SECURITY-INTELLIGENCE AGENCY

PUBLIC REPORT
2019/20

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, recognized by its developed capabilities, excellent employees and strong partner ties.

Contents

Introductory remarks

Dear Readers,

we deliver the sixth Public Report in a volatile and challenging security period. Our society, together with the whole world, has been fighting the outbreak of a disease caused by the novel virus and COVID-19 desease, which has created an unprecedented upheaval in our way of life, economy and all social activities. In addition, our capital city was struck by a destructive earthquake in March, undermining our security situation and perception of safety.

Natural disasters are not within the primary scope of work of the Security and Intelligence Agency (SOA). These phenomena are within the jurisdiction of other authorities; Croatian public health, Civil Protection and other bodies. Nonetheless, in this situation, we have put our capabilities and knowledge at their disposal, so that we could enhance the security of our citizens.

The threats that we address differ from natural threats in cognizance and intention. Whether it be terrorism, extremism, foreign espionage or organized crime, there is always a single or several individuals actively and intentionally seeking to undermine our national security or the security of our citizens. Our task is to recognize such intentions and phenomena, act pre-emptively and report our findings, intelligence and possible consequences to our end-users.

Even in the time of the outbreak of COVID-19 the threats that SOA addresses remain present and real. Moreover, some of them, such as terrorism or organized crime, may even be reinforced if their members assess that security forces are overexerted because of the effects of the pandemic. Therefore, our pertinent task is to ensure continuity of operations in the crisis period.

Much like the public health system in the case of a viral pandemic, the Agency deals with challenges whose actors seek to remain invisible, but whose repercussions are visible and threaten our national security. It is therefore our duty to act pre-emptively in the face of such challenges and report reliable intelligence to the relevant authorities.

In addition, our task is to maintain the preparedness level to respond to those security challenges which are dormant at the moment, but carry a risk of emerging. We must therefore think long-term, consider all challenges, however uncertain they may be, plan our resources and carefully build up our capabilities.

This Public Report confirms that the Republic of Croatia remains a safe and stable democracy. Despite all challenges that we face, there are currently no indications of serious undermining of national security and our democratic constitutional order. As in the previous reports, this Public Report contains statistics for the last year and outlines the current security environment.

In this Report, we have focused on two long-term trends in the security and intelligence community. Firstly, the increasing importance of cooperation among the European security and

intelligence agencies and secondly, the growing shift of the security and intelligence operations to the cyber sphere.

The first trend is evidenced in the launch of the Intelligence College in Europe. SOA has been trusted with organizing the signing of the Letter of Intent on the establishment of the College in Zagreb in February 2020. On this occasion, 23 European intelligence communities gathered to mark the conception of the common European intelligence culture. Through this long-term strategic project we will build a stronger European security and intelligence cooperation.

SOA has been chosen to preside this large-scale European project in its inaugural year, which further confirms our success and trust that our partners have in our capabilities.

The Agency also presided over the Counter Terrorism Group (CTG) in the first half of 2020. The Group gathers security and intelligence agencies of the EU member states and other Western European countries.

The trust we enjoy among our partners is the result of our active contribution to the common European security and the Euro-Atlantic partnership.

The second trend we have chosen to focus on is the cybernetics in the security and intelligence operations. One of the chapters is therefore dedicated to the Agency's role in the protection of the national cyberspace and the newly set up Centre for Cyber Technology.

We were delighted that we were given the opportunity to open the Cybertech Global 2020 conference with a presentation of our Centre for Cyber Technology before 18, 000 participants.

Investment in cyber technologies enhances our national security and response capability. This enables us to reassure the Croatian society that all resources that are invested in the Agency are engaged into modern capabilities necessary for active and consistent protection.

As every year, I encourage all young, educated and interested candidates to pursue a career at the Agency. We take pride in our thorough but objective selection process. The work that we do is challenging, noble and directed at achieving common good. We are looking to invest in expertise and talent that will take over the responsibility for our nation security in the ensuing years.

SOA is one of the pillars of resilience of our society and our institutions. We are dedicated to performing our tasks responsibly, at any time, despite all the risks they carry. In doing so, we support our fellow citizens and state bodies, we raise awareness of our presence and activities, and ensure that they can rely on us for security.

Croatian citizens can be confident that the Security and Intelligence Agency is staffed by competent and reliable professionals, who live among them and with them, looking after our common security.

Director

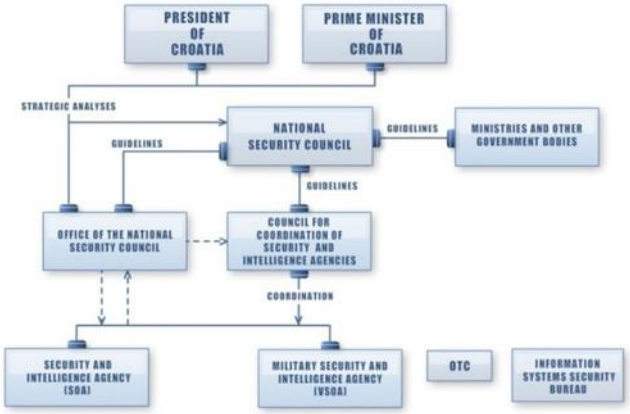
Daniel Markić

SOA

collects and analyses intelligence significant for national security and informs the state leadership and other relevant bodies

SOA is a part of the national and homeland security system

SOA (the Agency) collects and analyses data significant for national security. We report our findings to the state leadership and other state bodies thus providing them with reliable intelligence support in decision-making relevant for Croatia's national security, interests and the well-being of its citizens.

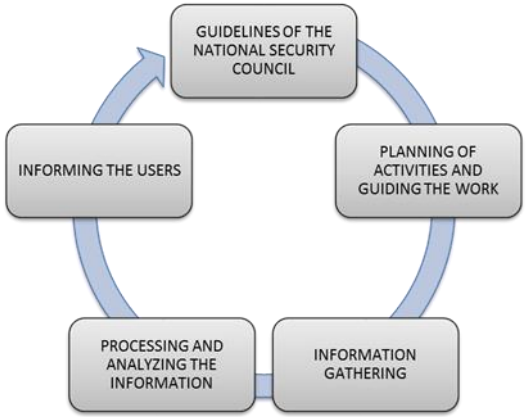


Security and intelligence system in the Republic of Croatia

The work of the security and intelligence agencies (SOA and VSOA) is directed by the President of the Republic and the Government through National Security Council (VNS), while the Council for the Coordination of Security and Intelligence Agencies (the Council) provides operative coordination. The Office of the National Security Council (UVNS) provides expert and administrative tasks for the VNS and the Council.

The work of SOA is jointly directed by the President of the Republic and the Government of the Republic of Croatia

SOA plans and carries out its activities on the basis of guidelines identified in the strategic and implementing documents. We report the end-users on the implementation of guidelines and objectives as well as on the collected intelligence.



SOA Intelligence cycle

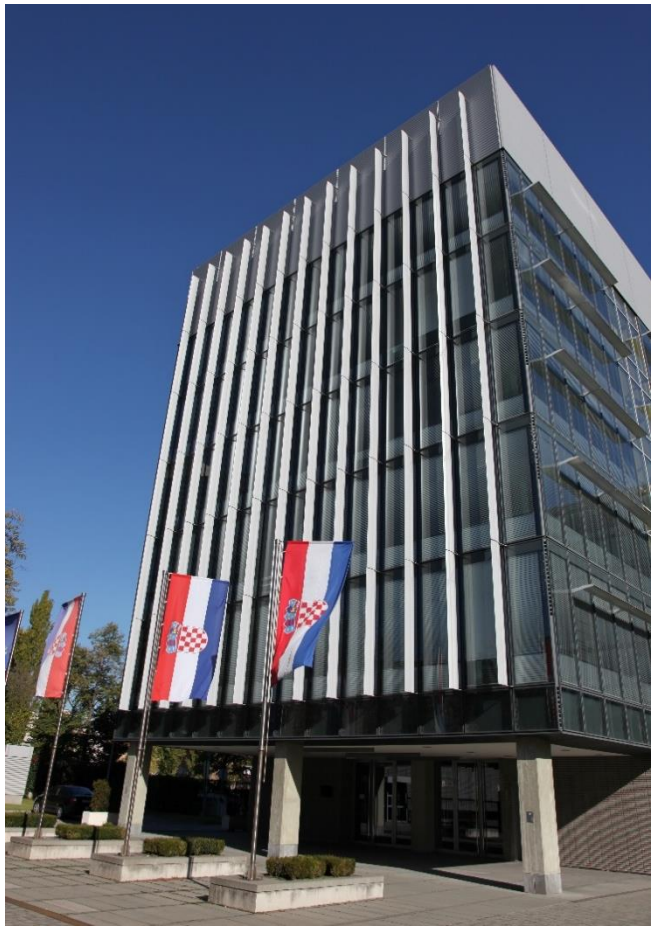
The fundamental strategic document which directs the work of SOA is the National Security Strategy which has been adopted by the Croatian Parliament. Along with this umbrella security strategy for the Republic of Croatia, the work of SOA is also governed by other strategic policy documents such as the National Strategy for the Prevention and Suppression of Terrorism and the National Cyber Security Strategy.

Besides the relevant strategies, the National Security Council issues Annual Guidelines that regulate the operations of the security and intelligence agencies.

The Annual Guidelines outline the priorities in the work of the security and intelligence agencies. They therefore serve as the basis for work planning, task execution and reporting activities. Additionally, they allow supervision over the expediency and efficiency of the Agency's work.

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.

Besides data collection and analysis, SOA carries out other counterintelligence activities with the purpose of enhancing the security framework of the Republic of Croatia; such as security vetting and assessment, protection and security of protected individuals, enhancing the information and cyber security.



SOA collects and analyses intelligence significant for national security

SOA is authorized 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 open sources and international exchange.

Any measures of covert intelligence collection that infringe the constitutional rights and freedoms of the individuals and citizens must be authorized 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.

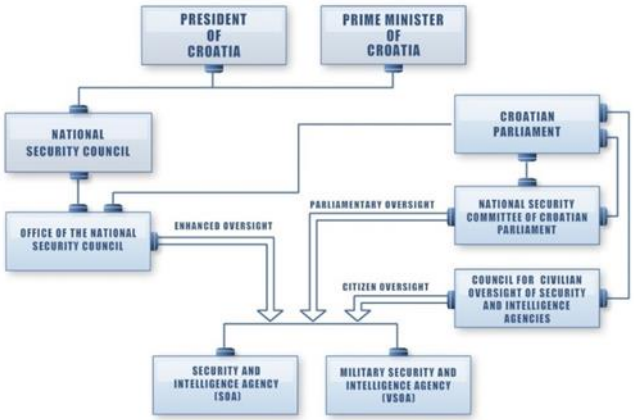
SOA operates from the headquarters in Zagreb, with 10 regional centres across Croatia.

