian territory to which Croatian soldiers and civilians — mostly from Croatian Danube region— were forcibly taken and abused.

Since our previous public report, there has been no tangible progress in the readiness of Serbian institutions to co-operate. Despite public statements announcing more intensive and concrete co-operation, no such co-operation has materialised in the period under review, notwithstanding Croatian initiatives.

The Western Balkans are still burdened by unresolved interethnic and interstate political-security issues

The stability and security of the Western Balkans, i.e., Croatia's Southeast neighbourhood outside the EU, is extremely important for Croatian national security. This is a region where Croatia has national, economic, security, trade, transport, and other interests. Any significant instability in this area has consequences for Croatian national security and interests. In addition, members of the Croatian people live in the Western Balkan countries, as a constituent people in Bosnia and Herzegovina (BiH) and as a national minority in other states.

This region, long characterized by unresolved interethnic and interstate issues, is finding it difficult to resolve these issues despite the engagement of the EU and USA. At the same time, the European integration process is proceeding very slowly or is stagnating.

In BiH, political instability continues due to differing views among the entities, constituent peoples, and political factions regarding the constitutional order and foreign policy orientation of BiH. Nevertheless, in March 2024, BiH opened EU accession negotiations.

The recent process that has generated the most instability in BiH is the conflict between the leadership of the Republika Srpska entity and the High Representative in BiH regarding authority issues, as well as actions by the Republika Srpska leadership that were ruled illegal by the BiH Court. The Republika Srpska leadership openly advocates the dissolution of BiH and seeks political support, particularly from Russia, and this conflict will continue to generate political and security challenges.

The demands of Croats in BiH for amendments to the Electoral Law, ensuring the legitimacy of the election of Croatian representatives (especially for the Croatian member of the BiH Presidency) in accordance with the Dayton Constitution, have yet to be addressed. At the same time, unitary political factions are attempting to achieve constitutional and electoral changes favourable to them by circumventing the provisions of the Dayton Constitution, for example, through lawsuits before the European Court of Human Rights (ECHR), whose rulings have mostly favoured the claimants. In this way, through the implementation of ECHR decisions, there is an attempt to deconstruct the Dayton Constitution without mutual agreement between the constituent peoples and outside the representative institutions of BiH.

The Republic of Serbia continues its policy of balancing between the West, Russia, and China, while tensions with Kosovo persist. Serbia actively promotes the concept of the "Serbian World," aiming to unite Serbs in neighbouring countries, particularly in BiH, Montenegro, and Kosovo, under the political umbrella of official Belgrade. The "Serbian World" concept, in many of its elements, mirrors the Russian concept of hybrid influence and leverage in neighbouring states, known as the "Russian World."

Recently, Serbia has faced several waves of anti-government protests, in which demonstrators demanded democratization, de-politicization of state institutions, strengthening media

freedom, and combating corruption. Students initiated the largest protests after 16 people died in November 2024 in Novi Sad when the rebuilt railway station canopy collapsed.

Amid a complex internal situation with growing social polarization, media close to the ruling structures in Serbia have intensified political and media narratives about “external and internal enemies” and a climate of national threat, aiming to discredit the student protests. In this context, Croatia is particularly marked as a “permanent anti-Serb factor” and as a state that organizes student protests and acts hostilely towards Serbia.

Senior political officials in Serbia have repeatedly claimed, even in official meetings, that the student protests represent a “coloured revolution” organized by certain Western countries and their intelligence services.

The regime of Aleksandar Vučić, using the security system and media under its control, attempted to discredit the student protests by constructing claims that the protests were organized by Croatian and other foreign services with the aim of “toppling Vučić and Serbia.” For instance, the regime-aligned media outlet Informer published, in real time, photographs, personal data, and movements of Croatian students during their tourist stay in Belgrade in December 2024, simultaneously labelling them as “Croatian spies,” directly endangering their personal safety. Upon returning to Croatia, an unknown person at official premises at the border crossing handed Croatian students a box containing rakija (liquor) with a message stating that they should “greet their colleagues from SOA.” In addition to Croatian students, other Croatian citizens experienced similar inconveniences during their stay in Serbia, with some detained and expelled from Serbia or denied entry. (Screenshot: Informer media posts)

Serbia–Kosovo relations remain unstable. In the past period, Kosovo authorities have been more active in closing parallel Serbian quasi-state institutions operating in the northern part of Kosovo, predominantly inhabited by Serbs. This is part of Pristina’s efforts to strengthen Kosovo’s state sovereignty in that area and limit Belgrade’s influence. Under such circumstances, the escalation of tensions in Kosovo remains a continuous risk, with the military presence of international forces continuing to play a role as a guarantor of security.

The armed attack by Serbian paramilitary formations on Kosovo police in the village of Banjska on 24 September 2023 demonstrated the presence of actors aiming to destabilize the security situation in northern Kosovo and sabotage the negotiation process.

