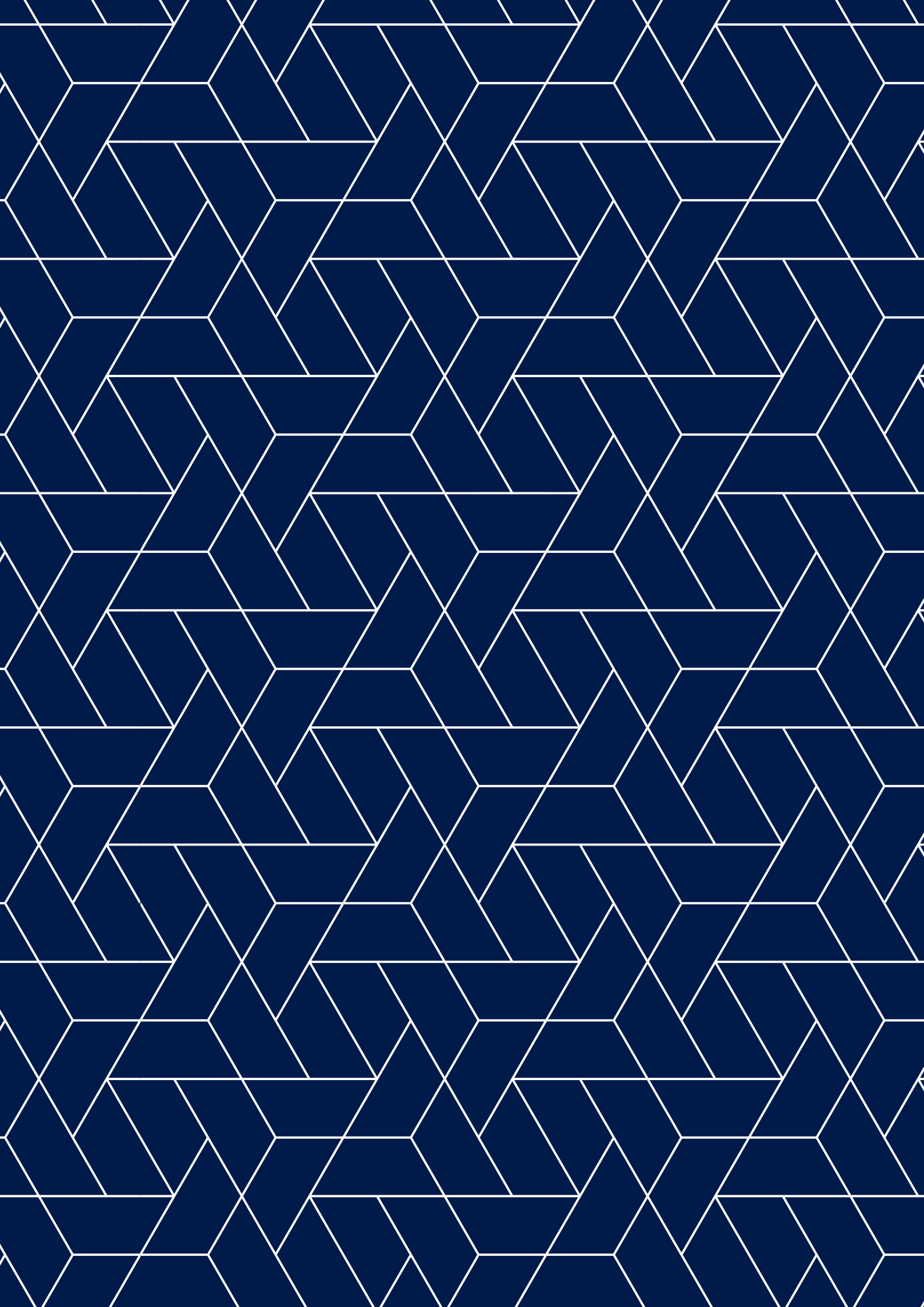
Security Sector Reform (SSR) in Practice in Europe and Central Asia – No. 1

DCAF Geneva Centre for Security Sector Governance
20TH ANNIVERSARY

INSIGHTS AND LESSONS LEARNED FROM CROATIA'S INTELLIGENCE REFORMS

By Dragan Lozančić



About DCAF

The Geneva Centre for Security Sector Governance (DCAF) promotes good governance and reform of the security sector. The Centre conducts research on good practices, encourages the development of appropriate norms at the national and international levels, makes policy recommendations and provides in-country advice and assistance programmes. DCAF's partners include governments, parliaments, civil society, international organisations and the range of security sector services, including the military, police, judiciary, intelligence agencies, and border security services.

Visit us at www.dcaf.ch

About the Series

The "SSR in practice in Europe and Central Asia" series comprises case studies in which security and justice sector practitioners reflect on experiences and offer personal insights about implementing reform in security sector institutions in transition environments, with a particular focus on the Western Balkans, Eastern Europe, the South Caucasus, and Central Asia. The papers provide insight into challenges and opportunities within security sector reform processes and address interests of practitioners, policy-makers, and researchers alike.

About the Author

Dr. Dragan Lozančić has been a government civil servant for almost three decades and has held several senior posts in the Republic of Croatia, including as the Director General of the National Protection and Rescue Directorate (2017 – 2018) and the Director of Croatia's Security and Intelligence Agency (SOA) (2012-2016). During his time as Director of SOA he introduced a robust set of reforms, promoted technological innovations and advanced an ambitious international cooperation agenda. Dr. Lozančić has also served in the Republic of Croatia Ministry of Defence for almost two decades and held several senior management posts, including being appointed by the government to the post of Assistant Defence Minister responsible for defence policy, planning and international security affairs.

The views and opinions expressed in this paper are exclusively those of the author and do not necessarily reflect the official policy or position of DCAF, SOA or the Republic of Croatia.

Acknowledgements

We would like to thank the members of the DCAF ECA editorial board for their dedication and the time they devoted to review this series.

Publisher

Geneva Centre for Security Sector Governance (DCAF)

Maison de la Paix
Chemin Eugène-Rigot 2E;
CH-1202 Geneva, Switzerland
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch

Proofreading

Sarabeth Murray, DCAF Geneva

Design and Layout

Rodrigo Amorim, DCAF Geneva

Insights and Lessons Learned from Croatia's Intelligence Reforms

By Dragan Lozančić

Intelligence reforms proved elusive in the early post-Cold War transitions to liberal democracy and free market economies. Some were still struggling decades after the fall of the Berlin Wall1. To be fair, much of the early concerns revolved around harnessing the armed forces and reforming defence in general. Away from the spotlight and often in the shadow of major political shakeups, security and intelligence services appeared to be unmoved by the changes taking place around them. They retained most if not all of their old habits well into the new millennium. "It is hard to find an ex-communist country in eastern Europe," writes The Economist, "in which the intelligence and security services are depoliticized and uncontroversial."[2] It often took headline-grabbing public scandals to reveal how deeply rooted these problems were.

A sense of being above the law was a notoriously avowed characteristic of the secret services. Such a notion is discordant with liberal democracy. The health of a democracy is heavily predicated on the rule of law and serving the public interest. Without a culture of accountability, effective oversight mechanisms, and properly implanted 'special powers' safeguards, it would be naively premature to close the chapter on our transition to democracy.

