**Report of the *Saeima*1**

**On Approval of the National Security Concept**

I inform that the *Saeima* has approved the National Security Concept at the sitting of 28 September of this year.

Chairperson of the *Saeima* D. Mieriņa

Adopted 28 September 2023

**National Security Concept 2023**

**1. Introduction**

The National Security Concept (hereinafter – the Concept) is a document prepared on the basis of the analysis of threat to the State specifying the basic strategic principles and priorities for the prevention of threat to the State to be taken into account when developing new policy planning documents, legal acts, and action plans in the field of national security.

In 2022, a new analysis of threat to the State was developed, and a new *Saeima* was elected. Thus, in accordance with the National Security Law, the current cycle for the development of a new Concept has arrived. However, significant deterioration of the international security situation after the full-scale military invasion of Ukraine initiated by the Russian Federation (hereinafter – Russia) on 24 February 2022 is an equally important factor prompting the review of the current Concept.

Threats which have a direct and indirect impact on national security of Latvia are discussed in this Concept. Threats to national security are related to the development of the situation in the international security environment, the war waged by Russia in Ukraine, the hybrid threat, to malicious cyber activities and tendencies of international terrorism. Although mitigated under the influence of objective circumstances, threats are still caused by long-term attempts of individual countries to influence the State of Latvia, its society, and values, the current course of the State foreign policy oriented towards the West, and also the internal political stability, using political, economic, and information means.

General priorities for the prevention of such threats are specified in the Concept according to each field of threat. The policy developed by State administration institutions, the measures planned and implemented thereby as well as the mutual cooperation in the field of national security must be based on the priorities laid down in the Concept. The Cabinet, on the basis of the priorities laid down in the Concept, shall draw up the National Security Plan which includes specific measures and means for the neutralisation and prevention of threat to the State.

**2. National Security and National Security Policy**

The existence of the State of Latvia depends on a responsible attitude of all inhabitants of Latvia towards the State and its security. National security and defence of Latvia is characterised by the readiness of the whole society and State authorities to overcome threats, the resilience towards negative external influence, and the ability to resist and continuously renew after challenges and crises. National security of Latvia is based on a comprehensive State defence system which promotes the willingness and readiness of inhabitants to defend the State, creates preconditions for overcoming threats, and ensures execution of the functions of importance to the State during crises and other shocks.

National security is an aggregate of circumstances achieved as a result of purposefully implemented measures. Implementation of specific measures by the State and society reduces the internal and external vulnerabilities of Latvia, and also enhances the overall capabilities and general readiness of the State to identify, prevent, and overcome threats to national security.

National security of Latvia has military dimension, foreign policy dimension, and internal security dimension which are mutually linked. The military dimension is characterised by the war waged by Russia in Ukraine and its potential development, and also by military activities of Russia in the Baltic Sea Region. The foreign policy dimension is characterised by the current unstable international security environment, potential changes therein, and external threats. The internal security dimension is characterised by ensuring of the fundamental values laid down in the Constitution of the Republic of Latvia by the State, and also security risks that are hybrid in nature and threats affecting all three dimensions.

Internal security is based on a cohesive civil society with a common understanding of the fundamental values and a wish to see Latvia as an independent, democratic, legal State that belongs to the Western world. Civil society is active, organising and participating in various civic activities, including involvement in State defence in critical moments. The capacity of the institutions that are part of the Civil Protection System and the development of their abilities are also of importance to the internal security dimension.

For efficient functioning of all the three abovementioned dimensions of national security, the capacity of the National Armed Forces (hereinafter – the NAF), the State Border Guard, State security institutions, law enforcement authorities, and the Foreign Service and their ability to react in case of threat are extremely important.

The participation of Latvia in the North Atlantic Treaty Organization (hereinafter – NATO) and the European Union (hereinafter – the EU) is an important basic element of national security of Latvia which adds to the national attempts of solving the issues related to national security and defence. According to the NATO principle of collective defence, military threat to Latvia is considered joint threat to the alliance.

The national security policy is a set of measures directed towards surveying, prevention, and overcoming of threats to national security. The scope and diverse nature of the potential threats to national security of Latvia exceed the competence of defence authorities and authorities of the system of the interior. Thus, the whole State administration as well as the society should get involved in identifying, prevention, and overcoming threats to national security. Taking into account the large number of authorities involved, centralised management of the national security policy and mutual coordination of such authorities are important.

The society and the support provided by it to the State administration institutions play an important role in implementation of the national security policy. Such support may be provided by educated and civically active inhabitants with adequate understanding and abilities to critically assess, for example, the content and meaning of information messages. A long-term national security policy is based on educating the society in the field of national security.

**3. Russia’s Aggression against Ukraine and Changes in the International Security Environment**

In waging full-scale hostilities in Ukraine, Russia has demonstrated its readiness to use the military force of the highest level against other countries, violating international law and disregarding humanitarian considerations. The Russian Government, together with its accomplice Belarus, are fully responsible for the aggression against Ukraine. The war waged by Russia in Ukraine has a direct negative impact on national security of Latvia as well as the security situation in Europe.

Russia’s unprovoked and full-scale military aggression against Ukraine, war crimes, unlawful annexation of individual territories of Ukraine, and also blackmailing of the international community by threatening to use weapons of mass destruction and causing nuclear disasters have destroyed the credibility of Russia as a responsible partner and has significantly affected the security situation in Europe. Russia’s aggression has deepened the existing challenges to security and stability and created new ones.

The overall security situation in Europe has become more unstable, complex, and fragmented than ever since the World War II. The current security situation in Europe is characterised by multilateral threats, starting with terrorism, violent extremism, and organised crime and ending with threats that are hybrid in nature and cyber attacks, instrumentalisation of migration, proliferation of weapons, and weakening of the arms control architecture. Financial instability, social and economic disparities can further exacerbate the dynamics of threat and affect security of Europe. Moreover, Russia’s activities have exacerbated the global food crisis and caused disruptions in energy resource supplies.