Pristina accused Belgrade of being behind the attack, which Serbian officials denied. Responsibility for the attack was claimed by Milan Radoičić, former deputy leader of the Serbian List, a political party of the Serbian community in Kosovo closely aligned with official Belgrade. Radoičić personally participated in the armed clash and fled to Serbia, questioned and criminal proceedings against him are still expected. It remains unclear how the mentioned paramilitary formation organized itself and acquired heavy military-grade weapons.



In an armed attack by a Serbian paramilitary group on a Kosovo police patrol in the village of Banjska, one police officer and three members of the group were killed, and several others were arrested. After the clash, members of the paramilitary group took refuge in a nearby monastery. In footage from the monastery, the leader of the paramilitary group, Milan Radoičić, can be seen. In the following days, the Kosovo police seized a significant amount of weapons, ammunition, and military equipment. (Screenshot: Kosovo Police)

In Montenegro, the socio-political rift between a pro-European Montenegrin option and a Serbian option — which is also pro-Russian and anti-Western — persists. Radical Serbian parties form part of the current governing coalition. While the government seeks to signal European commitment, the influence of Serbian political forces with nationalist and anti-Western positions can hamper EU-integration and foreign relations with EU members.

Alongside its religious role, the Serbian Orthodox Church (SPC) wields significant national and regional political influence. Its leadership supports and promotes the “Serbian World” concept, particularly highlighting BiH, Montenegro, and Kosovo as belonging to that space. Illustrative was the participation of the SPC leadership in the First All-Serb National Assembly (“One nation, one assembly — Serbia and Srpska”) in Belgrade on 8 June 2024, alongside political leaders of Serbia and Republika Srpska. The assembly served to re-package the nationalist idea “one

nation, one faith, one state”, foregrounding Republika Srpska and also drawing Montenegro into that narrative.



On 22 April 2025, Serbian Orthodox Church Patriarch Porfirije thanked President Putin for Russia’s support and stance on Kosovo, Republika Srpska, and Montenegro, expressing the desire that, in a future geopolitical realignment, Serbs would be close to the “Russian World”. He described Serbia’s student protests as a “colour revolution”, claiming Western centres of power seek to break Serbian identity and culture. (Photo: Office of the President of the Russian Federation)

Russia continues efforts to slow and obstruct Euro-Atlantic integrations in the Western Balkans. It offers political, diplomatic, military, and intelligence backing to Serbia’s foreign-policy aims (primarily regarding Kosovo and Republika Srpska), as well as support in domestic political processes. Russia leverages traditional ties with Serbia — and with Serbs in other states, notably in Republika Srpska — as a basis for political, security, and economic co-operation.

Russia has strengthened its intelligence presence in Serbia, including officers previously expelled from EU countries where they covertly operated as diplomats. Having found shelter in Serbia, these intelligence officers can continue activities unimpeded. At the same time, Serbia and Russia are formalising closer intelligence co-operation.

SRBIJA ▾ GRADANI ▾ POSAO ▾ MEDIJI ▾ VLADA ▾ KONTAKT ▾

VLADA REPUBLIKE SRBIJE
U službi građana

Pretraga...

ODABERITE KATEGORIJU:

- Vlada Srbije
- Aktivnosti premijera
- Aktivnosti potpredsednika
- Aktivnosti Vlade
- Kosovo i Metohija
- Politika
- Ekonomija
- Stop korupciji
- Kultura i vera
- Sport
- Konferencije za novinare
- Intervjui
- Linkovi
- Izdvojene teme
- COVID-19 - arhiva

MEDIJI VESTI AKTIVNOSTI POTPREDSEDNIKA

Čitaj mi

Nastavak bliske saradnje sa Ruskom Federacijom u oblasti bezbednosti

Beograd/Moskva, 22. mart 2025.

Potpredsednik Vlade Republike Srbije Aleksandar Vulin boravi u zvaničnoj poseti Moskvi, gde se danas sastao sa sekretarom Saveta bezbednosti Ruske Federacije Sergejom Šoiguom.

Vulin je izrazio zahvalnost Šoiguu na podršci Ruske Federacije legitimim i legitimim organima Republike Srbije u ponovnom uspostavljanju reda i stabilnosti u državi.

Šoigu se zahvalio potpredsedniku Vulinu, kao dokazanom i iskrenom prijatelju Rusije, na doprinosu u očuvanju prijateljstva i bliskih odnosa naroda dveju zemalja.

Potpredsednik Vlade je istakao da je Šoigu dokazani prijatelj Srbije, koji je uvek u teškim vremenima bio uz srpski narod.

Tokom sastanka je konstatovano da je nedavni razgovor predsednika Srbije Aleksandra Vučića i predsednika Ruske Federacije Vladimira Putina dao novi zamah u daljem jačanju odnosa i saradnje dveju prijateljskih zemalja.

Vulin je obavestio Šoiguu i da je Srbija ispravila grešku, koju je napravila prilikom glasanja o rezoluciji Generalne skupštine Ujedinjenih nacija, i da je promenila svoj glas u uzdržan.

