

National Situation Report 2026/1

Hybrid Threats and Response Capability
Mental Resilience

Imprint

Media owner, publisher and editor:
Federal Chancellery Republic of Austria, Office of Crisis Management
Ballhausplatz 2, 1010 Wien
+43 1 531 15-0
bueroksb@bka.gv.at
bundekanzleramt.gv.at
Photo: BKA/Tarek Wilde
Layout: BKA Corporate Identity & Communication Design
Printed by: Digitalprintcenter des BMI
Vienna, 2026

Dear Readers,

I am pleased to present the first whole-of-government strategic situation report 2026 – the Nation Situation Report 2026/1. This document focuses on two areas of particular importance to our state's security and resilience: hybrid threats and our capability to respond to them, as well as the mental resilience of our society.

Hybrid threats are among the most formidable security challenges of our time. Their particular danger lies in the fact that they rarely manifest themselves openly, explicitly or suddenly. They operate insidiously, subversively and often below the threshold which triggers an immediate and clear confrontation. Disinformation, cyber-attacks, drones, foreign influence on the domestic economy and on research, as well as the deliberate weakening of public trust can blend without this interaction being apparent at first glance.

This is where the greatest menace of this phenomenon lies: it attacks not only individual systems, institutions or areas of responsibility, but the very foundations of a state's and society's ability to act. Hybrid threats aim to create uncertainty, shake confidence, paralyse decision-making processes and undermine societal cohesion. It is precisely because their impact often only becomes fully apparent once considerable damage has been done that they are particularly difficult to detect and combat effectively. Furthermore, aggressors can employ an almost infinite variety of forms of hybrid threats. The analyses in this situation report have focused on five of the currently most relevant forms.

A society's mental resilience is the first line of defence – not only, but also in the face of hybrid threats. If people are no longer able to make sense of information, recognise manipulation, maintain trust in politics, public authorities and institutions, and retain their ability to exercise sound judgement even under pressure, all other defensive measures taken by a state are thrown into disarray.

A common, whole-of-nation situational assessment is therefore of central importance. An effective response capability can only be established if the relevant actors, stakeholders and large sections of the population share a similar threat assessment. This situation report is therefore also intended as a contribution towards creating a common basis for evaluation, prioritisation and further action.

I would therefore like to thank everyone who has contributed to the preparation of this Situation Report, and I would like to express my sincere gratitude and appreciation to you all. Yours is a significant contribution to the strengthening of Austria's national security and whole-of-nation resilience.

Dr Peter Vorhofer

Advisor to the Federal Government in matters pertaining to National Security, National Resilience, Comprehensive National Defence, Crisis Preparedness and Crisis Management



Dr Peter Vorhofer

Content

Legal Basis.....4

Methodology.....5

Summaries.....6

Hybrid Threats and Response Capability.....6

Mental Resilience.....8

Whole-of-government Courses of Action.....11

Hybrid Threats and Response Capability.....11

Mental Resilience.....15

Legal Basis

The Federal Crisis Resilience Act (*Bundes-Krisensicherheitsgesetz – B-KSG*) came into force on 1 January 2024. This Act comprehensively advanced the whole-of-government coordination of national security and whole-of-government crisis management. The purpose of the Act is to ensure national security and resilience through stronger networking and cooperation between all actors in the face of new and complex challenges. Newly created structures and processes are intended to improve coordination between, and make more efficient use of, the expertise and capabilities of the various ministries. In addition, the Federal Crisis Resilience Act provides, for the first time, a legal definition of the term “crisis” as well as specific procedures for the identification of the same.

At the head of the structures established under the Federal Crisis Resilience Act are the Advisor to the Federal Government in matters pertaining to National Security, National Resilience, Comprehensive National Defence, Crisis Preparedness and Crisis Management, and his or her deputy. They are supported by the Office of Crisis Management, based in the Federal Chancellery.

Advice to the Federal Government is provided on the basis of, inter alia, a biannual whole-of-government strategic situation report (National Situation Report). It is generated periodically and holistically on the basis of individual situation reports pertaining to the areas of security, health, energy, climate and environment, the economy, intelligence developments, and defence policy. However, it also employs a topic-focused approach to deal with focus areas, using ministerial expertise as well as that of other relevant actors where appropriate, in a whole-of-government strategic approach.

