Internal Security Review
2026, no. 34, pp. 423–441

https://doi.org/10.4467/20801335PBW.26.020.23382

ARTICLE

Communications within the state administration as the foundation of a nation's resilience: the case of Poland[1]

DAVID CYBULSKI

War Studies University

https://orcid.org/0009-0003-9195-4407

Abstract

The purpose of this article is to present the role and current state of communications among the agencies of the modern administration of the Republic of Poland. The article addresses legal, organisational, and technical aspects of communication within the state administration. It highlights serious systemic deficiencies related to the functioning of existing communication systems in the civilian structures of the state, which may affect Poland's ability to respond effectively to emerging threats to national security. The fundamental problem here is the lack of a unified state perspective on the establishment and operation of communication between its various components, namely security agencies,

[1] The article is based on the master's thesis entitled *Łączność i komunikacja administracji państwa w sytuacji zagrożenia bezpieczeństwa narodowego: na przykładzie Polski* (Eng. Communications and connectivity of public administration in situations of national security threat: the case of Poland), which was defended at the Faculty of Political Science and International Studies of the Warsaw University. The author used excerpts from chapters I, II and IV. The thesis was awarded in the 15th edition of the Head of the Internal Security Agency national contest for the best doctoral, master's or bachelor's thesis on state security in the context of intelligence, terrorist and economic threats.

emergency services, and public administration. It is therefore necessary to urgently modernise the state communications subsystem for crisis management purposes in the context of contemporary challenges.

Keywords electronic communication, telecommunications, emergency communications, crisis management

Introduction

The contemporary national security environment is characterised by evolving threats, including cyber attacks, terrorism as well as hybrid activities. In such circumstances, traditional, linear crisis management models prove inadequate, and the state's ability to respond effectively depends increasingly on the quality of information flow between key actors in the security system. In this context, the communications subsystem takes on particular importance, as it not only provides the technical infrastructure for the operations of the public administration, emergency services and entities responsible for critical infrastructure protection, but is also responsible for the smooth functioning of the entire crisis management system.

The digitalisation of administration and the growing complexity of the threat landscape mean that the effective and secure exchange of information has become essential to countering incidents that affect the functioning of the state, whether physical or digital in nature. At the same time, numerous documents, such as post-audit reports of the Supreme Audit Office, indicate that the current communications systems within the public administration are often not fully adapted to its modern operational and technological realities. This is evident, among other things, in the fragmentation of telecommunications solutions, the lack of a unified information exchange architecture, shortcomings in interoperability, as well as significant susceptibility to design errors or human errors.

The research question is: to what extent is the current public administration communications subsystem resilient to current threats to national security, and what changes could enhance its effectiveness? Answering this question requires treating communications as a complex socio-technical system in which the legal framework, organisational solutions, technologies and user competencies are mutually interdependent. The hypothesis put forward in the article assumes that the existing public administration communications system – developed over the years on a departamental basis (to meet the needs of individual departments

only) and in a piecemeal fashion – does not provide sufficient coherence or resilience against contemporary threats, and that it is possible to identify realistic ways to optimise it.

The article reviews the regulatory framework governing communications for national security purposes, covering both legislation and implementing regulations, as well as selected strategic documents. Furthermore, the main categories of risk were identified and classified – ranging from planning and design errors, through operational issues and restrictions on technological sovereignty, to cybersecurity threats. Subsequently, proposals were put forward for modernisation, covering both the integration of existing systems and the potential of new technologies, as well as the concept of an integrated national communications subsystem.

The following methods were employed: analysis of legal acts, review of the literature on national security and telecommunications, as well as analysis of the technical documentation for selected systems. Examples of solutions implemented in France and Australia were also highlighted. System analysis was also employed to treat the communications subsystem as part of a larger whole – the national security system – and to assess its functioning in terms of coherence, redundancy and resilience. The scope of the analysis has been deliberately limited to communication solutions within the public administration, excluding mass communication between citizens and military communication, which allows for an in-depth examination of the issue from the perspective of state institution.

The article forms part of a broader body of research into the modernisation of national security systems in the context of digital transformation and escalating geopolitical tensions. It argues that the issue of communications – often perceived as a technical domain – should be treated as a strategic element of national security, requiring a coherent public policy and conscious investment decisions. The proposed conclusions and recommendations may serve as a starting point both for further research and for conceptual work relating to the modernisation of the national communications subsystem of the public administration for the purposes of crisis management.

