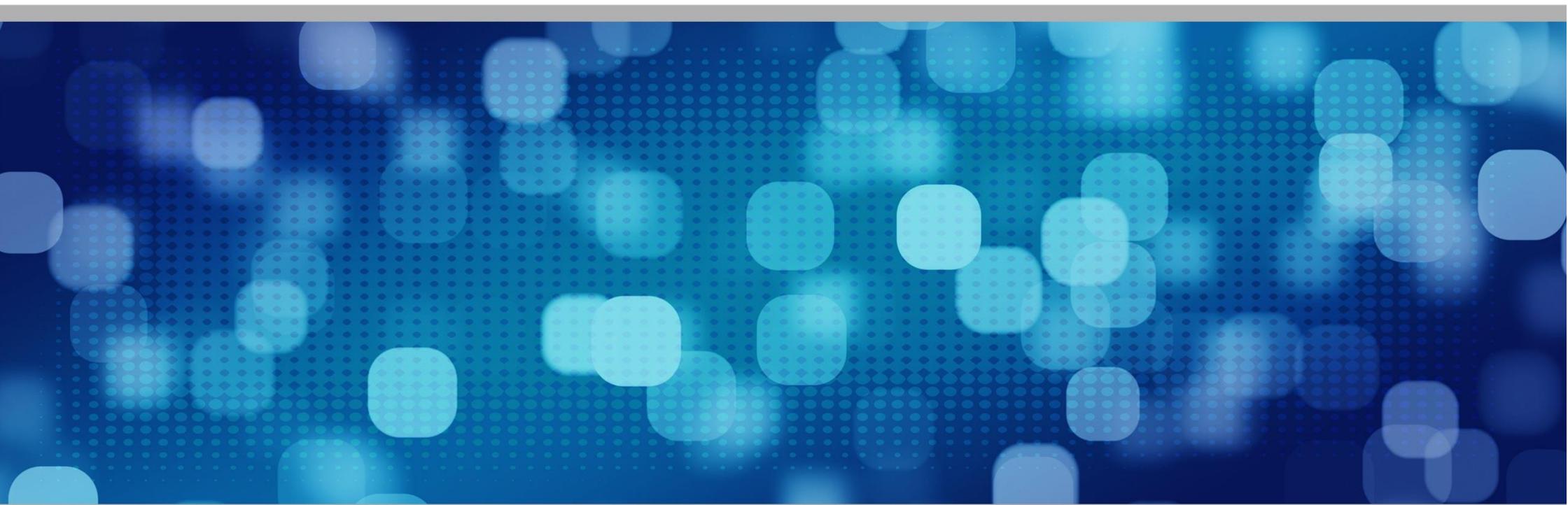




SECURITY-INTELLIGENCE AGENCY
2018







Our Mission

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

Our Vision

A modern, efficient and responsible security-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.....	1
SOA	3
The global and European security environments	7
The Republic of Croatia.....	12
The southeast neighborhood.....	16
International security and intelligence cooperation.....	21
Counter Terrorism Group (CTG)	24
APT attacks	26
An example of SOA operation:	27
<i>Big Data</i>	28
Internet trolling.....	30
Transparency and efficiency	32
A career in SOA	35



Introductory remarks

Dear Readers,

It is with distinct pleasure that I present the fifth public report on the work of the Security and Intelligence Agency (SOA). The objective of the public reports is to inform the public on the state of national security under the jurisdiction of SOA and our activities in the reporting period.

These public reports serve to reconcile two seemingly contradictory principles. On the one hand, for legal and security purposes, a significant part of our operations must remain confidential, while on the other hand, as a responsible state authority, we strive to inform citizens of the work we carry out in order to protect the security, values and interests of the Croatian society.

Croatian citizens invest financial and other resources into SOA and we give back by working responsibly and professionally in order to strengthen the security and the freedom of the Croatian society. We therefore consider it our duty to report Croatian citizens on our work. I believe that public reports reinforce citizen confidence into our ability to protect national security.

Furthermore, we maintain that the public is entitled to relevant information pertaining to challenges that we as a community face because that allows us to raise security awareness and build up the capabilities of the society in relation to security challenges.

Global security issues are becoming increasingly complex and the number of challenges and threats has been soaring with rapid and unanticipated changes. Reliable intelligence has become the pivotal prerequisite for optimal decision-making at national level. This very fact speaks to the importance that SOA has in the system of national and homeland security.

In order to best respond to the dynamics of security challenges, along with daily operative and analytical tasks, we have continuously invested in the development and modernization of our human and technical capabilities. We approach SOA development in a systematic manner taking a long-term view. We place great emphasis on responsible and prudent financial management and controlling.

Sustained efforts are taken in enhancing international partnerships and relations, most notably with NATO and the European Union. International security-intelligence cooperation multiplies our capabilities and allows us a better insight into transnational security threats and challenges. It gives me great pleasure to highlight the reputation that SOA enjoys with our international allies and partners, who have recognized us as a competent, trustworthy and reliable agency.

This public report will inform the public on the Counter Terrorism Group composed of intelligence agencies from 30 European countries, including SOA. The Counter Terrorism Group is one of the most prominent international platforms in which SOA takes



part so as to protect both the Croatian national security and the European security.

For five years SOA has been organizing the NATO Counter Terrorism Panel on combating terrorism which bring together experts from NATO member states and select partner states. This is another indicator of the Agency's contribution to national and international security and combating terrorism.

Public reports offer us an excellent opportunity to inform the wider public on the impacts of technological advancements on our operations and report on security trends in our field.

For the purpose of this report we have prepared an overview of our activities and a recap of the security status, along with several texts that offer a detailed insight into specific topics that affect security and intelligence. We look deeper into the impact that new technologies and Big data have on our operations, how the Internet and social media can be used for hybrid warfare and we address the transparency of security-intelligence agencies in developed democracies. As an agency, we have joined them by releasing these public reports. We hold that these texts will help to raise public awareness related to security phenomena, and therefore facilitate better understanding of our work and challenges we are facing.

This public report is particularly directed at young, competent and educated individuals considering a career in SOA. We have embarked on a generational renewal of the Agency and we are

searching for best candidates willing to take on work for the common good in the protection of all our citizens, in the upcoming decades. Candidates are guaranteed a demanding and objective recruitment process, with selection in line with the principle of excellence.

Even though our many successes will never be publicly disclosed, citizens' trust is a duty for SOA and it drives us further to give our best in the protection of national security on a daily basis. We bear this in mind as we press on with our responsible tasks, because our citizens and our homeland deserve no less.

Director

Daniel Markić



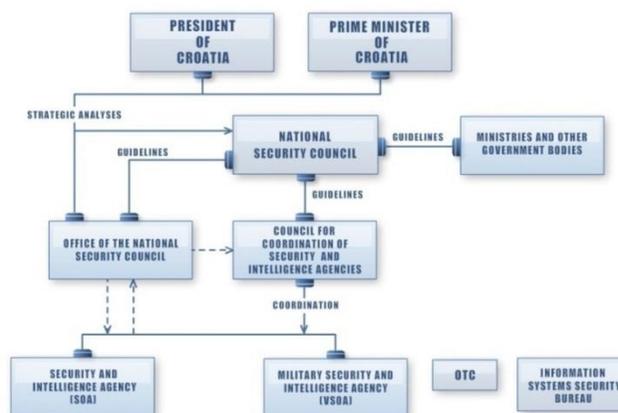


SOA

provides intelligence support to the state authorities and competent bodies in efficient and timely decision-making

SOA role in the national and homeland security system

The Security and Intelligence Agency (SOA) collects and analyses data that pertains to the national security and reports the findings to the state authorities. In this manner SOA provides intelligence support to the state authorities and competent bodies for efficient and timely decision-making. Using intelligence and analysis allows SOA to take informed decisions with regard to the protection of the national security, interests and nationals of the Republic of Croatia.



Security-intelligence system in the Republic of Croatia

The work of the security-intelligence agencies (SOA and VSOA) is directed by the National Security Council (VNS), while the Council for the Coordination of Security and Intelligence Agencies (Council) provides operative coordination. The Office of the

National Security Council (UVNS) and the Council provide both agencies with expert and administrative tasks.

Guidelines and reporting

SOA operational guidelines and objectives are set forth in strategic and implantation plans which are the basis for task planning, operational activities and reporting on findings to the end-users.



Strategic documents which govern SOA operations include the recent National Security Strategy as the umbrella security strategy as well as other strategic policy documents such as the National Strategy for the Prevention and Suppression of Terrorism and the National Cyber Security Strategy. The National

Security Council issues Annual Guidelines that regulate the operations of security-intelligence agencies.

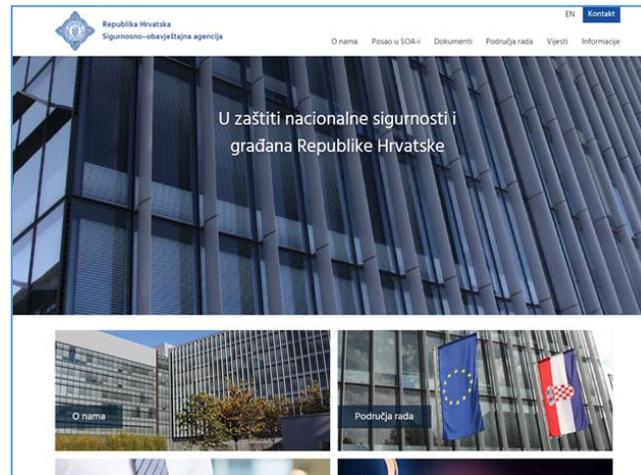
The annual guidelines for security-intelligence agencies for 2018 had been aligned with the guidelines laid down in the National Security Strategy, with particular emphasis on duties of the security-intelligence agencies as part of the Homeland Security System.

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-intelligence analysis and data.

Besides intelligence 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, strengthening of the information security and promoting security awareness and culture.