Yugoslav Legacy

The State Security Service of the former Yugoslavia, still best known by its earlier acronym 'UDBA', was a notorious instrument of totalitarian power that went well beyond its formal internal security mandate (counterintelligence). Its main purpose was to protect the state from its enemies at home and abroad. Cradled between the Warsaw Pact and NATO, and besieged by its own internal complexities, the former Yugoslavia's survival greatly depended on an effective intelligence capacity. While many of its perceived threats were indeed real, some were arguably not. The State Security Service had its central federal headquarters in Belgrade and semi-autonomous administrative branches in each of the Yugoslav republics. With its bendable constraints, it was ruthless and unscrupulous in pursuing its mission. It relished in its 'extendable' enforcement powers of investigation, interrogation, secret surveillance, and making arrests. Its clandestine modus operandi provided ample cover for abuse, intimidation, and torture. It had established a vast network of informants and had accumulated hundreds of thousands of files on its own citizens. It was also responsible for dozens of kidnappings and murders of political dissidents, activists, opposition groups, and other deemed enemies of the state. Criminals were often recruited to handle its dirty work. With the dissolution of the former Yugoslavia and the transition to democracy in the early 1990s, Croatia and the other republics went their separate ways, inheriting the fragmented manpower, infrastructure, and vast data bases from the former system. Unfortunately, they also inherited a mindset that they were above the law and an aversion to external scrutiny. Some of the new republics were less successful than others in shedding these legacies.

The mood must have been lackluster, if not defiant, within the elitist-minded intelligence ranks of the secret services. The 'old guard' had a direct stake in preserving a lucratively cultivated status quo. It deemed itself an exclusive 'members only' club and had successfully opposed intrusions into its world of secrets. Not only were they reluctant to have their powers checked but facing liability for their actions was an uncomfortable thought. I can only imagine how the notion of external, independent scrutiny by parliamentarian, judiciary, or other bodies must have been disturbingly indigestible.

1 See Craig S. Smith, "Eastern Europe Struggles to Purge Security Services," The New York Times, December 12, 2006.
2 "Spy scandals in eastern Europe reveal some damaging hang-ups," The Economist, December 19, 2006.

The consequent years of Euro-Atlantic integration ushered in a new era. Many security services have profoundly changed. A new generation of operatives and analysts have replaced the Cold War workforce. They would have an unprecedented opportunity to work closely with their new Western partners and allies. The shared interests and values within the EU and NATO, as well as the growing transnational nature of security challenges like terrorism, opened significant new prospects for intelligence cooperation. Joint covert operations and intelligence sharing became the new norm. It also opened education and training opportunities for the new cadre of intelligence professionals.

Yet, intelligence organizations would remain burdened by their unsettling legacies, inherent complexities (secrecy), and fragile vulnerabilities to abuses of power and human rights violations.

Weighing Legacies and Ambitions

"My main worry is that he does not have any operational or intelligence-related experience," complained a senior ranking member of parliament to a journalist after an October 2012 closed-door hearing in the Domestic Policy and National Security Committee of the Croatian Parliament. The Committee had just voted unanimously to support my nomination as director of Croatia's Security and Intelligence Agency (SOA). The thirteen-member cross-party Committee, headed by a ranking member of the main opposition party, was required by law to provide a preliminary opinion on a candidate before a formal appointment by the President and Prime Minister. While the opinion is non-binding, it provides an opportunity for members of parliament (MPs) to address concerns, raise questions, and weigh in on executive nominations.[3]

The hearing lasted several excruciating hours as MPs posed a wide range of professional and personal questions. What are our most significant national security challenges? Can you and how would you improve the agency? Do you believe that merging the foreign intelligence and internal security services into a single agency (SOA) was a good idea? Why do you think that you are best qualified to lead the agency? What can you do to promote gender equality in the agency? These were just some of the many questions put to me.

I became the director of SOA after moving over from the Ministry of Defense, where I had been the Assistant Minister for Policy and had already dedicated over two decades of my life to public service. In particular, I had extensive experience with international and inter-institutional cooperation, including working on security and defense reforms, NATO-related issues, and EU negotiations and formulating national security strategy, policy, and legislation. I had apolitical convictions and no political party affiliation. Accepting the reigns of our nation's civilian intelligence service was anything but an easy personal decision.

The Agency's senior leadership briefed me on our past and present activities. I had mixed feelings early on. I was impressed and yet somewhat ambivalent. It appeared we were collecting the necessary information and analyzing it adequately. And in a timely manner, we provided completed products to the proper authorities, hoping that they would make well-informed decisions and take appropriate action to safeguard our national interests. After all, I thought, this is what it was all about.

'Skeletons in the closet'

It was not long before I came to appreciate the true complexities of my job, including the 'skeletons in our closet', the systemic shortfalls behind the façade, and the many other challenges we still faced.

The intelligence community's evolution naturally reflected much of Croatia's own hardships, challenges, and achievements. Its Yugoslav legacy, war of independence, and Euro-Atlantic aspirations all play a part in shaping how far we have come and where we are today. Along the way, Croatia adopted good governance principles of intelligence management, shared by its many Western contemporaries. That these espoused Western standards, underscored by far-reaching oversight measures, went unchallenged and were never seriously in doubt illustrated Croatia's determination to join the ranks of the like-minded club of democracies of NATO and the EU.

3 While regulations outline the procedures for appointments and removals, there are no set requirements or qualifications that a nominee needs to meet in order to be appointed as director of SOA. National approaches vary and often depend on a variety of factors.

Much of the groundwork to bring Croatia's intelligence structures into the mold of its Western counterparts and instill democratic principles of oversight, control, and accountability, as well as establish a bulwark of safeguards against abuse of power, were well in place long before I came to the Agency. While these principles were in effect constraints, adhering to them offered our best chance to garner public trust and confidence. They are also the basis of our legitimacy, integrity, and credibility in difficult times, serving to discourage the misuse or abuse of power by political authorities. Unfortunately, even the most prominent democracies are not immune to abuse. Over the years, numerous contingencies would test our own limits.

Case Study: 'Skeletons in the Closet' - Allegations of Unlawful Hiring

In February 2014, media reports emerged about SOA's irregular hiring practices between 2006 and 2008. The parliamentary oversight committee announced a formal inquiry and established a working group of seven of its thirteen permanent members (four MPs from the ruling coalition and three from opposition parties). Upon their request, the MPs received a detailed classified report from SOA. They were also briefed in the parliament by the director of SOA and his staff on SOA's recruiting history, methodology, criteria, and regulations. The MPs also visited SOA's headquarters, receiving full access to examine all documents related to the case. By late May, the committee adopted conclusions that were critical of previous hiring practices and appointments. The main opposition party MPs issued a separate, dissenting opinion. Both were leaked to the media. The case was also reviewed by the Office of the National Security Council and investigated by the state prosecutor. No charges were ever filed and no one was ever held accountable. The National Security Council met on July 4 and issued a public statement that alleged wrongdoing yet shied away from making direct accusations of unlawful behavior. The statement also described SOA's irregular hiring practices as "unacceptable" and a "risk to security", undermining SOA's "reputation and credibility." The statement further concluded that the formal regulations and measures recently adopted would prevent similar occurrences in the future.