Legal framework

Ensuring the continuous and reliable exchange of information has been recognised in Poland as one of the cornerstones of national security and the efficient functioning of public administration, particularly in crisis situations, emergencies or the threat of armed conflict. As a result, an extensive system of legal acts has been created to regulate the structure, operation and protection of the systems comprising the state's

communications subsystem, covering both government systems and publicly available commercial systems capable of serving as backup communications for state authorities.

Under the *Act of 26 April 2007 on crisis management*, certain communications systems and ICT networks were classified as critical infrastructure (Article 3 point 2(b) and (c)). The Act imposes an obligation to draw up and update crisis management plans, which must also take into account ICT and communications issues (Article 6(5b)), and to establish rules governing the flow of information within the national crisis management system (Article 11(2) point 8). The Act clearly states that communications systems forming part of the critical infrastructure – both government systems and certain commercial systems – are subject to special protection against threats.

The *Act of 10 June 2016 on anti-terrorist activities* regulates the protection of ICT infrastructure against terrorist incidents and the rules governing the exchange of information between public administration bodies and services in the event of such threats. It provides, among other things, for the possibility of temporarily adapting and installing wired and wireless communications systems for the purpose of securing high-risk events, with certain exemptions from building regulations, in order to ensure communications for the relevant services (Article 13). The Act also introduces a system of alert levels and CRP alert levels (relating to Poland's cyberspace), which are declared by order of the Prime Minister. For the communications subsystem, the following tasks are particularly important in relation to the above levels: informing subordinate personnel, verifying the operation of communication systems, intensified monitoring of ICT systems and electronic communications integrity, ensuring that administrators and decision-makers are on duty, reviewing backup ICT infrastructure, as well as implementing post-incident plans at the highest terrorist threat levels[2].

The *Act of 11 March 2022 on the defence of the Homeland* provides a comprehensive description of the state's responsibilities in the field of military security, including matters relating to the organisation of communications for defence purposes. One of the central elements of the Act is the military telecommunications system (Article 17), which connects the Polish Armed Forces and the Ministry of Defence with other public administration bodies and – if necessary – with civil society organisations serving the interests of defence[3]. It is

[2] *Regulation of the Prime Minister of 25 July 2016 on the scope of undertakings carried out in particular alert levels and CRP alert levels.*

[3] *Regulation of the Minister of National Defence of 20 April 2022 on the operation of the military telecommunications system.*

designed to ensure the functioning of the national security management system and the smooth operation of the state in times of war, external threats and major crises, which requires communications systems to be, among other things, scalable and highly resilient – that is, to maintain their integrity and availability under extreme conditions. The Act also provides for the possibility of placing certain entities of key importance to national defence under military control, including telecommunications operators. In practice, this means that, for example, a mobile phone operator may be placed under military control so that, in the event of a threat, its network remains available for use by the state administration and the armed forces.

The *Act of 12 July 2024 The Electronic Communications Law* sets out the rules governing the operation of the telecommunications and electronic communications market. It also imposes obligations relating to national defence, national security, as well as public safety and order. It requires telecommunications operators to draw up action plans for situations involving specific risks and to ensure the continuity of service provision, and grants the President of the Office of Electronic Communications (UKE) the power to impose specific obligations on them, for example regarding the maintenance of network operations. A key aspect of the state's communications subsystem is the obligation imposed on entrepreneurs to provide services to state authorities in the event of a specific security threat, a state of emergency or war. The Act also requires operators to provide the President of the UKE with information on the telecommunications infrastructure they possess, which is necessary for the development of communications systems for defence and security purposes. This enables the state authorities to plan the use of public networks as part of the security system.

The *Act of 29 August 2002 on martial law and the powers of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland* (Article 21 point 6) grants the state authorities the right to temporarily restrict civil rights and freedoms, including the freedom to use communications systems. This allows certain services to be reduced or suspended for the general public in order to ensure that the public administration bodies, the military and the emergency services have priority access to communications. These regulations also make it possible to utilise commercial communications systems as backup links, while limiting public usage of these systems in such a way that the infrastructure does not become overloaded at a critical moment.

The *Act of 5 December 2024 on civil protection and civil defence* which has been in force since 2025, fills the existing regulatory gap in the area of civil defence and streamlines the civil protection system in times of peace, crisis and war. Among other things, it defines the infrastructure necessary for the performance of civil

protection tasks, including communications infrastructure and ICT systems, as a fundamental prerequisite for the effective coordination of activities across different levels of administration. Pursuant to Article 71, a list of communication tools comprising the state administration's communication system has been drawn up: alarm sirens and public address systems, warning systems (including the Regional Warning System), local and national newspapers, radio and television, the ALERT RCB system, warnings sent via digital technologies, as well as the administration's official information services.