Organization and authorities

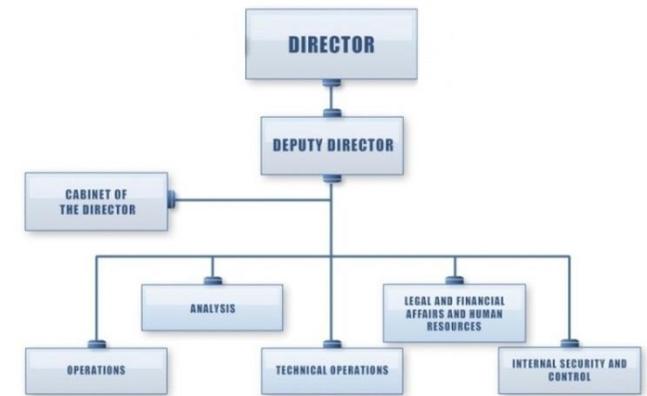
SOA operates from the headquarters in Zagreb, with 10 regional centers across Croatia.



SOA new website (www.soa.hr)

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 public sources and international exchange.

Any measures of covert intelligence collection that infringe the constitutional rights and freedoms of 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.

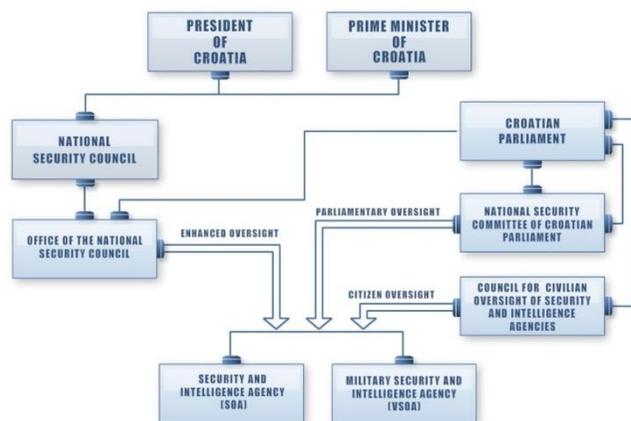


SOA HQ organizational chart

Oversight system

SOA is under three tiered external oversight: parliamentary oversight is carried out by the Croatian Parliament through the Domestic Policy and National Security Committee, expert oversight is carried out by the Office of the National Security Council, and civilian oversight that is carried out by the Council for the Civilian Oversight of the Security-Intelligence Activities.

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.



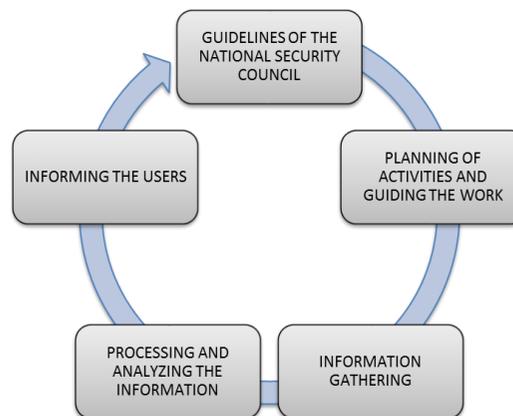
Organizational chart of the oversight system

Scope of work

Pursuant to the Security and Intelligence System Act, the National Security Strategy and Annual Guidelines for Security-Intelligence Agencies, SOA 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 intelligence 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. intelligence of particular importance to the national security of the Republic of Croatia.



SOA Intelligence cycle

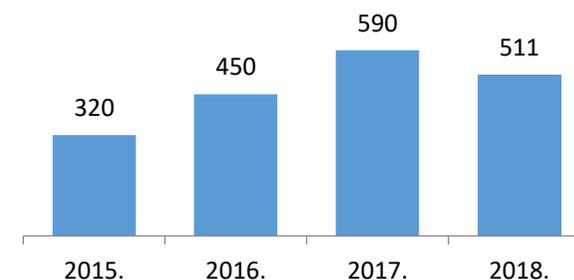
Areas of SOA security-intelligence operations:

- Terrorism and extremism,
- Foreign intelligence activities that pose threats or challenges to the values and interests of the Republic of Croatia,
- Processes in the security 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.

SOA in numbers

In 2018 SOA delivered 511 analytical reports to the state authorities (the President of the Republic of Croatia, the Prime Minister, the Speaker of the Croatian Parliament), containing security-intelligence analysis and data.

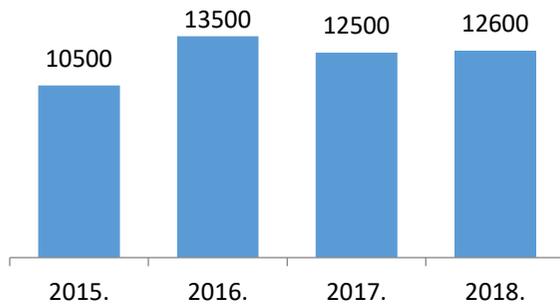


Indicative number of security-intelligence delivered to the state leadership, by years



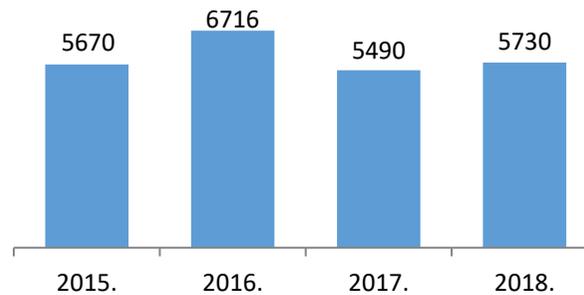
The substantial volume of analytical work is an indicator of efforts in intelligence collection, but it also reflects the complexity of the security situation.

As an integral part of the national security system, SOA 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, Ministry of Defense, Ministry of Economy etc.). In 2018 SOA delivered approximately 12,600 various pieces of security intelligence to other state authorities.



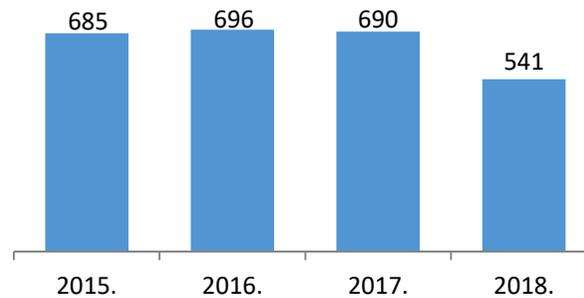
Indicative number of security-intelligence delivered to end users, by years

In 2018 SOA performed 5730 security vetting procedures in the context of preventive operations and enhancing information security (including basic security screenings and those with the purpose of granting access to classified data). Additionally, SOA carries out security screenings of legal entities.



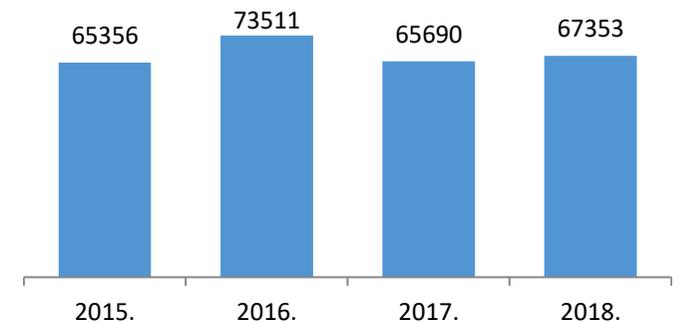
Number of security vetting procedures, by years

Throughout 2018, 541 security assessments were delivered, related to the movement and residence of protected facilities. Approximately 24,000 security screenings were performed in connection with individuals with direct access to protected individuals, facilities and premises.



Number of security assessments, by years

Security issues pertaining to foreign nationals and citizenship procedures have been increasingly using up SOA capabilities, most significantly in relation to asylum seekers. 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



The global and European security environments

have been characterized by geopolitical rivalry and rapidly changing circumstances

Global security trends

The global security environment is characterized by numerous dynamic challenges in the light of rapid unpredictable changes. Globalization and interdependence of the global economy arising from the development of new technologies and communication channels have accelerated all societal processes. Internet's role as a catalyst in the formation and support of societal and security processes worldwide has been gaining prominence.



Global security conditions have been developing against the backdrop of geopolitical and economic rivalries between the great powers coupled with inter-state tensions and conflicts as well as lengthy intra-state conflicts which in return replicate those geopolitical rivalries. 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. Multilateralism has continued to decline with non-Western actors strengthening their presence in international

relations. The United States have consistently pursued a foreign policy based on a new concept of economic and security interests, while reviewing their trade relations with China. The US have insisted on further investments in NATO's deterrence capabilities. Russia has set out to enhance its military, energy and economic global presence, while China has pursued global economic ambitions. Apart from state actors, emerging non-state actors have been adding to the complexity of the global security outlook and have been affecting global processes.

Geopolitical and economic rivalries can to a large extent be attributed to a global shift and redistribution in the global power arena. They shape regional and local security processes, including the European and Croatian security as well as the security situation in Croatian neighborhood.

In the framework of geopolitical rivalries, security interests of states have been underscored by their needs for expansion or containment of spheres of influence and values. Protection of economic interests, securing access to valuable resources such as water, food, energy, communications, and most importantly new technologies and industries, have also informed security interests.

Global security is affected by a variety of other factors such as climate change, sharp population growth in underdeveloped countries, population decline in developed countries, uneven access to resources and poverty.

All of those factors consequently lead to intra-state and regional conflicts, mass migration, terrorism, social unrest, institutional collapse in declining states, outbreaks of communicable diseases and other security challenges.

Contemporary international conflicts increasingly involve the use of unarmed tactics employing soft war in inter-state conflicts characterized by low intensity of military operations with use of a wide spectrum of means such as diplomatic, information, media and other hybrid warfare activities. Therefore, a significant part of inter-state conflicts has moved into the information and cyber sphere.

At the same time, ICT development has allowed unprecedented opportunities - connecting the world with new technologies is creating emergent industries and opportunities for global development. While there are positive aspects to these processes, they simultaneously breed new security risks and challenges. This is particularly striking in the development of 5G technologies, AI and the Internet of things.