The present Situation Report was created taking a topic-focused approach. Owing to its security-sensitive nature, only extracts from the Situation Report can be reproduced in the following document.

Methodology

The National Situation Report summarised here comprises the areas of “hybrid threats and response capability” and “mental resilience”. Both areas were prepared employing the same methodology. In the specialist boards, established pursuant to the Federal Crisis Resilience Act, individual situation reports were created in which both areas, including their sub-chapters, were elaborated on the basis of the following frameworks:¹

1. qualitative and quantitative description of the status quo
2. derivation of consequences of remaining in the status quo
3. courses of action which, from an expert perspective, would contribute to improving the status quo

The individual situation reports from the specialist boards were subsequently consolidated by the Advisor to the Federal Government and the Office of Crisis Management and expanded to include whole-of-government aspects and courses of action. The thematic structure of the individual situation reports was retained for the National Situation Report.

As with previous National Situation Reports, there was an exchange with academics seconded by the Austrian Academy of Sciences (Österreichische Akademie der Wissenschaften – ÖAW). During this exchange, the subject areas of the Situation Report were examined and discussed from a scientific perspective in order to further develop the holistic analysis of the topics.

Despite its holistic, inter-ministerial nature and the approach taken in its preparation, the Situation Report is nevertheless subject to certain limitations. The content primarily consists of the individual situation reports provided by the participating ministries and specialist boards described above. This means that a certain degree of content pre-selection takes place already in the drafting stage, which has a direct impact on the content of the final Situation Report. As is also the case with academic publications, a fully comprehensive examination of the topics covered in this Situation Report is therefore not feasible, even though this is aimed for to the extent possible.

Furthermore, there may only be indirect responsibilities and thus routine steps pursued by the civil service regarding the subject areas described. In certain areas, this may mean that data which would have been of interest for the analyses in this Situation Report are not available to the contributing ministries and could therefore not be included.

¹ The editorial deadline for the submission of contributions from the various ministries was 3 March 2026; consequently, the information provided relates for the most part to that date. In a few instances, measures which were in the process of being finalised at the time were taken into account.

Summaries

The following is a summary of the areas analysed.

Hybrid Threats and Response Capability

Whilst hybrid threats are by no means a new concept, the term has come under significantly greater public and political scrutiny in recent years, particularly in the context of Russia's war of aggression against Ukraine and its implications for European security.

Austria, too, is a target of hybrid attacks and activities and faces a multifaceted spectrum of threats below the threshold of open military confrontation. Other European states are confronted with similar challenges, which is why intensive exchange and the closest possible coordination between EU Member States in this area creates significant synergy effects. Effective defence and thus the preservation of sovereignty requires first and foremost the identification of hybrid threat scenarios as such, the development of appropriate response mechanisms and their deployment in a concerted manner.

Since hybrid threats, by their very nature, tend to be as subliminal as possible and often seek to influence the population's beliefs and behaviour directly, a clear attribution of individual activities is usually not possible, and the only expedient measure is the creation of a conspectus of numerous incidents by means of analysing so-called "weak signals". To this end, this Situation Report has identified five priority areas which, due to their significant societal leverage and potentially serious consequences – despite the relatively limited resources deployed by hybrid actors – warrant particular attention in hybrid threat assessment:

Foreign Information Manipulation and Interference (FIMI)/ Disinformation

As part of the hybrid spectrum, FIMI poses a complex and long-term challenge to democratic states, as well as a serious threat to European and national security. FIMI increasingly contributes to the destabilisation of democratic societies by repeatedly calling into question political, regulatory and scientific authorities. The associated activities are not deployed haphazardly or purely opportunistically, but form part of an alternative, anti-democratic information ecosystem characterised by strategic, forward-looking planning and comprehensive preparation; one that is broadly conceived, long-term and targeted. In the long term, therefore, strengthening societal resilience is of crucial importance in order to reduce vulnerability to FIMI and disinformation, and thus to preserve the integrity of democratic processes and societal cohesion.