A new legal framework

The current foundation of Croatia's security-intelligence system was outlined and defined by an all-encompassing and unifying law in 2006.[4] It was the culmination of many years of post-conflict transformation and the final intelligence-related step towards Euro-Atlantic membership. To its credit, the law is comprehensive and yet concise. It indisputably marked the start of a new era as far as Croatia's intelligence community was concerned. Civil society groups, some academic experts, and opposition parties had some doubts, pointing to unchecked approval of certain special measures (surveillance) and shortfalls in oversight. On a practical note, and despite several disturbing scandals, it is remarkable how well this law has endured the test of time.

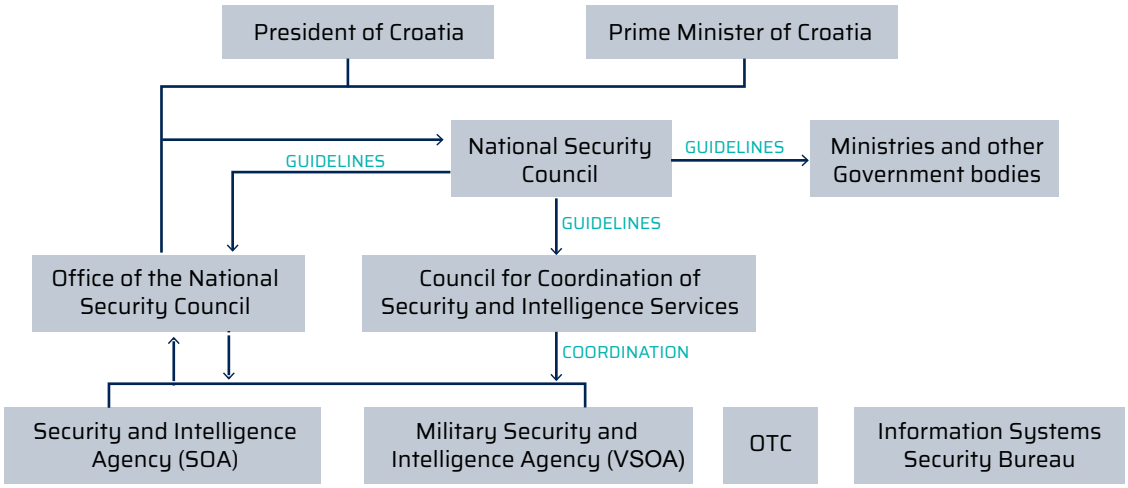
The law forged a merger of the (foreign) Intelligence Agency and the Counterintelligence Agency. SOA emerged as a single civilian service responsible for external and internal security, with regional offices throughout the country. The law also established a military intelligence agency (VSOA) and an Operational Technical Center (OTC), the latter an independent body that manages the interception of telecommunications[5]. By introducing effective executive control through the National Security Council and multiple, wide-reaching oversight structures,[6] the groundwork for promoting the rule of law, accountability, and basic democratic principles was initiated. These new mechanisms would be frequently tested. SOA's 2015 membership in the Club de Berne - Europe's discreet intelligence sharing forum - and its robust international cooperation with the world's leading democracies acted as a testament to its overall accomplishments.

4 The Law on the Security and Intelligence System of the Republic of Croatia, adopted in 2006, introduced a series of systemic changes.

5 The Military Security and Intelligence Agency (VSOA), SOA's sister agency within the Ministry of Defense, was responsible for military and defense threats to Croatia's national security. OTC stands for the Operational-Technical Centre for Telecommunications Surveillance. For a complete overview of Croatia's intelligence system, see https://www.soa.hr/en/about-us/security-intelligence-system-of-the-republic-of-croatia/.

6 The law outlined three independent but somewhat loosely-linked oversight structures: parliamentary (committee of members of parliament), administrative (experts), and civilian (non-governmental).

Croatia's Security-Intelligence System



SOURCE: HTTPS://WWW.SOA.HR/EN/ABOUT-US/SECURITY-INTELLIGENCE-SYSTEM-OF-THE-REPUBLIC-OF-CROATIA/

An uphill battle: building public confidence

The agency, nevertheless, has not been immune to accusations of abuse of power, cover-ups, or rights violations, leading often to open public criticism and suspicion. Apart from a few highprofile instances, allegations of wrongdoing rarely had an appropriate conclusion. The effectiveness of parliamentary oversight was overly dependent on party partisanship. Classified information was often leaked for self-serving political purposes or with the intent of publicly discrediting opponents. In two separate, highlypublicized scandals during my own tenure, the parliamentary oversight committee investigating allegations of misconduct split along party lines. In both cases (illustrated), perceptions that the committee's conclusions would hurt their respective political parties outweighed MPs' obligation to act as impartial arbiters. Partisan politics prevailed over duty, integrity, and higher moral standards. It is no wonder we never mustered the courage to openly gauge popular opinion. Building public confidence would become a personal aspiration, one I hoped all future directors would champion.

My attention, as if by default, shifted towards the 'nuts and bolts' of our core business of collecting, analyzing, and distributing intelligence. At the same time, I thought it was equally important to assure that we had the proper support functions well aligned. Underestimating their significance in an organization dominated by operatives and analysts was a trap I would not allow myself to be lured into. All the pieces of the organization needed to fit together well.

Embarking on Reforms

Measuring our effectiveness was not going to be easy. Agency pundits argued that our success be measured by 'things that do not happen' rather than by 'things that do'. For example, short of an outright terrorist attack, we should assume that our counterterrorism efforts were working. Keeping SOA from the front page of the newspaper topped our level of ambition. But it does not take a lot of wisdom to realize that this line of reasoning can be flawed. So, it was not apparent whether we were, in fact, doing a good job, were simply lucky, or fell somewhere in-between.

The world around us was in a state of flux. A diverse range of factors would affect our work. Not only was our threat environment rapidly changing, but alongside advances in technology, shifting domestic demands, pressing competition, and increasing international interdependencies, we were experiencing our own 'growing pains' as an agency. We needed to pose many questions to ourselves. Is our role changing? Were traditional intelligence tenets and approaches still useful? What kind of knowledge and which skill sets would we need in the future? How does new technology affect our work? What kind of people should we be hiring and how should we train them?

The key basis of intelligence endeavors, conventionally the capability to acquire information, appeared to be shifting in favor of a capacity to manage, sort, and make sense of large amounts of information

and data, often readily available to a wide array of other actors as well. Security risks and threats were changing, making it increasingly difficult to address them on our own. Thus, alliances and partnerships became important assets and key power multipliers. Terrorism and other transnational challenges accelerated international cooperation to unprecedented levels. In Croatia, governmental expectations and public attitudes were changing. This called for a fundamental reevaluation of SOA's practices.