Societies and individuals have become dependent on ICT which has rendered them vulnerable to cyber attacks and cybercrime. Cyber attacks and cyber manipulations have become a part of daily experience. There are numerous possibilities for attackers to remain anonymous and even to carry out secret attacks. Geographical and organizational dispersion facilitated by unlimited communication possibilities allows the evidence to be easily concealed.

A particularly sensitive area of cyber security is related to the theft of classified, personal and other sensitive data. The capability of cyber attackers to cause casualties and substantial material damage in the physical world has been on the rise. Equally, the likelihood of interfering with social and democratic processes through dissemination of misinformation and fake news has been growing.



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 attack planning.

European security, EU and NATO

Croatian wider security environment is dynamic and challenging. The European Union (EU), as a broader framework within which the Republic of Croatia acts, has been facing a series of internal and external security challenges. In particular, they pertain to the

emergence of radicalism and terrorism in European societies, discussions on the Common European Asylum System and strengthening external borders, issues of energy security, dissemination of misleading and fake news, cyber attacks and cybercrime.

Simultaneously, the EU has been experiencing an internal reshuffle, in the context of Brexit combined with a growth of anti-systemic and Eurosceptic parties and movements.

The EU has borne consequences of global geopolitical tensions across a variety of societal and security issues, most notably in terms of deteriorating relations between the West and Russia, which have been reminiscent of the Cold War era. A number of issues remains open; transatlantic partnership, relations with Russia, China and Iran as well as the issue of stabilization of crisis hot spots in the wider European environment e.g. Syria and Libya. Reducing migration pressures in the south and south-east Europe remains a substantial challenge before the EU.

The EU is aiming to build up its energy security, and one of the most important factors of that security is the reliability of natural gas supply. Roughly 40% of the total natural gas consumption in the EU is supplied from Russia, with the EU being the largest market for Russian gas. Certain Eastern EU member state rely entirely on Russian gas. The EU is looking to advance the diversification of sources and supply routes. In this respect, LNG terminals serve as one possible option of diversification. The EU



therefore considers LNG projects in the Baltics and SE Europe as those of common interests.



North European gas pipeline - plan and realization

SE Europe gas supply diversification includes the Republic of Croatia through the LNG terminal project on Krk, which has a significant strategic potential for strengthening European energy independence and security.

In the fallout of the Ukrainian crisis and conflict along with the Crimean annexation, NATO has increased efforts in enhancing deterrence and defense capabilities. NATO has enhanced its forward presence in the eastern part of the Alliance since 2017,

with active participation of the Republic of Croatia. NATO has been working on combating terrorism, dealing with cyber attacks and hybrid threats. Member states have launched a discussion on the issue of the cost-sharing formula and increasing budgetary provisions for defense. At the same time, the EU has been striving to strengthen its security and defense dimension while enhancing the cooperation with NATO.



Russian-Western relations have been marred by a variety of issues such as the Russian annexation of Crimea, indications of Russian interference in democratic processes in the West, election interference, dissemination of fake news and cyber attacks.

Following President Putin's re-election, Russia has maintained the continuity of the existing foreign and domestic policies; attempting to contain NATO and EU expansions, curbing their influence in East and SE Europe while exerting greater influence on the continent. Russia has continuously engaged in the policy

of reinforcing relations with members of the Commonwealth of Independent States, which it has regarded a sphere of influence and has maintained presence in crisis hot spots such as Syria.

The EU has imposed sanctions on Russia since 2014 in response to Russian intervention in the crisis in Ukraine and the annexation of Crimea. EU and NATO relations with Russia have further deteriorated following the Sergej Skripal poisoning case in the UK. The Republic of Croatia has participated in the coordinated response of the majority NATO and EU member states by expelling one Russian diplomat from the Russian Embassy in Zagreb. In the concentrated blow of 29 states and NATO allies, a total of 153 Russian diplomats have been expelled.



Alexander Petrov

Ruslan Boshirov

The British police release photographs of two Russian nationals named as suspects in the attempted murder of Sergej Skripal

Instability belt around Europe

A belt of instability that encircles Europe from the south and penetrates the continent from the east continues to generate the most significant challenge to European security. The belt extends throughout North Africa, across the Middle East, the Caucasus and Central Asia to Ukraine. This area has been characterized by numerous armed conflicts and tensions, terrorist groups, crisis hot spots and frozen conflicts, as well as widespread poverty and rise of radicalism and extremism.



As such, the belt has been a long-term source of various security challenges and threats to the continent such as terrorism, illegal migrations, proliferation of WMD, organized crime, extremism, crisis hot spots and armed conflicts.

Major events in the civil war in Syria in 2018 included the collapse of the so-called Islamic State (ISIS), expansion of the Damascus-government controlled territory in the southwest, Kurdish forces advances in the northeast and Turkish military intervention in the northwest. Since the outbreak, the conflict in Syria has drawn in multiple global and regional powers such as Iran, both politically and military.

Active crisis hot-spots have remained in Yemen, Libya, Afghanistan and Iraq, together with permanent incidents arising from the long-standing Israeli-Palestinian conflict.

The security situation in East Ukraine has remained unstable. Despite diplomatic efforts, there has been little significant progress in the implementation of the Minsk Agreement.

Terrorism threat to Europe

Terrorism is still the most prominent and the most visible threat to the international security and the security of European citizens.

Terrorists continue to demonstrate readiness and capabilities necessary to carry out the most brutal forms of attacks on soft targets with high potential for casualties. These mostly include unprotected public facilities with a large density of people such as promenades, shopping malls, promenades. Terrorists are prompted to use improvised means in attacks, such as knives, motor or heavy vehicles. In doing so, terrorist cells are proficient users of contemporary communication technologies, specifically

the Internet and social media, as a means of planning attacks, dissemination of terrorist ideology, recruitment and supporter training. It is expected that this mode of operation will continue in the future and that new ways of technology misuse for the purpose of terrorist activities and organization of terrorist attacks will be consistently explored.

ISIS and Al-Qaeda remain the two most significant terrorist threats on the global level. On the back of defeats in Syria and Iraq, ISIS has been seeking a way to survive and has used new terrorist attacks as a way of demonstrating its operational capabilities.

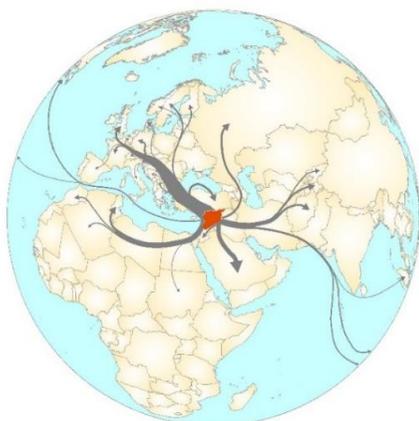
Although ISIS has recently proven to be more successful in recruitment of new supporters and in organization of terrorist attacks, Al-Qaeda remains a severe threat to the European and the global security.

In 2018 nine terrorist attacks were registered (four in France, two in Great Britain, and one in Belgium, the Netherlands and Spain), carried out by individual attackers on randomly selected targets using widely accessible weapons. In Europe, 33 terrorist attacks were carried out in 2017. The highest death toll was recorded in Great Britain (35), followed by Spain (16), Sweden (5) and France (3).

The decrease in the number of terrorist attacks is a result of more efficient efforts of European security-intelligence systems and the fall of ISIS in Syria and Iraq, which significantly diminished ISIS



attack planning and execution capabilities. In 2017 1,219 individuals across 18 EU member states were apprehended on terrorism charges.



Repatriation flows of ISIS Jihadists

While the risk of terrorism remains high in Western Europe and medium in Croatian south-east neighborhood, in the Republic of Croatia it has remained low. In addition to returning ISIS Jihadists, currently the most prominent threats to European states arise from domestic Islamist terrorist cells and individuals.

In the aftermath of ISIS defeat and loss of territory, thousands of foreign fighters and their families have been seeking to either relocate to other crisis hot spots or to return to their home countries.

Nearly 5000 individuals from Europe have participated in conflicts in Syria/Iraq, fighting for Islamic terrorist groups. Roughly 1000 individuals from Croatian southeast neighborhood had left for Syria and Iraq. Of the total number of foreign fighters, one third has already repatriated, while a quarter have lost their lives. Their repatriation poses a significant security risk for European societies and highlights the need for de-radicalization programs.

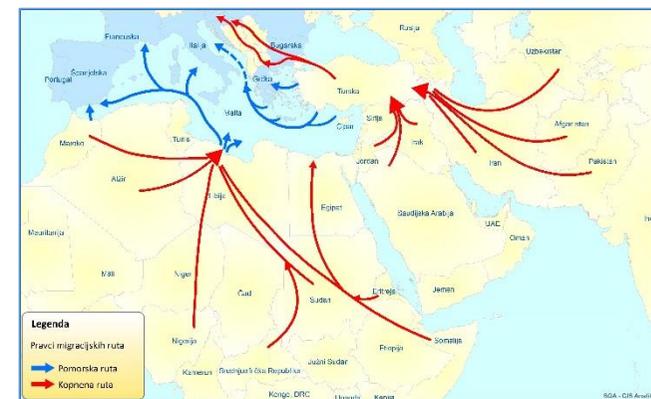
This is especially pertinent for children of returning fighters who had been exposed to terrorist indoctrination and military training in areas under ISIS control, and had in certain cases, participated in war crimes. Another distinct challenge comes from prison radicalization, where offenders who had been convicted of terrorist crimes in their home countries engage in grooming and radicalization of other convicts.



ISIS used children to carry out liquidations of prisoners

Illegal migrations towards Europe

The trend of migration from Middle East and Africa towards Europe has continued on all Mediterranean routes, although the volume has decreased. In 2018 the total migration flow intensity towards the EU decreased by about 25% year-on-year, primarily due to a reduction in the number of migrants on the central Mediterranean route leading from Libya to Italy. This decrease stems from tightened Italian measures and agreements with Libya. However, at the same time, the intensity of migration flows in the West Mediterranean route towards Spain has doubled, while the migration flows towards the so-called Balkan route have grown by a third, as most migrants attempt to cross the Croatian territory in order to illegally make their way to Western Europe. The Balkan route has become exceedingly attractive for organized crime groups engaged in migrant trafficking.