Cyber attacks

Due to their increasing frequency, cyberattacks have evolved from technical fringe phenomena to core threat to the entire state. Critical infrastructure is particularly vulnerable in this regard, as disruptions or failures can trigger significant cascading effects. The boundaries between state action and cybercrime are becoming increasingly blurred, as formally independent actors are used to conceal state responsibility. In view of these risks, too, the question of digital sovereignty is moving further into the focus of national security.

Threats Posed by Unmanned Aerial Systems (Drones)

In recent years, autonomous and semi-autonomous weapon systems, in particular unmanned aerial systems such as drones, have rapidly gained in significance. Their diverse range of applications and relatively low costs make their use in modern conflicts exceptionally effective and efficient. Furthermore, as hybrid weapons, they can cause significant damage with relatively little effort. This fact is also taken into account in Austria's capability planning. Both civilian and military measures are required to improve detection and defence capabilities.

Foreign Interference in Science, Research, Technology and Innovation

This form of hybrid threat places increasing pressure on international cooperation in science, research, technology and innovation, as geopolitical tensions increasingly turn knowledge and innovation into strategic resources and contested assets. A wide range of methods is used to initiate the transfer of critical knowledge and technologies to the detriment of Europe, or to influence research maliciously. In Austria, observers have noted that this is no longer carried out solely by the already known key actors themselves, but increasingly also by proxies and non-state actors.

Threats to the Austrian Economy

In 2025, the Austrian economy found itself caught in a tug of war between complex international networks, technological innovations and geopolitical conflicts. Concomitantly, the threat posed by state-sponsored industrial espionage, hybrid influence and criminal cyberattacks grew. Today, companies across all sectors need not only remain economically competitive, but also actively safeguard their core competencies, production processes and research data. Sectors with a high export ratio are especially vulnerable, whilst infrastructure is regarded as a key factor in economic stability.

Mental Resilience

The concept of mental resilience is closely related to that of Psychological National Defence, but extends significantly further and, unlike Psychological National Defence, does not automatically assume an aggressor-driven scenario. Accordingly, the activities focussing on creating a society that is as resilient as possible are as diverse and intricate as the challenge demands.

At the heart of all state efforts towards mental resilience lie the concepts of democracy and the rule of law as guiding principles and the fundamental organisational framework of the Republic of Austria. Psychological National Defence and the will to defend the country, a basic understanding of democracy among the population, as well as trust in the rule of law and science, aim to create a shared ideational basis for decisions among the population. This is the fundamental prerequisite for understanding what elevates society, and, by extension, a state, to a collective worth defending, and it fosters the readiness and the will to defend oneself against attacks.

Resilience fundamentally begins with being prepared, which first and foremost requires knowledge of potential threats, demands both the decision and the will to prepare, and ultimately involves evaluating and stockpiling the resources needed to cope. The state plays an elementary role in this regard, since issues of security, the safeguarding of the means of subsistence and protection against threats constitute a basic need, the fulfilment of which, in democratic societies, is delegated in key respects to state authorities.

In order to make these abstract concepts – such as security, democracy and the rule of law – more tangible and measurable within a Situation Report, a series of factors have been defined which, when considered together in practical terms, constitute essential components of mental resilience:

Psychological National Defence, the Will to Defend the Country and Civilian Service

Since its enshrinement in the Austrian Federal Constitution in 1975, Psychological National Defence has formed the ideational foundation for Military, Civil and Economic National Defence. Together, these four sub-areas form the framework of Comprehensive National Defence – a fundamental element of Austria's security architecture. With the end of the Cold War's logic of confrontation in the 1990s, Comprehensive National Defence lost prominence in the public eye.

However, against a backdrop of increasing security-political tensions, hybrid threats, disinformation, societal polarisation and climate change, Comprehensive National Defence is once again gaining in importance. The population's concrete willingness to take responsibility for the country's security can be described, in the context of Comprehensive National Defence, in terms of the will to defend the country, with Civilian Service (as alternative service in lieu of military service) also being recognised as a separate pillar.

Societal Security Awareness

In light of current security and geopolitical developments, a society's security awareness can be linked to the concept of mental resilience. The individual, subjective perception of a sense of security is an important prerequisite not only for the identification of challenging situations, but also for the ability to respond to them adaptively.