On je ponovio molbu koju je predsednik Vlade Srbije Miloš Vučević uputio ruskoj strani da specijalisti iz te zemlje učestvuju u istrazi o navodnom korišćenju zvučnog topa tokom protesta 15. marta.

Sagovornici su postigli dogovor o nastavku bliske saradnje u oblasti bezbednosti između dve države.

Arhivska fotografija

In March 2025, during student protests, the Government of the Republic of Serbia thanked the Russian Federation for its assistance “in restoring order and stability in the country.” On that occasion, then Deputy Prime Minister of Serbia Aleksandar Vulin met with the Secretary of the Russian Federation Security Council, Sergey Shoigu. Vulin emphasized that Russian special services were assisting Serbian authorities in suppressing the protests and that Serbian and Russian services had previously officially agreed on cooperation in combating “colour revolutions.” The Serbian authorities describe the student protests as a “colour revolution financed and organized by Western intelligence services.” An example of cooperation between Serbian and Russian security services is the case in which the Serbian Security Intelligence Agency (BIA) published a report from the Russian security service FSB regarding the use of so-called sonic cannon during a large student protest in Belgrade on 15 March 2025. In the report, the FSB denied the use of acoustic devices to disperse the protest and noted “there are public indications of a staged provocation involving a specially prepared group of individuals and the use of smartphones to synchronize movements, simulating the effect of a sonic cannon, as well as blocking emergency services.” (Screenshot: Serbian Government)

Russia’s hybrid-influence tools also operate from Serbian territory. In November 2022, RT Balkan (RT in Serbian language) was launched in Serbia, alongside the local branch of Sputnik. These media are used to disseminate pro-Russian and anti-Western narratives across the Western Balkans.

Organized crime from the Western Balkans is active in drug trafficking

Collecting data and monitoring the activities of domestic and transnational organized crime groups represent a continuous task for SOA. SOA also examines the methods of financing international organized crime, the potential corruptive influence of individuals from the criminal milieu on the Republic of Croatia, and money laundering modalities.

From the Western Balkans, the most significant are the “Serbian-Montenegrin” organized crime groups, which primarily engage in international drug trafficking and continuously seek to strengthen their operations. In recent periods, armed clashes and targeted killings among these rival criminal groups have continued, posing risks to public safety and citizens’ lives.

Their most profitable activity remains cocaine trafficking from South America to Europe and in recent years, numerous international police operations resulted in a large number of arrests. In addition to international drug trafficking, organized crime groups are involved in facilitating illegal migration, smuggling and illicit trade in weapons, as well as explosives.

Regional organized crime groups continuously attempt to recruit individual Croatian citizens as collaborators, such as sailors and skippers for maritime drug trafficking, as well as members of the domestic criminal milieu who occasionally assist in concealing their presence in Croatia, obtaining forged Croatian documents, attempting money laundering in Croatia, and similar illegal activities.

Members of the international criminal milieu seek to exploit free movement within the EU Schengen area for covert entry into Croatian territory and for criminal activities. Consequently, SOA initiates procedures to ban entry to Croatia or to expel organized crime members from the country and this preventive security measure has in recent periods, been applied to several dozen individuals.

SOA provides support to the Ministry of the Interior in intercepting smuggling activities across Croatian territory, with particular attention to the trafficking of weapons and explosives from the Western Balkans. In circumstances where weapons are easily accessible in Balkan countries, some of these weapons end up in the hands of migrant smuggling networks. There is also the possibility that illegally obtained arms could be used to carry out terrorist attacks.

SOA continuously monitors the potential for weapons to be trafficked to crisis hotspots or countries under international sanctions, as well as issues related to proliferation and dual-purpose goods.

SOA has developed international cooperation on suppressing of international crime issues, as well as collaboration with the police and other national authorities.

Illegal migration remains intense under the influence of unstable global conditions

SOA continues to analyse data and assess trends related to illegal migrations. Following Croatia's accession to the Schengen Zone, there has been an expected increase in migrant pressure on the Croatian border and consequently, heightened activity by transnational smuggling networks.

The fact that most illegal migrants do not possess documents to prove their true identity, presents a particular security risk. Uncontrolled arrivals of migrants with unknown or false identities increase the risk of transit for members of terrorist or paramilitary groups, as well as criminal organizations from crisis hotspots.

The gathering of larger groups of migrants near the Croatian border, as well as their transit through Croatian territory, pose security risks in terms of strengthening smuggling networks, conflicts between migrant groups, self-radicalization of dissatisfied migrants, attempts at violent group border breaches, the spread of false and alarming information, and an increase in the number of extremist groups in society.

On certain segments of migrant routes in the Western Balkans, there are armed smuggling groups that increasingly clash with one another, using both cold weapons and firearms. Smuggling networks utilize communication platforms and social media (e.g., Telegram groups) for coordination and among other things, offer migrants forged documents from EU countries.