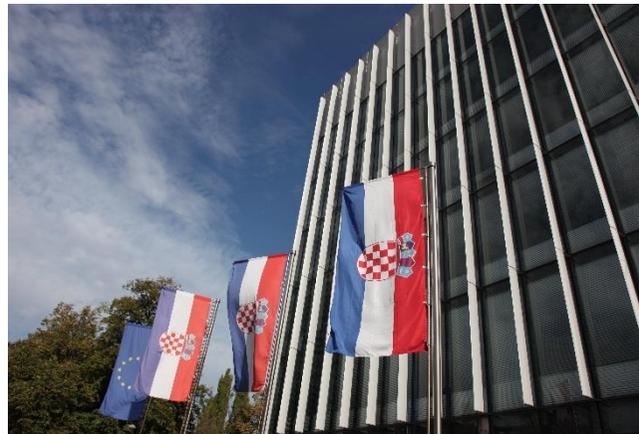


Overland and maritime routes of illegal migrations towards Europe

The Republic of Croatia

is a safe and stable democracy

The security situation in Croatia is stable and there are currently no indications or visible possibilities of wider destabilization.



SOA HQ in Zagreb

Terrorism threats

In the territory of the Republic of Croatia, the terrorism threat level is low. However, given the nature of modern terrorism threats, the Croatian membership in the Euro-Atlantic associations and the Western democratic value system, the developed tourism sector and the visibility of the Republic of Croatia in the global media, there is a potential risk of terrorist threats in the Republic of Croatia as well. Furthermore, there is a constant risk of the so-called lone wolves, who could carry out a terrorist act independently, triggered by publicly announced calls by terrorist groups to carry out attacks. These individuals do

not have to be directly associated with terrorist organizations, and they can become self-radicalized online or using social media, which makes them difficult to detect. Moreover, many independent terrorist attacks were carried out by people with mental disorders.

Seven individuals who (also) hold Croatian citizenship have been located on the ISIS-controlled territory, two men and five women. None of them were radicalized in the Republic of Croatia, nor have they joined ISIS from the Republic of Croatia. According to uncorroborated data available, two men have been killed while fighting for ISIS, while certain women have gone to civilian camps controlled by the Kurdish-Arab SDF-forces in Syria. Generally speaking, the women had joined ISIS to accompany their jihadist husbands, and some have given birth to children during their stay in Syria and Iraq. Their exact location and fate are yet to be confirmed due to the chaotic situation after the fall of ISIS.

Extremism

No type of extremism, regardless of its ideological, religious or national grounds, has gained wider public support, a significant number of followers, or a significant disruptive potential in the Republic of Croatia. Extremist group members have very little potential to cause violence, incidents or conflicts on a larger scale, and their activities do not constitute a significant threat to the national security. Consequently, the threat of extremism and undermining of the democratic constitutional order and the



extremism-related violence is currently low in the Republic of Croatia.

The extremist-minded individuals and groups will try to connect with ideologically close groups/movements abroad. In the Republic of Croatia, there has not been significant anti-immigrant extremism, although the trend of anti-immigrant movement is on the rise in Europe which, in the medium term, could lead to the strengthening of similar groups in the Republic of Croatia.

Although Islamist radicalism in the western countries of the EU and the countries neighboring Croatia in the southeast had gained a significant number of supporters, it failed to attract a greater number of followers in the Republic of Croatia. This refers to a several dozen individuals of the Salafi movement who do not advocate violence. Some of the main reasons for the lack of significant Islamist radicalism in the Republic of Croatia are the good position, reputation and integration afforded to the Islamic communities in the Croatian society.

Economic security

In the reporting period SOA gave special attention to supporting competent state authorities in the field of protection of the fundamentals of the economic system of the Republic of Croatia, as was the Agrokor case. Based on its competence in the protection of the fundamentals of the economic system of the Republic of Croatia and the suppression of economic crime, with

Agrokor defined by law as a company of systemic importance for the Republic of Croatia, SOA reported on the circumstances and potential consequences of the Agrokor case in terms of national security and economic interests of the Republic of Croatia. With its work SOA has supported other competent state authorities in the protection of economic interests and the legal system of the Republic of Croatia. Pursuant to relevant legal provisions, in such complex cases SOA reports state authorities, ministers and other state officials, and submits intelligence related to their scope of work.

In addition, at the request of the Domestic Policy and National Security Committee of the Croatian Parliament SOA has delivered a status report on the situation in Agrokor and its possible impact on the national security. The Committee has discussed the report at the session attended by SOA Director.

Energy security

The European Energy Security Strategy for improving the security of SE Europe gas supply includes the Republic of Croatia through the LNG terminal project on Krk, which has a significant strategic potential for strengthening European energy security.

The European Commission has published a comprehensive LNG strategy, which allows all EU Member States access to LNG in the event of an energy crisis. The strategy has also intensified the development of the LNG terminal project on Krk island, which

carries a significant regional potential because it is an alternative gas supply option for the neighboring countries.

Liquefied natural gas (LNG) accounted for about 14% of gas imported in the EU in 2017. In line with the estimates that natural gas consumption in the EU will grow in the future, LNG terminals are becoming an important factor in enhancing security and diversification of supply, as well as regulation of the natural gas market. LNG is an energy source of the global market, therefore the sole supplier dependence is avoided. LNG terminals are particularly important for energy security in the event of a supply crisis because they offer additional options for overcoming such events.

In the EU, there are 24 large LNG terminals. All are import terminals, while Norway and Russia also have export LNG terminals. Currently, Europe is deliberating or planning to build another 22 large LNG import terminals, 9 of which should be floating terminals, including the terminal on Krk.

The development of an LNG terminal on Krk would represent the realization of the Three Seas Initiative as well as the integration of the energy systems of the Baltic, Adriatic and Black Sea regions, and the inclusion of their potential in strengthening the energy security of the EU.

The Ionian Adriatic Pipeline (IAP) which should connect to the Southern Gas Corridor (JPK) in Albania, and via Montenegro and

Bosnia and Herzegovina connect to the pipeline network of the Republic of Croatia also carries potential for diversification of gas supply.



Constructed and planned pipelines and LNG terminals in southeast Europe

Corruption, economic and organized crime

Corrupt business practices and non-transparent investments cause significant damage to the economy. Institutional misuse and corruption can negatively affect the free market, competitiveness, the country investment attractiveness, and the overall economic development and international reputation of the country. These particularly complex forms of corruption, misuse and misconduct in business, cash extraction and money laundering also have an international dimension.

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

Regional criminal groups tend to use the territory of the Republic of Croatia to carry out their illicit activities, such as trafficking - drugs, illegal migrants, arms and high-profit goods. They cooperate with individuals and groups from the Republic of Croatia and hire them to carry out specific criminal activities. These groups seek to exploit the territory of the Republic of Croatia as a hiding ground from competing and rival criminal groups and to avoid criminal prosecution in their home countries. Members of organized crime groups seek to corruptly act against individuals in state institutions in order to entice them to engage in malpractices and favor organized crime.

In recent years, numerous conflicts between rival criminal groups have occurred in countries neighboring Croatia and there has been a constant risk that a portion of these conflicts could spill over to the Croatian territory.

Foreign intelligence activities

Some countries engage in intelligence activities and intelligence collection in the Republic of Croatia. 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 Southeast Europe, which is still in the process of accession to European and Euro-Atlantic integrations. Therefore, the Republic of Croatia is primarily a subject of intelligence interest of countries which perceive NATO and the EU as a security challenge or a threat, and which intend to exert influence in Southeast Europe that is not aligned with the Euro-Atlantic perspective of the region.

The main points of interests for foreign intelligence in the Republic of Croatia include, among other things, processes taking place within NATO and the EU, Croatian positions related to NATO, EU and Euro-Atlantic integration, Croatian policies towards the SE neighborhood, energy security and issues pertaining to Croatian economy.

Information operations against the Republic of Croatia

Fragmented data, fake or distorted news disseminated to impose an opinion about an event and/or change public awareness and attitudes, portraying the Republic of Croatia, the EU and NATO in a bad light, are occasionally published in the public and media. The goal of such media releases is to affect the stability of the Croatian state institutions and the regional environment, to falsely present the Republic of Croatia as an unsound member of NATO and the EU, and to weaken the Euro-Atlantic and European unity.



TERORIZAM 892

EKSKLUZIVNA ISPOVIJEST BIVŠEG SARADNIKA SOA (VIDEO): Tražili su od mene da prebacim oružje iz Doboja u mesdžid Stranjane

Objavljeno: 19.03.2019. u 11:19h

Pripadnik selefijskog pokreta H.Č. iz Zenice skoro četiri mjeseca saradivao sa hrvatskim obavještajcima. Prilikom vrbovanja prijetili mu zabranom ulaska u Hrvatsku. Za dobro izvedenu akciju prebacivanja naoružanja, obećavali mu posao u Hrvatskoj za njega i njegovu porodicu. SOA preko hrvatskog tjednika Nacional priznala kontakte sa ovim svjedokom.

LEGLIO TERORIZMA 2261

KONZUL IVAN BANDIĆ KOORDINIRAO AKCIJOM: Hrvatski obavještajci vrbovali selefije da prenose oružje u mesdžide u BiH

Objavljeno: 13.03.2019. u 17:32h

Kako bi se potvrdili navodi Kolinde Grabar Kitarović da je BiH „leglo terorizma“, hrvatski obavještajci organizirali slanje oružja u mesdžide. U akciju bio uključen i zamjenik ministra sigurnosti BiH Mijo Kresić, te novinar RTRS-a Mato Đaković

An example of false media releases in the neighboring countries where SOA was accused of forcing Salafis to transport weapons to Bosnia and Herzegovina. In July 2018, the same medium published fake news that Nikolai Patrushev, Secretary of the Security Council of Russia, visited Croatia.