SOA HQ organizational chart

SOA is under permanent three tiered external oversight

The security and intelligence agencies in the Republic of Croatia are under a permanent three tiered external oversight; parliamentary, expert and civilian.

The parliamentary oversight is carried out by the Croatian Parliament directly and 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 that is carried out by the Council for the Civilian Oversight of the Security and Intelligence Agencies.



Organizational chart of the oversight system

The Republic of Croatia is one of only a few countries in the world that has established civilian oversight over the security and intelligence agencies.

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.

In addition to external oversight, SOA has a system of internal oversight over the constitutionality and legality of the activities of all organizational units and employees, data protection and counterintelligence protection.

All three oversight bodies (Office of the National Security Council, Council for the Civilian Oversight of the Security and intelligence Agencies, Domestic Policy and National Security Parliamentary Committee) conducted oversight in 2019 and found no illegality in the work of SOA.

SOA's activities are aligned with the guidelines of the state leadership

Pursuant to the Security and Intelligence System Act, SOA's operations on the territory of the Republic of Croatia are focused on the prevention of those activities or actions that may threaten the constitutional order and undermine security of the state bodies, the citizens, the national interests and the national security.

Moreover, SOA collects, analyses, processes and assesses data relating to foreign states, organizations, political and economic alliances, groups and individuals, namely those that point to intentions, capabilities, covert plans and clandestine activities that threaten national security, i.e. data of particular importance to the national security of the Republic of Croatia.

The relevant legal and strategic documents outline the following areas of SOA's security and intelligence operations:

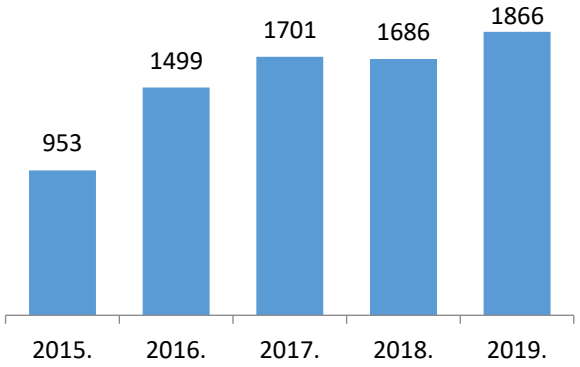
- Terrorism and extremism,
- Foreign intelligence activities that pose threats or challenges to the values and interests of the Republic of Croatia,
- Security and other processes in the environment that impact the Republic of Croatia and its interests,
- Global processes, security and challenges affecting the Republic of Croatia and its interests,

- Protection of the economic system and suppression of organized crime and corruption that undermine national security,
- Economic and financial processes that affect the economic interests and the stability of the Republic of Croatia,
- War crimes, detained and missing persons,
- Counterintelligence protection and security of protected individuals, facilities, premises and critical infrastructure.

In 2019 SOA consistently reported the state leadership

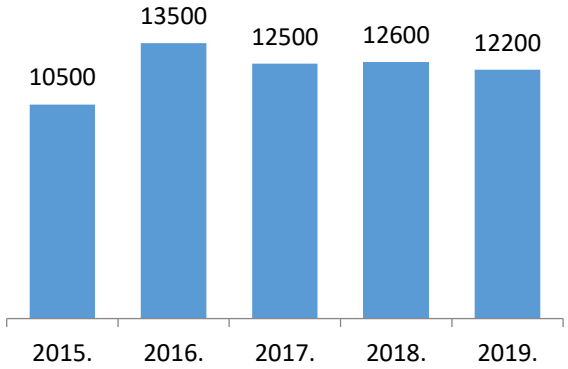
SOA reports the President of the Republic of Croatia, the Speaker of the Croatian Parliament, the Prime Minister and the Office of the National Security Council on all significant intelligence and security assessments. In 2019 SOA delivered them with 440 analytical reports.

The reports to the state leadership and relevant authorities primarily included security and intelligence and analyses as well as other reports containing intelligence.



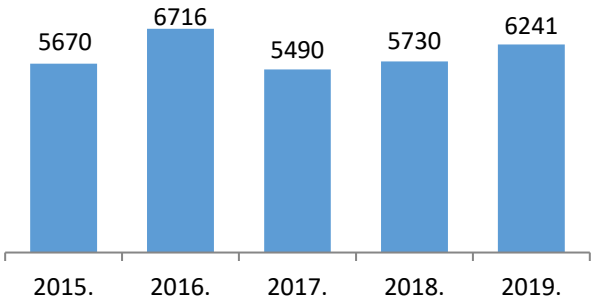
Number of security and intelligence information and analysis delivered to the state leadership and relevant bodies, by years

SOA, as an integral part of the national and homeland security system, cooperates and delivers intelligence and security assessments to other competent authorities (Ministry of the Interior, Ministry of Foreign and European Affairs, the State Attorney's Office, Croatian State Prosecutor's Office for the Suppression of Organized Crime, Ministry of Defence, Ministry of Economy etc.). In 2019 SOA delivered approximately 12200 different pieces of security intelligence to other state authorities.



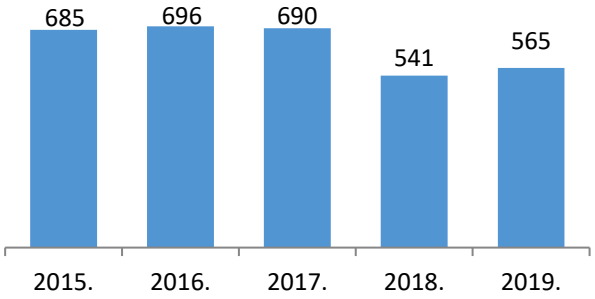
Indicative number of security and intelligence delivered to end-users, by years

SOA performed 6241 security vetting procedures in the context of pre-emptive operations and enhancing information security (including basic security vetting and those with the purpose of granting access to classified data). Additionally, SOA carries out security vetting of legal entities.



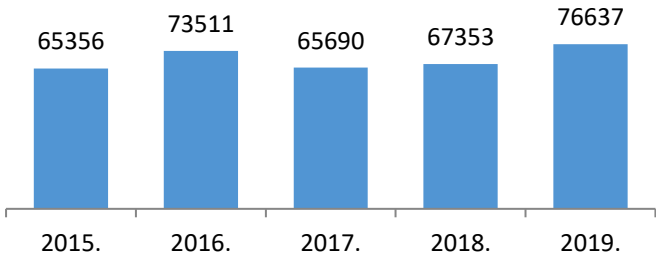
Number of security assessments, by years

In 2019 there were 565 security vetting procedures in regard to the movement and residence of protected individuals and protected facilities. Approximately 24000 security screenings were performed in connection with individuals with direct access to protected individuals, facilities and premises.



Number of security vetting procedures, by years

Security issues pertaining to foreign nationals and citizenship procedures have been increasingly using up SOA's capabilities, most significantly in relation to asylum seekers in the Republic of Croatia. Number of security vetting procedures related to regulating status issues of foreign nationals and citizenship procedures marked the previous year. Such operations are expected to grow in the ensuing periods, due to general migration trends.

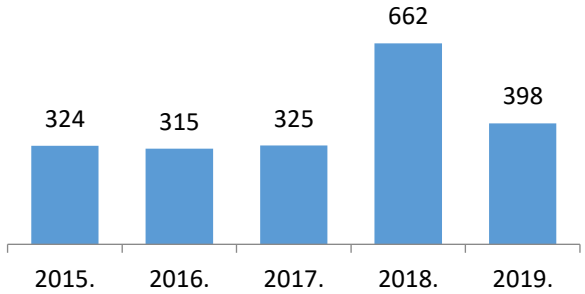


Number of security vetting procedures related to regulating status issues of foreign nationals and citizenship procedures, by years

At the request of the Ministry of Interior, SOA participates in the procedures for international protection (asylum and subsidiary protection), delivering opinion on the application. SOA approaches each case individually and conducts interviews with applicants for international protection.

SOA's growing investment in development and modernization

SOA is funded through the state Budget of the Republic of Croatia. SOA's Budget is subject to regulations pertaining to public finance in the Republic of Croatia. The Agency's Budget in 2019 amounted to HRK 398 million.



SOA's budgetary trajectory by years in HRK mil

A one-off Budget increase in 2018 was a result of booking related to a large-scale infrastructure project.

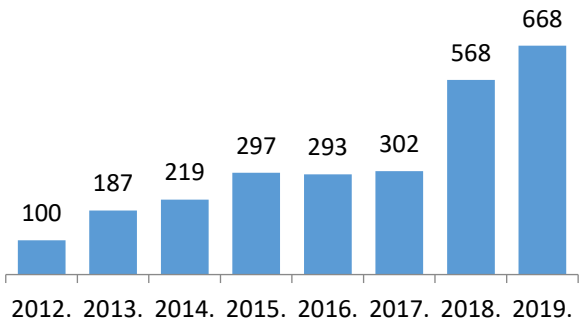
The increase in SOA's Budget in the recent years highlights the investment that the Republic of Croatia has made in strengthening security in the period of increasingly complex security challenges. This increase in the Budget marks the beginning of substantial investment in capability-building which will contribute to the overall long-term security of the Republic of Croatia.

The budgetary increase for the intelligence-security agencies corresponds to Western European trends, particularly in the light of intensified terrorist and hybrid threats, increasingly complex global geopolitical situation and growing demand for capability-building in the context of technology development.

As per the Security and Intelligence System Act, and in line with best 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.

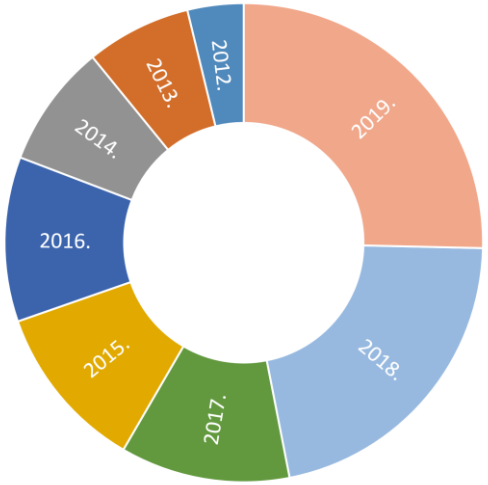
The largest share of the Budget is allocated for people force expenditures, followed by operating and capital expenditures. In order to enhance capacity-building, special attention is devoted to the allocation of funds for development and modernization.

In the period 2012 - 2019 the Agency recorded a sevenfold increase in the annual investment in development and modernization..



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

In line with the Agency's Development Plan, the investment in development and modernization is being consistently built up in order to allow us retain top capabilities necessary for responding to all future security and technological challenges.



Nearly 50 percent of the total investment in development and modernization was realised in 2018 and 2019

Security environment

driven by dynamic and volatile security challenges

Global security environment is driven by security challenges and geopolitical rivalry between the great powers

Global security environment continues to be marked by numerous, dynamic and complex security challenges. The rapid speed and unpredictability of the security challenges complicate monitoring and assessment.