Russia perceives its aggression against Ukraine as part of a broader conflict that reflects its opposition to the West in general, but particularly to the USA. Under the cover of the war inflicted in Ukraine, Russia tries to return the world to a policy of spheres of influence. The Russian Government is actively trying to maintain the existing and create new so-called spheres of influence through its military intervention in Georgia and Ukraine, *de facto* control over Belarus, and also permanent presence of Russian troops in protracted conflicts, including in Moldova. Russia is also present in other parts of the world, for example, in Libya, Syria, the Central African Republic, and Mali. It opportunistically uses instability and complex internal political situation in these countries, including through the use of disinformation and mercenaries, for example, the Wagner Group, a private military company. Russia also continues to militarise the Arctic and to increase tension in this region.

With its unprovoked and unjustified military aggression against Ukraine, Russia has grossly violated the United Nations (hereinafter – the UN) Charter and other international law. In threatening European and international security and stability, Russia has already been ignoring the international norms since its military aggression in Georgia in 2008.

General deterioration of the international security situation has reached a level where there is a basis for including the issues regarding joint efforts to ensure strategic stability and to maintain non-proliferation of weapons of mass destruction, arms control, and disarmament regime on the agenda of intergovernmental negotiations.

The war waged by Russia against Ukraine has partly destroyed the existing arms control architecture. Russia has continuously failed to fulfil in good faith its obligations in arms control mechanisms. Its approach has been manipulative, selective, and deliberately misleading. For several years, Russia has questioned the integrity of the existing rules, clearly violating or avoiding compliance with the obligations laid down therein. At the same time, any attempts to review the existing arms control architecture or to replace it with negotiations for new instruments will not automatically lead to positive changes but rather divert attention from Russia’s aggressive activities in Europe. Therefore, any solutions in the future should be based on strict mutual proportionality and verifiability.

Belarus has been posing a threat to regional stability and security since the internationally unrecognised presidential election in August 2020. The authoritarianism observed in Belarus manifests itself in violent repression against inhabitants of this country and opponents of the regime, in active military support for Russia’s aggression against Ukraine and hybrid tactics against the EU. Increasing dependence on Russia turns Belarus into an instrument at the disposal of Russia in order to achieve its aggressive goals. Belarus has *de facto* lost its status of a nuclear-weapon-free zone. Belarus continues the instrumentalisation of migration initiated in 2021, seeking to destabilise the situation on the border with Latvia and other EU Member States by employing hybrid methods. Thus, Belarus poses serious threats to NATO and the EU external border.

Hybrid activities performed by authoritarian regimes and non-state actors are becoming increasingly intense and diverse. The range of hybrid threats is extensive, covering both economic as well as energy blackmail and intervention in the fields of science, finance, and education. Hybrid activities are carried out in order to weaken the Western unity, democratic values, decision-making, and overall ability to resist or delay activities of aggressors.

Issues such as diversification of energy sources, protection of critical infrastructure, and security of supply chains have become increasingly relevant in Europe since Russia’s full-scale invasion of Ukraine. When transitioning to new energy sources and supply routes, it is important not to create new dependencies, in particular on authoritarian regimes.

The most effective way of combating hybrid threats is to promote national and collective resilience by identifying and addressing vulnerabilities and dependencies. The hybrid threat affects both the governmental and non-governmental sectors, therefore an approach involving the entire State administration and society in strengthening resilience should be used to reduce it. Latvia should also provide any support possible to our partners, in particular EU enlargement countries, enhancing their resilience and ability to resist hybrid attacks.

China’s economic, military, and technological capabilities have grown rapidly in recent years as a result of which China more insistently seeks to strengthen its global political influence and to implement security interests which includes offering an alternative perspective and driving initiatives that affect multilateralism, adherence to democratic norms, global development, and security policy. Thus China’s interests often come into conflict with the Western stance based on universal values and the global security architecture. The relationship between the West and China is multifaceted, characterised by both cooperation and dialogue, and also competition and systemic contradictions. China seeks to restrict access to its market and to change international standards according to its interests. It implements its policy by increasing its presence in the world, including in seas and space, and also using a wide range of influence instruments.

Joint military training of Russia and China is part of a strategic partnership between the two countries and their approximation efforts aimed at the Western countries and envisaging joint positioning with Russia, including in global security issues. China’s role and involvement in regional tensions are increasing. Development of China’s military capabilities, including strategic armament systems, can be observed. China has significantly developed its military means. Its aim is to complete the overall modernisation of its armed forces by 2035, thus potentially affecting the regional and global security. At the same time, China demonstrates a dismissive approach to engaging in negotiations for arms control, disarmament, and non-proliferation.

The hybrid operations and disinformation campaigns implemented by China pose risks not only in the Indian and Pacific Ocean region but also beyond it. It is in the interests of Latvia to strengthen cooperation with partners in the Indian and Pacific Ocean region in order to address regional challenges in common security interests. It is essential in both the public and private sectors to continue working on reducing strategic dependencies and vulnerabilities, including by carefully assessing China’s investments in all sectors of the economy.

Security situation in the Middle East, North Africa, and the Sahel region is closely linked to European and international security in general. Severe consequences of the shocks of economic and social nature caused by political instability, violence, armed conflicts, food shortage, and climate change in this region increase the risks of migration, radicalisation, and terrorism. These risks come with the potential of rapid escalation.

Terrorism in all its forms and manifestations poses the most direct threats to international security. Unpredictability and cross-border spread of the terrorism threat increase not only due to political instability and violent conflicts but also along with the development of modern technologies. The development of modern technologies increases the risks of using, for example, drones, 3D printers, cryptocurrencies, and opportunities provided by artificial intelligence for terrorist purposes.