Moreover, for certain topics, media releases include notions that seek to undermine the international reputation of the Republic of

Croatia and expand the narrative about illegal and illegitimate activities of the Croatian institutions, both today and during the formation and liberation of the Croatian state during the Homeland War.

Cyber security

The Republic of Croatia, especially since joining NATO and the EU, has become a target of progressive and constant cyber attacks. This refers to very specific and well-planned campaigns primarily aimed at confidential data theft. It is expected that this kind of threats will continue, and it is very likely that attacks will become more sophisticated. The chapter on APT attacks includes more details about advanced cyber threats which the Republic of Croatia has been facing.

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.

SOA has been focused on establishing the place of residence of individuals suspected of war crimes and the location of individual and mass graves of people missing in the Homeland War. In the process, close cooperation with citizens who can disclose information on the missing persons and possible burial sites plays

a crucial role. SOA guarantees anonymity and discretion to such persons.

Demographic trends

The Croatian population is characterized by an extremely negative demographic structure and trends of demographic processes, aging population and disruption in the age distribution. In the long term, protraction of these demographic trends will inevitably affect the overall social and economic development of the Republic of Croatia.





The southeast neighborhood

is still characterized by instability and difficulties in the process of Euro-Atlantic integrations

Security trends in the Croatian surroundings

The southeast neighborhood of the Republic of Croatia is still unstable and not fully consolidated in terms of security and politics. The complexity of the current security and political situation in the southeast neighborhood is confirmed by the fact that some countries still function with active involvement of the international community and it is unlikely that this situation will change soon.

The impact of the legacy arising from the breakup of the former Yugoslavia and the wars of the 1990s is still evident, as well as the impact of many years of inter-ethnic tensions. Additionally, political clientelism, high levels of corruption and organized crime, weaknesses in the rule of law, poor economic outlook, intensified activities of external actors, especially countries that oppose the expansion of the Euro-Atlantic integrations in this area, and radical Islamist and nationalist forces, as well as difficulties in the Euro-Atlantic integrations all have a significant impact.

Challenges in relation to the stabilization of the southeast neighborhood and integration into Euro-Atlantic associations

Countries that perceive EU and NATO as political and security challenge are exceptionally active in Croatia's SE neighborhood, which still remains excluded from Euro-Atlantic associations, in order to decelerate or disable further spread of NATO and the EU. They also use intelligence activities, including efforts to

directly influence political processes in the neighboring countries and political destabilization attempts. The most obvious example is the prevented coup d'état in Montenegro that was attempted during parliamentary elections in October 2016, with the purpose of destabilizing the country just before its accession to NATO. In Montenegro, 14 Russian, Serbian and Montenegrin nationals have received long-term prison sentences for the attempted coup d'état.

The Prespa agreement on the name change was successfully ratified and the Republic of Northern Macedonia signed a protocol on the accession to NATO in February 2019, which is seen as the continuation of the Euro-Atlantic perspective of the Croatian southeast neighborhood and the expansion of the Euro-Atlantic zone of stability and security in this part of Europe.

In the regional context, stabilization process are taking place. A particularly important process is the Belgrade - Priština negotiations on the future state relations between Serbia and Kosovo, which are EU mediated.

Stability remains fragile and the effects of the progress achieved in the southeast Europe could be cancelled out. The presence, involvement and overall engagement of the international community in the political, economic and security plan are essential for maintaining stability.

In some neighboring countries, there have been efforts to portray the Republic of Croatia in a negative light, mostly by publishing fake news in the media and on social networks. These efforts are particularly expressed in the media circles which oppose the



Euro-Atlantic integrations and portray NATO and the EU negatively. In this regard, in October 2017, for the purposes of the Domestic Policy and National Security Committee of the Croatian Parliament, SOA delivered a report on information operations that are weakening the international position of the Republic of Croatia.

The position of Croats in the SE neighborhood

In accordance with the National Security Strategy, one of the four fundamental national interests of the Republic of Croatia is the concern about equal position, sovereignty and survival of Croats in Bosnia and Herzegovina and the position of the Croatian national minority in other countries.

The position of Croats in Bosnia and Herzegovina has been marked by efforts to achieve a gradually diminished political equality with the other two constituent peoples in accordance with the existing constitutional system of Bosnia and Herzegovina and the Dayton Accord.

In the international context, the fact remains that the Croats and their elected representatives in Bosnia and Herzegovina have been portrayed in some political circles and the media as opponents of the European and Euro-Atlantic integrations and values, which is an instrument of weakening the credibility of the Croatian claims in Bosnia and Herzegovina for achieving constitutional equality in the political circles of NATO and the EU.

The trend of economic migration of Croats from Bosnia and Herzegovina has continued, which together with the aftermath of the war expulsion, threatens the survival of Croats living there and the multi-ethnic character of Bosnia and Herzegovina.

With regard to the Croatian national minority in Serbia, last year talks with representatives of the Serbian authorities commenced, in the context of negotiations on Serbia's membership in the EU, which should begin to resolve problems and reach European minority standards for the Croatian community in Serbia.

Terrorism

Countries in the southeast neighborhood still suffer from issues of Islamist radicalization in parts of their societies and Islam related terrorism.

Throughout June and July 2017, ISIS members from countries in the southeast neighborhood reiterated earlier threats to peoples and countries of Southeast Europe, including Croats and the Republic of Croatia through the ISIS magazine Rumiayah.

Since 2015, there have not been terrorist attacks in Southeast Europe, but a few have been successfully prevented in police and security operations. For example, in April 2018, two Salafis were arrested in Bosnia and Herzegovina in connection with planning terrorist attack. In June 2018, radical Islamists from Kosovo were arrested in Belgium for planning attacks. Moreover, in May 2018, a court in Kosovo sentenced nine persons to prison for planning

terrorist attacks in Albania during the Albania vs Israel soccer match in November 2016.



An excerpt from the Bosnian issues of the ISIS magazine on the occasion of the terrorist attack in Barcelona celebrating 146 killed and wounded

About 1,000 people, supporters of jihadist Salafi movement, most of whom joined ISIS, have left the area of SE Europe for the war-

torn Syria and Iraq. A significant portion of them have also participated in armed combat. About a third of the fighters have repatriated, while a fourth of them has been killed in combat. Due to the chaotic situation in Syria and Iraq, as well as military defeat of ISIS and the loss of territory, it is difficult to collect the data on their locations and fates.

A significant number of returnees from ISIS represents a security risk, especially for countries that receive great numbers of repatriates. These are individuals who had participated in combat on the side of a terrorist organization. They are military-trained and have been further radicalized on the battlefield.

Countries of the southeast neighborhood have prosecuted repatriates from terrorist organizations. However, due to short prison sentences given (usually 1-3 years), some of the convicts are already at large, while many are expected to serve their sentences shortly.

Another security challenge for the Republic of Croatia is transit of foreign nationals across the Croatian territory, for whom there are indications of supporting terrorist activities. This is highlighted in the context of migration flows across the Croatian territory. To reduce the risk of this challenge, SOA has taken appropriate preventive actions in order to protect the Republic of Croatia and other European countries.



Jihadists Alija Keserović and Amir Selimović from Bosnia and Herzegovina on ISIS recordings from 2016 threatening with terrorist attacks (left) and recorded after the surrender to the Kurdish forces in March 2019 (right)



Extremism

The societies of countries in the southeast neighborhood are still burdened with religious and national extremism.

Great Serbia-related extremism has been continuously present in the neighboring countries, as well as the denial of territorial integrity and sovereignty of the Republic of Croatia, such as extremist messages at public and sporting events, public gatherings of Great Serbia extremists, and destruction of Croatian national symbols.



The meeting of the Serbian Radical Party of Vojislav Šešelj held in Hrtkovci, Serbia in May 2019. Vojislav Šešelj was convicted of persecution and deportation of Croats from Hrtkovci in 1992 by the Hague Tribunal. At the meeting, a map of "Great Serbia" was hung, covering a significant portion of the Croatian territory and other neighboring countries.

Countries in the southeast neighborhood are burdened by the expansion of radical interpretations of Islam that do not recognize the viewpoint of the official Islamic communities, the law, or the democratic government of the host country.

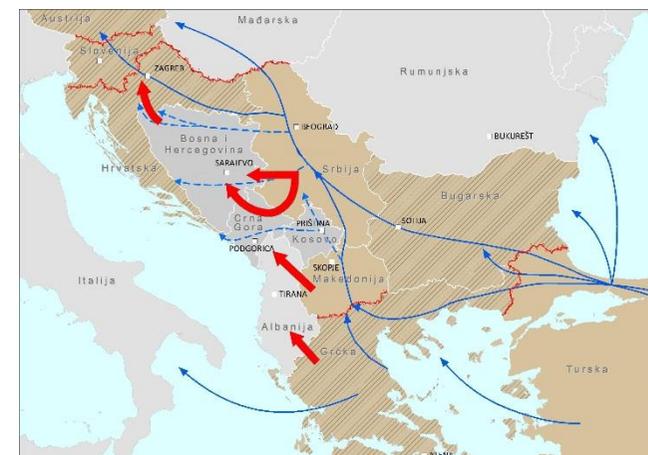
The existence of radical Islamist enclaves in neighboring countries, and especially the repatriation of jihadists from Syria to their home countries in the SE neighborhood, could lead to a higher degree of radicalization and the spread of radical interpretations of Islam, in addition to the related security risk.

The so-called Balkan route of illegal migration

In 2018, the overall number of illegal migration to Europe decreased, but migration along the so-called Balkan route increased by approximately one third. In addition to the insufficient capacity of countries and branched out trafficking networks, 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 southeast neighborhood and the migrant home countries.

Trafficking routes have diversified with the intensification of migration. Due to enhanced border controls on the usual routes, alternative routes have opened that go further south than the usual ones. In 2018 migrants increasingly used the route through Albania and Montenegro to Bosnia and Herzegovina, and then further to the Republic of Croatia.

Therefore, in 2018 the pressure of illegal border crossings from the western part of Bosnia and Herzegovina to the Republic of Croatia significantly increased, with the involvement of organized criminal groups in human trafficking.