The development of new technologies and communications against the backdrop of the widespread globalization of social, financial and economic processes additionally increases the number of stakeholders and further compounds and accelerates all processes. Internet, that is the cyberspace, has become the primary channel of global communications and interactions.

The existing world order has been changed under the pressures of political, economic, technological, security and other changes and shifts in power relations. The dynamics of changes and their development remain demanding to predict.

Global security environment, complicated by the existence of numerous hot spots which generate instability, has been characterized by geopolitical and economic shifts in the relations of the great powers, growing types and expanding reach of hybrid warfare, rise in the number of cyber-attacks, as well as the increase in the number of non-state actors that impact the security situation.

Global security environment hinges on the relations between the great political, military and economic powers, the USA, Russia, China and the European Union either as an integration or its individual members.

International mechanisms and agreements that had been put into place in the aftermath of the Second World War and disarmament agreements have been under increasing pressure. The Strategic Arms Reduction Treaty New START between the USA and the Russian Federation is set to expire in 2021, and the issue of Chinese participation in such an agreement has been raised.

Simultaneously, a number of states across various regions in the world have been building up new weapon systems and strengthening their military capabilities, which has boosted higher military expenditure on the global level.

The USA, with a global alliance network, has retained their dominant political, military and economic power worldwide. They have consistently built their foreign and security policy on a new concept of economic and security interests.

The US - Chinese relations, characterized by a strategic rivalry of these two states, have come to the forefront of the development of global security and economic situation. Global economic conditions have recently been impacted by the US - Chinese trade tensions and allegations coming from the USA that China employs unfair and unlawful measures to grow its economy.

China has global economic ambitions and seeks to extend its economic involvement across all continents, by participating in the development of infrastructure projects and by expanding its technology. China has invested extensively in infrastructure projects as part of the Belt and Road Initiative, a global infrastructure development strategy which is the centrepiece of Chinese global ambitions and growing economic presence worldwide. After the USA, China is the single largest trade partner of the EU, while the EU is the largest trade partner to China. Nevertheless, the EU has characterized China as an economic competitor and a systemic rival that has promoted alternative models of governance.

Chinese tech companies have been developing new technological standards and have been taking over the leading role in the development of digital services. Europe has been closely monitoring the spread of 5G technology facilitated by Chinese companies while maintaining an open discussion on the intelligence prospects of 5G for data utilization and the obligation of Chinese companies to share these data with the Chinese authorities. Besides strengthening its economic power, China has significantly enhanced its military capacity and capability.

Russia has been seeking to replicate its renewed military power and enhanced political apparatus in the international arena and to strengthen its economic and energy presence in the world. It has set out to compensate for its limitations in military capabilities and economic reach through influence operations as well as foreign policy and energy tools and hybrid operations. In certain hot spots such as Syria, Russia has engaged significant field military capabilities.

Russia has been maintaining consistent foreign and domestic policy. It 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 Crimean annexation. The relations with the West have been strained because of indicators of Russian hybrid operations directed at Western states, dissemination of fake news and cyber-attacks originating in the Russian territory. The most recent case of the poisoned Russian dissident Alexei Novalny will further frustrate the Russian-West relations.

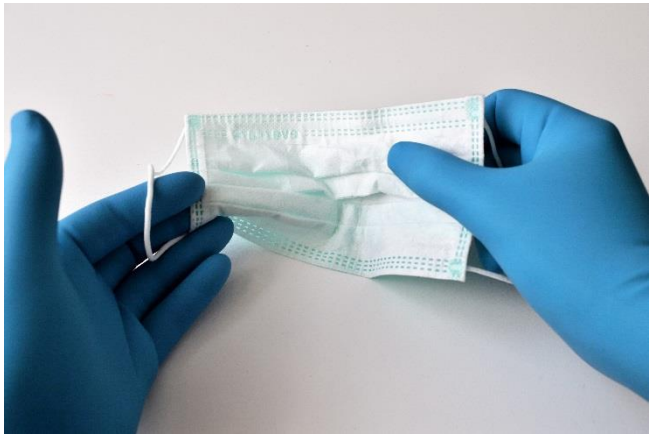
Encouraged by their mutual opposition to the global US - West dominance, Russia and China have been reinforcing bilateral relations. China is Russia's single largest trade partner and there are plans to double the bilateral trade by 2024. However, their relations can be put under strain by challenges such as growing Chinese influence in the states that Russia has regarded a sphere of influence, such as Central Asia.

A belt of hot spots extending from Central Asia, across the Middle East to North and Sub-Saharan Africa has been experiencing numerous armed conflicts, terrorist attacks, failed states, devastated economies, humanitarian crises, unemployment and mass migration. In these hot spots, rival policies of global and regional powers come head-to-head, including engagement of military capabilities.

Global security environment is also impacted by other processes including climate change, outbreaks of communicable and other diseases, population booms in the developing countries, resource depletion and destruction of nature. These processes reinforce internal and regional conflicts, mass migration, social tensions and unrest, terrorism, institutional collapse in the failed states and systematic violations of human rights.

Outbreak of COVID-19 will impact global security

COVID-19 pandemic will affect human health and will have major repercussions on all other aspects of life, in particular economic, political and security environment worldwide. The economic downturn caused by the pandemic could have an adverse impact on global security environment. Those states which have failed to adequately respond in order to prevent the pandemic and mitigate the economic repercussions arising from it, might be exposed to deterioration of security conditions due to the rising dissatisfaction of the population, the disintegration of public health systems, widespread poverty, rising crime, extremism, social unrest, terrorism and both internal and external migration.



As any large-scale crisis, the outbreak of COVID-19 pandemic has disrupted a variety of processes and it will have a long-term impact on global geopolitical and economic changes. The pandemic has, for example, raised the issue of the EU dependency on medical equipment, medicines and other essential products which are manufactured outside Europe, most notably in China. Similarly, the pandemic has raised the issue of security of the global supply chains.

Throughout the pandemic certain states have continued to use the media space for disinformation purposes, focusing on either the existing or fake weaknesses of the West in efficient efforts to combat the spread of the disease, while at the same time diverting attention from their own internal weaknesses. In doing so, they have disseminated the narrative of failure and lack of solidarity in the European Union during the pandemic, and aggravated the spread of distrust among the member states and their general public.

The EEAS - European External Action Service project EUvsDISINFO has highlighted in its reporting efforts in monitoring public disinformation related with COVID-19. The reports emphasize operations such as EU-hostile media broadcasting narratives on the collapse of the EU. Nevertheless, what causes additional concern is the fact that such media have broadcast disinformation detrimental to public health, such as conspiracy theories and messages that public health measures (e.g. handwashing) do not help.

In addition, terrorist groups such as ISIS have urged their supporters to exploit the focus of the European societies on COVID-19 to carry out terrorist attacks.

A piece of news from the media in the neighbouring country. The news states that in a convoy carrying Russian medical help to Italy in March 2020, in the vicinity of the Italian-US air base in Aviano, the Russian "brothers" had hung Serbian flag as a message to "NATO aggressor"

Security shifts to the cyber sphere

The resurgence of political processes in the sphere of geopolitical rivalry, similar to those of the Cold War era, has contributed to an increase in intelligence activities, data collection as well as hybrid operations and state-sponsored cyber-attacks.

Security processes and trends are driven by the development of new technologies, which bear new risks and threats. Therefore, new technologies require competent state security organisations. Such technologies include cloud computing, 5G mobile networks or the Internet of Things, but they also include a wide range of areas affected by these disruptive technologies such as smart cities and autonomous vehicles.

Due to the large-scale involvement of state-sponsored attackers, cyber-attacks have been increasingly becoming more complex and more frequent, and causing more extensive damage. These attacks are aimed at not only data theft (political or industrial espionage), but also at damaging critical infrastructure, financial extortion and theft of intellectual property. They are facilitated by the possibilities of concealing the identity of attackers and their geographical dispersion.

ICT has been misused for radicalization and dissemination of extremist ideas which can lead to violence and terrorism. Likewise, it is also used as a tool in terrorist recruitment and training and for attack planning.

A particularly sensitive area of cyber security is related to the theft of classified, personal and other sensitive data, undermining operations of critical systems and services. The likelihood of interfering with social and democratic processes through dissemination of disinformation and fake news has been growing.

Arrest warrant for seven Russian nationals suspected of involvement in hacking operations of the Russian military service GRU. The operations involved hacking, influence and disinformation operations to undermine anti-doping efforts, sports federations and anti-doping officials

The EU Council's Decision from 30 July 2020 imposed the first ever sanctions against cyber-attacks. The sanctions were imposed in response to cyber-attacks that have had an adverse impact on the European security and the economy. Restrictive measures were imposed against six individuals and three institutions from Russia, China and North Korea. The institutions under sanctions include the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), a Chinese company Haitai Technology Development and a North Korean company Chosun Expo.

European security faces numerous challenges

The European Union (EU) has been facing numerous security challenges arising from the instability in the European environment such as migration pressures. Simultaneously, it has been compounded by internal security challenges such as advancing radicalism and terrorism in certain societies.

Internal political processes have been marked by Brexit, internal integration processes and issues of democratic and economic development.

Foreign policy topics of interest include the development of the Euro-Atlantic partnership, relations with Russia, China and Iran, issues of enlargement in Southeast Europe and the role of the EU in the stabilization of crisis hot spots in the European neighbourhood.

One of the outstanding internal issues pertains to the further development of the security and defence dimension in the EU, particularly in the context of complex geopolitical and economic relations with Russia and numerous crisis hot spots in the European neighbourhood. In such complex security environment, the member states have been reinforcing the security and intelligence dimension of the integration.

In the fallout of the Ukrainian conflict and Russia's annexation of the Crimea, NATO has enhanced its defence capabilities in Europe, including pre-emptive engagement at the Eastern border of the Alliance and large-scale military exercises.

The Republic of Croatia, in line with its economic and other capabilities, has participated in the overall enhancement of NATO's defence capabilities and in the pre-emptive defence engagement.

In the context of economic and security consequences of the COVID-19 pandemic, the EU has been deliberating forms of defending the underperforming strategic companies from hostile takeovers by non-European actors originating in countries whose governments often make clandestine state subsidies to their business.

EU increasingly reliant on LNG gas supply

Energy security and dependence of a significant number of member states on the import of Russian gas remain of the highest importance for the EU. The Southeast and Central Europe are particularly affected by the Russian dominance in the gas supply. Thus, the issue of gas supply diversification remains pertinent. This matter is reflected in the significance and potential of the LNG terminal on the island of Krk, which will have a regional impact.

Russia has sought to maintain the dominant position in the gas supply of Europe and with that purpose it has launched projects to construct the new gas pipeline Nord Stream 2 and to extend the TurkStream to serve its geopolitical and economic interests. Additionally, declining prices of the liquefied natural gas (LNG) have contributed to a rapid growth of the European LNG market, bolstered by investment in transport and distribution infrastructure. All of these factors have led to a decrease in the supply of Russian gas to Europe in 2019 by 9 percent, down to 147.4 billion cubic meters (bcm) year-on-year.