Agency self-assessment

During my first year in office, we established a working group of SOA experts, tasked with evaluating our challenges and shortfalls. It was an intra-service evaluation or self-assessment of the Agency. After several months, they produced an extensive report of their findings along with a relevant set of wide-ranging recommendations. While the findings prompted heated discussions within the Agency's senior leadership, the working group's conclusions were difficult to ignore. The report would later become the basis for our strategic development plan[7].

The role of SOA remained largely unchanged, although we acknowledged the need for vigilance and flexibility when dealing with future uncertainties. We would continue to provide an important service in safeguarding Croatia's national security. Yet, we were also struggling to shed the burden of an entrenched 'doing it the old way' intelligence culture. There was a need to narrow our efforts and become more mission-focused and goal-oriented. Likewise, we wanted to tilt the balance in favor of investing more in our future as opposed to our congenital preference to dealing with current events or the 'problem of the day'. In effect, we needed to treat our intelligence efforts as if it were an 'enterprise'.

Identifying intelligence requirements and priorities

Our transformation would call for greater emphasis on strategic and corporate-like thinking in order to determine how we might accomplish our mission. In close collaboration with our customers—the president, government and state institutions that act upon our products or benefit from our actions—the first imperative was to set clear intelligence requirements and priorities. In previous years, our annual policy directives were vague, exceedingly broad, and often copied and pasted from previous years. We also had to establish a means of gauging customer satisfaction. Were we meeting their intelligence needs and living up to their expectations?

Investing in developing new capabilities

As with any organization, managing our resources and assets was critical. Our most valuable resources were, and will continue to be, our people (I apologize for the cliché). Even as we adopt new technology, our people will be the ones who will have to use it. Our recruitment, hiring, and career management needed a complete overhaul[8]. Previously, little systematic emphasis was placed on training and we did not pay much attention to developing future leaders. Our budget was strained by salary allocations and high maintenance costs. It left little room for investing in new capabilities and it was highly unlikely our budget would increase. We needed to 'tighten our belt' and make a serious attempt at realigning our financial expenditures. And we did just that. In less than two years, we cut personnel costs by ten percent and more than doubled our investments. Without raising our level of ambition, namely a higher threshold on annual investments in modernization and development, we could well jeopardize our ability to accomplishing our mission in the future[9].

Moving towards new paradigms

We also felt it was time to challenge the old secrecy-entrenched paradigm and gradually open-up to the public. After all, our role, as prescribed by law, was not only to safeguard (often abstract) national interests and the constitutional order, but it was also our job to protect our citizens. They also needed to recognize the benefits from the service we provided or, at the very least, be informed of what we do, and moreover, of the threats our nation faced. However, not everyone in Croatia's intelligence community agreed. "It would suffice," a senior official told me, "that only a few of us in government are aware of the Agency's merits." But public perceptions fueled by years of critical media coverage convinced me otherwise.

7 Unfortunately, both documents are highly classified and not publicly available. The challenge of generating an objective assessment of an intelligence agency's performance is greatly limited by its iron veil of secrecy and closed doors to outsiders.

8 A major scandal erupted in 2014 when a whistleblower revealed classified information to the media that pointed to earlier employment irregularities in SOA. It eventually led to a parliamentary committee investigation, the conclusion of which showed a split along political lines between ruling coalition and opposition MPs.

9 As its recent public documents indicate, SOA has continued to increase its investments in modernization and capability development ever since.

Earning public trust and respect through effective oversight

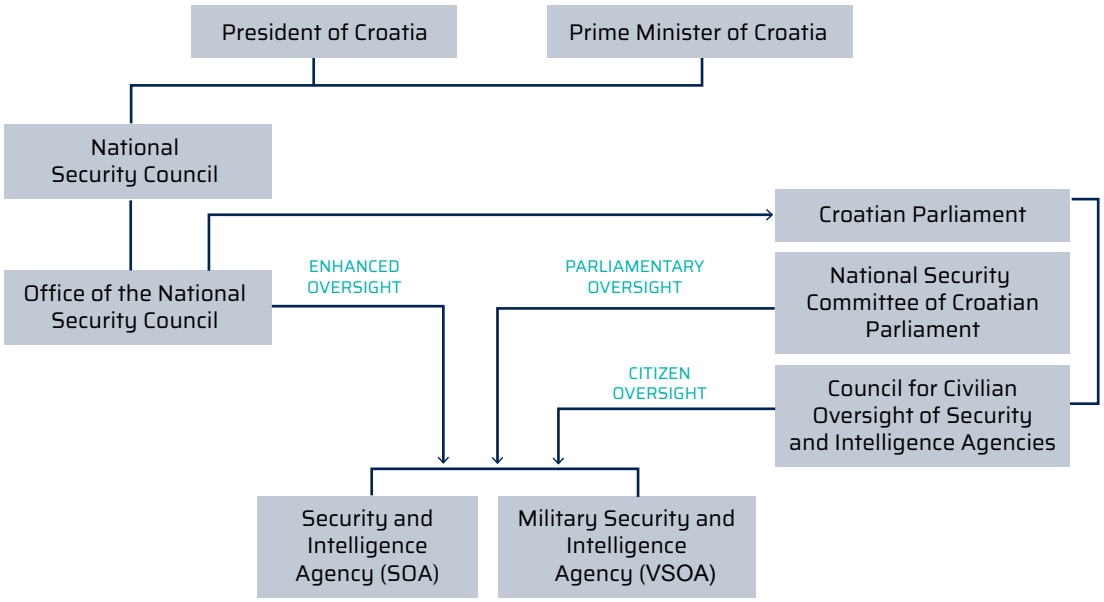
Our intent was not to gain society's respect out of fear, as in the past, but out of conviction in the justification and legitimacy of our actions, as well as out of confidence in our competence. Strong public trust and support would go a long way in helping us accomplish our mission. But unlike other government ministries and institutions, our ability to explain ourselves or defend our actions is significantly limited. We had to rely on others, especially those institutions with control and oversight responsibilities.

I was fully aware that our three-layered oversight bodies—a standing, bipartisan parliamentary committee, the Office of the National Security Council, and the Civilian Oversight Committee—had an important role to play. With essentially unlimited investigative access and oversight powers, they were well placed to examine complaints, establish the facts and verify the legitimacy of any questionable activity. Once activated, the oversight bodies were authorized to interview any agency staff member and review all case-related documents.[10] While they may overlap in their inquiries, their respective oversight capacities and authorities differ greatly, as each body technically plays a unique role. The parliamentary committee has statutory precedence as Article 80 of Croatia's Constitution specifically tasks parliament with exercising oversight over "security services".

The parliamentary committee can defer oversight to one of the other two bodies. In that sense, the Office of the National Security Council has the expertise and knowledge to look into issues independently or in support of a parliamentary inquiry. They have an experienced staff and conduct preplanned, annual oversight inspections, which they report to the president and prime minister. This enables them to have a special appreciation and thorough understanding of how SOA operates. Likewise, the civilian committee is a unique oversight mechanism not found in many democracies. The committee is responsible to the parliament and consists of seven individuals appointed to a four-year mandate. Their value lies in their authoritative capacity to investigate individual claims of abuse, allowing the parliamentary committee to concentrate on the more serious cases.