Directions of illegal migration along the so-called Balkan route

The Republic of Croatia is still a transit country for migrants on their route to reach the desired destinations within the Schengen area.

Transnational organized crime

In the southeast neighborhood, conflicts between members of organized crime groups have been frequent. In recent years,

dozens of members of organized crime have been killed in the conflicts.

Despite the efforts of countries in the southeast neighborhood, organized crime remains strong and well-organized with numerous international connections.



trafficking as a result of the migrant pressure on the Balkan route.

In recent years, organized crime groups from the southeast neighborhood have gradually taken an increasingly important role in drug trafficking (e.g. cocaine from South America) in the EU, and have been increasingly active in arms and people trafficking. For example, 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 2018, several attempts of arms trafficking to Western Europe over the territory of the Republic of Croatia were prevented, and criminal groups have been increasingly active in people



International security and intelligence cooperation

enables better protection of national security and a more powerful development of SOA capabilities

Security and intelligence work is directed to international cooperation. Modern security threats and challenges are characterized by complexity and transnationality, thus a close international cooperation between security and intelligence agencies is required for their prevention and countering.

SOA international cooperation is approved by the National Security Council. SOA has developed a network of partnerships with various agencies worldwide that allows exchange of intelligence in the interest of the security of the Republic of Croatia, as well as capability building in cooperation with partners.

Bilateral security and intelligence cooperation takes place at various levels with respect to common interests and mutual security challenges. At the multilateral level, SOA is a member of all relevant European security and intelligence platforms, and is particularly active in those that operate in the context of the EU and NATO. SOA has liaison officers in some countries, and a certain number of employees work in the bodies of NATO and the EU. Certain foreign security and intelligence agencies have also set up their liaison officers in Zagreb.

In recent years, international meetings and activities at all levels have been increasing, with a large increase in the number of exchanged intelligence in international cooperation.

Since May 2018, SOA has been partnering up with the Polish Security Agency ABW as part of the EU project to raise capabilities in the area of national security. ABW and SOA have

partnered on the project "Raising capabilities of national security services, public administration staff and research and development centers and developing their cooperation in the domain of national security".

The project is co-financed from the European Social Fund, and it is aimed at empowering public administration for a more effective identification and countering of terrorism and asymmetric threats based on the transnational experience. ABW has chosen to partner up with SOA because of the Agency's previous activities, the ability to contribute to the objectives of the partnership, and experience in similar international projects.

The partnership agreement for the project was signed by the SOA and ABW directors at the opening ceremony of the ABW Terrorism Prevention Centre of Excellence. The project will develop a new model of response to terrorist and asymmetric threats by raising standards; ensure the exchange of intelligence and experiences in the context of national and international cooperation; conduct analytical training and training of security system officials and employees of the public administration in the area. The model is planned to be implemented in cooperation with international partners, international organizations, research centers and think-thanks.



NATO Counter Terrorism Panel 2019, organized in Croatia by SOA in cooperation with the Slovenian agency SOVA

Intelligence and Security Service of the Republic of Slovenia's Ministry of Defence), Daniel Markić (Security and Intelligence Agency of the Republic of Croatia), Rajko Kozmelj (Slovenian Security and Intelligence Agency), Goran Nikolovski (Administration for Security and Counterintelligence of the Republic of North Macedonia's Ministry of Internal Affairs), Zoran Ivanov (Intelligence Agency of the Republic of North Macedonia)

On 12 April 2018, the EC Commissioner for Security Union Julian King visited SOA. Current security threats and challenges to the European Union, such as terrorism, organized crime and cyber security were discussed at the meeting.



The signing ceremony of the SOA and ABW agreement



The Panel welcomes directors of military and civil security and intelligence agencies (from left to right): Goran Vasilevski (Military Security and Intelligence Agency of the Republic of North Macedonia), BG Ivica Kinder (Military Security and Intelligence Agency of the Republic of Croatia), Dejan Matijević (Military



SOA Director and EC Commissioner for Security Union Julian King

As in preceding years, in 2018 and 2019 SOA hosted the NATO Counter Terrorism Panel attended by more than 100 experts from about 30 NATO members and selected partner countries who discussed anti-terrorism measures and activities.

SOA Director participated at the inaugural session of the Intelligence College in Europe that was held on 4 and 5 March 2019 in Paris, France, under the auspices of the French President Emmanuel Macron.



Intelligence College in Europe is a platform for the exchange of non-operational intelligence, aiming to establish a common, European strategic intelligence culture in the context of global security and geopolitical changes.

At the inaugural session, SOA Director was one of four panelists - agency directors. Besides SOA Director, panelists included directors of the French security agency DGSI and intelligence agency DGSE, and the director of the Spanish intelligence agency CNI.



Panel at the inaugural session of Intelligence College in Europe on 5 March 2019 in Paris

SOA participates in international security discussions and deliberations at the highest level. SOA Director participated at the 54th and 55th Munich Conference that took place in February 2018, and 2019. At the conference, as the only representative from this part of Europe, SOA Director participated in round tables dedicated to intelligence, which were attended by the directors of the largest agencies in the Western world.



SOA Director at the meeting of the Croatian Prime Minister Andrej Plenković with the Secretary General of NATO Jens Stoltenberg at the 55th Munich Conference held in 2019



Counter Terrorism Group (CTG)

is a platform for a common European response to combat the threat of international terrorism

Terrorism is a transnational phenomenon and international cooperation between security-intelligence agencies is necessary in order to successfully preserve the common security from the threat of terrorism. With the rise in terrorism threat in Europe over the recent years, international security and intelligence cooperation has become more intense and successful.

SOA is very active internationally, bilaterally and multilaterally in preventing and countering terrorism threats. One of the most important multilateral forums of European security agencies addressing terrorism is the Counter Terrorism Group (CTG).

The Counter Terrorism Group is a grouping of security agencies of the EU member states, Norway and Switzerland. The Group was founded in the fall of 2001, and it includes 30 security agencies in total. SOA joined the Counter Terrorism Group in 2013.

Although the Counter Terrorism Group is not formally a part of the security architecture of the EU, it brings together the agencies from the EU member states, and it is chaired by the member of the group that belongs to the country that holds the EU presidency, a position that rotates every six months. SOA has thus already started preparations for taking over the presidency of the Counter Terrorism Group in 2020.

The objective of the Counter Terrorism Group is to improve cooperation between agencies in preventing and countering terrorism, as well as to ensure fast and secure exchange of intelligence. Cooperation within the Counter Terrorism Group has been constant and intensive.



A video clip from an ISIS video published in 2015 "announcing" the spread of the so-called Islamic State to the countries of Southeast Europe, including Croatia.

In addition to the regular exchange of intelligence related to terrorism, the Counter Terrorism Group works on common analytical projects to further analyze the phenomenon of terrorism, its causes and trends and to identify preventive and suppressive measures. Furthermore, the Counter Terrorism Group delivers threat assessments to the EU officials.

In 2016 the Counter Terrorism Group established a common mechanism for intelligence exchange in order to exchange data on terrorism threats more quickly and efficiently, pursuant to national legislation of the member states.

This intelligence exchange mechanism has yielded excellent results in countering terrorism, including prevented terrorist attacks and arrests of several individuals who had planned or had been preparing terrorist attacks.



The mechanism includes a common hub in the Netherlands, where agency employees of the members work together to counter the threat of terrorism.

APT attacks

have become an increasingly significant threat to national security

NATO and the EU members are often under attacks by malicious cyber campaigns aimed at undermining the protected communications and information systems. The Republic of Croatia has been a target of a series of cyber attacks in recent years.



These were the so-called APT attacks (Advanced Persistent Threat) which are long-term undetected attacks characterized by high level of expertise, highly complex organization and a plan of attack that includes careful targeting (government agencies, critical infrastructure etc.), acquisition of the necessary IT infrastructure that ensures the anonymity of the attacker (usually located in third states), tactics for malicious software implementation (fake e-mail, web links, an "infected" device, etc.), infection of the target's ICT system and activation of malicious software in order to steal confidential data from the target, disable its activities, or harm the system.

Due to their complexity and costliness, it is reasonable to suspect that APT attacks are sponsored by certain states. The attacks have largely targeted protected communications and information systems of state institutions of NATO and the EU members, aimed at collecting intelligence on their diplomatic, military and economic activities. Some of these hacker APT groups are Turla and APT28/Sofacy which have been attacking protected communications and information systems of the members of NATO and the EU for years.

To prevent unauthorized access to protected communications and information systems of state authorities which are aimed at undermining national security, SOA participates in proactive cyber protection of key state authorities. As a result, more attacks have been discovered at an early stage which has facilitated threat mitigation, and potential harm has been avoided.

With the upcoming Croatian presidency of the EU Council in 2020, and bearing in mind the targets of previous APT attacks, there is a risk of increased frequency of APT attacks on communications and information systems of state authorities of the Republic of Croatia. Therefore, in cooperation with other competent bodies, SOA has improved the defense against these kinds of threats to the national security.



An example of SOA operation:

An attempted APT attack on a state authority of the Republic of Croatia

A civil servant employed by a state authority of the Republic of Croatia received an email in which they were notified about an upcoming international conference with a topic related to their field of work.

The email had an attachment, which was a document acting as a registration form for the conference. Although this was an actual conference with the correct time and venue, the email was fake. After realizing that the sender's email address was not affiliated with the conference organizers, the civil servant contacted the information security advisor instead of opening the attachment.

Based on forensic analysis of the email, competent professional agencies have established that the attachment had contained a sophisticated malicious code. Opening the attachment would have activated a malicious code that would have compromised the civil servant's computer and would have allowed the attacker to collect confidential data.

Using social engineering techniques, the email had been tailored to target a specific civil servant, in order to encourage the opening of the attachment and to bypass a set of security controls on the computer.

Social engineering is a use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes, in this case to open the attachment with registration form that is of professional interest to the civil servant.

It is important to note that the targeted civil servant had not necessarily kept the data required by the attacker on their computer, but that their computer could have served as a base from which the malicious code could have spread to other computers. Therefore, all employees of state authorities should be aware of the possibility of APT attacks and the way in which they are carried out.

