Republic of North Macedonia
**Ministry of Defence**

# CYBER DEFENCE STRATEGY

March 2026

# Contents

## Foreword

The security of citizens, the protection of sovereignty and territorial integrity, as well as the preservation of democratic values and the rule of law, are fundamental functions of the state. The fulfillment of these functions requires a stable and integrated defence system, based on a long-term vision, clear institutional accountability and continuous development of capabilities.

Pursuant to the Defence Strategy, the Ministry of Defence adopts the Cyber Defence Strategy (2026–2030), with a view to systematically strengthening defence capabilities in cyberspace as an integral part of the integrated defence of the Republic of North Macedonia. In modern security environment, cyberspace is an operational domain in which the disruption of communication and information systems can directly affect the capability to command, control and execute military missions. Hence, cyber defence is defined as a permanent military task that is carried out in peace, emergency and wartime.

This Strategy translates strategic commitments into clear guidelines for management, planning and capability development. It establishes an institutional position that cyber defence is a prerequisite for the operational readiness of the Army and that its development must be treated with the same level of priority as other combat and support capabilities.

As a NATO member, the Republic of North Macedonia has an obligation to ensure the interoperability, reliability and resilience of its military systems. The contribution to collective defence is not measured only through the physical deployment of forces, but also through the capability to operate securely and seamlessly in a digital and hybrid environment. Cyber defence is an integral part of national obligations within the Alliance and the capability to participate in international missions and operations.

The Strategy recognizes the interdependence between military systems and other elements of the national critical infrastructure. The defence system relies to a significant extent on civilian communication, energy and information capacities, which can also be the target of cyber attacks. Therefore, the Strategy envisages cooperation with the competent state authorities and the private sector, while strictly preserving the operational autonomy and security control over military systems.

This Strategy establishes clear responsibilities, coordination mechanisms and principles of action in crisis situations, with the aim of enhancing national and allied cyber resilience and ensuring effective defence of the state in operational cyberspace.

## Introduction

The development of the Cyber Defence Strategy (2026–2030) sets out the Ministry of Defence's long-term approach to protecting and maintaining military operational capabilities in cyberspace. The Strategy recognizes cyberspace as an operational environment in which military effectiveness, command structure and national security interests are constantly challenged and exposed to complex hybrid influences.

The Strategy draws on the principle "resilience first". It ensues from the realistic assumption that hostile activities are continuous, that strategic competition takes place below the threshold of armed conflict and that disruptions in cyberspace have a high probability of coinciding with military-political crises. Hence, the defence system must be designed to function under pressure, absorb disruptions and quickly restore functionality without jeopardizing the mission.

This includes ensuring continuity of command and control, secure and protected communications, disciplined identity and access management, segmentation of critical systems, constant monitoring, organized and practiced incident response, as well as systematic and predictable recovery. Deterrence is based primarily on the principle of denial achieved through the construction of a strengthened, adaptable and renewable defence system that limits the impact and reduces the ability of the adversary to achieve significant strategic effects.

The Strategy is structured around four interconnected implementation pillars for the period 2026–2030, aimed at achieving four strategic outcomes by 2030: professional and sustainable cyber personnel, a modernized and resilient defence digital infrastructure, a management and operational framework aligned with NATO standards and international cooperation, and a fully operational capability for defensive cyber operations with rapid response elements.

With the implementation of the Strategy, by 2030, the defence system should be capable of maintaining essential mission functions in the event of an attack on digital infrastructure, effectively coordinating actions in the event of serious incidents, and with the capability to contribute to collective defence, based on resilience, interoperability, and disciplined institutional accountability.

## Vision

With the implementation of the Cyber Defence Strategy, the Ministry of Defence and the Army of the Republic of North Macedonia will possess an integrated, operationally ready and interoperable cyber defence capability that ensures continuity of command and control, protection of communication and information systems, and freedom of action in cyberspace in peace, crisis, and armed conflict.