Strengthening mental resilience is enshrined in the current Austrian Security Strategy as part of Comprehensive National Defence, with the aim of raising awareness of security risks and the necessity for action in the changed security environment, so as to ultimately enable an informed and capable population, together with provisions made by the state, to interpret these uncertainties and cope with them resiliently. With regard to foreign and security policy, it is evident that a clear majority of 75 per cent are in favour of maintaining neutrality; however, 55 per cent believe that the European Union should have a common security and defence policy.

Trust in Democracy, the Rule of Law and Science

Trust in democracy, in the rule of law and science forms an essential element of the mental resilience of modern, liberal societies. It not only enables the legitimisation and acceptance of political decisions, but also strengthens the trust of those subject to the law in the fundamental principles of the rule of law, thereby creating a positive emotional bond with democratic processes. Furthermore, a solid foundation of trust in democratic institutions, fundamental principles and scientific discoveries fosters individual willingness to work in solidarity to tackle common challenges our society faces. Particularly against the backdrop of hybrid threats, polarisation and growing scepticism vis-à-vis state institutions, it becomes clear that trust is not a constant, but must rather be actively nurtured at all levels and continually renewed.

Psychological Resilience, Health Literacy and Climate Resilience

A society's psychological resilience, health literacy and climate resilience strengthen the individual and collective capability to cope with complex challenges and long-term stresses. Through their interplay, these dimensions help to strengthen individual self-efficacy, adaptability and a sense of responsibility, thereby increasing societal resilience vis-à-vis multifaceted challenges. What all three dimensions have in common is that, alongside education and public communication, incentive schemes can also promote effective behavioural patterns at an individual level.

Media Consumption and Media Literacy

The consumption of high-quality media with high journalistic standards as well as a high level of media literacy are key prerequisites for the mental resilience of modern societies. The growing tension between processing emotional stimuli and reacting to objective facts produces a loss of shared reality and, consequently, a weakening of societal resilience. High-quality media provide guidance, contextualise complex issues and thereby strengthen the ability to cognitively process uncertainty and the pressures of a crisis. Media literacy complements this function by empowering the public to critically scrutinise (digital) sources, in the ideal case recognise manipulation strategies, and evaluate information in a reflective manner. Particularly in light of the rapidly growing prevalence of disinformation and FIMI activities, it is clear that these skills will increase in importance in democratic societies – among both young people and adults.

Participation in Cultural Life

Culture is a core aspect of identity and can, because of the freedom with which it is shaped within democratic structures, be very quickly and directly attacked, undermined or generally threatened by alternative narratives. Culture, as a fundamental human right and a strategic resource, is indispensable for democratic and societal resilience. The loss of cultural assets, as well as of cultural practices, is irreparable and therefore painful for individual identities, which is why attacks in this area also have an immediate destabilising effect on the community.

Strengthening cultural resilience to crises, integrating cultural aspects into state crisis, conflict and disaster management plans, and pursuing an inclusive cultural policy which promotes access, participation and artistic freedom not only reinforce democratic values, societal cohesion and trust in democratic institutions, but are also integral levers in the strengthening of domestic security architecture. In a broader definition of the concept of culture, natural landscapes can likewise be of great significance to a society's cultural understanding. In Austria, between the Pannonicum and the high-alpine zones, there is a unique diversity of endemic plants and animals concentrated within a very small area; its striking landscapes form also a sense of identity and cultural significance for a large part of the population and can therefore be viewed as part of the national cultural heritage.

Whole-of-government Courses of Action

The following whole-of-government courses of action are derived from the findings of the Situation Report summarised above. The implementation of these courses of action could make a significant contribution to further enhancing national security and state resilience.

Hybrid Threats and Response Capability

- **Strengthening democratic resilience through mental resilience** in order to achieve a **deterrent effect**
... because Foreign Information Manipulation and Interference (FIMI) deliberately exploits existing societal tensions and conflicts, distorts information spaces and thereby permanently undermines the functionality and legitimacy of democratic decision-making processes.²
- **Raising awareness amongst media operators** that they themselves can be used as **hybrid tools** by actors
... because FIMI specifically seeks to influence information channels, distort narratives and undermine trust in journalistic work, thereby weakening a central pillar of democratic opinion-forming.
- **Targeted support for EU providers to drive the scaling up of digital ecosystems and reduce dependencies on corporations in third countries. This also includes refraining from contracting international or external providers for current or future procurements**
... because Austria's dependence on digital services and providers from third countries needs to be reduced, and a switch to EU providers should therefore be made as soon as possible.