One of the key projects provided for in the Act on civil protection and civil defence is National Secure Communications System (hereinafter: SBŁP), which is overseen by the Minister responsible for home affairs (Article 15(1) point 24). The system is intended to serve as an integrated, secure and highly available communications platform for key government bodies, emergency services, civil protection agencies and the armed forces, linking various existing departmental systems via appropriate interfaces and standards. The Act identifies several functional variants of the SBŁP: open system (SBŁP-J), multipoint video conferencing system (SBŁP-V), mobile radio system (SBŁP-M), trunked radio system (SBŁP-T) and satellite communications system (SBŁP-S). All these modules are intended to provide end-to-end encryption and meet the minimum ICT security requirements set by the Council of Ministers, commensurate with the level of threat (Article 78 point 2).

In addition, the *Act of 5 August 2010 on the protection of classified information* sets out the rules governing the processing of classified information in ICT systems. For the communications subsystem, this means that it is necessary to design separate, accredited systems for classified communications, such as classified fixed-line communications systems (SBŁP-N), and, to some extent, SBŁP-M and SBŁP-S. The processing of classified information is permitted only in systems designed for that purpose, including those specifically accredited by the Internal Security Agency (ABW) and the Military Counterintelligence Service (SKW). This makes the distribution of data – such as intelligence or operational information – logistically more challenging, while at the same time enhancing protection against interception. It also necessitates the creation of specialised networks as well as end devices for authorised users.

Risk analysis for the communications subsystem

The communications subsystem of the public administration is one of the cornerstones of crisis management and the national security system in the broadest sense.

It is key to the effective management of personnel and resources, both in terms of prevention and during the response to crisis situations, where the transmission of information via technical means of communication remains a fundamental criterion for integrated resource management[4]. At the same time, there are no alternatives to modern ICT systems, which means that the need for the state to prioritise the development, maintenance and security of these systems is beyond dispute. Without appropriate technological solutions, even the best-prepared and highly specialised administration will not be capable of effectively carrying out its tasks, as it will lack the tools for efficient coordination of activities at the tactical, operational, and strategic levels, which risks deepening the crisis.

The importance of communications systems for national security is confirmed by strategic documents, including the National Security Strategy of 2020. It states that satellite and mobile communications networks form the basis for the exchange of information and are a key component of national security capabilities and the state's preparedness for emergencies[5]. Communications systems have been designated as part of the national critical infrastructure, and the strategic document emphasises the need for the further development of secure, modern telecommunications networks.

The development of communications subsystem in Poland to date has been fragmented and sector-specific. The lack of a comprehensive, top-down programme for building a unified national communications system has meant that individual agencies and services have created their own solutions tailored to current needs and capabilities. As a result, there are systems in place that are often not integrated with one another, either technically or organisationally[6]. The exchange of information between ministries, services and even across different levels of public administration (central, provincial, district and municipal), is hindered. The crisis management system and the national security management system do formally have a defined hierarchical structure, however, the lack of uniform communication both vertical and horizontal creates a risk of decision-making paralysis, duplication of tasks and fragmentation of efforts in the event of a real threat. This is also indicated by the Supreme Audit Office, which in its numerous audit reports pointed to the problem of the lack of a unified digital radio communication system for emergency services

[4] J. Pilżys, *Zarządzanie systemami łączności i transmisją danych w sytuacjach kryzysowych* (Eng. Management of communications and data transmission systems in emergency situations), "Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2015, vol. 8, no. 1, p. 45.

[5] *National Security Strategy of the Republic of Poland 2020*, Warszawa 2020, p. 8.

[6] M. Gawroński, *Systemy teleinformatyczne wspomagania kierowania systemem bezpieczeństwa narodowego* (Eng. ICT systems supporting the management of the national security system), "Wiedza Obronna" 2014, no. 2–3, pp. 61–63.

and crisis management structures. It assessed that this negatively affects information flow and the effectiveness of operations[7].

An important aspect of developing any ICT system is its proper planning and design. Standards in the field of systems and software engineering, such as ISO/IEC/IEEE 24748-1 standard, cover the entire system life cycle: concept, development, production, utilisation, support and, ultimately, retirement[8]. Each of these stages is closely interrelated, and errors made during the planning phase may accumulate in subsequent phases of the project. In the case of systems of national importance, particularly those with a nationwide scope, incorrect assumptions, underestimation of costs and timelines, the selection of unsuitable partners, failure to analyse users' actual needs, or the decision not to incorporate redundancy may lead to a situation in which the system fails to fulfil its basic function.

