

# CONNECTIONS

---

## THE QUARTERLY JOURNAL

CONNECTIONS SPECIAL ISSUE



PARTNERSHIP FOR  
PEACE CONSORTIUM  
OF DEFENSE  
ACADEMIES AND  
SECURITY STUDIES  
INSTITUTES

WINTER 2021

# TRANSFORMING INTELLIGENCE SERVICES

---

EDITORS:  
AIDA ALYMBAEVA AND PHILIPP FLURI

# *Partnership for Peace Consortium of Defense Academies and Security Studies Institutes*

## **The PfP Consortium Editorial Board**

Sean S. Costigan	Editor-In-Chief
Torsten Stauffer	Managing Editor
Aida Alymbaeva	International University of Central Asia, Bishkek
Pal Dunay	George C. Marshall Center, Garmisch-Partenkirchen
Philipp Flury	Geneva Centre for Security Policy, Geneva
Piotr Gawliczek	Cuiavian University in Wloclawek, Poland
Hans-Joachim Giessmann	Berghof Foundation, Berlin
Dinos Kerigan-Kyrou	Joint Command & Staff Course, Military College, Irish Defence Forces
Chris Pallaris	i-intelligence GmbH, Zurich
Tamara Pataraiia	Civil Council of Defense and Security, Georgia
Todor Tagarev	Bulgarian Academy of Sciences, Sofia
Eneken Tikk	Cyber Policy Institute, Jyväskylä

The views expressed and articles appearing in all *Connections* publications are solely those of the contributing authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

This edition is supported by the United States government. The Consortium's family of publications is available at no cost at <http://www.connections-qj.org>. If you would like to order printed copies for your library, or if you have questions regarding the Consortium's publications, please contact the PfPC at:  
[PfPCpublications2@marshallcenter.org](mailto:PfPCpublications2@marshallcenter.org).

Dr. Raphael Perl  
Executive Director

Sean S. Costigan  
Editor-In-Chief and Chair, Editorial Board



ISSN 1812-1098, e-ISSN 1812-2973

# CONNECTIONS

## THE QUARTERLY JOURNAL

**Vol. 20, no. 1, Winter 2021**





## Contents

### Vol. 20, no. 1, Winter 2021

#### Editorial

- Lessons from the Post-Totalitarian Transformation of Intelligence Services 5  
*Aida Alymbaeva and Philipp H. Fluri*

#### Research Articles

- Transformation of State Security and Intelligence Services in Poland – A Job Still Unfinished 9  
*Agnieszka Gogolewska*
- Lessons Learned from Military Intelligence Services Reform in Hungary 33  
*Andras Hugyik*
- Intelligence and Security Services Reform and Oversight in Ukraine – An Interim Report 51  
*Philipp Fluri and Leonid Polyakov*
- Infogate Influences on Reforms of South Africa’s Intelligence Services 61  
*Glen Segell*
- Indonesian Intelligence Reform: Recent Challenges and Opportunities for Encouraging Democratic and Professional Intelligence 75  
*Mufti Makarim A.*

## Table of Contents

Governance Challenges of Transformative Technologies	91
<i>Marina Caparini and Agnieszka Gogolewska</i>	



## **Lessons from the Post-Totalitarian Transformation of Intelligence Services**

***Aida Alymbaeva and Philipp H. Fluri***

The reform of intelligence and state security services in the ‘new’ democracies that emerged since the end of the Cold War has remained under-documented and under-analyzed for a long time. This is especially true for smaller countries. Whereas this fact certainly can be explained with the sensitive nature of the business, the lack of data resulted in important lacunae for understanding these services, and obviously also for lessons to be drawn from the transformation processes. This special issue of *Connections* intends to fill some of the gaps. The editors are delighted to present studies on transformation processes in the structures, legislation, management, and oversight of intelligence and state security services in Hungary, Indonesia, Poland, the South African Republic, and Ukraine.<sup>1</sup>

Various contributors felt encouraged to share data and analysis on ongoing processes of intelligence reform and the evolution of surveillance. Whereas the security of states and alliances remains the main challenge for the established services in democratic states, surveillance technologies have been developed and deployed for business and private use. The dimensions and importance of such commercial surveillance programs do not seem to be sufficiently understood, and therefore remain unrestrained by national legislation and governmental oversight. This collection also presents forward-looking analysis on possible consequences and governance challenges of pandemic surveillance and “surveillance capitalism.”

---

<sup>1</sup> Three early contributions, respectively on the post-Cold war intelligence reforms in the Czech Republic, the Slovak Republic, and Latvia, were published in the Summer-Fall 2019 edition of *Connections: The Quarterly Journal*, <https://doi.org/10.11610/Connections.18.3-4>.

Authors offer their views on lessons to be learned in transforming and reforming intelligence services in their respective countries. One of the common features they underline is the delegation of police functions to intelligence services, leading to overlapping mandates with other security agencies. This situation is typical for the post-communist countries (e.g., Poland and Ukraine), where mandated tasks of intelligence agencies have included investigation and pre-trial functions. Authors draw attention to the fact that multi-tasking is heavily influenced by the lingering Soviet legacy when these countries failed to fully overcome it. The cases in this issue show intelligence sector transformations as results of traumatic catalysts rather than gradual evolution. Authors recommend acting decisively and rapidly in such cases. They also argue that unless there is a specific necessity, the reform of the sector is not going to happen quickly.

Weak civilian control is pervasive in the area discussed, along with poor parliamentary control and a dearth of citizens' watchdogs. In addition, limited or non-existent judicial oversight of intelligence agencies is regarded by contributors as a significant shortcoming. They underline that accountability and effectiveness of intelligence services remain limited, as is the public trust. While national legislation on civilian oversight is nominally in place, civilian control is hampered by the dominance of presidents over legislatures and the politicization of the intelligence sector (e.g., the articles on Indonesia and Ukraine), the inadequate capacity of parliamentarians and parliamentary staffers, and insufficient pressure from civil society. In addition, judicial control is only vaguely articulated in national regulatory frameworks.

Another challenge outlined by the authors is the disproportionate use of intelligence and surveillance methods by governments to combat the global COVID-19 pandemic. The powers of intelligence services have been extended for mass surveillance in many countries. Yet, as the authors note, the weakness of civilian control could induce the services to continue using this extended power in the post-Covid situation. This may seriously infringe on the privacy rights of citizens, as proposed in some papers. Moreover, contributors alarm that regulatory activities of many countries, including the EU, in the realm of Artificial Intelligence do not match the pace of development of these technologies. Authors call for immediate actions of governments in this domain.

As a whole, this issue represents a collection of papers featuring these and other setbacks of intelligence sector transformation in different countries and regions. Progress of reforming intelligence services is also highlighted.

The editors are convinced that this special issue will help to fill important gaps in the discussion of intelligence services transformation and oversight.



## **Disclaimer**

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

## **About the Authors**

**Aida Alymbaeva** is Director of the Center for Social Innovation and Development in Bishkek, Kyrgyzstan, and Lecturer at the International University of Central Asia. Aida is an experienced researcher and consultant with a demonstrated history of working in the management consulting industry. Skilled in research, policy analysis, and project management, she holds a Master of Science degree in Public Policy Analysis from the Rochester Institute of Technology.

*E-mail:* aidarochester@gmail.com

Dr. **Philipp H. Fluri** was a co-founder and long-time deputy director of the Geneva Centre for Security Sector Governance (DCAF; earlier Geneva Centre for the Democratic Control of Armed Forces) and the founder and executive director of DCAF Brussels. He was subsequently an Executive-in-Residence at the Geneva Centre of Security Policy and the Sergio de Mello Chair at the Seton Hall University School of Diplomacy and International Relations. He is currently a professor in the Department of International Affairs at the Wenzao Ursuline University (WZU) in Kaohsiung, Taiwan.

*E-mail:* drphilippfluri@gmail.com





Research Article

## Transformation of State Security and Intelligence Services in Poland – A Job Still Unfinished

*Agnieszka Gogolewska*

*European University of Information Technology and Economics In Warsaw,  
<http://www.eu.edu.pl/>*

**Abstract:** Since 1989, the Polish intelligence sector has been undergoing a democratic transformation which has turned into a continuous institutional change. In the process, the old communist services were abolished and new ones established in parallel with setting up executive and legislative oversight structures. But while the intelligence institutions and the oversight structures, on the whole, meet democratic standards and do not appear to threaten the constitutional system or citizens' rights in any systemic way, the more recent developments in the sector demonstrate that democracy in Poland has not in fact been consolidated. The state proved incapable of forming any dependable and effective model of control over the security sector in the sense of exercising both political guidance and democratic oversight. The intelligence services and some security institutions continue to enhance their prerogatives in the realm of covert operations, democratic control mechanisms are not sufficiently effective, and the issues of the communist past continue to be a disruptive factor. Under the circumstances, it is hard to single out good practices; rather, one should speak of lessons learned.

**Keywords:** intelligence oversight, judicial control, civil watchdogs, post-communist transition, transformation, Poland.

### The Lonesome Transformation in Poland

After the fall of communist systems in 1989-1990, the reforms of civilian and military security services in the emerging democracies of Central Eastern Europe were imminent. Introducing democratic control was one of the most significant transformation challenges, not the least because the very concept was unfamiliar to politicians and political scientists alike. But while there was abundant liter-

ature on the theory and practice of past democratic transformations of civil-military relations, the theory of security sector reform was just emerging, and the post-communist transitions turned to be its main testing ground.

In Poland, the post-1989 democratic reforms of the military enjoyed strong external institutional and financial support: lectures by prominent politicians and academics visiting the country, foreign fellowships available to Poles, and networking activities available and funded within the framework of Partnership for Peace throughout the 1990s. Above all, the reforms supported the ultimate political goal—full-fledged membership of Poland in NATO—and the democratic control over armed forces was a *sine qua non*.

No such backing was available to the reformers of post-communist security and intelligence services. The history of security sector reforms could not provide much background knowledge or tools for introducing intelligence oversight. There was no external, NATO-like institution that could propel reforms in anticipation of future political gains. Moreover, the security services had traditionally been the mainstays of communist power, enveloped deep in secrecy and notorious for oppressing opposition activists. More importantly, the fall of communist systems did not immediately lead to the collapse of those secret structures in Poland, nor did it instantly cut off the functionaries from their covert resources. Hence the incumbent democratic governments, still weak and besieged by political and economic problems, were reluctant to move in aggressively and to formally abolish the communist security services in their entirety, fearing possible consequences. The approach to the security sector was initially lenient and took place in several small steps, thus involuntarily laying the foundations for a number of future problems. This cautious approach might have also contributed to the lack of clarity in the institutional design of the sector and power overlaps characterizing the post-communist security and intelligence services in Poland.

## Conceptual Problems

Conventionally, there is a clear distinction between intelligence-gathering responsibilities, typical of intelligence services, and policing/ law enforcement functions, characteristic for the police, border guards, and customs. This distinction is reflected in the literature on the subject, for example, the toolkit for intelligence oversight published by DCAF.<sup>1</sup> Unfortunately, the Polish civilian services have never even come close to such a clear-cut division of tasks. Despite several conceptual and legislative attempts to clarify the division, the post-communist intelligence services have never let go of their policing and law enforcement prerogatives. Many experts have criticized the lack of clarity in this respect

---

<sup>1</sup> Hans Born and Gabriel Geisler Mesevage, "Introducing Intelligence Oversight," Tool 1 in *Overseeing Intelligence Services. A Toolkit*, ed. Hans Born and Aidan Wills (Geneva: DCAF, 2012), [https://www.dcaf.ch/sites/default/files/publications/documents/Born\\_Wills\\_Intelligence\\_oversight\\_TK\\_EN\\_0.pdf](https://www.dcaf.ch/sites/default/files/publications/documents/Born_Wills_Intelligence_oversight_TK_EN_0.pdf).

over the years. Both functionaries<sup>2</sup> and academic researchers<sup>3</sup> have stressed overlaps of tasks and powers between the security and intelligence services and pointed to the purely arbitrary distinction drawn between them, lacking conceptual premises.

The duty to gather, analyze and share intelligence is not a distinctive feature of the intelligence sector in Poland since similar duties are performed by several other security institutions in their respective fields. Law enforcement duties cannot be treated as an indicator of the type of service either due to the overlaps and similarities between security and intelligence services. The same is true for the right to carry out covert and intrusive surveillance operations vested in several agencies in Poland.<sup>4</sup> So the fact that any given agency is authorized to interfere covertly with private property or use intrusive surveillance techniques does not place this agency in the intelligence sector in Poland.

Since the conceptual lines of division are so blurred, the only way to identify and delineate the intelligence sector is by following the practical approach taken by the executive authorities and reflected in the wording of the laws, both existing and projected. The laws point to five currently existing services as the so-called “special services,” i.e., representing the intelligence sector. These are:

1. Internal Security Agency, in Polish *Agencja Bezpieczeństwa Wewnętrznego*, ABW, i.e., civilian counterintelligence;
2. Foreign Intelligence Agency, in Polish *Agencja Wywiadu*, AW, responsible for the information gathering abroad;
3. Central Anticorruption Bureau, in Polish *Centralne Biuro Antykorupcyjne*, CBA, the main organ for monitoring the implementation and effectiveness of countercorruption regulations and investigating breaches of legal provisions in that respect, mostly (but not exclusively) concerning companies and public entities or state functionaries;

---

<sup>2</sup> See the interview with the former functionary of the Internal Security Service ABW and former Head of Foreign Intelligence Service AW, Col. Grzegorz Małecki at <http://www.defence24.pl/plk-grzegorz-malecki-panstwo-musi-byc-swiadome-roli-i-istoty-swoich-sluzb-wywiadowczych-wywiad>. He voiced similar concerns about the lack of clarity in the functions of the Polish intelligence services in conversations with the author.

<sup>3</sup> Among the academics, the most notable right-wing analyst of security and intelligence sector reform is professor Andrzej Zybertowicz from Toruń University. He published numerous articles and books on the transformation, mostly critical of the conceptual approach to the reforms. See, i.e. “Chory rdzeń państwa” (“The Sick Core of the State”), interview with prof. Andrzej Zybertowicz, *Rzeczpospolita daily*, April 26, 2004.

<sup>4</sup> Beyond the intelligence sector, the power to use covert surveillance techniques has been vested in several other security services in Poland: Police, including Central Investigative Bureau, Border Guards, Customs Services, Military Police and Treasury Intelligence, each in its respective field. The last of these is subordinated to the Ministry of Finance and criticized by some for its very extensive covert competencies. Despite this fact and the very name implying the function of intelligence gathering, the service is not considered as part of the intelligence sector.

4. Military Counterintelligence Service, in Polish *Służba Kontrwywiadu Wojskowego, SKW*, responsible for counterintelligence in Poland and protection of military operations abroad;
5. Military Intelligence Service, in Polish *Służba Kontrwywiadu Wojskowego, SWW*, in charge of military intelligence and covert operations abroad.

## Security and Intelligence Sector under the Communist Regime

In terms of institutional design, the security and intelligence sector in the final stage of the communist regime in Poland was relatively simple. The civilian part was composed of the main police force called People's Militia (*Milicja Obywatelska, MO*), the intelligence service called Security Service (*Służba Bezpieczeństwa, SB*) and several minor police-like formations with anti-riot functions. Legally, all those services were covered by one bill<sup>5</sup> and were subordinated to the Minister of Interior. However, the real subordination was along political lines, as the Minister of Interior was always a high-ranking member of the Central Committee of the Communist Party. In the late 1980s, the Security Service (*SB*) numbered 24.3 thousand functionaries and had over 90 000 agents registered as secret operatives. *SB* was tasked with safeguarding the internal and external security of the state; however, the term 'security' was mainly understood in terms of political compliance. Therefore, the Service was primarily engaged in surveillance of the political opposition both in Poland and abroad.

Regarding the military sector, the post-WW2 military intelligence was organized into separate structures within the MoD. Before 1990, by order of the Minister of National Defense of November 15, 1951, the military intelligence was embedded in the Ministry of National Defense structures as the Second Directorate of the General Staff of the Armed Forces, subordinated to the Minister. Military intelligence officers were part of the repressive political apparatus of the communist regime. However, their focus was more abroad, especially concerning the Vatican policies and opposition emigrants in Europe. Additionally, military intelligence was a statutory intermediary in the Polish foreign arms trade and controlled the state-owned company CENZIN, tasked with the sales of armaments. It was a highly profitable source of operational funds and one that often bordered on criminal activity. Additionally, military intelligence operatives were often placed in management positions in Polish foreign trade companies, which resulted in several criminal affairs in the later period of transformation.

From 1957 until 1990, counterintelligence was embedded in the Ministry as the Military Internal Service, responsible for counterintelligence but also for political compliance of the military and hence was much despised by the members of the Armed Forces at large. There was no separate legal bill to regulate its func-

---

<sup>5</sup> Ustawa z 31 lipca 1985 r. o służbie funkcjonariuszy Służby Bezpieczeństwa i Milicji Obywatelskiej Polskiej Rzeczypospolitej Ludowej.

tioning; instead, their structures and functions were regulated by the minister's internal orders.<sup>6</sup>

## **Transformation of the Civilian Intelligence Services**

Reforms of civilian and military intelligence services in post-communist Poland did not follow the same paths. In the civilian sector, the old communist Security Service *SB* managed to survive the first (partially) free elections of June 4, 1989, and the inception of the non-communist government. Former members of the opposition were dragging their feet in taking over the Ministry of Internal Affairs. Initially, the Ministry of Internal Affairs remained within the purview of the high-ranking communist regime representative, General Czesław Kiszczak, and his officers, while the security service *SB* continued to function largely unhindered. Consequently, the first reorganization of communist security services was introduced by the very communist general and mainly served to facilitate the process of concealing the crimes and abuses of the communist service from the new government. The first non-communist Deputy Minister of Internal Affairs, Krzysztof Kozłowski, was appointed on March 7, 1990. Ultimately, the last communist representatives left the government in July 1990. Only then the opposition really took over internal affairs and initiated the post-communist transformation in the civilian security sector. Unfortunately, the timespan between the creation of the non-communist government in the autumn of 1989 and the takeover of the internal affairs in March 1990 gave the communist functionaries plenty of time to destroy or remove to private lockers a considerable part of the archives. It was a reason why many former opposition activists claimed that the communist security services were offered impunity which became a source of many political troubles in the years to come.

At the outset of reforms, there were plans to establish a parliamentary commission to investigate the communist Security Service crimes and make them known to the public. Such an extraordinary parliamentary commission was set up early on after the free elections of June 1989, perhaps too early, because it failed to deliver substantial results.

### ***Milestone # 1: Bill of April 6, 1990, Creating the First Post-communist Civilian Intelligence Service***

On April 6, 1990, the parliament adopted a ground-breaking set of reforms initiating the democratic transition of the civilian security sector. The package included the following acts:

- Bill on the Post of the Minister of Internal Affairs;
- Bill on the Police;

---

<sup>6</sup> Jan Bodakowski, "Służby specjalne (wywiad, kontrwywiad, безпеka) PRL," *Salon 24*, October 5, 2010, <https://www.salon24.pl/u/jan-bodakowski/235906,sluzby-specjalne-wywiad-kontrwywiad-bezpieka-prl>.

- Bill on the Office for State Protection, in Polish *Urząd Ochrony Państwa*, UOP.

Based on art. 131 of the Bill on the Creation of the State Protection Office UOP,<sup>7</sup> the old Security Service SB was formally abolished, and all former functionaries were discharged from service. Subsequently, based on Resolution # 69 of the Council of Ministers (government) of May 21, 1990, the former members of the communist services *could* apply for work in the newly created Office for State Protection UOP or the new Police, pending a positive outcome of the vetting process by the special governmental commission.<sup>8</sup> The process is commonly known as “the verification of the functionaries of the Security Service SB.” All former officers were given the application forms and had to submit their applications until July 4, 1990. Only officers under 55 were eligible to apply; anybody over 55 was automatically retired. The same verification procedure was mandatory for the candidates to the Office for State Protection and the Police. It was a matter of an individual decision whether the candidate applied. The commission declined applications in cases when an officer was suspected of brutal surveillance and persecution of former opposition activists, a member of the senior leadership of the Security Service before 1989, or known for alcohol abuse. Anybody who was disqualified could first appeal to the same regional commission that took the original decision and then to the Central Vetting Commission. The subsequent decision of the latter was final and binding.

The verification was conducted in July and August 1990. 14,5 thousand former functionaries of the communist Security Service SB submitted their applications and underwent the vetting procedure. This number amounted to approximately 60% of the former staff of the communist service. Of those, 10,439 people were assessed positively. It is worth noting that only 8,681 officers were positively appraised at the first round of verification; the remaining staff was qualified as a result of their successful appeal. Importantly, a positive decision of the commission did not equal automatic acceptance in any of the new services. The ultimate decision was to be taken by the respective regional commanders of the Police and the Chief of UOP.<sup>9</sup>

As consequent events demonstrated, many of those officers should not have been positively appraised. The rather weak hold of the former opposition on the Ministry of Interior, their limited knowledge of the field or the archives, and the haste could all account for the imperfect vetting process. Therefore, it is not sur-

<sup>7</sup> Ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa.

<sup>8</sup> Resolution No. 69 of the Council of Ministers of 21 May 1990 on the procedures and conditions for the admission of former Security Service officers to serve in the Office of State Protection and other organizational units subordinate to the Minister of Interior and to employ them in the Ministry of the Interior.

<sup>9</sup> Rafał Leskiewicz, “Formalno-prawne aspekty powstania Urzędu Ochrony Państwa,” in *Urząd Ochrony Państwa 1990-2002* (Warszawa: Agencja Bezpieczeństwa Wewnętrznego, 2015), 53-79.



prising that the process was criticized as insufficient in delivering justice.<sup>10</sup> The acceptance of so many former regime officers into the new service was also the primary source of distrust that many former opposition activists demonstrated towards the post-communist intelligence sector, although often the accusations were not supported by documentation.<sup>11</sup>

### **The First Postcommunist Intelligence Service UOP, 1990-1996**

The new Office for State Protection *UOP* was formed within three months following the passing of the founding Bill of April 6, 1990. By the decision of the Minister of Internal Affairs, UOP initially numbered 5,522 officers, organized in one central structure in Warsaw and 14 regional offices. The Office for State Protection was subordinate directly to the Minister of Internal Affairs and was on a par with other security services, such as the Police, Border Guards, Firefighters, or Office for Government Protection. It was a two-in-one structure – UOP was responsible for intelligence and counterintelligence functions, and the division of duties was purely internal. The Chief of Service was appointed by the Prime Minister upon the motion of the Minister of Internal Affairs and following the positive opinion from the Political Advisory Committee to the Minister of Interior. Effectively, the Chief of UOP was one of the closest collaborators of the Minister, and any vital information would be passed on via the Minister to the Prime Minister and elsewhere.

The Bill of April 6, 1990, defined the scope of duties of the new intelligence service in a rather traditional way, protecting state security and the constitutional order. More specifically, UOP was responsible for:

- surveillance and monitoring of threats to national security, defense, sovereignty, integrity, and international position of the state;
- preventing and detecting crimes of espionage and terrorism and other crimes against the state security as well as prosecuting the perpetrators;
- protection of classified information, monitoring as well as preventing any breaches of such information;
- gathering intelligence and preparing analyses essential for national security and sharing information with the highest state authorities and the central administration.<sup>12</sup>

---

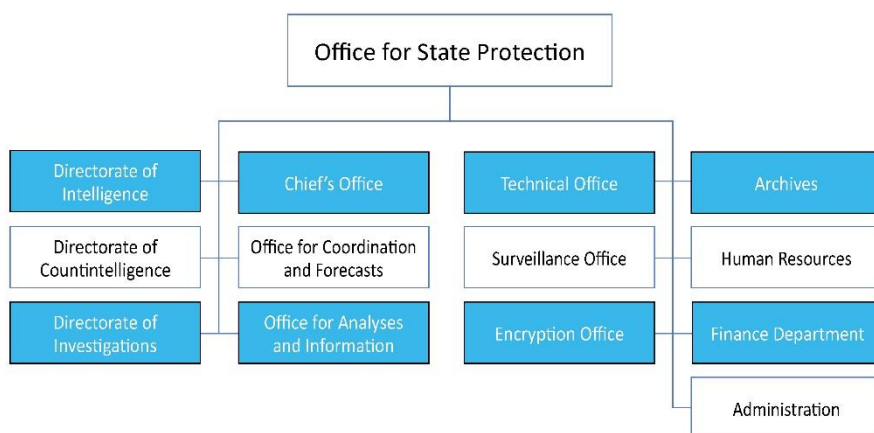
<sup>10</sup> Antoni Dudek, *Reglamentowana Rewolucja. Rozkład Dyktatury Komunistycznej w Polsce 1988-1990* (Warszawa, 2009).

<sup>11</sup> See Andrzej Zybortowicz, *W Uścisku Tajnych Służb. Upadek Komunizmu i Układ Postnomenklaturowy* (Warszawa, 1993).

<sup>12</sup> Zarządzenie nr. 39 prezesa Rady Ministrów z dnia 4 lipca 1990 roku w sprawie szczegółowego określenia zadań oraz struktury organizacyjnej Urzędu Ochrony Państwa, in *Historyczno-prawna Analiza Struktur Organów Bezpieczeństwa Państwa w Polsce Ludowej (1944-1990)*. Zbiór studiów, ed. A. Jusupović and R. Leśkiewicz (Warszawa, 2013), 305-307.

The first intelligence service in democratic Poland can be defined as essentially a counterintelligence service with a mixture of intelligence gathering and policing functions, working in new structures but banking on knowledge and, to a degree, on procedures derived from the old communist service.<sup>13</sup> The founders of the democratic intelligence service lacked the knowledge or experience to propagate intelligence-gathering missions or even to aptly use and share the acquired intelligence.<sup>14</sup> Article 11 of the Bill on *UOP* only stated that the Office is under obligation to inform the Prime Minister and the Minister of Internal Affairs about any issues *essential to the security of the state*.

Figure 1 presents the structure of the central Office for State Protection in the years 1990-1996.



**Figure 1: Structure of the Central Office for State Protection, 1990-1996.**

### ***Milestone # 2: Reorganization of the Office for State Protection, 1996. Nascent Executive Oversight of the Intelligence Service***

In 1996 came the first democratic reform of the security sector in post-communist Poland. The reform was the corollary of the changing security situation both in Poland and in the region. With the fall of the last communist regimes in Central and Eastern Europe and the onset of technological revolution came the era of organized crime transcending borders and challenging traditional security structures. Another incentive for the change was purely internal. It concerned the growing power of the Ministry of Internal Affairs, which was quickly becoming

<sup>13</sup> See Andrzej Misiuk, "Cywilne Służby Specjalne w Polsce po 1989 r. Próba Refleksji," in *Urząd Ochrony Państwa*, 41-50.

<sup>14</sup> In some private interviews, former UOP officers remembered the cases when the government politicians demanded that the cases of theft of expensive alcohol from their studies be investigated, insisting that it falls within the purview of special services.

ing a supreme security institution with the powers of control over all the law enforcement, police, and intelligence services and hardly controllable itself.

Based on those premises, the parliament introduced a package of legislative changes. Regarding the Office of State Protection *UOP*, three important changes were introduced.<sup>15</sup> First, its scope of duties and responsibilities was substantially amended. Secondly, the service became directly subordinated to the Prime Minister. The Chief of *UOP* was now accountable to the Prime Minister. Last but not least, to aid the supervisory function of the Prime Minister, a special advisory and consulting institution was established within the structure of the Prime Minister's Office, called "College for Intelligence and Security Services."<sup>16</sup> This was the first such institution dedicated to the oversight of the intelligence sector in Poland. Despite its inherent limitations and deeply political character, it contributed to the development of executive oversight practice in Poland.