Of course, practically all of this takes place behind closed doors in order to protect SOA's classified information, as well as its agents, sources, and clandestine modus operandi.

Intelligence Oversight



SOURCE: HTTPS://WWW.SOA.HR/EN/ABOUT-US/OVERSIGHT/

10 According to Article 105, Section 3, of the Law on the Security and Intelligence System of the Republic of Croatia, the right to see classified case-related information does not include access to the identity of SOA's sources or intelligence information provided by foreign services without their consent.

Accusations of misappropriate conduct, whether by the Agency or individual officers, needed to be investigated thoroughly and immediately.[11] While the oversight bodies can act independently, the executive level (the president and prime minister) can also ask the Office of the National Security Council to examine an incident, and has the primary responsibility of holding SOA accountable. It does not end there. The conclusions of an investigation and any subsequent measures had to be appropriately communicated to the public so that trust be maintained or restored.

This was already a well-established model, common in Western democracies. In practice, unfortunately, it does not always function as expected. Party politics and self-serving interests can easily inhibit the process, as can a lack of political will or resolve. And the world's most prominent democracies have yet to discover a cure for political immaturity, delinquency, or folly. In liberal democracies, intelligence agencies are powerless as elected officials legitimately and rightfully hold the reigns of oversight. Nevertheless, they play a crucial 'national watchdog' role that holds SOA accountable, thereby directly impacting on the public confidence we were seeking to achieve.

I had no illusions of the challenges ahead.

Charting a new course of modernization and transformation

In essence, it came down to a simple choice: risk being overtaken by the changing circumstances or adapt and attempt to pilot the service on a desired course of forward-looking modernization and transformation. This was not a difficult decision as I was strongly committed to leaving SOA a better, more capable, and accountable institution at the end of my four-year term as director.

I was determined to introduce a strategic rationale as a starting point and tap into our nation's potential. In doing so, we consulted Croatia's top corporate leaders and technology experts. We established formal partnerships with leading academic and research institutions. We also sought support from key international partners. Eventually, we identified three strategic objectives.

Strategic impact

First, we wanted our efforts to have a strategic impact. Intelligence work should have an unswerving effect on security policy. It should lead to direct actions by other institutions or represent a basis for making important governmental decisions. We should be collecting actionable information. But for that to happen, there must be consistent interaction between intelligence officials and policymakers. Intelligence requirements must be prioritized, clear, and regularly reassessed. We cannot afford to waste resources on efforts that result in a widely disseminated, yet rarely useful, product. We should concentrate on important issues and utilize our comparative advantage.

Internal cohesion and aspiration for excellence

Second, we wanted to maximize internal cohesion and institutionalize a perpetual aspiration for excellence. The transient security environment and the rapid development of technology call for an organization that encourages innovation and creativity. Our headquarters, regional centers, and operatives must share a clear mission focus and have to act in unison. We need to be able to transfer knowledge from one generation to the next, while developing new skills that our agents will need in the future. This is especially true for services with modest resources and capabilities. It implies a greater emphasis on education and training, as well as the creation of mission-focused efforts and flexible special-task teams.

Strong international partnerships

Third, we needed to build strong international partnerships. Given the transnational nature of most threats, it is difficult to imagine any service that can single-handedly meet its national security requirements. Intelligence cooperation is no longer an option; it is a necessity. The interconnectivity of our societies alone requires a modern service to have a network of international relationships. Building trust and confidence are key ingredients for effective cooperation. Several multilateral and regional forums provide frameworks

11 In 2019, as it had not been adequately regulated in the past, Croatia adopted a new 'whistleblower protection' law, concerning the protection of individuals that report work-related wrongdoings. See https://www.cms-lawnow.com/ealerts/2019/11/experts-welcome-croatias-new-whistleblower-act-but-warn-of-flaws?cc_lang=en.

for cooperation throughout Europe.[12] Cooperation can also be effective at the bilateral level or in efforts where only a few services are involved. Not only is it imperative to establish lasting institutional links, but, because security and intelligence officials are career professionals, it is especially important to create personal relationships as well.

These objectives are interrelated and mutually supportive. They defined the foundation of our strategic development plan, presented to the president and the government in my first year as director. The plan was also adopted by a cross-party, unanimous vote in Croatia's parliamentary intelligence committee. This has been instrumental in pushing forward the many new efforts, initiatives, and projects undertaken since. Fortunately, it called for few changes to our organizational structure, which would be subject to external (executive) approval.

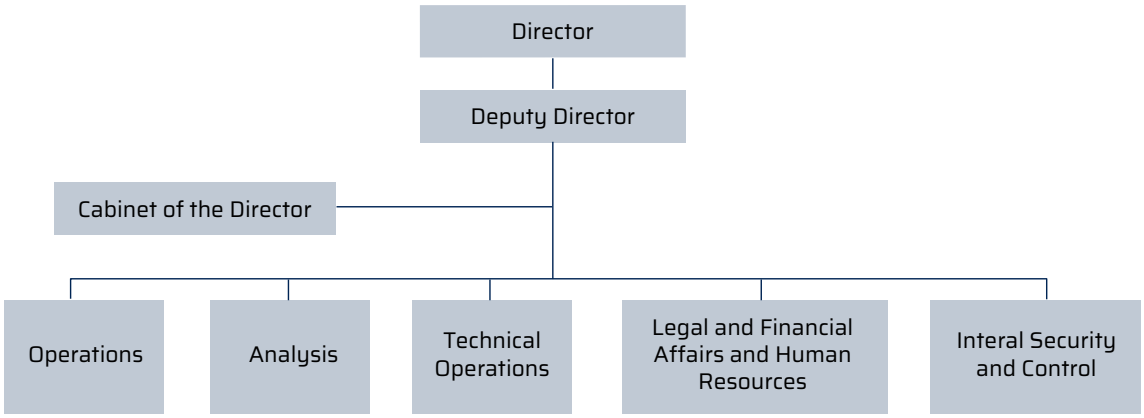
Decentralize authority

One of my avowed aims was to decentralize authority, define clearer responsibilities, and create a more balanced relationship between main power brokers in the Agency. SOA had been highly centralized, with operations and an all-powerful director promoting an organizational culture of dominance. The way to change that was to delegate authority and promote a 'whole of agency' approach to accomplishing our mission. It meant greater visibility for technical experts and support staff. A senior management board was established to discuss options and priorities, as well as to prepare proposals for formal adoption. Most of our efforts fell into three general categories:

- collection, operations, and analysis capabilities;
- technology and modernization; and
- organization, management, and business processes.

New initiatives ranged from institutionalizing operational lessons learned and developing modern HUMINT capabilities to establishing a novel hiring scheme and an automated career management and planning system. In addition, several important technological projects were embarked upon, in order to allow us to keep up with global trends. Unfortunately, some initiatives had to be abandoned. We assessed our annual achievements and either modified individual priorities or adopted new ones. But perhaps our most noteworthy achievement was the leadership and agency-wide teamwork behind each of these efforts. That could well be the critical factor guaranteeing SOA's sustainability and future development.