One example of such negligence is the fire on the Łazienkowski Bridge in Warsaw in 2015. It caused damage to key fibre optic links, which led to a temporary disconnection from the network for some central government departments, including the Ministry of Defence[9]. In turn, nationwide failures of the Emergency Call Centres dispatch systems in 2021 and 2024 led to a situation in which dispatchers were unable to assign tasks to emergency medical teams in the usual way, and the solution was to record requests manually[10]. These incidents could have had a much milder impact if, at the design stage, provisions had been made for the redundancy of independent channels, alternative transmission routes and procedures for switching between them.

Equally important is how the communications systems are operated. The utilisation phase does not mark the end of the system's life cycle – it is during

---

[7] Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli: Organizacja i przygotowanie do działań ratowniczych na autostradach i drogach ekspresowych* (Eng. Report on the results of the inspection: Organisation and preparation for rescue operations on motorways and expressways), 2017, p. 11.

[8] ISO/IEC/IEEE 24748-1 – Systems and software engineering – Life cycle management – Part 1: Guidelines for life cycle management.

[9] M. Gąsior, *W pożarze mostu spłonęły łącza MON. Kilka instytucji bez dostępu do internetu* (Eng. Communications systems of the Ministry of National Defence were destroyed in the bridge fire. A few institutions without internet access), naTemat, 15 II 2015, https://natemat.pl/133507,w-pozarze-mostu-splonely-lacza-mon-kilka-instytucji-bez-dostepu-do-internetu [accessed: 18 III 2026].

[10] *Drugi dzień z awarią systemu ratownictwa medycznego. Ministerstwo uspokaja* (Eng. The second day of the emergency medical system failure. The Ministry is reassuring the public), TVN24, 15 V 2021, https://tvn24.pl/polska/awaria-systemu-ratownictwa-medycznego-st5095494 [accessed: 18 III 2026]; *Ogólnopolska awaria Centrum Powiadamiania Ratunkowego 112* (Eng. Nationwide outage of the 112 Emergency Call Centre), Onet, 16 XII 2024, https://wiadomosci.onet.pl/kraj/awaria-centrum-powiadamiania-ratunkowego-112/bltrlw7 [accessed: 18 III 2026].

day-to-day use that it is put to the test by end-users, while at the same time the experience necessary for its further improvement is gathered. The key role is played by user preparation. If users are not properly trained, and the system interface turns out to be too complex or unintuitive, there is a risk that in practice they will bypass the intended solutions and resort to out-of-system channels. A user's pursuit of convenience in the area of communication can lead, for example, to the use of popular instant messaging applications that are not designed for the exchange of classified information or information regarding crisis situations. In recent years, there have been examples of commercial applications being used to transmit sensitive information, including in the US and Polish administrations, where important decisions were consulted using publicly available services[11]. Such practices undermine information security level and demonstrate that communications systems must be designed taking into account not only technical requirements and security standards but also ergonomics, ease of use and user habits.

Proper operation requires detailed operational procedures and regular exer-cises. The procedures should precisely describe the actions of users and administrators, as well as include contingency plans, modes of operation in the event of partial infrastructure loss, or the occurrence of security incidents. Exercises – including both crisis simulations and stress tests – enable us to verify design assumptions, identify bottlenecks and maintain staff competence at the required level. The lack of exercises, or their cursory nature, leads to a gradual loss of the ability to use systems in non-standard situations. This means that in a real crisis, personnel may spontaneously resort to unauthorised tools, thereby compromising information security and the continuity of the institution's operations.

In the organisational dimension, the issue of technological sovereignty takes on particular significance. The use of hardware and software solutions from third countries poses a risk of losing control over key information security parameters: confidentiality, integrity and availability. Examples of such threats include both government recommendations[12] to avoid using certain foreign security products in critical systems and cases of backdoors being discovered in devices and

[11] J. Goldberg, *The Trump Administration Accidentally Texted Me Its War Plans*, The Atlantic, 24 III 2025, https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/ [accessed: 18 III 2026]; Z. Wanat, *Leaked email scandal engulfs Poland's political elite*, Politico, 24 VI 2021, https://www.politico.eu/article/leaked-email-scandal-engulfs-poland-political-elite-mails-hacking/ [accessed: 18 III 2026].