Cyber defence is treated as a permanent military mission and an integral part of defence planning, risk management, and force development. The systems of the Ministry of Defence and the Army will be designed and operated with built-in resilience, capable of withstanding, absorbing, and rapidly recovering from sophisticated cyber attacks without disrupting operational readiness and mission execution.

The vision implies the establishment of clear command responsibility, constant situational awareness, adaptable defence and coordinated response, in full compliance with the standards and principles for collective defence in the cyber domain at the national and international level.

The Ministry of Defence will develop a cyber capability that not only protects, but also provides operational advantage and strengthens national and allied resilience in operational cyberspace.

## Mission

The mission of the Ministry of Defence and the Army in the cyber domain is to protect, secure and maintain the resilience of communication and information systems, networks and data of importance to defence, in order to guarantee uninterrupted command and control, for secure decision-making and effective execution of national and allied missions.

This mission is conducted through:

- establishing a coherent cyber defence management system with clearly defined competencies and responsibilities;
- development and maintenance of technical and operational capacities for prevention, detection, defence, response and recovery from cyber incidents;
- integration of cyber defence into all levels of military planning, preparation and operations;
- development and retention of professional staff with capabilities aligned with national and international standards;

– ensuring interoperability and information exchange at the national level and with allies within the framework of collective defence.

Cyber defence is implemented as a continuous function, based on risk assessment, the principle of resilience, and full compliance with national legislation and international law.

## 1. Strategic posture

The Strategy is adopted as a framework for the implementation of cyber defence in the Ministry of Defence and the Army. It operationalizes the guideline set out in the Defence Strategy that the achievement of defence goals requires continuous monitoring of the security environment, coordinated planning, and the development of appropriate capabilities.

At the same time, the Strategy is aligned with the National Cyber Security Strategy 2025–2028, by introducing relevant national principles such as risk-oriented management, resilience, security built into system design, and coordinated incident management.

Within the framework of defence planning, this Strategy is a document that provides guidelines for the development of defence policies, ministerial instructions, doctrinal changes, planning documents and implementation programs. It provides a basis for the development of capabilities, the implementation of innovative approaches, the definition of training priorities and the implementation of activities to determine and assess readiness within the structures of the Ministry and the Army.

The Strategy covers the defence system as a whole: the Ministry of Defence, the General Staff as the authority holding the military command responsibility, subordinate structures, the various defence systems, as well as the services necessary to ensure operational capability. It also applies to military networks and communications, information systems that support command and control, as well as the management and control mechanisms necessary to ensure their confidentiality, integrity and availability in conditions of constant threats in cyberspace.

The Strategy consciously avoids duplicating the national civilian cybersecurity framework. Instead, the Ministry of Defence will maintain its own defence-operational capability, cooperate through formal coordination processes, and contribute to the overall state resilience when necessary, while fully preserving operational autonomy over military systems and communications.

The Strategy does not prescribe specific technical solutions, products or tools. Technical choices will be determined through subordinate plans, decisions on the implementation of infrastructure solutions and envisaged operational procedures. This document sets out the political guidance and the assurance discipline against which those choices will be assessed in terms of their contribution to the operational readiness and resilience of the defence system.

In modern military operations, operational capability depends on the integrity, availability and reliability of information systems and communication links. Here, the effects of cyber attacks are rarely isolated; they can be synchronized with disinformation, sabotage or broader hybrid pressure to disrupt decision-making and weaken the military response. Therefore, the defence system must proceed from the assumption that cyber disruptions will be constant in peacetime conditions and will intensify in crisis conditions, with sophisticated actors seeking to exploit dependencies and organizational weaknesses, rather than simply “disrupting” an individual system. Hence, this Strategy treats cyber defence as ensuring the mission in order to protect the ability to command, communicate, coordinate and sustain forces, in conditions of dependence on civilian infrastructure.

## 2. Legal and institutional framework

The Ministry of Defence retains political authority for defence policy, resource allocation and the fulfilment of national and allied commitments in the cyber domain. The General Staff retains responsibility for the integration of cyber defence into combat readiness, operational planning and execution through the chain of command. This division reflects the essential democratic arrangement of civilian control and military command responsibility and is a prerequisite for disciplined and effective cyber defence.