In the aftermath of the legislative change, the responsibilities of the Office of State Protection shifted further away from classic intelligence-gathering towards investigative and counterterrorist functions, keeping intact the counterintelligence and classified information protection duties. A number of new investigative functions were added to the scope of duties of *UOP* in the field of economic crimes, adding to the already existing overlap between the Police, undergoing similar reforms at that time.<sup>17</sup> Namely, the reformed *UOP* was now responsible for:

- conducting reconnaissance and countering threats to national security, defense, sovereignty, integrity, and the international position of the state;
- preventing, countering, and disrupting acts of espionage and terrorism;
- preventing, detecting, and investigating economic crimes, including corruption, and prosecuting their perpetrators;
- conducting surveillance, investigating, and countering transnational crimes, including the illegal production, possession, and sale of weapons, ammunition and explosives, narcotics, psychotropic drugs, and nuclear and radioactive materials and prosecuting their perpetrators;
- protection of classified information, including encryption of classified and sensitive information, exchanged between governmental institutions;

---

<sup>15</sup> Ustawa z dnia 8 sierpnia 1996 r. o zmianie ustawy o Urzędzie Ochrony Państwa z 6 kwietnia 1990 r., Dz.U. 1996, No. 106, poz. 496.

<sup>16</sup> The exact translation of the name of the institution from Polish would be "College for Special Services." That corroborates all the terminology-related problems in defining the meaning of "security sector" in Poland. The services commonly called 'intelligence' in most democratic countries, in Poland acquired the name 'special,' initially by habit, only to be incorporated later in the language used in legislative acts.

<sup>17</sup> Misiuk, "Cywilne służby specjalne w Polsce," 46-47.

- information and analyses.

In the aftermath of the changes, the Office started to widely employ covert methods of surveillance, investigation, interception of communication, etc. Also, after 1996 UOP was undergoing constant internal structural changes.<sup>18</sup> The seemingly never-ending internal transformations were accompanied by personnel reassignments and relocations and were perceived by most intelligence officers as disruptive to professional conduct.

### ***Milestone # 3: Dissolution of the Office for State Protection UOP and Establishment of Separate Civilian Intelligence and Counterintelligence Agencies***

The last few years of the workings of the Office for State Protection were wrought with controversies and marked by increasing politicization of the service. The biggest scandal came at the end of 1995, when the then Chief of UOP, Andrzej Milczanowski, gave a speech at the Lower Chamber of the Parliament (Sejm) and publicly accused the Prime Minister in office, Mr. Józef Oleksy, of being the Russian spy nicknamed *Olin*. A huge political scandal followed, with Mr. Oleksy stepping down (though not immediately). Still, the Prime Minister denied being the spy and a subsequent investigation failed to produce unquestionable evidence of such activities.<sup>19</sup>

The Olin scandal instilled deep distrust of UOP in post-communist political forces. Another major reform of the intelligence sector followed the scandal. In 2001, the post-communist coalition won the election and formed a Government. Subsequently, on May 24, 2002, the parliament adopted the new Bill on the creation of the Internal Security Agency, *ABW* and the Intelligence Agency *AW*.<sup>20</sup> Thus, the Office for State Protection *UOP* was by a counterintelligence service (*ABW*) and the entirely new foreign intelligence service (*AW*). In theory, the goal was to separate counterintelligence and internal security duties from foreign intelligence. Hence *ABW* was to be the main institution responsible for the protection of the internal security and constitutional order in Poland. Its range of activities was very similar to that of its predecessor UOP:

- protection of national integrity, sovereignty, and independence, and countering threats to national defense;
- detection, surveillance, and countering the threats of espionage and terrorism;
- detection, reconnaissance, and countering economic crimes;

<sup>18</sup> The series of internal structural transformations were introduced by the resolutions of the Prime Minister of December 6, 1996, August 19, 1998, May 12, 1999, and April 9, 2001. In 2002 the service was disbanded.

<sup>19</sup> "Wszystkie służby III RP. Od UOP przez WSI do ABW i SKW," [wiadomosci.dziennik.pl/polityka/artykuly/559825,sluzby-iii-rp-historia-powstanie-uop-abw-wsi.html](http://wiadomosci.dziennik.pl/polityka/artykuly/559825,sluzby-iii-rp-historia-powstanie-uop-abw-wsi.html).

<sup>20</sup> Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz.U. 2002 nr 74 poz. 676.

- surveillance and investigation of acts of corruption by public functionaries, posing a threat to national security;
- investigation and prevention of illegal sales of weapons and ammunition, the proliferation of WMD, drugs, and transnational crimes of similar nature;
- protection of classified information;
- gathering and analyzing information vital for protecting internal security and constitutional order and sharing it with relevant government institutions.

The new Intelligence Agency numbered 1,000 people and was designed as an intelligence service of a more traditional outlook, tasked with the protection of external security of the state and gathering, analyzing, and sharing intelligence with relevant institutions on issues essential to the national security and international position of Poland as well as its economic and defense potential. Further to this, the AW was responsible for:

- reconnaissance of external threats to the sovereignty, integrity, and security of the state;
- protection of diplomats, diplomatic institutions, and Polish representatives working abroad from the activities of foreign intelligence services;
- provision of encrypted communication between Polish diplomatic institutions abroad and relevant institutions in Poland;
- reconnaissance of international terrorism and transnational organized crime;
- reconnaissance and countering of illegal international sales of weapons, ammunition, WMD, drugs, etc.;
- gathering of intelligence on international hot spots, conflicts, and crises abroad that may affect national security;
- electronic counterintelligence.

Both newly created services were subordinated directly to the Prime Minister. However, the change aimed not only to reform the scope of duties and prerogatives of the civilian intelligence sector but, perhaps, and equally importantly, it was a political act of retaliation against the now-defunct UOP post-communist politicians perceived as inimical and prejudiced. Soon after the new Bill came in force, the newly appointed Chief of ABW, Andrzej Barcikowski, hastily discharged 420 former UOP officers.<sup>21</sup> The redundancies were mainly for political reasons.

The final act of the intelligence sector reform of 2002 took place four years later under the successor right-wing government with the creation of the third and so far last civilian intelligence service, the Central Anticorruption Bureau (in Polish, *Centralne Biuro Antykorupcyjne*, CBA). The law was adopted on June 9,

---

<sup>21</sup> "Porządki po Nowku," interview with Andrzej Barcikowski, *Trybuna*, July 2, 2002.

2006.<sup>22</sup> CBA is responsible for monitoring, surveillance, detection, investigation, and countering corruption and bribery among public functionaries (whose list has constantly been growing since then) and for investigating and countering economic crimes that may cause substantial financial loss to the State Treasury, local government budgets or public finances. In parallel, those duties were withdrawn from ABW, albeit not completely. CBA was created in a form resembling a police force, without the internal system of ranks typical for other services, with the police-like investigative and covert surveillance powers, and with the type of mission that would invite controversies in any democracy due to its potential edge against opposition parties. It numbers slightly over 800 functionaries, mostly deriving from the Police or investigative directorates of ABW.<sup>23</sup> Not surprisingly, it was not long before such controversial operations were made known to the public in the form of scandalous, covert operation against former President Aleksander Kwasniewski (unsuccessfully) aimed at detection of his secret funds, as well as arresting the opposition party local government politician Beata Sawicka who was later acquitted of charges by the court.

#### ***Prospective Milestone # 4: Projected Reform of the Civilian Intelligence Services Sector, 2018***

Despite seemingly never-ending reforms, politicians continue to express their dissatisfaction with the intelligence services in Poland. With the radical right-wing government now in power in Poland, the next round of reform was announced. The government adopted the project for an amended bill on ABW and AW to transform the sector again.<sup>24</sup>

Paradoxically, in organizational terms, the project partially puts the sector back into the 1990s, as it plans to subordinate the Internal Security Service ABW back to the Minister of Internal Affairs. The reform will also disrupt the institutional design of the intelligence sector as the Intelligence Agency AW will continue to be subordinated directly to the Prime Minister. It is not clear at the moment where the Central Anticorruption Bureau CBA would go. Furthermore, the College for Special and Intelligence Services will be abolished, and the new Committee of the Council of Ministers (i.e., the Government) for the Security of the State will be created to replace the College. It will have a similar composition and advisory role as the College; however, its controlling powers will be more limited.

Also, given the projected law, the overlap in the scope of duties of services will only grow. According to the project, ABW will be in charge of investigating financial/ corruption crimes exceeding 16 mln PLN (3.8 mln Euro). Effectively, CBA will be reduced to investigating lesser corruption and financial crimes, below

<sup>22</sup> Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym Dz. U. z dnia 23 czerwca 2006 r.

<sup>23</sup> See Marek Henzler, "Etaty i budżety służb specjalnych," <https://www.polityka.pl/tygodnikpolityka/kraj/1500287,1,etaty-i-budzety-sluzb-specjalnych.read>.

<sup>24</sup> See <https://mswia.gov.pl/pl/aktualnosci/11902,Rzad-przyjal-projekty-ustaw-o-ABW-i-AW.html>.

the 16 mln PLN threshold. Furthermore, ABW will be assigned to pursue the most serious economic crimes, acts of organized crime, illegal sales of drugs, weapons, and WMD proliferation. Those activities should be carried out in coordination with the Police and other security institutions. At the same time, lesser crimes in this domain will be passed over to CBA, the Police, and the remaining institutions of the security sector.

## **Transformation of the Military Intelligence Sector**

The reform of military services took a different path. The military counterintelligence structures were disbanded by the order of the Minister of National Defence on April 22, 1990. Based on the structures of the Second Directorate of General Staff and three directorates of the former Internal Military Service, the new military intelligence was formed, first in the form of a new Directorate of Intelligence and Counterintelligence embedded in the General Staff by the Order on July 27, 1990. Then, on July 22, 1991, the new Inspectorate of Military Intelligence Services was created. In terms of legal regulations, until August 2003, the Inspectorate was legally based on Article 15 of the amended Law on universal military service.<sup>25</sup> The Inspectorate was subordinated to the Minister of National Defense (except for the period 1994-1995, when it was under the Chief of the General Staff).

However, it was not until July 9, 2003, that the separate Bill on Military Intelligence Services<sup>26</sup> was adopted. According to the Bill, the Military Intelligence was responsible for tactical and reconnaissance operations that would provide intelligence on defense planning, the organization, armaments, and technology of foreign armies, as well as for the tasks in the field of military counterintelligence and the protection of classified information in international activities of the Polish Armed Forces.

The Military Intelligence Services (*Wojskowe Służby Informacyjne, WSI*) were strongly criticized because they never underwent any vetting procedures, even to the limited extent found in the civilian sector.<sup>27</sup> Instead, the Service was formed as a result of internal reorganization. But while it is true that military intelligence WSI did not experience any institutional verification of the personnel, certain informal, internal vetting procedures had been implemented during the first transformation of 1990. According to various sources,<sup>28</sup> around 1,000 officers were discharged from service or left voluntarily. This amounted to approximately 40% of the original personnel strength. Further, about 70% of the

---

<sup>25</sup> Ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej z 21 listopada 1967 (Dz.U. z 1992 nr 4 poz. 16 i Dz. U. z 1994 nr 43 poz. 165).

<sup>26</sup> Ustawa z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych, Dz.U. 2003 nr 139 poz. 1326

<sup>27</sup> Grzegorz Mafecki, "UOP na tle innych służb europejskich," in *Urząd Ochrony Państwa*, 104.

<sup>28</sup> Personal interviews of the author with former officers of the Military Intelligence.

former officers in commanding positions either left or were discharged even before the new military intelligence WSI was formed. Still, from the formal point of view, the post-communist service was essentially a simple continuation of the former communist service, burdened with either undesirable people or practices from the past.

The military intelligence was never fully trusted by the post-Solidarity governments, despite the apparent need for their professional involvement with the deployment of Polish troops in Iraq and Afghanistan. When the right-wing Government took office in 2005, the dissolution of WSI was imminent. The overwhelming majority of 367 MPs (out of 460) adopted the presidential legislative project to dissolve the existing Military Intelligence Services WSI and form two new services. Only 44 MPs from the post-communist party opposed the bill. The new law was adopted on June 9, 2006,<sup>29</sup> providing for:

- dissolution of the Military Intelligence Services WSI by September 30, 2006;
- creation of the Liquidation Committee led by the right-wing politician Antoni Macierewicz;
- formation of two new military services replacing WSI: Military Intelligence Service SWW and Military Counterintelligence Service SKW.

The professionalism of the new military services was often questioned as the recruitment was largely closed to any seasoned professionals. At the same time, in February 2007, the Liquidation Commission, headed by Macierewicz, published a report in which the former Military Intelligence Service WSI was declared a criminal organization, alienated from the intelligence sector, engaged in illegal operations, and evading civilian control. The report claimed that Russian agents saturated WSI throughout the 1990s, and the Polish military intelligence service was fully aware of the fact and tolerated the agents. The so-called *Macierewicz's second list* was subsequently made public and proved to be highly disruptive to Polish military intelligence. It revealed its structures and working methods and, worse still, published the non-verified and error-strewn list of secret agents of the communist military intelligence, many of them still active many years later. This action resulted in the weakening of Polish military intelligence for many years to come, libel suits from the unjustly accused (most won in courts), and, worst perhaps, dismantling the counterintelligence protection of Polish soldiers on missions in Iraq and Afghanistan.<sup>30</sup> The Minister of National Defense Radosław Sikorski initially demanded the instant dismissal of Antoni Macierewicz from his subsequent position of the Chief of Military Counterintelligence. When Prime Minister Jarosław Kaczyński refused, Sikorski himself resigned.

<sup>29</sup> Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Dz.U. 2006 nr 104 poz. 709.

<sup>30</sup> Łukasz Rogojasz, "Łukasz Rogojasz," *Newsweek*, Polish edition, November 9, 2015, <http://www.newsweek.pl/polska/antoni-macierewicz-raport-wsi-lista-macierewicza-specsluzby,artykuly,371988,1.html>.



## **Democratic Oversight of Intelligence Services**

As any nascent democracy, Poland experienced difficulties in establishing democratic oversight of the security sector. The oversight institutions have been established in Poland, but the control mechanisms have never been properly consolidated. On the contrary, since the transformation of 2002, the civilian intelligence sector has managed to increase its independence and decrease the degree of democratic oversight, among other things, taking full advantage of European antiterrorist directives but also fostering informal ties with political parties.

### ***Legislative Oversight***

The legislative oversight is carried out mainly by the Parliamentary Commission for Intelligence Services. Its composition and prerogatives are regulated by the Rules of Procedure of the Sejm<sup>31</sup> (lower chamber of the Polish parliament). The Commission's role is mainly to scrutinize the most important documents pertaining to intelligence sector institutions and their operations and give opinions. Among the documents, routinely scrutinized by the Commission, are projects of relevant legislative acts, guidelines for annual activities of the services prepared by the Prime Minister and Minister of Defense for civilian and military services respectively, annual plans of service activities and subsequent annual reports, and last but not least, projected state budgets in the part related to the intelligence and reports on the execution of those budgets. The Commission is also to be informed and consulted on candidatures for chiefs of the intelligence services and the deputies. It gives an opinion in the case of any planned dismissal. It merits a mention that while the issuance of the formal opinion from the Commission is a necessary condition for taking further steps in the legislative or executive processes pertaining to the intelligence organizations (approving laws, budgets, appointments, or dismissals), it is not, however, necessary to acquire a *positive* opinion from the parliamentary Commission for the legislature or the executive to go ahead with the scheme.

The Commission is entitled to demand complete information or relevant documents from the services, particularly if the MPs acquire information about possible irregularities in the service operations. There is a caveat here, however, which may hinder effective control. According to the Law on the protection of classified information, all the MPs (with the sole exception of chairpersons of both chambers of the parliament) have to obtain personal security clearances to gain access to classified information. The screening procedure is carried out and the clearances are issued (and possibly revoked) by the Internal Security Service ABW. The whole process of issuance is obscure, and the appeal procedure complicated (Prime Minister, then the courts), which leaves ABW an option to deny the clearance or revoke it if any MP is particularly 'difficult' from the point of view of the intelligence officers. There were such cases in the past concerning

---

<sup>31</sup> Załącznik do uchwały Sejmu RP z dnia 30 lipca 1992 r. – Regulamin Sejmu RP (tekst jednolity M.P. 2012 poz. 32 z późn. zm.)

opposition politicians. One such case involves Zbigniew Wasserman, who subsequently became Minister-Coordinator of Intelligence Services in 2005 but had been earlier denied security clearance while being a member of the parliamentary opposition.

Another potential impediment to effective legislative oversight is that the Commission always has a majority of governing party representatives. As a result, the MPs are usually reluctant to hold the executive branch to account and seldom issue controversial opinions. For example, the only registered activity of the Commission in 2018 was the positive opinion on dismissals of previous and appointments of new chiefs of intelligence services following the Prime Minister's decision to change the heads of services. The register of 2017 activities looks similar. Furthermore, the upcoming reform of civilian intelligence services planned by the present government was not discussed in the documents processed by the Commission. The Commission's activities are limited to statutory duties and respond to the demands of the executive, without playing any role in substantial monitoring of the operations of the services and striving to correct the system of oversight.

The weakness of the legislative oversight was vividly demonstrated in the dramatic events related to the 2007 botched *ABW* operation of arresting Barbara Blida, former minister of construction in the preceding government, suspected of corruption. The operation ended with Mrs. Blida committing suicide in the course of arrest by shooting herself in her own bathroom. Subsequent investigations by many institutions showed that the arrest was politically motivated and that the operation was ill-prepared, and the *ABW* officers did not follow the procedures. At the end of 2007, a special parliamentary investigative commission was created to investigate the case. Yet, despite the change of government in 2008 and three more years of existence, it never came to any substantial conclusions.<sup>32</sup>

### *Executive Oversight*

The executive leg of intelligence oversight is represented by the institution originally established in 2002. Its composition and rules of functioning were defined by the Resolution of the Prime Minister of July 2002.<sup>33</sup> Uncharacteristically for the Polish political scene, the College's institutional design was left largely intact until 2018, when the Government revealed plans for its abolition. The College is an institution chaired by the Prime Minister and includes the following members of the Government:

- Minister of Internal Affairs
- Minister of Foreign Affairs
- Minister of National Defense

<sup>32</sup> <http://orka.sejm.gov.pl/SQL.nsf/pracekom6?OpenAgent&SKBB>.

<sup>33</sup> Rozporządzenie Rady Ministrów z dnia 2 lipca 2002 r., Dz.U.02.103.929.

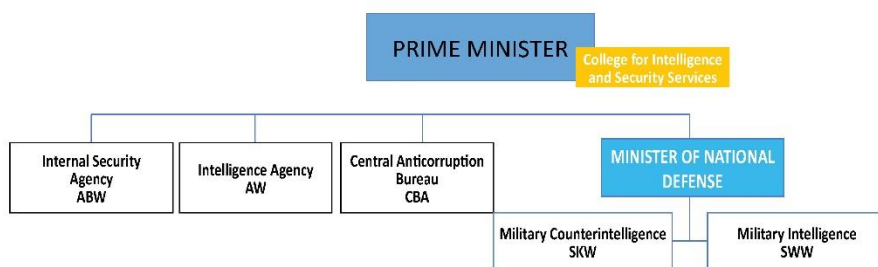
- Minister of Finance
- Head of National Security Office (presidential institution)
- Minister Coordinator of Intelligence Services (if appointed).

Chiefs of the intelligence services (ABW, AW, CBA, SWW, SKW) participate in the meetings, but the Bill makes it clear that they are *not* members of the College. The Chairperson of the parliamentary Commission for Intelligence Services is also entitled to participate in College sessions and is notified for each upcoming meeting. The College's role is to give opinions on all documents pertaining to intelligence, starting with appointment and dismissal of the chiefs of services, through projects of legislative acts, budgets, guidelines for annual planning, annual plans and reports, to the issues of coordination of intelligence activities with any other security service. The College also commonly puts current matters on the agenda, taking advantage of the obligatory presence of all relevant decision-makers in the field of state security.

If used properly, the College could become a powerful instrument of intelligence control and might facilitate the sharing of intelligence with government members. However, it did not become a robust oversight institution, primarily due to the lack of focus on effective oversight and sharing intelligence among the politicians. The composition of the College makes it an appropriate body for substantive discussion on important matters, and the presence of the Prime Minister and all the chiefs of services facilitates control and coordination. The College meetings are classified and take place in the special safe room in the Prime Minister's Office, protected from interception of any kind. Over the years, a minor information leak to the media occurred only once, making it an impressive record compared to the parliament or other government institutions. Therefore, the idea that a new round of intelligence reform is coming, the College will be disbanded, and some new body created is rather disturbing.

Finally, there is the position of the Minister-Coordinator of Special Services. However, his appointment is optional for any Prime Minister. Such a minister without portfolio (or recently just undersecretary of state) does not have independent powers or an institutional place of his own in the government structures. His actual importance strongly depends on the support of the Prime Minister. For that reason, he is hardly a controlling authority; rather, he serves as a liaison between the services and the government and is used as an expert in internal government workings.

The present structure of the intelligence sector and subordination lines are presented in Figure 2.



**Figure 2: Structure and Subordination of Intelligence Sector in Poland, 2018.**

### *Judicial Control/ Civil Watchdogs*

In discussions on intelligence oversight in Poland, one cannot but notice the weakness of the judicial control of the intelligence sector and the scarcity of citizens' watchdogs. The judicial branch does not have any specially designated role in the systemic oversight of the intelligence sector. Similarly, there is no specified procedure for complaints against the services. Often, the court proceedings are stalled by problems with access to classified information or lack of experience with security issues on the part of the judges.

There is a degree of irony in the fact that it was the judicial sector, after all, that managed to curtail the growing powers of the intelligence services to carry out covert, intrusive operations. That was achieved against the background of the utterly inert executive and legislative oversight bodies. The Constitutional Tribunal abolished some controversial prerogatives of the security and intelligence services and forced legislative changes in this respect.<sup>34</sup> More information on that subject can be found in the subsequent section discussing the operational powers of intelligence services.

Regarding the civil watchdogs, it seems that, after the initial extensive development of civil society in the 1990s, the process has stalled, and civil activities in the security area are now few and limited. That does not mean, however, that they are non-existent. At least two professional watchdogs carry out systematic oversight of legislative regulations and covert activities of the intelligence and security services and deliver public reports. These are the Panoptikon Foundation<sup>35</sup> and the Helsinki Foundation for Human Rights,<sup>36</sup> both actively monitoring the sector and providing invaluable insights.

<sup>34</sup> See Marta Kolendowska-Matejczuk, "Ile ograniczeń, a ile wolności w społeczeństwie obywatelskim w kontekście zapewnienia bezpieczeństwa państwa i obywateli," in *Ochrona informacji niejawnych, biznesowych i danych osobowych*, ed. Małgorzata Gajos (Katowice, 2012), 53-69.

<sup>35</sup> Panoptikon Foundation, <https://en.panoptikon.org/>.

<sup>36</sup> Helsinki Foundation for Human Rights, <http://www.hfhr.pl/en/foundation/>.

## **The Problem of Covert Surveillance Powers**

At the heart of the problems with democratic control of the intelligence sector in Poland lies the unsolved and unregulated issue of how to control the use of covert surveillance and intrusive investigative methods without jeopardizing the assets and putting intelligence operations at risk. From the start of the democratic transformation in Poland, the mix of police, law enforcement, and intelligence-gathering powers vested in the intelligence services opened the way to their heavy reliance on using covert, intrusive methods of investigation and surveillance. With time, this reliance only grew stronger. Since the early 1990s, several legislative attempts were made to regulate the covert powers of investigation and surveillance by a separate bill, the disclosure of such information, and its ultimate disposal. The first semi-complete legislative project was created in 2008 by the parliament. It included the definition of covert surveillance and the investigations linked to the goal of such activities.<sup>37</sup> The works on that project were abandoned though, and the same happened to several other attempts. Consequently, the term “covert surveillance and investigation activities”<sup>38</sup> has been widely used in several legislative acts pertaining to security and intelligence services and their activities. Yet, none of them gives a legal definition or sets limitations to such activities. As a result, the scope of powers and the constraints have been defined by the services’ practice and their internal regulations.<sup>39</sup>

The enhancement of covert powers began in 2003 when Polish intelligence services (and the Police) obtained the right to request telecommunications data (granted by the law on the telecommunications sector, not the intelligence bills). Paradoxically, the arrival of the European directive on data retention<sup>40</sup> and its incorporation into the Polish law gave the services almost unlimited and uncontrolled access to telecommunication data and provided a strong incentive to augment their powers of direct surveillance. In parallel, it limited the opportunities for control over the secret intelligence operations. But while the European directive aimed at countering terrorism, the Polish law did not provide for such limitation with regard to requesting telecom data. Effectively, the right to obtain individual telecommunication data was granted to the intelligence services unreservedly, without imposing any restriction or additional requirement for justi-

---

<sup>37</sup> Draft Bill on covert surveillance activities of February 7, 2008, parliamentary printout no. 353.

<sup>38</sup> In Polish “działania operacyjno – rozpoznawcze” or to translate exactly “operational and surveillance activities,” which collectively signify the operations with the use of covert human intelligence, intrusive investigations, direct surveillance, eavesdropping, interception of communication data, gathering of bulk data and the likes.

<sup>39</sup> Dariusz Laskowski, “Prawne aspekty funkcjonowania służb specjalnych z perspektywy potrzeb obronnych państwa,” *Obronność. Zeszyty Naukowe* 2, no. 10 (2014), 71.

<sup>40</sup> Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, abolished 2014.

fication. Before long, it became the favorite method of any investigation carried out by the intelligence services (or the Police, for that matter), without considering its proportionality to the potential threat or a requirement that it be a genuine threat to national security. In the record year 2014, the services asked for disclosure of telecommunication data 2.35 million times.<sup>41</sup>

The indiscriminate right to demand telecommunication data helped deepen the intelligence services' secretive culture and weaken external controls. The services were reluctant to disclose even the exact number of requests for information they lodged with telecom providers within a given period. In 2009, the Helsinki Foundation for Human Rights in Warsaw asked *ABW* for such statistics for 2002-2009, and it was denied information. The Internal Security Service *ABW* claimed that the information was secret and could not be disclosed as public information. The Foundation appealed to the administrative court against the decision. After several years of going back and forth, the court ruled in favor of the Foundation. However, the law had changed in the meantime, and the whole case could not be used for further reference or as a case of good practices.<sup>42</sup>

Looking back at the development of the intelligence sector's covert powers between 2003 and 2018, one can notice that, despite being better positioned to exert scrutiny and oversight, neither legislative nor executive institutions played any part in curtailing the growing independence and secrecy of the services. Instead, the judicial sector and some civic foundations played that role, proving to be more effective than designated control bodies. In 2005, acting on the motion of the Ombudsperson, the Constitutional Tribunal declared several regulations in the Law on Police unconstitutional. More specifically, the Tribunal abolished the articles that permitted the situation when data acquired by the services without prior judicial authorization (in the course of covert operations) could be stored indefinitely and could be used as legally sanctioned evidence in the criminal court proceedings. The corollary of the sentence was the amendment of legal regulations in all relevant bills, including the laws on the intelligence sector.<sup>43</sup> The second round of legal changes limited the covert powers of the services concerning the indiscriminate and disproportionate use of telecommunication data by the security and intelligence sector. Finally, on July 30, 2014, the Constitutional Tribunal, again acting on the motion of the Ombudsperson and several civil watchdogs, declared those regulations unconstitutional and allowed 18 months to make the relevant laws compliant with the Constitution. Unfortunately, the sentence did not indicate how precisely the legal regulations should be changed, leaving the problem entirely to the discretion of the politicians.

<sup>41</sup> "Rok z ustawą inwigilacyjną. Co się zmieniło," *Fundacja Panoptikon*, January 18, 2017, <https://panoptikon.org/biblio/rok-z-ustawa-inwigilacyjna>.

<sup>42</sup> Arkadiusz Król, "Działalność Operacyjna Służb Specjalnych w Systemie Bezpieczeństwa Państwa," *Przegląd Bezpieczeństwa Wewnętrznego* 9, no. 5 (2013), 287-289.

<sup>43</sup> Król, "Działalność Operacyjna Służb Specjalnych w Systemie Bezpieczeństwa Państwa," 283-285.