[12] *Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z dnia 30 maja 2022 r.* (Eng. Recommendation from the Government Representative for Cybersecurity of 30 May 2022) (DC.WFKSC.7250.1.2022), Kancelaria Prezesa Rady Ministrów, 2022, p. 1.

software[13] used for processing sensitive data. Reports of the possibility of remotely compromising advanced military systems or exfiltrating medical data by exploiting vulnerabilities in monitoring devices show that a lack of full control over technology can be exploited to exert political pressure, destabilise healthcare systems or disrupt the operations of the armed forces. In the case of Poland, there is a risk of losing access to transnational data sources, such as NATO and the European Union or its own systems located outside the country (diplomatic missions, satellite constellations). A rational solution is to build redundant, independent communication channels and to develop national capabilities in communications system design and production, which would allow greater independence from foreign suppliers and reduce the risk of technological blackmail.

From a technical perspective, the security and resilience of communications subsystem are based on ensuring specific information security attributes. Standards from the ISO/IEC 27000 family and related standards primarily highlight in this regard confidentiality, integrity, and availability, as well as authenticity, accountability, validity and completeness of data[14]. In the context of state communications, this means that information must be available to authorised entities when needed, cannot be altered or destroyed in an unauthorised manner, must come from reliable sources, and any actions taken on it should be attributable to a specific user or process. In addition, information used in the decision-making process must be up-to-date and complete in order to be processed into reliable operational knowledge. The absence of any of these attributes may lead to incorrect decisions, delays or a complete paralysis of activities.

Furthermore, a major challenge is ensuring interoperability and compatibility of the solutions used. Individual services and state institutions use a variety of systems, frequencies, protocols and standards that are not always consistent with one another. The lack of national standards for emergency communications and a common platform for information exchange means that, in situations requiring cooperation, delays, misunderstandings and interruptions in the flow of data may occur[15]. System fragmentation also increases the scale of an attack – maintaining multiple incompatible solutions makes it difficult to effectively secure and monitor these systems. In the face of a growing number of cyberattacks, including those

[13] *Contec CMS8000 Contains a Backdoor*, CISA 2025, p. 1 et seq.

[14] PN-EN ISO/IEC 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary, Polski Komitet Normalizacyjny, Warszawa 2012, p. 14, 17.

[15] M. Bieńkowski, *Funkcjonowanie systemu ochrony ludności w Polsce* (Eng. The operation of the civil protection system in Poland), "Kontrola Państwowa" 2019, no. 5, pp. 60–62.

from advanced, state-sponsored APT (advanced persistent threats) groups, an approach is needed in which communications security is viewed as part of the state's constitutional duty to ensure the safety of its citizens, rather than as a cost. This requires the use of strong end-to-end encryption, consistent software updates, network segmentation, the application of the principle of least privilege and solutions for strong, preferably multi-factor, user authentication.

All the risks identified lead to the clear conclusion that Poland should consistently develop a coherent, unified national communications subsystem that integrates existing departmental systems and ensures the secure, resilient and effective exchange of information at all levels of governance as well as cooperation. This marks a shift away from the island model towards a deliberately designed, scalable and redundant architecture, based on national technological capabilities and shared standards. Only in this way can it be guaranteed that, in crisis situations, including hybrid operations or armed conflicts, the state apparatus will be able to effectively carry out its tasks and protect the safety of citizens.

Possibilities for resolving the communication impasse

Currently in Poland, various institutions and ministries use their own solutions, often duplicating each other (e.g. two secure mobile communications systems – CATEL and SKR-Z or several email environments for the same classification levels – CATEL and Classified Email System OPAL) that are not compatible. The lack of unified system and common standards means that information is often exchanged between systems manually, which slows down the response time to emergencies and increases the risk of error.

The lack of uniformity in systems also generates costs and risks at several levels. Firstly, investment outlays multiply – the state finances many parallel projects, which strains the budget and limits funds for infrastructure modernisation or innovations. Secondly, dispersion of systems expands the attack vector: each new platform must be individually monitored, updated, tested and secured, which complicates vulnerability management across the entire administration. Thirdly, this necessitates maintaining a large number of specialists across multiple institutions – individual units must have their own maintenance and security teams, which not only increases costs but also creates situations where staff growth in one institution comes at the expense of weakening another. In this context, the need for a new, integrated approach is becoming increasingly evident – one that, on the one hand, allows for flexibility and meets the specific requirements of different institutions,

and on the other hand, ensures the coherence and interoperability of the entire state communications subsystem.

One possibility is to adopt a layered architecture, inspired by the *European Interoperability Framework*[16]. In such a model, individual institutions could still use their respective interfaces and applications (e.g. different messaging apps, video conferencing platforms or IP telephony systems), but all data exchange would take place through a shared transport and semantic layer (Table 1). Communication functions would be separated from the medium used – the same conversation or message could pass through a cellular network, fibre optic cable, radio or satellite, while maintaining uniform encryption standards and metadata. It would be crucial to implement real-time protocol translators that would automatically convert messages between different formats and protocols without losing information about the sender, recipient, confidentiality level or message priority. This approach would be complemented by intelligent routing mechanisms that select the optimal transmission channel depending on the context – such as the importance of the message, available links, network load or the type of device the recipient has.