The war initiated by Russia also leads to increased risks of the spread of radicalisation and violent extremism and to unpredictability of activities of extremist individuals. In addition to that, risks such as illicit trafficking of firearms and challenges posed by chemical, biological, radiological, and nuclear threats (CBRN) also increase.

**Priorities for Addressing the Threat Posed to the International Security Environment:**

**Strengthening of NATO’s Collective Defence and the Eastern Flank**

It is in the interests of Latvia and its allies to find sustainable long-term security solutions. To ensure NATO’s compliance with future challenges and needs, the allies approved the new NATO Strategic Concept at the Madrid Summit in 2022. NATO reaffirms in this document the collective defence as the basic task of the alliance, and also provides guidelines on how NATO should adapt to changes in the security situation around the world and highlights the main tasks of the alliance, i.e. strengthening of deterrence and defence, crisis prevention and management as well as cooperation in the field of security. NATO has recognised Russia as the main threat to the Euro-Atlantic security, peace, and stability.

The work on implementation of the tasks identified at the Madrid Summit continued at the Vilnius Summit in 2023. It is essential for Latvia to achieve that NATO adjusts to the current security situation as soon as possible: practical implementation of NATO’s “forward defence”, ensuring the feasibility of regional plans, increasing the presence of allied forces in Latvia, and also strengthening of air and missile defence. The ability to objectively evaluate and respond to hybrid threat and the possibilities offered by new technologies also plays an important role in these efforts. At the same time, Latvia should continue developing the necessary capabilities of host nation support.

Participation of Finland and the anticipated participation of Sweden in NATO and their integration into the military structures of the alliance play an indispensable role in strengthening the security environment of the Baltic Sea Region and promoting Baltic-Nordic cooperation.

**Strengthening of the EU’s International Role**

It is in the interests of Latvia to promote further consolidation of internally and externally strong EU as a globally influential union of nation states united by common democratic values and support for human rights. It is important to continue strengthening the EU relations with the United Kingdom and Norway, transatlantic relations with the USA and Canada, and also to promote further consolidation of like-minded countries in the region. Further support should also be given to the fulfilment of criteria, the achievements of each country, and the EU enlargement policy based on European values.

**Engagement in International Efforts to Achieve Cessation of Hostilities in Ukraine**

Rule-based international order and reliability should be strengthened for an efficient multilateral approach to international relations. Such approach should be consistently implemented in any relations with Russia and Belarus to prevent the recurrence of similar crimes of aggression in the future. It will be the main priority over the next few years to limit the threats posed by Russia.

**Active Foreign Policy Activity of Latvia in Various International Formats**

Latvia is an active and reliable member state in international cooperation formats with values based on international law. Latvia maintains an active dialogue and promotes close regional cooperation with the Baltic and Nordic countries as well as Poland in its foreign policy. In security policy, special attention is devoted to consultations and shaping of unified policy with NATO allies and the EU Member States. Latvia is constructively operating in various multilateral formats, including issues related to ensuring peace, security, sustainable development (innovative and environmentally friendly economy, rule of law and good governance, international cooperation, and quality education), respect for women’s rights, digitalisation, encouraging of best practices in climate solutions, use of the development of responsible technologies, and others. Latvia plans to contribute to the tackling of these significant tasks by becoming a non-permanent member of the UN Security Council in 2026–2027.

**4. Prevention of Military Threat**

The full-scale war initiated by Russia against Ukraine overall increases the military threat to Latvia. Despite significant losses, Russia is and will remain the main source of threats to security of Latvia, and also a threat to the Baltic Sea Region as a whole. Russia will learn from its mistakes and implement targeted measures to restore its combat capabilities. Russia will respond to the joining of Finland, and also to the expected joining of Sweden to NATO by deploying additional conventional forces in the Baltic Sea Region. This may be followed by more frequent and larger joint military exercises of Russia and Belarus in the strategic direction of the West. Russia will try to compensate for it losses of conventional forces in the war in Ukraine by increasing threats of using nuclear weapon, and also hybrid warfare instruments.

Russian ideologists and propagandists are creating a negative and aggressive attitude towards the Baltic State within the society of this country. Russia is still using a wide range of means at its disposal, including disinformation, to influence politics in the Baltic States.

Russia is ready to use military force for the achievement of its geopolitical goals. Although the conventional capabilities of the Russian Armed Forces have proven to be weaker than previously assessed (corruption, poor technical condition, low training level), this has not deterred the Kremlin from continuing the war. After losses and retreat, Russia has not abandoned its initial goals, it has only changed its tactics and adapted to a prolonged form of warfare. Russia keeps finding ways of compensating for losses of manpower and military equipment, shortage of technologies and ammunition, while the Russian society remains apathetic and passive, encouraging the Kremlin to continue its hostilities.

Belarus plays an important role in Russia’s hostilities against Ukraine as its authoritarian leader is trying to present himself as Russia’s most significant strategic partner on the European continent. Russia used the territory of Belarus for force generation in the most important direction of attack before the invasion of Ukraine in February 2022.

The territory of Belarus is still used for aviation and missile strikes, logistics – the movement of forces and equipment, supply, rotation, treatment of the wounded, repair of the damaged equipment, and also for maintaining constant pressure to divert Ukrainian forces away from the main war zones. Where necessary, Russia can count on the possibility of reusing the territory of Belarus for aggression against the neighbouring countries.

Russian forces establish a ruthless occupation regime in the occupied Ukrainian territories, committing war crimes and violence against civilians and turning it into a standard practice. Although the war crimes committed by Russia affect the attitude of the international community towards the country, there is no indication that they would lead to public condemnation in Russia itself; on the contrary, Russia’s official position and public attitude encourage and promote crimes against civilians in the occupied territories. As regards the internal policy, discontent manifested in the Russian society is controlled to the maximum extent possible, ensuring stability of the existing regime over the next few years. As aggression against Ukraine continues and propaganda intensifies the message of the so-called “total war”, support for the ruling regime can even increase within the Russian society.