According to the European Commission data, the EU experienced record LNG consumption in 2019 (108 bcm), or approximately 22% of the total gas consumption in the EU. This accounted for 27% of total imported gas to the EU. Of the imported gas, 30 bcm, 21 bcm and 17 bcm were imported from Qatar, Russia and the USA, respectively.

The belt of instability poses security threats to Europe

The belt of instability that encircles Europe continues to pose the greatest challenge to the European security. The belt extends throughout North Africa and across Middle East to Central Asia. Intense armed conflicts, such as those in Libya and Syria, have continued in the region. The conflicts have also been characterized by foreign interventions.

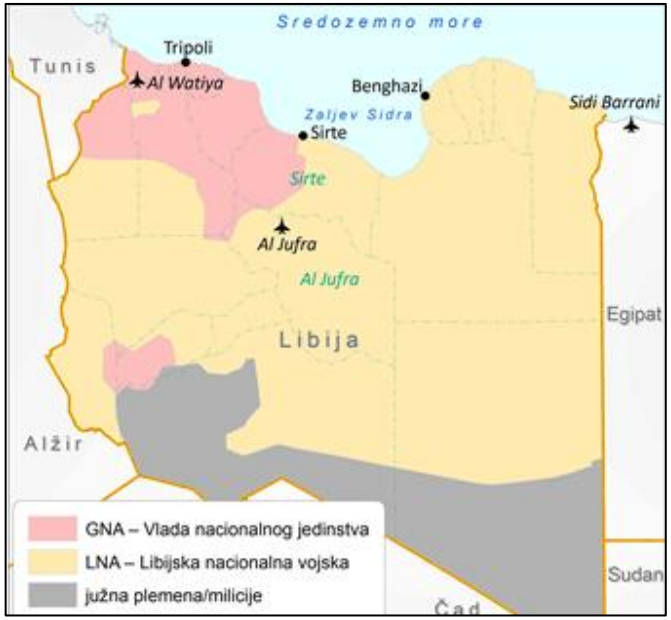
The belt has been a long-term source of various security challenges and threats such as terrorism, illegal migrations, proliferation of WMD, organized crime, extremism and armed conflicts. In addition, countries in the region have been struggling with collapsing institutions, failing economies, corruption, unemployment and poverty.

Europe has also been struggling with frozen conflicts, with no signs of breaking an impasse and no political resolution in sight, in the areas ranging from Ukraine to crisis hot spots in the Caucasus.

Syria remains the most complex global crisis hot spot. The conflict in Syria has seen both political and military involvement of a number of global and regional powers. For example, Russia and Iran have shown active military involvement as allies of the government in Damascus, whereas areas controlled by rebel groups have Turkish military presence. The government in Damascus has managed, with the Russian and Iranian military and political support, to regain most of the territory and to launch military operations, thus reducing the area of last strongholds controlled by rebel groups in the northwestern governorate of Idlib. Turkish military is also present in the area, sparking numerous incidents and armed conflicts with Syrian forces and their allies. In 2019, following the US withdrawal from the area, Turkish troops launched several operations in the area controlled by the Kurds, pushing Kurdish forces away from parts of the Syrian-Turkish border.

After Russia intervened in Syria and consequently strengthened its position in this region, it has also been trying to increase its influence in Libya, another major crisis hot spot in the Arab world.

Since May 2019, Libya has been struggling with another civil war waged between internationally recognized government in Tripoli and forces of the Libyan National Army under the Tobruk-based government, which is not recognized internationally, and which controls majority of the Libyan territory. Turkey has shown active support for the government in Tripoli, whereas Egypt recognizes the authority of the Libyan National Army. After one year, the conflict continues, with no political resolution to the crisis in sight. The parties to the conflict in Libya recruit Syrian fighters as mercenaries. The European Union Naval Force Mediterranean Operation IRINI was launched on 25 March 2020, near the Libyan coast, with the aim to enforce the arms embargo to Libya, prevent the illicit export of petroleum and disrupt human trafficking. The Republic of Croatia took part in the operation.



The situation on the front lines in Libya in July 2020

Military escalation of tensions between the USA and Iran poses possibly the greatest threat to the stability in the Middle East. Iran has been actively involved in all crisis hot spots in the Middle East. In addition, its relations with Saudi Arabia and Israel have been especially strained.

Decreasing petroleum prices and COVID-19 health care crisis might further destabilize weaker countries in the Middle East and Africa, whose income is most heavily reliant on sales of crude oil.

Yemen, Afghanistan and Iraq remain active crisis hot spots and long-standing Israeli-Palestinian conflict remains unresolved as well. The USA has been actively involved in negotiations with the Taliban to arrange a ceasefire in Afghanistan. In addition to the Taliban, ISIS has also been active in Afghanistan and terrorist attacks are commonplace.

Frozen conflict in Ukraine also continues and despite diplomatic efforts and new political leadership, no significant headway has been made in the implementation of the Minsk Agreement. After presidential election results were published, declaring a victory of the long-term president Lukashenko sparked massive opposition protests in Belarus, claiming the elections were rigged.

Border and economic disputes between the countries in the gas-rich region of Eastern Mediterranean have intensified, and the Greek-Turkish dispute over sea border delimitation remains an open question.

Terrorism still a threat to Europe

Islamist terrorist organisations continue to pose a major terrorist threat to Europe.

Although the Islamic State (ISIS) has suffered a military defeat in Syria and Iraq, its network, members and supporters remain a serious and global threat. This is also the case with Al-Qaeda.

Outside Europe, the greatest terrorist threats remain in crisis hot spots and destabilized areas with active ISIS and Al-Qaeda branches (Middle East, North Africa, Sahel, and Horn of Africa, Arabian Peninsula and middle and Southeast Asia).

While the risk of terrorism remains high in Western Europe and medium in Croatian south-east neighbourhood, in the Republic of Croatia this risk remains low.

In addition to ISIS returnees, local Islamist terrorist networks, their members, and self-radicalized individuals pose a major threat in the European countries.

Terrorist groups use the Internet and modern communication technologies to recruit members, train them and instruct them on their course of action.

ISIS propaganda is still primarily used to recruit and radicalize terrorists and to incite them to commit terrorist attacks in Europe. Against this backdrop, the use of the Internet to self-radicalize members of terrorist groups poses a major risk, as this is difficult to detect and uncover, and account should also be taken of the fact that a significant number of them suffer from mental health disorders.

On 27 October 2019, ISIS leader Abu Bakr al-Baghdadi committed suicide in his hiding place by detonating a suicide vest, during the US military operation in the north of Syrian governorate of Idlib, near the Turkish border

Terrorist groups constantly seek new ways of exploiting and misusing new technologies for terrorist attacks.

Terrorist attacks committed in Europe in recent years have been carried out by self-radicalized individuals in unprotected areas with large crowds. The attacks were committed by using cars, trucks and knives.

Ayman Zawahiri, leader of Al-Qaida

Since 2017, the number of terrorist attacks in Europe has declined significantly. Terrorist organisations carry out terrorist attacks in third countries as well, in their attempt to attack Western targets and values.

Local Islamist terrorist organisations pose a threat in other parts of the world as well. In April 2019, in Sri Lanka, a series of suicide attacks on churches and hotels were carried out, leaving 258 persons killed, of whom 45 were foreigners. Similarly, in Nigeria, terrorist attacks are frequently carried out by Boko Haram organisation.

Several factors have led to a decrease in the number of terrorist attacks in Europe. The ability of Islamist terrorist groups to plan and carry out their attacks has been diminished as a consequence of the losses they suffered in the areas in which they planned their operations. On the other hand, the efficiency of security and intelligence and law enforcement agencies has increased and cooperation between international security and intelligence and police agencies has intensified.

In recent years, some western countries have seen a rise in cases of the so-called far-right terrorism, i.e., armed attacks targeting primarily minorities and foreigners. A case in point is the attack carried out on 15 March in New Zealand against mosques, during Friday Prayer, leaving 49 people killed and the attack in Hanau, Germany, carried out on 19 February, leaving 9 people dead. These kind of attacks were carried out by a single gunman, suffering, as a rule, from a mental health disorder, and without affiliation with any terrorist organisation, organized support or involvement of other persons.

Security risks posed by ISIS fighters returning to their home EU countries

Following a military defeat of ISIS, thousands of captured fighters and their families, who joined them in Syria and Iraq, are being detained mostly in camps controlled by Syrian Democratic Forces (SDF). The repatriation process to their home countries is underway. Former ISIS fighters are held in prisons controlled by SDF forces while women and children are held in closed camps. A large number of women in camps remain highly radical and continue to support terrorism, subjecting their children to the same indoctrination.

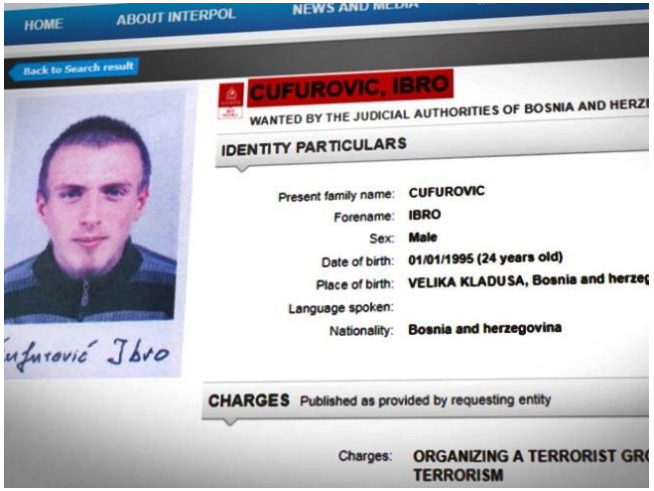
Since the beginning of the civil war in Syria, more than 5000 individuals have joined Islamist terrorist groups in Syria and Iraq. 1700 individuals have returned to their home countries in the EU and most returned before ISIS's defeat in Syria.

A total of around 1000 individuals from Croatian SE neighbourhood have left for Syria and Iraq, most of them joining ISIS. 25% of them have been killed, 30% remain in the area and 45% have returned to home countries in the Southeast Europe. During 2019, 136 individuals, of whom 12 former ISIS fighters and the remaining women and children, returned from Syria to the neighbouring countries in the Southeast.

The return of jihadists poses a great security risk for Europe, especially for the countries with a significant number of returning fighters, who fought on the side of terrorist organisations,

underwent military training and were further radicalized and traumatized on the battlefield.

Adequate deradicalization programmes and prosecution of returning fighters - former members of terrorist organisation will play a significant role in the reduction of such risks.