Ultimately, the parliament passed a separate bill, dealing collectively with the required amendments in relevant bills on all the security and intelligence services authorized to carry out covert activities. The Bill, adopted on January 15, 2015,<sup>44</sup> was immediately nicknamed “The Surveillance Bill” as it did more harm than good to curb the services’ appetite for personal data acquisition. In the common opinion of watchdogs and independent experts, in fact, the new law facilitated the access of the services to certain categories of data while further diminishing the transparency of their covert activities. Specifically, in striving to regulate the data acquisition processes, the new Bill introduced a new category of data that can be disclosed to the services, namely the data on the use of the internet by individuals. Even more, if any intelligence service concluded an agreement to that effect with the internet service provider, the data will be disclosed through a dedicated link without even the provider knowing the content of the data disclosed. Previously such arrangements were only possible with telecommunication companies; now, the security and intelligence sector won additional powers and further diminished oversight. The purpose of obtaining such data has been defined very widely in the new law as being in connection with “prevention and investigation of criminal acts as well as in order to save the life or health of natural persons.” The Bill did establish some judicial control over acquiring such data, but the control is retrospective, information aggregated, and the present law does not provide any measures to stop such process before it happens. It is also practically impossible to judge whether the data was acquired in connection with legally authorized causes for such request, or it was legally dubious, as the new law allows for the gathering of data on the “just in case” basis, previously not allowed with the telecommunication data.<sup>45</sup>

In brief, one may say that intelligence services in Poland, supported by politicians, were very proficient in using the European directives aimed at improving the efficiency of counterterrorist activities in order to increase their covert surveillance and investigatory powers beyond justifiable levels—Poland not being precisely the terrorist hub of Europe—and to limit the effective oversight from any external institutions. Sadly, such an approach to European directives seems like a Polish ‘trademark.’ When the EU was debating the data retention directive, Poland postulated 15 years period of data retention, the longest proposed by any EU country. When the PNR Directive<sup>46</sup> came into force, it was incorporated into Polish national law in an all-inclusive manner so that the PNR regulations also cover domestic flights. Part of the fault may lie with the European legislators who never included any provisions for obligatory national checks on the data acquisition, allowing for national incorporation of the regulations in the manner

---

<sup>44</sup> Ustawa z 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. 2016, poz. 147), dalej: tzw. ustawa inwigilacyjna, ustawa.

<sup>45</sup> “Rok z ustawą inwigilacyjną. Co się zmieniło,” 2-12.

<sup>46</sup> Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

exceeding the original cause of action. But more importantly, the situation is blatant proof of the weakness of all the state oversight and control institutions and their apparent inability to counter the increasing secrecy of intelligence services. To dot the 'i', the case of the so-called Police directive<sup>47</sup> should be mentioned here. This directive is supposed to provide a degree of protection of natural persons from excessive personal data processing practices. Yet, it is clear that the Polish government is dragging its feet in preparing the legislative regulations to adopt it to national law.<sup>48</sup>

## Tentative Conclusions in Lieu of Good Practices

Looking back at the history of democratic transformations of the intelligence sector in Poland, it is difficult to point to practices that had proved unequivocally successful in the course of reforms. Rather, it is the case for lessons learned, which may help with recommendations for avoiding certain mistakes and achieving higher success with less cost in the future.

Dealing with the communist past of the services and vetting former communist officers appears to be the most important and most disruptive issue throughout the history of the post-communist transformation of intelligence. In post-1989 Poland, there were three options for dealing with the past: 1) the policy of "thick line," proposed by the first post-communist Prime Minister Tadeusz Mazowiecki and offering to close the past accounts on day one and never look back; 2) the so-called "zero option," consisting in getting rid of all the former functionaries of the communist regime and starting new services from scratch; and 3) the option of central vetting of former officers thus limiting the access of officers of the old regime to the new services. Each option had (and still has, for that matter) its supporters and opponents among the politicians. However, the problem was that each option was applied partially and to a limited extent in different places. There was never a binding decision taken by any government to apply one of those options in its entirety and end the discussion. Consequently, the debate on historical injustices is still ongoing. Politicians from the first post-communist government are accused of betraying the nation. The subsequent rounds of reforms of the intelligence sector always have had a backdrop of historical resentments. Those unsealed historical accounts have been partly the reason for the recurrent waves of institutional transformations of the services,

<sup>47</sup> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

<sup>48</sup> Letter from deputy Minister of Internal Affairs in response to watchdog enquiry, see <https://www.rpo.gov.pl/sites/default/files/odpowied%C5%BA%20MSWiA%20z%2015%20listopada%202017%20w%20sprawie%20wdra%C5%BCania%20dyrektywy%20ODO.pdf>.



which in the long run contributed to the politicization of the sector, had an adverse effect on the officers' professionalism, and hampered the relations between the politicians and the functionaries.

Secondly, the democratic intelligence sector in Poland has not been formed along any conceptual lines. Rather, it was affected by the existing security situation and current political priorities, combined with the traditional scope of responsibilities inherited from the communist period. Hence the inherent overlap of intelligence, policing, and law enforcement powers and responsibilities, particularly in civilian and military counterintelligence services. Given the combination of investigative and policing prerogatives, the services shifted the focus to enhance their powers of covert and intrusive operations. This, in turn, has led to increased secrecy of the intelligence sector and weakened the effectiveness of the oversight.

Thirdly, the legislative and executive oversight institutions have been successfully established following commonly recognized democratic principles but were never properly consolidated in their functions. As a result, the oversight bodies have all the tools at their disposal necessary to exert their powers but remain reluctant to do so. Also, until recently, no special judicial authorities have been established to monitor the sector, although, in practice, the judicial branch proved to be most efficient in curtailing the undesirable processes of deepening secrecy in the services. Last but not least, the prolonged and complicated process of transforming the sector has resulted in highly dispersed legislative regulations pertaining to the security sector and the lack of definition or regulations of some key aspects of the functioning of the intelligence.

Still, the transition of the security sector in Poland should not be looked at too critically. The services, in general, accepted the civilian leadership and oversight of often inexperienced politicians and, with the dubious exception of the OLIN case over a decade ago, they have never appeared a serious threat to the sovereignty or integrity of the democratic state (notwithstanding some unsubstantiated accusations of certain politicians). The services were also reconciled with the successive rounds of institutional reforms and, in contrast to the military, never openly challenged the politicians. Finally, the post-1989 intelligence services did register some notable successes. All in all, it seems that the main problem of the Polish transformation is the impeded development of the democratic system, which was successfully established but failed to fully consolidate into a mature democracy with a robust civil society. This has led to certain alienation of the intelligence sector and permanent distrust between the politicians and the services.

Based on those observations, the following recommendations for the democratic transitions of the intelligence sectors may be formulated:

1. Historical past should be dealt with knowingly, purposefully, and without undue delay. Politicians should hold some sort of national discussion in this respect and legitimize their decisions about the inheritance of the past regime and the functionaries of the predecessor institutions, what-

ever the decision might be. Leaving the historical resentments unresolved will inevitably lead to undermining the democratic legitimacy of the new intelligence institutions in the future;

2. The powers and responsibilities of the intelligence sector should be delineated as clearly as possible at the start of the transformation, with some conceptual underpinning of the institutional design to justify the division of prerogatives. It would be advisable to avoid excessive fragmentation of the sector and overlaps of powers as that will complicate control and coordination procedures, lead to intra-services rivalries and increase the budget for intelligence;
3. Covert surveillance prerogatives should be legally regulated early on, preferably through a separate bill or as part of laws on individual services; above all, the field of covert operations should not be left for the services to define and decide what can be done and what not;
4. While drafting new directives, European legislators need to take into account the possibility of undermining democratic oversight in transitional states and unduly enhancing the powers of intelligence services. Therefore, it is recommended to impose in the directives some obligatory constraints on the use of new powers, if only for educational reasons.

## Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

## About the Author

**Agnieszka Gogolewska** is an e-learning consultant, scenario writer, academic lecturer, and author. Since 2010 she is a Senior Lecturer at the European University of Information Technology and Economics in Warsaw. Her main research interests are in democratic transitions and security sector reform, processes of democratization and de-democratization, intelligence and security studies.



## Lessons Learned from Military Intelligence Services Reform in Hungary

*Andras Hugyik*

**Abstract:** The classic types of national security services are external and internal intelligence services, as well as integrated, internal, and external intelligence organizations. From a professional perspective, external and internal intelligence cannot be interpreted as entirely independent. Some theoretical schools consider internal intelligence (counterintelligence) part of intelligence; others attribute a significant distinction between internal and external intelligence. Regarding the number of national security services, two trends are observed in countries comparable to Hungary in the last decade. One is the increase in the number of services reflecting the increasing number and complexity of tasks and threats; the other is the decrease in the number of services through the integration of existing organizations, usually due to financial reasons.

In Hungary, military internal and external intelligence were merged in 2012, establishing an integrated organization, the Military National Security Service (MNSS). Although an impact assessment did not precede the merger, the official evaluation of the Court of Auditors in January 2014 stated that the creation of NMSS resulted in savings in public money and this new organizational form ensured the better implementation of unchanged tasks.

This article briefly presents the current political situation in Hungary, the Hungarian secret services, the development of the Hungarian Defence Forces in the past decade, the reasons for reforming the special military services, the periods, the aims, and the results of the integration process. It provides general and specific conclusions and lessons learned from military intelligence services reform in Hungary.

**Keywords:** military, intelligence, external intelligence, internal intelligence or counterintelligence, military intelligence reform, lessons learned, Hungary, political situation, Hungarian Defence Forces, national security services.

## Introduction

### *National Security Services*

Generally, we distinguish between two types of national security services. One is the internal intelligence service (or counterintelligence), which collects and manages information about a country's internal security. Its task is to protect the state, the territory, and society from foreign interference (subversion, espionage, political violence). The information collected by this service contributes to upholding and guaranteeing the internal security of the state and society. The other is the external intelligence service, aiming to learn about the probability and consequences of events of foreign origin that pose a threat to the country. Therefore, such services collect information relating to foreign governments, organizations, non-governmental formations, foreign state intelligence services, or agents that pose an actual or potential threat to the country and its foreign interests. Information gathered by external intelligence services serves the enforcement of national interests, including political, economic, military, scientific, and social interests.

The tasks and objectives of these two types of information-gathering services are therefore different. The nature and extent of the threats they address also vary. The management, control, and supervision systems of these services must reflect these differences. Because a state's internal intelligence service (counterintelligence) collects information about its own citizens, mostly within the country, its activities require strict control. This is necessary so that the interests of deterrence do not prevail unrestrictedly against the rights of individual citizens and legal entities.

Intelligence or information gathering organizations (internal and external intelligence) usually perform three main tasks: information gathering, analysis, and internal protection of these activities (protection against phenomena that endanger their own activities).

Secret actions are also a controversial but undoubtedly necessary element of the activities of the intelligence services of modern democracies. The CIA defines covert actions as operations that affect the activities of governments, events, organizations, and individuals in the conduct of foreign policy in a manner that does not disclose the customer of those operations.<sup>1</sup> The boundaries between the activities of external and internal intelligence services have never been strictly separable. Both types see the fight against terrorism, organized crime, drug trafficking, and smuggling as their own task, both internally and externally. As the DCAF Intelligence Working Group elaborates:

---

<sup>1</sup> DCAF Intelligence Working Group, "Intelligence Practice and Democratic Oversight – A Practitioner's View," Geneva Centre for the Democratic Control of Armed Forces, Occasional Paper No. 3, Edition in Russian (Geneva, July 2003): 12-13, 17, 28, [https://www.dcaf.ch/sites/default/files/publications/documents/op03\\_intelligence-practice\\_ru.pdf](https://www.dcaf.ch/sites/default/files/publications/documents/op03_intelligence-practice_ru.pdf).

The establishment of a centralized service may be a justified need, as the security of a country can only be achieved through close cooperation between internal and external intelligence services. If, for example, an extremist group plans an armed attack on the country and gathers information to carry it out, it is up to internal intelligence to detect the act. If the said group receives support from a neighboring state in the form of assisting in the immediate preparation of the attack and in training the participants in the territory of the neighboring state, it is already the responsibility of external intelligence to detect this. In this situation, only a centralized integrated organization that coordinates the activities of the external and internal intelligence services can respond effectively to the threat.<sup>2</sup>

According to a rigid and now outdated sectoral model supported by only a few countries, intelligence is only one of the foreign branches of national security activity. According to the modern conception, however, intelligence is a basic activity, the main task and method of all national security—i.e., ‘secret’—services, which Hungarian law calls “secret information gathering.” It means that internal and external intelligence conduct a common activity, namely information gathering. It is not the foreign or domestic orientation that distinguishes the internal and external intelligence services, but the area of operation (foreign or domestic) and the operational, technical, and organizational aspects. Strict enforcement of operational security and conspiracy requirements, for example, is just as important at home as it is abroad but can be achieved under different conditions and in part by different methods.

## **National Security Services of Hungary**

### ***Hungary 2020 – Political Situation***

The temporary collapse of the hegemony of neoliberalism in some Central European countries after 2008 led to a wave of populism in these countries. Populist parties and movements include both left- and right-wing actors. One of their few common characteristics is that they all criticize the ruling elite and its ideology, claiming that elites oppress the people and the nation. According to the left-wing rhetoric, the social and economic policy of Orbán’s populist government is strengthening the nation’s capitalist class, selling out cheap workforce to foreign industrial investors while disciplining the workers, and performing centralized control of the poor living primarily in rural areas. The purpose of its cultural policy is to promote the official Hungarian ideology of the era before 1938 – a conservative, Christian, nationalist ideology, with historical lies, an unjust social system, hostile atmosphere, and the (yet hidden) intention to recover territories lost after World War I. Orbán perceives the neoliberal European Union, the international capitalists’ secret fraudulent practices represented by George Soros, and migrants as enemies in order to declare his political opponents as the enemy of the nation and take the role of its rescuer. While the government is attacking

---

<sup>2</sup> DCAF Intelligence Working Group, “Intelligence Practice and Democratic Oversight.”

some of the EU values in political fora and is confronted loudly, it is a subordinated ally of European capitalists in terms of economic processes.<sup>3</sup>

Due to Viktor Orbán's new nationalist regime-building politics, democracy, the rule of law, and pluralism in Hungary have become limited and resulted in the establishment of a country with illiberal democracy. In Hungary, those in power suggest that leftists and liberals are not part of the nation, and anything that is left or liberal, be it the person, any artwork, or just a point of view or an approach, should be deemed as alien and rejected since it goes against the official national Christian conservative course.

Orbán's political views are faithfully reflected in his speech on August 20, 2020, at the inauguration ceremony of the Monument of National Cohesion commemorating the 1920 Trianon Peace Treaty. Prime Minister Orbán said in this speech that "Western Europe, weakened by embracing the ideas of a God-less cosmos, rainbow families, migration and open societies is losing its leading position in the world and is becoming less and less attractive for Central Europeans." He called on Central European countries that want to maintain their Christian heritage to create a strong coalition that can help reorganize Europe. Orbán added that the main lesson of the past century is that nations need to fight and show their strength to maintain their sovereignty and freedom. Orbán formulated the seven tenets of Hungary's nation-minded policies in the 21<sup>st</sup> century: the homeland exists only as long as there is someone there to love it; every Hungarian child is a new 'lookout'; truth is worth little without power; Hungarians will only get to keep what they can defend; "every match lasts until we win"; it is the country, not the nation that has borders and that no Hungarian is alone.<sup>4</sup> Accordingly, Hungary makes significant investments in developing its defense forces and modernizing its national security services.

### ***Hungary's National Security Services – A Brief Historical Overview***

Upon breaking away from the Soviet-led regime, five national security services were created in Hungary: the National Security Office (NSO, civilian counterintelligence service); the Information Office (IO, the civilian external intelligence service); the Military Security Office (MSO, the military counterintelligence); the Military Intelligence Office (MIO, external military intelligence).; and the Special Service for National Security (SSNS), responsible for providing special tools and methods of secret information gathering for other security services as customers

<sup>3</sup> Tamás Gerőcs and Csaba Jelinek, "The System of Hungarian National Cooperation in the Context of the European Union – on Hungary's EU Integration in a Historical Sociological Approach," *Analízis* (2018): 12-33, quote on p.23, in Hungarian, [http://www.regscience.hu:8080/xmlui/bitstream/handle/11155/1768/jelinek\\_nemzeti\\_2018.pdf](http://www.regscience.hu:8080/xmlui/bitstream/handle/11155/1768/jelinek_nemzeti_2018.pdf).

<sup>4</sup> Viktor Orbán, "West 'Lost Its Appeal,' Hungarians 'Champions of Survival'," *MTI-Hungary Today*, August 20, 2020, <https://hungarytoday.hu/orban-speech-august-20-survivors-west-central-europe>.

(e.g., wiretapping). SSNS was separated from the rest of the agencies to allow for an equal distribution of power among them.

A minister without a portfolio oversaw the civilian national security services (NSO, IO, and SSNS), while the military intelligence services were subordinated to the Minister of Defense. In the meantime, the National Security Office was renamed, the new name being Constitutional Protection Office (CPO). Further, the Counter-terrorism Center (CTC), subordinated to the Ministry of Interior, was established in 2010 by bringing together the terrorism-related information gathering and the operational response to acts of terrorism. An organization with such a combination of responsibilities is unique in Europe. A new organization of the Ministry of Interior was created to combat corruption within the law enforcement agencies, including national security services, by reorganizing the previous agency with such responsibilities, the Protective Service of Law Enforcement Agencies (PSLEA). The powers of PSLEA have subsequently been extended, and its name was changed to National Protective Service (NPS). The parliamentary control of those services has been and will be carried out by the Committee of Defense and Law Enforcement and the National Security Committee.

Taking advantage of the two-thirds majority in the Parliament, Orbán's government introduced major changes in the country's national security system during his second and third terms. Shortly after Orbán's government took office for the second time, the provision of the National Security Act to prevent the Minister responsible for law enforcement from controlling civilian national security services was abolished. This change terminated the public agreement and openly reverted to earlier times when the Ministry of Interior had been the primary protector of the regime. The Constitutional Protection Office and the Special Service for National Security were placed under the supervision of the Minister of Interior. The authorization of police units to carry out covert intelligence-gathering was extended. The position of the Minister without portfolio in charge of the civilian intelligence services was abolished, thus disrupting the unified government control of the civilian services. The Information Office was finally placed under the authority of the Minister of Foreign Affairs. Surprisingly, the Minister of Interior was appointed to lead the Government task force handling the Ukrainian crisis. The professional expertise of the task force was questioned when, in the last wave of staff cuts, several experts with outstanding capabilities, who had graduated in the former Soviet Union, spoke the target languages, and had possessed knowledge of Russian-Ukrainian culture, were removed from the Military National Security Service (MNSS). In the wake of the refugee crisis in 2015, the Parliament transferred the authority to declare a refugee-related state of emergency from the President of the Republic to the Government (Minister of Interior). The military troops involved in the protection of borders were placed under the authority of the Police.

Upon amendment of the National Security Act, the Counterterrorism Information and Criminal Analysis Center (CTICAC) was established under the supervision of the Ministry of Interior and received special national security functions

(integrated analysis and assessment, coordination, tasks assignment, performance evaluation). An agency with these functions would require centralized, governmental, and not ministerial supervision. Thus, in 2018, to offset the increasing power of the Minister of Interior, the oversight of CTICAC was transferred to the State Secretariat for National Security, established within the Prime Minister's Office. CTICAC as an "intelligence center" should have been established by amending the Act CXXV of 1995 (National Security Act), not under separate legislation. At the same time, it would have been more appropriate to set up an integrated analysis-assessment, coordination, task assignment, and performance evaluation organization under the supervision of the Prime Minister (for example, through an Information Analysis and Assessment Center for National Security), and to place the Counterterrorism Information and Criminal Analysis Center under the responsibility of the Minister of the Interior, possibly the Head of the National Police, but with limited authority and detailed legal definition of cooperation obligations.

The National Security Authority, established on the basis of Hungary's NATO membership to enforce the requirements of the Alliance's security regulations, was integrated into the organization of the Ministry of Interior in the new government cycle starting in 2014 as a department-level organization. With this, the Ministry of Interior has gained an overview of the confidentiality aspects of international information exchange conducted by the Ministry of Foreign Affairs and the Ministry of the Interior while excluding itself from the independent oversight of confidentiality. At the turn of 2011 and 2012, the government achieved its old objective by merging the two military national security services, namely the Military Intelligence Office and the Military Security Office.

Figure 1 shows Hungary's national security services operating in 2020 and the characteristics of the services.

## **Integration of the Military Intelligence Services**

### ***Development of the Hungarian Defense Forces***

Hungarian Defense Forces (HDF) is the official name of the Hungarian Armed Forces. Since 2007, the armed forces are under a unified command structure. The Ministry of Defense maintains political and civil control over the army. A subordinate Joint Forces Command is coordinating and commanding the HDF units. The Hungarian Defence Forces had 28,000 personnel on active duty. In 2019, military spending was \$1.904 billion, or approximately 1.2% of the country's GDP, well below the NATO target of 2%. Military service is voluntary, though conscription may occur in wartime. According to the Hungarian Constitution, the three pillars of the nation's security are the strength of the HDF, the Alliance system, and the citizens.





**Figure 1: National Security Services of Hungary.**

The Hungarian government aims to make the military one of the “most decisive” armies in the region. An increased budget will be available for a larger force, and the defense budget will reach 2 percent of GDP, or 1 trillion HUF, by 2024. The defense and armed forces development scheme, named Zrínyi 2026, and the increased budget will enable the acquisition of state-of-the-art technologies to ensure that the army maintains 21<sup>st</sup>-century capabilities.

The potential of the national economy ensured opportunities to develop the armed forces, unprecedented for the past 25 years. The MoD elaborated medium- and long-term strategies to enable the army to respond appropriately to both present and future challenges. Under the Zrínyi 2026 program, the government will change soldiers' personal equipment such as clothing and weapons and modernize the Army and the Air Force.

Hungary's defense forces plan to buy 40 new helicopters in the coming years (twelve Russian-made Mi-24 helicopters are currently under comprehensive modernization in Russia and will be in service until 2025). The Hungarian Defense Forces have already purchased two transport planes, which will be in service in 2020. They can carry military personnel and their individual equipment, as well as smaller supplies. They will also be equipped with capabilities to carry out air rescue missions. Hungary needs larger aircraft as well, capable of carrying large military supplies and equipment and fitted with aerial refueling capability.

As part of its commitment to NATO, Hungary is replacing its heavy ground forces equipment. Following the tanks and artillery, it is now the turn of the infantry fighting vehicles, which form the backbone of the capabilities set. One of Europe's foremost maker of army equipment will cooperate with Hungary to create a joint venture and production facility in Hungary to manufacture the most modern infantry fighting vehicle.

The military contributed some 15,000 soldiers to Hungary's border control efforts in the last years. At the same time, the Hungarian armed forces participated in some 40 international exercises, while some 1,000 troops served in international missions. Hungary's voluntary reserve force of 5,300 is under development into a national network with units in each district of the country. The government greatly appreciated the work of soldiers, and their salaries have been raised by more than 40 percent since 2015.

The HDF development priorities are establishing a supportive and involved population and a voluntary reserve force, adequate military strength (replacing air force and heavy ground forces equipment), improved resilience to hybrid and cyber threats, and effective internal and external intelligence. To make military internal and external intelligence more effective, in 2011, the parliament decided to merge the two military intelligence services.

Before describing the integration process and its consequences and effects, I will present the military secret services merged one by one.

### ***History of the Military Security Office***

At the time of the change of social system, the organization, personnel, and working methods of the III/ IV Directorate of the Ministry of the Interior (the military internal intelligence directorate) were essentially transferred to the successor organization, the Military Security Office (MSO). At the time, the country's political and economic leadership needed the expertise of experienced, trained military internal intelligence personnel.

The “regime change” of 1989-90 did not affect the MSO markedly. The organization’s notion of “the enemy” remained essentially unchanged: it continued to focus on examining the reliability of our own external intelligence officers and detecting the military intelligence activities of all foreign countries.

The Military Security Office lived its heyday under the leadership of Géza Stefán, who became Director-General in 1994 and held this position for 15 years – an unprecedented achievement in the history of the Hungarian public administration.

After retiring with the rank of a four-star general, he continued to run the office as a “civilian employee,” and with each change of government managed to gain and maintain the trust and satisfaction of both leading parties, the Socialist Party and the Young Democrats (Fidesz).

Furthermore, as an excellent national security expert who graduated in the Soviet Union and was familiar with the Russians, he enjoyed the goodwill of the new Western Allies and Moscow simultaneously. Thus, he formed a kind of a bridge between former Cold War opponents, bringing together Russian and Allied secret services in the fight against global threats such as proliferation, terrorism, the illegal arms trade, and organized crime.

However, according to a widespread view in the secret service circles, the real explanation for his performance was that he carefully kept the personnel files of former informants obtained in his previous position in the Directorate of Internal Security of the Ministry of the Interior, which proves that a significant part of the ‘new’ Hungarian political and economic elite cooperated secretly with that Directorate. Although there is no evidence to support this view, it is in any case strange that the Hungarian Parliament has not yet adopted a so-called “agents law” on disclosing the names of former state security agents.

There have also been lows in the history of the Military Security Office, such as the involvement in mafia crimes related to oil imports and serial killings of ethnic Roma citizens, and the attempt to ‘occupy’ the Military Intelligence Office around the turn of the century, when, with the support of the government, a deputy director-general was transferred temporarily from the Military Security Office to the Military Intelligence Office. The attempt then failed but was repeated by the second Fidesz government with complete success by merging the two military services in 2011-2012.<sup>5</sup>

The organizational structure of the Military Security Office in 2011, before integration, was as follows: the Legal and Audit Department, the Department of Internal Security, the Human Resources Department, the Education Department, the National Security Office (with publically unknown purpose), and the Data Repository were directly subordinated to the Director-General. The Administrative Directorate, the Operations Directorate, the Evaluation, Analysis and Infor-

---

<sup>5</sup> Naive Balfácán, “The Fifth Generation of Traitors,” *National Security Reading Diary*, October 19, 2018, 1-2 and 8-9, [https://naivbalfacan.blog.hu/2018/10/19/102\\_epizod\\_499#more14309193](https://naivbalfacan.blog.hu/2018/10/19/102_epizod_499#more14309193) and <https://drive.google.com/open?id=11EqIL8uCN3G-D6tF73cr0Or07XbRuRf>.

mation Directorate, and the Personnel and Industrial Safety Directorate were under the authority of the Deputy Director-General, reporting directly to the Director-General.

### ***History of the Military Intelligence Office***

The legal predecessor of the Military Intelligence Office, the Second (Foreign Intelligence) Directorate of the General Staff of the Hungarian People's Army, occupied a very prominent place among the military intelligence services of the member states of the former Warsaw Pact. This is due to the so-called Conrad case.<sup>6</sup> Conrad was the head of the confidential documents' handling office of the 8<sup>th</sup> US Infantry Division stationed in Germany and the star agent of a spy network named after him. He was recruited by Hungarian foreign military intelligence in 1975 by another American soldier, Zoltan Szabo of Hungarian descent, a Vietnam veteran. Szabo was successfully involved in the work of the 2<sup>nd</sup> Directorate of the General Staff of the Hungarian People's Army in 1971.

Szabo served in Bad Kreuznach, from where he knew Conrad, and they both recognized the opportunity offered to them by the security deficiencies of the 8<sup>th</sup> Division's confidential documents handling office. Conrad smuggled (and then smuggled back) and copied top-secret documents from the confidential documents handling office on a large-scale, and sent the copies (or sometimes the 'discarded' originals) to Hungarian foreign military intelligence through the Kercsik brothers. The Kercsik brothers were doctors living in Sweden. They traveled a lot in Europe and transported the 'material' to Vienna in their medical bags, which they passed in secret meetings to an officer of the 2<sup>nd</sup> Directorate of the General Staff.

For almost twenty years, the Conrad Group provided invaluable information to Hungarian—and through it, Soviet—military intelligence, immensely threatening the security of the United States, Germany, and NATO as a whole. The documents handed over included original NATO military-operational (defense) plans, detailed organizational, armaments, combat readiness data, the nuclear force alert system, and the location of the nuclear mines. With this information, the Soviets could have occupied the whole of Western Europe in a short time by launching an unexpected attack, and the United States could have avoided that only if ready to escalate to a global nuclear war with the Soviet Union.

In the period of social changes, Hungary needed US goodwill, and the outbreak of the Conrad affair came at the worst possible time in the 1980s. Professionally, this was the greatest success in the history of Hungarian military intelligence, but politically it was the most severe and unpleasant heritage of the Kádár regime. As a result, the government had to apologize publicly and express regrets that, by handing over intelligence information to the Soviet Union, Hungary threatened the security of the United States and Western Europe.

---

<sup>6</sup> Balfácán, "The Fifth Generation of Traitors."

After the regime change, the staff reductions affecting the Hungarian Defence Forces over the years naturally affected the legal successor of the 2<sup>nd</sup> Directorate of the General Staff and, consequently, the Military Intelligence Office. By the summer of 2007, the initial staff of 1963 melted down to 733. At that time, at the initiative of the Director-General of the Military Intelligence Office, the Minister of Defense ordered a full review of its operation in order to meet growing international obligations and enhance information gathering and reporting. Following the screening, in 2008, the following directorates and other organizational elements were established under the authority of the Director-General of the Military Intelligence Office: HUMINT (Human Intelligence) Directorate; SIGINT (Signal Intelligence) Directorate; Directorate for Information Analysis, Evaluation, and Reporting; Human Resources Directorate; Security and Administration Directorate; Directorate for Logistics, Development, and Finance; Planning and Coordination Department; the National Security Secretariat (with unknown purpose); Attachés' offices. The Military Intelligence Office operated military attaché offices in 19 countries, and our military diplomats were accredited to a total of 56 countries. This figure has changed and continues to change due to evolving military relations, the security situation, and budgetary considerations. Attaché offices are managed and supervised by the Minister of Defense through the Deputy State Secretary for Defence Policy of the Ministry of Defense and the Director-General of the Military Intelligence Office (currently Military National Security Service). Multiple accreditations (a defense attaché representing the Ministry of Defense of Hungary in one foreign country is also accredited to other countries) and the regional military attachés (stationed in Budapest and regularly visiting the countries where they are accredited) allow to perform military diplomacy tasks cost-effectively.

### ***The Merger of Military Intelligence Agencies***

According to the political leaders, by 2011, a single organization has become necessary to properly manage military intelligence and counterintelligence activities, allowing more prudent use of budgets. (In the longer term, the expected savings resulting from the reduction of properties used by the two predecessor organizations alone will amount to several hundreds of millions of forints.) The integration was done in two stages. The first phase was carried out between August and November 2011 with the following objectives: to create conditions for speedier information flow; to facilitate more efficient use of resources; to eliminate duplication of efforts to enhance the effectiveness of operations; to increase the efficiency of protecting Hungarian troops deployed in operations; to operate fewer properties and thus reduce expenditures. The period between January 1 and April 30, 2012, can be designated as the second phase of integration, characterized by the following tasks to establish a new organizational model: development of unified management of military intelligence and counterintelligence activities; optimization of management levels and senior positions; revision of internal rules and the operational instruction system; review of

cooperation agreements, implementation of logistic, personnel-related, and technical integration.<sup>7</sup> A new Organizational and Operational Policy was developed under the statutory requirement. It detailed the functions of the Military National Security Service (MNSS) and the basic rules governing its organization, management, and operation under the relevant legislation.

In terms of Parliamentary oversight, democratic control has been exercised by the Parliament's Committee of Defense and Law Enforcement and the National Security Committee.

### ***Expansion of the MNSS Functions***

The amended National Security Act added a new responsibility to the scope of MNSS national security activities. Previously, this task was not included among the responsibilities of any of the predecessor organizations. MNSS's new responsibility entails the collection of information about cyber activities compromising defense interests. The primary task of the new organizational unit responsible for the above function is to address the challenges faced by the IT systems and thwart cyberattacks attempting to compromise defense- and national security interests.<sup>8</sup> To comply with the statutory requirements, a Cyberdefense Center was founded on March 1, 2016. With its three departments, it is able to perform all activities related to incident management, the exercise of authority, and vulnerability assessment and analysis.<sup>9</sup>

The Reconnaissance Department within MNSS, founded on June 1, 2014, took over the responsibilities of the General Staff of the Armed Forces' Reconnaissance Department disbanded on this date. With this organizational transformation, the tactical reconnaissance capabilities of the Hungarian Defense Forces (HDF) and strategic intelligence capabilities of the Ministry of Defense were placed under single professional management, and the Director-General of the MNSS exercises professional control over the HDF reconnaissance capabilities. This solution allowed for centralized management and decentralized execution of tactical and strategic level reconnaissance and intelligence activities.

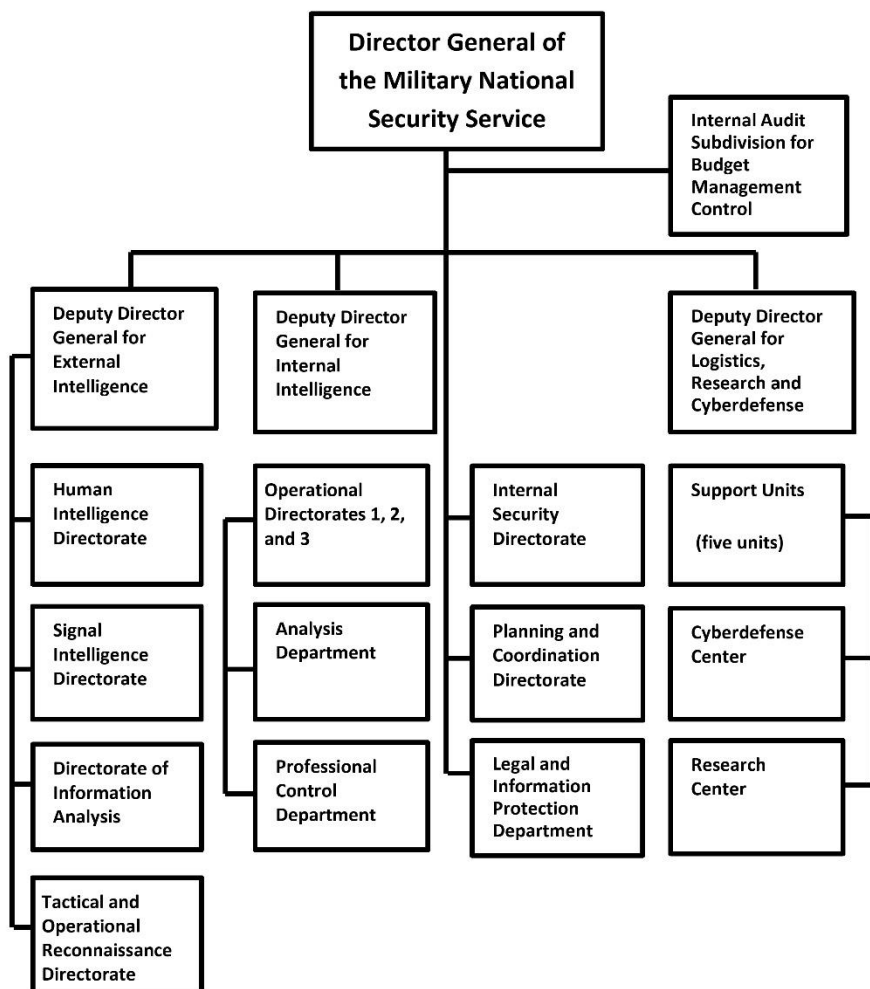
New opportunities emerged for electronic specialization within the HDF, which opened up opportunities to form and develop new intelligence branches (e.g., IMINT capabilities, ground moving target detection capabilities).

The current structure of the Military National Security Service is shown in Figure 2.

<sup>7</sup> Kenedli Tamás, "The Most Important Features of the Professional Development of the Military National Security Service in Recent Years," *National Security Review* (2020): 74-94, <https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1397>.

<sup>8</sup> Gergely Szentgáli, "To Serve in Silence. Situation in and Transformation of the Hungarian National Security Sector between 2010 and 2014 - Part 2," *Military Science*, no. 3-4 (2015): 84-86, in Hungarian, <https://core.ac.uk/download/pdf/42939777.pdf>.

<sup>9</sup> Szentgáli, "To Serve in Silence."



**Figure 2: Structure of the Military National Security Service.**

## **Findings, Conclusions, and Lessons Learned**

In its January 2014 report on the merger of the two military intelligence agencies, the State Audit Office (SAO) states: “Generally, it can be established that founding MNSS resulted in savings of public resources and, at the same time, considering that the basic tasks remained unchanged while the staff was reduced, a more efficient organizational structure was established, creating the circumstances necessary to encourage further development in terms of professional activities.” One of the issues regarding this report is that the adoption of findings concerning the execution of professional, specialized tasks falls outside SAO’s competence since it lacks the necessary expertise. Another issue is that the

budget calculations contradict each other. According to the SAO report, the aggregate expenditures effected for and by the Military Security Office and the Military Intelligence Office prior to the 2011 merger amounted to HUF 12,019.5 million, while the annual expenditures for and by MNSS in 2012 stopped at HUF 11,327.0 M. In other words, by the end of the 2012 financial year (MNSS's first year), the operation of the new organization resulted in savings of HUF 692.5M, which was mainly attributed to the staff reduction.<sup>10</sup>

**Table 1. Yearly Budget of the Military Security Office (MSO), the Military Intelligence Office (MIO), and the Military National Security Service (MNSS) in the Period of 2010-2018.<sup>11</sup>**

	2010	2011	2012	2013	2014	2015	2016	2017	2018
<b>MSO</b>	2,5	2,6							
<b>MIO</b>	9,2	9,4							
<b>Total</b>	11,7	12,0							
<b>MNSS</b>			11,3	10,9	10,4	14,9	18,5	34,6	28,2

As the credibility of the SAO report ought not to be questioned, my observations are limited to a few remarks: Previously, the Military Intelligence Office employed 733 people, while Military Security Office's headcount was 225. Just before the merger, the former organization's staff was cut by 155 (21.15%), and that of the latter by 62 people (27.56%). The original organizations carried out the personnel reductions, and the substantial expenditures involved did not affect the 2012 MNSS budget. Financial experts argue that staff reductions in operation support and logistics result in annual savings of HUF 1.55 billion. Taking this into consideration, the 2012 budget savings seem quite modest. This is even more awkward if we also consider the attaché offices' budgets. According to the SAO report, if the aggregate costs of approximately twenty attaché offices are the equivalent of 100 units in 2010, these costs amounted to 120.2 units in 2011 and 85 units in 2012, which should have also resulted in significant savings.

The finding contending that the creation of MNSS resulted in the saving of public assets is definitely true; however, in MNSS' first year, these savings did not meet the expectations.

<sup>10</sup> State Court of Auditors, "Report on the Control of the Military National Security Service," State Court of Auditors (January 2014), 11, <https://www.knbsz.gov.hu/hu/14018j000.pdf>.

<sup>11</sup> Tamás, "The Most Important Features of the Professional Development;" Szentgáli, "To Serve in Silence;" State Court of Auditors, "Report on the Control of the Military National Security Service."



Several Hungarian studies <sup>12</sup> discuss the assessment of MNSS' operation, and these studies consistently and firmly state that the merger was successful and has improved the standards of intelligence and counterintelligence activities. Without questioning the conclusions of said studies, I would offer a few facts here. First, the number of MNSS' initial personnel should have been equal to the total number of staff employed by the Military Intelligence Office (578) and the Military Security Office (163) right after the staff cut (741) while, based on a Minister of Defense decision, MNSS received more positions and started its operation with 825 personnel. It is not known when this ministerial decision was made – before the start of the staff reduction or after its end. If the decision was made after the staff reduction, the dismissal of 84 officers was unnecessary. Second, the most important positions in terms of execution of the merger (the management of the department coordinating domestic and foreign operations, the senior positions of the personnel and training department, responsible for the practical execution of the merger, as well as the management of the Internal Security Directorate) went to officers from the Military Security Office. As a consequence, young, highly qualified, and language-savvy intelligence officers, NCOs, and civilian colleagues became redundant on fabricated reasons or security concerns. In contrast, many older, relatively unqualified intelligence officers who did not speak any language were brought in. Third, the majority of the upper management positions of the Military National Security Service were occupied by officers of the National Security Office, even though based on the pertinent legislation and the ministerial instructions, the Military Security Office was the organization to be disbanded and merged into the Military Intelligence Office when the latter organization only changed in its name (Military National Security Service). The predominance of military counterintelligence and its values might facilitate the emergence of ungrounded caution and permanent suspicions in intelligence activities, adversely affecting the efficiency of foreign intelligence.

Based on the above, including the radical cut of the attaché office budgets, I am positive that in the first year of the merger, MNSS's foreign intelligence opportunities significantly narrowed down, but without compromising the performance of the basic task (continuous gathering of information in specific directions).

The most *important conclusions* and *lessons learned* from the reform of the Hungarian military intelligence services are the following:

1. As the internal intelligence (counterintelligence) service of a state gathers information domestically about Hungarian citizens, their activities require close control. In Hungary, in the case of the Military Security Office, this control was not efficient. Therefore, upon merging the two military intelligence agencies, counterintelligence had a better starting position and acquired a larger influence in the integrated organization than is its actual significance. This circum-

---

<sup>12</sup> Balfácán, "The Fifth Generation of Traitors;" Kenedli, "The Most Important Features of the Professional Development."

stance might affect the effectiveness of foreign intelligence for the years to come.

2. The integration of the two military intelligence agencies was not preceded by a thorough impact study supported by research. Staff reduction was executed like in the disciplined military, but the personnel requirements of the allocated tasks had not even been assessed. So, managers implementing the integration continuously faced the financial, human resources management, and professional integration challenges of mergers and reorganizations. They were eager to find the best solutions to the anomalies, yet this could not compensate for the inadequate reform preparation. This should serve as an example to be avoided by any country.

3. When merging two government offices, it is essential to respect professional considerations and political neutrality fully. These principles should also be respected in the appointment of members of the top leadership of the new organization. Unfortunately, this was not the case when the Hungarian military secret services were merged. The post of Deputy Director-General of the merged organization was given to the former "intelligence adviser" of the ruling party (Young Democrats – Fides), a patron of the speaker of Parliament, without a military degree and knowledge of any foreign language. His nearly one and a half year of activity has done a lot of harm to the new organization. The circumstances of his replacement are still obscure. According to the press, he wiretapped his superior, the Minister of Defense, and therefore had to resign. Further, a widespread view in the secret service circles claimed that he wanted to get the MNSS Director-General position without coordinating his actions with all the key figures in Fides.

4. The most used justification for all mergers is eliminating duplication of efforts between the organizations to be merged. In the case of military intelligence agencies (military counterintelligence and intelligence), this duplication may be present, but not to the extent where this could not be solved by the amendment of the respective organizations' operational and organizational policies.

5. If a counterintelligence officer sees a top-secret document left on the table, he/she will want to know who left it on the table. If an intelligence officer sees the same document, he/she will be interested in its content. The two functions require two different approaches and methodologies, not to mention the differences in the personality traits necessary for their performance. If both the intelligence and the counterintelligence officer perform their own task, it will most likely be clear to both who left the secret document on the table and also what the document contains. Official mutual information exchange can confirm the authenticity of the information obtained by the agencies independently from each other. The merging of military intelligence and counterintelligence is therefore not absolutely necessary. Still, the need for more effective action against new types of threats (e.g., hybrid warfare, information operations) may justify the merger.

## **Closing Remarks**

The history of the Military National Security Service dates back to the time between the two world wars. The current integrated foreign (external) and domestic (internal) intelligence organization was established in 2012 by merging the Military Intelligence Office and the Military Security Office of the Republic of Hungary. Despite many shortcomings in its preparation and implementation and the lessons learned, the merger was a success. The organization currently has a wide range of responsibilities: a collection of military information in foreign countries (including by secret means and methods) on which government decisions are based, detection of foreign military secret services' activities in Hungary and protection of Hungarian military units against them, protection of personnel involved in crisis response operations abroad, implementation of national security and lifestyle checks of Service's personnel, gathering information on terrorism and organized crime, cyber defense, and scientific activities. Civilian control of the Service is exercised through the Military and Law Enforcement Committee and the National Security Committee of the Hungarian Parliament. This parliamentary control is extremely important. Without full publicity, it is not possible to assure the citizens that the operation of the Service is not detrimental to their interests or that it is efficient from a budgetary point of view. However, it is not felt that the organization has an appropriate communication strategy to deal with the public. Although the instructions on external communication have been issued by the Director-General of the Service and the secret service nature of the organization should be acknowledged, the information content available on the Service's website does not help the organization's direct social acceptance and integration.

## **Disclaimer**

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

## **About the Author**

**Andras Huguik**, Ph.D. in military science, is a retired police colonel, a Chief Councilor of the Hungarian Police. He is a military engineer, investigator, and political expert. He is a former adviser to GUAM, OSCE, EUBAM, and UN – OPCW Joint Investigation Mechanism. Before joining the international organizations, he served in the Military Intelligence Office, the Protective Service of Law Enforcement Agencies, and the Counterterrorism Center of Hungary.  
E-mail: seniorhuguik@gmail.com





Research Article

## Intelligence and Security Services Reform and Oversight in Ukraine – An Interim Report

*Philipp Fluri*<sup>1</sup> and *Leonid Polyakov*<sup>2</sup>

<sup>1</sup> Wenzao University, Taiwan, <https://c041.wzu.edu.tw/>

<sup>2</sup> Center for Army, Conversion and Disarmament Studies, <https://cacds.org.ua/>

**Abstract:** Though Ukraine was among the first successor states of the Soviet Union to create a legal framework for the activities of its intelligence and security community, said framework addressed inherited and unreformed structures. Subsequent reform plans have not led to the success desired by Ukraine's international partners and, we must assume, a majority of the Ukrainian voters and taxpayers. Among the reform demands is also the credible subordination to parliamentary oversight, which, though stipulated by law, has effectively been neutralized by reference to subordination to the President in the same law. Who would want to be controlled by an ever-undecided parliament if a personalized oversight by the President and the expert committee of the National Security and Defence Council is the possible alternative? As a consequence, the Security Service of Ukraine (SSU) remains subject to much criticism – for the corruption of some of its representatives, for overlapping mandates with other security institutions, and for lack of control other than by itself and the changing presidents and their administrations.

**Keywords:** defense reform, intelligence reform, state security, state security reform, civilian oversight, parliamentary oversight, NATO, EUAM, DCAF, SSU, VR, Verkhovna Rada.

### Introduction

In this article, we will look at three intelligence services of Ukraine and recent developments in their legal, managerial, and oversight structures: the Security Service of Ukraine (SSU – Sluzhba Bezpeky Ukrainy SBU, we use 'SSU' for the purposes of this article), the Main Intelligence Directorate of the Ministry of De-

fense (Golovne Upravlinnia Rozvidky – GUR), and the Foreign Intelligence Service of Ukraine (Sluzhba Zovnishnioyi Rozvidky, further – SZR) – a political intelligence branch of the SSU, which was separated from the latter in 2005.

## A Brief History of Reform Plans for the SSU

The Security Service of Ukraine (SSU) is the state's special purpose law-enforcement body, and by the existing law entrusted with a variety of mandates: to protect state sovereignty, the constitutional order, territorial integrity, the economic, scientific and technical, and defense potential of Ukraine, the state's legal interests and civil rights from intelligence and subversion activities of foreign services and from unlawful interference of organizations, groups, and individuals. It is also tasked with ensuring the protection of state secrets.

Currently, the SSU has a number of functions that overlap with the mandates of other institutions, including the fight against corruption.<sup>1,2</sup>

With more than 30,000 employees, the SSU is more than seven times the size of the UK's comparable service, the MI5. The Service's agents perform not only traditional intelligence-gathering and counterintelligence roles but also such roles as combating economic crimes utilizing the SSU investigative powers, which in most Western democracies would be seen as law-enforcement functions. This conglomerate of functions, some of them overlapping with those of other services, have created a hybrid animal difficult if not impossible to control, whose activities over the years have been overshadowed by accusations of blackmail, abuse of power, corruption, secret jails, extortion, and links to Russian security – in short, a service which Western counterparts are hesitant to engage with. Repeated calls for reform, including from within the Service, have not yet led to desired results.

Early discussions on SSU reform took place during the years the Ukraine-NATO Joint Working Group on Defense Reform (2005-2009) was active. A streamlining of the SSU's functions was again stipulated in the 2014 Parliamentary Coalition Agreement. In early 2016, a permanent international advisory group on the SSU reform was established with the participation of the represent-

---

<sup>1</sup> The SSU was formed on September 20, 1990, as a successor service to the KGB branch in the Ukrainian SSR. As such it inherited all of the Ukrainian KGB's personnel. The need to reform the service and give it a national profile was seen immediately after independence. The Ukrainian Parliament, the Verkhovna Rada (VR), adopted the pertinent Regulation *On the Establishment of the National Security Service of Ukraine* on 20 September 1991, with the *Law On the Security Service of Ukraine* to follow on March 25, 1992.

<sup>2</sup> An English version of the currently valid Law "On the Security Service of Ukraine" (1992. Last revised in 2015) can be found in subsequent volumes of *The Security Sector Legislation of Ukraine* (published by NATO/DCAF/the Verkhovna Rada of Ukraine and the Defence and Security Council of Ukraine since 2002), e.g., in Oleksandr Lytvynenko, Philipp Fluri, and Valentyn Badrack, eds., *The Security Sector Legislation of Ukraine* (Geneva-Kyiv, 2017), 313-324, [https://www.dcaf.ch/sites/default/files/publications/documents/Security%20Sector%20Legislation%20Ukraine%202017\\_eng.pdf](https://www.dcaf.ch/sites/default/files/publications/documents/Security%20Sector%20Legislation%20Ukraine%202017_eng.pdf).

atives of the EU Advisory Mission for Civilian Security Sector Reform Ukraine (EUAM), the NATO Representation Office in Ukraine, the NATO Center for Information and Documentation in Ukraine, and other international organizations.<sup>3</sup>

A Concept paper for SSU reform based on NATO standards was drafted in July 2016 and submitted to state institutions for approval.

In March 2017, then-President Poroshenko announced a comprehensive reform of the SSU, aimed specifically at transferring part of its functions to other law-enforcement institutions – the National Anticorruption Bureau of Ukraine, the yet-to-be-organized State Bureau of Investigations, and the National Police.

Poroshenko also claimed that the reform would introduce civilian parliamentary oversight of the SSU. The National Security and Defence Council of Ukraine (NSDC) was supposed to review the Concept without delay. This is where the process has been stalling since, and revision of the existing Law on the Security Service of Ukraine effectively delayed.<sup>4</sup>

A comprehensive summary of the reform arguments *pro* and *con* can be found in the *Proceedings of the Third International Conference on Governance and Reform of State Security Services in the Monitoring Ukraine's Security Governance Challenges* cycle.<sup>5</sup> It made the resistance of substantive parts of the staff to reforms (in times of war!) obvious, along with the relative powerlessness of civil society and the international advisors (the latter in fact going back to the activities of the Ukraine-NATO Joint Working Group on Defence Reform in 2005-2009).

In a gesture of openness, Andriy Bodrunov of the SSU Centre for Reform Support introduced the draft Concept of SSU Reform and the Plan for its Implementation until 2020<sup>6</sup> to a public conference in 2017. The plan for self-reform of the service foresaw, *inter alia*, the legislative separation of SSU tasks and powers

---

<sup>3</sup> NATO representatives and European Union Advisory Mission in Ukraine (EUAM) collaborators even drafted a reform proposal in 2016 that was intended to name the necessary ingredients of such a reform policy in light of NATO member countries best standards. The proposal suggested to eliminate SSU law-enforcement functions and hand them over to the newly established National Anti-Corruption Bureau (NABU) and the National Police. That would leave the SSU to work strictly as an intelligence agency, focusing on counterespionage, counterterrorism, cybersecurity, and security analysis.

<sup>4</sup> An argument frequently raised against parliamentary oversight is the allegation that MPs lacked the proper understanding of both intricacies of security work and its pre-conditions, such as secrecy. This in spite of the presence of retired intelligence officers among MPs – a fact which caused to the former Deputy Chairperson of the VR Oksana Syroid to speak of a “clash of civilisations” within the very parliament. See Philipp H. Fluri and Oleksiy Melnyk, eds., *Citizens of Ukraine on Security: Personal, National, and its Elements - Survey 2* (Geneva/Kyiv, 2017), 11. Admittedly, subsequent parliaments have interpreted parliamentary immunity rather indulgently – for a discussion on parliamentary ethics and its excesses see Irina Suslova, Philipp Fluri, and Valentyn Badrack, *Parliamentary Ethics in Ukraine* (Kyiv-Geneva, 2017) [in Ukrainian].

<sup>5</sup> Fluri and Melnyk, eds., *Citizens of Ukraine on Security*. Electronic versions of the publication to be found on [ukrainesecuritysector.com](http://ukrainesecuritysector.com), and [academia.edu](http://academia.edu).

<sup>6</sup> Fluri and Melnyk, eds., *Citizens of Ukraine on Security*, 16-19.

from those of other intelligence and law-enforcement bodies of Ukraine, including those newly established, as well as the elimination of functions alien to the mandate of the SSU; the establishment of a credible civilian democratic oversight; the optimization of the organizational structure and adequate staffing, including the elimination of structures alien to the mandate; the provision of proper legal and social protection of service personnel; and the greater involvement of the special services of the SSU in international cooperation.<sup>7</sup>

As major objectives of the reforms were named increased public trust in the Service, including respect for its representatives; the enhancement of institutional capabilities of the Service as a specialized state body in the field of counterintelligence and the protection of state secrets, and as the main body within the national system for fighting terrorist activities; the separation of functional tasks and powers of the Service and other law-enforcement bodies and state bodies fighting corruption and organized crime, and protecting state interests in the economy, information and cyber sectors; a limitation of the pre-trial investigative powers of the Service, and the gradual demilitarization and optimization of the ratio of military to civilian positions in the Service in line with Ukraine's changing security environment.

### **SSU Reform in the Zelensky Era**

In his inauguration speech on May 20, 2019, Ukrainian President Zelensky called on the Verkhovna Rada (VR, the Parliament of Ukraine) to dismiss the heads of the SSU, the Prosecutor General's Office, and the Defense Minister. SSU Head Vasyl Hrytsak then reportedly resigned on his own initiative.

New hands in both government and the international advisory teams took over after the 2019 elections, which brought a newly established political party to power, proving a rather complete disenchantment with 'old' elites (including those favored by Western political parties).

The slow reform of the SSU was again seen as a priority by the Deputy Head of the EU Advisory Mission Frederik Wesslau:

As for the reform of the Security Service of Ukraine, I think it is one of the most challenging but also one of the most needed reforms. It will require strong political will.<sup>8</sup>

According to Wesslau, the reform of the Security Service of Ukraine and parliamentary control are important because this will make the security sector more transparent and efficient and will increase the level of trust in Ukrainian security agencies. This would also strengthen democracy in the country. Reportedly,

---

<sup>7</sup> Whereas it is true that cooperation between the SSU and Western services goes back to early post-Soviet years it is equally true that full cooperation among equals including comprehensive data exchange has not taken place until today (the authors).

<sup>8</sup> "Wesslau: Reform of Ukraine's Security Service Is One of the Most Needed," *ukrinform*, May 23, 2019, <https://www.ukrinform.net/rubric-defense/2706674-wesslau-reform-of-ukraines-security-service-is-one-of-most-needed.html>.



“Zelensky and his team understand the need to report and set it as one of their priorities.” According to Wesslau, drafted laws on reform will need to be reviewed: “we have seen the draft laws and do not think they meet Euro-Atlantic standards.”<sup>9</sup> That especially refers to parliamentary control. A further crucial aspect of interoperability was said to be the civilianization of the Service.