Despite the significant losses suffered by the Russian Armed Forces in Ukraine, their military potential remains high. Russia has sufficient financial resources and military reserves to continue the war. Russia also has nuclear weapons to continue confrontation with the Western countries. Therefore, Moscow still endangers and will continue to endanger Russia’s neighbouring countries. Currently all military resources of Russia are directed towards achieving victory in Ukraine but this will certainly change when the war ends.

It is expected that attempts to destabilise the situation in the Baltic States will continue or even intensify, using the means available to Russia. If Russia succeeds in strengthening its position, it will attempt to acquire additional instruments of influence in a broader region, including the Baltic States, seeking to maintain and strengthen the Russian language and cultural environment, the media supporting Russia’s position in both Russian and other European languages. Russia will also continue to use the hybrid methods or military operations in order to extend its influence.

Lessons learned in the war will change the Russian Armed Forces. Selection of more capable commanders, fight against corruption, and other changes can increase the operational effectiveness of the Russian Armed Forces more quickly than establishing the planned new units and restocking the modern military equipment. In order to produce new military equipment, Russia will need Western technologies that are included in the list of sanctions, but Russia has repeatedly demonstrated that it is capable of systematically bypassing the sanctions. It might take up to ten years to restock the equipment to the pre-war level, but until then Russia will be able to make use of the repaired older generation equipment that is still available.

**Priorities for the Prevention of the Military Threat:**

**Further Strengthening of the Comprehensive National Defence System and Implementation of a Model of the Culture of Readiness for Actions**

Development and security of the State of Latvia are linked to the overall unity of the society. Defence of the State of Latvia and its further growth are a joint responsibility of the society as a whole which is implemented from the individual and non-governmental sectors to the State level. The joint responsibility is implemented with the help of further implementation of the model of a comprehensive national defence system, covering a wide range of measures to strengthen the deterrence and defence capabilities and to promote resilience of the society.

A developed culture of readiness for actions and a unified set of democratic values are prerequisites for the resilience of the society and the survival of the State, envisaging the readiness of the society to act in case of crisis and war, the ability to ensure uninterrupted functioning of all sectors, and support for the NAF defence operations.

**Strengthening of the National Deterrence and Defence Capabilities of the NAF**

The cornerstone of Latvia’s deterrence and defence is formed by the NAF military capabilities and the strategy for their use, NATO’s collective defence mechanisms, and strategic partnerships at bilateral and multilateral levels. Latvia, together with its allies, maintain and develop combat capabilities, demonstrating commitment and readiness to defend Latvia against any kind of threat. The NAF units demonstrate high combat readiness and respond to various security challenges, and also provide the necessary support to civilian authorities.

It is necessary to invest and develop a significantly larger army that is ready for combat. Implementation of the national defence service will ensure personnel for the development of the NAF priority capabilities, an increase in the personnel, and also trained reserve soldiers for high and general readiness reserve units, thus contributing to the structural transformation of the NAF in the long term. Gradual implementation of the national defence service will promote increase of the NAF combat capabilities, at the same time strengthening the link between the society and the NAF and promoting the public understanding of national defence.

**Strengthening of NATO’s Collective Defence System**

Latvia’s defence is developed within the scope of NATO’s collective defence which is the strongest instrument for the deterrence of the enemy. NATO is a nuclear alliance, providing a nuclear deterrence umbrella to all members of the organisation. Latvia ensures its role in promoting this important mission. To deter the enemy from attacking Latvia and ensure immediate defence, it is important to ensure that NATO’S “forward defence” is developed and put in practice.

National deterrence and defence capabilities are also enhanced by efforts of strategic partnerships and international cooperation, providing both additional military and security support and investing in the existing international rule-based order.

**Development of the Military Capacity of Transport Infrastructure**

To develop NATO’s ability to respond to any external threat in Latvia and to ensure the principle of NATO’s collective defence, it is necessary to develop dual-use infrastructure projects included in the Trans-European Transport Network (TEN-T), increasing their military capacity and support function, thus creating multifunctional transport corridors with the ability of servicing large-scale military transports.

**5. Prevention of Threat Caused by Foreign Intelligence and Security Services**

Work against Latvia is being implemented by intelligence and security services of several states (hereinafter – the intelligence and security services). Activities carried out by the Russian intelligence and security services are aggressive and pose a significant threat to both collective security of NATO members and the EU Member States and national security of the State of Latvia. Russia’s policy involves the preparation for the most extensive conflict with NATO possible. This sets the framework for the activities of the Russian intelligence and security services – Russia develops and elaborates not only scenarios for military attacks but also plans to weaken the enemy in all areas and phases of hybrid warfare. Threats to Latvia’s security are also posed by Belarusian intelligence and security services which increasingly coordinate their activities with the Russian intelligence and security services.

The Russian intelligence and security services are implementing a targeted and systematic work in order to obtain intelligence regarding the most essential aspects of the foreign policy, security policy, internal policy, economy, and energy policy of Latvia, and also following the social processes and the mood of the society. In the context of the war waged by Russia in Ukraine, the intelligence priority is the political and military support provided to Ukraine by the Western countries, including Latvia, and also the formation of action policy towards Russia.

Security policy, military and civil defence capabilities, critical infrastructure, crisis management mechanisms, and border security of Latvia are significant targets for intelligence of the Russian intelligence and security services. The increasing isolation of Russia and tension in relations with the Western countries will increase the Kremlin’s demand for intelligence data. It is expected that the intensity of espionage activities against the Western countries, including Latvia, will increase.