An arrest warrant for ISIS member, sentenced, in December 2019 in Bosnia and Herzegovina, to four years in prison on terrorism charges. He joined ISIS in 2014 and fought in Syria. Following a defeat of ISIS and his capture, in April 2019, he was repatriated, together with his wife and two children, from Syria to Bosnia and Herzegovina. During the trial, he admitted to his involvement in ISIS.

Some countries have seen a phenomenon of Islamic radicalization among prison population. In this context, ISIS returnees serving their prison sentence among general prison population pose a significant risk. In addition, practice shows that, in the neighbouring countries, sentences of only several years are handed down for involvement in terrorist organisations. Consequently, a significant number of prisoners are near the end of their prison term or have already been released. In some countries the practice is to prosecute only returning men, whereas returning women do not face prosecution and remain free regardless of their possible radicalization and terrorist activities.

This highlights the importance of deradicalization programmes and the fact that there are many repatriated children who were subjected to indoctrination and training in the terrorist-controlled areas, and who also participated in combats and were traumatized by the experience, and in many cases by the deaths of family members.

Some countries in the SE neighbourhood are still struggling with the issue of Islamist radicalization and terrorism in parts of their societies.

Another security challenge for the Republic of Croatia is transit of foreign nationals, for whom there are indications of supporting terrorist activities, across the Croatian territory. This is further highlighted in the context of migration flows across the Croatian territory.

Security environment in the Western Balkans remains unstable

Croatia's neighbouring countries in the Southeast, i.e., the Western Balkans as they are referred to in EU documents, are still struggling with a number of security, political, economic and social challenges.

All Western Balkan countries express their intentions of accessing the EU. In addition, Western Balkan countries, apart from Serbia, express their intention of accessing NATO as well. At the same time, countries such as Russia and China seek to strengthen their position in the area.

This area is faced with troubled economy, corruption and organized crime, political clientelism and weaknesses in the rule of law. Southeast countries are also struggling with radical Islamist and nationalist forces and with obstacles to their accession to the Euro-Atlantic integration. Some countries in the SE neighbourhood still function with active involvement of the international community and their mechanisms.

This situation opens the door to external actors, especially to countries whose interests and views do not align with the Euro-Atlantic perspective for this area, i.e., whose aim is to hinder the Euro-Atlantic integration in the area. To achieve their goals, these actors resort to intelligence ad hybrid activities.

On 17 November 2019, a YouTube video was published, showing a Russian assistant military attaché in Serbia handing over money to an unnamed Serbian Army officer

Despite the fact that the EU integration process has slowed down, the accession of Montenegro and North Macedonia to NATO provided stability and good outlook for the countries in the region. At the same time, because of their accession to NATO, some countries that perceive NATO as a security threat might exploit certain internal processes in new NATO members with the aim of destabilizing them. Unresolved interethnic relations and tensions in certain countries are sometimes exploited to promote foreign geopolitical goals.

The society in Montenegro is divided between pro-western forces supporting independence and pro-Serbian forces who are against the country's membership in NATO and are in favour of stronger ties with Russia.

There are several stabilization processes underway in the SE neighbourhood. These processes have an impact on overall political and security circumstances in the region. Two of such crucial processes are agreements on internal functioning of Bosnia and Herzegovina (BiH) and negotiations to normalize relations between Serbia and Kosovo. The international community is actively involved in both processes. Complex political situation in BiH has faced setbacks in many processes. Kosovo is also struggling with political instability following fall-elections in 2019.

In the context of foreign policy and security, Serbia keeps balancing its ties with Russia and the West. For instance, as an EU candidate country, Serbia has continuously failed to follow restrictive EU measures imposed against Russia. Over the past years Serbia has placed significant emphasis on strengthening and promoting its ties with China.

In some neighbouring countries, efforts have been made to negatively portray the Republic of Croatia, mostly by publishing fake news in the media and on social networks. In some neighbouring countries, anti-western sentiment is prominent, especially in the media reports.

Countries in the SE neighbourhood are also struggling with religious and national extremism.

Great Serbia-related extremism has been continuously present in the neighbouring countries, as well as the denial of territorial integrity and sovereignty of the Republic of Croatia, and other neighbouring countries such as Kosovo, BiH and Montenegro. Such extremism is reflected and espoused in public appearances and gatherings held by extremist organisations advocating the idea of Greater Serbia and other public gatherings, used to promote extremist messages and destroy Croatian national symbols. Greater Serbian extremism and ideology promote messages against enlargement of the EU and NATO to include Southeast Europe, and emphasizes its allegiance to Russia.

Radical interpretation of Islam continues in the SE neighbourhood. Enclaves advocating radical interpretation of Islam and refusing to recognise the legal and democratic order of their host country pose a security risk. Further security risk is also posed by jihadists from Syria/Iraq returning to home countries. In fact, many of them had gone to the war zones from those enclaves. These two factors might lead to further radicalization and radical interpretation of Islam.

The position of Croats in Bosnia and Herzegovina has been marked by efforts to achieve political equality with the other two constituent peoples in accordance with the existing constitutional system of Bosnia and Herzegovina. In addition to political context, the trend of economic migration of Croats from Bosnia and Herzegovina has continued, which threatens the survival of Croats living there and the multi-ethnic character of Bosnia and Herzegovina.

Strong presence of transnational organized crime in Southeast Europe

Organized crime groups originating in the SE neighbourhood of the Republic of Croatia pose a major risk for the country. These groups have strong ties with organized crime groups in Croatia.

Despite the efforts of countries in the SE neighbourhood, organized crime remains strong and well-organized with numerous international connections, including ties with Croatian criminal groups. Conflicts between and killings of members of opposing criminal groups have, for years, been commonplace in the SE neighbourhood, with several dozens of them killed. Armed conflicts between those groups are frequent also outside their own countries.

The so-called Balkan route serves as the main route for the supply of heroin to Europe, and is very important for marijuana trafficking.

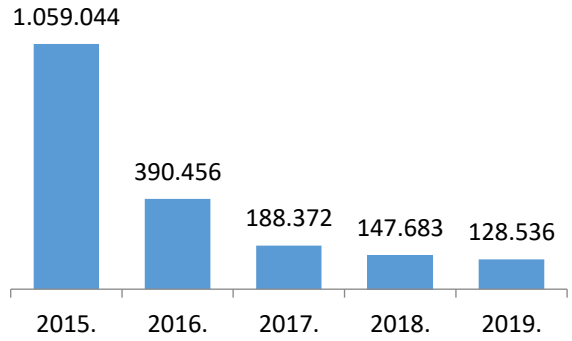
In recent years, organized crime groups from the SE neighbourhood have gradually taken an increasingly important role in drug trafficking in the EU, for example, supplying cocaine from South America.

In addition, organized crime groups from the SE neighbourhood are also actively involved in human and arms trafficking. Migration intensity along the Balkan route and closure of some borders along these routes have led to an increase in human trafficking.

There have been many attempts to smuggle arms into Western Europe across the Croatian territory. Several such attempts were prevented in 2019. In terms of arms trafficking, there is a constant risk of trafficking of goods which might be used as components for weapons of mass destruction.

Stronger pressure of illegal migrations towards Europe across the Croatian territory

The intensity of migration flows towards Europe from the Middle East, Central Asia and Africa has continued. According to the data provided by the UN's International Organisation for Migration (IOM), the number of migrants arriving to Europe has been decreasing. In 2019, there were 128,536 migrants recorded.

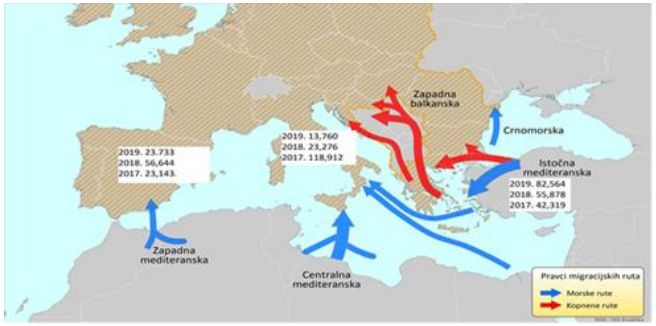


The registered number of migrants entering Europe, broken down by year (source: IOM)

The total migration flow intensity has decreased over the recent years, primarily due to a reduction in the number of migrants on the central migration route leading from Libya to Italy, renewed armed conflicts in Libya and tightened Italian measures.

Despite the overall decline, migration flows along the so-called Balkan (east Mediterranean) route have intensified over the past three years, as most migrants attempt to cross the Croatian territory in order to illegally make their way to Western Europe.

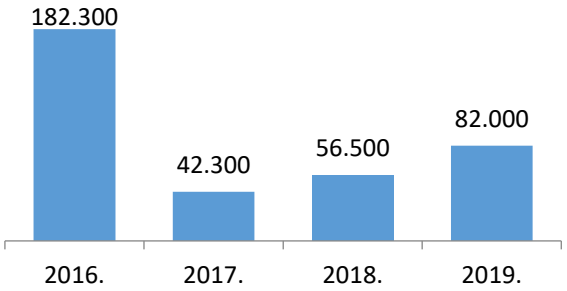
Turkey remains the main entry point for migrants arriving from Asia and Africa and heading towards the EU. Consequently, the Balkan route has become the main route for most migrants making their way to the EU. This means that the Balkan route has become exceedingly attractive for organized crime groups engaged in migrant trafficking. Most migrants along the Balkan route attempt to reach EU through the BiH territory.



Mediterranean migration routes

According to Frontex data, in 2019, more than 82000 illegal migrants were detected along the Balkan route, an increase of 46% year-on-year.

Ramped-up controls along migrant trafficking routes have led to their diversification. For several years now, the migration flow has been the most intensive along the migration route stretching from Serbia towards western BiH, where migrants attempt to make their way towards western EU across the Croatian territory.



The number of illegal migrants along the so-called Balkan route, by years (source: Frontex)

According to IOM data for 2019, of the total number of migrants along the Balkan route, 24% were from Pakistan, 18% from Afghanistan, 10% from Syria, 9% from Morocco, 8% from Iraq, and 31% from other Asian and African countries.

Countries along the Balkan route lack sufficient capacities to accommodate a larger number of migrants, and consequently, migrant pressure leads to strengthening of criminal networks. In addition, the increase in the number of migrants on the Balkan route was also facilitated by the liberalization of visa regimes between some countries in the SE neighbourhood and the migrant home countries.

The security situation in Croatia

is stable and there are currently no indications of wider destabilization

The security situation in Croatia is stable. In 2019, there were no events or incidents which could have posed a significant threat to security in the Republic of Croatia.

There are currently no indications or visible possibilities of wider destabilization.

In the territory of the Republic of Croatia, the terrorism threat level is low

In the territory of the Republic of Croatia, the terrorism threat level remains low. Although the likelihood of possible terrorist attack cannot be ruled out, there were no indications of increased terrorism threat in the Republic of Croatia in 2019. However, one Croatian soldier was killed and two were injured in a terrorist attack carried out by the Taliban, targeting NATO-led Resolute Support mission in Afghanistan in 2019.