Table 1. Concept for the development of an integrated national communications system.

Layer	Description	Examples of standards
Application	Tools tailored to the institution's needs	Threema OnPrem for public authorities, Matrix for security agencies
Semantic	Dictionaries, translators and data exchange schemes	XML GovCore, JSON-LD with EU Vocab ontologies
Transport	Universal protocols for encrypted communication	TLS 1.3, QUIC, SCIP for voice
Physical	Technology-neutral network infrastructure	SD-WAN, 5G NSA, campus networks

Source: own elaboration.

Inspiration for this approach comes from solutions implemented in other countries. The French Tchap system, launched in 2019, is based on open, decentralised Matrix protocol, which allows for building a federated communication

[16] *Europejskie Ramy Interoperacyjności* (Eng. European Interoperability Framework), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/ia/europejskie-ramy-interoperacyjnosci [accessed: 30 III 2026].

architecture – each ministry or agency can maintain its own server, retaining control over its data, while at the same time remaining in secure contact with other administrative units[17]. The Matrix protocol also enables the creation of so-called bridges to other platforms (e.g. XMPP, IRC, Slack), which facilitates secure contact with external partners while maintaining security standards and compliance with regulations, such as the eIDAS Regulation[18]. The Tchap system offers, among others, end-to-end encryption, integration with the national electronic identity system and mechanisms for the automatic deletion of messages. Its effectiveness was confirmed during the 33rd Summer Olympic Games in Paris, when there was a significant increase in the number of users, messages sent and chat rooms created for the purpose of coordinating security and logistics[19].

Another example of a solution aimed at secure communication integration of a distributed government structure is Australian GovLINK. The system managed by the Department of Finance creates an encrypted environment for the exchange of information between federal and state agencies as well as selected public and private sector partners[20]. It is based on a federated architecture and common security standards (e.g. S/MIME, X.509), which allows agencies to retain their own systems while utilising uniform mechanisms for authentication, encryption and digital signatures.

Both examples show that open protocols, a federated architecture and robust cryptographic algorithms can effectively overcome the problem of a lack of uniformity across systems while preserving the autonomy of individual institutions.

In the Polish context, the benchmark for this direction of change is the SBŁP project. It is intended to become a multi-layered, integrated system, overseen by the Minister responsible for home affairs. The system is designed to combine various communication channels – from fixed-line and radio networks, through mobile networks, to satellite networks – into a single, coherent communications

---

[17] C. Dussutour, *French government launches in-house developed messaging service*, *Tchap*, European Commission, 10 XII 2021, https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/french-government-launches-house-developed-messaging-service-tchap [accessed: 19 III 2026].

[18] eIDAS (*Electronic IDentification, Authentication and Trust Services*) – unified standard for electronic identification and trust services of the European Union, operating on the basis of *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*.

[19] *Tchap, the French administration federation: past, present and future - Julie Ripa*, YouTube, 29 X 2024, https://www.youtube.com/watch?v=m1roliPrNqc [accessed: 19 III 2026].

[20] GovLINK, Australian Government – Department of Finance, https://www.finance.gov.au/government/whole-government-information-and-communications-technology-services/govlink [accessed: 19 III 2026].

environment for the public administration. The most important task of the SBŁP is to ensure the continuity of communications between state authorities both in peacetime and in times of crisis or war, as well as to facilitate interoperability between separate systems within the civil sector, security services and military structures. The project involves identifying several functional components: SBŁP-J, SBŁP-N, SBŁP-V, SBŁP-M, SBŁP-T and SBŁP-S. All of them are based on certified cryptographic solutions.

A key advantage of the SBŁP concept is the ability to utilise existing infrastructure, such as OST112 and GovNet networks, both for open and classified systems. This would help to reduce costs and speed up the implementation of the system. Integration with existing solutions (e.g. the use of CATEL system in the SBŁP-M component) will increase channel redundancy and enable a gradual transition from distributed solutions to a more cohesive architecture. At this stage, however, it has not been revealed whether the SBŁP will be an entirely new system designed from scratch, a collection of modified existing solutions, or a combination of both approaches. There are strong indications that, for economic and organisational reasons, the evolutionary approach may prevail, involving a gradual integration and unification.