SOA Organizational Structure



SOURCE: HTTPS://WWW.SOA.HR/EN/ABOUT-US/STRUCTURE/

12 My successor was able to assemble representatives of 23 entities within the European intelligence community in Zagreb on 26 February 2020 to sign a letter of intent on establishing the "Intelligence College of Europe," a forum for cooperation on intelligence training, education, and knowledge exchange. Although a French initiative, SOA has played an active role and will preside over this initiative in the first year of its infancy.

I was confident that we had set in motion a process that would shape our intelligence efforts into a highly effective public service enterprise. While this almost business-like approach had its limitations, it was undeniably useful in removing a sense of complacency and igniting a desire to do more, perform better, and reach new heights. Our stakeholders should accept nothing less because protecting our vital interests and our national security depended on it.

Trends, Opportunities and Challenges

The expertise that intelligence agencies provide to policymakers exists within a new, highly competitive arena and we have to accept that we no longer have an intellectual monopoly on intelligence. There is a proliferation of open-source, readily available analyses produced by a variety of actors, including private companies, think tanks, universities, media outlets, and individual experts empowered by the internet. Commercial competitors, including those that hire former intelligence experts, are also rapidly emerging and offering their services on the open market. Further, our political leaders and policymakers are better informed than ever before and often have their own, usually well-informed sources.

From collection to validation of information

The timeliness, reliability, and flexibility of our tradecraft will be tested like never before. We will have to be much better at not only collecting information, but more importantly, at distinguishing, sorting and analyzing data. And we will have to do it faster and present our conclusions in a more convincing manner than previously envisaged. The rise of misinformation and disinformation complicates matters, as we find ourselves in a so-called era of 'post truths'. What is real news and what is 'fake news' will be increasingly harder to distinguish. So, rather than being called upon to provide information, we may be increasingly asked to provide clarity, validate facts, or simply confirm their reliability.

Expectation management

Stakeholders will expect intelligence services to foresee even those marginal dangers on the very periphery of the threat spectrum. They will also presume that we have mystical, sometimes supra-state powers to prevent threats. While the essence of our work is to provide early warning and analytical insight on security issues, expectations are sure to surpass realities. For starters, intelligence agencies do not have a crystal ball to predict the future and they certainly do not have the answers to all of our nation's woes. Intelligence cannot be a substitute for policy-making. Rather, intelligence agencies serve the policy-making process. SOA's utility lies in knowing what is needed (intelligence requirements) and how the service that it provides is used (policy decisions). Intelligence constraints cannot be used as an alibi for inaction nor compensate for other institutions not doing their job. The policy-makers' predicament, as Henry Kissinger noted long ago, is that decisions will often have to be made long before enough is known to fully justify them.

Cooperation within multi-institutional platforms

Effectively tackling future challenges will increasingly depend on SOA's capacity and ability to work within domestic multi-institutional platforms. SOA does not have police or law enforcement powers. The information it collects, while useful to police and state prosecutors, cannot be used in criminal proceedings. Its relationship with law enforcement bodies has been tempestuous although tolerable at best. While a growing overlap in responsibility frequently leads to mild friction, there is a strong mutual need to coordinate and cooperate. SOA has signed agreements with law enforcement bodies and several other key national partners. Whether we face a domestic terrorist threat, subversion, extremism, high crimes and complex corruption cases, cyber-attacks, or other illicit activity, our ability to work together is critical to our effective response as a nation.

Consequences of digitalization and new technologies

Technology provides security services with a plethora of new opportunities in both intelligence collection and analysis. We live in an increasingly digitalized society that produces vast, previously unimaginable amounts of data. Advances in artificial intelligence can help with the heavy lifting. But our adversaries can also exploit it. While encryption enables secure communication, it also makes it exceptionally difficult for security and law enforcement agencies to intercept the communication of suspected terrorists and criminals.

The public also has increasing demands, constantly shifting in emphasis between security and privacy. People are understandably skeptical of and resistant to the covert and intrusive powers that intelligence agencies have at their disposal. While privacy is a fundamental right, it can be legitimately outweighed by national security and public safety concerns. However, the safeguards in place and extent to which intelligence and law enforcement agencies can use their intrusive powers of investigation and surveillance may vary. In our digitalized society of overlapping and interconnected networks, the introduction of technological innovations into the market often occurs before corresponding domestic legislation can be adapted.

Case Study: Accusations of Unlawful Surveillance

In late May 2014, a former minister, who had recently been removed by the ruling coalition government, accused the prime minister of abuse of power, claiming that he and his family were targets of unlawful surveillance by security services. After ordering the Office of the National Security Service to immediately investigate the allegations, the President called a press conference revealing their findings that SOA was not involved in any way. Within a few days, the parliamentary intelligence oversight committee announced that it had received a formal complaint and would launch an official inquiry. The committee requested reports and organized visits to SOA, the police headquarters, and the OTC (a separate agency responsible for telecommunication interception). While visiting the OTC, in addition to checking if there was ever a wiretap targeting the former minister, several MPs used the occasion to check on several other cell phone numbers unrelated to the case. The media reported that one of those belonged to a local politician that was indeed under a separate, high-profile investigation. Another telephone number belonged to one of the committee members. In the media mayhem that followed, committee MPs accused each other of violating procedural standards. Eventually, the oversight committee concluded that they were not able to determine any abuses, although opposition MPs complained that they were not convinced enough to rule out 'foul play' of the police. Over a year later and after a change of government, an internal affairs police report was leaked to the media indicating that while the former minister was neither under surveillance nor had a wiretap on his telephone, he had been under criminal investigation. The report also confirmed that there was nothing unusual about the investigation.

Balancing privacy rights and effective intelligence capabilities

Access to vast stores of digital information and data retention, vital to security and law enforcement agencies' investigative work has been highly debated. Personal data protection and privacy concerns are high on the EU agenda. Sharing personal data, like the Passenger Name Record (PNR), so crucial when tracking the movement of terrorist suspects, had been stymied until a few years ago.[13] Ever since, the EU's commitment to secure the continent has led to harmonized enforcement legislation that takes into account data protection while making it easier for prosecutors, police and security services to collaborate in cross-border investigations in order to combat crime, terrorism and cyberattacks more effectively across the continent. Finding an appropriate balance between protecting individual privacy and assuring effective intelligence capabilities will be the object of many future disputes. Events will likely determine relative shifts in favor of one or the other.

Initiating public dialogue on the role and future of intelligence

An open and comprehensive public discussion on this balance and on the future of intelligence in general has yet to occur in Croatia. After a quarter of a century, we were still struggling to come to terms with communist-era and post-war legacies. Our polarized and highly charged political environment had little sympathy for an institution like SOA. I was convinced that it was time to cross some traditionally forbidden boundaries.