2 The impact of FIMI campaigns on elections has already reached other EU Member States and Austria's neighbouring countries (e.g. Slovenia, France, Germany, etc.). It is highly likely for Austria also to be affected in the future if FIMI actors deem this to be in their interest.

- **Further development and expansion of the state's attribution capabilities**
... because Austria's capacity to provide the necessary information in the required quantity and quality under time pressure could be optimised. A technical implementation in the whole-of-government context for all domains would be appropriate. The Federal Ministry of Defence's project on the Situation Report on Hybrid Threats can be cited as a positive example.³
- **Introduction of mandatory resilience tests for critical infrastructure** via the NIS⁴ mechanism
... because the NIS Act has established the legal framework for critical infrastructure in Austria, and this should be implemented on a regular basis.⁵
- **Integration of cybersecurity management into general risk and crisis management**
... because it has been noted that, in many cases, cyber security management is still too isolated from general risk and crisis management, which makes it difficult to address threats holistically.⁶
- **Development of an overarching strategy on Autonomous Systems & Security** (inter-ministerial and extending beyond the topic of 'drones')
... because an overarching strategy is essential to clarify the responsibilities, powers and capabilities of the individual stakeholders.
- **Establishment of binding fail-safe, redundancy and human-in-the-loop requirements for critical applications**
... because regulatory obligations minimise potential risks (Preparedness Union Strategy, keywords: preparedness by design).

3 Furthermore, there appears to be a need for formal threat modelling in order to systematically identify threats and to illustrate the interactions and inter-sectoral consequences of the manifestation of crisis scenarios.

4 NIS = Network and Information Security

5 Testing crisis, emergency and business continuity plans is already a mandatory part of the NIS Directive as amended (NIS-1) and also forms part of the implementation regulation and will therefore be part of the NIS2 regime in future. It should be noted that the NIS regime applies ex ante only to 'critical infrastructure'. For 'important facilities' under NIS2, the Network and Information System Security Act 2026 (in line with the NIS2 Directive) only permits 'ex-post' supervision. Any amendment requires a two-thirds majority in the National Council.

6 This interconnection has already been implemented very successfully in the energy sector and can serve as a model. See, in particular, the Risk-Preparedness Plan for the Electricity Sector of the Republic of Austria, https://www.bmwet.gv.at/dam/jcr:4552770c-26c1-45fa-93ec-9c509883ee6b/AT_Risk_Preparedness_Plan_Electricity_2026_EN.pdf, as well as the Gas Preventive Action Plan, the Gas Emergency Plan, and the Contingency for the Secure Supply of the Republic of Austria with Crude Oil and Petroleum Products, <https://www.bmwet.gv.at/Themen/Energie/Versorgungssicherheit/gas.html>, <https://www.bmwet.gv.at/Themen/Energie/Versorgungssicherheit/erdoel.html>.

- **Conducting regular security/penetration tests** (including red teaming) and **incident simulations**
... because these can demonstrate the practical implementation of theoretical concepts (e.g. further development of Austro Control's capabilities).
- **Expansion of detection and defence capabilities** (including mobile anti-drone systems)
... because the current capacities for identifying and countering unmanned aerial vehicles such as drones in Austria and Europe need to be increased in order to ensure comprehensive security.
- **Alignment of procurement cycles for operational and defence systems** in line with technological developments
... because the prevailing innovation cycles for autonomous systems sometimes span just a few months, and current procurement cycles do not reflect this progress. It is essential that, in this area, rapid procurement is prioritised over a technically optimal solution.
- **Establishing clear powers of intervention and regulatory responsibilities in the event of the misuse of drones**
... because, at present, legal action against misuse is only possible to a limited extent.
- **Development of military capability for integrated air defence across all necessary ranges**
... because capability development in the field of air defence must be guided primarily by military threat scenarios. To this end, primarily kinetic weapons are procured and employed to counter airborne threats. The employment of these systems in densely populated areas is therefore not possible without restriction, at least in peacetime. In peacetime, the employment of drone defence systems within the electromagnetic spectrum requires close coordination with other ministries (e.g. the Ministry of the Interior).
- **Establishment of voluntary stress tests** against drone attacks to ensure the resilience of critical infrastructure in EU Member States
... because these can highlight gaps in resilience and help to close them. A positive example here is the intensified use of testing procedures, also within the framework of the Directive on Security of Network and Information Systems (NIS2 Directive).