In 2024, approximately 29,000 illegal migrants entered Croatia, representing a decrease of about 60% compared to 2023. According to Frontex data, around 239,000 migrants entered the EU irregularly in 2024 (38% fewer than in 2023), of which 69,436 entered Europe via the Eastern Mediterranean route (14% more than the previous year), mostly from Afghanistan and Syria. The Eastern Mediterranean route - that partly passes through Croatian territory - was the busiest route for migrant entry into the EU in 2024, while 66,766 migrants entered via the Central Mediterranean route (59% fewer than in 2023). Women accounted for only about 10% of irregular migrants, and minors represented around 16% in 2024.

In 2024, the entry of Russian nationals into Croatia continued, mainly members of ethnic groups from the Russian North Caucasus republics. Among them, SOA identified individuals linked to their security and paramilitary structures, who may pose a security risk.

A significant part of the migration pressure on Croatia results from visa-free regimes that certain neighbouring countries have with states from which a large number of migrants originate. In this way, migrants legally enter the Western Balkans, from where they attempt to cross illegally into Croatia and, ultimately, the EU.

There has also been a significant increase in the number of criminal offenses related to migration, as well as in the number of arrested smugglers. According to the Ministry of the Interior, the police arrested more than 1,500 smugglers in 2023, and this number increased to over 1,800 in 2024.

Through cooperation with international partners, SOA participates in safeguarding European security

Security and intelligence systems of democratic states, particularly those within NATO and the EU, are increasingly intensifying and expanding their cooperation. SOA is recognized as highly active in contributing to the strengthening of European and Euro-Atlantic security and intelligence platforms.

International security and intelligence cooperation occurs across all areas of activity through the exchange of data, alerts, and assessments; joint operational work on specific security issues; sharing of experiences; joint training; and other forms of collaboration.

International cooperation may be conducted bilaterally, while multilateral security and intelligence platforms are becoming increasingly important.

SOA has established cooperation with dozens of European and global security and intelligence agencies. Bilateral cooperation with partners depends on the specific characteristics of each country and shared interests and security challenges. SOA maintains most intensive bilateral cooperation with the security and intelligence agencies of democratic states, namely, members of NATO and EU.

SOA is a member of all relevant European and regional multilateral security and intelligence platforms. Within EU and NATO frameworks, SOA is highly active in the work of the respective security and intelligence bodies. In recent years, SOA has chaired all major European security and intelligence platforms.

Some multilateral platforms also involve operational cooperation, in which the security services of EU member states and other Western European countries jointly respond to security threats to Europe.

An example of non-operative multilateral cooperation is the Intelligence College in Europe (ICE), launched in Zagreb in February 2020, where member states develop a common European intelligence culture and cooperation with the civilian community. The academic program of the Intelligence College involves the Faculty of Political Science, the Faculty of Humanities and Social Sciences at the University of Zagreb and since 2024, the University of Defence and Security “Dr. Franjo Tuđman.”

A particularly significant contribution of SOA to strengthening and developing the capabilities of European security and intelligence systems is the establishment of the Centre of Excellence for Open Source Intelligence (OSINT). In 2023, the Croatian Parliament passed a law establishing the OSINT Centre of Excellence, which began operations in early 2024. Currently, nine European countries are participating in the Centre: Croatia, Germany, France, Spain, Italy, Hungary, Poland, Austria and Switzerland. A Memorandum of Understanding has been signed with the EU Intelligence and Situation Centre (EU INTCEN). More information on the activities of the OSINT Centre of Excellence can be found at www.osintcoe.hr.

SOA is the most significant body in Croatia's security and intelligence system in terms of scope of tasks

Security and Intelligence System of the Republic of Croatia

The security and intelligence system is part of Croatia's national security framework. SOA is the largest and in terms of scope of tasks, the most significant body within Croatia's security and intelligence system.

The security and intelligence system of Croatia, is defined in the Security and Intelligence System Act. Two security and intelligence agencies operate in Croatia: SOA, which performs security and intelligence tasks in the civilian sector, and the Military Security and Intelligence Agency (VSOA), which performs security and intelligence tasks in the military and defence sector.



Diagram of the Security and Intelligence System of the Republic of Croatia

Both the Croatian President and Croatian Government, through the Council for National Security (VNS), direct work of the security and intelligence agencies. The VNS examines and assesses security threats and risks, and issues appropriate conclusions.

Within the VNS, the President and the Government jointly establish the Annual Guidelines for the work of the security and intelligence agencies, which contain topics and priorities essential for achieving Croatia's national security objectives. Based on the Annual Guidelines, SOA plans its work and reports to its users; the guidelines also serve as the basis for oversight of agency activities and for evaluating the fulfilling of SOA's tasks.

In addition to the Security and Intelligence System Act of the Republic of Croatia and the Annual Guidelines, SOA's work is also influenced by other legal and strategic acts. One such act is the Cybersecurity Act of 2024, which designated SOA as the central state body responsible for cybersecurity.

Operational coordination of agency work, as well as the implementation and development of decisions by the President and the Government on the guidance of SOA and VSOA, is conducted by the Security and Intelligence Agencies Coordination Council (the Council). The Council is chaired by the Deputy Prime Minister responsible for national security, and his Deputy being the National Security Advisor to the President. Other members of the Council include the directors of SOA and VSOA and the Head of the Office of the Council for National Security (UVNS). Other persons may participate in Council work at the invitation of the Council's chair.