SOA published its first annual public report in 2014. At the time, while we knew we were entering uncharted territory, I am not sure that we fully realized all of the risks involved. Nevertheless, it was widely praised for its openness and for shedding light on a daunting subject matter. The report underscored that SOA is bound by clear legislative constraints as well as checked by executive, parliamentary, and civilian

13 The Council of the EU adopted the PNR directive in April 2016, allowing its member states a two-year period to comply and harmonize their domestic laws, regulations, and administrative provisions.

oversight. It also provided an unclassified security assessment and some fundamental information on developments within the service. SOA has continued to release an annual public report.[14]

In line with this new openness policy, documents belonging to the old Yugoslav secret service were declassified and sent to the National Archives in 2015. I am not sure why this step was not taken earlier. While this landmark event should serve to dispel skeptics, it will also surely benefit historians, journalists and academic researchers alike. It was also a symbolic gesture implicitly intended to reflect our new forward-looking approach. We expect it to help build confidence and address the public's legitimate desire for access to information.

SOA has also initiated dialogue with experts and civil society groups, a move recognized by EU institutions that promote fundamental rights and freedoms.[15] In 2014, SOA held its first of what would become an annual roundtable discussion with representatives of human rights groups and non-governmental organizations. While the first series of events, which I personally attended, were expectedly awkward, later meetings reflected a growing shared understanding of each actor's respective role. The results of this dialogue include increased transparency and more information on SOA's role in its annual public reports. Similar meetings have been held with the media, students, and expert groups. Such open and frank discussions have proven useful for all.

Looking Ahead: Understanding Our Security

I asked a senior operative, after an intelligence briefing, what we were looking to collect. This was in my early days at the agency. "Everything," was his response, "everything and anything we can get our hands on." That cannot be right I thought to myself. Surely, we did not have all the time in the world or unlimited resources to try to collect 'everything'. We would later encourage the National Security Council to adopt more prioritized intelligence guidance. The world around us was likely to become increasingly complicated, with vast amounts of irrelevant information and competing narratives inhibiting our analytical capacities. SOA's ability to provide clarity and understanding would be an invaluable contribution.

We are living through one of the most astonishing transformations of our understanding of security. From the Cold War uncertainties of a nuclear war to today's competing national interests and intricate arrays of transnational security challenges, I hesitate to suggest that the world is a safer place. Understanding the complexities of a collapsing, rules-based world order and making sense out of what is really going on is difficult even for the most astute analysts and pundits. We label threats as 'asymmetric' or 'hybrid' before we fully understand them and reach conclusions before we frame the problem. Unless time constraints require immediate action, taking the time to understand an issue is time well spent. The history books are full of intelligence blunders based on misperceptions, miscalculations, or misjudgments.

Assessing a nation's security is very serious business. There are many uncertainties and many ways to get it wrong. Giving in to our emotional sentiments or personal biases leads us to reach poor conclusions. Being egged on by higher authorities to reach skewed conclusions that support a predetermined storyline should be equally troubling. It is critically important to recognize these pitfalls.

Importance of getting our perceptions right

It all begins with, and very much depends on, our perceptions. Our intelligence experts scan our surroundings, interpret what is going on and assess the risks, threats, and challenges. Their perceptions matter. We rely on them to be knowledgeable, unbiased, and, above all, accurate. What we perceive to be threats to our national security, real or imaginary, will be real in our government's consequential actions and responses. Hence, our assumptions, calculations, and conclusions should always be subject to thorough scrutiny.

Our Agency is tasked with combatting terrorism, illicit trafficking (of migrants, weapons, and narcotics), corruption, transnational and complex criminal activity, radicalism, and extremism. Cyber threats, mass migration, and the proliferation of weapons of mass destruction, as well as concerns over our economic well-being, critical infrastructure protection, and energy security, also cram the growing list of tasks that our policymakers expect us to tackle. Of no less concern are the risks posed by hostile intelligence services

14 See https://www.soa.hr/en/documents/public-reports/.

15 See "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Mapping Member States' legal frameworks," FRA – European Union Agency for Fundamental Rights, 2015, p. 32.

involved in espionage. Increasingly, our adversaries are trying to steal classified information or industrial secrets or attempting to influence policy and public opinion in their favor. Some of these challenges can be quite contentious.

Croatia's Security and Intelligence agency (SOA)

- SOA's roots go back to the turbulent and violent break-up of Yugoslavia in the early 1990s, as intelligence played an important role in Croatia's war of independence (1991-1995).
- After several rounds of restructuring, SOA was established out of a 2006 merger of the Counterintelligence Agency (POA) and the Intelligence Agency (OA).
- Serving both foreign intelligence and domestic security purposes, it has its main headquarters in Zagreb, regional offices throughout the country, and stations abroad.
- SOA's mission is to "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." (Source: SOA)
- Its main tasks include countering terrorism and violent extremism, counterintelligence, tackling organized crime and corruption, cybersecurity, protecting classified information, performing security vettings, and collecting foreign intelligence.
- According to media reports, its personnel size is estimated to be between 900 and 1000 employees.
- SOA's 2020 budget is about 55 million Euros.

For more information, visit SOA's official website at https://www.soa.hr/en/about-us/.

When crime, corruption, and politics mix

Crime, corruption, and politics can be inextricably intertwined to create a formidable dilemma. The situation can be further complicated by the involvement of high-ranking politicians or influential individuals. While internal security services, as a general rule, should not run criminal investigations, there are exceptions when a situation poses a clear and pressing danger to the democratic order.[16] Such situations may not always be self-evident. Sometimes senior security officials are called upon to make difficult 'damned if you do, damned if you don't' decisions. On the other hand, security services can also easily stray off course and, before anyone realizes, suddenly find themselves in a compromising position.

Having a healthy understanding of security, clear intelligence guidance, and well-defined rules of engagement can help steer senior management in the right direction.

16 Parliamentary Assembly, Committee on Legal and Human Rights Report, Council of Europe, "Control of internal security services in Council of Europe member states," Document 8301, March 23, 1999.

Appreciating the inherent flexibility of national security

The notion of national security is so inherently flexible that, if stretched enough, it can easily conform to a self-serving narrative. In the past, secret services enjoyed widely unchecked powers. The Yugoslav secret service was notorious for recruiting criminals who have committed serious crimes to carry out their dirty work abroad. Dozens of dissidents and other enemies of the regime were murdered abroad by these hired thugs. Sometimes the assassinations were intentionally brutal and gruesome. Many of these criminal relationships remained intact well after the dissolution of the former Yugoslavia and the transition to democracy. Illicit smuggling, questionable business deals, rigged public tenders and corrupt privatization schemes often occurred under the protection and watchful eyes of the secret services.

The problem can become even more acute in cases of systemic corruption and 'state capture'. Crime, corruption, politics, and the secret services become practically indistinguishable. In such instances, it takes extraordinary effort to restore order and the rule of law.

Protecting our new vulnerabilities

The interplay of technological innovations and social networking require particular attention. Navigating through an era of 'post truths', 'fake news' and 'information warfare' will not be easy. More than ever, we will have to ask ourselves if we have the right skill sets.

Technological developments have fast-forwarded our societies into an uncharted and largely unregulated territory of dynamic new opportunities and vulnerabilities. Our citizens' private lives, our economies, and our essential services, whether finance, health, energy, or transport, all increasingly depend on digital information and communication technologies. It has fundamentally altered our society, from the way that we do business to the way that we interact with one another. Those with adversarial intentions increasingly find it easier to disrupt our way of life. A simple cyber-attack on providers of public or commercial services can result in dangerous and disruptive consequences ranging from public disturbance to serious economic damage and can even put lives at risk.