Concurrently with gathering intelligence and strengthening the positions of the agency, the Russian intelligence and security services are launching short-term and long-term measures with the objective of influencing: they are creating a network of agents of influence, conducting research and strengthening of the levers of influence, and also implementing targeted operations of influence in order to advance decision-making, socio-political processes, and the public opinion in a manner favourable to the Kremlin. Operations of influence are carried out by combining different methods, including agents of influence, cyberspace, and information space where social networking and video sharing platforms are a significant component. Thematic measures of influence are most often associated with the efforts to promote tension in the society of Latvia, distrust in State authority and politics, and also dissemination of the Kremlin’s world vision in specific groups in society.

The Russian intelligence and security services carry out activities against Latvia by working from different positions – from Russia and its territory, in the border area, under the cover of diplomatic representation offices, in third countries, within the framework of international organisations, and also in the cyberspace and information space. As traditional espionage opportunities diminish, the threat posed by the activities carried out by the intelligence and security services from the territory of Russia increases. Nationals of Latvia travelling to Russia and Belarus have an increasing risk of falling under the attention of the intelligence and security services of these countries.

Special units have been established within the Russian intelligence and security services to carry out aggressive special operations abroad. For the purpose of carrying out such operations, officers of the intelligence and security services can travel individually or in a group using their real or false identities. As the confrontation with the Western countries resulting from the war waged by Russia in Ukraine increases, the risk of aggressive operations carried out by the Russian intelligence and security services in Latvia will also increase. The task of the Russian intelligence and security services is to develop capabilities in order to be able to direct a wide range of operations against Latvia in case of a conflict – provocations, destructive actions and diversion, information warfare, cyber attacks on critical infrastructure, and disruption of the operation of significant sectors of the State.

The strategic objective of State security institutions (the State Security Service, the Constitution Protection Bureau, and the Defence Intelligence and Security Service) is to ensure a set of pre-emptive and preventive measures to neutralise the threat posed by foreign intelligence and security services to national security and interests of Latvia, and also to the collective security and interests of NATO and the EU. The priority tasks must be based on the strengthening and improvement of the existing activity of State intelligence and security services according to the existing types of threat.

**Priorities for Elimination of Threat Caused by Foreign Intelligence and Security Services:**

**Strengthening of Counterintelligence and Preventive Measures, Development of Capabilities**

The task of State intelligence and security services is to perform continuous counterintelligence measures, identifying the activities implemented by foreign intelligence and security services which are being implemented against Latvia and nationals of Latvia, using a wide range of methods. The counterintelligence activity should be directed not only towards the discovering and neutralisation of employees of foreign intelligence and security services and their agency as well as the protection of information of significance to national security and of critical infrastructure, but also towards the identification of the agents of influence and operations of influence, inter alia, discovering information operations carried out on media and social networking and video sharing platforms.

Taking into account the intense interest of foreign intelligence and security services in the defence abilities and security of the external border of Latvia, complex counterintelligence measures should be strengthened at sites and in objects where the military forces and infrastructure of the NAF and the allies, the units of the State Border Guard are concentrated, as well as in the territories of the border area. Increased counterintelligence work should be implemented in objects of critical infrastructure.

It is necessary to intensify counterintelligence measures within groups in society which, according to certain criteria, correspond to the priority target groups of foreign intelligence and security services in deploying measures of influence and establishing the agency network and are potentially more susceptible to these risks. State security institutions should continue working on identification of these groups and evaluation of their views and potential actions, while also cooperating with other State authorities within the scope of this work.

Capabilities of State security institutions should be strengthened to identify operations of influence and information carried out by foreign intelligence and security services on social networking and video sharing platforms. Action schemes should be further improved in cooperation with other authorities to terminate the identified operations quickly and to neutralise them efficiently. Technical solutions at the disposal of State security institutions for both monitoring activities on social networking and video sharing platforms and taking other counterintelligence measures should be further developed.

**Coordinated Cooperation of State Security Institutions with Foreign Partner Services**

Mutual cooperation between the State security institutions of Latvia and also their cooperation with partners of NATO members and EU Member States is an essential tool for the identification and prevention of the threat caused by foreign intelligence and security services and for the strengthening of collective security. The security threat increasing in the region and the changing working methods of foreign intelligence and security services require particularly dynamic communication between State security institutions in order to identify changes in a timely manner, to take into account partner experience, and to establish a joint approach for mitigation of specific risks and neutralisation of threats. Strengthening of coordinated cooperation mechanisms should be continued.

**Interinstitutional Approach and Public Involvement for Comprehensive Identification and Prevention of Threats**

State security institutions should, according to their competence, strengthen cooperation with other State and local government authorities, and also the non-governmental and private sectors which can contribute to the identification of activities of foreign intelligence and security services and to the establishment of general resilience. It should be taken into account that the Russian intelligence and security services carry out special operations abroad, their officers are given false identities, and their intelligence activities involve agents whose movement and residence abroad are legitimate.

As the threat posed by foreign intelligence and security services increases, it is important that the society is able to recognise signs which indicate potential security risks posed by these services. State security institutions should inform and educate the society about the security risks posed by foreign intelligence and security services so that inhabitants would turn to State security institutions in cases when they suspect intelligence activities being carried out by foreign intelligence and security services.

Such practice should also be strengthened in State authorities where the assessment of security risks should be established as a systematic practice within the scope of their functions. Educational work regarding the risks posed by foreign special and security services should be performed in respect of persons travelling to high-risk countries, and also measures should be taken to restrict such travelling practice in specific State administration and private sectors.

**6. Prevention of Threat Caused to Internal Security and Constitutional System**

After Russia’s full-scale invasion of Ukraine, the importance of internal security has rapidly increased both at the national and EU levels. The unstable international security environment and deterioration of security situation in Europe pose several threats to Latvia, in particular in the fields of security of the Eastern border of the State, illegal migration, cohesion of society, hybrid attacks, and organised crime.