In order to ensure unity of effort within the defence system, the Ministry of Defence and the Army will establish a central coordinating body in the domain of cyber defence, as the authority for policy harmonization, implementation oversight, and consolidated reporting on the state of readiness and key risks. This body will have clearly defined authorities and responsibilities, in order to ensure systemic compliance. This Strategy establishes that the designated central coordinating body in the domain of cyber defence will be responsible for ensuring policy coherence within the Ministry, standardization of procedures, maintenance of a framework for measuring performance and institutional maturity, as well as integration of reports in order to ensure better decision-making by the Ministry on issues relevant to cyber defence.

Operational execution remains within the Army chain of command and designated operational elements, including cyber incident response capabilities and continuous monitoring and response capacities. The role of the central coordinating body in the cyber defence domain is not operational command, but rather ensuring systemic cohesion: uniform standards, enforceable priorities, clearly defined responsibilities, and ensuring verification of cyber defence readiness.

Cyber defence must operate continuously, but at the same time be able to adapt and strengthen in a controlled and legally coherent manner in line with the escalation of the security environment. Therefore, this Strategy establishes four activation levels, which aim to guide preparedness, decision-making and coordination, without creating technical or institutional ambiguity.

1. In a **Regular Defence Posture**, cyber defence is a permanent function aimed at prevention through disciplined management, continuous monitoring, reducing vulnerabilities and providing recovery measures. The goal of this posture is the readiness of the cyber defence system by building a level of resilience that allows for a manageable, rather than chaotic, escalation. This phase ensures regular validation, integration of cyber aspects into training and continuous improvement based on lessons learned and assessed risks.
2. In conditions of **Increased Alertness**, triggered by heightened geopolitical tension, credible threat indicators, or increased hostile activity targeting national institutions, the defence system intensifies monitoring, accelerates the application of security updates and the treatment of risks to mission-critical systems, increases the readiness of rapid response teams, and introduces tighter control over configuration changes. An important segment in this phase is the setting of priorities such as directing attention and resources to mission-critical functions and ensuring that management has a clear picture of the current risk and its operational implications.
3. In conditions of a **Defence Crisis**, triggered by significant national cyber incidents, hybrid pressure affecting defence readiness or an imminent threat to the security of defence operations, the defence system enters a crisis mode of operation. Decision-making in the cyber domain becomes time-sensitive, escalation procedures are shortened, and coordination with national crisis management structures becomes continuous. The priority is to ensure continuity of command, secure communications and stabilization of defence services. The system must be able to function in a degradation mode, maintain essential functions and quickly restore critical services, while preserving classified information and operational security.

4. In a **Conflict Situation**, activated in the event of armed conflict or equivalent situations, cyber defence becomes inseparable from operational survivability. The defence system must assume continuous hostile activity targeting its digital infrastructure and operate with disruption as an expected condition. Decision-making focuses on sustaining the mission, protecting forces, and preserving operational freedom of action. Coordination with allies becomes essential to ensure interoperability and support, with the defence system having to maintain its own minimum functional capability while integrating into the collective defence framework.

The anticipated activation levels should be reflected in subordinate directives, readiness checks, anticipated procedures and notifications, so that escalation results in predictable institutional behavior, not improvisation.

Civilian control is exercised through guidelines defined by the Ministry, which approve strategic plans, establish accountability mechanisms, and allocate appropriate resources.

Military command responsibility is realized by ensuring readiness, discipline, integration of cyber defence into operational planning and its execution through the chain of command and control. Operational autonomy in cyber defence implies that the Army retains full authority over the operation, protection and restoration of military networks, systems and communication infrastructure. Therefore, this Strategy establishes that decisions in the domain of cyber defence that affect mission-critical functions must remain within the framework of defence command arrangements, with clearly defined escalation thresholds to ministerial leadership when it comes to decisions of strategic importance.