- **Ensuring that the implementation of measures to enhance research security at and by universities, higher education institutions and academic research organisations is embedded within the relevant governance instruments (e.g. service level agreements), is continuously reviewed and is further developed through specific projects**
... because this can promote and ensure a uniform security standard.
- **Expanding awareness-raising advisory services regarding the forms and risks of foreign influence on companies and research institutions, in order to increase resilience in the applied RTI sector (Research, Technology and Innovation)**
... because the increasing complexity of the threat landscape posed by foreign influence heightens the need for awareness-raising and information provision for RTI-intensive organisations. Targeted prevention programmes for managers and staff can help foster up-to-date security awareness and enhance research security in the applied RTI sector.⁷
- **Investment screening regarding critical infrastructure to identify foreign direct investment (FDI), particularly in strategic sectors**
... because Austria must not rely on foreign investors in the critical infrastructure sector.
- **Strengthening national key industries of strategic importance through whole-of-government support measures (rail technology, tunnelling, transport engineering)**
... because this enables Austria to act more independently when necessary and reduces its reliance on external markets.
- **Maintaining strategic reserves to provide a buffer in the event of supply disruptions**
... because strategic stockpiling, such as the strategic gas reserves or oil stockpiles, has proven its worth in Austria and can be further expanded.

⁷ Guides and guidance documents for the Austrian RTI sector and industry on various aspects of research security have been drawn up by the Federal Ministry of Innovation, Mobility and Infrastructure and are close to completion. The next steps are the coordination with the Federal Ministry of Women, Science and Research and the Federal Ministry of Economy, Energy and Tourism, as well as institutions of the Federal Ministry for Innovation, Mobility and Infrastructure and the Austrian Council for Sciences, Technology, and Innovation prior to their planned publication. The Austrian Research Promotion Agency is also required to embed research security in its processes.

Mental Resilience

- **Building on the measures already introduced, the further development and strengthening of the existing integration of Psychological National Defence into the education system**, particularly in the areas of political education and civics, as well as **the maintenance and intensification of cooperation** with existing and new partner institutions
... because the teaching of Psychological National Defence is becoming increasingly important in light of geopolitical and societal changes, and the methods of teaching must adapt to these dynamics.
- **Involving and providing further training for teachers, head teachers and stakeholders** in the **further development of curricula**, as well as **continuously reviewing the curricula** in light of societal and technological developments
... because this is necessary to sustainably reinforce the required paradigm shift and ensure that school education remains relevant to future challenges.
- **A greater focus on establishing a comprehensive culture of security and defence in educational institutions** (schools and adult education), with particular attention to specific people and age groups
... because the population's willingness to defend the country must be strengthened as an essential element of Austria's Psychological National Defence.
- **Continuation of efforts to expand the scope of Civilian Service** (as an alternative to military service) **through legislation and to further develop its structure**, for example through an extended period of service and improved personnel planning to ensure long-term operational capability, as stated by the Military Service Commission regarding Civil National Defence
... because alongside national service, alternative service also needs to be further developed.

- **Amending the Civilian Service Act⁸ to create the possibility of deploying Civilian Service personnel in the event of extraordinary Civilian Service in the field of essential public services (electricity generation, water supply, refuse collection, street cleaning, energy supply companies, postal services, etc.) without the need for recognition as a Civilian Service organisation**
... because this is currently impossible and represents a key measure in supporting critical infrastructure in times of crisis.
- **A greater focus on the principles of Psychological National Defence in the Civilian Service training programme**
... because this thematic focus is not yet incorporated to the extent required. This question was also raised within the context of the Military Service Commission.
- **Greater emphasis in Austria on the principle of Comprehensive National Defence (resilience), which extends beyond the military** (projects such as barracks self-sufficiency by 2030), such as the Resilience Strategy to safeguard essential services against sabotage and hybrid attacks
... because the limitation of the concept of national defence to the military sphere during the past 30+ years is not only outdated but also misrepresents and oversimplifies the reality of a state's defence remit.
- **Targeted strengthening of initiatives in digital political education and media literacy** (fake news, disinformation, AI) and the provision of digital teaching materials
... because the societal relevance of these questions must be imparted.
- **Strengthening the Third Mission⁹ of science and research**
... because open discourse can strengthen public trust.
- **Safeguarding and strengthening the re-socialisation function of penal and preventive detention enforcement** by sustainably ensuring effective re-socialisation, including preventive measures. In doing so, greater **emphasis** should be placed on **imparting the values and principles of Psychological National Defence to prisoners**
... because this promotes stabilising effects amongst prisoners, reduces the risk of reoffending and thus makes a direct contribution to societal resilience and the perception of security.