Regional members and supporters of Islamist terrorist organisations and returnees from Syria/Iraq pose the greatest risk in terms of terrorism threat. There are only a few dozen members of the Salafi movement in the Republic of Croatia and they do not advocate violence or terrorism.

The experience of the western countries shows that terrorist attacks are often carried out by self-radicalized persons suffering from mental health disorders. Therefore, there is an underlying risk that individuals might become self-radicalized and, prompted by terrorist propaganda or mental health disorder, might carry out terrorist attacks.

One of the risks is also the transit of persons, who support or advocate terrorist groups, across the territory of the Republic of Croatia. To reduce the risk of this challenge, SOA has taken appropriate pre-emptive actions in order to protect the Republic of Croatia and other European countries.

Of the total of seven (also) Croatian nationals (two men and five women) in the ISIS-controlled area, available data indicates that two men and one woman were killed in 2017 and 2018 in Syria/ Iraq. The remaining women are still in civilian camps controlled by Kurdish-Arab forces in Syria.

Extremism in the Republic of Croatia has not gained momentum or public support

No type of extremism, regardless of its ideological, religious or national grounds, has gained wider public support and has very little potential to undermine democratic rule of law, incite violence, incidents or conflicts on a larger scale. Extremist groups have very few members, are not organized and enjoy poor public support. Consequently, no type of extremism in the Republic of Croatia constitutes a significant threat to the national security and the threat remains low.

Extremist members of sports fan groups occasionally clash, disrupting public order and destabilizing security in certain communities. Violence among sport fans has a tendency to turn into inter-ethnic conflicts.

Although the Western Europe has seen an increase in the so-called far-right or anti-immigrant extremism, there is no serious anti-immigrant extremism in the Republic of Croatia. However, the trend of strengthening of anti-immigrant movements in Europe could lead to a similar trend in the Republic of Croatia.

Although Islamist radicalism in the Southeast Europe has gained a significant number of supporters, it has failed to attract a greater number of followers in the Republic of Croatia and poses no threat to the national security. Islamist radicalism in the Republic of Croatia refers to a several dozen individuals of the Salafi movement who do not advocate violence.

Foreign intelligence activities towards the Republic of Croatia have been particularly evident in the aftermath of its accession to NATO and the EU, and due to the Croatian role in the stabilisation processes in Southeast Europe

Some countries engage in intelligence activities and intelligence collection in the Republic of Croatia. These are the countries that have unresolved issues with the Republic of Croatia, or perceive the Republic of Croatia, separately or as a member of the Euro-Atlantic integration, as a rival or security or political challenge.

Main points of interests for foreign intelligence in the Republic of Croatia include, among other things, positions and processes within NATO and the EU, Croatian policies towards the SE neighbourhood and unresolved issues, inter-ethnic relations, energy security and issues pertaining to Croatian economy.

Intelligence activities towards the Republic of Croatia have been particularly evident in the aftermath of its accession to NATO and the EU, and due to the Croatian position and role in the stabilisation process of Southeast Europe, which is still in the process of accession to European and Euro-Atlantic integrations.

Some foreign agencies have attempted to use Croatian territory in their intelligence activities towards third countries.

In this respect, countries that perceive NATO and the EU as a security challenge or threat, see the Republic of Croatia as a point of intelligence interest. These countries have made attempts to gain wider influence in Southeast Europe, which does not align with Euro-Atlantic perspective of the area.

SOA Director takes part in a panel discussion on fake news and disinformation at the European Commission's security symposium held on 15 October 2019

Foreign intelligence activities include dissemination of information towards the Republic of Croatia, which means that fragmented data, fake or distorted news disseminated to shape an opinion about an event and/or change public awareness and attitudes, are published in the public and media.

The aim of such activities is to negatively portray the Republic of Croatia, the EU and NATO and to undermine the stability of government institutions and the region, to portray the Republic of Croatia as an unreliable NATO and EU member, and to weaken Euro-Atlantic and European partnerships.

News websites and media platforms, and sometimes even scientific institutes, are exploited to spread fake news, thus lending credibility and legitimacy to fake news and misleading statements.

SOA invests in the enhancement of national cyber security

Global cyber threats have been on the rise and a growing number of sophisticated cyber threats, together with an increasing reliance of modern societies on cyber technologies calls for a new approach.

As a NATO and EU member, the Republic of Croatia has been the target of cyber-attacks sponsored by certain states. The attacks were carefully planned, advanced and persistent (APT - Advanced Persistent Threat) and characterized by high level of expertise where the perpetrators were able to evade detection for a longer period. The most common goal of APT attacks is to steal classified information (political or industrial espionage). However, the attacks might also aim to damage national critical infrastructure or key digital services of the country. There has been a growing trend within organized crime to use complex tactics and techniques of APT attacks for ransomware or for frauds in the financial sector.

Consequently, SOA has initiated, in cooperation with other competent authorities, an extensive process of prevention and protection of the national cyberspace. As part of this process, in 2019, SOA set up a Centre for Cyber Technology. The purpose of this Centre is to protect national cyberspace from state-sponsored cyber-attacks and APT campaigns, by using a network of sensors placed within the bodies under protection.

The Centre ensures a fast and efficient application of security and intelligence and other technical information and knowledge, gained through international security and intelligence exchange and other available global sources.

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 and intelligence capabilities, and its aim is to detect, prevent and attribute state-sponsored cyber-attacks and APT campaigns targeting the Republic of Croatia. Consequently, the risk of compromising key national information sources is minimised.

Cyber APT attacks target carefully chosen and closely examined targets, and are carried out by hacker groups linked to intelligence systems in specific countries. Over the recent years, the Republic of Croatia has been the target of a dozen cyber APT

attacks. Following the establishment of the Centre for Cyber Technology, SOA is nowadays able, by means of a network of sensors, to detect on a daily basis, hundreds of thousands security-related issues, which are prioritized and dealt with, in cooperation with several national bodies with different functional and sectoral competence.

In the course of 2019, five sophisticated state-sponsored cyber APT attacks were detected and prevented, including attacks on the Ministry of European and Foreign Affairs and Ministry of Defence. There has been a growing trend of frequent cyber APT attacks against the Republic of Croatia in 2020. The trend has been further bolstered by the outbreak of COVID-19 pandemic, used as a pretext to carry out further cyber-attacks.

As in previous years, there has been an increase in various cyber activities categorized as cyber-crime. The global trend of using complex tactics and techniques of APT attacks to target business systems of strategic and major companies has led to the same trend in the Republic of Croatia, a case in point being the cyber-attack on INA oil company.

Consequently, SOA's Centre for Cyber Technology and its protection of national cyberspace, although primarily focused on the state and public sector, is open to other sectors as well.

LNG terminal to strengthen energy security of the Republic of Croatia and neighbouring countries

The EU's ambitious decarbonisation policy and dynamic changes in the energy and technology sector require a ramp-up of capacities to enable the economy to adapt to such environment.

Current situation regarding energy security the Republic of Croatia requires less rely on imported energy, diversifying supply routes thus ensuring security of supply and reducing vulnerability and susceptibility to external factors, and use of new technologies based on renewable resources.

Future LNG terminal on the island of Krk

As a result, the construction of new LNG terminal on Krk is underway, the aim of which is to strengthen energy security of Croatia and neighbouring countries.

Geopolitical circumstances have direct implications for energy security and energy markets, resulting in great volatility in oil prices on the global market. COVID-19 pandemic has further destabilized oil prices on the global market.

The consequences of COVID-19 pandemic will also have an impact on economic security

In line with its legally defined authorities, SOA provides continuous support to competent state authorities in the field of protection of the fundamentals of the economic system of the Republic of Croatia, especially economic operators exerting significant impact on economic situation in Croatia. SOA provides the state leadership and decision-makers with information relevant for their scope of work.

Given the fact that SOA's continuous task is to combat economic crime, the Agency reports its findings to the State Attorney's Office and the Croatian Police.

Croatia has an open economy, focused mainly on the EU markets, and with tourism sector accounting for a significant proportion in GDP structure. Consequently, economic disruptions caused by the outbreak of COVID-19 pandemic will have an impact on the Croatian economy.

During the COVID-19 crisis, the Republic of Croatia has introduced a number of measures with the aim of safeguarding economic stability. The European Union has relaxed its budgetary rules thus allowing the governments of member states to support the recovery of their economies. The recovery of Croatian economy relies heavily on the recovery of the overall EU economies.

Corruption and economic crime hinder development and prosperity

Not only does corruption in public administration, government institutions and authorities and state-owned companies have an adverse social impact but it also poses a significant threat to economic development of the Republic of Croatia. It hinders the proper functioning of the market and economic growth, reduces the amount of public finances and leads to state budget shortfalls.

Public procurement processes and their misuse are particularly sensitive areas in suppressing corruption and economic crime.

Criminal groups and individuals use various fraudulent transactions and frauds to make illicit financial gains. They are also involved in corruptive activities aimed at authorities at different levels.

Given the large financial amounts and complexity of projects, major infrastructural projects, including EU - funded projects, are vulnerable to the risks of corruption.

There has also been 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 companies, cash extraction and money laundering also have an international dimension.

SOA reports its findings concerning corruption and organized crime to the Police and State Attorney's Office of the Republic of Croatia.

Organized crime groups have ties with regional crime groups

The cooperation between members of Croatian and regional crime groups has intensified. The groups exchange and engage members from criminal groups in neighbouring countries to carry out criminal activities on their territories, providing also logistic support for activities on the territories of other countries.

Transnational cooperation between criminal groups has been strengthened especially in the field of drug trafficking. Several Croatian nationals were apprehended in an international police operation carried out in September 2020 on the Canary Island (territory of the Kingdom of Spain). They were suspected of trafficking large quantities of cocaine on cruising sailboats. Cocaine was intended for the European illegal drug market.

The pressure of illegal migration spurred the growth of organized human trafficking.

As in previous years, there have been attempts of arms trafficking from the territory of Southeast Europe, across the territory of the Republic of Croatia. The arms were intended for the markets of west and north Europe.

Frequent armed clashes between organized crime groups from the neighbouring countries have continued over the years, leading to brutal killings of members of opposing factions. There is a risk that some of these clashes might take place on the territory of the Republic of Croatia.

Opposing criminal groups often clash in places gathering large crowds.

SOA's interest is also focused on war crimes and people missing in the Homeland War

One of the priorities of the security and judicial system is to determine the fate of persons missing in Homeland War, identify mass and individual graves and to prosecute war crimes.

In cooperation with other competent authorities, SOA continues to actively collect intelligence and documentation in order to identify the perpetrators, victims and circumstances of war crimes committed during the Homeland War, to determine the locations of mass and individual graves of persons missing in Homeland War and to determine the location of persons suspected of war crimes.

Further development of the Republic of Croatia is hindered by negative demographic trends

Negative demographic structure and negative population growth in the Republic of Croatia do not pose a direct threat to national security, however, should such trends continue, they will in the long-run hinder further social and economic development of the Republic of Croatia.