An International advisory group composed of representatives of the European Union, NATO, and the US participated in an August 13, 2019 meeting with (then acting) SSU head Bakanov and National Security and Defense Council chief Danyliuk on SSU reforms. Danyliuk was quoted by the BBC Ukrainian Service as saying a law was in preparation that would strengthen the SSU’s core functions of “counterintelligence and combating terrorism.”

## **SSU Reform – Interim Observations**

In its own Ukrainian way, and possibly not yet adequately appreciated by its Western partners, the SSU has implemented at least some of its self-declared reform steps. Thus, the Service is about to succeed in giving itself a people-friendly image, protecting people’s interests, and the nation’s national and human values.

Public relations have become an important part of the image change. The Service frequently informs about its operations.

However, as long as the SSU remains porous vis-à-vis the Russian Security Service, with an over-fraught mandate, military structures, and without a credible parliamentary oversight by a credible parliamentary committee or subcommittee, Western services can be expected to stay at a distance.<sup>10</sup>

## **Simple and Mixed Examples of Reform: GUR and SZR**

### ***Military Intelligence – GUR***

Rather different from the complex and heavily charged story of SSU is the simpler case of the Main Intelligence Directorate of the Ministry of Defense (Golovne Upravlinnia Rozvidky, further – GUR). The founders of the GUR had prior experience of service in the KGB military counterintelligence and the GRU

---

<sup>9</sup> “Wesslau: Reform of Ukraine’s Security Service.”

<sup>10</sup> Among the spectacular defections was former SSU head Oleksandr Yakymenko’s flight to Russia, days after pro-Russian president Yanukovich had fled the country. Along with Yakymenko thousands of highly classified documents were said to have been irretrievably gone missing. After the Russian invasion of the Crimea a substantive number of Ukrainian SSU collaborators switched sides, not all of them leaving the Service. On April 14, 2020, the SSU announced the arrest of LTG Valeriy Shaytanov who had headed the anti-terrorist division playing a prominent role in negotiating ceasefires and prisoner exchanges with Russia-backed militants in Eastern Ukraine (April 14, 2020 15:58 GMT/RL Ukrainian Service). Shaytanov stands accused of having provided information to Moscow about secret operations against Russia-backed separatists in eastern Ukraine and having recruited additional agents.

(Glavnoe Razvedyvatelnoye Upravleniye) the Soviet Army's General Staff. However, contrary to the SSU, the GUR was created from scratch once Ukraine became independent from the USSR, and with a rather clear mandate. This naturally freed the GUR from the tail of bad habits and helped to build a purely national military intelligence agency in terms of spirit, organization, and oversight.

For about three decades, one did not hear much criticism of the agency, whether about its performance or its organization, which does not mean that there were no problems. Insiders and knowledgeable experts are aware of certain issues of personnel and operational-related nature, but these issues never caused much attention outside of the intelligence community. Besides, from the start of Russian aggression in 2014, the overall performance of the GUR has been seen mainly as positive.<sup>11</sup> At least in the public eye.

Consequently, there was and is not much talk about reform of the GUR as an organization, especially when compared with SBU. However, in terms of democratic oversight standards, there are some nuances definitely deserving closer attention.

Though an agency formally subordinated to the MoD, the GUR *de-facto* enjoys a significant degree of independence from the Minister of Defense in terms of the budget and subordination. First, the GUR has its own line in the state budget completely independent of the MoD budget. Second, because of the complexity in the chain of command, where GUR is positioned as a servant of three masters. In addition to the traditional two—the civilian Minister of Defense and the uniformed general Commander-in-Chief of the Armed Forces—the Head of GUR has a direct reporting line to the Supreme Commander-in-Chief of the Armed Forces, the President. In the latter case, it means talking regularly not only to the President but also to select officials of the Presidential Administration and the leadership of the National Security and Defense Council headed by the President. Some former Heads of GUR were allegedly seen more often in the Presidential Administration than in the MoD.

In case the Head of GUR is a seasoned diplomatic person, this complexity in the executive oversight may not be a problem for GUR itself. However, this triple subordination contributes to the political weakening of the position of the Minister of Defense. It further limits the instruments of administrative control of the minister, who has no control over military counterintelligence (which belongs to the SSU), a merely symbolic military police (lacking operational-investigative powers), and limited control over military intelligence.

---

<sup>11</sup> "(The) Ukrainian defense intelligence and the State Border Guard Service's intelligence arm are widely judged to have been performing effectively since the beginning of the 'hybrid war' with Russia." Maksym Bugriy, "Intelligence Reform in Ukraine Falls Short," *Eurasia Daily Monitor* 14, no. 106, September 6, 2017, <https://jamestown.org/program/intelligence-reform-in-ukraine-falls-short/>.

## **Foreign Intelligence – SZR**

GUR's sister agency—the foreign intelligence service of Ukraine (Sluzhba Zovnishnioyi Rozvidky, further – SZR)—is a political intelligence splinter of the SSU, which was separated from the latter in 2005.<sup>12</sup> Therefore, internally, it inherited the institutional cultures and structures from the SSU. However, it inherited neither the political status and influence of the SSU nor (what became a real problem after the start of Russian aggression in 2014) an appropriate budget (which it still had while being part of the SSU).

Compared with SSU and GUR, the SZR is neither a simple nor a complex example of intelligence reform. On the one hand, there is a clear chain of command – the Head of the SZR is directly subordinated to the President. But on the other, in the absence of effective parliamentary control over intelligence in terms of proper expertise and oversight of personnel appointments, the Head of SZR and his deputies are hostages to one person's personal preferences and interests, of the President only. As a result, Ukraine has seen periods, even during the war, when the unwelcome Head of SZR could not personally meet the President for a very long time. Moreover, at times the top position at SZR has been vacant for over a year. Or recall the recent chain of appointments to the Head of SZR post for a period of just a few months.

Yet another side of the lack of effective parliamentary control over intelligence and unstable political support for the SZR in the Presidential Administration was the chronically low budget of the SZR. Between 2014 and 2018, it was critically low.<sup>13</sup> For any intelligence service in a global environment, operating without money is close to nonsense. It is a big risk to national security, especially when at war with a regional superpower, heavily relying on its foreign intelligence instruments. Therefore, looking at the budgetary numbers, one does not need insider's knowledge to conclude that the foreign intelligence service of Ukraine is weak and in need of reform, including budgetary reform.

As in the case of the SSU, there was not much evidence of any plan to reform the SZR for many years.<sup>14</sup> In 2017-2019, facing growing criticism from the parliamentary committee on security and defense and the interested public, certain reforms of the SZR were conducted in accordance with the top-secret decree by President Petro Poroshenko, *"On the Concept of Reforming the Foreign Intelli-*

---

<sup>12</sup> For details on the SZR earlier years, see: Leonid Polyakov, "Paramilitary Structures in Ukraine," in *Almanac on Security Sector Governance in Ukraine 2010*, edited by Merle Maigre and Philipp Fluri (Geneva: DCAF, 2010), 125-187, <https://ukrainesecuritysector.com/wp-content/uploads/2016/01/Almanac-on-Security-Sector-Governance-in-Ukraine-2010.-english.pdf>.

<sup>13</sup> See: "Foreign Intelligence Service Received only 8 % of What it Needs, – MP Levus," *CENZOR.NET*, June 21, 2017, [https://m.censor.net/news/445005/slujba\\_vneshneyi\\_razvedki\\_profinansirovana\\_tolko\\_na\\_8\\_ot\\_potrebnosteyi\\_nardep\\_levus](https://m.censor.net/news/445005/slujba_vneshneyi_razvedki_profinansirovana_tolko_na_8_ot_potrebnosteyi_nardep_levus).

<sup>14</sup> "The attitudes toward the complex task of reforming the SSU or the Foreign Intelligence Service could, heretofore, probably best be characterized as if it's not broken, don't fix it." Bugriy, "Intelligence Reform in Ukraine Falls Short."

*gence Service of Ukraine in Accordance with NATO Standards*” of July 30, 2018. The SZR budget started to grow steadily from then on.<sup>15</sup>

Nevertheless, President Volodymyr Zelensky, elected in 2019, was apparently not impressed by the performance of the allegedly reformed SZR. During his first year in office, he substituted heads of the agency three times. In June 2020, during the ceremony of the introduction of his third appointee, former Head of GUR (in 2015-2016), LTG Valeriy Kondratiuk, President Zelensky specifically underlined the need for SZR reform and expressed expectations that the new Head would be able to conduct it successfully.<sup>16</sup>

## Conclusions

Among the three services discussed, the creation of the Military Intelligence Service GUR was the least problematic. The SSU will remain problematic, at least in the eyes of Western experts and potential partners for closer cooperation, as long as its profile remains ‘mixed’ and thus indebted to the Service’s past, combining intelligence with law-enforcement functions. The ‘cultural’ revolution necessary to make such transformation possible has not yet taken place. Subsequent teams of Western advisors to the Service *and* the political decision-makers, including in the VR, will have to deal with this.

To a degree, the slow pace of reforms in primary Ukrainian intelligence services is a result of being held hostage to the pace of political developments in Ukraine. Weak parliamentary control (inability to create an intelligence committee in the parliament), complicated system of executive control – all contributed to problems with intelligence budgets, delays upon delays in SSU reforms, agencies’ leadership reshuffles, and limited cooperation with foreign partners from democratic countries.

---

<sup>15</sup> See: “The Head of the Foreign Intelligence Service gave an interview for the journalists of LB.ua,” *LB.ua*, January 24, 2019, [https://lb.ua/news/2019/01/24/417974\\_egor\\_bozhok\\_v\\_rf\\_reshenie.html](https://lb.ua/news/2019/01/24/417974_egor_bozhok_v_rf_reshenie.html).

<sup>16</sup> See: “Zelenskyi set the task to reform the Foreign Intelligence Service,” *UKRINFORM*, July 6, 2020, <https://www.ukrinform.ru/rubric-politics/3041917-zelenskij-porucil-reformirovat-sluzbu-vnesnej-razvedki.html>.

## **Disclaimer**

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

## **About the Authors**

Dr. **Philipp H. Fluri** - see the short CV on p. 7 of this issue

**Leonid Polyakov** is a former Deputy Defence Minister of Ukraine. Currently, he chairs the Expert Council at the Ukrainian think tank Center for Army, Conversion, and Disarmament Center.

E-mail: leonpol2006@gmail.com





## Infogate Influences on Reforms of South Africa's Intelligence Services

*Glen Segell*

*Department of Political Studies and Governance, University of the Free State, South Africa, <http://www.ufs.ac.za>*

**Abstract:** The hypothesis is that intelligence reform and intelligence sector reform result from traumatic catalyst rather than gradual evolution, reactionary rather than proactive, and not soon or quickly. The threat environment, an emergency, a necessity, e.g., democratization, gross failure, and scandals, are causes for reforms. The case is South African intelligence services. South Africa is significant due to diverse and constantly changing operational environments: the Cold War, decolonization of Africa, apartheid, post-Cold war, and post-Apartheid democratization. From the first non-military intelligence agency created in 1968, the Bureau of State Security, it was clear the nature of intelligence was such that the balance between secrecy, transparency, and accountability would always be a fine one to strike. The relationship between the political echelons, e.g., the Prime Minister and the Bureau's Director, was too close and so allowed misuse of state funds. The uncovering of the abuse of state funds, the Infogate scandal, had an influence on subsequent reforms, including those for democratization to abolish apartheid and introduce a "one-man, one-vote democracy," achieved in 1994. Reforms through legislation, jurisdictions, restructuring, micro-managing intelligence, merging apartheid and opposition intelligence services, and creating post-apartheid intelligence services are examined in this article. The experience teaches us that errors can be avoided by not making uncoordinated, piecemeal changes; every reform is unique and rarely easy; operationalizing legislative mandates of transformation is more difficult than anticipated. The reform process starts with reflecting the envisaged ideal situation, yet the outcome is not always as expected and thus requires more reforms.

**Keywords:** South Africa, Infogate, intelligence reforms, intelligence sector reforms, democratization, Cold War, Apartheid.

## Introduction

The hypothesis underlying this article is that intelligence reform and intelligence sector reform tend to result from traumatic catalyst rather than gradual evolution. Hence, reforms are more reactionary than proactive. Unless there is a specific necessity, then reform will not happen soon, quickly, or ever. Typically, an intelligence agency is created due to the threat environment or an emergency and is disbanded as a result of a change in the threat environment. Among other necessities are, for example, democratization, a gross failure, or a scandal.

This hypothesis is examined in the case of the South Africa intelligence services. There has been continuous reform due to a changing threat environment, for example, decolonization in Sub-Saharan Africa, the Cold War, the Apartheid era, and the post-Cold war and post-Apartheid eras. They went hand-in-hand with introducing a “one-man, one-vote democracy” that was achieved in 1994. The reforms examined in separate sections in this article involve changes in legislation and jurisdictions, restructuring, micro-managing intelligence, merging apartheid and opposition intelligence services, and creating post-Apartheid intelligence services.

The premises of the hypothesis were evident from the onset with the creation of the first non-military intelligence agency in 1968, the Bureau of State Security (BOSS). From the onset, it was also apparent that the nature of intelligence was such that the balance between secrecy, transparency, and accountability would always be a fine one to strike. The relationship between the political echelons, including the Prime Minister and BOSS’s Director, were too close and so allowed state funds to be misused.

An intelligence service must not influence government policy, engage in acts of surveillance of the population and violence en masse, violate citizens’ rights and abuse them, and misuse state funds. For in a democracy, the intelligence services should serve the state and not the opposite. Yet, this is what happened in BOSS. Maybe because South Africa under Apartheid (1948-1994) was not a democracy. Most of its citizens who were non-white were denied through legislation to elect or be elected. There was no accountability and transparency of government activities, actions, and the use of state funds that are usually to be found in a democracy.

The uncovering of the misuse of state funds is known as the Infogate scandal. All subsequent reforms, including those to suit new operational environments and democratization, were all influenced by the trauma of this gross misconduct. The following reforms had the transparency in the use of state funds as their key element and aimed to make the intelligence sector more accountable for its actions and activities.

The lessons from creating BOSS and subsequent reforms (1968-1998) are that every reform is unique. Reform is almost never easy. In tense situations that require reforms, errors can be avoided by not making uncoordinated, piecemeal changes. Operationalizing any changes that include legislative mandates of transformation is always more difficult than anticipated. There are no good



sources about the future, so while the process to be addressed in reform starts with reflecting the envisaged ideal situation, the outcome is not always expected. And while there was a linked process of democratization to end apartheid, with that of intelligence reform and intelligence sector reforms, they should have begun earlier rather than later.

## **Intelligence Services Requirement**

The Union of South Africa was formed in 1910, in the aftermath of the Anglo-Boer War (1899-1902), by merging two former British colonies, the Cape and Natal, and two independent states, The Transvaal and the Orange Free State. The National Party won the post-World War II elections and introduced in 1948 a legislated system of racial segregation known as the Apartheid Laws. In 1961 the National Party declared South Africa a Republic and left the British Commonwealth. The Apartheid was a political system with the legislated white rule only by descendants of European settlers and the subjugation of all indigenous non-white people, who did not have the right to elect or be elected.<sup>1</sup>

The South African security services were entrusted with enforcing the Apartheid policies. Their activities, successes, and failures were in part shaped by the de-colonial process faced by neighboring states in sub-Saharan Africa and by the Cold War. South Africa was rationalized as being in the Western Bloc because it was not communist and because it was fighting counter-insurgency campaigns against Eastern Bloc forces. Yet, South Africa had little or nothing in common with other Western Bloc countries and had no formal treaty ties. It was capitalist but not democratic because of apartheid.<sup>2</sup>

Western states friended South Africa because it was located geo-strategically at the southern tip of Africa where the Atlantic and Indian Oceans meet. Its sea routes and ports were of strategic importance for Western Europe and North America for trading with the Far East because the large oil tankers from the Middle East could not navigate the Suez Canal, and during Middle East wars, the Suez Canal was closed.<sup>3</sup>

South Africa was fighting against Eastern Bloc-supported forces domestically and externally. Domestically for the anti-Apartheid movement was supported by the Eastern Bloc. The Soviet view was that Apartheid was Imperialist. So, anti-Apartheid forces such as the African National Congress (ANC) were sponsored by the Eastern Bloc as a colonial struggle. These forces conducted guerrilla and terrorist activities within South Africa from 1961 until the end of apartheid in 1994

---

<sup>1</sup> Roger B. Beck, *The History of South Africa* (Westport, CT: Greenwood Press, 2013), 3-10.

<sup>2</sup> William Blum, *West-Bloc Dissident: A Cold War Political Memoir* (New York: Soft Skull Press, 2001), 190.

<sup>3</sup> Irina Filatova and Apollon Davidson, *The Hidden Thread: Russia and South Africa in the Soviet Era* (Johannesburg: Jonathan Ball, 2013), 23.

as part of the freedom movement struggle. There was active Soviet Union involvement, for example, led by KGB Colonel Joe Slovo. South Africa went so far as to attempt to assassinate him but only succeeded in killing his wife, Ruth.<sup>4</sup>

South Africa was also fighting against Eastern Bloc communist forces externally, for example, against Cuban and East German troops and the local forces that they supported in the de-colonial independence struggles in the neighboring states of Angola, Mozambique, and Rhodesia (now Zimbabwe). The aim of the involvement of the South African security services in the regional sub-Saharan Africa conflicts was to create buffer zones against encroaching communist forces aimed at toppling the Apartheid regime.<sup>5</sup>

### The Birth of the Intelligence Service BOSS

In 1963, Mr. B.J Vorster, the Justice Minister under Prime Minister H.F. Verwoerd, examined the option to form South Africa's first non-military intelligence agency in addition to its small military intelligence gathering capability. There was growing resistance against apartheid, for example, the Sharpeville incident in 1961.<sup>6</sup> After Voster became Prime Minister in 1966, there were the first skirmishes between South African military forces and Eastern Bloc forces in the Caprivi Strip bordering Angola and South-West Africa (now Namibia).

Based on these perceived security needs, both domestically and externally, the South African Cabinet approved in 1968 the implementation of a new centralized security service called the Bureau of State Security (BOSS). Its first Director would be General Hendrik van den Bergh of the South African Police Security Branch. He was a close confidant of Prime Minister Voster since the 1940s. He was also appointed as Security Advisor to Vorster. Attached to the Prime Minister's office, he would be in command of all security and intelligence chiefs in the country, including the military, and report only to Vorster.

BOSS became more than an intelligence service and was well known for atrocities. Although van den Bergh denied BOSS's use of hit squads against its enemies, he is nevertheless remembered for sanctioning the use of torture, assassinations, and other tactics against the government's enemies, and he once told a government commission, "I have enough men to commit murder if I tell them to kill. I don't care who the prey is. These are the type of men I have."<sup>7</sup>

---

<sup>4</sup> Alan Wieder, *Ruth First and Joe Slovo in the War Against Apartheid* (Auckland Park, South Africa: Jacana, 2013), 57.

<sup>5</sup> Chris Saunders, "South Africa's War, and the Cuban Military, in Angola," *Journal of Southern African Studies* 40, no. 6 (2014), 1363-1368, <https://doi.org/10.1080/03057070.2014.964933>.

<sup>6</sup> Ron Nixon, *Selling Apartheid: South Africa's Global Propaganda War* (London: Pluto Press, 2016), 12-14.

<sup>7</sup> Peter Parker and Joyce Mokhesi-Parker, *In the Shadow of Sharpeville: Apartheid and Criminal Justice* (London: Palgrave Macmillan, 1998), 121.

## **The First Reform: Legislation**

On May 13, 1969, Minister of the Interior S.L. Muller introduced the framework of BOSS in the "Public Service Amendment Bill (1969)," which he said was responsible only for "coordination" and would draw personnel from other security and intelligence organizations. It outlined that BOSS's control would rest with the Prime Minister and that the civil service Public Service Commission would have no control over its powers, functions, and duties.<sup>8</sup>

The data shows that the release of the expenditures for the next Tax Year April 1969/ April 1970 saw an increase of 188% over the previous year to BOSS. On the other hand, Military Intelligence's (MI) budget was reduced from the previous year by two-thirds. This led to a publicized struggle between MI and BOSS.<sup>9</sup> To hide this, a week later, the "Security Services Special Account Bill (1969)" was passed, which saw the use of money allocated to BOSS as confidential. This effectively halted the public feud and ensured that BOSS would not be subject to an audit by the Auditor-General as other government departments.<sup>10</sup>

Moreover, the "General Law Amendment Bill (1969)" was passed that prevented the Prime Minister, van den Bergh or cabinet ministers from giving evidence or producing documents in court that might prejudice state security. This caused outrage throughout the South African legal community, who considered that it could no longer protect citizen's rights from the Government executive.<sup>11</sup>

## **The Second Reform: Jurisdictions**

Perhaps because of this outrage on September 5, 1969, Prime Minister John Vorster announced the formation of a commission led by Justice H.J. Potgieter to establish the guidelines and mission for BOSS. In practice, however, the "Commission to Inquire into Certain Intelligence Aspects of State Security," known better as the Potgieter Commission, was only tasked to investigate the clashes between BOSS and MI and define who had primary responsibility for intelligence gathering in South Africa.<sup>12</sup>

---

<sup>8</sup> South African Government, "Public Service Amendment Bill (1969)," accessed September 3, 2020, <http://www.saflii.org/za/cases/ZARMC/1969/2.pdf>.

<sup>9</sup> Alex Hepple, "South Africa's Bureau for State Security," *The World Today* 25, no. 10 (October 1969), 436–439.

<sup>10</sup> South African Government, "Security Services Special Account Act 81 of 1969," accessed September 3, 2020, <https://www.gov.za/documents/security-services-special-account-act-20-may-2015-1043>.

<sup>11</sup> South African Government, "General Law Amendment Act 101 of 1969," accessed September 3, 2020, <https://www.gov.za/documents/general-law-amendment-act-20-may-2015-1017>.

<sup>12</sup> "Prime Minister John Vorster appoints a Commission of Inquiry under Justice H.J. Potgieter, of The Appellate Division of the Supreme Court," *South African History Online*, accessed September 3, 2020, <http://www.sahistory.org.za/>.

The Potgieter Commission took its time and only reported back on February 2, 1972, leading to the "Security Intelligence and State Security Council Act (1972)." The Act would form the State Security Council under the control of the Cabinet and establish it as the government's national center for operational security. The BOSS head van den Bergh, who was a close ally of the Prime Minister, was favored by the Act giving him greater power beyond just overseeing a "co-ordinating service." It enabled him to influence all aspects of South Africa's policy on subversion, counterespionage, and political and economic espionage.<sup>13</sup>

By 1975 the anti-Apartheid movement intensified with increased Eastern Bloc support. The neighboring states of Angola and Mozambique that had been Portuguese colonies attained independence after a regime change in Portugal, and Rhodesia (now Zimbabwe) was in an all-out civil war. The government feared that South Africa would be next. The government was divided on how best to counter the Soviet involvement in Angola that threatened to spread south and into South Africa. Defense Minister P.W. Botha and the Chief of the Army General Magnus Malan advocated an all-out invasion into Angola to end the Soviet involvement. On the other hand, Prime Minister Vorster and General van den Bergh favored only a limited, covert operation into Angola.<sup>14</sup>

The latter option was chosen, though the South African military intervention in Angola failed. In sight of the Angolan capital, South African forces were repulsed by a fresh influx of Cuban troops. The United States, which had covertly backed the operation, was forced to withdraw its support when the American Congress vetoed the American President Ford administration's request for funding. As a result, South Africa was forced to withdraw from Angola and then faced a protracted counter-insurgency war in South West Africa that bordered Angola until the former became independent as Namibia in 1989.<sup>15</sup>

Although it was a military operation, BOSS became involved in the Angolan war. It should have been the role and task of Military Intelligence to handle all matters in that conflict. The BOSS involvement was understood because of the close relationship between van den Bergh, head of BOSS, and Prime Minister Vorster. This bothered the then Minister of Defense, P.W. Botha, as BOSS had become increasingly powerful to the point where it wielded more influence than both the Ministries of Defense and Foreign Affairs.<sup>16</sup>

---

<sup>13</sup> "Security report by Justice H.J. Potgieter's Commission of Inquiry on State Security," *South African History Online*, accessed September 3, 2020, [www.sahistory.org.za/](http://www.sahistory.org.za/).

<sup>14</sup> Jannie Geldenhuys, *At the Front: A General's Account of South Africa's Border War* (Jeppestown: Jonathan Ball, 2009), 63-65.

<sup>15</sup> Elaine Windrich, *The Cold War Guerrilla: Jonas Savimbi, the U.S. Media and the Angolan War* (New York: Greenwood Press, 1992), 145.

<sup>16</sup> James Barber and John Barratt, *South Africa's Foreign Policy: The Search for Status and Security, 1945-1988* (Cambridge: Cambridge University Press, 1990), 327.

## **The Infogate Scandal**

The close relations of Prime Minister Voster to BOSS's van den Bergh led to the Infogate scandal. The scandal resulted from one of many strategies promoted and implemented by BOSS – engage in information operations, a propaganda war, both for apartheid and against the Eastern Bloc threat domestically and externally. The goal of the strategy was to influence the local and global media and hence the opinion of both public and political leadership. The ends were seen to be essential or even existential for these projects. The tactics, or means, would be to create front organizations and media projects.

The scandal was a greying of the lines of legality in the allocation of funds and the shifting of funds from the defense budget to BOSS. The illegality was the masking or covering of the funding from the normal governmental audit process, in sum, misappropriating and misusing state funds which BOSS had masked for secret front organizations and media projects.<sup>17</sup>

The change in the country's leadership would lead to a change in the entire scheme of such things. On October 2, 1978, B.J. Vorster resigned as Prime Minister to become State President. On October 9, 1978, Defense Minister P.W. Botha was appointed as the new Prime Minister. The decade-long struggle of roles and funding between BOSS and Military Intelligence would lead the former Defense Minister as the new Prime Minister to examine all aspects of BOSS.<sup>18</sup>

The issue that alarmed BOSS was the future of its clandestine projects and their funding. Fearing this, BOSS officials shredded any document that could be used against them. Despite this attempt, they would be unmasked due to another investigation.<sup>19</sup>

This investigation was initiated in the autumn of 1978 by the Minister of Finance, Owen Horwood, under the auspices of Judge Anton Mostert to probe exchange-control monetary violations. Justice Mostert informed the public of the scandal on November 3, 1978, with the newspaper heading "It's all True." The Rand Daily Mail newspaper broke the story of its opposition newspaper The Cit-

---

<sup>17</sup> Graham Macklin, "The British Far Right's South African Connection: A.K. Chesterton, Hendrik van den Bergh, and the South African Intelligence Services," *Intelligence and National Security* 25, no. 6 (2010), 823-842, <https://doi.org/10.1080/02684527.2010.537879>.

<sup>18</sup> South African Government, *South African Department of Information Scandal: Erasmus Commission of Inquiry*, Reference FCO 105/175, The National Archives (TNA), Kew, United Kingdom.

<sup>19</sup> C. Barron, "The Judge Was a Pawn in PW's Cover-up Bid," *Sunday Times*, Insight, April 25, 1999, 3.

izen as being a government plot created using funding officially allocated to other purposes.<sup>20</sup>

Prime Minister Botha then instituted a judicial commission of inquiry into the whole affair of front organizations and masked funding under the chair of Mr. Justice Roelof Erasmus. The scandal was to culminate in the resignation of the State President, B.J. Vorster (former Prime Minister), and a Cabinet Minister, Dr. Connie Mulder. They, together with Dr. Eschel Rhoodie (Secretary of the Department of Information) and the chief of BOSS, General Hendrik van den Bergh were found to be the main protagonists in the illegal appropriation of state funds. In a spate of reforms due to the Infogate scandal, BOSS was replaced by the National Intelligence Service (NIS) in 1980.<sup>21</sup>

### The Third Reform: Restructuring

In October 1978, Deputy Defense and Intelligence Minister Kobie Coetsee was appointed by Prime Minister PW Botha to lead a commission of inquiry into intelligence gathering and who would be the lead agency. Reforms introduced intended to overcome the challenges and issues of financial misappropriation and the close collusion of appointed and elected officials.<sup>22</sup> Owing to trauma from the Infogate scandal, reviews, accountability and transparency, and division of authority would become a standard operating procedure for all subsequent reforms for the next 20 years.

The intelligence-gathering ability of BOSS was split amongst four agencies, the Department of Military Intelligence (DMI), a revised BOSS, the Security Branch of the Police, and various sections within the Foreign Affairs services. Yet, one dilemma was clear from the onset, that the rise of P.W. Botha to be Prime Minister was influenced by his former role as Minister of Defense. Accordingly, he wanted to see the South African Defence Force's (SADF) power increase in the Cabinet and, with that, the power of the Directorate Military Intelligence (DMI).<sup>23</sup>

The revised BOSS was brought under tighter control as a cabinet portfolio called National Security managed directly by Prime Minister Botha, who also held the Minister of Defense portfolio. He reformed BOSS into a new agency based around research and analysis and removed its covert operational function.

---

<sup>20</sup> South African Government, *South African Department of Information Scandal: Erasmus Commission of Inquiry*, Reference FCO 105/175, The National Archives (TNA), Kew, United Kingdom.

<sup>21</sup> South African Government, *South African Department of Information Scandal*.

<sup>22</sup> Petrus Swanepoel, *Really inside BOSS: A Tale of South Africa's Late Intelligence Service* (South Africa: Derdepoortpark, May 2007), 17-19.

<sup>23</sup> Chris Dempster, Dave Tomkins, and Michel Parry, *Fire Power* (London: Corgi Books, 1978), 33.

He transferred that to the Security Branch of the police. BOSS was then renamed the Department of National Security (DONS) with Alec van Wyk as its new head.<sup>24</sup>

Then a professor of political science from the University of the Orange Free State, Professor Niel Barnard, was appointed in November 1979 to form a new intelligence service. Barnard, whose doctorate dissertation had been on the "Total Onslaught" of communism and decolonization against Apartheid in South Africa, would take over the South African Department of National Security (DONS) after the retirement of van Wyk. The now newly named National Intelligence Service (NIS) was announced on February 6, 1980. Barnard forced the retirement of many of the previous BOSS/DONS personnel.<sup>25</sup>

### **The Fourth Reform: Micro-managing Intelligence**

By the early 1980s, South Africa under Apartheid was characterized by heightened repression, with intense surveillance of the domestic society and population. This was seen as required to maintain white control of the state and combat South Africa's non-white liberation movements banned in 1961. As the State of Emergency took effect in 1986, anti-apartheid activists were detained without trial, and hit squads eliminated scores of prominent activists. Legally sanctioned hit squads also conducted repeated assaults on neighboring countries against freedom fighter/ terrorist bases.<sup>26</sup>

Security policy and strategy were brought under the direct control of a State Security Council (SSC), chaired by the President. The SSC engaged in the micro-management of intelligence implemented as a National Security Management System (NSMS) aimed to ensure a "total strategy" with white political control by "winning hearts and minds" (WHAM). The NSMS was structured down to the local level with Joint Management Committees (JMC's). The intelligence forces were from both the military (Civil Cooperation Bureau) and the police (Security Branch). This was not too different from BOSS's propaganda projects in the 1970s, yet funding was independently audited.<sup>27</sup>

The Cold War ended in 1989, and Eastern Bloc forces withdrew from sub-Saharan Africa, for example, East German and Cuban troops. By then, there were no European colonies in Africa. Without this external threat, the South African military lost its predominant influence over political life in the country. And so,

---

<sup>24</sup> Maritz Spaarwater, *A Spook's Progress: From Making War to Making Peace* (Cape Town: Zebra Press, 2012), 87.

<sup>25</sup> James M. Roherty, *State Security in South Africa: Civil-military Relations Under P.W. Botha* (New York: M. E. Sharpe, 1992), 107.

<sup>26</sup> Harold Wolpe, *Race, Class, and the Apartheid State* (Trenton, NJ: Africa World Press, February 1990), 56-62.

<sup>27</sup> Annette Seegers, "South Africa's National Security Management System, 1972-90," *The Journal of Modern African Studies* 29, no. 2 (June 1991): 253-273, <https://doi.org/10.1017/S0022278X00002743>.

there was a need for further intelligence reforms. The NSMS, including the JMCs, was disbanded in 1989 by the last State President to preside over apartheid, President F.W. de Klerk. He reduced the SSC to an ordinary cabinet committee.<sup>28</sup>

## The Fifth Reform: Merging Apartheid and Opposition Intelligence Services

The next catalyst determining intelligence reforms to replace the NSM and JMC system was in August 1991. A National Peace Accord was accepted by all the major political parties to disband apartheid and introduce democratization. The Convention for a Democratic South Africa (CODESA), convened in December 1991, would see fruition in the “Transitional Executive Authority (TEC) Act (1993).”

Based on the TEC Act, the Sub-Councils on Defense, Law and Order, and on Intelligence were established. The Sub-Council on Intelligence proposed the creation of a national capability from the amalgamation of six disparate intelligence entities (Apartheid services, the liberation movements, and the former Bantustan states of Transkei, Ciskei, Venda, and Bophuthatswana) into two new civilian intelligence structures.<sup>29</sup>

The subsequent “White Paper on Intelligence (1994),” produced by the transitional government, was tasked with defining how to interpret and translate a broad definition of security into intelligence functions. Clearly influenced by the Infogate scandal, it determined the role of intelligence would be based on a premise written in Section 3.3, “Towards a new national security doctrine that would have emphasis on ‘transparency and accountability.’ In short, democratisation ensures ‘good governance.’”<sup>30</sup>

Further, the White Paper provided the policy framework for the development of the intelligence structures, which included domestic and foreign intelligence, military intelligence, and crime intelligence, as well as a mechanism for coordination (National Intelligence Coordinating Committee) and mechanisms for control and oversight, especially of the use of state funds. So that there could be no misunderstanding, Annexure A, “The Code of conduct for intelligence workers” was stipulated as (8) “Shall commit themselves to carry out their duties without

---

<sup>28</sup> Robert D’A. Henderson, “South African Intelligence Transition from de Klerk to Mandela: An Update,” *International Journal of Intelligence and CounterIntelligence* 8, no. 4 (1995): 471-485, <https://doi.org/10.1080/08850609508435299>.

<sup>29</sup> Timothy D. Sisk, “South Africa’s National Peace Accord,” *Peace & Change: A Journal of Peace Research* 19, no. 1 (January 1994): 50-70, <https://doi.org/10.1111/j.1468-0130.1994.tb00598.x>.

<sup>30</sup> South African Government, “Intelligence White Paper, 1994,” accessed September 1, 2020, <https://www.gov.za/documents/intelligence-white-paper>.



seeking personal gain or advantage by reason of the duties, facilities, funds, and knowledge entrusted to them.<sup>31</sup>

### **The Sixth Reform: Creating Post-Apartheid Intelligence Services**

In 1994, “one-man, one-vote democracy” was introduced in South Africa, thereby abolishing apartheid. The all-white National Party that had been in power since 1948 lost to the African National Congress, which has ruled since. There was no longer the external threat of the Cold War and Eastern Bloc forces in Africa supporting decolonization or an internal threat of militant anti-Apartheid forces. With this came commissions of inquiry into the intelligence services, the role the services play in the government, and how they help shape government policy.

The same essential procedures for overcoming challenges and issues that Prime Minister Botha had applied in 1978 to terminate BOSS after the Infogate scandal were also applied by the new President Nelson Mandela in 1994, as South Africa's first non-white President. These were a review of the means to meet the needs, a change in the security and intelligence services' structure to serve this, a change in those heading them, legislation to ensure checks and safeguards, and a structure for independent auditing of finances.

Democratization led the process where the “South Africa Constitution (1994)” reflects key departure points for all the security services in Article 198 (4) “The security services must be structured and regulated by national legislation.” And following this Article 210, “the coordination of all intelligence services; and civilian monitoring of the activities of those services by an Inspector appointed by the President.”<sup>32</sup>

In conforming to this, the “National Strategic Intelligence Act (1994)” brought into existence two civilian intelligence services, one for domestic intelligence, the National Intelligence Agency (NIA), and another for foreign intelligence, the South African Secret Service (SASS).<sup>33</sup>

To ensure accountability and transparency of these, in the Parliamentary process that debates and votes on the annual budget for the state, multi-party parliamentary committees were formed. Their purpose was to execute legislative oversight of the intelligence domain, including the use of state funds. In addition, various mechanisms were created by the “Intelligence Services Oversight Act (1994),” for example, the Joint Standing Committee on Intelligence (JSCI), and

---

<sup>31</sup> South African Government, “Intelligence White Paper, 1994.”

<sup>32</sup> South African Government, *The Constitution of the Republic of South Africa, 1996*, accessed September 1, 2020, <https://www.justice.gov.za/legislation/constitution/SACConstitution-web-eng.pdf>.

<sup>33</sup> South African Government “National Strategic Intelligence Act, 1994,” accessed September 1, 2020, [https://www.gov.za/sites/default/files/gcis\\_document/201409/act39of1994.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/act39of1994.pdf).

the Inspector General (appointed by the President after nomination by the JSCI and approved by Parliament).<sup>34</sup>

Due to the trauma of the Infogate scandal, where the undue closeness of individuals led to the misuse of state funds, the Act created the National Intelligence Coordinating Committee. Among other things, it would oversee the use of funds and would report to the whole Cabinet. It would also prioritize intelligence activities within the intelligence community.<sup>35</sup>

Lessons gained from the Infogate trauma, where BOSS and Military Intelligence (MI) had clashed, were incorporated into the “White Paper on Defense (1996).” Section 1.1 places emphasis on “openness and accountability.” Section 11.2 obligates defense intelligence services to the same legislation as non-military intelligence services and so too to accountability and transparency, including for the use of state funds. Section 4 gives the Joint Standing Committee on Defense and the Joint Standing Committee on Intelligence in Parliament oversight powers on intelligence.<sup>36</sup>

In 1996, to prevent the situation whereby BOSS had dominated, as one agency, all domestic as well as foreign intelligence and also domestic security and given its abuse of citizens, the “National Crime Prevention Strategy (NCPS) (1996)” implemented changes within the intelligence structures for crimes. All ongoing criminal intelligence actions involving the police, the defense forces, the National Intelligence Coordination Committee, and the Departments of Justice, Correctional Services and Welfare would be separate but coordinated and also collaborate with the NIS, the SASS, academic analysts, and NGO’s.<sup>37</sup>

Given the corruption exposed in the Infogate scandal, where the entire intelligence apparatus had been in the hands of only two people—the Prime Minister and Director of BOSS—now the two civilian agencies (NIA and SASS) and the intelligence units of police and defense forces would be driven by the Minister of Intelligence acting in consultation with the Minister of Defense and the Minister of Safety and Security. Further, an additional position, a Coordinator for Intelligence, was created with responsibilities for coordinating the supply of intelligence by the different agencies to intelligence clients.<sup>38</sup>

---

<sup>34</sup> South African Government, “Intelligence Services Oversight Act 40 of 1994,” <https://www.gov.za/documents/committee-members-parliament-and-inspectors-general-intelligence-act>.

<sup>35</sup> “National Intelligence Coordinating Committee [NICOC],” *globalsecurity.org*, accessed September 10, 2020, <https://www.globalsecurity.org/intell/world/rsa/nicoc.htm>.

<sup>36</sup> South African Government, “White Paper on Defence, 1996 & Defence Review, 1996,” accessed September 10, 2020, <https://static.pmg.org.za/docs/2004/appendices/040817wpaper.htm>.

<sup>37</sup> South African Government, “National Crime Prevention Strategy: Summary,” accessed September 1, 2020, <https://www.gov.za/documents/national-crime-prevention-strategy-summary>.

<sup>38</sup> South Africa Government “National Strategic Intelligence Act.”

When there is cause for concern, then a Ministerial Review Commission on Intelligence can be convened. An example of this was the abuse of position within the National Intelligence Agency in 2006. The report of the Commission was released to the public in September 2008.<sup>39</sup>

## **Conclusion**

The hypothesis of this article was that intelligence reform and intelligence sector reform are the result of traumatic catalyst rather than gradual evolution, reactionary rather than proactive, and are not quick. The threat environment, an emergency, another necessity, e.g., democratization, gross failure, and scandals, are causes for reforms.

The case examined was South African intelligence services. South Africa is significant due to diverse and constantly changing operational environments: the Cold War, decolonization of Africa, Apartheid, post-Cold War, and post-Apartheid democratization. From the first non-military intelligence agency created in 1968, the Bureau of State Security, it was clear that the nature of intelligence requires striking a fine balance between security, secrecy, transparency, and accountability. The relationship between appointed and elected officials, the Prime Minister and the Bureau's Director, was too close, and state funds were misused.

The uncovering of the misuse of state funds, the Infogate scandal (1978), influenced intelligence reforms and intelligence sector reforms for the subsequent 20 years. The reforms examined were legislation, jurisdictions, restructuring, micro-managing intelligence, merging apartheid and opposition intelligence services, and creating post-Apartheid intelligence services. An important legacy from the Infogate scandal was that each reform included mechanisms, structures, and legislation to implement accountability and transparency to ensure that state funds would not be misused again.

Democratization, abolishing apartheid, and a "one-man, one-vote democracy" achieved in 1994 added weight to the reforms. Democratized South Africa post-Cold War has a remarkably reformed intelligence services sector vastly in contrast to that of the Cold War and Apartheid that was militarized, highly repressive, and focussed as an instrument of population control

There are no good sources about the future. It would be a mistake to assume that everything about the South African experience is relevant to the experiences of other countries. Yet several lessons can be drawn: every reform is unique and almost never easy, operationalizing any changes, including legislative mandates of transformation, is more complex than anticipated, and while the process to be addressed in reform starts with reflecting the envisaged ideal situation, the outcome is not always as expected.

---

<sup>39</sup> Lauren Hutton, "Overview of the South African Intelligence Dispensation," Intelligence Studies at the Research Institute for European and American Studies, November 22, 2008, [www.rieas.gr/images/HOUTONSA.pdf](http://www.rieas.gr/images/HOUTONSA.pdf).

South Africa's case shows that reforms of intelligence and the intelligence sector are iterative with the democratization process and that reform should begin earlier rather than later in the overall progression of democratization. The process of reforms to be addressed starts by convening reviews, commissions of inquiry, or ministerial task teams. Then legislation by defining the security vision and framework in law, followed by marketing the new elements to all, accelerating reforms, developing or strengthening managerial ability, providing clear guidance, insisting on accountability and financial transparency and ensuring parliamentary oversight, instituting procedures for authorizing operations, and confirming the legality of operations. Above all, errors can be avoided by not making uncoordinated, piecemeal changes.

### Disclaimer

The views expressed are solely those of the author and do not represent official views of the PFP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

### About the Author

Dr. **Glen Segell** (FRGS) is a Research Fellow at the University of the Free State, South Africa, and a Research Fellow at the University of Haifa, Israel. He was born in South Africa and educated to a BA and MA at the Hebrew University Jerusalem and to a DPhil at the University of Oxford. He also holds editorial, research, and teaching positions in the United Kingdom. He specializes in intelligence studies, civil-military relations, and strategic communication and consults as an expert for NATO, holding the rank of Brigadier-General (Reserves). He was involved in active security and intelligence operations, including Psychological Warfare in Iraq, Kuwait, Sudan, and Libya. He has published a substantial number of peer-reviewed articles and books. E-mail: [glen@segell.com](mailto:glen@segell.com)  
<https://orcid.org/0000-0002-4186-2761>



# Indonesian Intelligence Reform: Recent Challenges and Opportunities for Encouraging Democratic and Professional Intelligence

**Mufti Makarim A.**

*Executive Office of the President of the Republic of Indonesia,*

<https://ksp.go.id/en/index.html>

**Abstract:** This article describes the dynamics of Indonesia's intelligence reform from combatant intelligence posture during the post-independence revolution of 1945 to the authoritarian state intelligence under the New Order regime after 1965, and to the era of intelligence reform after the 1998 reformation movement. Recently, the challenges for Indonesian intelligence institutions have shifted from the need for legislation and political policies to the need for a democratic intelligence posture and the ability to face emerging security threats. Another challenge is the sectoral rivalry between the military, police, and strategic intelligence services, all of which are oriented towards internal security threats and domestic intelligence operations. Domestic threats form a contested operational domain, a 'grey' zones of defense, security, and intelligence threats.

**Keywords:** intelligence reform, military, Orde Baru, Soeharto, BIN, Covid-19, pandemic.

## Introduction

*"For Your Eyes Only"*<sup>1</sup>

On July 3, 2020, President Joko Widodo (Jokowi) signed the *Peraturan Presiden* (Presidential Decree, Perpres) Number 73 of 2020 concerning the Coordinating Ministry for Political, Legal and Security Affairs (*Kementerian Koordinator Bidang Politik Hukum dan Keamanan*, Kemenkopolhukam). Interestingly, this Presiden-

---

<sup>1</sup> Inscription on the Entrance of the State Intelligence Agency (BIN) Office, South Jakarta.

tial Decree eliminates the coordinating function of the Ministry regarding the *Badan Intelijen Negara* (State Intelligence Agency, BIN), which has been regulated in Presidential Decree Number 43 of 2015. Thus, the President is the only user and direct ‘manager’ of all operations and institutions of this Indonesian strategic intelligence agency.

The public trauma from extraordinary intelligence ‘powers’—especially military intelligence—permitting control of the public sphere and the political system has not completely disappeared yet. In a country that has experienced 32 years of authoritarian of the *Orde Baru* (New Order) rule (1965-1998), the arrangement of all intelligence elements in government agencies and ministries remains an important issue. For the generation who experienced the socio-political atmosphere in that era, a strict and non-tolerant position towards distortions of authority and primary duties and functions of intelligence is absolute, non-negotiable.

One of the factors causing the extraordinary strategic intelligence ‘power’ was the full control of intelligence by President Soeharto during the *Orde Baru* era. Without a democratic system of checks and balances and the formation of an oligarchic government supported by military forces and businessmen, cronies of the rulers, President Soeharto used intelligence to promote not only the interests of state security but also his own and his family’s political and economic interests.

“The return” of the President’s full control over BIN has brought back memories and concerns about the potential for ‘misuse’ of intelligence for the government’s political interests. Especially in the midst of the current momentum of the Covid-19 pandemic, where the President has the authority to take fast, unpopular, and emergency political and policy steps, including the deployment of military and intelligence forces to support efforts to deal with the threat of the Covid-19 pandemic. Concerns were raised regarding the function of BIN as a tool for the political interests of the President.

The government rejected this issue and allegation. “BIN is directly under the President because the President directly needs intelligence products,” stated Mahfud MD, Coordinating Minister for Political, Legal, and Security Affairs, on his official Twitter on 18 July 2020.<sup>2</sup> This is in accordance with the principle of the President being the single client of BIN. Although officially removed from coordination under Kemenkopolhukam, Mahfud emphasized that his ministry could still ask BIN for information. “As a minister, I always get information from the Head of BIN and often ask BIN to give presentations at ministerial meetings,” he said.<sup>3</sup>

This article will briefly retrace the history of Indonesia’s strategic intelligence dynamics since its inception and provide an analysis of the current status of po-

<sup>2</sup> See <https://nasional.kompas.com/read/2020/07/20/09300611/kini-di-bawah-presiden-ini-sejarah-singkat-bin?page=all>.

<sup>3</sup> See <https://nasional.kompas.com/read/2020/07/19/11344241/bin-tak-lagi-di-bawah-kemenko-polhukam-ini-penjelasan-mahfud-md>.

litical democratization in general and intelligence reform in particular after 1998. The article will respond to concerns over the backflow of democracy with the full control of the president over BIN. The views expressed here are purely personal and are not related to the opinions or attitudes of any government agencies.<sup>4</sup>

## **Intelligence after the 1945 Proclamation of Independence**

The history of Indonesian intelligence parallels the history of the independence revolution after the *Proklamasi Kemerdekaan* (Proclamation of Independence) on August 17, 1945. The intelligence agents' talents that were 'scattered' among the Japanese military-educated youths in 1943 were consolidated into a strategic intelligence force, whose primary mission was to defend the independence from an attack by the Allied forces and the Dutch who wanted to regain control of Indonesia.

Zulkifi Lubis, born in Banda Aceh on 26 December 1923, a military officer who was the Chief of Staff of the Army in 1955, is considered the 'founder' of Indonesia's strategic intelligence, currently known as BIN. Lubis is a graduate of the Nakano Military Intelligence School founded by the Japanese occupation in 1943 [in Tangerang city, Banten province] and is the best graduate of the school's first class. With 40 former soldiers of *Pembela Tanah Air* (Homeland Defenders, PETA), formed by the Japanese Military, in August 1945, Lubis ran the first intelligence agency of the Republic of Indonesia called the *Badan Istimewa* (Special Agency).<sup>5</sup>

Lubis had experience in intelligence operations since his early graduation from the Nakano Military Intelligence School. In 1944 he was stationed at Japan's Regional Intelligence Center in Singapore. He studied a lot and participated in Japanese intelligence operations in the Greater Asia war of conquering Indochina. So, when Indonesia became independent in August 1945, Lubis, who was 19 years old when he was recruited for intelligence school, became one of the Indonesian ex-Japanese militaries who had more combat intelligence experience than anyone in Indonesia. This new country needed an intelligence capability to defend its independence, which is reflected in the name of the *Badan Istimewa*. The initial 40 members of this agency, all of whom were alumni of the Japanese military, were trained quickly by Lubis to master the principles of intelligence, psychological warfare, and sabotage. Then they were dispatched to all regions

---

<sup>4</sup> Studies on Indonesian intelligence reform divide the dynamics of intelligence into four periods, namely: 1) Period in support of military operations (1945-1958); 2) Period supporting the implementation of political policy (1959-1965); 3) Period in favor of regime sustainability; and 4) Period of support to restoration of security. See Ali A. Wibisono, "Reformasi Intelijen dan Badan Intelien Negara (Intelligence Reform and State Intelligence Service)," in *Panduan Pelatihan Tata Kelola Sektor Keamanan untuk Organisasi masyarakat Sipil: Sebuah Toolkit* (Security Sector Governance Training Guide for Civil Society Organizations: A Toolkit), ed. in Mufti Makaarim A., et al. (IDSPS-DCAF, 2009), 11.

<sup>5</sup> See <http://www.bin.go.id>.

of the island of Java with the mission to seek support to defend the Republic and oversee the enemy's movements.<sup>6</sup>

In early May 1946, special training was conducted in the Ambarawa city [Central Java province] area for newly recruited agents. As a result, about 30 young graduates became the first batch members of the *Badan Rahasia Negara Indonesia* (Indonesian State Secret Agency, BRANI). This agency became the 'umbrella' for the Intelligence movement with several *ad hoc* units, including units for overseas operations.<sup>7</sup> BRANI was formed by Lubis on May 3, 1946, as an umbrella organization for the *ad hoc* units formed by field commanders and spread throughout Java. Lubis also moved outside Java by ship to form field units in Bali, Kalimantan, Maluku, Nusa Tenggara, Sulawesi and Sumatra. Lubis himself raised funds and resources to carry out operations abroad, to garner support for the republican army that was short on weapons, ammunition, and medicine.<sup>8</sup>

The civilian-controlled Ministry of Defense proposed to President Soekarno to form a strategic intelligence organization with a "civil character," which did not come under the auspices of the military. In July 1946, defense minister Amir Sjarifuddin tried to create a "*Badan Pertahanan B*" (Defense Office B) headed by a former police commissioner. Then he unified all intelligence agencies under the Ministry of Defense on April 30, 1947. Despite President Soekarno's support, BRANI was eventually disbanded and changed to *Bagian V* (Part V) of *Badan Pertahanan B*. *Bagian V* [also called KP V] as a "small unit" of *Badan Pertahanan B* that could not work optimally. Upon the fall of Sjarifuddin from the Cabinet, *Bagian V* was dissolved, and Lubis carried out an intelligence 'purge' of members of the *Partai Komunis Indonesia* (Indonesian Communist Party, PKI) who Sjarifuddin had recruited. The "Madiun Rebellion" in 1948, which was crushed by the military, resulted in the arrest and silent execution of Sjarifuddin.<sup>9</sup>

When Amir Sjarifuddin's Cabinet fell in January 1948 [a few months before the Madiun rebellion], the government included the disbanded Intelligence *Bagian V* as an element in the *Bagian I Staf Umum Angkatan Darat* (Part I of the General Staff of the Army, SUAD). Lubis was back to be the leader and concurrently the head of the *Markas Besar Komando Djawa* (Java Command Headquarters, MBKD-I). After the transfer of sovereignty from the Netherlands, the intelligence organization became the *Intelijen Kementerian Pertahanan* (Ministry of

<sup>6</sup> See Ken Conboy, *Intel Menguak Tabir Dunia Intelijen Indonesia* (original title: *Intel Inside Indonesia's Intelligence Service*) (Pustaka Primata, 2008), 1-2. For the English Edition see Ken Conboy, *Intel Inside Indonesia's Intelligence Service* (Equinox Publishing, 2004). See also <https://historia.id/militer/articles/zulkifli-lubis-bapak-int-indonesia-DrBXE>.

<sup>7</sup> See <http://www.bin.go.id>. BRANI is spelled similarly to to Indonesian word 'berani' (brave or bold).

<sup>8</sup> Conboy, *Intel Inside Indonesia's Intelligence Service*, 3-5.

<sup>9</sup> Conboy, *Intel Inside Indonesia's Intelligence Service*, 7-8. See also Hariyadi Wirawan, *Evolusi Intelijen Indonesia* (Evolution of Indonesian Intelligence), in *Reformasi Intelijen Negara* (Reform of State Intelligence), ed. Andi Widjajanto (Pacivis UI-FES, 2005), 28-29.



Defense Intelligence, IKP), with Lubis remaining as its head. Lubis then formed the *Biro Informasi Angkatan Perang* (Armed Forces Information Bureau, BISAP) in 1952, which was in charge of preparing strategic information for the Minister of Defense and the Chief of Staff of the Armed Forces, General TB Simatupang. He also initiated further education for intelligence which took place in Kaliurang, Yogyakarta Province.<sup>10</sup> BISAP itself was considered sub-optimal in carrying out its strategic intelligence function, one of the factors being Lubis' 'feud' with General AH Nasution,<sup>11</sup> the top leader of the Army, so that Lubis had to deal more with the military "internal politics."

In the same year, Vice President Mohammad Hatta and Minister of Defense Sri Sultan Hamengku Buwono IX accepted an offer from the United States Central Intelligence Agency (CIA) to train Indonesian professional intelligence candidates on Saipan Island, the Philippines.<sup>12</sup> This tacit US assistance was organized through the Bureau of Security or *Dinas Chusus* (DC) – the ministry-equivalent body that coordinated Ministry of Defense operations, and not through BISAP, which the Vice President and Minister of Defense considered 'unreliable.' Thus, the Bureau of Security compiled a roster of 50 civilians to compete in Central Java, and 17 of them were the first to attend this training. In February 1953, they returned to Indonesia and found many changes. BISAP had been disbanded, Army Chief of Staff General AH Nasution—who was Lubis' "mortal enemy"—was fired by President Soekarno,<sup>13</sup> Lubis was appointed as Deputy of *Kepala Staf*

---

<sup>10</sup> See Hendri F. Isnaeni, "Zulkifli Lubis, Bapak Intelijen Indonesia," *Historia*, February 2, 2016, <https://historia.id/militer/articles/zulkifli-lubis-bapak-intelijen-indonesia-DrBXE>.

<sup>11</sup> Nasution is a designer of the *Dwifungsi ABRI* (*Angkatan Bersenjata Republik Indonesia*) or Dual-function of Armed Forces of the Republic of Indonesia which was delivered in 1958 and later adopted during the Soeharto administration. This concept is a way for ABRI not to be under civilian control, but at the same time not to dominate so that it becomes a military dictatorship. On 17 October 1952, Nasution [and General Simatupang] mobilized their troops to encircle the Presidential palace to protest civilian interference in military affairs, and aimed the cannon muzzle at the palace. Sukarno out of the Presidential Palace to meet the demonstrators and finally convinced both the soldiers and civilians to return home. The aftermath of this incident was Nasution's dismissal in December 1952. On 7 November 1955, after three years of exile, Nasution was re-appointed to his old position as *Kepala Staf Angkatan Darat* (Army Chief of Staff), and Lubis was displaced.

<sup>12</sup> See <http://www.bin.go.id>.

<sup>13</sup> Another version states that the 17 October incident [as the first open conflict between the army and civilian politicians] was triggered by a session of the *Dewan Perwakilan Rakyat Sementara* (Provisional People's Representative Council, DPRS) which discussed the modernization of the Army, which was considered to be their internal authority under the leadership of Nasution and Simatupang. On 17 October 1952, officers from the Army Headquarters together with several regional commanders went to the Palace to meet President Sukarno, asking him to take power and dissolve the Provisional Parliament. Sukarno did not give in to military pressure and Nasution, as the top officer of the army headquarters, resigned afterwards. See Kisenda Wiranatakusumah, *Civil-Military Relations in the Late Suharto Era*, Thesis (Naval Postgraduate School, 2000), 17-21.

*Angkatan Darat* (Chief of Staff of Army); and after BISAP was disbanded, all military services included and operated their respective intelligence organizations. The Security Bureau installed these Saipan alumni in the *Ksatria Graha* (Ksatria Firm). They run intelligence operations under the Security Bureau.<sup>14</sup>

On December 5, 1958, President Soekarno formed the *Badan Koordinasi Intelijen* (Intelligence Coordinating Board, BKI) and appointed Colonel Pirngadi as its head. This agency aimed to rearrange the coordination between all the scattered elements of intelligence to consolidate the President's power, who had to deal with rebellions and attacks by civilian and military opposition. Furthermore, on November 10, 1959, BKI became the *Badan Pusat Intelijen* (Central Intelligence Agency, BPI), headquartered at Jalan Madiun Jakarta and headed by Dr. Soebandrio, who was also the Minister of Foreign Affairs and a trusted confidant of the President. During the 1960s and until the end of the *Orde Lama* (Old Order) era, Soebandrio's influence on the BPI was very strong in the wake of the war of Communist and non-Communist ideology in the military, including the Intelligence.<sup>15</sup>

By November 1965, BPI became a 'tool' in the battle of Subandrio's interests, linked to the claim to protect President Soekarno from the planned coup of the *Dewan Jenderal* (General Council of the Army). Allegations of collaboration between the Army and American and British intelligence to overthrow President Soekarno, who was considered to be protecting the PKI and "making political space" for the party, were flatly rejected by the Army's leadership. On September 30, 1965, seven Army officers in Jakarta and two in Central Java became victims of the "30 September Movement" attacks. The ability of the military to take control quickly after this event was the "end to the political career of Subandrio and the PKI." The Army's counterattack was carried out under the command of Major General Soeharto based on the *Surat Perintah 11 Maret* (Order of 11 March 1966, Supersemar) from President Soekarno to "restore security," which included a provision for cleaning up BPI.

The Army "took over" BPI, appointing Brigadier General Sugiharto as acting chief of BPI in December 1965. Earlier in November, he was promoted to be Chief of Army Intelligence, replacing Brigadier-General Siswondo Parman, one of the officers killed in the September 30 kidnapping incident. Between 18 and 21 March 1966, several high-ranking BPI officials considered PKI sympathizers were arrested and sentenced to prison. Subandrio himself was tried and sentenced to death (he was imprisoned, but the sentence was never carried out).

Theoretically, the type of Intelligence-State interaction formed in this period is "Political Intelligence." Even during 1950-1959, Indonesian intelligence activities did not receive much attention due to the relatively volatile political conditions. After the Republic of Indonesia was officially recognized on August 15, 1950, the intelligence agencies in Indonesia were reactivated. Indonesia had to

<sup>14</sup> Conboy, *Intel Inside Indonesia's Intelligence Service*, 9-14.

<sup>15</sup> See <http://www.bin.go.id>.

direct intelligence operations to deal with internal threats. However, the dominance of militarization in the previous period led to the construction of political intelligence only in 1958 when Sukarno formed BKI, which was later changed to BPI. In 1950-1958, military intelligence still dominated the operational activities of the intelligence services, even though they were not directed to face a specific external threat. This politicization process began in early 1952 when the Chief of Staff of the Armed Forces TB Simatupang formed BISAP as an intelligence agency to support his office and the Defense Ministry. However, due to its structural marginal position and limited resources and funds, BISAP could not do much and was dissolved in the following year.<sup>16</sup>

### **Orde Baru (New Order) Intelligence 1965-1998**<sup>17</sup>

Major General Soeharto was put in charge of the *Komando Operasi Pemulihan Keamanan dan Ketertiban* (Operation Command for Restoring Security and Order, KOPKAMTIB), formed three days after the “September 30 Movement” attacks. He took decisive actions to restore security and ‘clean-up’ the sympathizers and PKI members, including those in the intelligence circle. Soeharto, who really understood the importance of the intelligence function and the need to move quickly, formed the *Satuan Tugas Intelijen* (Intelligence Task Force, STI) in all regions under the *Komando Daerah Militer* (Regional Military Command, KODAM). STI was a support operation for KOPKAMTIB led by all KODAM Commanders to carry out investigations and perform other intelligence activities.

The structure of the guerrilla warfare in the post-1945 independence war, which divided the territory of Indonesia into military command areas, was adopted as a manifestation of Nasution’s “middle way” concept to meet the military needs of ‘eradicating’ the PKI and holding political control as a form of *Dwifungsi ABRI*. At every level of civilian government, there is a military element included in a forum called the *Musyawarah Pimpinan Daerah* (Council of Regional Leadership, Muspida), usually led by elements from the military. This arrangement has survived to this day (see Table 1). In most cities and provinces, Governors and mayors are appointed by President and usually are ABRI officers.<sup>18</sup> The definite advantage Soeharto gained from this activation of territorial commands was the degree of power and military intelligence operations that the structure could carry out, which kept Suharto ‘updated’ with “any threat” even from the village level.

---

<sup>16</sup> See Andy Widjajanto and Artanti Wardhani, *State-Intelligence Interaction 1945-2004* (Pacivis UI & FES, 2008), 70-71.

<sup>17</sup> Soeharto administration called his period as *Orde Baru* (New Order) as a replacement of President Soekarno era’s that he called as *Orde Lama* (Old Order).

<sup>18</sup> See Salim Said, *Soeharto’s Armed Forces: Problems of Civil Military Relations in Indonesia* (Pustaka Sinar Harapan, 2006), 20-22.

**Table 1. Parallel Civil Bureaucracy and Army Territorial Command.<sup>19</sup>**

MILITARY STRUCTURE	CIVIL ADMINISTRATION
<b>KODAM</b> (as Regional Military Command)	Province
<b>KOREM</b> (as Sub-Regional Military Command)	Residency
<b>KODIM</b> (as District Military Command)	District
<b>KORAMIL</b> (as Sub-District Military Command)	Sub-District
<b>BABINSA</b> (as Village Development Non-Commissioned Officer)	Village

On August 22, 1966, with support from President Sukarno, Suharto established the *Komando Intelijen Negara* (State Intelligence Command, KIN) with Brigadier-General Yoga Sugomo in the lead. The head of KIN is directly responsible for reporting to Soeharto. As a strategic intelligence agency, BPI, which was already under the Army's control, was merged into KIN which also had *Operasi Khusus* (Special Operations, Opsus) under Lieutenant Colonel Ali Moertopo with assistants Leonardus Benyamin (LB) Moerdani<sup>20</sup> and Aloysius Sugiyanto.<sup>21</sup> KIN was a new agency reporting on national and international security issues, including political, social, economic, and other matters related to military security at home and abroad. Soeharto led this institution himself in his early days, placing his confidants in key positions. Less than a year later, on May 22, 1967, when Suharto officially became President, he issued a *Keputusan Presiden* (Presidential Decree, Keppres) to designate KIN as the *Badan Koordinasi Intelijen Negara* (National Intelligence Coordinating Board, BAKIN). Major General Soedirgo became the first head of BAKIN. Like in KIN, the upper echelon included predominantly military officers, although the middle and lower levels were also filled with civilian bureaucrats. BAKIN was designed as a civilian institution. However, in reality, top military officers retained strong control over BAKIN.

<sup>19</sup> See Said, *Soeharto's Armed Forces*, 22.

<sup>20</sup> Moerdani is known as a military officer who has been involved in the intelligence activities a lot, so his figure is often considered mysterious. Moerdani was directly involved in the military operation handling the hijacking of Garuda Indonesia Flight 206 at Don Mueang Airport, Bangkok, Thailand on March 28, 1981, an event that was later documented as the first plane hijacking in Indonesian airline history and the first act of jihadist terrorism in Indonesia. He is also considered by many as the figure responsible for the Tanjung Priok incident (the attack on a mosque congregation) and the mysterious shootings in the 1980s when hundreds of people who were considered criminals were found dead on the streets. In a government position, apart from serving as ABRI Commander in 1983-1988, he also served as Minister of Defense and Security and also Commander of KOPKAMTIB.

<sup>21</sup> August 22 is celebrated as the anniversary of KIN, which is currently BIN, <http://www.bin.go.id>.

Apart from being known as the military order, the *Orde Baru* was marked by the permeation of intelligence of all aspects of people's lives. BAKIN became a strategic intelligence operation vehicle for all issues, apart from KOPKAMTIB, which carried out the purge of the PKI and its sympathizers through the military territorial Command structure and the STI. Opsus, which was initially an intelligence operation aimed at seizing West Papua from the Netherlands and enabling the confrontation with Malaysia, was later mobilized to spy on social, political, and religious life in society, especially individuals and groups that could potentially oppose the Soeharto government, as well as to conduct intelligence operations facing the threat of separatism in Aceh, Papua, and East Timor.<sup>22</sup> Thus, the military bodies attached to the civilian government ultimately carried out an intelligence 'function' to guard against what the *Orde Baru* called latent dangers and security threats. In this context, cases of violence and human rights violations occurred massively, reversing the socio-political dimension (e.g., limiting the space for expression, arresting and killing political activists or opposition leaders) as well as the social and cultural economy, e.g., by forced taking of people's land and destruction of the environment and forests 'escorted' by military and intelligence organizations.

Soeharto's strategy in the 1970s was to create 'contestation' between institutions so that they could never 'unite' against Suharto, who ended up placing all intelligence agencies under his direct control. Even though Soeharto designated BAKIN as a strategic intelligence agency, he did not immediately disband KOPKAMTIB and Opsus. Soeharto also 'strengthened' the figure of the "Intelligence Assistant" under the Ministry of Defense and Security who was expected to direct concurrently the ABRI's (Commander of the Armed Forces of the Republic of Indonesia) controlled territorial military intelligence units, KOPKAMTIB, and BAKIN, which often ran overlapping operations and even competed with the aim of securing Soeharto's interests. Moerdani, who was entrusted with leading the Strategic Intelligence Center under the Ministry of Defense and Security when he was appointed Commander of ABRI in January 1983, formed the *Badan Intelijen Strategis* (Strategic Intelligence Agency, BAIS) and built an international network by controlling defense attaches in Indonesia's Embassies. With large

---

<sup>22</sup> Moerdani, who had experience as Intelligence Assistant to the Minister of Defense and Security, Assistant Intelligence to the Commander of KOPKAMTIB, Head of the *Pusat Intelijen Strategis* (Strategic Intelligence Center, Pusintelstrat), and Deputy Head of BAKIN, was deeply involved with the issue of the decolonization of East Timor. In August 1975, Moerdani began sending Indonesian soldiers under the guise of volunteers to infiltrate East Timor. The situation intensified on November 28, 1975, when Fretilin declared the independence of East Timor. Intelligence operations ceased and the military operation, Operasi Seroja (military invasion) was initiated instead. Although Seroja was not an intelligence operation, Moerdani continued to be involved, this time as an invasion planner and the person behind of intelligence component of the operation.

budget support and a strong network at home and abroad, BAIS eventually became the intelligence agency that stood out and outperformed other agencies.<sup>23</sup>

BAIS itself has been criticized for establishing a one-sided perception of what a national security threat constitutes by making civilians from various critical groups a threat. By using the term to identify groups in conflict with the Pancasila ideology—the official state ideology as stipulated by the constitution—BAIS divides the sources of the threat into the following categories:

- 1) Left radical groups: those who have a social-democratic or communist/Marxist political orientation;
- 2) Right radical groups, namely those in political organizations that promote the discourse of Islamic law; and
- 3) Other radical groups, namely NGOs that are dissatisfied and disappointed with the government, such as *Imparsial* and *KontraS* (two out of dozens of Indonesian NGOs campaigning for human rights and security sector reform).<sup>24</sup>

Soeharto-Moerdani's relationship became increasingly tenuous towards the end of the 1980s. Soeharto, who was aware of the emergence of international and national political pressures on the issue of democracy, changed his strategy to safeguard his power by 'embracing' the Islamic groups that he managed to raise in the *Ikatan Cendekiawan Muslim Indonesia* (Indonesian Muslim Intellectuals Association, ICMI). Soeharto automatically developed a new 'green' ABRI style to eliminate the impression of his anti-Islamic attitude. Under ABRI Commander General Faisal Tanjung—a Muslim and loyalist of Soeharto, appointed in May 1993—BAIS was disbanded and changed to the *Badan Intelijen ABRI* (ABRI Intelligence Agency, BIA) with many personnel changes to erase Moerdani's influence in the Indonesian intelligence world.<sup>25</sup> At BAKIN, Suharto deliberately appointed Lieutenant General Moetojib, a TNI officer who was not too influential and did not disobey. While BAIS attempted to mobilize Islamic groups by creating a combination of military-intellectual Muslim elites at ICMI, BAKIN's orientation shifted to monitoring pro-democracy movements and political activists who increasingly opposed Suharto's rule in the 1990s.<sup>26</sup> Previously, in 1988, along with Moerdani's descent, KOPKAMTIB was also changed to the *Badan Koordinasi dan Stabilitas Nasional* (National Stability and Coordination Agency, Bakorstanas). Moerdani's footsteps immediately disappeared.

<sup>23</sup> See Aleksius Jemadu, "State Intelligence Agency," in *2007 Security Sector Reform Almanac*, ed. Beni Sukadis (Lesperssi-DCAF, 2007), 92-93. See also Widjajanto and Wardhani, *State-Intelligence Interaction*, 79-93.

<sup>24</sup> See Rizal Darma Putra, "Strategic Intelligence Agency (BAIS)," in *2007 Security Sector Reform Almanac*, 106-107.

<sup>25</sup> See Salim Said, *Soeharto's Armed Forces*, 86.

<sup>26</sup> Jemadu, "State Intelligence Agency," 93.

## **Intelligence Reform Era after 1998**

When Soeharto 'resigned' from his post as President in May 1998 at the pressure of the political pro-democracy movement and a decrease in support of the civilian political elite, his successors could not immediately make radical changes to the structure and culture of the intelligence services. It is noteworthy that Soeharto's people filled ABRI and all intelligence agencies, remaining *de facto* loyal to the former rather than the new ruler. The only option was to put "trustworthy people" in the lead. At BAKIN, president BJ Habibie, who replaced Suharto, chose Lieutenant General ZA Maulani. President Abdurrahman Wahid, who was elected in 1999, appointed Lieutenant General Arie J Kumaat (some sources state that he was 'forced' to appoint Arie because there was no other loyal figure capable of controlling BIN – still dominated by military elements). President Megawati Soekarnoputri, elected in 2001, appointed Lieutenant General AM Hendropriyono. BAKIN then changed its name to BIN, with the main functions and tasks stipulated in Presidential Decree Number 103 of 2001.

The positions of head of BIN tend to be political rather than professional ones. The tradition of choosing a President's confidant continued during the days of President Susilo Bambang Yudhoyono (SBY) and President Joko Widodo (Jokowi), who had also elected former high-ranking police officers. President SBY appointed Major General Syamsir Siregar,<sup>27</sup> General (Police) Sutanto, and Lieutenant General Marciano Norman. Meanwhile, President Jokowi appointed senior retired officers, Lieutenant General Sutiyoso and General (Police) Budi Gunawan – who are currently still in office.

As stated above, Suharto's rule, which fell due to various pressures,<sup>28</sup> left one problem for the new government; military structures that were still loyal to Suharto. ZA Maulani, who was the head of BAKIN under President Habibie, in an interview in the media expressed Soeharto's disappointment with the civilian elite who 'betrayed' him by quoting Suharto's statement, "I have nurtured and promoted them since the beginning of their career but when I really needed their

---

<sup>27</sup> The last rank of Siregar before retirement was Major General with the post of Head of BIA. He was appointed after retirement so that he did not get a promotion.

<sup>28</sup> Sukardi Rinakit mentioned several factors that caused Suharto's fall, including: 1). International political pressure, especially from the United States and the IMF. This pressure uses the issue of human rights violations, the kidnapping of activists and the continuing violence in Aceh, Timorleste and Papua. This pressure also led to a worsening economic situation; 2). The elite conspiracy, especially the ICMI leadership, which withdrew support, mobilized demonstrations and urged the leadership of the *Majelis Permusyawaratan Rakyat* (People's Consultative Assembly, MPR) to ask Soeharto to resign; 3). A shift in support within the military, especially from 'red-white' (nationalist as symbolized by the colour of Indonesian flag) to 'green' (close to Islamic political groups) military lines. In an extreme way, this situation is referred to as the contestation between the factions of "Political Islam" and "Pancasila" which led to the May 1998 riots that took place a few days before Soeharto stepped down. See Sukardi Rinakit, *The Indonesian Military After the New Order* (ISEAS, 2005), 3-4.



support, they rejected me.”<sup>29</sup> The change of attitude of the army, loyal to Suharto, to find a mechanism to reform the security sector, involving the military, police, and intelligence, could only be gradual and full of compromises, without completely alienating them from the practical political space and state policy-making, which in fact was the authority of the civilian political authority.

BAKIN, which later became BIN, is still under the scrutiny of the military, especially concerning their alleged connection to a number of social conflicts and violent acts that occurred after 1998, seen as a reflection of Soeharto’s ‘anger.’ There are three views formed at this time. *First*, the accusation that all forms of chaos were caused by operations in loyalty to the *Orde Baru*, carried out widely and systematically with massive and terrible effects. *Second*, although the pressure of the new government on the security apparatus to overcome this security disturbance has strengthened, the actions taken have been slow and sub-optimal.<sup>30</sup> There are allegations of deliberate failure to deal with this chaos properly, again rooting in loyalty to the *Orde Baru*. *The third* view states that this chaos is a strategy of consolidating security actors to test their position in the eyes of the civilian government, and when the civilian government asks for action by the apparatus, then there is a negotiation regarding the weight of pressure for reform and what ‘may’ or ‘should not’ be carried out.

Efforts to promote intelligence accountability are not an easy matter. The case of the death of human rights activist Munir Said Thalib<sup>31</sup> on a flight from

<sup>29</sup> Rinakit, *The Indonesian Military After the New Order*, 5.

<sup>30</sup> During the reign of President Abdurrahman Wahid, conflicts over ethnic issues in Kalimantan and religious issues in Maluku occurred. My experience of being part of one of the palace’s information sources at that time shows that the President lacked the support of valid information from the field, was unable to control military manoeuvres that worsened the conflict by turning it into a business arena, and failed to maximize the effect of intelligence operations for prevention and creation of normal conditions. The image of the President as a defender of religious and ethnic minorities, able to orchestrate reform, was ‘thwarted’ by the machines in the government organizations at that time. One monumental example is the entry of Laskar Jihad, a paramilitary group led by alumni of the Afghanistan war, to Maluku to participate in conflicts over religious issues. The president firmly ordered all security and intelligence apparatus to prevent their entry, but there was no maximum effort, even allegations emerged that they were deliberately given space to attend. In the end, Maluku conflict became one of the entry points for the Jemaah Islamiyah and al-Qaeda terrorism movements, a training camp and recruitment of new cells and networks, and thus sow the seeds of radical movements and terrorism that lived and spread in Indonesia to this day.

<sup>31</sup> Munir Said Thalib is an idealistic human rights activist who defends victims of violations and is willing to confront the military and police to fight for the rights of these victims. Threats of murder and intimidation to force Munir to stop his activities while leading KontraS and Imparsial (the two strongest human rights advocacy organizations in Indonesia founded by him) are nothing new, including monitoring and attempts to thwart his defense activities carried out by elements of the security forces directly or indirectly. Before leaving for Amsterdam, Munir admitted he received a phone call and a request from the ‘agent’ (who was later determined, based on the



Indonesia to Amsterdam on September 7, 2004—a suspected “intelligence operation” after the 1998 reforms—is deadlocked. The legal process only tried one field actor, who was said to be “an intelligence agent” and found him guilty, and one official at the leadership level of BIN who communicated with the agent but was eventually acquitted. To date, there has been no new progress in law enforcement in this case, and the issue and allegations of intelligence operations remain a mystery. This case adds to a series of data on attacking and silencing opposition groups and human rights defenders that should not have happened during the reform era. Such cases raise the awareness that the posture of new intelligence institutions and operations will not be possible if we refer to the organizational realities and existing legal basis because they are a product of the authoritarian politics of the *Orde Baru*. What should be worrying is not the new rules promoted but the current absence of norms of democratic oversight over intelligence.

The State Intelligence Law was finally issued at the end of 2011, 12 years after the reform started. This law, adopted as a result, among other reasons, of the pressure after the murder of human rights activist Munir, is indeed forward-oriented and may contribute to the success of intelligence reform, preventing the repetition and tradition of authoritarian intelligence in the style of the *Orde Baru*. Intelligence services should abandon the old paradigm in understanding threats and pay close attention to new challenges such as global terrorism. Sectarian politics need to be strengthened at home. Intelligence should contribute to creating a peaceful world free from new threats such as environmental damage and disease outbreaks.

### **Legislation, State Intelligence Governance, and Intelligence Reform**

Since the beginning of the 1998 reforms, the pressure from civil society to carry out intelligence reform was not strong enough. Apart from the structural political change such as democratic elections and amendments or cancellation of articles of the constitution and authoritarian legislation, the main security sector issues were only marginally addressed. Security sector reform started with separating the two institutions previously part of ABRI – the *Tentara Nasional Indonesia* (Indonesian National Army, TNI) and the *Kepolisian Negara Republik Indonesia* (Indonesian National Police, Polri). Other key issues were the human rights violations during the *Orde Baru* era, revocation of ABRI’s dual function, the release of the *Orde Baru* political prisoners, and post-1997 economic recovery.<sup>32</sup>

---

results of the police investigation, to be the perpetrator) for a meeting on the Jakarta-Singapore flight, before continuing to Amsterdam. This information has been conveyed directly by Munir to his family and friends before he died.

<sup>32</sup> To understand the dynamics of the civil society movement in pushing for security sector reform, especially reform of the military, police and intelligence in Indonesia in the 1998-2006 period, see Mufti Makarim A. and Sri Yunanto, eds., *Efektivitas Strategi Organisasi Masyarakat Sipil Dalam Advokasi Reformasi Sektor Keamanan di Indonesia*

Pacivis UI underlined the challenges of avoiding security disruption and conflict, which made the civilian elite ‘compromise’ not to put too much pressure on the military because they were needed to restore security. This need for the ‘military’ was seen in the appointment of military officers such as ZA Maulani, Arie Kumaat, and AM Hendropriyono as heads of BAKIN (which later became BIN).<sup>33</sup> At that time, Aceh, Timor-Leste, and Papua presented a serious threat of separatism, and social conflicts with religious and ethnic backgrounds emerged in Maluku, Sulawesi, and Kalimantan.

In the Soekarno era, the challenge for the intelligence organization was with the BKI coordination system at the level of institutional leadership (such as the Head of the Attorney General’s Office and the Military Leadership) who were not active in technical coordination activities. In practice, leaders often appoint officials not competent to make direct decisions or of low rank. As a result, BKI, which was established based on Government Regulation no. 64 of 1958, was only less than a year old. President Soekarno then formed BPI through Government Regulation no. 8 of 1959 and gave it not only coordination authority but also the right to conduct intelligence operations. Subandrio, as Head of BPI and concurrently Deputy Prime Minister One (with a ‘rank’ equivalent to a four-star officer) and the Minister of Foreign Affairs, was expected to exercise effective control over the internal intelligence. However, after the September 30 incident, Subandrio was removed from his position and tried, while the BPI was changed to KIN by President Sukarno with the leadership of Major General Soeharto<sup>34</sup> (who later ‘overthrew’ Soekarno). KIN was then stipulated based on *Keputusan Presiden* (Presidential Decree) number 181 of 1966, which was later changed to BAKIN based on *Keputusan Presiden* number 70 of 1967.

Like BPI, BAKIN does not only coordinate intelligence agencies in the ministry and the military but also conducts intelligence operations. The change to BIN, which was initially regulated based on *Keputusan Presiden* number 5 of 2002, was also accompanied by a mandate to continue with the same authority. As on previous occasions, building an effective BIN faced certain difficulties, e.g., the rivalry among the departmental intelligence agencies. Furthermore, its institutional status was weak – whereas BIN is only based on a *Keputusan Presiden*, the institutions and ministries that must be coordinated are formed based on a Law so that their position is ‘higher.’<sup>35</sup>

The process of drafting the law on intelligence proposed in the 1998 reform package was callous. There were pros and cons regarding the need for this law, and the draft proposed by the government was heavily criticized. Still, the draft

---

1998-2006 (The Effectiveness of the Strategy of Civil Society Organizations in Advocating for Security Sector Reform in Indonesia 1998-2006) (IDSPS, 2008).

<sup>33</sup> Widjajanto and Wardhani, *State-Intelligence Interaction*, 93.

<sup>34</sup> See Irawan Sukarno, *Aku ‘Tiada’ Aku Niscaya Menyingkap Lapis Kabut Intelijen* (I ‘un-exist’ [but] I Undoubtedly Unveil the Fog of Intelligence) (Yayasan Pustaka Obor Indonesia, 2011), 53-55.

<sup>35</sup> Sukarno, *Aku ‘Tiada’ Aku Niscaya Menyingkap Lapis Kabut Intelijen*, 57-59.

provided the law enforcement authority to intelligence apparatus with exclusive powers in civilian strategic intelligence operations. It lacked, however, provisions for intelligence accountability and professionalism. For civil society, the draft submitted for discussion in parliament would have the same legitimacy as intelligence organizations and operations undertaken under authoritarian rule.

Fortunately, during discussions at the DPR, there were changes and improvements, although not all of them had become more moderate and accommodated proposals by NGOs. Matters that still needed to be improved when this law was passed were then challenged in the Constitutional Court. And even though, in the end, civil society 'lost' in this judicial review lawsuit, this example shows the hope of contributing to the creation of intelligence that is in line with the principles of democracy and the rule of law adopted by Indonesia. With the existence of this Law, intelligence posture, organization and operations are reflected and can be monitored by the public and parliament. The task that awaits in the future is to supervise the implementation of this legislation, including evaluating the reform process of BIN and intelligence organizations at the ministerial and institutional level (including in the military and police) so that they work in compliance with existing legal provisions.

### **Closing: Actual Challenges of Indonesian Intelligence**

From 1945 to the present, the state intelligence organization has changed its 'official' name six times, namely BRANI (Indonesian State Secret Agency), BKI (Intelligence Coordinating Agency), BPI (Central Intelligence Agency), KIN (National Intelligence Command), BAKIN (National Intelligence Coordinating Agency), and BIN (State Intelligence Agency). The idea of a change was carried out with the aim of improving and strengthening this organization. However, our history proves that this is not easy.

Intelligence as the "first line of battle" requires adaptation to the times and threats. The orientation in institutional development is on the improvement that synergizes five aspects; democracy and the principles of the rule of law, professionalism, adaptation to technological developments, the ability to read contemporary threats, and transformation of the capabilities provided by the state to get maximum results.