Planning and implementing such a transformation requires a phased approach. In the pilot phase, the foundation of a new system can be built based on open protocols (such as Matrix), and a limited number of ministries can be integrated with it, practically testing the interoperability and security mechanisms. The next phase involves expanding the scope to additional institutions and implementing protocol translators for legacy systems, enabling them to exchange information without the need to immediately replace the entire infrastructure (e.g. from TETRA metadata to JSON-LD standard or Matrix to XMPP format). At the same time, it would be advisable to carry out certification of compliance with established security standards (e.g. ISO 27001) and develop common security policies, which could eventually be partially automated. In the long term, integration with communication systems at the European Union level would also be possible, in line with promoted concepts such as GovStack, which envisage building standardised, modular components that can be combined as needed[21].

The benefits of implementing an integrated, interoperable communications system are multifaceted. In addition to reducing response times in crisis situations and enhancing information security, a significant reduction in infrastructure maintenance costs and greater resilience to failures and attacks can be expected. However, achieving success still requires maintaining a balance – the system must

[21] GovStack, https://www.govstack.global/about/ [accessed: 19 III 2026].

be uniform enough for all institutions to cooperate seamlessly, yet modular enough to be adapted to the specific tasks of individual users and to evolve with changes in technology and threats. If the SBŁP is designed as an open, interoperable platform rather than yet another closed, limited-scope departmental system, it could become the foundation for a new standard in national communications.

Summary

Communications subsystem of the public administration is one of the key determinants of a state's resilience to contemporary threats, and its effectiveness results from the simultaneous influence of four factors: legal framework, quality of planning and design processes, technological maturity and competencies of users. Despite the existence of extensive telecommunications infrastructure, the current communications system is not fully integrated, which leads to delays, dysfunctions, and increased vulnerability to disruptions in crisis situations. Thus, the hypothesis regarding the inadequacy of the current communications system in relation to contemporary threats has been confirmed.

In practical terms, a model for optimising the communications subsystem has been proposed, in which diverse systems and transmission media are integrated through coherent planning, organisational and technical layers. This model assumes the use of existing infrastructure resources, their gradual integration, and new functionalities enabling the automatic routing of information traffic through various channels, depending on priority, data sensitivity and the availability of links. Such an approach to modernisation reduces the risk of loss of communications in extreme situations and limits costs by moving away from duplicating solutions in favour of deliberate consolidation.

The article clarifies the criteria for assessing the resilience of communications systems in terms of four complementary dimensions:

1) legal (compliance and completeness of regulations),
2) planning (quality of functional concepts),
3) redundancy (ensuring multi-channel communication),
4) integration (the actual ability of systems to interoperate).

This approach encourages a move away from a simplistic, infrastructure-focused view of communications and allows it to be integrated into mainstream research on the national security system.

Limitations of the study – in particular, the lack of full access to operational data and to the detailed specifications of the SBŁP system under development – highlight the need to continue work on the empirical verification of various options

for integrating existing systems. Further research into federated architectures, protocol translation mechanisms and data exchange standards between security entities for implementation in government communications systems should be considered particularly worthwhile.

The findings of the research lead to an unequivocal conclusion: investment in digital transformation and integration of communications system are not merely a matter of technical modernisation, but a prerequisite for maintaining the state's actual operational capability in the 21st century. The implementation of the presented recommendations may lead to shorter response times for the administration, security and emergency services in crisis situations, which will have a direct impact on the continuity of operations of the public institutions, the protection of the population as well as the maintenance of national stability in the context of growing strategic uncertainty.

Bibliography

Bieńkowski M., *Funkcjonowanie systemu ochrony ludności w Polsce* (Eng. The operation of the civil protection system in Poland), "Kontrola Państwowa" 2019, no. 5, pp. 52–70.

Contec CMS8000 Contains a Backdoor, CISA, 2025.

Gawroński M., *Systemy teleinformatyczne wspomagania kierowania systemem bezpieczeństwa narodowego* (Eng. ICT systems supporting the management of the national security system), "Wiedza Obronna" 2014, no. 2–3, pp. 47–86.

Pilżys J., *Zarządzanie systemami łączności i transmisją danych w sytuacjach kryzysowych* (Eng. Management of communications and data transmission systems in emergency situations), "Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2015, vol. 8, no. 1, pp. 33–49.

Internet sources

Drugi dzień z awarią systemu ratownictwa medycznego. Ministerstwo uspokaja (Eng. The second day of the emergency medical system failure. The Ministry is reassuring the public), TVN24, 15 V 2021, https://tvn24.pl/polska/awaria-systemu-ratownictwa-medycznego-st5095494 [accessed: 18 III 2026].