UVNS handles expert and administrative tasks for both the VNS and the Council, carries out professional oversight of the security and intelligence agencies, and enables the VNS to evaluate agency performance.

Among other bodies in the security and intelligence system, the Information Systems Security Bureau (ZSIS) performs tasks in the technical areas of information systems and network security for state authorities, while the Operational-Technical Centre for Telecommunications Surveillance (OTC), at the request of SOA and other authorized bodies, conducts activation and management of secret telecommunications surveillance measures, services, and traffic, subject to the appropriate order and approval.

Role of SOA

SOA has two primary areas of activity: security work and intelligence work.

The security segment of SOA's work involves collecting and analysing data to detect and prevent actions by individuals or groups aimed against the existence, independence, unity, and sovereignty of the Republic of Croatia, against the violent overthrow of state authority, the endangerment of human rights and fundamental freedoms, and against the foundations of Croatia's economic system.

The intelligence segment of SOA's work involves collecting and analysing political, economic, scientific-technological, and security-related information concerning foreign states, organizations, political and economic alliances, groups and individuals, as well as other relevant data.

While some countries have separate agencies for security and intelligence work, Croatia has combined these two areas within SOA since 2006.

With the Cybersecurity Act, SOA gained a third important area of work: performing the duties of the central state body for cybersecurity.

Organization and Structure

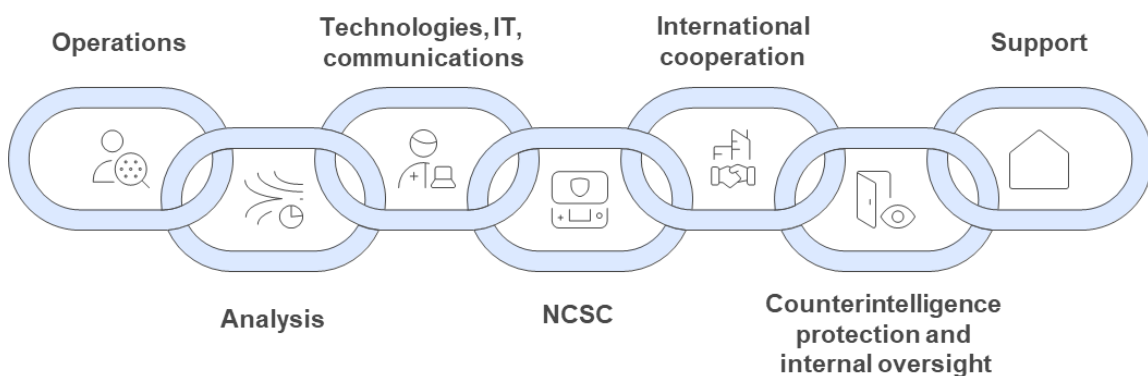
By Government Regulation, with the consent of the President of the Republic of Croatia, SOA adapted its structure in 2024 to new security circumstances and needs. Within SOA, the National Cyber Security Centre (NCSC) was also established.

SOA's work is managed from its headquarters in Zagreb, while the entire territory of Croatia is covered through four regional centres with corresponding organizational units.

The headquarters of SOA is structurally composed of seven main divisions:

- Operations, responsible for data collection,
- Analysis, which analyses data and produces relevant analytical outputs,
- Special technologies, IT, and communications,
- National Cyber Security Centre (NCSC),
- Counterintelligence Protection and Internal Oversight,
- International Cooperation,
- Human Resources, Legal, and Material-Financial Affairs.

SOA is managed by a Director, or in their absence, a Deputy Director, appointed jointly by the President and the Prime Minister of Croatia. The Director's term lasts four years. From 1 September 2024, following the departure of the then Director to an EU position, SOA has been managed by Deputy Director Hrvoje Omrčanin.