8 The English translation of the German original "Zivildienstgesetz" is, depending on the source, sometimes also referred to as "Alternative Service Act", as it refers to the option for conscientious objectors to complete an alternative service in lieu of compulsory military service in Austria.

9 The term 'Third Mission' refers to the societal mandate of universities and higher education institutions to impart knowledge, alongside research and teaching, to all sectors of society.

- **Continuous implementation of the Austrian Strategy for Adaptation to Climate Change**, in order to promote a holistic approach to adaptation and to avoid maladaptation and path dependencies
... because the effects of climate change can cause mental and physical stress, and adaptation to climate change has a significant impact on the mental resilience of the population. The security-political implications of climate change must also be addressed in a whole-of-nation manner.
- **Promotion of measures to increase individual climate resilience**, such as information and awareness-raising campaigns on climate literacy and personal preparedness, or tax incentives for personal preparedness, including support services to facilitate practical implementation (funding requirements, expert advice, etc.)
... because this promotes individual resilience vis-à-vis climate change and has a positive impact on the protection of our livelihoods.
- **Expanding incentive schemes** for the public to adopt a **resilient lifestyle** (e.g. in the shape of a 'resilience pass') in the areas of mental and physical **health**, as well as **climate and the environment**, including supporting **communication measures** aimed at relevant **target groups**
... because this promotes effective behavioural patterns and can strengthen the resilience of society as a whole. Whilst incentive schemes do exist to some extent in these areas, their potential has not yet been fully realised.
- **Strengthening digital media and AI literacy** amongst the public in the context of school and adult education
... because FIMI techniques and digital disinformation are evolving rapidly, and digital media literacy and the scrutiny of contents are extremely effective and, concomitantly, relatively cost-effective measures to counter these developments.

- **Recognising cultural heritage institutions¹⁰ (priority list) as part of Austria's critical infrastructure**
 ... because cultural heritage sites and institutions are not yet obliged to put protective measures in place (e.g. against natural disasters) and this is the only way to ensure that important cultural assets are better protected in the event of a crisis or disaster. This would take account of the significant influence of culture on personal, societal and national identity, thereby also sustainably strengthening the psychological resilience and cohesion of the population in the face of attacks, crises and disasters. See also the handbook Emergency Management in Museums and Cultural Heritage Institutions.¹¹

- **Integration of cultural aspects into national crisis, conflict and disaster management plans**
 ... because this question is currently not given sufficient consideration at the whole-of-government level, so that culture, both as a potential source of conflict and as an essential resource for society, is not adequately recognised.

¹⁰ Cultural heritage institutions include, inter alia, museums, archives, buildings and sites of particular cultural, historical or religious significance (e.g. Schönbrunn Palace and Gardens, Hohen-salzburg Fortress, Dürnstein Church, the State Opera, archaeological sites such as Carnuntum, etc.). They house cultural assets or are cultural assets in their own right. They may also be sites where intangible cultural heritage is practised or preserved. Particular attention should be paid to UNESCO World Cultural and Natural Heritage sites; cf.: <https://www.unesco.at/en/culture/world-heritage/the-world-heritage-list>.

¹¹ Elke Kellner (ed.) on the initiative of the Working Group on the Protection of Cultural Heritage (comprising representatives from ICOM Austria, the Federal Ministry for Housing, Arts, Culture, Media and Sport, the Federal Monuments Office, the Austrian Armed Forces, the Austrian National Commission for UNESCO and the Austrian National Committee of the Blue Shield).