Intelligence College in Europe

was set up to develop a shared strategic intelligence culture

On 26 February 2020, the Letter of Intent concerning the development of Intelligence College in Europe was signed in Zagreb. The College is a platform which promotes and facilitates a dialogue between European intelligence communities, decision-makers and academic community to enhance strategic thinking and mutual knowledge and to develop a shared European intelligence culture.

The Intelligence College has three missions:

- to raise awareness of intelligence-related issues among decision-makers and the public,
- to foster better mutual understanding of intelligence-related work and European policies creation,
- to enhance European strategic thinking among intelligence professionals, in cooperation with European universities and think-tanks.

The idea was initiated by French President Emmanuel Macron in his speech delivered in September 2017 at the Sorbonne, calling for a stronger Europe. Macron said that he would like to see the establishment of a European intelligence academy to strengthen the links between intelligence communities in EU member states through training and exchange activities.

The ceremony of signing of the Letter was organized by the SOA in cooperation with the temporary College Secretariat based in Paris. 30 countries were invited to become members of the College (27 EU member states + United Kingdom, Norway and Switzerland). 23 countries signed the Letter of Intent (France, Germany, Italy, the Netherlands, Hungary, Austria, Belgium, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Latvia, Lithuania, Malta, Norway, Portugal, Romania, Slovenia, Spain, Sweden, and the United Kingdom).

At the ceremony it was proposed that SOA should take over the presidency of the College for the first year, to be followed by the United Kingdom and Italy. After its first year of presidency, SOA would remain part of this three-member group.

SOA Director signs the Letter of Intent concerning the development of the Intelligence College in Europe

This was the biggest public event SOA has ever organized to date. SOA has organized other major but closed conferences, such as the biggest NATO terrorism expert conference organized every year in May. However, this conference has a public

dimension to it and is a sign that European intelligence services are starting to become more open towards the public. In this context, the aim is to enhance the visibility of intelligence sector in Europe.

The ceremony of signing the Letter of Intent was attended by Croatian state leadership, headed by Andrej Plenković, Croatian Prime Minister

The College provides a network and fosters a spirit of collegiality between European intelligence communities in order to facilitate the sharing and cooperation between them. The aim is also to bring intelligence community closer to other communities, academic community being one of them.

Intelligence communities tend to be closed and have a specific business culture. In this way they seek to improve their dialogue with other communities. It is therefore essential to lay the foundations necessary to facilitate discussion and exchange of views between European services, and with other institutions.

The College is not an operational platform. It is not an intelligence-sharing forum. The College was not launched as part of the EU organisational structure, although its membership is closely linked to the EU (EU member states, United Kingdom, Norway and Switzerland).

The College is a network and has no bigger permanent or governing structures. The aim is to provide a more flexible work framework. Its activities will mostly include seminars on specific security issues, to be held in member states wishing to organise specific events. On 17 December 2019, SOA organized a round table to discuss the role of security and intelligence systems in modern day security-related context. The round table was attended by panellists and university students from Zagreb and Split (Faculty of Croatian Studies, the Faculty of Humanities and Social Sciences, Faculty of Political Science, University Department of Forensic Sciences in Split and Military Leadership and Management study programme).

Signatories have oversight and voting rights in the steering body, especially in relation to the schedule and scope of activities to be implemented. The College is comprised of Members and Partners, which may eventually become members of the College later. The College Secretariat will be based in Paris.

The College consists of three components: academic, reflective and strategic - communicative:

- Academic component consists of modules to be held at various universities, and attended by employees working for various bodies in member states. This will allow the participants to build a network of contacts and knowledge.
- Reflective component includes strategic thinking on current and future challenges faced by many member states. It will include a wide range of topics such as: impact of new technologies on security, future of terrorism, intelligence work, and protection of privacy and similar. Conclusions will be published in scientific and academic journals in order to share the ideas and concepts and invite wider public discussion.
- The aim of strategic and communication component is to raise public awareness of intelligence-related issue, especially within the European institutions. One of the aims is also to ensure that decision-makers have a better understanding of intelligence work (officials, Parliament members, judges and similar). Better understanding and knowledge of intelligence communities will facilitate decision-making and discussions about the development of intelligence communities.

SOA Centre for Cyber Technology

presented at the conference Cybertech Global 2020 in Tel Aviv

SOA Director gives a presentation at Cybertech Global 2020, held on 29 January 2020 in Tel Aviv, Israel:

When you see director of a secret service, you probably expect to hear him say that we live in precarious times. In fact, I can personally assure you that it is so.

The time we live in is characterized by complex security challenges and technological progress constantly generates new and disruptive technologies. Today, each traditional security challenge, such as terrorism or foreign espionage, is reflected in the digital world as well. Cyber space has thus added another dimension to security and intelligence work.

Terrorists use cyber space to spread their ideologies, share the know-how, recruit new followers, communicate, plan terror attack and finance their efforts with cybercurrencies. Today's spies no longer risk their lives carrying small cameras to photograph a few pages of a classified document. Instead, they are able to download gigabytes' worth of classified documents one thousand km away if they are able to penetrate a secured system. In the Big Data era, secret services do not struggle with lack of information, rather they have problems selecting and triaging enormous amounts of data generated online by the second.

New and disruptive technologies change all aspects of life, including security and intelligence work of every service in the world. One the one hand, these new technologies enable developing new capabilities which were up till recently inconceivable to secret services. On the other, they may also be used to threaten national and international peace and stability.

A deep fake video showing a celebrity like Bar Rafaeli or Gal Gadot can be a media bomb, but a deep fake video of a world leader calling to war may lead to real bombs! The role of security and intelligence services in the digital world will increasingly consist of separating the truth from the lies.

Technological advancement has a significant disruptive effect on our operational efforts as well. In this tide of technological progress and society's digital transition, Croatian Security-Intelligence Agency is doing its best to ride the wave of technological changes by developing new capabilities and adding a digital aspect to its activities.

We, as a service, consider the protection of our cyber space from Advanced Persistent Threats (APT), state sponsored cyber-attacks and attacks capable of endangering our national security and interests especially important in today's digital world. In that sense, we are expected to be proactive in neutralizing cyber risks.

We have and develop the potential to respond to these challenges, namely:

- people,
- technology,
- partners' network - national and international, and most importantly, what sets us apart, we have
- intelligence.

We have merged these four elements (people, technology, partnerships and intelligence) into one unit: the Cyber Centre.

In other words, we have envisioned a centre that will be at the very top in all of these elements and able to meet all our national needs and tasks.

We have envisioned a centre that will bring together outstanding intelligence work and latest technologies in cyber security.

The centre has a comprehensive approach to monitoring cyber threats, with the aim of including the most important national public and private stakeholders into an integrated protection system.

This means that, in terms of cyber security, we support close coordination within the state sector, national cooperation of public, academic and private sectors and intensive international cooperation.

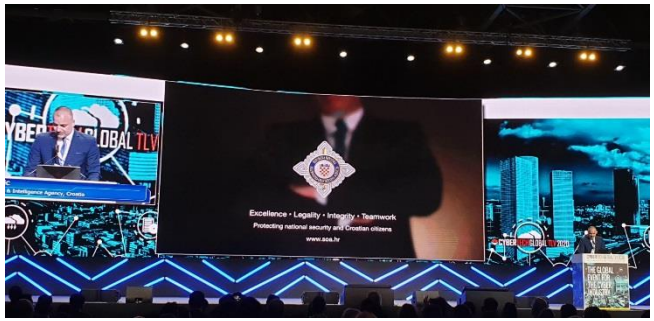
In this context, we are open to cooperating with any partner able and willing to help us perform our tasks thoroughly and professionally and expand our knowledge so that we remain at the top of technological advancement.

We are a small service facing big and global challenges. We are not alone in this; we have many friends and allies.

We strongly believe there is only one path towards fulfilling our vision and tasks and that is the path of excellence in all aspects:

- We want to provide top training and skill sets to the centre's staff;
- The technology we use must be top notch;
- Our partnerships, both national and international, must be built on mutual trust and benefits of cooperation,
- The information we have must be precise, timely and reliable.

People, technology and partnerships are our ticket to the future. That is why we look forward to travelling there and taking each step towards strengthening our cyber capacities! In that future, we wish to be known as "the little agency that could".



Deepfake

as an example of possible misuse of disruptive technology

Disruptive technologies are innovative or new technologies that significantly alter existing or create completely new industries. Their impact sometimes radically changes the way of life, behaviour, thinking and doing business.

Disruptive technologies have been a part of the entire human history, helping the mankind to make progress. Some of the examples include: the invention of script 5,500 years ago and the beginning of recorded history, the invention of the steam engine leading to the industrial revolution, to name but a few. One of the most significant examples is the Internet. However, there are security implications to the development of technology. For example, the invention of the machine gun, seemingly of little significance, has changed the warfare completely, causing millions of fatalities in armed conflicts.

Many technologies that are being developed nowadays can be disruptive to all spheres of life. These technologies include mobile internet, AI, Internet of Things, electric and autonomous vehicles, 3D printers, drones, robots and various applications of biotechnology.

Disruptive technologies have changed societies and profoundly affected security. Depending on the application, such technologies may have a positive impact on the general security, but they may also be misused for undermining the security of individuals, groups or national security.

Great advances in machine learning, AI and digital video editing have made it possible to alter and fake faces and voices in videos, in order to manipulate and misrepresent that an individual had said or done something. Such fake video materials are known as deepfake. Deepfake technology has become more sophisticated, persuasive and available.

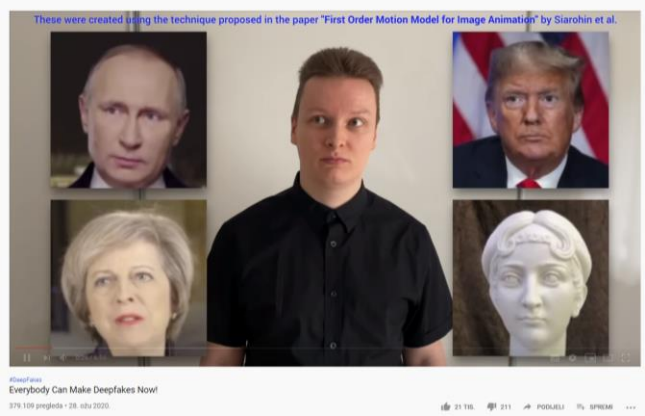
The term deepfake is a portmanteau of deep learning as a segment of AI and fake which indicates manipulated and artificially generated video.

With advances in technology, it will be increasingly difficult to distinguish fake from the real video and audio, because it will be possible to produce voice, speech, movements, facial expressions and other characteristics which are almost identical to the real characteristics of the person imitated by the technology.

For example, from a sample of someone's voice it is possible to generate fake speeches and statements that the speaker has never made. With such application, new technologies can become a tool in the information activities across the society.