The Ministry of Defence will participate in national crisis management structures through defined coordination links and harmonized procedures for information exchange, harmonization of public communication and mutual support. In the event of major national cyber incidents affecting broader societal stability, the defence system will share information relevant to national security, in full compliance with the Law on Security of Classified Information as well as the laws and bylaws on security of classified information.

In situations where national crisis management, led by civilian structures, requires insight into the state of the defence system, in conditions where a disruption of civilian critical infrastructure affects defence readiness, the Ministry of Defence and the Army will provide updated information on the situation, impact assessments and coordination points, retaining full authority for technical and operational measures within their own networks and systems.

The Strategy mandates the establishment of a permanent mechanism for civil-military coordination, which will function regularly in peacetime conditions and will transition to a continuous engagement regime in crisis conditions. This means that, according to the Strategy, the participation of the Ministry and the Army is integrated into the national crisis management framework, while at the same time preserving the clarity of the defence command structure.

## 3. Cyber Defence Challenges

The defence system operates in an environment where adversary cyber activity is persistent, adaptive, and often integrated into broader hybrid campaigns. Sophisticated actors seek to provide long-term access, intelligence advantage, and the ability to disrupt decision-making at critical moments. The pressure is rarely publicly announced; it accumulates through reconnaissance, compromise of supply chains, abuse of user rights and authorities, and the gradual erosion of trust in systems and information.

In such conditions, the traditional distinction between “peace” and “conflict” becomes blurred. The defence system must start from the assumption that functioning in conditions of active cyber threat is the basic condition, not the exception.

Strategic readiness cannot be measured solely through equipment and training schedules. It must include the ability to maintain functional command and control, preserve the integrity of operational information, and continue operations in the face of disruption. Therefore, cyber defence is treated in this Strategy as a key component of operational capability and a prerequisite for readiness.

State-sponsored actors pose the highest risk, as they combine technical sophistication, long-term persistence, and strategic intent. In a defence context, their goals often include gathering operationally relevant information, preparing destructive options in times of crisis, and undermining confidence in collective security.

Criminal actors pose a significant secondary risk, as their methods such as extortion, ransomware, and man-in-the-middle access can cause a high level of disruption, and their infrastructure can be exploited by more sophisticated actors.

Ideologically motivated actors can create reputational damage and operational distraction, especially during politically sensitive periods, but their strategic impact is usually limited unless their activities are synchronized with broader campaigns.

The defence system must protect against the full spectrum of threats, but priority must be given to threats that most significantly impact the mission. Systems that support command and control, force readiness, mobilization, intelligence support, and operational communications require the highest level of resilience and assurance.

Modern defence capability relies on interconnected information systems and functional linkages that go beyond the direct control of the Ministry and the Army. Civilian infrastructure, especially the energy system and telecommunications, create systemic risk, as its disruption can cause cascading effects on defence readiness. The Strategy explicitly recognizes the increased risk arising from such functional linkages and the fact that the resilience of these entities becomes an integral part of military readiness.

Supply lines pose an additional systemic risk. Defence systems are developed and maintained through suppliers, integrators, and service providers. A supplier compromise can directly impact defence operations. Therefore, this Strategy treats supply line security and the principle of “security by design” in the procurement process as mission imperatives, not as an administrative formality.

Complexity and legacy (obsolete) systems are also risk drivers. Defence infrastructure has been evolving for decades, often with accumulated technical challenges. In times of crisis, a fragile legacy environment increases the likelihood that defence measures will cause unintended disruptions. Therefore, modernization and resilience are not treated as “IT upgrades,” but as investments in resilience necessary for continuity of operations.

New technologies simultaneously increase the possibilities for the development and use of communication and information systems and threats. Automation can accelerate defensive and offensive actions. Artificial intelligence enables faster reconnaissance, adaptive phishing campaigns and manipulation of information, including synthetic media that can undermine trust, through content such as “deepfake”. While the development of quantum computing represents a future potential disruption of existing cryptographic mechanisms.

In such a security context, prevention alone is structurally insufficient. The defence system must assume that attempts at compromise will be constant and that in some cases they will succeed. Resilience, through limiting the scope of disruption, maintaining essential functions, and rapid recovery, is the only stable basis for maintaining operational readiness in conditions of uncertainty.

# 4. Guiding principles

This Strategy is implemented through six guiding principles. Each principle represents a direction for building the defence capability in cyberspace. Following the principles in the implementation of the strategy should contribute to cyber defence being operationally established, based on assessed risk, adapted to the modern operational environment, based on standards, with incorporated structured cooperation and institutional accountability. These principles aim to prevent cyber defence from being treated as an isolated technical program, but rather as a defence capability that must be planned, financed, trained and operationally functional.

## 4.1 Operational setup

The principle of operational cyber defence deployment exists to protect and secure the results of defensive actions.

Strategic goals applying this principle are:

- Full integration of cyber defence into operational planning and execution in all domains, so that cyber aspects are embedded in strategic planning, readiness, exercises and mission execution. The practical implication is that cyber defence requirements will be treated as an integral part of operational readiness criteria, and cyber risk will be expressed in operational terms as an impact on command, tempo, logistics and mission success, and not exclusively in technical categories.
- Ensuring continued operational effectiveness of command and control systems even in the face of an active cyber threat. This includes designing the defence system and training personnel to maintain the mission in the face of disruption, degradation, or hostile cyber activity. Each mission-critical function that relies on digital services is determined to have defined procedures for operating in degraded infrastructure, defined recovery objectives, and regularly practiced continuity procedures.

## 4.2 Risk assessment based planning

The principle of cyber defence planning based on risk assessment defines that threats to the mission must be monitored and measures taken to manage them.

The strategic goals from applying this principle are:

- Integration of intelligence-led threat assessment capability development into the structure of organizations. Prioritizing investments is based on valid threat assessments, mission criticality analysis, and strategic risk exposure. This requires establishing a structured risk assessment mechanism and regularly engaging management in addressing cyber risk as a significant segment of defence planning.
- Aligning the allocation of resources based on mission importance and cyber-attack risk. This means that assets and measures and activities will be concentrated where the operational impact is highest, in mission-critical functions, critical communications and systems necessary to meet national and collective security commitments. This means that less important systems will also be protected, but not at the expense of critical defence infrastructure.

## 4.3 Monitoring and integration of new technologies

The principle of monitoring and integrating new technologies represents an adaptation to the modern operational environment. Cyber defence must reflect the reality of a hybrid, multi-domain, and information-saturated conflict.

The strategic goals from applying this principle are:

- Development of capabilities for effective operation in hybrid and multi-domain threat scenarios. Cyber defence to be integrated into exercises and operational assumptions, where disruption of information infrastructure, manipulation of information and parallel physical outages are treated as real, not exceptional conditions.
- Anticipate and respond to emerging technological and operational challenges. Maintain an adaptive posture by continuously assessing emerging threat methods and technological changes, such as automated attacks and cryptographic risks. This does not mean speculative technology programs, but disciplined monitoring of trends related to procurement, training, and implementation of resilience.

### 4.4 Standardized operational discipline

The principle of standardized operational discipline is an approach based on strictly defined standards that should define the guidelines for functioning within national and international frameworks.

The strategic goals from applying this principle are:

- Incorporating the principles of "security by design" and "zero-trust" throughout the entire life cycle of defence systems. This means that security requirements will be an integral part of procurement, approval of infrastructure solutions, and system management, so that new solutions do not create weak and vulnerable structures.
- Compliance with the requirements for cooperation with national institutions and international partners through the adoption of relevant international standards and frameworks in the field of cyber defence, with the aim of ensuring operational interoperability and confidentiality.

### 4.5 Structured cooperation

The principle of structured cooperation for implementing cyber defence refers to cooperation with civil authorities, critical infrastructure entities, industry, the academia, and international partners, but it must be realized through formal processes that protect sensitive information and preserve command autonomy.