As a domain gradually taking center stage, cyberspace is now firmly in the crosshairs of law enforcement and intelligence agencies. With its inherent complexities and ambiguities, cybersecurity will surely dominate our agenda, consume our resources, and generate new controversies. We cannot afford to be caught off guard.

Non-traditional challenges and complex phenomenon

If that were not enough to worry us, what role, if any, will security and intelligence services play as our societies increasingly face the risks of infectious diseases (pandemics), climate change, environmental degradation, and other complex phenomena? We cannot simply dismiss such challenges. While they fall outside of our traditional purview, these risks are part of a wider security context and bring serious political, social, and economic consequences. Disregard for such phenomena risks pushing intelligence towards irrelevance. Security services that ignore these challenges, without seeking to acquire at least a basic understanding of them, do so at their own peril.

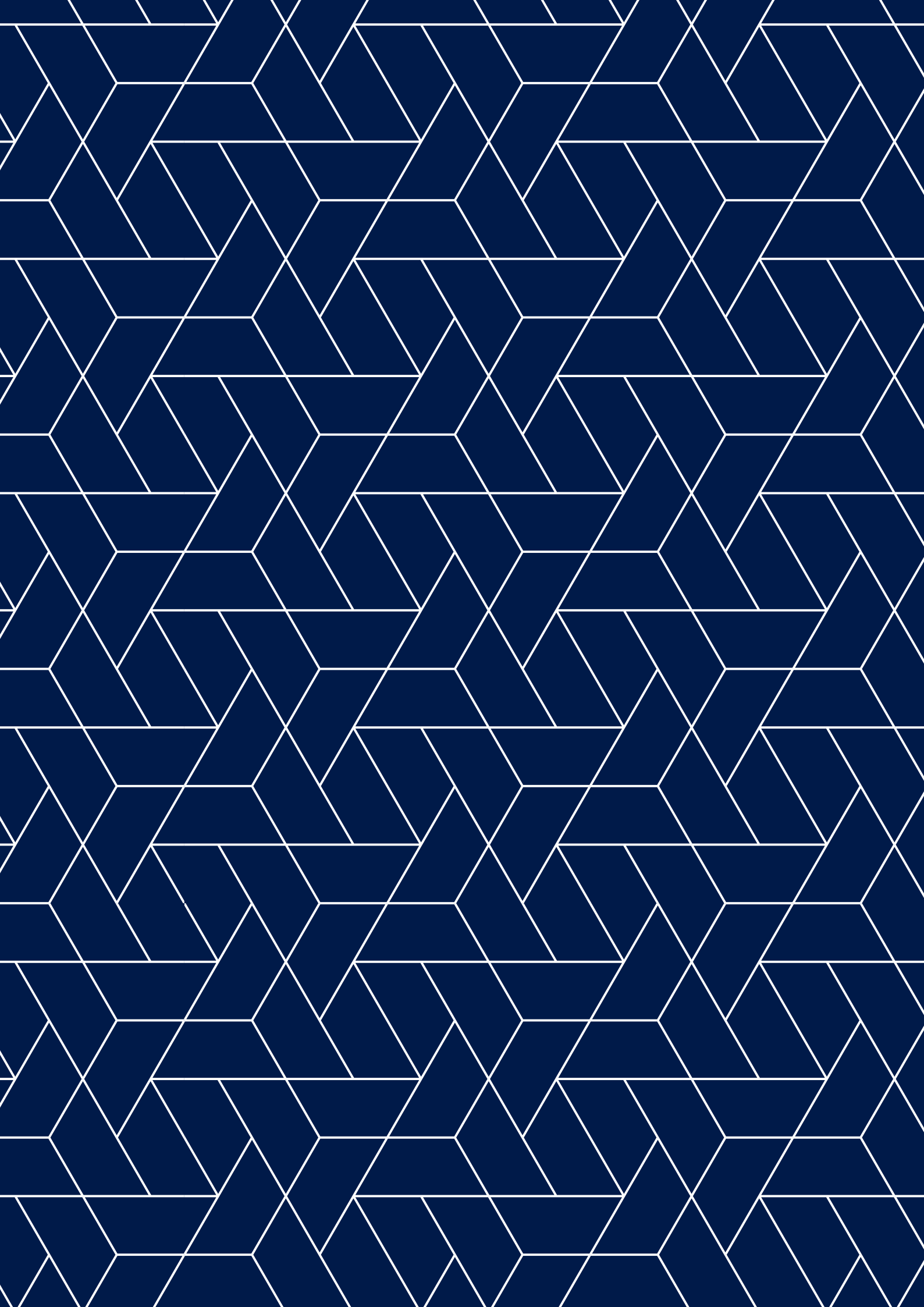
Conclusions

The countries of Eastern Europe, from the Baltics to the Balkans, as well as the countries of the former Soviet Union, have haphazardly faced the prospects of intelligence reforms in their democratic transitions. Many, like Croatia, have struggled well after the end of the Cold War. Yet, each is in a unique position to shape the extent and dynamics of its intelligence reforms. And there is no guarantee that this will be a pleasant or risk-free venture. Each has to come to terms with its past, meet its current demands, manage its expectations, and embrace its future potential. In the meantime, the world is constantly changing, as old assumptions prove unreliable and new challenges emerge. It can be a delicate balancing act requiring significant political will and commitment.

Croatia's experience offers some important insights and lessons. Intelligence reforms are continuous and require long-term efforts. Moreover, a reliable measurement of effective governance is the test of time. In practice, parliamentary oversight has yet to rid itself of partisan politics. Croatia's desire to join NATO and the EU provided a strong incentive to instill value-based principles shared by Western democracies. Along the way, we quickly realized the benefits of accountability, oversight, and safeguards against abuse. Specifically, SOA's capabilities have improved, self-confidence among its ranks has increased, and public support has grown. The publication of its first unclassified report resulted in a remarkable increase in SOA employment applications. Here was proof that adopting good governance principles translates into capacity building.

There is also a strategic, and perhaps entrepreneurial, aspect to SOA's transformation. It has adopted a corporate mindset in its approach to public service. The Agency has undertaken a self-assessment as a basis for its strategic development, not exactly a trivial endeavor for an intelligence organization. SOA received unanimous cross-party praise for its strategic development plan in the parliamentary intelligence oversight committee. The Agency is better able to recognize emerging threats in a timely manner, and plays a leading role in our national cybersecurity efforts. But, as proudly showcased in its 2019 public report, SOA's most impressive achievement is its continued commitment (since 2012) to annually increasing investments in modernization and development.

SOA's reforms have gone hand in hand with Croatia's democratic transition and Euro-Atlantic integration. The agency's membership and active role in key international fora, as well as its close cooperation with security and intelligence services of like-minded Western democracies, provides it with amplified opportunities to effectively accomplish its mission. It also attests to SOA's notable decades-long progress. With a maturing oversight capacity and greater transparency, SOA is better placed to develop the capabilities needed to address the future security challenges it will face.



DCAF Geneva Centre for Security Sector Governance

20TH ANNIVERSARY

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva