Int. j. adv. multidisc. res. stud. 2026; 6(4):891-895

Received: 08-06-2026
Accepted: 18-07-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Selected Aspects of Counterintelligence Protection of the Polish Coast in the Polish People's Republic

Rafał Piotr Depczyński
Institute of Security and Administration, Pomeranian University, Starogard Gdanski, Poland

Corresponding Author: **Rafał Piotr Depczyński**

Abstract
This article explores selected aspects of counterintelligence protection of the Polish coast during the period of the Polish People's Republic (PPR). Most of the material used for this study was obtained from the private, declassified archives of a now-deceased officer of the Internal Military Service of the PPR. Additional insights were drawn from an interview conducted with him prior to his passing. The purpose of the article is to shed light on the nature of counterintelligence measures undertaken by officers in the Polish Navy during the mid-1970s, and to examine how intelligence threats were perceived, analysed and addressed at the time.

Keywords: Counterintelligence, Navy, Classified Information, Counterintelligence Protection, Espionage

Introduction

The issue of protecting classified information in the armed forces holds immense significance for the national security of any state. History shows that failing to uphold basic principles of secrecy has at times led to irreversible consequences—not only for specific military operations but also for national security as a whole. In the mid-1970s, the Armed Forces of the Polish People's Republic numbered over 350,000 soldiers. Most were conscripts undergoing compulsory military service, which involved mandatory reporting for duty and two years of training.[1]

As a result, the military often enlisted individuals with little formal education and no real understanding of the sensitivity of the information they would encounter. It was not uncommon for a conscript with only a primary school education to obtain professional qualifications—such as heavy vehicle driving licence—during their service. There were also cases where conscripts assigned to Naval units saw the sea for the first time only upon arrival at their designated base. Given such realities, it is clear that protecting classified information and conducting effective counterintelligence during this time posed significant challenges. Thus, a key research problem lies in the objective evaluation of the counterintelligence efforts of the PPR, particularly in relation to the protection of classified information in the armed forces, especially considering the technical capabilities available during that period.

The primary aim of this article is to present the methods employed by military counterintelligence officers of the Polish People's Republic in the mid-1970s, as well as their professional approach to the issue of information protection. Interviews with former officers who served in the Internal Military Service during that period offer valuable insight into the structure and practices used to safeguard military secrets in the PPR. These insights provide a broader understanding of counterintelligence operations during the period in question. The publication is divided into several parts. The introduction is followed by a discussion of general aspects of the military secrecy protection system in the PPR Armed Forces, including the terminology and definitions used at the time, as well as examples of how the special services operated during that period. The analysis enables the formulation of relevant, objective conclusions. The article also presents a number of real-life incidents that occurred along the Polish coast during the specified timeframe. One of the key advantages of this paper is that it draws on firsthand accounts from individuals directly engaged in counterintelligence operations.

[1] From 1990 to 2009, the length of compulsory military service was progressively shortened—to 18, 15, 12, and finally 9 months in the later period.

General Aspects of Classified Information Protection

An analysis of the classified information protection system in the PPR Armed Forces reveals that secrecy protection played a vital role in the system—serving both internal needs and external security objectives. The effectiveness of this system was determined by its capacity to efficiently prevent unauthorised access to classified information and to promptly detect and address any breaches that might occur. Its overall effectiveness was influenced by both objective and subjective factors, including primarily:

- Activities carried out by potential adversaries, especially those exploiting the contacts between Polish citizens and foreigners;
- The degree of awareness within the entire personnel of the Polish Armed Forces, as well as among employees of state institutions, regarding the threat of espionage and the need to guard against it, especially among those with access to classified data;
- The efficiency of the protection system as a whole, understood as a set of properly directed and consistently implemented normative, organisational and technical measures.

The definition of information constituting state and official secrets in 1970s Poland was established by the Regulations on the Protection of Secrets in the Armed Forces of the Polish People's Republic (ref. Gen. Staff 675/75). This normative act provided definitions for numerous concepts.

The term information was understood to encompass any data shared orally or contained in:

- Written documents, copies, plans, maps, technical documentation, publications, images, sketches, drawings, photographs, audio tapes or other physical media;
- Devices, tools, instruments (including prototypes and models), or other objects or devices.

The term state secret referred to information whose disclosure to unauthorised persons could jeopardise the national defence, state security or other critical political or economic interests of the PPR. Meanwhile, the term official secret referred to information acquired by an adversary or soldier in connection with their work or service, the disclosure of which to unauthorised individuals jeopardise a socially justified interest.

Other terms were defined in subsequent normative acts. For example, under Article 124 of the Penal Code in force at the time (1969), espionage was understood as the act of transmitting any information of interest to a foreign intelligence service. Unauthorised persons were defined as individuals without a permit for handling classified work, or those in possession of such a permit but not officially involved in the specific matters at hand. Classified information referred to non-public information constituting a state or official secret, marked with one of the following classification levels: 'Top Secret—Special Importance,' 'Top Secret' or 'Confidential'.[2] The definition of classified work encompassed all official activities involving the possession, processing or any use of information constituting a state or official secret. Military secrets were defined as state or official secrets specifically related to military affairs.

Importance of Information Acquisition and Security

The struggle between states to protect their own information and acquire that of others has existed for centuries and continues to this day. The experiences of the First and even more so the Second World War made it abundantly clear that national security depended heavily on the protection of sensitive information and the success of intelligence operations. The imperative of employing all available means of reconnaissance is nearly universally acknowledged among military strategists. Intelligence on enemy forces, capabilities, and intentions is fundamental to shaping strategic plans and guiding operational choices.

The American intelligence theorist Sherman Kent identified several key areas typically pursued by foreign intelligence services:

- The size of the armed forces, their organisation and tactical operations;
- Weapons depots, airbases, maintenance facilities, shipyards;
- Military conscription methods and their effectiveness;
- Training, quantity and quality of officers;
- Data on senior military leadership;
- Command staff efficiency;
- The strength and characteristics of military traditions;
- The degree of societal respect for and perception of the armed forces;
- Aviation navigation hazards (e.g. weather, wind, gases, natural and man-made obstructions such as power lines);
- Air defence capabilities and systems;
- Camouflage techniques and their effectiveness;
- Troop morale and the wellbeing of their families;
- Level of civilian defence readiness.[3]

Intelligence operations are based on both the sources and the methods used to acquire information. According to U.S. intelligence expert Harry Ransom, American intelligence historically relied on the following sources to varying degrees:

- Covert operations, clandestine sources and secret agents – 20%;
- Media, radio broadcasts, tourists and publications – 25%;
- Reports from U.S. government agencies operating abroad – 25%;
- Military and defence attachés – 30%.[4]

It should be emphasised that in intelligence work, the decisive factor is primarily the volume of information delivered, rather than its perceived importance. In terms of significance, 20% of the information may outweigh—and often does outweigh—the same or even a substantially higher percentage obtained from other sources.

In the 1970s, foreign intelligence collected data from every possible source: pilots flying over East Germany with film cameras, articles in the Soviet press, and emigrants arriving from behind the 'Iron Curtain'. For trained intelligence

[2] Currently, pursuant to Article 5 of the Act of 5 August 2010 on the Protection of Classified Information, the applicable classification levels are: 'Top Secret', 'Secret', 'Confidential' and 'Restricted.'

[3] See S. Kent, *Strategic Intelligence for American World Policy*, Princetown University Press, 1949.

[4] See H. Ranson, *Central intelligence and national security*, Cambridge 1958.

officers, even individuals like a worker in an ammunition plant, a dock labourer in a major port or a farmer counting military vehicles near a road could be considered valuable information sources.

It is important to underline that humans remain the key element in both the acquisition and protection of classified information. Although modern intelligence agencies now utilise a wide range of advanced technical methods, they will never cease relying on human sources. This is due to the fact that certain highly sensitive pieces of information simply cannot be obtained without human involvement. These include:

- Personal attributes of senior military leaders;
- Data on the attitudes and dispositions of national leaders;
- Intelligence on the long-term intentions of personnel, and operational and technical departments in matters of national defence.

Such intelligence is often acquired either through direct observation carried out by intelligence personnel or by exploiting excessive and careless talkativeness. History offers numerous examples of intelligence successes and failures directly linked to indiscretions by individuals from various backgrounds—proving that loose talk can shape the outcome of a conflict.

In January 1916, while the United States was still neutral, an American businessman travelling through Central Europe found himself in Warsaw. At a formal dinner he attended, he was seated next to a high-ranking German staff officer. The officer engaged him in conversation and began criticising the U.S. for siding with Britain and France. He believed it would come to nothing, as the war would soon be over. He went on to reveal that Germany was preparing a major offensive on Verdun, which he claimed would decisively end the war. In the course of his indiscreet remarks, he went so far as to disclose the exact date of the offensive—20 February 1916. This information soon reached Marshal Joseph Joffre, who, taking into account other intelligence as well, judged it credible and ordered preparations to repel a German attack. The offensive did indeed begin on the night of 20–21 February 1916, and would go down in history as the largest battle of the First World War. The fact that it ended in a French victory was, at least in part, a consequence of the indiscretion and bravado of a German officer.[5]

Foreign Intelligence Operations in the Polish People's Republic

In the 1970s, foreign intelligence activity in Poland frequently involved Western diplomats surveilling military installations, primarily through observation and photography. Increased surveillance activity was also detected in the coastal region of Poland, where dozens of incidents involved diplomatic staff near naval units and facilities. During military exercises held from 3–10 September 1974, several diplomats, including military attachés from the U.S., Great Britain and Canada, were observed in the Hel and Tricity areas.[6]

This activity also extended to foreign tourists engaging in surveillance of military infrastructure. In a single year during the mid-1970s, authorities recorded nearly 200 instances of foreign nationals exhibiting interest in military facilities. These included photographing military objects, unauthorised entry onto military premises, suspicious behaviour and conducting surveillance. As a result, over 100 individuals were detained and handed over to the state security services. In about half of the cases, administrative measures were taken (such as expulsion or fines), and in one case, a formal investigation was initiated.

Among those conducting surveillance, the majority—over 120 individuals—were citizens of the Federal Republic of Germany. Most were interested in military sites in northwestern Poland. At Polish Navy facilities, approximately 70 incidents of foreign nationals trespassing on military grounds were recorded, nearly half involving taking photographs. Investigations revealed that foreign tourists—mostly from West Germany, East Germany and Sweden—often rented accommodation in advance from professional military personnel.

Foreign intelligence efforts also included radio-electronic reconnaissance, which remains one of the fundamental methods of obtaining information about other states. This was carried out using technical equipment installed on reconnaissance aircraft, naval vessels or at electronic intelligence stations, through the systematic interception of military, diplomatic and commercial radio communication networks. Western countries focused on tracking changes in the positioning, size and defence capabilities of Warsaw Pact military forces. According to U.S. sources, 80% of intelligence was gathered by intercepting signals and information transmitted via communication systems of various countries.

Press intelligence was also a major component of espionage activities. The so-called open-source intelligence (OSINT) continues to hold considerable importance to this day. Newspapers and specialised military publications have long been, and continue to be, subject to systematic and meticulous analysis by adversarial intelligence services. This is primarily due to the fact that the materials published in such outlets cannot omit key new developments in national defence. Moreover, the boundary between what is general and what is specific is often difficult to define. In many cases, article content reflected not merely individual opinions but also doctrines developed within military staff divisions. Press intelligence experts search for precisely such insights and attempt to reconstruct broader conclusions from these fragments. Evaluative elements found in publications allow analysts to draw general conclusions regarding trends in the development of a state's military potential.

Ultimately, foreign intelligence operations also involved agent-based activities. Cases of espionage—both carried out and attempted—recorded in the mid-1970s show that foreign intelligence networks were a constant and serious threat to state and official secrets in the Polish People's Republic. Agents of foreign services were often recruited from among tourists or merchant ship crews. Consequently,

[5] W. Łuków, *Motywy ujawniania tajemnicy wojskowej, Biuletyn Głównego Zarządu Politycznego Wojska Polskiego*, Publishing House of the Ministry of National Defence, Warsaw 1974., p. 10.

[6] The data used in this article are based on oral information provided by a now-deceased officer of the Military Internal Service of the Polish People's Republic.

PPR military intelligence agencies maintained close surveillance of such individuals, particularly foreign sailors disembarking on Polish soil.[7]

Classified Information Protection System in the Polish People's Republic

An effective system for the protection of classified information is designed to counteract the multifaceted, intensive and continuous intelligence activities of foreign states. Its core components include:

- Building a constant awareness of intelligence threats and the need for protection, supported by the active involvement of all military personnel. This awareness must be continuously reinforced through training, education and preventive measures.
- A reliable and integrated classified information protection system, combining legal, organisational and technical measures.
- Fostering awareness of the constant threat posed by foreign intelligence and the need to guard against it, considered both in terms of individual responsibility for one's conduct and supervisory responsibility for maintaining compliance with secrecy protocols among subordinate personnel.

The classified information protection system includes the following components:

- Protecting military areas and facilities against external reconnaissance;
- Using camouflage and deception techniques;
- Protecting classified documents;
- Protecting classified information in press, broadcast media and military technical publications;
- Ensuring ICT system security;
- Securing classified information when using technical communication systems;
- Guarding against radio-electronic surveillance;
- Managing secrecy in official dealings with civilian entities;
- Complying with personnel security regulations for individuals involved in sensitive duties;
- Protecting classified information in private interpersonal communications.

A well-functioning classified information protection system also placed significant emphasis on the recordkeeping of official foreign travel by military personnel. Under the legal framework in force at the time, soldiers were required to obtain official authorisation before travelling abroad. To that end, soldiers submitted a written, formal request to their superiors, who then notified the counterintelligence service. The latter maintained records of such trips and assessed it for patterns or repeated travel by the same individual.

Between 1944 and 1989, the Polish Armed Forces maintained dedicated departments and units responsible for the protection of classified information. While the structure and subordination of these bodies varied over time, one of their constant and primary objectives was the protection of state secrets. To this end, these services conducted, among other things, agent-based (operational), preventive, and analytical activities.