Dussutour C., *French government launches in-house developed messaging service*, *Tchap*, European Commission, 10 XII 2021, https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/french-government-launches-house-developed-

-messaging-service-tchap [accessed: 19 III 2026].

Europejskie Rady Interoperacyjności (Eng. European Interoperability Framework), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/ia/europejskie-ramy-interoperacyjnosci [accessed: 30 III 2026].

Gąsior M., *W pożarze mostu spłonęły łącza MON. Kilka instytucji bez dostępu do internetu* (Eng. Communications systems of the Ministry of National Defence were destroyed in the bridge fire. A few institutions without internet access), naTemat, 15 II 2015, https://natemat.pl/133507,w-pozarze-mostu-splonely-lacza-mon-kilka-instytucji-bez-dostepu-do-internetu [accessed: 18 III 2026].

Goldberg J., *The Trump Administration Accidentally Texted Me Its War Plans*, The Atlantic, 24 III 2025, https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/ [accessed: 18 III 2026].

GovLINK, Australian Government – Department of Finance, https://www.finance.gov.au/government/whole-government-information-and-communications-technology-services/govlink [accessed: 19 III 2026].

GovStack, https://www.govstack.global/about/ [accessed: 19 III 2026].

Ogólnopolska awaria Centrum Powiadamiania Ratunkowego 112 (Eng. Nationwide outage of the 112 Emergency Call Centre), Onet, 16 XII 2024, https://wiadomosci.onet.pl/kraj/awaria-centrum-powiadamiania-ratunkowego-112/bltrlw7 [accessed: 18 III 2026].

Tchap, the French administration federation: past, present and future - Julie Ripa, YouTube, 29 X 2024, https://www.youtube.com/watch?v=m1roliPrNqc [accessed: 19 III 2026].

Wanat Z., *Leaked email scandal engulfs Poland's political elite*, Politico, 24 VI 2021, https://www.politico.eu/article/leaked-email-scandal-engulfs-poland-political-elite-mails-hacking/ [accessed: 18 III 2026].

Legal acts

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Official Journal of the EU L 257 of 28 VIII 2014).

Act of 5 December 2024 on civil protection and civil defence (Journal of Laws of 2024, item 1907, as amended).

Act of 12 July 2024 The Electronic Communications Law (Journal of Laws of 2024, item 1221,

as amended).

Act of 11 March 2022 on the defence of the Homeland (consolidated text, Journal of Laws of 2025, item 825, as amended).

Act of 10 June 2016 on anti-terrorist activities (consolidated text, Journal of Laws of 2025, item 194).

Act of 5 August 2010 on the protection of classified information (consolidated text, Journal of Laws of 2025, item 1209).

Act of 26 April 2007 on crisis management (consolidated text, Journal of Laws of 2023, item 122, as amended).

Act of 29 August 2002 on martial law and the powers of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland (consolidated text, Journal of Law of 2025, item 504).

Act of 21 June 2002 on the state of emergency (Journal of Laws of 2017, item 1928).

Regulation of the Minister of National Defence of 20 April 2022 on the operation of the military telecommunications system (Journal of Laws of 2022, item 870).

Regulation of the Prime Minister of 25 July 2016 on the scope of undertakings carried out in particular alert levels and CRP alert levels (consolidated text, Journal of Laws of 2022, item 2065).

Other documents

ISO/IEC/IEEE 24748-1 – Systems and software engineering – Life cycle management – Part 1: Guidelines for life cycle management.

Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli: Organizacja i przygotowanie do działań ratowniczych na autostradach i drogach ekspresowych* (Eng. Report on the results of the inspection: Organisation and preparation for rescue operations on motorways and expressways), 2017.

PN-EN ISO/IEC 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary, Polski Komitet Normalizacyjny.

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z dnia 30 maja 2022 r. (Eng. Recommendation from the Government Representative for Cybersecurity of 30 May 2022) (DC.WFKSC.7250.1.2022), Kancelaria Prezesa Rady Ministrów, 2022.

National Security Strategy of the Republic of Poland, Warszawa 2020.

David Cybulski

Specialist in the field of cybersecurity. He gained professional experience in the private sector and in state administration. Passionate about innovative cybersecurity solutions and new techniques used in cyberattacks by APT groups, with particular emphasis on social engineering attacks. His scientific interests include the protection of critical infrastructure, the activity of selected APT groups, the security aspects of Shadow IT and Cyber Threat Intelligence / Threat Hunting activities towards selected cybercriminal groups.

Contact: dcybulski@proton.me