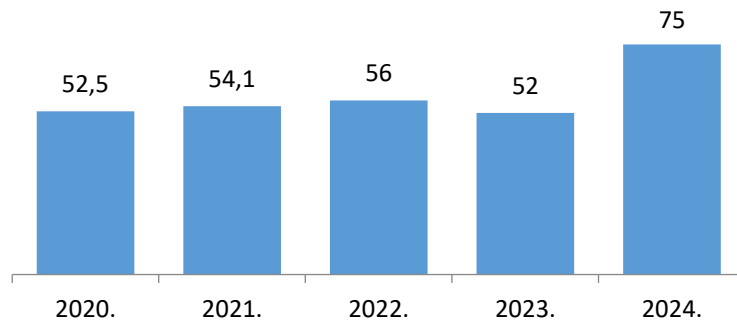
Main organizational units of SOA

Budget Management

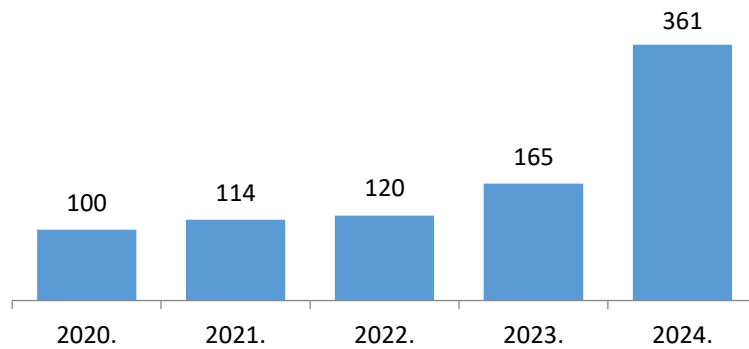
In 2024, SOA's budget amounted to approximately 75 million EUR. The increase compared to previous years is the result of a general rise in expenditure for state administration employees, as well as increased investment in national security, particularly in the field of cybersecurity.

The structure of the budget, as well as data on SOA's financial operations, are classified. This is a legal restriction applied in other EU and NATO member states as well. The largest portion of SOA's budget is spent on employee costs, followed by daily and operational expenses, with a significant share allocated to development and modernization.

Development and modernization of capabilities are conducted according to plan, taking into account SOA's tasks and needs, as well as security challenges to which SOA must be prepared to respond. Both the absolute and relative amounts allocated by SOA for modernization have been steadily increasing. Over the past five years, SOA has more than tripled its investment in new technologies and the modernization of its operations.



SOA budget trends by year, in millions of Euros



Index of funds invested in development and modernization from 2020 to 2023

(2020 = 100)

In planning and executing its budget, SOA implements all prescribed measures to ensure the lawful use of budgetary funds and reports its expenditures to the competent state authorities.

Oversight of SOA's Work

SOA collects data important for national security through communication with citizens, requesting official information from state and local authorities and legal entities, from public and open sources, by applying covert measures and procedures, and through data exchange with partner agencies.

The application of measures that temporarily restrict certain constitutional human rights and fundamental freedoms requires approval of the Supreme Court, while certain measures prescribed by law, may be approved by the SOA Director.

To ensure the legality of its operations, particularly in the application of covert collection measures, SOA is subject to continuous tri-level oversight:

- Parliamentary oversight is conducted by the Croatian Parliament, either directly or through the Committee on Internal Policy and National Security;
- Expert oversight is carried out by the UVNS. UVNS oversight enables the President of the Republic and the Government of Croatia to monitor the work of security and intelligence agencies. It also includes evaluation of the implementation of decisions by the President and the Government in directing the work of these agencies;
- Civilian oversight is conducted by the Council for Civilian Oversight of Security and Intelligence Agencies. Civilian oversight is a mechanism that is rare in democratic states.

Since the legality of SOA's work is also subject to judicial review, a fourth, so-called judicial level of oversight can also be recognized.

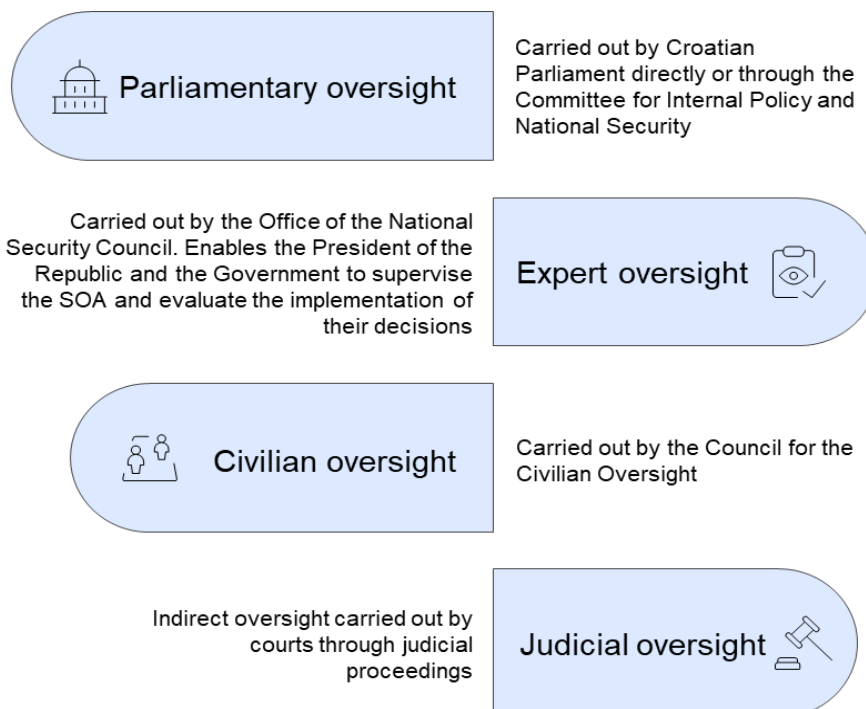


Illustration of external oversight of the legality of SOA's work

Oversight Bodies have broad powers in conducting supervision, such as reviewing SOA documents, holding interviews with the Director and SOA employees, and more. According to the results of oversight conducted in recent years, no illegalities in SOA's operations have been identified.