The strategic goals from applying this principle are:

- Integration of civil-military cooperation to implement cyber resilience by establishing formal coordination procedures with national civilian authorities and crisis management structures, ensuring timely escalation and coordination in national crisis situations, in accordance with the national cyber crisis management framework.
- Strengthening integration in collective cyber defence with international partners. This Strategy requires active participation in allied mechanisms for information exchange and the implementation of exercises, with the aim of validating interoperability, decision-making and coordinated response in the event of a real cyber attack.

### 4.6 Institutional responsibility

The principle of institutional responsibility ensures that cyber defence must not depend on individual expertise or short-term projects.

The strategic goals from applying this principle are:

- Establishing clear governance, authority and accountability. This principle requires the Strategy to formally define roles and responsibilities within the defence system, including a central cyber defence authority responsible for coherence, oversight and reporting, as well as clearly defined operational responsibilities through the chain of command.
- Since cyber defence fundamentally depends on trained and permanent personnel, it is necessary to create a system that will ensure sustainable development and retention of personnel, and organizational maturity for cyber defence. This means developing career paths, professional education, and retention mechanisms, so that expertise becomes an institutional capability, not an individual advantage.

# 5. Strategic areas of development

The implementation of the Strategy is realized through the development of strategic capabilities defined by four fundamental pillars. These pillars represent structured areas aimed at achieving measurable results in cyber defence readiness by 2030, by strengthening operational cyber readiness and mission assurance, establishing risk-based management and effective strategic oversight, promoting interoperability and compliance with standards within the framework of collective defence, as well as developing sustainable human capital and organizational resilience.

Each pillar is defined through its strategic perspective, implementation logic, expected level of maturity by 2030, and contribution to continued operational readiness.

## 5.1 Pillar 1: Operational Cyber Readiness and Mission Assurance

The first pillar aims to transform the integration of cyber defence into an operational capability that directly supports military effectiveness and continuity of command. This pillar focuses on embedding cyber defence into operational doctrine and planning, protecting mission-critical functions, implementing segmentation and disciplined identity and access management, and structurally integrating procedures for operating in a disrupted mode of operation.

This pillar requires disciplined assurance of recovery capability. The defence system must be able to predictably and timely restore critical services. Operational readiness will be measured not only through detection and response, but also through the ability to maintain mission continuity and restore essential services within defined time targets.

In order to improve operational awareness of cyber situations and the possibilities for coordinated response, the Ministry of Defence will provide conditions and resources for the functioning of the SaOC, within the Ministry of Defence and the Army, responsible for continuous monitoring of information networks and infrastructure, coordination in response to cyber incidents and support for defence operations in cyberspace. To strengthen operational resilience, the Army will develop a deployable cyber defence capacity capable of supporting deployable units of the Army.

The Ministry of Defence and the Army will establish standardized procedures for reporting and responding to cyber incidents affecting defence information networks and infrastructure, which will define risk levels for the purpose of timely decision-making and efficient coordination between all levels.

By 2030, mission-critical functions are expected to have explicit cyber resilience requirements, continuity measures are designed and practiced, and management at relevant levels understand the relationship between cyber conditions and their decision-making space. Cyber aspects are integrated into exercises as an operational stressor, not as a technical “add-on.”

## 5.2 Pillar 2: Risk-based management and strategic oversight

The second pillar structurally integrates threat-driven planning, threat prioritization, and accountability. Management must answer three questions at any given time: which risks are critical in a cyberattack, what measures are being taken, and how is preparedness being verified?

This pillar requires the establishment of a formal framework for assessing cyber risk related to defence missions, clear escalation protocols and an annual strategic review that will inform capability development and budgeting. Measurable performance indicators linked to mission outcomes, not just technical parameters, will be applied.

The Ministry of Defence and the Army will ensure the long-term sustainability and operational capability of cyber defence capabilities provided through national investments and contributions from NATO Allies and international partners. Sustainability planning will encompass life cycle management requirements, including maintenance, licensing, technical support, and personnel training.

By 2030, cyber risk will be integrated into defence planning cycles, procurement, and readiness reporting. A central coordinating body in the cyber defence domain will maintain a maturity framework and provide regular oversight and accountability.