Irawan Sukarno conveyed an interesting view that (Indonesian) intelligence in the future should aim to win the peace. The administration of intelligence becomes more complex as unconventional battlefields emerge, which are much more challenging than conventional ones. Unconventional warfare has more complex dimensions, strategies, dynamics, risks, and ranges; it cannot be faced with just armed military forces but requires "civilian forces" tailored to the type of battle being faced.<sup>36</sup>

In conclusion, we want to underline three main issues. First, the experience of the militarization of intelligence and the use of intelligence organizations for

---

<sup>36</sup> Sukarno, *Aku 'Tiada' Aku Niscaya Menyingkap Lapis Kabut Intelijen*, 208-210.

the benefit of the elite should serve as a lesson for the restructuring and reform of intelligence into a professional agency, independent from politics and serving the interests of the state solely. Second, the temptation to return to an operating posture and a domestically oriented threat view, especially to ‘attack’ political opposition and control the public, should be resisted. It has bad precedents and will never help form a modern intelligence organization. And third, the challenges faced by Indonesia, including the Covid-19 pandemic currently sweeping the world, should be used to prove the resilience of intelligence work. The image of “*Intel Melayu*” (an intelligence agent who only can frighten the public by showing their identities) still attached to our intelligence agents should change. When this happens, then the public concern about the President’s status as a single user of BIN and the politicization of this organization will be out of place.

## Disclaimer

The views expressed are solely those of the author and do not represent official views of the PFP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium’s editors.

## About the Author

**Mufti Makarim A.** is an expert on Politics, Defense, and Security at the Executive Office of The President of the Republic of Indonesia since January 2020. Previously, apart from his position as a researcher and consultant on defense and security issues, Mufti conducted advocacy, research, and empowerment of civil society organizations on security sector reform, conflict studies, human rights, and counter-terrorism. He was involved with KontraS (The Commission for the Disappearances and Victims of Violence) in 1999-2007 and IDSPS (The Institute for Defense, Security and Peace Studies) in 2007-2013 – the time when Indonesia’s CSOs left a mark on reforming security actors—including the intelligence—as well as the civilian authority as part of Indonesia’s democratization and reform. After 2013, Mufti focused on his professional consultancy and research for the government, non-government and private sectors.  
E-mail: makarimalahlaq@gmail.com



M. Caparini & A. Gogolewska

*Connections QJ* 20, no. 1 (2021): 91-100

<https://doi.org/10.11610/Connections.20.1.06>

Research Article

## Governance Challenges of Transformative Technologies

*Marina Caparini*<sup>1</sup> and *Agnieszka Gogolewska*<sup>2</sup>

<sup>1</sup> *Stockholm International Peace Research Institute, <http://sipri.org>*

<sup>2</sup> *European University of Information Technology and Economics In Warsaw, <http://www.eu.edu.pl/>*

**Abstract:** The rise of digital information and exponential technologies are transforming political/geopolitical, social, economic, and security arrangements. The challenges they pose to governance is unprecedented, distorting and used to manipulate public discourse and political outcomes. One of the most profound changes triggered by the unconstrained development of innovative technologies is the emergence of a new economic logic based on pervasive digital surveillance of people's daily lives and the reselling of that information as predictive information. EU responses to this new environment have been slow and inadequate. Establishing effective controls over the actors and processes harnessing innovative technologies will require not only specialized data governance skills but a deeper understanding of the impact of these technologies, the forging of partnerships across the public-private divide, and the establishment of greater political and social accountability of corporate actors involved in their development and application.

**Keywords:** Data governance, artificial intelligence, governance, public policy, surveillance capitalism, data privacy.

### Introduction

The rise of innovative technologies is having a transformative impact on contemporary society. Two types of technologies stand out. The first is digital information and telecommunications, which has been developing ever more rapidly since the 1980s and is now entering the fifth-generation cellular wireless, or 5G,

enabling better connectivity and transfer of larger amounts of data than ever.<sup>1</sup> The second cluster of technologies, although differently engineered, are collectively defined as “exponential technologies” due to their unprecedented rate of technical progress.<sup>2</sup> They include advanced robotics and drones, augmented and virtual reality, 3D printing, biotech, blockchain, the Internet of Things (IoT), autonomous vehicles and, of course, machine learning, which is also known as Artificial Intelligence (AI).<sup>3</sup>

The new technologies have already found many applications for enhancing safety<sup>4</sup> and security. They also have disrupted traditional ways of sharing information and have possibly undermined democratic principles and processes. They are the ultimate game-changer, globally disrupting existing political, economic, and security arrangements, empowering certain actors while subverting or overturning long-established governance processes and control regimes. The scale of challenges posed to governance is unprecedented and requires a heightened understanding of the fundamental impact new technologies have on our social, political, economic, and geopolitical spheres. It is also imperative that policy-makers and those who assist them develop a much deeper technological awareness and interest in exerting effective controls over the actors and processes by which these technologies are harnessed.

## Innovative Technologies and Security

The new technologies are ‘data-hungry,’ gathering and producing enormous and ever-increasing amounts of data and posing significant challenges to effective government control over the instruments of national security and even the executive’s ability to control their own agents in the security sector. Traditionally, data was fragmented and managed in data silos. But the accelerated data-generating technologies of today demand a different management model founded on data security and cross-sectoral, holistic approaches to data governance.<sup>5</sup> Moreover, the safe use of exponential technologies in any security domain re-

<sup>1</sup> Sascha Segan, “What Is 5G?” *PC Magazine*, February 25, 2021, <https://www.pcmag.com/article/345387/what-is-5g>; John McCann, Mike Moore, and David Lumb, “5G: Everything You Need to Know,” *techradar*, May 2021, <https://www.techradar.com/news/what-is-5g-everything-you-need-to-know>.

<sup>2</sup> Creative HQ, “What is Exponential Technology?” <https://creativehq.co.nz/what-is-exponential-technology/>.

<sup>3</sup> For an excellent guide to exponential technologies, see: “Exponential Technology Trends that Will Define 2019,” *SU Blog*, December 10, 2018, <https://su.org/blog/exponential-technology-trends-defined-2019/>.

<sup>4</sup> Ilya Pozin, “6 Innovative Technologies Designed To Improve Our Safety,” *Forbes*, November 19, 2015, <https://www.forbes.com/sites/ilyapozin/2015/11/19/6-innovative-technologies-designed-to-improve-our-safety/>.

<sup>5</sup> “Data Governance in the Age of Exponential Technology,” *Information Week*, December 28, 2018, <https://www.informationweek.com/big-data/data-governance-in-the-age-of-exponential-technology/a/d-id/1333558>.

quires supplying reliable data to responsible agencies. Therefore, governments need to acquire skills in data governance alongside traditional governance practices. Some government agencies have recently begun moving from data centers to cloud computing.<sup>6</sup> However, industry sources suggest that public authorities in many countries have resisted moving government data to the cloud and only 10-20 percent of government work uses the cloud,<sup>7</sup> a sign that many governments are poorly prepared for this qualitative change.

Innovative technologies of today do not have the same properties as the systems of the past. Among the critical elements are small pieces of hardware such as processors, graphics cards, and miniature webcams, or intangibles such as dedicated software, algorithms, or technical know-how associated with machine learning and AI development. Moreover, these innovative technologies tend to be dual-use. For example, a drone equipped with day and night vision cameras and a radar for use in geological mapping surveys can become an instrument for military or law enforcement surveillance by simply changing the end-user.<sup>8</sup> Similarly, while encryption of telecommunications data is necessary to protect business or security operations from competitive intelligence, it may also be used to conceal organized criminal activity from an investigation by law enforcement agents.<sup>9</sup> And machine intelligence that has been employed to refine internet browser search platforms can also be applied to the means of warfare, from data fusion to autonomous unmanned weapons systems and cyberwar. Such factors make the most advanced technologies difficult to control by traditional export control regimes.<sup>10</sup>

To make matters more complicated, artificial Intelligence turns technologies into “black boxes” that, intentionally or not, maybe opaque even to experts.<sup>11</sup> Non-specialists in governments and society may, for all intents and purposes, be technically illiterate vis-à-vis AI-based devices, raising further challenges to their

---

<sup>6</sup> Barb Darrow, “Why the U.S. Government Finally Loves Cloud Computing,” *Fortune*, September 2, 2016, <https://fortune.com/2016/09/02/us-government-embraces-cloud/>.

<sup>7</sup> IBM, “Transforming Government with Cloud Technologies,” <https://www.ibm.com/downloads/cas/MEK8LK2B>.

<sup>8</sup> Pix4D, “4 Reasons Drones Will Revolutionize Accident Scene Response,” Medium.com, May 26, 2016, <https://medium.com/the-science-of-drone-mapping/4-reasons-drones-will-revolutionize-accident-scene-response-a1db234eecf>.

<sup>9</sup> Europol, “Internet Organised Crime Threat Assessment 2018,” <https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018>.

<sup>10</sup> Jade Leung, Sophie-Charlotte Fischer, and Allan Dafoe, “Export Controls in the Age of AI,” *War on the Rocks*, August 28, 2019, <https://warontherocks.com/2019/08/export-controls-in-the-age-of-ai/>.

<sup>11</sup> Will Knight, “The Dark Secret at the Heart of AI,” *MIT Technology Review*, April 11, 2017, <https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/>.

effective governance and control.<sup>12</sup> AI specialists are quickly becoming one of the most sought-after resources in the new global economy. Their importance in driving further innovation and their concentration in a handful of the largest global tech firms are becoming an issue of national well-being in the coming decades and a component of geopolitical competition, particularly with China.<sup>13</sup> In a recent example, the President of the United States issued the *Executive Order on Maintaining American Leadership in Artificial Intelligence*. Among other things, the Order provides for changes in immigration policy, allowing to recruit and retain specialists in the field of AI development<sup>14</sup> – yet another sign of the importance of long-term technological leadership.

As there will be many different actors working on transformative technologies across the public and private sectors, new tools of security governance are needed that can encompass non-governmental actors and commercial actors in the shaping of national security. Thus, the governments of today need to find ways to cooperate effectively with large private enterprises, small startups, NGOs, universities, research institutes, and even individuals. Only in such a way can they keep abreast of developments and yield a degree of influence and control over the activities of the private entities if they constitute a threat to the country's national security or political stability.

## Innovative Technologies and the Civic and Political Sphere

Innovative technologies are increasingly affecting the quality and nature of the political sphere through several interrelated processes. The media and information landscape has undergone important changes, and a large proportion of individuals within the body politic now receive much of their news through social media.<sup>15</sup> Social media affects the way that information is consumed and opinions are formed.<sup>16</sup> Consumers of social media have become subject to an “echo

<sup>12</sup> See Amitai Etzioni and Oren Etzioni, “Should Artificial Intelligence Be Regulated?” *Issues in Science and Technology* 33, no. 4 (Summer 2017), <https://issues.org/perspective-should-artificial-intelligence-be-regulated/>.

<sup>13</sup> Ann Scott Tyson, “In Race to Dominate AI, US Researchers Debate Collaboration with China,” *The Christian Science Monitor*, May 3, 2019, <https://www.csmonitor.com/World/Asia-Pacific/2019/0503/In-race-to-dominate-AI-US-researchers-debate-collaboration-with-China>.

<sup>14</sup> “Maintaining American Leadership in Artificial Intelligence,” Executive Order 13859 of February 11, 2019, <https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence>.

<sup>15</sup> In 2018 some two-thirds or 68% of Americans accessed news on social media. Elisa Shearer and Katerina Eva Matsa, “News Use Across Social Media Platforms 2018,” *Pew Research Center*, September 10, 2018, <https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/>.

<sup>16</sup> Ana Lucía Schmidt, *et al.*, “Anatomy of News Consumption on Facebook,” *Proceedings of the National Academy of Sciences of the United States of America* 114, no. 12 (March 2017): 3035-3039, <https://doi.org/10.1073/pnas.1617052114>, <https://www.pnas.org/content/114/12/3035>



chamber” effect due to personalized search engine algorithms that tend to steer us towards those who think like us, filtering the articles and websites that are returned in online searches and narrowing the number of news sources we select.<sup>17</sup> The resulting “filter bubble” delivers articles that tend to reflect, reinforce and amplify our existing beliefs.<sup>18</sup> Further, the more active a community (of like-minded individuals) is on social media, the more segregated it is from differing views, and the more polarized its views become.<sup>19</sup>

As intelligent applications have progressed, so has the potential to manipulate and polarize political discourse.<sup>20</sup> Digital technologies can perform face swaps in real time; Adobe is creating a “Photoshop for audio” that can edit dialogue as easily as a photo; Canadian Lyrebird offers a service that can fake an individual voice based on only a few minutes of audio. When Google made its TensorFlow code open-source, it swiftly led to FakeApp, enabling a convincing swap of someone’s face onto footage of somebody else’s body.<sup>21</sup> Recently, the company OpenAI has created a fake text editor that reportedly is so good at imitating a given writing style and subject that they have not released it for fear of its malicious use.<sup>22</sup> In the future, the corruption of data and deliberate misinformation using these technologies may undermine national justice systems and initiate or aggravate existing conflicts. The pervasive penetration of the Internet and the ease with which anonymous actors can spread mis- and dis-information has opened democratic systems to political manipulation. As demonstrated by the now-defunct Cambridge Analytica—the data firm which improperly accessed the user data of up to 87 million Facebook users to build voter profiles in attempts to sway the 2016 US presidential election in favor of Donald Trump and was implicated in misinformation that swayed the UK Brexit referendum—the misuse of such technologies has a significant potential to confuse public discourse and sow discord.

---

<sup>17</sup> Schmidt, *et al.*, “Anatomy of News Consumption on Facebook.”

<sup>18</sup> Eli Pariser, “Beware Online ‘Filter Bubbles,’” *TED2011*, March 2011, [https://www.ted.com/talks/eli\\_pariser\\_beware\\_online\\_filter\\_bubbles](https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles).

<sup>19</sup> Roheeni Saxena, “The Social Media ‘Echo Chamber’ is Real,” *Ars Technica*, March 13, 2017, <https://arstechnica.com/science/2017/03/the-social-media-echo-chamber-is-real/>.

<sup>20</sup> This 100% fake video of Barack Obama vividly demonstrates the corruption of what was once considered hard data. See James Vincent, “Watch Jordan Peele Use AI to Make Barack Obama Deliver a PSA about Fake News,” *The Verge*, April 17, 2018, <https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peelee-buzzfeed>.

<sup>21</sup> Tad Friend, “How Frightened Should We Be of A.I.?” *The New Yorker*, May 7, 2018, <https://www.newyorker.com/magazine/2018/05/14/how-frightened-should-we-be-of-ai>.

<sup>22</sup> Alex Hern, “New AI Fake Text Generator May be too Dangerous to Release, Say Creators,” *The Guardian*, February 14, 2019, <https://www.theguardian.com/technology/2019/feb/14/elon-musk-backed-ai-writes-convincing-news-fiction>.

The problem has been publicly recognized. According to the recent survey, a majority of Europeans (85 %) described fake news as a problem in their countries. A further eight out of ten (83 %) said “fake news” was a problem for democracy in general, while over a third (39 %) said national authorities should be responsible for combating the rise of “fake news.”<sup>23</sup>

Furthermore, the new surveillance technologies empower security institutions to a degree that renders traditional methods of government oversight ineffective. A case in point is the commercial spyware called Pegasus. Once installed, it allows operators unlimited access to private data in mobile phones, including passwords, contact lists, calendar events, text messages, and live voice calls from popular apps. The Citizen Lab has identified 45 countries where Pegasus operators may have been conducting surveillance operations. At least ten operators appeared engaged in cross-border surveillance.<sup>24</sup> Even if laws allow only for remote electronic invigilation without recording or storing the data, given the technical abilities of the spyware, it would be very difficult to prove the intelligence services to be on the wrong side of the law unless they admitted to wrongdoing. Thus, executive oversight of the services is becoming illusory, as is the protection of privacy for citizens.

### **The New Economic Logic of “Surveillance Capitalism”**

The impact of innovative technologies now extends well beyond the realms of law enforcement, internal and national security and warfare, and beyond the manipulation of the political and civic spheres. We witness the emergence of complex, data-driven, interconnected technological systems that penetrate all spheres of human activity. Digital technologies permeate our activities, words, images, and interactions in our homes and places of commerce, media, education, leisure, and communities, and our social interactions. Moreover, the information from these technologies is harvested to an unprecedented degree, packed into highly predictive profiles, and openly sold to any interested actor, with an almost complete lack of legal constraint or government oversight.

According to Shoshana Zuboff, the profound changes wrought by the relatively unconstrained and unregulated development of innovative technologies over the past 20 years have given rise to a new economic logic that is the successor of industrial capitalism. Data tracking and mining of web engines and social media applications, smart devices, and sensors enable commercial actors to compile detailed profiles of individuals, their daily habits and activities, their likes

---

<sup>23</sup> “New Report Highlights Inconsistent Approach to Combating Disinformation,” Oxford Internet Institute, University of Oxford, August 22, 2019, <https://www.oii.ox.ac.uk/news/releases/new-report-highlights-inconsistent-approach-to-combatting-disinformation/>.

<sup>24</sup> Bill Marczak, *et al.*, “Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries,” *The Citizen Lab*, University of Toronto, September 18, 2018, <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.

and dislikes. Volumes of data on every activity, spoken or written word, and even the emotions we display are collected by the devices and technologies that surround us and resold as predictive information by and to commercial actors in a new economic and social logic of accumulation that has been termed “surveillance capitalism.”<sup>25</sup> In surveillance capitalism, profits derive from the surveillance and modification of human behavior. Data based on real-time surveillance of people’s daily activities, conversations, emotions are monetized and sold and resold to companies that want to influence people and modify their behavior at scale.<sup>26</sup> According to Zuboff, all those developments have led to the creation of a behavioral futures market that trades in predictions of human activity.<sup>27</sup> This market in predictive human futures is extremely lucrative: Google’s profits increased 3,500 percent over four years on the back of its rapid development in this area. Surveillance capitalism is now ubiquitous, with the impetus to Hoover behavioral data encompassing not only Silicon Valley firms and technologies but other industries and firms.<sup>28</sup>

But while the big data collection and packaging is pervasive, serious information asymmetries hamper understanding by societies and governments. Commercial actors assert proprietary control over such data, which is combined and resold manifold times, with an underlying logic of using it to influence future behavior. Google Nest, a smart home temperature system, provides a telling example. Its data scraping and collection through the related suite of apps and features is so extensive that it would require a diligent client who installs a single thermostat to review almost 1000 related privacy agreements.<sup>29</sup> This indicates the additional problem of lack of informed consent to the collection and reselling of data about consumers. Such systems pose huge challenges to the ability of people and their governors to understand and govern them. Developments in scope and scale have overwhelmed and bypassed traditional approaches to governing these spheres through law and policy, to the extent that a growing number of observers maintain they pose unprecedented implications for human agency and autonomy.<sup>30</sup>

---

<sup>25</sup> Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

<sup>26</sup> Shoshana Zuboff, “The Secrets of Surveillance Capitalism,” *Frankfurter Allgemeine Zeitung*, March 5, 2016, <https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html>.

<sup>27</sup> Zuboff, *The Age of Surveillance Capitalism*.

<sup>28</sup> Shoshana Zuboff, “Facebook, Google, and a Dark Age of Surveillance Capitalism,” *Financial Times Magazine*, January 25, 2019, <https://www.ft.com/content/7fafec06-1ea2-11e9-b126-46fc3ad87c65>.

<sup>29</sup> Guido Noto La Diega and Ian Walden, “Contracting for the ‘Internet of Things’: Looking into the Nest,” Queen Mary School of Law Legal Studies Research Paper no. 219/2016, February 1, 2016, <https://ssrn.com/abstract=2725913>.

<sup>30</sup> James Bridle, *The New Dark Age: Technology and the End of the Future* (London: Verso Books, 2018).

## Regulations

So far, EU responses to the advent of transformative technologies have been slow and disappointing on most counts and failed to deliver qualitative change in legislative frameworks of member states. For example, the regulatory activities of the EU in the realm of Artificial Intelligence do not match the pace of development of those technologies. The EU has so far elaborated the set of EU guidelines for trustworthy AI being: (1) lawful, (2) ethical, and (3) robust, and is now entering the stage of the high-level committee and voluntary pilot projects.<sup>31</sup> It is hardly an adequate response to the technological revolution and does not yet require a standardized and coordinated response from national legislatures in member countries.

Introducing new EU regulations fostering the use of new technology for European security has been slow, too, as is the case for drone flights. EU regulators since 2015 have failed to go beyond establishing the European Union Aviation Safety Agency and updating aviation safety rules.<sup>32</sup> Consequently, despite successful testing of drones for maritime surveillance,<sup>33</sup> Frontex, for example, has been prevented from using unmanned aerial vehicles along the Mediterranean coast due to a lack of regulations.

In some cases, regulatory efforts have even inadvertently over-exposed the EU citizens to electronic surveillance, as in the case of the EU directive on data retention in telecommunication.<sup>34</sup> The directive aimed to enhance efforts against terrorism. However, it also paved the way to intensified surveillance of citizens by intelligence services in several European countries such as the Czech Republic, Cyprus, Estonia, Finland, France, Germany, Ireland, Poland, and the UK by embedding the rights of services to unrestricted use of telecommunication data in national laws. Predictably, the services started using the data out of pro-

<sup>31</sup> European Commission, "Ethics Guidelines for Trustworthy AI," <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

<sup>32</sup> European Commission, "Impact Assessment Accompanying the Document 'Proposal for a Regulation of the European Parliament and of the Council on Common Rules in the Field of Civil Aviation and Establishing a European Union Aviation Safety Agency, and Repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council'," [https://eur-lex.europa.eu/resource.html?uri=cellar:ec9e79f3-9ce9-11e5-8781-01aa75ed71a1.0001.02/DOC\\_2&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:ec9e79f3-9ce9-11e5-8781-01aa75ed71a1.0001.02/DOC_2&format=PDF).

<sup>33</sup> Frontex, "Frontex Begins Testing Unmanned Aircraft for Border Surveillance." See also Ilkka Tikanmäki, Jari Räsänen, Harri Ruoslahti, and Jyri Rajamäki, "Maritime Surveillance and Information Sharing Systems for Better Situational Awareness on the European Maritime Domain: A Literature Review," in *Digital Transformation, Cyber Security and Resilience of Modern Societies*, ed. Todor Tagarev, Krassimir T. Atanasov, Vyacheslav Kharchenko, and Janusz Kacprzyk (Cham: Springer, 2021), 117-135, [https://doi.org/10.1007/978-3-030-65722-2\\_8](https://doi.org/10.1007/978-3-030-65722-2_8).

<sup>34</sup> Directive 2006/24/EC of the European Parliament and of the Council of March 15, 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, abolished 2014.

portion and without connection to national security threats. In Poland, for example, the intelligence services asked for disclosure of telecommunication data a record 2.35 million times in 2014.<sup>35</sup>

Privacy protection has been another challenge to EU regulators. While the General Data Protection Regulation (GDPR) establishment is a step in the right direction in terms of privacy, it is an inadequate response to the major issues raised by innovative technologies and the behavioral futures market. The European Commission, alongside the national governments, was passive and ineffective in holding Cambridge Analytica and Facebook responsible for interfering in national electoral processes and undermining democratic systems. The outcome of the Brexit vote was heavily influenced by the largely illicit actions of Facebook and Facebook-related campaigns, breaking British electoral laws and subverting democratic procedures.<sup>36</sup> However, attempts to hold Mark Zuckerberg and Facebook accountable have failed. And since the Brexit vote, the practices of collecting behavioral data to predict and influence future behavior have grown apace.

## **Conclusions**

As innovative technologies transform the economic, security, and arguably political logic of contemporary life, policy-makers and legislators need to become far more technologically literate. The Congressional hearings of April 2018 in which Mark Zuckerberg responded to questions posed by US senators and members of the house of representatives clearly demonstrated the failure of many in the American governing class to understand some of the most basic aspects of modern digital platforms.<sup>37</sup> However, the problem goes even deeper, reflecting our inability to find ways to understand and think about exponential innovative technological change and the convergence of multiple technologies. Better understanding by policy makers of these processes is necessary if laws on exponential technologies are to be effectively regulated and controlled, and if governments aim to effectively minimize the harm to their citizens and political system from their effects. Regulations should not only concentrate on the technological or organizational side of affairs; legislators should also find ways to provide for greater political and social accountability of corporate organizations involved in developing, selling, or applying innovative technologies.

---

<sup>35</sup> "Rok z ustawą inwigilacyjną. Co się zmieniło," *Fundacja PANOPTYKON*, January 18, 2017, <https://panoptykon.org/biblio/rok-z-ustawa-inwigilacyjna>.

<sup>36</sup> See Carole Cadwalladr, "Facebook's Role in Brexit and the Threat to Democracy," TED2019, April 2019, [https://www.ted.com/talks/carole\\_cadwalladr\\_facebook\\_s\\_role\\_in\\_brexit\\_and\\_the\\_threat\\_to\\_democracy](https://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy).

<sup>37</sup> "Zuckerberg Explains the Internet to Congress," <https://www.youtube.com/watch?v=ncbb5B85sd0>.

## Disclaimer

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

## About the Authors

Dr. **Marina Caparini** is a Senior Researcher and Director of the Governance and Society Programme at SIPRI. Her research focuses on peacebuilding and the nexus between security and development. Marina has conducted research on diverse aspects of security and justice governance in post-conflict and post-authoritarian contexts, including police development, intelligence oversight, civil-military relations, and the regulation of private military and security companies. She has recently focused on police peacekeeping and capacity-building, forced displacement, and organized crime. Prior to joining SIPRI in December 2016, she held senior positions at the Norwegian Institute for International Affairs, the International Center for Transitional Justice, and the Geneva Centre for the Democratic Control of Armed Forces.

E-mail: [marina.caparini@sipri.org](mailto:marina.caparini@sipri.org)

**Agnieszka Gogolewska** - see the short CV on p. 32 of this issue.

## *Connections: The Quarterly Journal* **Submission and Style Guidelines**


*Connections* accepts manuscripts in the range of 2,000 to 5,000 words, written in a lucid style for a target audience of informed defense and security affairs practitioners and academics. All manuscripts should be submitted to the *Connections* editorial office electronically at [PfPCpublications2@marshallcenter.org](mailto:PfPCpublications2@marshallcenter.org) or uploaded to the journal website via <https://connections-qj.org>. They should feature the author's name, current institutional affiliation, and a provisional title at the top of the first page, and should include footnotes where necessary. Additionally, authors should provide a manuscript abstract and keywords.

Preferred themes for journal future editions include:

- Arctic Exploitation and Security
- Arms Control and European Rearmament
- Challenges and Opportunities in Intelligence Sharing
- Countering and Preventing Violent Extremism
- Cybersecurity
- Defense Institution Building
- Future Security Scenarios
- Hybrid Warfare
- Limitations of Naval Power
- Migration and Refugees
- NATO's Unstable Periphery
- Putin's Russia: A Threat to Peace or a Threat to Itself?
- Terrorism and Foreign Fighters
- Trends in Organized Crime

For questions on footnotes and references, please refer to the Chicago Manual of Style, at [http://www.chicagomanualofstyle.org/tools\\_citationguide.html](http://www.chicagomanualofstyle.org/tools_citationguide.html).

Unsolicited manuscripts are accepted on a rolling basis at the discretion of the PfPC Editorial Board.



**Authoritarian systems are based on intelligence and state security services protecting the ‘state’, if not the people. But what happens to them once the totalitarian state goes out of business? This special issue of Connections looks at successful and promising transitions and transformations towards the democratic Rule of Law and seeks to establish commonalities in the transition processes.**

**For all information regarding  
CONNECTIONS, please contact:**

**Partnership for Peace – Consortium  
Managing Editor – LTC Torsten Stauffer  
Gernackerstrasse 2  
82467 Garmisch-Partenkirchen, Germany  
Phone: +49 8821 750 2333  
E-Mail: [PfPCpublications2@marshallcenter.org](mailto:PfPCpublications2@marshallcenter.org)**

**ISSN 1812-1098  
e-ISSN 1812-2973**