In addition to overseeing the legality of SOA's work, UVNS conducts annual oversight of the professional and operational standards across all segments and organizational units of SOA. Therefore, UVNS oversight reports also include assessments of these aspects of work, along with professional comments and recommendations aimed at further improving the quality of SOA's operations. UVNS submits its oversight reports to the state leadership.

In addition to external oversight, SOA has an internal oversight unit, a separate organizational division responsible for monitoring the legality of the work of SOA's organizational units and employees, the protection of classified information, and counterintelligence protection.

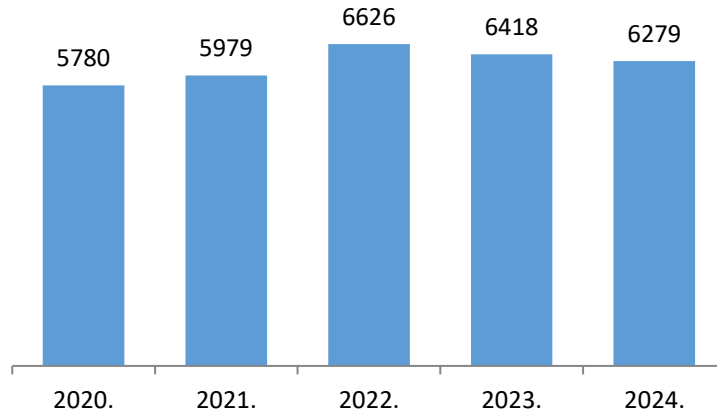
Reporting to Users

SOA reports all significant data, analyses, and assessments relevant to national security equally and simultaneously to the President of the Republic of Croatia, the Speaker of the Croatian Parliament, the Prime Minister, and the Head of UVNS. In 2024, SOA provided each of them with 593 pieces of information and other analytical reports.

As part of the national and homeland security system, SOA continuously cooperates with other state authorities and provides them with the data and assessments necessary for the performance of their duties. Depending on the type of information, SOA shares its data and analyses with the Ministry of the Interior, Ministry of Foreign and European Affairs, State Attorney's Office, Office for the Suppression of Corruption and Organized Crime, Ministry of Defence, Ministry of Economy, and others. In 2024, SOA sent approximately 9,100 different security and intelligence reports to other state authorities, which is in line with the multi-year average.

Security Vetting

As part of its preventive work and efforts to strengthen information security, SOA conducts security vetting, including basic vetting and vetting for access to classified information. Over the past three years, SOA has conducted more than 6,000 vetting procedures annually. Nearly 80% of these vetting procedures are for access to classified information at various levels, while approximately 20% consist of basic vetting.

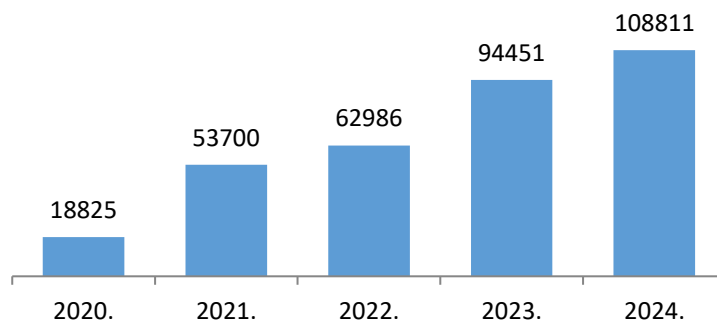


Number of security vetting procedures conducted by year

In 2024, 551 security assessments were conducted related to the movement and stay of protected persons and protected facilities, representing an increase of approximately 5% compared to 2023.

The number of vetting procedures in the process of resolving status issues for foreigners and citizenship continued to grow, with a total of 108,811 individuals screened in 2024. Most of these checks were carried out in the process of issuing visas to foreign nationals in Croatia.

In handling applications for international protection (asylum and subsidiary protection), SOA also participates by providing opinions to the Ministry of the Interior, with each case being assessed individually.



Number of SOA vetting procedures in the process of resolving all status issues for foreigners and citizenship by year

SOA continuously receives job applications and conducts candidate selection procedures

Despite technological advancements, the abilities and competencies of SOA employees are decisive for the quality of work and the fulfilment of SOA's tasks. Due to the specific nature of security and intelligence tasks, as well as the risks and potential dangers to which employees may be exposed, SOA is legally obliged to protect the identities of its staff.

The total number of employees and the employee structure at SOA are classified. The majority of SOA employees are officials, while a smaller portion are administrative staff. Women make up approximately 40% of SOA's workforce and have equal opportunities to their male colleagues regarding assignment to specific positions and the performance of tasks.

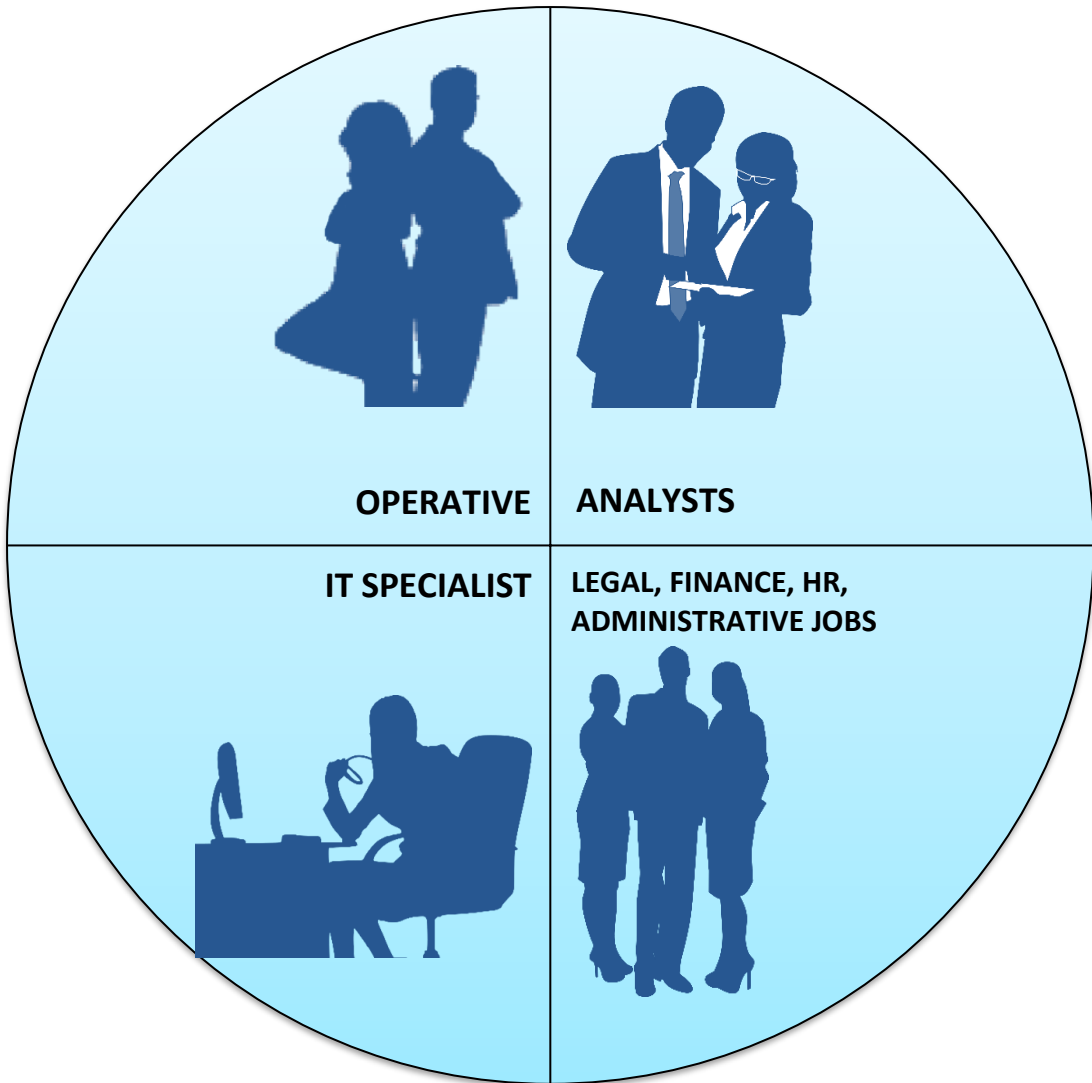
Given the breadth of tasks and duties, SOA employs staff with various profiles and levels of education. Positions at SOA cover operational, analytical, technical-IT, financial, legal, human resources, administrative, security, and other segments. Three-quarters of SOA employees hold some form of higher education.

SOA does not conduct public recruitment tenders, but there is continuously open opportunity to apply for a job, with recruitment procedures and testing conducted throughout the year. Information on employment at SOA can be found on the official website, www.soa.hr, and interested candidates can apply via the web form available there.

All received applications are considered, and candidates with the necessary qualifications, skills, and personal attributes required for specific positions are invited to proceed further. SOA guarantees equality and objectivity in the candidate selection process for all applicants.

The selection process includes, among other things, security clearance, various knowledge and skills tests, psychological assessment, and medical examination. Candidates whose results best match the required employee profile are selected. Both candidates with and without work experience may apply for positions at SOA.

SOA invites all individuals who believe that their qualities, skills, and motivation can meet the challenges of working in a modern security and intelligence environment, and who wish to contribute to the well-being of the Republic of Croatia and its citizens, to apply for a job at SOA. This includes individuals with secondary education, who perform operational and technical tasks, as well as various administrative and support roles.



Security-Intelligence Agency
Savska cesta 39/1
10000 Zagreb

CONTACT:

Phone: 01/ 377 22 22

E-mail: informiranje@soa.hr

www.soa.hr