### 5.3 Pillar 3: Interoperability, standards and integration

The third pillar aligns the cyber defence posture within national and international cooperation frameworks through the application of relevant international standards. This pillar encompasses alignment with standards, mechanisms for secure information exchange, participation in national and allied exercises, and disciplined civil-military coordination in line with the national crisis management framework.

By 2030, the defence system should be able to reliably and securely exchange threat information with national institutions and international partners and allies, integrate into external operational networks when necessary, and participate in joint cyber resilience activities to validate its own resilience and ability to recover.

### 5.4 Pillar 4: Human capital and organizational resilience

The fourth pillar aims to build a sustainable, professional and adaptive cyber capability. Cyber defence is primarily a human-enabled capability, therefore career paths, professional education aligned with allied programmes, personnel retention mechanisms and reserve capacity structures will be established. The development of a cyber reserve concept will be legally and operationally regulated, with the possibility of regular training and predictable mobilisation.

The Ministry of Defence and the Army will support the development of cyber personnel through clearly defined roles and responsibilities, defined professional development, and continuous training at a technical level, aligned with international and NATO standards. This includes advanced technical training in the cyber domain, participation in cyber exercises and training, and cooperation with allies to achieve operational interoperability.

By 2030, the defence system will maintain a stable corps of professionals in management, operational, and validating functions, with continuous training and the capacity to be reinforced in crisis conditions.

## 6. Strategy implementation

The implementation of this Strategy will be carried out through a disciplined management system, clearly defined competencies and measurable accountability. Cyber defence readiness will be treated as an integral part of the operational readiness of the defence system. The central coordinating body in the domain of cyber defence will provide regular and consolidated reporting to the management on the state of readiness, key risks in the implementation and progress in the development of capabilities.

If the development of cyber capabilities is to be realized in conditions of limited human and financial resources, priority will be given to mission-essential functions and critical dependencies. The capability will be built through professionalization, continuous training, staff retention and selective partnerships, with the responsibility for cyber readiness being embedded in the overall structure of the defence system, and not limited to a single organizational unit.

Procurement and risk management will be key tools for ensuring resilience. Security requirements will be integrated into the specifications and life cycle of systems, and risks associated with legacy technologies, suppliers and organizational set-up will be subject to continuous oversight. Readiness will be confirmed through regular evaluation and independent assessments, with the possibility of revising the Strategy if the security environment or implementation results so require.

## 7. Conclusion

The Cyber Defence Strategy confirms the political intent and direction for the development and implementation of cyber defence capabilities in the Ministry of Defence and the Army, with the aim of ensuring operational capability in cyberspace in the period 2026–2030. It is based on the inevitable reality that sophisticated hostile activities will continue, and threats in cyberspace will increasingly coincide with broader political and security crises. In such conditions, deterrence is achieved through denial, which means ensuring a defence system that is resilient, capable of recovery, interoperable and functional even in conditions of disruption.

The Strategy establishes three institutional commitments that define success by 2030:

- Cyber defence will be treated as a requirement for operational readiness, fully integrated into planning, exercises, and mission assurance.
- Management discipline will be established through clearly defined accountability, measurable readiness, and continuous reporting, ensuring that progress is visible and accountable.
- Building resilience as a systemic feature, through modernized and segmented infrastructure, structured cooperation with civilian authorities and trusted partners, as well as professional staff structurally integrated into career paths, rather than individual engagement.

The Defence Strategy requires coordination between military and civilian components as a prerequisite for effective defence implementation. This Cyber Defence Strategy responds to that obligation in the cyber domain by clearly defining roles, establishing coordination without institutional ambiguity, and building a defence system capable of maintaining readiness in the face of an active cyber threat.

With the implementation of this Strategy, the Ministry of Defence strengthens the sovereignty of the Republic of North Macedonia through the practical ability to decide and act under pressure, to fulfill national defence obligations, and to contribute to collective defence in a timely and reliable manner by ensuring security, interoperability, and resilience.

MINISTER OF DEFENCE

Vlado Misajlovski