This technology may also be misused for the production of fake video and audio with the aim of influencing democratic elections, financial and economic processes, general social attitudes on current topics, crisis decision - making processes, or to spawn panic and social anxiety.

Materials such as fake compromising videos may be used by terrorist and organized crime to blackmail and extort individuals. Fraudulent behaviour is another distinct possibility. For example, it is possible to fake video calls which can mislead individuals into thinking that they are speaking with a person close to them, when in fact they are communicating with a digitally generated image controlled by malicious intents.



Deepfake video (screenshot: Youtube (Two Minute Papers))

The technology of deepfake video production has been available for several years. It includes options for generating videos where one person assumes digital control of another individual's face and can make facial expressions and produce sentences which are then superimposed in a deepfake video on another individual's face and voice in real time.

The misuse of such technology has been a growing threat to privacy and national security, and the dissemination of deepfake materials can have a devastating impact on social divisions and undermine citizens' trust in state institutions and the media.

Debates about the prevention of misuse of deepfake videos have been emerging, and one of the most significant tasks for national security systems will be finding ways to recognize and prevent their adverse impact on democratic and security processes.

Security vetting

as a pre-emptive tool for enhancing the security of the Republic of Croatia

Security vetting is a type of pre-emptive activity. The aim of such activities is to strengthen security of organizations, that is, to prevent individuals who are subjects of security concerns from accessing sensitive data or serving in such capacities that would allow them to undermine security and interests of the Republic of Croatia.

Security vetting is a legally defined procedure whereby competent authorities establish the existence of security impediments for natural persons and legal entities. Security vetting procedures are carried out by the competent security and intelligence agency. SOA conducts all security vetting procedures related to civilians.

Security vetting is a significant segment of the Agency's work carried out regularly at the headquarters and at all centres. In 2019 the Agency completed a total of 6241 security vetting procedures. All security vetting procedures are aligned with the EU and NATO standards. In the light of the fact that security vetting infringes personal data, a transparent procedure of data verification has been established as per the Security Vetting Act.

Types of security vetting

There are three types of security vetting:

- security vetting for access to classified information,
- basic security vetting,
- security vetting for the protection of protected persons and facilities.

Security vetting for access to classified information is performed for natural persons who, within their scope of work or authorities, need access to information classified above the Restricted level or for legal entities which conclude contracts with state and/or other bodies classified above the Restricted level. The request for security vetting for access to classified information is submitted to the Agency by the Office of the National Security Council. Furthermore, the Office of the National Security Council issues certificates on the conducted security vetting for individuals who have access to classified information.

Security vetting for legal entities is conducted for the purpose of obtaining certificate of business security and includes, among other details, verification of the ownership and ownership structure, intelligence on companies overall business operations and financial obligations, security vetting of the owner and employees and other intelligence impacting business security. The request for security vetting for legal entities is submitted to the Agency by the Office of the National Security Council.

The Agency carries out basic security vetting and security vetting for access to classified information exclusively at the request of other authorities (with the exception of security vetting of the Agency employees), and subsequently reports back to these authorities on the conducted security vetting.

Basic security vetting is carried out for individuals appointed to a special duty, high-ranking state officials, new hires or employees of authorities significant for national security and other jobs. The request for basic security vetting is submitted to the Agency by the competent authority (for example the authority appointing or hiring the vetted person).

In addition to these three types of vetting, the Agency also carries out security vetting for persons who have direct access to protected persons and facilities, which is conducted at the request of the state authority competent for security and/or counterintelligence protection of protected persons, by applying the procedures established for security vetting for access to 1st, 2nd and 3rd degree classified information. The degree of security vetting in this case is determined by SOA on the basis of submitted data.

Degrees of security vetting

Security vetting procedures are carried out as 1st degree security vetting, 2nd degree security vetting and 3rd degree security vetting. 1st degree security vetting is conducted on the basis of the security questionnaire for 1st degree security vetting in line with procedures stipulated by the relevant acts. The same logic is applied to 2nd and 3rd degree security vetting.

Pursuant to legal provisions, 1st degree security vetting grants widest access to the data pertaining to the vetted person, while 3rd degree security vetting grants limited access.

Moreover, the Agency is legally obliged, as per the relevant act, to submit a report on the conducted security vetting to the relevant authority which has requested the 1st degree vetting in the period not less than 30 and not exceeding 120 days, the report on 2nd degree security vetting within the period not less than 20 and not exceeding 90 days, and the report on 3rd degree security vetting within the period not less than 10 and not exceeding 30 days from the day of receipt of the request.

Security vetting procedure

Security vetting procedure is conducted on the basis of the questionnaire for security vetting. An integral part of the questionnaire is the consent of the vetted person. The vetted person fills out the questionnaire personally and signs the consent for the security vetting. SOA shall not conduct security vetting without obtaining prior consent of the vetted person.

Security impediments

Security impediments in security vetting procedures for access to classified information include false data stated in the questionnaire for security vetting, facts that are stipulated by special Act as impediments for employment in the civil service, imposed disciplinary sanctions and other facts that constitute reasonable doubt in the trustworthiness or reliability of the person to administer classified data.

Security impediments in basic security vetting procedures are facts which indicate misuse or risk of misuse of official position or duty, rights or authorities to the detriment of national security or interests of the Republic of Croatia.

Security impediments in security vetting procedures for the protection of protected persons and facilities, are the facts which indicate the risk to their security.

The assessment to determine the security impediments is carried out by the competent authority, which had requested the security vetting, based on the report submitted by SOA.

Career at SOA

is a unique and challenging opportunity

Employment at SOA provides a unique career opportunity for challenging and dynamic work in the interest of the general well-being of the Croatian society.

We recognize our employees as our most valuable resource. Technological advancements and reliance on contemporary technologies have not reduced the importance of the human factor in the success of security and intelligence activities which still depends on the competencies, knowledge and skills of operatives.

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

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. This legal provision is standard in many other democratic European states.

Security and intelligence activities that the Agency addresses require experts from a variety of fields and specializations. These professionals are engaged in analytical and operative work, development of technology, count-intelligence protection, legal and financial operations and development of human resources.

The Agency employs candidates from a variety of educational, backgrounds such as legal professionals, economists, forensic scientists IT specialists, political scientists, linguists, electrical engineers and the like. The educational requirement for most posts at the Agency is a university degree, while some posts require a relevant diploma of secondary education (administrative assistants, security guards etc.)

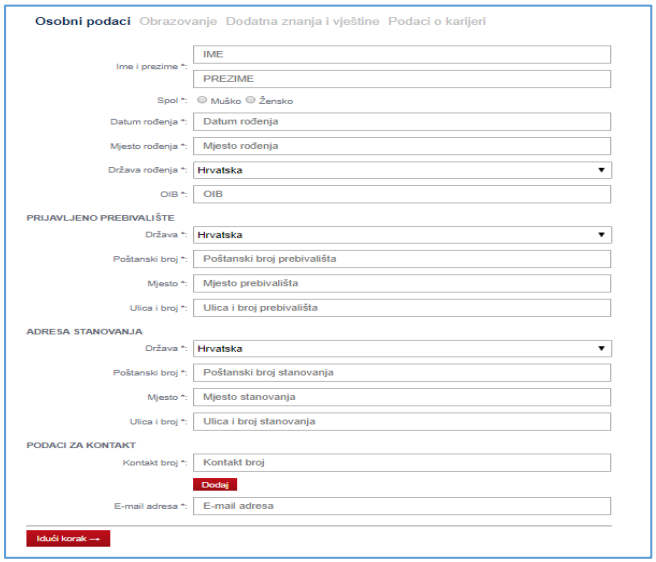
Over three-quarters of SOA's employees hold advanced and higher degrees. Women make up approximately 40% of the people force. The average age of the Agency's employees is between 40 and 50, with a third of our people force is under the age of 40.

SOA provides opportunities for professional development across a variety of fields and specializations. SOA provides its employees with opportunities for professional training and development. We are particularly focused on the transfer of knowledge and training for new hires who join us as trainees and who are expected to take on more responsible tasks in the future. As part of human resource development, the Agency invests in professional training and specialized courses.

In line with our needs, we employ competent and educated individuals with appropriate knowledge, skills and motivation for contemporary security and intelligence work. A thorough selection and recruitment procedure is carried out to best respond to the defined needs.

In accordance with the relevant legislation, an administrative competition is not required for employment at the Security and

Intelligence Agency. We invite all interested candidates to apply by submitting their applications using the web forms at www.soa.hr/hr/posao/.



Application forms available at www.soa.hr

All candidates must meet general requirements for employment in public administration and specific requirements of security and intelligence work such as particular level of medical and psychological abilities, particular level of expert knowledge and skills. Additionally, candidates are required to meet security standards, as established in the security vetting procedure.

All submitted applications are considered. In line with the Agency's current needs, candidates that meet the qualification requirements are invited to participate in the selection process. All candidates whose competencies, knowledge and skills meet the Agency's requirements 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. The selection procedure also includes polygraph testing. Those candidates whose assessment results best match the person specification for the relevant post will be selected.

SOA invites all potential candidates to submit an application for employment. While previous working experience is not necessary, it is not a disadvantage for employment at the Agency. All candidates whose qualifications and competencies correspond to the Agency's current needs will be considered in the recruitment and selection process.

The Agency mostly employs operatives in the regional canters across the Republic of Croatia. Analyst and IT specialist are usually based at the headquarters in Zagreb.

SOA is interested in experts of various specializations and profiles, and for this report we have selected three main types of posts. If you feel that you match the requirements of some of the following posts at SOA, we invite you to submit your application. If a career in these three segments does not appeal to you, you may consider applying for a post in some other segment, such as finance, accounting, linguistics and translations, HR management, psychology etc.

OPERATIVE (M/F)

University graduate (secondary education for some posts)

Dynamic and curious

Developed soft skills

Resourceful in unpredictable situations

Willing to take on field work

Strong independent performer and a team player

Detail oriented

Personally and professionally stable and resilient

Ready to take on challenges

Reliable and trustworthy

Keen to learn and develop

ANALYST (M/F)

University graduate in social sciences, humanities or technical sciences

Interested in social issues with a wide area of interests Systematic and analytical

Developed skills of objective reasoning

Competent in analysing and presenting complex subjects

Developed deducing skills

Open minded and competent in scenario planning

Highly developed written and oral communication skills with ability to express oneself clearly and concisely

Keen to learn and develop

IT SPECIALIST (M/F)

University graduate in technical sciences (information technology, mechanical engineering, electrical engineering, computer science etc.)

Keen to take on challenging projects Result oriented

Focused on practical application of technical and information systems

Keen team player

Reliable and trustworthy

Keen to learn and develop

Photos: SOA, screenshot (social media, news sitesi)
Images: Pixabay
Maps: SOA

Security and Intelligence Agency
Savska cesta 39/1
10000 Zagreb

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

www.soa.hr