Agent-based operations focused primarily on detecting breaches of official or state secrecy and taking suitable action. There were documented instances of classified information being disclosed not only by sailors and conscripted soldiers, but also by non-commissioned officers and even commissioned officers.

One example of the rapid response by the Military Counterintelligence Service of the Polish People's Republic in the 1970s to an attempted recruitment of a Polish Navy officer involved a case in which a young, well-groomed Navy captain, travelling in uniform on official duty aboard an express train from Gdynia to Warsaw, was approached in his compartment by an attractive woman, who later turned out to be an agent of a foreign intelligence service. Friendly conversation, shared interests, and the private setting (they were alone in the compartment) led the two to plan lunch together the next day and to reserve rooms on the same floor in a Warsaw hotel. Neither of them, however, was aware that the officer was being accompanied by a so-called 'escort'—a special services officer assigned to discreetly safeguard the classified documents the captain was transporting. The swift response of the 'escort' officer triggered an immediate operation that not only prevented the disclosure of classified information to a foreign intelligence service but even led to the recruitment of an asset for Polish intelligence within the home country of the aforementioned female agent.

In particularly sensitive cases involving the transport of 'top secret – special category' documents along the entire route from the Navy Headquarters in Gdynia to the Ministry of National Defence in Warsaw, the officer responsible for the documents was assigned overt (but covertly armed) protection, usually in the form of two additional officers whose presence was known to the courier. The procedures in such cases also required the deployment of an additional 'escort' officer—armed with a concealed sidearm—whose presence was unknown to all the previously mentioned personnel.

Unfortunately, despite these safeguards, there were instances in which classified information leaked to unauthorised individuals in remarkably trivial ways. In one such case, a conscripted sailor serving in a Navy unit shared numerous details about training and operational activities with a former colleague who had left the service. He mentioned, for instance, that flights on certain aircraft were suspended because the pilots were away, that the unit had received a prototype plane equipped with new systems, that a tear gas alert had taken place, and that a group of pilots was scheduled for training missions on a specific date. Importantly, every detail he shared was true.[8] Naturally, counterintelligence responded appropriately to the incident.

Conclusion

The incidents outlined above indicate significant involvement by the PPR's Military Counterintelligence Services in safeguarding the Polish coastline from foreign intelligence threats. Their meticulous handling of the issues reflects a well-organised structure and a high level of commitment among the personnel in these units.

[7] For a more detailed account of a counterintelligence operation conducted by PRL services against a West German spy, see: R.P. Depczyński, *Wojna wywiadów. Sprawa Dietricha Wolfa*, Publishing House of Circle No. 31 of the Association of Former Officers of Military Intelligence of the Polish People's Republic, Gdynia 2019.

[8] W. Łuków, Motywy ujawniania …, op. cit., p. 47.

In terms of the aspects presented, the author believes that counterintelligence units performed their duties effectively. Such effectiveness was likely made possible by their virtually unrestricted budget and the relatively advanced technical resources available to them at the time. During the period under review, the Polish coastline was repeatedly targeted in attempts to access military and classified state information. Although it is likely that foreign intelligence agents succeeded in acquiring such information on multiple occasions, the measures outlined in this article indicate that PPR military counterintelligence was largely effective in countering these efforts.

Objectively speaking, the professionalism of these services was rooted in rigorous training and a stringent culture of accountability for any failure to perform duties. Each facility officer reported directly to the Commander of the Military Counterintelligence Service, who, during routine briefings, required precise statistical reports supported by comprehensive source documentation. Even minor discrepancies in reporting could lead to disciplinary action, often resulting in the officer's removal from military counterintelligence—a reassignment that came with the forfeiture of a significant financial bonus.

In conclusion, counterintelligence operations along the Polish coastline during the analysed period were conducted with notable effectiveness. Particularly noteworthy were the meticulous execution and substantial volume of surveillance activities. Furthermore, the thoroughness with which these tasks were carried out likely reflects a considerable commitment of military resources and personnel to safeguarding classified information.

References

1. Kent S. Strategic Intelligence for American World Policy, Wydawnictwo Princetown University Press, 1949.
2. Łuków W. Motywy ujawniania tajemnicy wojskowej, Biuletyn Głównego Zarządu Politycznego Wojska Polskiego, Publishing House of the Ministry of National Defence, Warsaw, 1974.
3. Ranson H. Central intelligence and national security, Cambridge, 1958.
4. Depczyński RP. Wojna wywiadów. Sprawa Dietricha Wolfa, Publishing House of Circle No. 31 of the Association of Former Officers of Military Intelligence of the Polish People's Republic, Gdynia, 2019.