Technical intelligence about the attempted attack was forwarded through a secure communication channel to other state authorities in order to establish the scale of the APT campaign.

As a result of the civil servant's diligence, the APT campaign had been successfully detected and the attempt to establish control over their computer was prevented, which subsequently prevented further compromising of the information system of the state authority.



Big Data

affects the characteristics of the modern security-intelligence

The security - intelligence system must be capable to detect and warn, and sometimes preventively act on the emerging and growing threats to the national security, even before they are realized. This functionality is referred to as Early Warning.

To achieve this, the security - intelligence system must segment the security environment, identify trends and develop scenario planning. The 2017 National Security Strategy highlights this area of SOA operations and its further development and improvement.

The early warning system is based on monitoring and detection of relevant indicators and their interdependence, which lead to certain outcomes of events. In this way, emergent and growing threats can be detected and warnings can be issued. The system also allows actors to take appropriate steps to mitigate the threat before it gets out of control.

The task of SOA analysts is to identify the indicators, monitor their development, dynamics and interaction and based on that, draw appropriate conclusions. SOA operatives are tasked with collecting intelligence of best possible quality in real time for each indicator which the analysts could then monitor.

Until recently, the most challenging security - intelligence work was intelligence collection. However, in today's information age and with the development of technology, one of the challenges in processing and analysis of intelligence has been the development of management skills and the use of the vast volume of available intelligence, the so-called Big data, the majority of which originates from open sources.

Big data refers to the exponential increase in the volume of digital data created by the new information technologies, such as mobile Internet, social media and the Internet of things. A significant analytical challenge is the processing and analysis of that vast volume of data.

The concept of security - intelligence has adapted to these circumstances. The traditional way of operations had included attempts to obtain mainly secret and protected data on a subject, while now an additional challenge is to identify and find reliable and relevant data in the large volume of available data created through Big data.

For example, research shows that in 2017 there were 2.7 zettabytes (2.7 billion terabytes) of data in the digital world globally, and that 90% of those data had been generated in the last two years. In order to process such large volumes of data, Big data analytics have been developing automatic data collection, storage and processing, i.e. specialized developed software.

However, despite the increasing number of available data and advanced software, the subjects of security-intelligence interest are complex phenomena that are composed of countless combinations that depend on human activities, relationships and decisions, which renders event predictions impossible to be exclusively carried out by software.

Furthermore, it should be taken into consideration that numerous data in the information space are inserted deliberately for the purpose of disinformation of rivals, propaganda, recruitment and



the like, and it is thus very difficult to distinguish correct from false information that appear, especially in a short amount of time. In this case, software cannot replace a human analyst, their insight, and even intuition.

For example, the large presence of ISIS fighters on social media has enabled security - intelligence agencies to learn extensively about ISIS, their scheduling, fighter profile, weapons and the like. However, despite this, the major challenge has been using these sources to detect their specific future decisions and intentions. An even more demanding task has been predicting the course of events in a social process that takes place through social media because the large number of actors, their interrelations, intentions and possible scenarios undermines reliable prediction.

One of the results of the Big data revolution is the change in the required profile of security - intelligence employees. A greater focus will be placed on ICT and computer science specialists in order to develop software and algorithms for the collection and processing of Big Data, and analysts who will be able to interpret this great volume of data. However, security - intelligence activity will continue to depend on the competence of data-collection employees, and the development of technology and Big data will present an additional challenge for them in terms of data collection methods.



In addition to the growth of Big Data, security - intelligence community has been facing with yet another challenge. The media and social networks deliver information and misinformation about events at unprecedented speed. While the media and social networks are overloaded with a substantial number of versions of an event, security - intelligence agencies have to deliver accurate and reliable data to end users in order to facilitate informed decision-making.

For accurate intelligence, it is necessary to obtain reliable and verifiable data, and the entire process is lengthy. This is particularly true in the context of Big data, i.e. a significant number of contradictory information that is often generated on a particular topic.

Therefore, in terms of time, the security-intelligence agencies are racing the media and social networks that are not obliged to

publish information which has been reviewed and founded on reliable collected data.

On one hand, Big data and the modern information age are majors challenges for all security - intelligence systems, which will significantly affect the paradigm of security - intelligence work in the future. On the other hand, the power of information has been becoming increasingly prominent, so in that sense, security - intelligence will become increasingly important.

Internet trolling

as a form of information operation

Social media have been becoming places where citizens get informed and through which they form their views on societal and political issues. Besides all the positive aspects of this process, social media and other online virtual meeting places can be misused in support of political and military actions and have been becoming increasingly significant in the so-called hybrid warfare.

Hybrid warfare refers to a complex strategy of activities against a rival involving the use of several conventional and unconventional methods of action, from military and diplomatic means to information and cyber activities.

Hybrid warfare is complex and not always obvious or clearly recognizable. It requires continuous detection, monitoring and collection of intelligence on potential threats in the field of hybrid warfare (diplomacy, information operations, military, economic, financial, legal and intelligence activities).

Manipulation of information, in such circumstances, is the basis of hybrid warfare that has been consistently exploited. Therefore, a continuous monitoring of information operations in the media is clearly needed, aimed at early identification of disinformation campaigns. The rise in globalization trends and the development of modern technologies, in particular ICT platforms, but also cyber capabilities, have rendered societies increasingly vulnerable in relation to disinformation campaigns.

This chapter deals with a part of hybrid warfare referring to the segment of information - psychological operations aimed at

shaping the target public opinion and its adaptation to particular political objectives and interests.



The fight for public sentiment in the world or in a target country can be equally important as the effect of troops in the battlefield. States and other non-state actors have been using the Internet and social media to obtain support for their activities, to expand the circle of supporters of their policies, as well as to deceive and intimidate rivals.

Throughout several global political or military-political crises, it has come to light that mass fake online identities and user accounts can successfully disseminate the preferred narrative through social media, blogs and comments on key websites, in order to manipulate and deceive the rivals or the general public.

Some actors have therefore resorted to the formation and continuous activity of the so-called hybrid trolls. Hybrid trolls' tasks are directed towards deliberate dissemination of misinformation, rumors and fake data by participating in targeted



thematic discussions online and overloading the cyberspace with messages that are designed to contribute to achieving the political goals of their principals. Hybrid trolls' planned, targeted and deliberate activities differ from ordinary Internet trolls who act individually and whose sole purpose is to provoke other participants of discussions on social media.

Hybrid trolls advocate specific political views which they disseminate in online discussions. Their activities are characterized by persistent and intense repetition of the same narrative, posting the same message from different IP addresses and under different names (nicknames), and sharing the same links etc. In this way, they intend to create an impression of mass political opinion they espouse and to impose this opinion as dominant and true.

Hybrid trolling is not aimed at achieving total victory over the rival, nor can that be achieved. It primarily seeks to undermine the credibility and stability of the targeted rival or government, and adversely affect the level of public support they enjoy. Once a political rival is sufficiently discredited in the public, the trolling campaign's principal has the possibility to "reasonably" use other, more conventional measures to achieve their objectives.

Hybrid trolling cannot produce results independently, but only as part of a broader media - information campaign. Unlike the information - psychological operations in the past, hybrid trolling is rapid and cost efficient, but it is difficult to obtain evidence of its effects.



Hybrid trolls can operate anonymously and safely from any location worldwide. At the same time, social media and the Internet allow hybrid trolls a virtually unlimited reach to target audiences in the dissemination of narratives and disinformation.

Cases have been recorded where the objective of trolling has not been sending messages or persuading the target audience into a narrative, but overloading the information space with fake news and useless data, in order to direct the attention of the public or obstruct discussions on a certain topic. In this way, mostly with fake news and "conspiracy theories", the public is being deliberately misled about the truth pertaining to an event or a process, and this subsequently reduces the public trust in traditional media, objective reporting and investigative journalism. Simultaneously, this approach has been used to undermine citizens' trust in state institutions.

Hybrid trolling exploits and misuses freedom of expression as one of the fundamental values of democratic societies, and therefore its complete suppression in democratic societies is practically impossible. One of the ways in which it may be suppressed is by raising public awareness of the working and messaging.



Transparency and efficiency

are the two guiding principles of security and intelligence agencies in democratic countries

Security and intelligence agencies for the most part operate secretly and covertly. The reason behind this is greater efficiency, protection of agency's subjects of interest, as well as the safety of individuals involved in security - intelligence operations. In this respect, transparency and public openness represent risks to the efficiency of performance.

At the same time, democratic societies expect an appropriate degree of transparency and social responsibility from all state institutions. Security - intelligence agencies are no exception. Moreover, because of their significant authorities and possibilities of accessing citizens' personal data, which sometimes even affects human rights, security and intelligence agencies should be under particular oversight and held accountable for the legality of their activities.

Therefore, oversight of security and intelligence agencies in democratic societies is especially prominent and their impartiality and professionalism are of utmost significance.

In the Republic of Croatia, a three tiered oversight mechanism is in place for security - intelligence agencies: the parliamentary oversight is carried out by the Croatian Parliament through the Domestic Policy and National Security Committee, the expert oversight is carried out by the Office of the National Security Council, and the civilian oversight carried out by the Council for the Civilian Oversight of the Security and Intelligence Activities.

Oversight of security - intelligence agencies is a guarantee that security - intelligence agencies will not be misused or act illegally in the course of their operations. However, in order to enhance

democratic principles of state authorities, security and intelligence agencies of developed democracies have been increasingly focusing on transparency of their work in relation to the public. They have been seeking to establish the right balance between transparency and efficiency of their work.

One of the mechanisms for achieving transparency are public reports which are released by security and intelligence agencies in democratic countries. In 2014, with its first public report, SOA made a breakthrough in democratic standards of developed democracies in security and intelligence matters.

For its first public report SOA received the recognition of the EU Fundamental Rights Agency (FRA), which highlighted SOA's public report in its report in June 2015 as an example of promising practices. Efforts to bring SOA closer to the public by working with civil society organizations, the media, and students were also commended.



