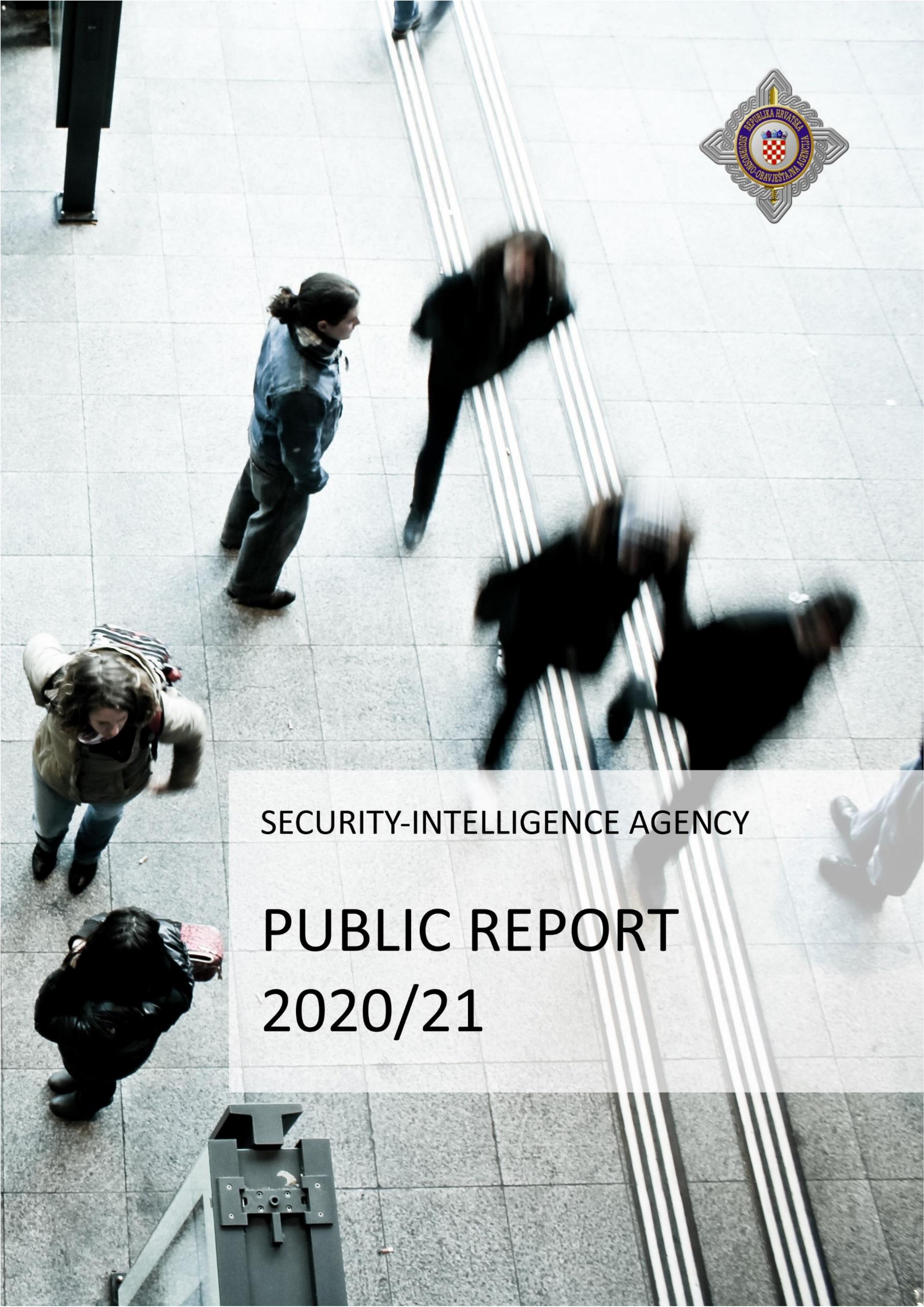


SECURITY-INTELLIGENCE AGENCY

PUBLIC REPORT 2020/21

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 a significant national influence and impact and a regional reach, recognised by its developed capabilities, excellent employees and strong partner ties.

CONTENTS

REPUBLIKA HRVATSKA
SIGURNOSNO-OBAVJEŠTAJNA AGENCIJA

Introductory remarks

Dear readers,

our public reports have become a great tool for keeping up with the changing and dynamic security landscape that we live in. This is our seventh report since we started publishing them in 2014. In this short period we have witnessed numerous and occasionally unexpected security trends and phenomena.

We have seen the creation, rapid expansion and territorial defeat of the so-called Islamic state, the largest terrorist organisation in the world; we have observed the spread of democratic values across the world being replaced by authoritarian tendencies and we have experienced a return to Cold War tensions, espionage, spread of fake news and propaganda; cyber technologies have enabled large-scale cyber attacks with the aim of theft of state and industrial data; illegal migration has grown exceedingly in Southeast Europe and hundreds of thousands of migrants have passed through this area; non-Western actors have been operating in our southeast neighbourhood, and reforms necessary to reach European standards have stalled; organised crime in this part of Europe has been further strengthened with strong interconnections and proliferation of illegal operations: crisis hot spots such as Syria and Libya have been sources of instability and threats since the first public report; we have observed a world increasingly dominated by processes of geopolitical repositioning and rivalry, with growing ambitions of economic, political and value challengers of liberal democracies in the international order; climate change has shown its consequences; despite 20 years of international efforts in democratisation, the Taliban have taken over Afghanistan, and lastly, we have been witnesses of the greatest pandemic in the modern history which has disrupted our daily lives at an unprecedented level and caused tremendous harm to the global economy.

At the same time, since our inaugural report, we have been able to observe a number of developments in the security sphere: our EU and NATO memberships have allowed us to multiply our capabilities and enhance our security mechanisms and connections with other democratic security and intelligence systems; European states have been growing closer in responses to common security threats; Croatian society and institutions have confirmed their stability and efficiency in many crisis situations; new infrastructure projects have reinforced our energy and national security; technological development has provided us with new capabilities and possibilities in the protection of national security; we have been training a new generation of our employees recruited and selected in open public calls.

All these changes and shifts indicate that security dynamics in the modern world move at an exceptionally rapid pace and are frequently unpredictable. New and non-traditional security threats have been intensifying, and the role of timely and accurate intelligence and assessments has become crucial.

Collecting intelligence and creating accurate insights into security and political processes has become a prerequisite for successful development. And this is exactly where the significance of security and intelligence work lies in the modern world. Such circumstances are a professional challenge for SOA. We are the state institution that brings security trends and scenarios to the attention of decision-makers. We warn of threats and challenges to national security, explore their background and possible consequences, and finally, enable informed decision-making for the purpose of the protection of national interests.

As in the previous years, this Public report confirms that the Republic of Croatia is a safe and stable democracy. In these challenging times and within a dynamic security landscape, there are no indications of serious destabilisation.

It is necessary to have capable and trained professionals, modern technology and flexible organisation to cope with the volatility in the world today. In order to realise our exceptionally important mission, at the Security-Intelligence Agency we continuously adapt our operations and work organisation, we invest in professional training and employee development, and we build up our technical capabilities.

We engage in planned development and with responsibility to public funding that Croatian citizens allocate for our work, so that we can develop capabilities that will provide the best possible protection in the future. We strive to carefully develop those capabilities that can be used in a wide range of tasks and that can be adapted to the specific needs and requirements of national security.

Our focus on performance, professional employee development and investment in new capabilities will allow Security-Intelligence Agency to carry out its mission as the leading state institution in the protection of national security, interests, democratic order and citizens of the Republic of Croatia.

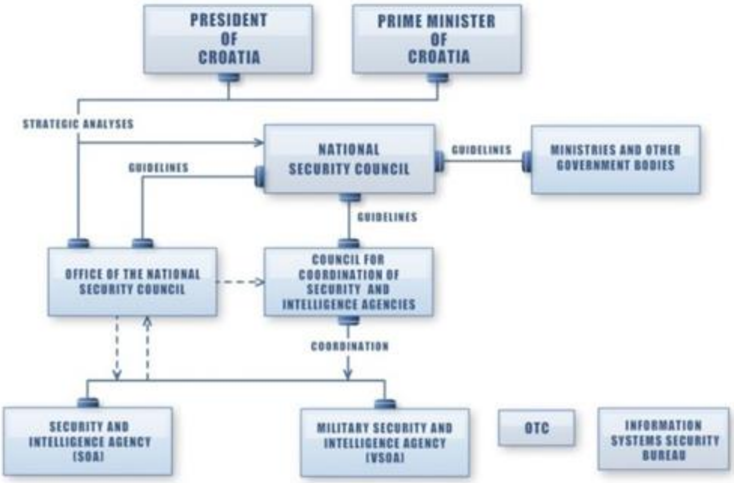
Director

Daniel Markić

Security-Intelligence Agency (SOA)

Security and intelligence system in the Republic of Croatia

The security and intelligence system in the Republic of Croatia is defined by the 2006 Security and Intelligence System Act. There are two security and intelligence agencies in the Republic of Croatia: Security-Intelligence Agency (SOA) is in charge of the civilian part of national security protection, while the Military Security-Intelligence Agency (VSOA) is responsible for the military and defence part of security issues.


PRESIDENT OF CROATIA
PRIME MINISTER OF CROATIA
STRATEGIC ANALYSES
NATIONAL SECURITY COUNCIL
GUIDELINES
GUIDELINES
MINISTRIES AND OTHER GOVERNMENT BODIES
GUIDELINES
OFFICE OF THE NATIONAL SECURITY COUNCIL
COUNCIL FOR COORDINATION OF SECURITY AND INTELLIGENCE AGENCIES
COORDINATION
SECURITY AND INTELLIGENCE AGENCY (SOA)
MILITARY SECURITY AND INTELLIGENCE AGENCY (VSOA)
OTC
INFORMATION SYSTEMS SECURITY BUREAU

Security and intelligence system in the Republic of Croatia

The work of the security-intelligence agencies is directed by the President of the Republic and the Government of the Republic of Croatia through the National Security Council (VNS). VNS, among other activities, directs the work of security and intelligence agencies, considers and assesses threats and risks, and outlines relevant guidelines and conclusions. The Council for the Coordination of Security-Intelligence Agencies (the Council) operationally coordinates the work of the agencies and implements the decisions of the President of the Republic and the Government of the Republic of Croatia which direct the work of SOA and VSOA. It also elaborates VNS decisions which pertain to operations of the security and intelligence system. The Office of the National Security Council (UVNS) the Council provides the VNS and the Council with expert and administrative tasks. UVNS carries out tasks which enable the VNS to evaluate and oversee the work of the security-intelligence agencies.

The Information Systems Security Bureau (ZSIS) is responsible for technical areas of information security and networks of state bodies. The Operational-Technical Centre for Telecommunications Surveillance (OTC) activates and manages the measures of covert surveillance of telecommunication services, activity and transmissions, at the request of SOA or other legally authorised state bodies, on the basis of appropriate warrants and approvals.

Scope of work

SOA collects and analyses information with the aim of detecting and preventing activities of individuals or groups that are directed against the independence, integrity and sovereignty of the Republic of Croatia or aimed at the violent overthrow of the constitutional order; threatening to violate human rights and fundamental freedoms or to endanger the foundations of the economic system of the Republic of Croatia. Moreover, SOA collects and analyses, processes and assesses intelligence relating to foreign states, organisations, political and economic alliances, groups and individuals and other intelligence of particular importance to the national security.

SOA is authorised by law to collect intelligence in a number of ways: in direct communication with citizens, by requesting access to official data, using covert measures and procedures, using public sources and international exchange with partner agencies. SOA also collects public and open-source data.

Any measures of covert intelligence collection that infringe the constitutional rights and freedoms of the individuals and citizens must be authorised by the Supreme Court of the Republic of Croatia or SOA Director, depending on the type of the measure implemented and in line with the provisions of the Security and Intelligence System Act.

SOA reports the end-users as stipulated by relevant legislation (state authorities, ministries and other state bodies) on the findings and assessments that pertain to national security in the form of security and intelligence analysis and data.

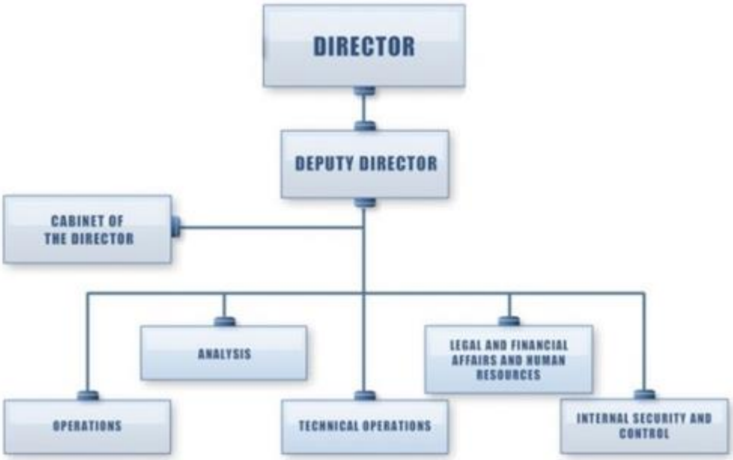
As an integral part of the national security system, SOA cooperates and delivers intelligence and security assessments to other competent authorities such as Ministry of the Interior (MUP), Ministry of Foreign and European Affairs, State Attorney's Office, Croatian State Attorney's Office for the Suppression of Organised Crime and Corruption (USKOK), Ministry of Defence, Ministry of Finance, Ministry of Economy and Sustainable Development etc.

Organisation and structure

SOA is headed by a director appointed by joint consent of the President of the Republic and the Prime Minister of the Republic of Croatia. Daniel Markić has served as the Director since 5 May 2016. On 6 May 2020 he was appointed for a second term. SOA Director is appointed for a four-year term.

SOA is organised in the following units:

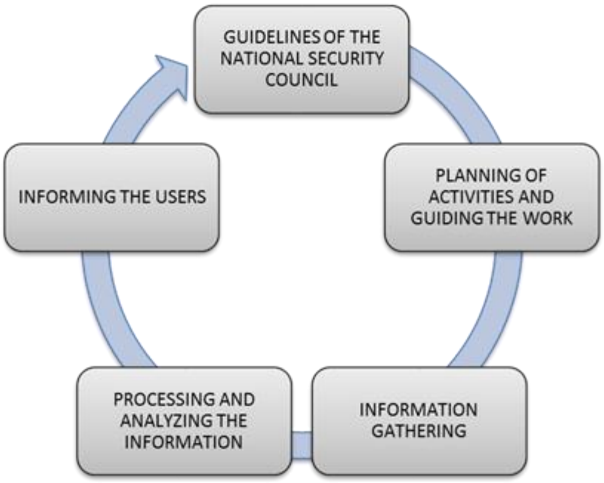
- Operations - responsible for intelligence collection,
- Analysis - in charge of intelligence analysis and preparation of analytical materials,
- Special technologies, IT and communication,
- Counterintelligence protection and internal oversight and,
- Human resources, legal and administrative affairs.



SOA organisational chart

Guidelines

At operational level, the National Security Council issues Annual Guidelines that regulate the operations of the security-intelligence agencies. The Guidelines are a tool which the President of the Republic and the Government of the Republic of Croatia employ to direct the work of the agencies and define issues significant for the protection and realisation of national security and national interests. SOA plans its operations and reports end-users in line with the Guidelines. The Annual Guidelines also serve as a framework for the implementation of oversight and to evaluate the performance of the Agency’s tasks.


GUIDELINES OF THE NATIONAL SECURITY COUNCIL
PLANNING OF ACTIVITIES AND GUIDING THE WORK
INFORMATION GATHERING
PROCESSING AND ANALYZING THE INFORMATION
INFORMING THE USERS

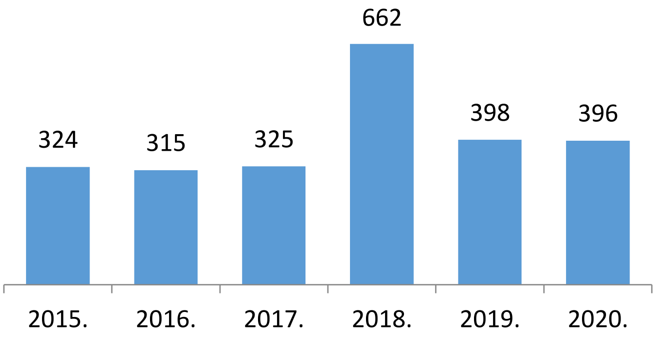
Intelligence cycle

In addition to the Annual Guidelines, SOA operations are directed by strategic and long-term documents such as the National Security Strategy and the National Strategy for the Prevention and Suppression of Terrorism.

Budget management

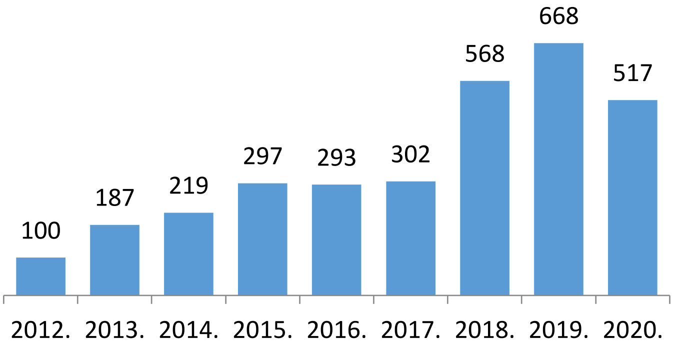
The Agency's Budget in 2020 amounted to HRK 396 million. As in the previous years, the largest share of the Budget was allocated for people force expenditures, followed by operating and capital expenditures.

As per the Security and Intelligence System Act, and in line with practices of the EU and NATO member states, the budgetary structure of the Agency is classified. Despite that, SOA complies with all measure pertaining to budget planning and realisation, as prescribed for the purpose of lawful and expedient allocation of budgetary funds. The Agency reports the relevant authorities on budgetary expenditure.



SOA's budgetary trajectory by years in HRK mil

The pandemic conditions and declining economic activity had necessitated a budget rebalance in 2020. As it was subsequently reduced, certain development and modernisation projects were postponed or delayed in implementation. A significant amount was nevertheless invested in development and modernisation in 2020, allowing the Agency ongoing advancement in capability-building and technological development. Funds allocated towards development and modernisation have been invested in a planned manner, in order to attain capabilities which will allow SOA to respond to a wide range of security and technological challenges.



Index of expenditure for development and modernisation 2012 - 2019 (budget realisation, 2012=100)

Outbreak of the COVID-19 pandemic impacts global security

In addition to all public health and economic consequences, the COVID-19 pandemic has had a significant impact on the development of global security. That impact ranges from the personal security of each individual and the state of security in particular states and regions, to geopolitical changes that will affect the overall world order and security.

The pandemic waves have burdened and overloaded health care systems. In an attempt to contain contagion and protect public health systems, states have restricted free movement of people, goods and services and closed some parts of their economies and social activities, propelling a global decline in economic activity and one of the deepest economic crises in recent history. The European Union GDP fell by 6% in 2020. Economies where services and tourism make up a significant part of the GDP, such as Croatia, Spain, Greece and Italy, have been particularly affected. The EU has responded to this challenge with a comprehensive set of relief and recovery measures.

In the economic and financial sectors, European companies have been intensely exposed to threats of unfair competition, intellectual property theft, and high-tech strategic companies have been exposed to threats of geopolitical takeovers. In situations when the value of shares of European strategic companies is considerably driven down by the outbreak of the pandemic, these takeover attempts come from foreign non-European actors originating in states whose governments often own such organisations or make illegal and clandestine state subsidies to their business. Some EU member states have already proposed a model of state share buy-back schemes and have been considering harmonising market principles with state intervention and protectionist measures.

Those states where economies are unable to overcome the difficulties caused by the economic and social disruption are at risk of rising unemployment and poverty, and consequently rising crime, internal and external migration, social unrest, extremism and discontent. In some states, the outbreak of the pandemic has delayed or halted the resolution of other social or political issues.

The sudden outbreak and the intensity of the pandemic make it a new and additional driver in the repositioning of the international relations. Disruptions in supply chains, manufacturing and supply and demand, particularly in the early stages of the outbreak, have revealed vulnerabilities of the globalised economic processes. The consequences of these disruptions have already come to light in the form of product shortages. Manufacturing processes have slowed down, prices of raw materials have gone up, causing inflationary pressures. Early in the pandemic there was a reduction in manufacturing, and in some instances production processes came to a halt. This was mainly the case in raw materials and in the construction sector. After the first wave of the pandemic the situation somewhat improved, and the economic activities picked up and demand rose sharply. Manufacturing processes were unable to keep up with this demand, which led to a fall in supply, shortage of raw materials and products, caused market disruptions and created serious increase in the price of goods and labour in the European and global markets. The EU member states have been individually trying to provide aid and relief to their struggling economies, however a need for a Union-level solution has been emerging.

Early on in the pandemic even highly developed economies experienced shortages of food and basic goods. This has raised awareness of the need for a more focused care of natural resources, such as agricultural land and the food industry, as one of the priorities of national security.

Many European states have been dealing with various attempts to exploit the public heath and economic crisis in order to generate illicit revenue. Shortages of personal protection equipment and resources early on in the pandemic necessitated that these goods be supplied through alternative channels, which created opportunities for various manipulations and illegal operations carried out by individuals and companies with the aim of generating illicit revenue.

The outbreak of the pandemic has further fuelled the rise of extremism and radicalism, especially in the context of the dissemination of disinformation and conspiracy theories about the European response to the crisis and the effectiveness of liberal democracies. The pandemic has provided a backdrop for new information activities in the geopolitical competition. Certain states have used the media space to highlight the weaknesses of the West in crisis management, while at the same time, they have covered up their own shortcomings. The objective of such influence operations is to feed public mistrust in democratic governments and portray authoritarian systems as much more efficient in all aspects of societal life. One of the areas targeted by these operations is the Western Balkans. This media space has been a particularly fertile ground for conspiracy theories and filled with disinformation about the pharmaceutical industry, the origin of the virus and the purpose of vaccines. Given the linguistic similarities of the South Slavic languages, the disinformation operations in the Western Balkans media space have also targeted public opinion in the Republic of Croatia.

Since the outbreak of the pandemic, Russia and China have moved on from *mask diplomacy* to *vaccine diplomacy*. Vaccine diplomacy was supported by state-controlled media with the aim of reducing public trust in vaccines developed in the West and the trust in the EU institutions.

The pandemic has also revealed the weaknesses of health care systems in crises. In some states, this has led to procurement of inadequate or faulty medical equipment. The pandemic experience has reinforced the importance of human and material resources, it has highlighted the importance of resilience of the heath care systems and confirmed the need for available scientific, R&D and manufacturing capacities in dealing with new health related challenges.

Terrorism remains a significant threat to Europe

At present there are no identified direct terrorist threats to Croatian institutions, citizens and interests coming from terrorist groups / organisations (irrespective of their ideology). Terrorist threat, i.e., the threat of organised attacks by terrorist groups remains low, although the probability of a terrorist attack (primarily carried out by independent perpetrators) cannot be ruled out.

ISIS and Al-Qaeda remain the two most significant terrorist threats to Europe, despite the fact that they have been considerably weakened and their capacity for external operations/attacks has been reduced. In the EU, the level of threat from Islamist terrorism varies from low in Central and Eastern European states, to medium or high in most Western European states.

In 2020 the EU member states reported to Europol a total of 57 carried out, failed or prevented terrorist attacks. Moreover, the United Kingdom reported 62 terrorist incidents and Switzerland reported two probable attacks. The total number of terrorist attacks remained approximately on the same level compared to 2019, with an increase in the number of successfully carried out attacks. In the terrorist attacks in 2020, there were 21 fatalities in the EU, three in the UK and 1 in Switzerland.

As in the previous years, the primary terrorist threat to Europe continues to come from radicalised individuals inspired by the Jihadist ideology. These are the so-called lone wolves, whose behaviour is unpredictable, without direct affiliation with terrorist organisations, but who could carry out a terrorist act independently, triggered by publicly announced calls by terrorist groups to carry out attacks. These traits make them difficult to identify as threats prior to committing a terrorist act.

These are also individuals who are already present on the EU territory and use widely available weapons to carry out their attacks (melee weapons, cars). All terrorist attacks in 2020 were committed following this method, with the exception of the Vienna attack on 2 November 2020 where firearms were used. Apart from the targeted murder of teachers in France, all victims of Islamist terrorist attacks were bystanders or security forces. Terrorist attacks in France demonstrate all the fanaticism and brutality of attacks committed (close combat weapons and beheading were used).

All Islamist attacks in 2020 in Europe were carried out by lone wolves, predominantly EU nationals and ISIS supporters, but without any real affiliation with terrorist organisations. At the end of the year, an incident was recorded in the Republic of Croatia, involving a mentally ill self-radicalised individual who had attempted to escape a psychiatric hospital and in the process attacked bystanders and police officers with scissors.

In addition to Islamist ideology, and in line with European trends, a security risk for the Republic of Croatia also comes from (self)radicalised individuals with extreme right-wing violent orientation, frequently very young and from dysfunctional families and communities. In October 2020, a self-radicalised individual committed an armed attack, with characteristics of a terrorist attack, on the seat of the Government of the Republic of Croatia on Saint Mark's Square, injuring a police officer in the process. Collected intelligence point to the fact that this was an individual with dissociative/bipolar disorder, which explaines committed suicide some 20 minutes after the attack.

In total, four attacks motivated by right-wing extremism were recorded in the EU in 2020. The attack in Hanau, Germany carried out in February 2020 was successful, with the lone wolf attacker killing 9 people. Planned attacks in Germany, Belgium and France were prevented.

All planned attacks inspired by left-wing extremist and anarchist ideology in the EU were prevented, almost all of them (24) in Italy and one in France.

Outside Europe, the greatest terrorist threat to European nationals and interests remains in crisis and destabilised areas with active ISIS, Al-Qaeda and affiliated cells (Middle East, North Africa, Sahel, Horn of Africa, Arabian Peninsula and Central and Southeast Asia). Despite military defeats in Syria and Iraq, ISIS has continued with active presence in crisis areas and is still capable of carrying out major terrorist attacks. On 26 August 2021 ISIS carried out a terrorist attack near the Kabul airport, killing over a 100 persons, including 13 American soldiers.

On 28 June 2021, SOA Director Daniel Markić spoke on Croatia's contributions to the fight against terrorism at the High-Level Conference of Heads of Counter-Terrorism Agencies of UN Member States

A continuous security threat to the Republic of Croatia comes from regional members and supporters of radical Islamism within Western Balkan communities which also include individuals who had failed to join I

SIS / Al-Qaeda in the crisis areas, as well as returning Jihadists and individuals convicted and serving prison sentences for terrorist acts, some of whom have already been released or are about to be released from prison.

Over 200 individuals convicted of terrorist attacks in connection to Jihadi terrorism are set to be released from prisons in Western Europe in 2023. Terrorist offenders rarely go on to deradicalise and pose a potential security threat after they serve their sentences and are released from prison.

Repatriation of ISIS fighters, their wives and children to Western Balkan states was halted due to the pandemic outbreak, but the process is expected to continue. Up to now, approximately 450 (out of roughly 1,000 individuals who had gone to Iraq and Syria) have returned to the Western Balkans countries. Approximately 300 individuals are still in Syria. No individuals from the territory of the Republic of Croatia have gone to the area. Several individuals with dual Croatian citizenship (with the exception of one individual) have been identified as held in prison camps under the control of the Syrian Kurdish forces. The camps accommodate several thousands of women and children, the vast majority of whom are highly radicalised and loyal to ISIS, where they raise their children in such an environment.

The co-called para-jamaat communities are still operating in the Croatian neighbourghood. They preach radical interpretation of Islam, fail to recognise the official Islamic communities and the democratic order in their home country, and endorse violence in the service of alleged protection of Islam. Supporters of radical Islam from Western Balkan states who reside in Western European states use the territory of the Republic of Croatia as as transit route.

An ongoing security risks arises from the possibility of terrorist groups using the Balkan migration route.

Military preparation (a practical
article on manual preparation
of bombs and weapons with
materials available in the market)

ISIS and Al-Qaeda have been persistently urging their supporters to engage in terrorist attacks, which would expose the pandemic-affected Western societies to even greater security threat. For instance, one Al-Qaeda - affiliated magazine ran an feature at the end of 2020, exploring various methods of attack in the West. The feature focused on poisons and arson.

Readers were urged to exploit the outbreak of the COVID-19 pandemic in the West for various forms of terrorist activity - ranging from using face masks to hide their identities during murders and robberies, to giving out face masks soaked in poison to passers-by. The piece argued that streets emptied by restrictive measures should be used for arson.

The central operative section of the magazine provided instructions for putting together an upgraded version of a Molotov cocktail. If closely followed, such instructions would result in a more lethal version of the standard gasoline - based device.

The magazine urged Muslim hackers to take advantage of the fact that West relies on AI and encouraged Al-Qaeda's cyber army to hack into computer systems in the defence industry, banks and nuclear facilities. The magazine also announced next issues, and contained a link that enables communication with readers.

Growing extremism in the pandemic

No type of extremism, regardless of its ideological, religious or national grounds, has gained wider public support in Croatia and there is very little potential to undermine democratic rule of law, cause violence, incidents or conflicts on a larger scale.

In the context of the pandemic, time spent in social isolation and increasingly online, intensifies the risk of access to extremist content and self-radicalisation. Individuals who suffer from mental health issues are at greatest risk of self-radicalisation, as they are particularly vulnerable to the adverse impacts of the pandemic. Such individuals, obsessed with extremist views, could also engage in terrorist activity.

In addition to Islamist and ideological extremism, the outbreak of COVID-19 pandemic has fuelled the emergence of various conspiracy theories whose advocates have been becoming susceptible to other radical ideas as well. Economic and social insecurity favour the development of all forms of radicalism in society. Individual perpetrators of terrorist attacks are often socially marginalised, and their social and economic perspective has been limited even further by the impact of the pandemic.

Despite the fact that Islamist extremism continues to represent the greatest security risk to Europe, in recent years, some Western states have seen a rise in cases of the so-called far-right terrorism, i.e, armed attacks targeting primarily minorities and foreigners. As with other security challenges, this European phenomenon reflects on the security situation in the Republic of Croatia. An armed attacked carried out by an individual perpetrator on the seat of the Government of the Republic of Croatia in October 2020, had some features of a far-right terrorist attack.

Some European states, primarily Italy and Greece, have experienced activities of left-wing and violent anarchist groups and individuals.

The Internet technologies allow such extremist actors to connect and network more. These possibilities are exploited both by Islamist cells, and by the radical European right-wing and left-wing scene.

The behaviour of a small group of individuals with extremist orientation in the Republic of Croatia is mostly channelled into promotion of neo-fascist ideology and conflict (up to now in the virtual space) with members and individuals of opposing ideologies. Growing online presence of virtual extremist groups and individuals who promote violence fuels the risk of radicalisation. For instance, within a smaller online group with younger membership there has been a noticeable trend of promoting violent neo-Nazi ideology that comes from Western extremist circles.

Greater Serbia-related extremism has been continuously present in certain neighbouring states, expressed as the denial of territorial integrity and sovereignty of the Republic of Croatia and neighbouring states, advocating the restoration of the so-called Republika Srpska Krajina and promoting intolerance towards other peoples or denying their identities. Such Greater Serbia-related and extremist messages have been occasionally publicly delivered by political and media figures from neighbouring states using social media or public appearances.

Most extremist messages and publications, irrespective of ideological affiliation, take place in the virtual environment. The authors of such extremist messages frequently do not even reside in the Republic of Croatia.

Violent clashes between members of extreme sports fan groups have continued. These conflicts disrupt public order and destabilise local security in certain communities. When it comes to fans of clubs from Croatia and Serbia, these clashes take on the character of inter-ethnic conflict.

The attack on Saint Mark's Square on 12 October 2020 has revealed all the complexity and unpredictability of the phenomenon of self-radicalised individuals, the so-called lone wolves. These potentially dangerous individuals are, irrespective of their ideology, prepared to commit terrorist attacks. They are self-indoctrinated mostly online, and often suffer from untreated metal disorders, introverted and violent to their close community.

The greatest challenge includes those individuals who are "invisible" to the security agencies, because they do not engage in contact with like-minded people and they do not publish extremist content. They can, therefore, remain unidentified up until the attack. This phenomenon is particularly dangerous in the context of the availability of weapons that had not been decommissioned from the war.

In line with Western European experiences, the radicalisation process is very complex and multi-layered, but it can be surprisingly rapid and efficient. Radicalisation in society is driven by dissatisfaction of certain segments of the society, poor socio-conomic conditions, lower educational levels, mental disorders, dysfunctional family and social environment.

A major factor is (self)radicalisation is extremist propaganda spread online and in the social media. The Internet is the key medium of communication, recruitment and radicalisation of supporters (irrespective of ideology). Its impact has grown significantly in the context of isolation imposed by restrictive measures in connection with the COVID-19 pandemic.

Combating radicalisation is a societal issue that requires a multidisciplinary approach with active participation of family, close community, educational institutions, state authorities, social services, health care, scientific institutions, media and other social and political stakeholders in order to diagnose the problem at an early stage while it is still reversible. The role of SOA is the prevention of radicalisation is in early warning, i.e., in detecting the process, identifying radicalisation actors and reporting to the authorities.

Foreign intelligence is continuously present

Intelligence, although mostly obscured from the public, is continuously present. The Republic of Croatia is the subject of intelligence interest of certain states that perceive Croatia as a security, economic or political rival, either individually or as NATO and the EU member.

The Republic of Croatia is subjected to intelligence collection in the interest of certain foreign intelligence agencies, but also to (dis)information operations aimed at shaping the public opinion, international position and the decision-making processes in Croatia.

There has been a surge in information operations, that is, dissemination of fake news to undermine the stability of state institutions and the region, to portray the Republic of Croatia as unreliable NATO and EU member and a factor that destabilizes neighbouringh countries and obstructs euroatlantic integrations. At the same time, intelligence operations are carried out to create discord inside the Euro-Atlantic organisations that Croatia is a member of.

News websites and social media platforms are exploited in this dissemination of information, and certain operations include spreading malicious theses on SOA and the Republic of Croatia even in scientific institutes, thus lending credibility and legitimacy to fake news and misleading statements. One such thesis is that the Republic of Croatia is the “major impediment and a factor threatening the peace in the West Balkans”.

Malicious and fake news that manipulate the efforts in the prevention and suppression of international terrorism pose a particular security burden, as was the case of fake news alleging that SOA and the Republic of Croatia were arming terrorists in BiH.

In terms of intelligence collection, the main points of interest for foreign intelligence in the Republic of Croatia include intelligence collection on security, political and economic processes in Croatia, in particular those that pertain to some open issues, as well as Croatian policy towards Western Balkans.

Foreign intelligence is also directed at intelligence collection in relation to Croatia’s membership in the EU and NATO. In this respect, states that perceive NATO and the EU as a security challenge or threat, perceive the Republic of Croatia as a point of intelligence interest.

Foreign intelligence is also focused on the strategic positioning of the Republic of Croatia in emerging and developing industries, such as new technologies and renewable energy sources, and projects that are of strategic importance for the region such as large-scale infrastructure projects.

In addition to traditional intelligence collection and operations, in recent years there has been a surge in cyber attacks on the information infrastructure of the state bodies for the purpose of espionage and data theft.

Although intelligence operations are clandestine in nature, a large number of cases have been publicly exposed recently. Most of the cases which have been broken by the media relate to the operations of Russian intelligence services in the EU and NATO member states. Officers of the Russian military intelligence service GRU are suspected of the deadly blasts at munition depots in the Czech Republic in 2014 and in Bulgaria in the period from 2011 to 2020. Earlier, GRU operatives had been suspected of an assassination attempt on the former GRU officer Sergei Skripal and his daughter in England (2018) and Bulgarian arms dealer Emilian Gebrev (2015). In April 2018, Dutch authorities arrested and expelled four GRU operatives who had been trying to hack the headquarters of the Organisation for the Prohibition of Chemical Weapons. In Croatia’s neighbourhood, GRU officers have been associated with the coup d’etat in Montenegro that was attempted in October 2016, on the eve of parliamentary elections and accession to NATO.

В ЄВРОПІ ВІДБУВАЛИСЯ ЗУСТРІЧІ ЄГОРОВА З ШАЙТАНОВИМ ТА ЗАВЕРБОВАНИМ НИМ АГЕНТОМ – «Н»

In May 2020, Ukrainian agency SBU arrested its General Valery Shaitanov on charges of collaboration with Russian intelligence services. SBU disclosed that the collaboration included the organisation of assassinations in Ukraine and that Shaitanov had also met with Russian intelligence officer on the territory of the Republic of Croatia.

Besides active efforts to combat covert operations of foreign intelligence, SOA is also tasked with enhancing counterintelligence and raising awareness of the security culture among individuals who could be exposed to foreign intelligence.

State-sponsored cyber attacks are increasingly prevalent in espionage

State-sponsored cyber attacks are organised and contracted by certain states, and they directly or indirectly engage a variety of organised actors to carry them out. These attacks are directed at carefully selected targets, which were previously well examined, and are carried out by state-sponsored cyber APT (Advanced Persistent Threat) groups that are closely affiliated with security-intelligence systems of certain states. Such cyber attacks primarily target the EU and NATO member states.

In recent years, the Republic of Croatia has been the target of several dozen state-sponsored cyber attacks. The nature of these attacks is best illustrated by the fact that the majority of them were attempts to hack into information and communication systems of the Ministry of Foreign and European Affairs and the Ministry of Defence.

Furthermore, such cyber attacks are used globally to disable and damage network and information systems which are relevant for key social and economic processes (critical infrastructure), which causes reputational damage to the state or large national companies and disrupt regular processes of societal importance.

States that sponsor cyber-attacks align cyber-attack targets with their national economic strategies and engage in efforts to profile certain APT groups for attacks on specific state bodies or economic sectors such as the energy or the aviation industry. Stolen intelligence is then used to further their political agenda or in industrial development (for example to copy industrial products). A series of cyber attacks on Western pharmaceutical companies was recorded during the outbreak of the COVID-19 pandemic, and throughout the process of vaccine development.

Cyber attribution is a process of assigning responsibility for cyber attacks which had caused a cyber incident or a cyber crisis. It is the result of a series of technical and analytical activities carried out by competent authorities at the technical and security-intelligence level. The overall aim is to discover and determine facts, connect them and assess probabilities, to facilitate evaluation and decision-making on the attribution of a cyber attack and to enable the choice of diplomatic instruments to be applied on each specific case of public attribution. The attribution can be performed in the national, the EU or NATO context.

In 2020, the EU commenced the process of public attribution for a series of cyber attacks attributed to actors from the Russian Federation, China and North Korea, including Russian military intelligence and a number of affiliated individuals and several state-sponsored APT groups from the three states. Appropriate sanctions have subsequently been imposed.

In response to the growing challenges in the cyberspace, SOA launched the Centre for Cyber Technologies in 2019. The purpose of the centre is to protect the national cyberspace. The

Centre for Cyber Technologies uses the SK@UT system to register several hundred thousand security indicative events on a daily basis.

In 2020, the Centre for Cyber Technologies confirmed 12 state-sponsored cyber attack on targets in the Republic of Croatia. Along with the growing trend in the number of attacks, the number of APT groups targeting the Republic of Croatia has also increased. The primary reasons driving this trend are Croatia's Presidency of the EU Council in the first half of 2020, the outbreak of the COVID-19 pandemic as a backdrop for cyber attacks and the considerably heightened visibility of the national cyberspace realised in the process of expanding the scope of the SK@UT system.

[SK@UT]

On 1 April 2021 the Government of the Republic of Croatia adopted a Decision on measures and activities for advancing national capabilities for timely detection and protection against state-sponsored cyber attacks, APT campaigns and other cyber threats. In order to ensure further protection of the national cyberspace, the decision permits key service operators, digital service providers, critical national infrastructure operators and other legal entities registered in the Republic of Croatia to join the SK@UT system.

The SK@UT system was developed jointly by SOA and the Information Systems Security Bureau with the purpose of advancing national capabilities for timely detection and protection against cyber attacks.

SK@UT serves as the central system for detection, early warning and protection against state-sponsored cyber attacks, APT campaigns and other cyber threats, consisting of a distributed network of sensors installed in key state bodies and legal entities.

This allows detection of sophisticated cyber attacks at the earliest stages and in any segment of cyberspace covered by the network of sensors. This approach combines the most complex technical systems for cyberspace protection and security intelligence capabilities, diminishing the risk of compromising key national information resources.

A further expansion of state-sponsored cyber attacks is expected, in particular within the framework of global processes related to the implementation of 5G technology and the current status of the COVID-19 pandemic. State-sponsored cyber APT groups have been persistently trying to adapt their tactics, techniques and procedures to the responses delivered by their targets, in an attempt to remain efficient.

When preparing and carrying out attacks, state-sponsored cyber APT groups primarily aim to exploit weak security awareness and education of users, and underdeveloped cyber security policies of public bodies and legal entities. This means that preventive measures carried out within all bodies (password management policies, software updates, two-factor authentication for emails, use of VPN for external access to servers) greatly reduce the possibility of cyber attacks and the probability of compromising information systems. The work of the Centre for

Cyber Technologies is focused on, among other things, identifying best practices in responding to detected state-sponsored cyber attacks.

Throughout 2020 and 2021 exceptionally sophisticated global cyber attacks on business management software companies have taken place, with the objective of compromising a large number of their users. In December 2020, a global supply chain cyber attack using SolarWinds software was detected. The SolarWinds software compromitation, used by approximately 18,000 businesses worldwide, was carried out in the period between March and May 2020 and the sophisticated breach was only discovered six moths later.

Another example of global cyber attacks is the exploit of 0-day vulnerabilities of Microsoft Exchange system that Microsoft reported in March 2021. More than 100,000 businesses globally were exposed in the attack.

Such cyber APT attacks underscore the high sophistication of state-sponsored APT groups and highlight the necessity of systematic application of cyber security measures at a wider national level.

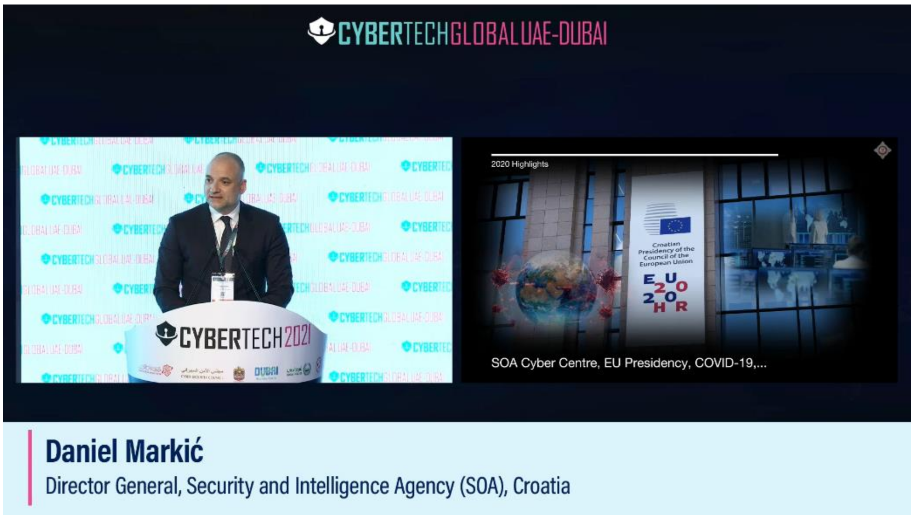
Another worrying trend is the accelerated transfer of sophisticated tactics, techniques and procedures used by state-sponsored APT groups to organised crime groups who then exploit them in malware attacks that target the financial sector or for ransomware targeting economic subjects.

Such attacks are directed at large and strategic companies. In the event of a successful attack, company operations and access to data are blocked, financial losses are inflicted and they are additionally blackmailed and threatened with public disclosure of the stolen business data. In May 2021, a malware attack was conducted on the Colonia Pipeline, the largest pipeline system which supplies oil to the US East Coast. Due to fuel supply disruption, the US authorities declared a state of emergency. In July 2021 a ransomware attack was carried out on the Kaseya software supply chain, which exposed 1,500 companies using Kaseya software.

In the early 2020, a malware cyber attack was carried out on the Croatian oil company INA. Besides economic harm that companies experience from such attacks, they also have an intelligence dimension, given that some companies possess classified business information and have access to trade secrets, personal and financial data on their customers, national analytics and sensitive industry insights.

Cyber resilience becomes the key to protecting national security

On 6 April 2021 SOA Director gave a presentation on the role of the Agency in the protection of the national cyberspace, at the Cybertech Global 2021 conference in Dubai, United Arab Emirates. Cybertech Global is cyber industry networking platform conducting industry related events and facilitating discussions about the latest technological innovations, and solutions in combating threats within the global cyber arena. It is one of the largest conferences of this kind in the wold. The conference features cyber industry executives, leading decision-makers from a wide range of states, technology experts, business leaders and many others.


CYBERTECHGLOBALUAE-DUBAI
CYBERTECH2021
2020 Highlights
SOA Cyber Centre, EU Presidency, COVID-19,...
Daniel Markić
Director General, Security and Intelligence Agency (SOA), Croatia

SOA Director's presentation is featured in full below:

As the director of an intelligence agency, whose job it is to look out for trends, it is my duty to alert the film industry of one great change they should prepare for!

Secret service operatives in all those blockbusters who jump on rooftops, race the streets of global cities, dodge machine gun bullets fired at them by bad guys and save the world from evil scientists will have to be replaced with smart young men and women who save the world clicking their mouse buttons, sitting in their ergonomic chairs in front of larger screens.

Croatian intelligence operatives are, of course, fit and ready as much as those blockbuster operatives, but we have recently been training more and more of those operatives who save the world with a click of their mouse.

Technological developments have forced us to step out of the mysterious world of intelligence into the public arena. And that is good; our citizens need to know that there are people and agencies working to protect their security in the cyberspace.

Cyber resilience has become the key to protecting national security in the digital age. However, we need all stakeholders involved in building a cyber-resilient community. It is therefore crucial to speak publicly about our role in enhancing cyber resilience. We believe that we are the backbone of this resilience.

At SOA, we kicked off 2020 very ambitiously. In January, we presented our Centre for Cyber Technologies to the world in Tel Aviv, and Croatia took over its first Presidency of the EU Council. Our ambitious plans in cyber resilience coincided with the Presidency, as we estimated that the occasion would capture greater interest from malicious state-sponsored cyber APT groups.

In the meantime, as the outbreak of the COVID-19 pandemic halted processes in the physical world, all important processes migrated to cyberspace. It was a signal that expectations from our Cyber Centre would rise significantly.

The Centre for Cyber Technologies, set up in 2019 within our Agency, has proven to be very efficient in the rapidly changing national and global circumstances in 2020.

Our assessments werecorrect: in 2020 the number of state-sponsored APT attacks in the Croatian cyber space doubled. The number of APT groups targeting Croatia also doubled.

Tactics, techniques and procedures (TTP) employed by APT groups have changed, and now both traditional and modern TTPs are used. The intention of the attackers is to minimize the digital footprint that they leave and thus obstruct the possibility of target states to attribute the attacks. Their aim is to avoid diplomatic and economic sanctions that have been becoming increasingly inconvenient for states that sponsor APT cyber attacks.

This problem is highlighted in the context of the fact that the European Union started imposing sanctions for cyber attacks last year. The sanctions were imposed against six individuals and three institutions from Russia, China and North Korea, including the Main Centre for Special Technologies of the Russian military intelligence service GRU.

Our membership in the European Union can help us reach this goal more easily, even though there are many challenges ahead of us. The new EU package of 16 December 2020, which consists of the NIS2 Directive, EU Cybersecurity Strategy and the Directive on the resilience of critical entities, is another challenge for national security in terms of further adaptation of national cyber organisations and coordination capabilities.

The strategic and technological risks associated with the launch of 5G have already started emerging in the implementation of the new generation of mobile network, as it merges the previously separated worlds of telecommunications and the Internet into a single cyberspace.

We are facing the Fourth Industrial Revolution with a cyber-physical approach set to transform our economies in the emerging digital era.

Recent global state-sponsored cyber attacks, the SolarWinds hack as the most serious attack on the global supply chain, and four 0-day exploits of Microsoft Exchange Server have exposed the challenges we will all be facing moving forward.

Resilience to threats is our common national objective and the mission of my Agency is to protect national security. Cyberspace has long been an integral part of national security. We develop resilience in the physical world, and similarly we are committed to building cyber resilience. With this purpose, we will continue to develop our Centre for Cyber Technologies.

As a security and intelligence agency, we hold several advantages; we have clever young men and women who are trained to protect the national security with a click of a mouse, we are ready to implement technological platforms for protection, we have developed a network of bilateral and international partnerships to advance our horizons and capabilities, and finally, we have the one thing that sets us apart from others - we have intelligence.

Therefore, all the ingredients to make it a success are there. It is now up to us to combine them and I look forward to being on the first line of defence of our national cyberspace.

Economic security is an important aspect of national security

A strong and resilient economy underpins national security. Economic security and a framework that enables economic development and advancement are essential for any state.

SOA monitors national, regional and global economic processes and trends that might reflect on the economic security, position and interests of the Republic of Croatia. As part of this task, SOA continuously monitors activities of numerous state and non-state actors in the economic sphere, as their behaviour might have an adverse impact on the interests of the Croatian economy, both domestically and internationally. In doing so, we consider the risks associated with intelligence and hybrid operations directed against Croatian or common European interests under the guise of legitimate economic activities. These activities include espionage, intellectual property theft, attempts to create economic dependence, media manipulation and the like.

The landscape of economic and financial crisis intensifies the risk of money laundering, as dubious investors and crime groups set up business operations under the pretense of job creation. Therefore, the available national mechanisms are being deployed more intensively in order to verify investments and prevent dubious investments.

The economic crisis caused by the outbreak of the COVID-19 pandemic has caused business hardship in many European strategic companies and the EU has been taking measures to protect them from hostile takeovers by non-European actors originating in states whose governments often own such organisations or make illegal and clandestine state subsidies to their business.

One of the significant segments of these activities is monitoring cyber security in the economic sphere, where the Agency deploys its capabilities to protect strategically important economic entities from advanced cyber attacks.

SOA monitors economic and financial processes that might impact the position of Croatian economic entities internationally, as well as trends and processes that could undermine the security of Croatian economic subjects that operate in unstable areas of the world.

Energy security is an integral part of national and international security. In that respect, SOA has engaged in monitoring processes in the energy sector. Energy security is a pertinent European and global security issue.

The European Union is particularly sensitive to the issue of security in the supply of natural gas. The EU consumes nearly 500 billion cubic metres of natural gas annually (the consumption declined to around 400 billion in the pandemic), and 90% of it is imported. Approximately 40% is imported from Russia, while the import from the USA has risen to 7% of the total European consumption.

Although asymmetric, the EU natural gas dependence on Russia is two-way, as Russia is considerably dependent on the EU customers. Therefore, the EU energy transition and future reduced reliance on fossil fuels, together with new carbon tax, could create challenges for the Russian economy.

The commissioning of the LNG Terminal on the island of Krk represents a remarkable factor in energy independence and diversification of gas sources for the Republic of Croatia and the neighbouring states. The construction of the South Gas Interconnection has commenced, and the pipeline will connect Croatian and Bosnian gas systems. A more resilient Croatian gas system will contribute to efforts in enhancing the energy security and stability in the neighbouring states.

The floating LNG terminal in Omišalj and the connecting pipeline Zlobin - Omišalj were commissioned on 29 January 2021. The connecting pipeline will be used to transport liquefied natural gas to the Croatian gas transmission system, giving both Croatia and Europe a new competitive route for the supply of natural gas.

Corruption undermines the state budget and the economy of the Republic of Croatia

In line with the relevant legal provisions in the Republic of Croatia, specialized police bodies and State Attorney's Office (DORH) are in charge of the suppression of corruption and related criminal proceedings (along with courts which belong to a separate branch of government).

Corruption and economic crime exert adverse impacts on the state budget and the economy, undermine public trust in institutions and political decision-making. As such, they are a potential threat to national security. Therefore, in cooperation with other competent bodies, SOA plays an important role in the prevention and suppression of corruption and economic crime. SOA carries out operative activities with the purpose of collecting intelligence that may point to the existence of corruption and crime. In such events, the Agency reports its findings to competent authorities (Ministry of the Interior, State Attorney's Office, Croatian State Attorney's Office for the Suppression of Organised Crime and Corruption, Ministry of Finance, Tax Administration).

Not only does corruption have an adverse social impact but it also poses a significant threat to economic development of the Republic of Croatia. It hinders fair market competition, slows down economic growth and leads to state budget and public finance shortfalls. In the long-term, corruption reduces public trust in the constitutional order and the efficiency of state authorities.

Corruption, defined as the misuse of public and state resources for personal gain, is mostly associated with abuse of position and authority in public administration, state institutions and authorities, and public companies.

Members of organised crime groups seek to corruptly act against government officials and managers in public companies at various levels in order to entice them to engage in malpractices and favour organised crime. Attempts to corruptly influence political, judicial, economic and other processes, as well as decision-making in matters of public interest, are particularly worrying. Public procurement processes are areas with heightened risk of their misuse, corruption and economic crime, specifically in the segment of large infrastructure projects.

The sphere of corruptive activities and economic crime also includes the interest in investing capital of unknown origin in the Republic of Croatia, with a risk that it could in effect be laundering of illegally obtained funds. These particularly complex forms of corruption, misuse and misconduct in business, cash extraction and money laundering also have an international dimension. The risks pertaining to money laundering, financial fraud and other forms of economic crime increase at times of economic downturns such as the one that was caused by the COVID-19 pandemic.

The issue of war crimes and missing persons in the Homeland War remains open

At the time of this report, the fate of 1,458 people and the burial locations of 400 fatalities from the Homeland War remain unknown, making a total of 1,858 open unresolved cases. SOA has continuously cooperated with competent authorities (Ministry of Croatian Veterans, Ministry of the Interior, VSOA) in order to determine the fate and burial locations of missing persons.

This is an extremely sensitive humanitarian issues, which also impacts inter-ethnic and international relations.

SOA continues to focus on efforts to identify the perpetrators, victims, witnesses and circumstances of war crimes committed during the Homeland War. The Republic of Croatia has issued arrest warrants for individuals suspected of war crimes who have been on the run from criminal liability. SOA has been focused on establishing the place of residence of these individuals, with the aim of prosecuting them before judicial bodies.

Global geopolitical and economic rivalries are dynamic and uncertain

Global geopolitical conditions have been influenced by growing regional rivalries in the context of a globalized economy marked by historically high interconnected and interdependent economic relations. During the Cold War, the West and the USSR operated separate economic systems with almost no mutual trade relations. Today, China, Russia, the USA and the EU have developed significant trade relations. China, the EU and the USA are the largest trade partners to one another. At the same time, Western states and China disagree over a number of economic and trade issues, and relations with Russia remain burdened with a number of political and economic matters, for instance the sanctions imposed on Russia over the Crimea annexation.

Global economic situation has been marked by a significant shift in economic activity to the Asia-Pacific region. The economies of present-day EU member states and the UK accounted for 28% of the total global GDP in 1989, the USA accounted for 22%, and China stood at only 4%, Thirty years later, the EU and the UK account for 16%, the USA stands at approximately 15%, and China has reached 18% of the total global GDP.

From the political perspective, there has been a noticeable competition between the Western liberal point of view and the Eastern authoritarian approach to the development of political and social value systems. In that respect, the EU has characterized China as an economic competitor and a systemic rival that promotes alternative models of governance.

There is a number of unresolved crisis hot spots in the EU neighbourhood. The EU's future relationship with Russia and China remains an open question, as well as the issue of energy security and the protection of fair market competition. While it has been consistently relying on NATO and the Euro-Atlantic partnership, the EU has continued to enhance its own defence capabilities by engaging in several military and defence initiatives.

The main issues of the US foreign security policy have included ongoing tensions with Russia, rivalry with China, relations with Iran and its nuclear programme, and the withdrawal from Afghanistan, where the US military presence provided stability to the wider Centra Asia region. The newly inaugurated administration in the USA has announced its intentions to renew the alliance network that it had been developing across the world.

The global dominance of the USA has been challenged by China, as it sets out to become the dominant global power. China has been promoting its model of government as an alternative to liberal democracy. Despite the outbreak of the pandemic, China has managed to sustain strong economic growth and it could emerge from the pandemic as the primary economic partner to a number of states.

In addition to enhancing its military capabilities, China has continued to purse a global economic policy. Growing reliance of global supply chains play to China's favour. The major project of China's economic policy is the Belt and Road Initiative launched in 2013, which has been focused on building a trade and infrastructure network in over 60 states in Asia, Africa and Europe. As part of the Initiative, Chinese state-owned banks engage in financing of the infrastructure projects by providing loans to developing countries. China has become the world's leading oil importer, supplying 40% of its oil demand from the Persian Gulf, while at the same time, the USA has decreased its dependence on oil imports from the Gulf.

China's relations with the West are burdened with the open issues such as the relationship with the USA, Taiwan's status, development of transport and military capabilities in the South China Sea, China's policy towards Hong Kong and the Uighur minority as well as trade issues such as intellectual property, expansion of new technologies, state subsidies and state ownership of companies, market competition and so on.

Russia has been predominantly focused on internal stability and on maintaining a dominant position in its immediate neighbourhood by reinforcing relations with members of the Commonwealth of Independent States, which it regards a sphere of influence. However, this dominance has increasingly been pressured by the rise of Chinese influence in Central Asia and growing Turkish influence in the Caucasus in the wake of the Azerbaijani-Armenian war and in Central Asia. Although Turkish-Russian relations, in particular economic relations, remain stable, their interests have collided in some crisis hot spots such as Libya and Syria. Russian policy relies on the great military capabilities as the state continues to invest in the modernisation of the forces. The Strategic Arms Reduction Treaty (New START) between the USA and the Russian Federation has entered into force and it is expected to last until 2026.

Russia has continued exerting efforts to limit the influence and prevent the enlargement of NATO and the EU in East and Southeast Europe. The majority of Western states have continued imposing sanctions on Russia because of the Crimea annexation. The relations with the West have been strained because of indications of Russian engagement in physical elimination of political opponents, hybrid operations directed at Western states, and cyber-attacks originating in the Russian territory.

Following the EU imposed economic sanctions over the annexation of Crimea, Russia has been turning its economic focus to Asia. This is a long-term and challenging project, in particular in relation to China which has been increasing the gap between two economies, most notably in the competitive areas.

Encouraged by their mutual opposition to the global US-West dominance, Russia and China have been reinforcing bilateral relations. At the same time, their relations have been pressured by China's efforts to suppress Russian economic interests in Central Asia. The land route of the Belt and Initiative cuts across this area. In 2021, railway transport between China and Europe via Central Asia nearly doubled. China is Russia's single largest trade partner, while Russia does not even make it on the list of China's top 10 trade partners.

Global security landscape is also impacted by other long-term processes including the growing impacts of climate change and its consequences, excessive depletion of resources and destruction of nature, loss of agricultural land and biodiversity, outbreaks of communicable and other diseases. These processes cause or reinforce other security challenges such as population migration, social tensions, intra-state and regional conflicts, crime, institutional and social collapse in unstable states and the like.

The Western Balkans undergoes a slow stabilisation process

Croatia’s southeast neighbourhood (Western Balkans) remains burdened by uncompleted stabilisation processes. This is an area marked by unresolved interstate and inter-ethnic issues, with difficulties arising from insufficient implementation of reforms in connection with their expressed intention of joining European integrations. Adverse political and economic conditions create a background for the strengthening radical and extremist tendencies, and social rifts in these fragile societies.

Developmental outlook of this area is further impacted by emigration from the Western Balkan states. This trend is expected to continue, and along with other trends it may carry security implications, which have already come to light during the pandemic outbreak in the form of labour shortages in the health care.

Social and inter-ethnic tensions may cause further conflict and incidents, in particular in areas with unresolved ethnic relations.

Political situation in BiH continues to be marked by internal political instability, caused primarily by differing views that the constituent peoples hold on the future constitutional order of the state, principally the issues of further centralization, foreign policy priorities and the unresolved issue of the collective equality of the constituent peoples, as guaranteed by the Constitution. Ongoing tendencies to gradually repeal the fundamental principles of the Dayton Peace Agreement, such as diminishing the constitutional right of Croats in BiH, could adversely impact the position of Croats as the smallest ethic group in the state, political stability and inter-ethnic balance and undermine the democratic legitimacy of the state.

Failure to reach a Serbian-Albanian agreement on the issue of Kosovo continues to drive instability in the region. A particular source of uncertainty in the Western Balkans arises from the social rift in Montenegro, where a considerable part of political power is held by anti-NATO, pro-Serbian and pro-Russian parties, in opposition to the so-called sovereign pro-Western streams.

In the regional context, certain policy makers on the state level in Serbia have promoted the concept of the “Serbian World”, which would unify all Serbs in Southeast Europe as a political and even state entity under the political direction set by Belgrade. Such ideas, promoted directly by the leadership of the Serbian government, serve to further destabilise sensitive inter-ethnic and international relations in Southeast Europe, particularly in relation to BiH and Montenegro.

In certain neighbouring states, efforts have been made to publish and disseminate media and public narratives that challenge the legitimacy and legality of the liberating military operations undertaken during the Homeland War. Facts are distorted to systematically portray the Republic of Croatia as a state that had originated from criminal activity and the actions of quisling Independent State of Croatia (NDH) from the Second World War.

Organised crime that has originated in the Western Balkans has remained strong, entrenched in social structures and in corruptive interests and ties with holders of political offices.

Non-Western actors have also been keen to promote their political, military and economic interests in this area. These actors seek to identify and exploit institutional and social weaknesses of the Western Balkan states to their advantage by employing the so-called soft powers, with the aim of strengthening their influence and occasionally, to drive the change in ethic and religious structure of the population of some areas.

The threat of radical Islamism has remained constant, while the risk of terrorism has grown due to repatriation of Jihadists who had been captured in Syria and Iraq, particularly in the absence of successful deradicalisation. In certain Western Balkan states, Salafi Jihadist para-jamaat communities have remained active. They fail to recognise the official Islamic communities and the democratic order in the home country, endorse terrorist operations and incite hatred and violence against all *infidels*, including Muslim dissidents.

The situation in the Western Balkans has been further compounded by the significant migrant inflow. This has been particularly strong in BiH, which has been used by migrants as an illegal point of entry to Croatia and the EU.

The European landscape is marked by instability

The belt of instability that stretches along the southern and eastern neighbourhood of the European Union continues to pose a security challenge. The primary sources of instability are crisis hot spots such as Syria and Libya where rival policies and interests of regional powers come head-to-head. Unresolved frozen conflicts are a source of political tensions with sustained possibility of outbreaks of armed conflicts, such as the conflict in the Nagorno-Karabakh region in the autumn of 2020 or the Gaza Strip conflict in the spring of 2021.

Following the withdrawal of international forces from Afghanistan, the Taliban have recaptured the capital Kabul and the entire territory of Afghanistan after 20 years of guerrilla warfare. Afghan institutions and the armed forces have since disintegrated, and the Taliban have come into possession of large quantities of modern weapons and military equipment. The case of Afghanistan highlights the rapid pace and the dynamics of security changes across the world, and further developments in Afghanistan will depend on internal processes in the country, policies of Taliban authorities, including their views on human rights and international terrorism, and the actions of international (regional and global) actors in relation to the Taliban regime. Deteriorating security conditions in Afghanistan will also have an impact on other security challenges, such as migration pressure on Europe and regional stability in Central Asia.

Tensions between the conflicting sides and more frequent exchanges of fire have occasionally been reported in the Donbas region, eastern Ukraine, resulting in military and civilian casualties on both sides. At the same time, the negotiation process between the conflicting sides has been stalled.

Starting in October 2020, the EU has imposed a series of restrictive measures on Belarus, in response to irregularities in the presidential election, repression of peaceful protests and forced landing of an Ryanair flight to Minsk and subsequent detention of journalist on board.

The European Union is also interested in resolving open issues at its external borders and in the region, such as the delimitation issues and resource exploitation in the eastern Mediterranean, resolving active and frozen conflicts in the neighbouring states, Iran nuclear programme, illegal migration and the like.

The militarily situation in the long-term crisis hot spots in Syria and Libya has stabilised, and there are currently no significant armed conflicts taking place in those states. On the political side, there has been little significant progress in resolving the internal situations that had caused the civil wars, thus leaving both states divided among conflicting sides, despite the fact that a truce had been signed in Libya after months of intense armed conflict and that an interim government was formed in the UN-led process.

The Horn of Africa remains a crisis area. In Ethiopia, the conflict between the central government and the local government in the Tigraj region has escalated into an armed conflict, and the conflict continued despite the federal army occupying the region. This conflict could also have a destabilising impact on the neighbouring Sudan and Eritrea, which are already burdened with numerous security and economic challenges. Somalia has been experiencing ongoing conflicts between the central government, backed by the African Union military mission, against the Al-Qaeda associated militant terrorist organisation Al Shabab. Islamist terrorist groups with ties to ISIS and Al-Qaeda, have been active in the Sahel states such as Mali, Burkina Faso and Nigeria, and continue to pose a threat to the wider environment.

Certain processes in the European landscape may also have stabilising impacts, such as the normalization of relations between the State of Israel and several Arab states.

In addition to all the security challenges they are overload with, the states in this area have also been impacted by the consequences of the COVID-19 pandemic, which compounds all persistent social and economic difficulties that these societies have already been facing. This means that the already weakened institutions and societies may further deteriorate in stability.

The social and security processes that will continue to cascade to Europe include rising extremism that can escalate to terrorism, growing poverty and unemployment, greater migration pressure towards the European Union, intensified organised crime and other.

Organised crime becomes transcontinental

The European Union has estimated that revenue from criminal activities in the main criminal markets in 2019 amounted to 1% of the EU GDP, or 139 billion EUR. The main criminal activities in Europe include drug trafficking, theft and burglary, business and financial fraud, crime related to waste and pollution management, illicit arms and explosives trade, match-fixing and betting fraud, migrant smuggling and human trafficking, forging documents and money, intellectual property theft and product counterfeiting. Organised crime groups in Europe operate across state borders, with growing use of violence, in terms of frequency and severity.

A particular challenge in the field of organised crime is money laundering, i.e., attempts to legalise funds acquired through criminal activities. Organised crime groups have been constantly seeking new ways to legalise money acquired in illicit activity, and specialised groups have emerged that develop complex money laundering schemes - professional money laundering networks.

The COVID-19 pandemic is another example where organised crime groups have once again demonstrated how quick they are to adapt to new circumstances. During the outbreak of the pandemic, organised crime groups in Europe have pivoted their activities towards counterfeiting and distribution of goods in great demand, cybercrime, burglary and various types of theft.

They were quick to exploit and abuse demand for and shortage of certain types of goods, especially personal protection equipment and medical equipment (face masks, plastic gloves, disinfectants), by redirecting a part of their activities to this market. They have often exploited acute demand for these goods to disproportionately drive up the prices and realise enormous profits, and they have also distributed counterfeit products which did not meet the basic standards.

Organised crime groups have exploited the fact that during the pandemic most people in isolation spent more time online, which opened up new possibilities for cyber attacks and various forms of online fraud. Similarly, they have been persistently coming up with new ways to use new technologies for criminal activities, such as using cryptocurrencies for money laundering and blackmail pay-outs.

With easing epidemiological restrictions, certain criminal activities will gradually return to pre-pandemic levels.

According to EUROPOL estimates, more than 50% of all reported suspected members of organised crime groups are not EU nationals. Half of them are from EU neighbouring states: Western Balkans, Eastern Europe and North Africa

Organised crime has become a significant factor of instability in the Western Balkans, and in certain states such crime has had a marked impact on political conditions and decision-making.

Organised crime which has originated in this area has been cascading over into the Republic of Croatia.

Serbian-Montenegrin organised crime groups have a particularly prominent destabilising role in this process. These are highly organised groups, with numerous membership, internationally active and ready to commit all forms of criminal acts. They have also been associated with local sport fan groups, which are used to distribute narcotics. Some of those local fan groups, after years of illegal operations at lower organisational levels, have grown into criminal organisations with a hierarchical structure and extensive narcotics distribution chain, and have also developed cooperation with major crime groups in the region.

Organised crime groups have established transcontinental cooperation and have been supplying large quantities of cocaine from South America, which they have been shipping by sea to ports in SE Europe, hidden in containers on overseas ships.

In April 2021, in the port of Ploče, the police seized approximately 574 kg of cocaine that had been shipped in a container transporting bananas from South America. Furthermore, the Balkan area has remained the main transit route through which heroin in delivered to the EU.

Organised crime exploits a large number of migrants in the Western Balkans, and therefore, a great interest in illegal border crossing, to realise great profits from people trafficking.

The territory of the Republic of Croatia has been used by organised crime groups and individuals to traffic arms, mostly remnants from 1990s wars in SE Europe, to Western Europe. These weapons can be used for armed criminal activities and terrorist attacks, and there has been a constant risk of using the territory of the Republic of Croatia for trafficking components of weapons of mass destruction.

Illegal migration poses a long-term social and security challenge

The area of SE Europe remains to be the route used by migrants to illegally reach developed Western European states. Despite the decrease in the number of illegal migrant entries from Turkey to Greece, the intensity of illegal migration in SE Europe has been on the rise. However, there have been changes in migrant flows on the so-called Balkan route. Some of the migrant groups have redirected the route from Serbia to Romania and further on to Hungary and Western Europe. Nevertheless, this redirection has not reduced the pressure on Croatian borders, which has remained constant and has been consistently increasing in the summer months. A significant number of migrants is still stationed in Bosnia and Herzegovina, with a steady influx of new migrants along the Western Balkan route.

According to Frontex data, during the 2020 pandemic year, 124,000 cases of illegal border crossings were recorded along the external border of the EU, which represents a 13% reduction year-on-year. There was a total of 16,969 crossing on the Western Mediterranean route (28% reduction compared to 2019), 35,628 along the Central Mediterranean route (an increase of 154% year-on-year) and 19,681 crossings on the Eastern Mediterranean route (76% decrease compared to 2019). However, although the Eastern Mediterranean route recorded a great decline in illegal migration in 2020, the total number of illegal migrants on the Western Balkan route rose by 78%, to 26,928 cases.

The majority of migrants originate from Syria, Morocco, Tunisia and Algeria. Men make up more than 90% of all migrants, and approximately 10% are minors.

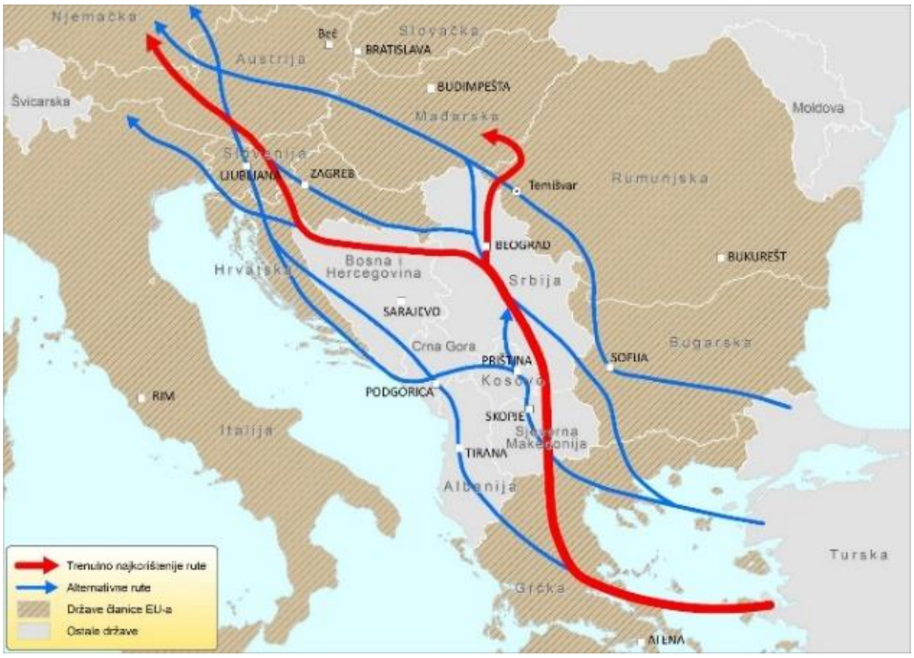
Although the migrant crisis in Turkey is currently stagnating, the unfavourable security and economic outlook in the countries of origin may trigger a new wave of migration on the Balkan route in the upcoming period. Moreover, Turkey’s policy towards the EU will significantly impact the influx of migrants to SE Europe. The development of the security situation in some states, such as Afghanistan, will impact the future development of migration pressure across SE Europe.

Deteriorating situation with the COVID-19 pandemic and the subsequent introduction of restrictive measures related to the freedom of movement, would slow down migrant flows, as it had already happened in March and April 2020.

After the EU imposed sanctions on the Lukashenko regime, Belarus registered a considerably higher migration pressure on the Lithuanian-Belarus border (predominantly coming from Iraq, Congo and Cameroon).

Illegal migration poses a significant social threat with a complex set of causes and consequences. In the context of the pandemic, illegal migration can pose a public health threat.

From a security point, illegal migration is a significant challenge in terms of identifying individuals with terrorist intentions. Several recent terrorist attacks in Europe have been carried out by individuals who had illegally entered Western European states (attacks in France and Germany), indicating that terrorist groups use illegal migration to transfer their members and supporters to Europe. These terrorist attacks also highlight that migrant population, often traumatized by the circumstances in the country of origin and difficulties in integration in the receiving states, can be radicalised.



Illegal migration routes in Europe and SE Europe

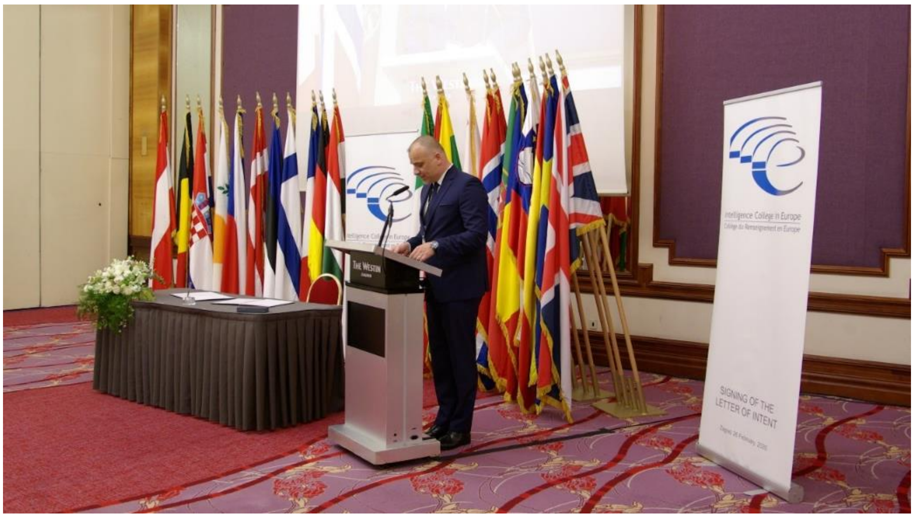
International cooperation as a significant segment of SOA operations

International cooperation represents an exceptionally significant segment of security and intelligence work. Through international cooperation, security and intelligence communities protect common values and interests, exchange information, warnings and assessments, and share experience and practices.

In the contemporary world, security issues are not of simply national significance or impact. Thus, the international dimension is present in all issues that security and intelligence agencies deal with.

SOA has developed international security and intelligence cooperation with many security and intelligence agencies, working together on a variety of common issues, depending on the specific security environment and interests in partner states.

As a security and intelligence agency of a NATO and the EU member state, SOA has been developing strong international partnerships in this circle in order to protect common values and interests. The Agency has also contributed to the relevant EU and NATO bodies in charge of security and intelligence issues.


Intelligence College in Europe
Collège du Renseignement en Europe
SIGNING OF THE LETTER OF INTENT
THE WESTIN

SOA Director gives a presentation on the occasion of the signing of the Letter of Intent concerning the establishment of the Intelligence College in Europe, in Zagreb, 26 February 2020

At the same time, SOA has been increasingly active in all multilateral forums which contribute to national and international security, and in particular those platforms which operate in the context of the EU and NATO, i.e., the European and Euro-Atlantic circle of values.

In line with the general trend of increasing openness to citizens, the European security and intelligence community has also been trying, as much as security and legal circumstance permit, to be more open to the general public. Public reports are one of such tools.

In the European context, one of the largest projects of opening the security and intelligence communities to the general public is the Intelligence College in Europe (ICE), which was launched on 26 February 2020 by signing the Letter of Intent in Zagreb. The College was joined by 23 European states. The College is a platform which promotes and facilitates a dialogue between European intelligence communities, decision-makers and academia to enhance strategic thinking and mutual knowledge and to develop a shared European intelligence culture. SOA chaired the College in 2020.

Some multilateral platforms have been established to counter common security threats. One of the most important and most successful platforms is the Counter Terrorism Group (CTG), which brings together security agencies of the EU member states and other Western European states. SOA chaired the Counter Terrorism Group in the first half of 2020.

From 2018 to 2020 SOA partnered up with the Polish Internal Security Agency (ABW) in the implementation of a project for more efficient identification and suppression of terrorist and asymmetric threats in public administration. The project was co-funded by the European Social Fund. ABW has chosen to partner up with SOA because of the Agency's previous activities, the ability to contribute to the objectives of the partnership and experience in similar international projects.

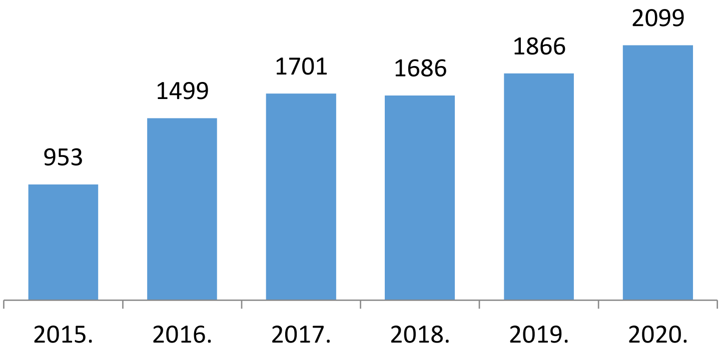
As part of the joint ABW and SOA project, an online conference on the topic of raising awareness in the prevention of terrorism was held 19 - 20 January 2021. The conference was hosted by the ABW Centre for Excellence in Terrorism Prevention. It was attended by representatives of security intelligence agencies and institutions from other states, international and academic organisations.

SOA has also contributed to the project by collecting and exchanging practices and experiences at national meetings, in expert meetings and international meetings with many foreign agencies and institutions, and it has also actively participated in the development of educational materials based on which Polish partners carried out national trainings for their employees in public administration and civil service.

Reporting end-users is a daily task at SOA

All relevant intelligence collected within the Agency’s scope of work was reported to the state leadership: the President of the Republic, the Speaker of the Parliament and the Prime Minister of the Republic of Croatia. In 2020, SOA delivered them with approximately 530 pieces of analytical work.

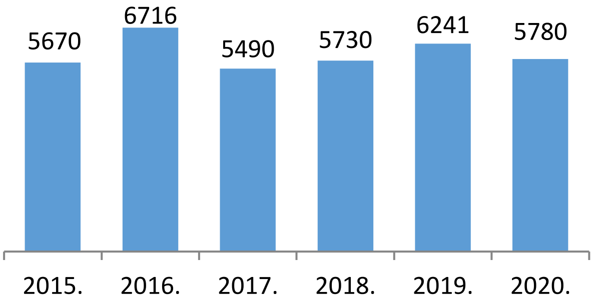
The reports to the state leadership and relevant authorities primarily included security and intelligence and analyses as well as other reports containing intelligence. The Agency made additional efforts in 2020 to intensify intelligence reporting during the outbreak of the pandemic.



Number of security and intelligence informations, reports and analysis delivered to the state leadership, by years

SOA, as an integral part of the national and homeland security system, continuously cooperates and delivers intelligence and security assessments to other competent authorities such as Ministry of the Interior, Ministry of Foreign and European Affairs, State Attorney’s Office, Croatian State Prosecutor's Office for the Suppression of Organised Crime etc. In 2020, SOA delivered approximately 9,300 different pieces of intelligence to other state authorities, which is below 12,200 pieces which had been delivered in 2019. This decline year-on-year in the number of intelligence is attributed to halted social, economic, political and other activities which carry security implications during the 2020 pandemic outbreak.

SOA performs security vetting procedures in the context of preemptive operations and enhancing information security (including basic security vetting and those with the purpose of granting access to classified data). Similarly to other areas, the pandemic outbreak affected the decrease in the security vetting procedures year-on-year. Nevertheless, despite the constraints, the Agency carried out a total of 5,780 security vetting procedures, which represents an increase compared to 2017 and 2018.



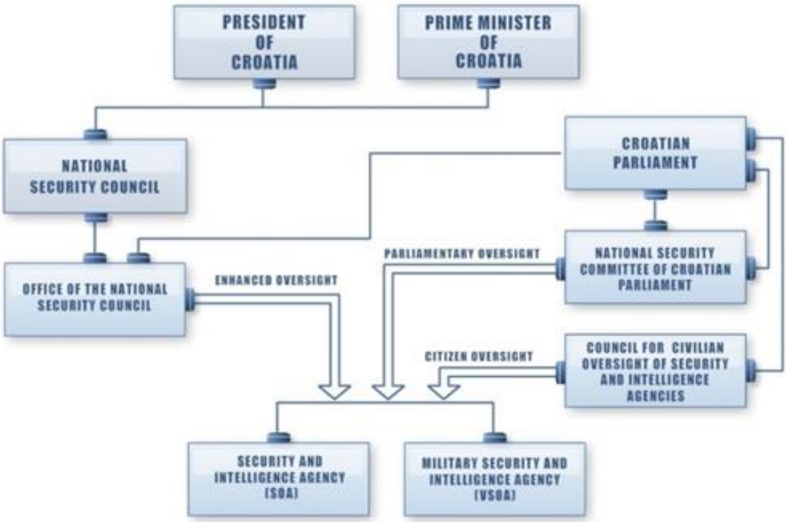
Number of security vetting procedures, by years

The outbreak of the pandemic has had the greatest impact on the number of security vetting procedures in regard to the movement and residence of protected individuals and protected facilities. In 2020, the Agency carried out 300 security vetting procedures in regard to the movement and residence of protected individuals and protected facilities, which is less than in 2019 when 565 such security vetting procedures were conducted. Approximately 23,000 security vetting procedures were performed in connection with individuals with direct access to protected individuals, facilities and premises, which is similar to 2019 level.

Security issues pertaining to foreign nationals and citizenship procedures have been increasingly using up SOA’s capabilities, most notably in relation to the issue of asylum seekers in the Republic of Croatia. The previous year was marked by a significant decline in the number of security vetting procedures related to regulating status issues of foreign nationals and citizenship procedures, caused by the closure of state borders during the pandemic. Such operations are expected to grow in the ensuing period, due to general migration trends. The number of these security vetting procedures amounted to 18,825 in 2020, compared to 76,673 in the previous year. At the request of the Ministry of Interior, SOA participates in the procedures for international protection (asylum and subsidiary protection), delivering an opinion on the application. SOA approaches each case individually and conducts interviews with applicants for international protection.

Oversight of SOA as part of democratic practice

In accordance with practices in developed democracies and due to the sensitive nature of SOA operations and the need to protect the rule of law and human rights, SOA is subject to rigorous oversight. In the Republic of Croatia, a three tiered oversight mechanism is in place for security and intelligence agencies: the parliamentary oversight is carried out by the Croatian Parliament through the Domestic Policy and National Security Committee, the expert oversight is carried out by the Office of the National Security Council, and the civilian oversight carried out by the Council for the Civilian Oversight of the Security and Intelligence Activities. Civilian oversight is an indicator of the democratic development of Croatian society since such an instrument is a rarity, even among the developed Western democracies.


PRESIDENT OF CROATIA
PRIME MINISTER OF CROATIA
NATIONAL SECURITY COUNCIL
CROATIAN PARLIAMENT
OFFICE OF THE NATIONAL SECURITY COUNCIL
ENHANCED OVERSIGHT
PARLIAMENTARY OVERSIGHT
NATIONAL SECURITY COMMITTEE OF CROATIAN PARLIAMENT
CITIZEN OVERSIGHT
COUNCIL FOR CIVILIAN OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES
SECURITY AND INTELLIGENCE AGENCY (SOA)
MILITARY SECURITY AND INTELLIGENCE AGENCY (VSOA)

Organisational chart of the external oversight system

When we take into account the fact that the Supreme Court approves the measures that temporarily restrict some constitutional human rights and fundamental freedoms, we may then speak about the fourth tier, the so-called judicial oversight which is carried out by the highest judicial instance in the country.

The oversight bodies have at their disposal broad possibilities of establishing facts such as an insight into SOA’s documents, interviews with the director and other employees etc. According to the results of the oversight carried out in 2020, no illegal actions were established in SOA operations.

In addition to external oversight, SOA has a system of internal oversight in place. An organisational unit tasked with oversight over the constitutionality and legality of all organisational units and employees, data protection and counterintelligence protection operates within the Agency.

Career at SOA is a unique opportunity

Despite technological advances and increasingly powerful tools for intelligence collection and processing, the human dimension of security and intelligence operations remains irreplaceable, and the human factor remains key to the success of organisations. Thus, operational performance and quality are mostly dependent on the competence, knowledge and skills of the employees.

The number of employees at SOA is classified information. The total number of employees is comparable to the levels in the security and intelligence agencies in the EU and NATO member states. The majority of SOA staff are civil servants.

Given the particular nature of the security and intelligence work, including the risks and dangers that our people power is exposed to, the Agency is obliged to protect the identity of the employees.

The educational structure of SOA employees is broad and is defined by the broad span of organisational needs. SOA employs experts in economics, finance, computer science, law, criminology, political science, sociology, languages, electrical engineering and other fields. Over three-quarters of the Agency's employees hold advanced and higher degrees.

SOA employs operatives, analysts, IT experts, financial experts, officers for human resources management, accounting, legal affairs, administration, archiving and security.

Women make up 40% of the staff and are equal in performing all tasks in the Agency's scope of work. The age of SOA employees generally ranges from 30 to 50.

Recruitment and selection process at SOA

An administrative competition is not required for employment at the SOA. SOA website (www.soa.hr) features a Careers section.

More information about a career at SOA is available at the link www.soa.hr/hr/posao-u- soa-i/, and all interested candidates may apply by submitting their applications using the web forms at www.soa.hr/hr/posao-u-soa-i/prijavi-se/#prijava-body.

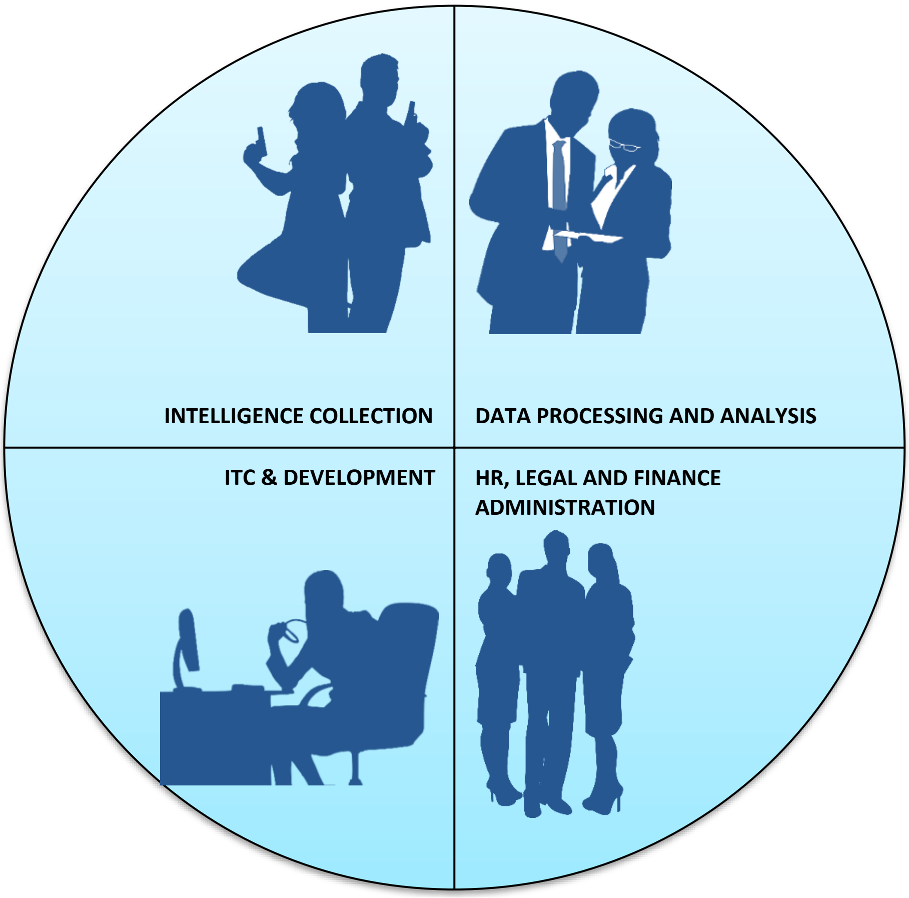
The recruitment and selection process is very important for selecting the best candidates for employment at SOA. SOA is interested in attracting young and educated candidates who possess the knowledge, skills and motivation for modern security and intelligence work and who are interested in working to protect the national security of the Republic of Croatia.

All submitted applications are considered by SOA. In line with the current needs, candidates that meet the qualification requirements for specific work places are invited to participate in the selection process, on equal terms.

The selection process includes security vetting, various knowledge and skills test, psychological assessment and medical assessment. Those candidates whose test results correspond most with the employee profile will be selected.

SOA invites all interested candidates who believe that their education and competence can be a good fit for a career in security intelligence and are interested in working to protect the national security of the Republic of Croatia, to apply for a position at the Agency. We guarantee a fair and through recruitment and selection process based on equal terms.

SOA offers diverse career opportunities, and here we have highlighted four major categories of workplaces; operatives who collect intelligence and are mostly based at the SOA regional centres across the Republic of Croatia, analysts who are in charge of data processing and analysis, IT officers, and various legal, financial, HR, and administrative officers.


INTELLIGENCE COLLECTION
DATA PROCESSING AND ANALYSIS
ITC & DEVELOPMENT
HR, LEGAL AND FINANCE ADMINISTRATION

Major categories of workplaces at SOA

This document is the property of the Security and Intelligence Agency. It is released with the purpose of informing the general public of the Agency's work, security challenges and threats. The Document is intended for public release, available electronically at www.soa.hr and may be used freely.

Images: SOA, Ministry of Defence, Government of the Republic of Croatia, Pixabay
Maps: SOA

Security-Intelligence Agency
Savska cesta 39/1
10000 Zagreb

CONTACT:
Phone: 01/ 377 22 22
e-mail: informiranje@soa.hr

www.soa.hr