As a result of the war, Russia has become radicalised and has activated aggressive rhetoric directed specifically towards NATO. From Russia’s perspective, hybrid warfare instruments (propaganda, disinformation, and other manipulations in the information space, cyber attacks, agents of influence, etc.) are still of vital importance in order to achieve its goals in NATO and EU countries. Russia’s hybrid threats to Latvia and the Western world as a whole will not only remain relevant over the next few years but are also likely to increase.

Russia’s aggressive policy at the regional and international levels, including the war initiated against Ukraine, and also cyber attacks and disinformation campaigns conducted against NATO and EU countries pose the greatest risks to Latvia’s internal security and constitutional system.

The war waged by Russia in Ukraine has strongly resonated within the society of Latvia, revealing differences in the belief systems, ideological convictions, and historical memories of certain groups in the society from the values held by the majority of the Latvian society. These differences are clearly demonstrated by sympathies towards the Kremlin expressed by some groups of inhabitants representing the minority of the Latvian society, their public support tor Russia’s aggression in Ukraine, and openness to Russia’s measures of influence.

The war waged by Russia in Ukraine has created not only a sense of insecurity and condemnation in the majority of the society but also a demand for more rapid renouncement of the Soviet legacy which manifested in 2022 as the dismantling of Soviet-era “monuments” by the government and many local governments. At the same time, such activities, and also the support provided by Latvia to Ukraine provoked a wave of aggression among the inhabitants who have a favourable view of the Kremlin. This aggression and hate which mainly manifest themselves in comments on social networking and video sharing platforms, but also in incidents often registered in a street environment, including against the refugees from Ukraine, have a negative impact on the internal security situation in general.

As latent ethnic tension persists, along with dissatisfaction with the current situation and aggressiveness, there is a risk that this tension might escalate under specific circumstances. Therefore, State security institutions, in cooperation with law enforcement authorities, should constantly monitor the development of the situation to prevent escalation of tensions and identify signals, in a timely manner, when external subjects try to take advantage of the abovementioned factors for their own interests. Law enforcement authorities should also consistently continue to follow the zero-tolerance principle towards any expressions of support for Russian aggression which appear in the public environment and information space.

Internal security is also affected by the deterioration of the demographic situation, the high level of poverty, income inequality within the society, and also the quality of education. Depopulation which is inevitable in the foreseeable future, and also ageing of the population will create increasing pressure on the State administration as a whole, weakening its ability to ensure quality performance of the functions of the society in the entire territory of the State. This will maintain increased dissatisfaction within the society with the insufficient capacity and work quality of the State administration and will continue to contribute to distrust of inhabitants in State authority.

Downsizing of labour resources and increasing competition for employees will affect all sectors of State administration. In the context of national security, challenges will increase in personnel recruitment in the defence, internal security, and justice sectors. These factors will also create increasing challenges to ensure protection of critical infrastructure at an adequate level. Development of the infrastructure in the interior and justice sectors can be hindered by the construction and building maintenance costs which keep increasing due to inflation. The abovementioned risks will contribute to new internal and external security challenges.

The main internal security risks related to the abovementioned factors include increasing crime, shadow economy, smuggling, alcohol consumption and use of drugs, non-compliance with different safety regulations and requirements at a household level and in entrepreneurship.

**Priorities for the Prevention of Threat Caused to Internal Security and Constitutional System:**

**Strengthening of Cohesive Society**

For the purpose of strengthening internal security and cohesive society, it is necessary to promote the unity of the majority of the society around common values, based on the independence of the State, its belonging to the Western world, the Latvian language as the only official language, and such understanding of history which condemns crimes against humanity committed by totalitarian regimes, and repeating of analogous historical events today.

Responsible State authorities should continue a targeted work to reduce the presence of legacy left by foreign regimes in the cultural environment of Latvia. It is equally important to perform a long-term work on the exhibition of commemorating evidence of events and personalities significant to the State of Latvia and its history by creating monuments and memorial places in the urban environment and by developing museum exhibitions. This work should be aimed towards strengthening the sense of belonging to the State of Latvia as well as a unified understanding of history within the society.

**Strengthening of Security and Defence of the State Border**

Security of the State border is a prerequisite for guaranteeing the inviolability of the State border and for preventing threat to the State. Work on strengthening the inviolability of the external border of Latvia which is also the external border of NATO and EU should be continued and construction of the external land border infrastructure and provision of technical equipment should be completed. Modernisation of telecommunications network infrastructure of the State border should be continued, ensuring compliance with the requirements for the European Border Surveillance System network. At the same time, State administration institutions should already work on specific deterrence and counter-mobility solutions in the border area which would deter a potential adversary from threatening security of Latvia.

Taking into account that Belarus continues to use migration in order to destabilise the situation on the border with Latvia by using hybrid methods, surveillance infrastructure should be improved at the Latvia–Belarus border to ensure smart and digital border surveillance as well as constant monitoring.

Risks of illegal migration and cross-border organised crime at the external border of Latvia are not decreasing, therefore efficient measures should be taken to reduce them, including strengthening the personnel capacity of border guards and customs officers, while ensuring control to prevent involvement of officials of the relevant State institutions in criminal offences that threaten inviolability of the State border.

Implementation of measures should be continued in cooperation with the NAF to ensure building of capacity of the State Border Guard (hereinafter – the SBG) and also equipping the external border of Latvia with mutually integrated technical means for border surveillance and border control. The SBG mobility should also be improved, including by planning and organising regular joint training for the SBG and NAF.

**Civil Protection and Disaster Management**

Experience of the previous years and lessons learned from crisis management, and also findings gained from the COVID-19 pandemic demonstrate that it is necessary to improve the crisis management system by establishing an inter-institutional crisis management mechanism of national level to ensure resilience and continuity of crisis management.