Promising practice

Publishing an annual activity report

Croatia's Security and Intelligence Agency (Sigurnosno-obavještajna agencija, SOA) has published an activity report explaining its role, duties, responsibilities and some of its current activities to the public for the first time. Prior to this, information related to SOA was considered classified. The agency launched a series of meetings with various target groups (civil society organisations, students and media) to bring its work closer to the public in 2014.

For more information, see: www.soa.hr

An excerpt from the report of the EU Fundamental Rights Agency, which refers to SOA's activities aimed at greater transparency

With these public reports SOA has joined numerous agencies in democratic countries which, just like SOA, report to the national and international public regularly on their activities and the security situation in their countries.

Examples are below - excerpts from the public reports of the Estonian, Swiss, Dutch, Swedish and German security/intelligence agencies:

44 INFLUENCE OPERATIONS

INFLUENCE OPERATIONS

Although Russian meddling in the internal affairs of several countries was exposed in 2017, this did not deter the Kremlin from undertaking new influence operations. In 2018, Russia's influence activities will be just as active as in past years.

For Russian special services, influence operations are an inexpensive, effective and well-established instrument in their arsenal. The capability in the field of information warfare is growing (see sidebar on information war units) and Russia is already well-prepared for more extensive disinformation campaigns.

Russia will continue its attempts to influence democratic decision-making processes in the West, especially in EU countries that have elections in 2018. The Kremlin believes that creating confusion in Western countries gives Russia greater freedom of action and increases its influence.

Increasingly Russia believes that the state is forced to wage a hidden political struggle against the West and this self-delusion is spurring it to expand its influence operations and information warfare capability. That means disseminating even more disinformation and more attempts to recruit Western

politicians, businessmen and opinion leaders abroad.

The aftermath of the Russian military intelligence operation in Montenegro and the intervention in elections in the West are good examples of how the Kremlin has been exposed and how operations that seemed audaciously successful on paper have actually produced the opposite result.

Since the US presidential election in 2016, awareness of the Kremlin's activity in the West has increased significantly. This has not deterred Russia and it is continuing its efforts to undermine – hack, leak or spread disinformation – supporting the European politicians who have proved suitable for the regime in Moscow. In 2017, "Moscow's hand" was detected in an impressive number of Western countries: the US, the UK, Germany, France, Spain, the Netherlands, Norway, Denmark, Sweden, Bulgaria, Montenegro, Malta and elsewhere. Moscow's attempts to influence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun Svizra

Swiss Confederation

Federal Intelligence Service FIS

SWITZERLAND'S SECURITY

Situation Report 2018
of the Federal Intelligence Service FIS



Facts about the Security Service



How we obtain information

MUCH OF OUR WORK IS concentrated on intelligence, especially our efforts concerning counter-espionage, counter-terrorism and counter-subversion.

Our intelligence gathering follows what is known as the intelligence cycle, i.e. direction, collection, processing, analysis and dissemination of information. There are various ways to collect intelligence:

- *Directed surveillance* – conducted by specially appointed Security Service staff.
- *Intrusive measures* – implemented by court decision only, and may include telecommunications interception, access to telecommunications data, secret camera surveillance, eavesdropping and postal interception.
- *Human sources* – people volunteering information.

- *Open sources* – such as the internet, newspapers, radio and television.
- *Information obtained through interrogations.*
- *Contacts with partner services* – the Swedish Security Service cooperates extensively with foreign intelligence and security services, especially in the area of counter-terrorism.
- *Contacts with other police authorities.*

Collected intelligence is processed and analysed. Prior to analysis, it is necessary to assess the credibility of the source and the accuracy of the intelligence. Once analysed, intelligence is passed on to relevant Service units, which decide on operational response, dissemination to appropriate recipients outside the Service and the focus for future intelligence gathering.

2017 REPORT ON THE PROTECTION OF THE CONSTITUTION
FACTS AND TRENDS

Espionage and other intelligence activities

States which strive to gain a knowledge edge in military (particularly strategic) or economic and technological contexts do not hesitate to procure the necessary information secretly and illegally by violating applicable law. In this context, their governments' political agenda dictates the priority areas of the individual intelligence services' activities.

Germany is of interest in its role as a geopolitical player, as a member of NATO and the EU and on account of its economic strength and innovative businesses. Oppositional groups from foreign intelligence services' home countries in Germany are another target of espionage activities. The consequences for Germany range from a weakening of its negotiating position to high material and economic damage and a potential impairment of its national sovereignty.

The Russian Federation, the People's Republic of China and the Islamic Republic of Iran are the major players behind espionage activities that are directed against Germany. Apart from that, other countries (including western countries) also play a role.

The **Russian intelligence services** invest a lot of organisational and financial effort to engage in espionage activities against Germany. With the use of cyberspace the extent of espionage has increased many times over. It is targeted at all areas of politics, economy, research and technology, with a focus on the political position of the Federal Government vis-à-vis the Russian Federation. The efforts of the Russian intelligence services focus in particular on those policy areas where decisions with a potential impact on Russian interests are taken. These policy areas include the alliance policy within NATO and the EU and Germany's foreign policy.

The tense relationship between the EU and Turkey and the resulting potential impact on the accession negotiations and the future of the EU – in particular after the so-called BREXIT vote – and the orientation of the Common Foreign and Security policy have been of particular interest to the Russian intelligence services.

Owing not least to the dwindling public interest, the Ukraine crisis which was very much in the fore in 2014 and 2015, has been overshadowed by other areas of tension such as the conflict in Syria. Nevertheless the question



A career in SOA

is unique and challenging, with excellent working conditions and opportunities for professional development

Employees are SOA's most valuable resource. Despite the fact that modern technologies allow for additional operational and analytical capabilities, security - intelligence activities are substantially defined by the competence, knowledge and skills of operatives and analysts.

In line with the mission and the broad scope of work, SOA employs experts of various specializations and profiles. The diversity in education and training allows SOA to monitor a wide range of security phenomena. SOA employs experts in economics, finance, computer science, law, criminology, political science, sociology, languages, electrical engineering and other fields.

The majority of SOA staff are civil servants, with a minor proportion of governmental employees. Three-quarters of SOA employees hold advanced and higher degrees. Women make up 40% of the staff and are equal in performing all tasks in the Agency's scope of work.

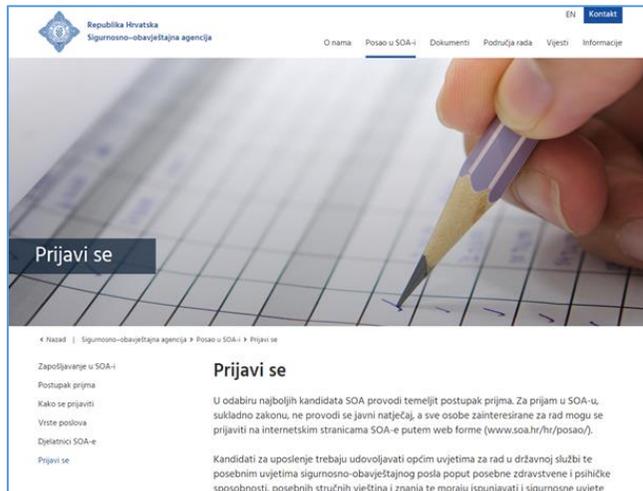
SOA staff are categorized by job descriptions. SOA operatives are responsible for data collection, analysts are in charge of analyzing the collected data, while IT specialists work on development projects and new technical solutions. In addition to the above, we employ officers for human resources management, accounting, legal affairs, administration and security.

SOA operatives are mostly based in the regional centers while analysts, IT specialists and other supporting professionals are usually based at the Zagreb headquarters.



SOA provides opportunities for professional development across a variety of fields and specializations. Particular focus is given professional development and training, both formal and practical.

In order to continuously improve quality of task performance SOA has kept an open application for interested candidates and has engaged in human resource renewal. SOA is interested in young, competent, educated and motivated individuals who will pursue a career at the Agency in the upcoming decades. A career in SOA is a unique and challenging opportunity with excellent working conditions and opportunities for professional development.



SOA website includes recruitment information and may be used by interested candidates to apply for a position

A thorough selection and recruitment procedure is carried out. In line with the relevant legislation, an administrative competition is not required for employment at the Security and Intelligence Agency. All interested candidates may fill out and submit their applications using the web forms at www.soa.hr/hr/posao/.

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

All submitted applications are considered by SOA. In line with the current needs, candidates that meet the qualification 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 as well as polygraph testing of the candidates. Those candidates whose test results correspond most with the employee profile will be selected.

Employment at SOA is an opportunity for a challenging and dynamic career on the protection of national security and in the interests and well-being of the Croatian citizens. Therefore, SOA invites all potential candidates to submit an application for employment. While previous working experience is not required, it is not a disadvantage for employment at the Agency. All candidates whose qualifications and competences correspond to the Agency's current needs and open positions will be considered in the recruitment process.

Application forms available at www.soa.hr

SOA is interested in experts of various specializations and profiles, and for this report we have selected three basic types of positions. If you feel that you match the requirements of some of the following positions in SOA, we invite you to apply:



OPERATIVE (m/f)

University graduate (secondary education for some positions)

Dynamic and curious

Highly developed communication and social skills

Resourceful in unpredictable situations

Willing to take on field work

Strong independent performer and a team player

Observant and detail oriented

Personally and professionally stable and resilient

Challenges do not intimidate you

Reliable and trustworthy

Keen to learn and develop



ANALYSTS (m/f)

University graduate in social sciences, humanities or technical sciences

Interested in social issues with a wide area of interests

Systematic and analytic

Developed skills of objective reasoning

Competent in analyzing 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

Reliable and trustworthy

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

Results oriented

Focused on practical application of technical and information systems

Keen team player

Reliable and trustworthy

Keen to learn and develop



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

Photo: SOA, the Government of the Republic of Croatia, screenshot (social networks, Twitter)

Illustrations: Pixabay

Maps: SOA



Security-Intelligence Agency
Savska cesta 39/1
10000 Zagreb

Phone: 01/ 377 22 22

E-mail: informiranje@soa.hr

www.soa.hr