It is necessary to implement a reform of the disaster management system in order to ensure equally efficient, rapid, and high-quality work of the services involved in disaster management within the entire territory of the State by improving cooperation and coordination of the services involved in response and disaster management, establishing disaster management centres, thus also improving the working conditions and occupational safety of personnel employed in the responsible authorities.

Work should be continued in the development and improvement of the understanding of the civil protection system among State and local government authorities as well as the society, including ensuring training on its key elements to promote the formation of a culture of public safety and readiness for crisis situations. State authorities responsible for civil protection and the NAF should provide support to local governments in developing civil protection plans, integrate therein actions in case of crisis and war.

It is necessary to introduce and ensure operation and maintenance of an efficient early warning system in order to notify inhabitants in case of crisis situations, supplementing the existing system with a cell broadcast solution.

**Resilience of Critical Infrastructure**

In order to effectively ensure safety of the inhabitants of Latvia, measures should be implemented with the aim of reducing vulnerability of its infrastructure which is relevant to stable and uninterrupted functioning of the society and economy.

Well-being of inhabitants and uninterrupted activity of national economy depend on critical infrastructure. It is crucial for providing services that are necessary for ensuring the continuity of the most essential social functions of the society and the functioning of national economy. Critical infrastructure should be protected against threats that can cause serious disruptions in its operations. Measures to protect critical infrastructure should be directed towards receiving timely information on a possible threat to the State and responding to, preventing, and overcoming such threats. State authorities, State security institutions, and commercial companies should take measures to strengthen resilience of critical infrastructure against potential threats, including reinforcing requirements for the people employed in this field.

**Strengthening of Capacity of Authorities of the Interior and Justice Systems**

Internal security institutions, law enforcement authorities, and also institutions of the justice system should correspond to modern requirements and should be capable of overcoming current challenges and threats. To prevent the threat to internal security and public order, work on strengthening the capabilities of authorities of the internal and justice systems, planning human resources, providing education and professional development at the appropriate level, ensuring competitive remuneration, and also implementing infrastructure construction and modernisation projects should be continued.

**7. Prevention of Threat Caused to the Information Space of Latvia**

Security of the information space of Latvia is an essential element for ensuring national security of Latvia. Strong and protected information space is based on potent local media of Latvia and quality local content in the Latvian language. It should be ensured that the entire society of Latvia is located within a unified information space, consumes unified content, thus interrupting the division of the society and promoting its cohesion on the basis of the official language. The future State policy on the protection and development of the information space should be fundamentally based on the values of the Latvian language and the Constitution. Such media policy and legal environment should be formed which support content in the official language.

Taking into account that the role of the official language is strengthened in all areas of life in Latvia, starting from 1 January 2026, the content created by the public media should also be only in Latvian and in languages belonging to the cultural space of Europe, thus promoting belonging of all inhabitants of Latvia to a unified information space based on the Latvian language and other languages of the EU, the European Economic Area, and the EU candidate countries. Termination of the State funding for content in the Russian language would complete the process of establishing a unified information space, while content in Russian would continue to exist in commercial media funded by private resources.

To strengthen the local media space, support for high-quality and reliable content in the Latvian language should continue. High-quality local content simultaneously reduces the risks of influence of external propaganda and increases public trust in local media. It is equally important to constantly increase the availability of content, especially the availability of subtitles and Latvian language option in programmes and services in Latvia.

This promotes the understanding of persons about what is heard and increases the possibilities of the inhabitants of Latvia to learn the official language. At the same time, the provision of subtitles is the only means by which part of the society with hearing impairments can be informed and receive quality information on events in Latvia and abroad. Thus, the provision of subtitles and other services related to the availability of content in electronic media programmes and services is also a matter of national security. Protection of the official language as a fundamental value of the Constitution forms an essential foundation of the information space of Latvia.

Before the attacks in Ukraine both in 2014 and 2022, Russia disseminated versatile propaganda messages internationally. Russia’s war propaganda and disinformation messages, and also other manipulations still continue, posing a threat to the information space of Latvia. Following Russia’s full-scale invasion of Ukraine, Latvia has taken several measures to strengthen its information space and to restrict programmes and services that support or justify Russia’s invasion of Ukraine. Russia’s massive propaganda campaigns and activities of information influence are primarily directed towards glorifying the ruling regime in Russia and justifying war crimes and crimes of aggression as well as violations of human rights committed by Russia. Despite the fact that the primary target audience of these propaganda campaigns is the society of Russia, they also reach an audience in Latvia.

A crucial role in the Kremlin propaganda directed against Latvia is played by the “opinion leaders” and “experts ”, i.e. persons who come forward with comments supporting the Kremlin or opinions on current issues, primarily reacting to events in Latvia or information on Latvia in the international environment. For these purposes, the Kremlin propaganda resources use both agents of influence and persons previously unknown to the general public in order to disseminate propaganda messages.

The audiovisual content of propaganda created in Russia is consumed by the audience in Latvia, also using social networking and video sharing platforms, and services provided by unregistered, unlawful content distributors. Taking into account the abovementioned facts, it is in the interests of the information space and national security of Latvia to continue monitoring any content related to Russia, including entertainment content (films, series, shows, etc.), which contains messages disseminated by Russia. Regular monitoring of such content would allow Latvia to identify potential violations and to take systematic actions in order to prevent the harmful impact of such content on the society.

Restriction of content distributed unlawfully is also relevant to the protection of the information space of Latvia. Work on restricting access to resources where different type of unlawful content is disseminated should be continued, concurrently improving the effectiveness of restrictive measures. Reduction of the spread of unlawful content in Latvia protects the local media market, prevents financial resources from diverting to unlawful content distributors, and also reduces the opportunities for the dissemination of propaganda in Latvia. It is also necessary to promote public awareness of the negative impact of unlawful content distribution on national economy and security of the information space of Latvia.

Capacities of human resources and technologies of the National Electronic Mass Media Council should also be strengthened in the future.

**Priorities for Ensuring Security and Protection of the Information Space:**

**Promotion of Information Literacy and Media Literacy of the Society**

It is essential to promote education for all members of the society, increasing their information literacy and media literacy skills so that people would be able to distinguish false news and disinformation, as well as the ability to critically assess the information disseminated in the information space should be developed to avoid spreading of unchecked news. This will strengthen the democracy of Latvia, promote independent judgement and decision-making of each member of the society, education, and overall public safety, while mitigating threats of the influence of external propaganda.

To achieve this goal, the education system should be prepared at all levels (lecturers of higher education institutions, skills of prospective and working, methodological teaching materials, etc.) to provide pupils and students with media literacy and critical thinking skills at a level which would allow them to identify risks in the information space. Targeted activities should also be used for reaching groups of inhabitants that are outside the education system in order to strengthen resilience in these groups of inhabitants against manipulations in the information space, against hostile messages and disinformation directed against the statehood.

Development of investigative and analytical journalism should be promoted, along with the creation of special media content aimed at exposing and debunking disinformation and manipulation and adapted, available, and appealing to different audiences of Latvia.

**Strong Local Media**

Strong and modern local media and high-quality local content in the Latvian language, and also diversity of media environment facilitate the provision of information necessary for inhabitants in order to make informed and fact-based decisions. Media environment is transforming, therefore it is important to promote competitiveness of all media, while preserving the diversity of regional media.

A unified and modern public media outlet should be established in Latvia, ensuring independent, adequate, and predictable funding.

As the global media service providers enter Latvia, the competition keeps increasing, and the use of traditional media platforms decreases, therefore media and their employees should continue to improve their skills and knowledge, including in the fields of media literacy, content creation, and technologies. Media should also ensure that content is disseminated on platforms corresponding to the modern requirements in order to maintain the audience in the information space of Latvia.

At the same time, understanding should be strengthened that electronic media adhere to ethical standards and responsibility for the disseminated content, regardless of the platform. The legal framework should be improved to ensure that laws the conformity with which is supervised by the National Electronic Mass Media Council in the electronic media environment are also applicable to the digital environment, for example, the conditions for the dissemination of advertising for commercial media or a commercial advertising ban for public media.

Latvian media should continue to be involved in national defence and crisis preparedness measures, including by engaging journalists in civil and military training, and also providing training and other support measures to ensure the continuity of media operations in crisis and threat situations.

**Safety and Skills of Journalists**

Overall, Latvia is a safe country for journalists. According to the 2022 World Press Freedom Index[[1]](#endnote-1) by Reporters Without Borders, Latvia has been ranked 22nd out of 180 countries.

Safety of journalists and media should be promoted both online and in the physical environment against different potential attacks from local and foreign subjects, including persons disseminating disinformation. This includes a crackdown on any case where media freedom and safety are jeopardized, following the zero-tolerance principle.

To enhance journalistic skills, Latvia should invest resources in the promotion of life-long learning of journalists, including in the issues related to content creation. It should be achieved that journalists are able to create reliable high-quality content, recognise false news and disinformation, and also inform the society of the creators and distributors of such content.

**Strong and Unified Strategic Communication of the State**

Work on strengthening and developing strong strategic communication skills within the government centre which works in synergy with strategic and efficient communication with its audiences implemented by State administration and local government institutions should be continued. The aim of such communication is to cultivate patriotism of inhabitants and their sense of belonging to the State of Latvia and its values, trust in State administration institutions, civic engagement in democratic processes and national development, and also knowledge, skills, and willingness to defend the State in crisis or threat situations. The State administration should continue to work uniformly and purposefully with priority target audiences, in particular youth and inhabitants in regions (particularly in border area municipalities of Latgale and Vidzeme).

**8. Prevention of Cyber Threats**

Following Russia’s full-scale invasion of Ukraine, a heightened activity of cyber actors supporting Russia and its actions was observed in the cyberspace of the countries supporting Ukraine, including Latvia. In 2022, Latvia’s cyberspace experienced the highest number of cyber incidents since such statistics have been recorded. Denial of service attacks carried out by the hactivist group KillNet were the most visible to the society, however, their overall impact on the operation of information systems can be regarded as insignificant. The most significant cyber operations that pose the greatest threat to national security continue to be those conducted by actors from different countries against critical infrastructure systems of Latvia’s public and private sectors and information technologies.

Moreover, the number of cyber attacks conducted from the territory of China increases in Latvia and other EU Member States. These attacks target State and local government authorities, critical infrastructure of information technologies, and also private sector companies and public representatives. In 2021, the EU called on China to prevent the use of its territory for malicious cyber activities, and also in 2023, information compiled by the EU Member States on performers of malicious activities whose operations are linked to China was published.

The EU, together with like-minded countries, expresses its support for the application of the existing international law and norms in cyberspace and the responsible behaviour of countries within it. Latvia cooperates within the EU and NATO formats to resolve the issues related to the attribution of cyber incidents.

The new Cybersecurity Strategy of Latvia 2023–2026 approved identifies the goal of the cybersecurity policy for the abovementioned period. This goal provides for the strengthening of security of the cyber space of Latvia by developing cyber defence capabilities, increasing resilience against cyber attacks, and promoting public understanding of threats in the cyber space, defining the following priorities: defence, deterrence, and development. The new Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 has come into force, providing for the implementation of measures to achieve a high common level of cybersecurity in all EU Member States. Latvia should introduce this Directive by 17 October 2025. The Directive imposes stricter cybersecurity requirements for subjects – providers of important and essential services, and also significantly expands the range of subjects to be supervised. A draft law“ National Cybersecurity Law” has been developed for the transposition of the provisions of the Directive, and it is intended that it will replace the existing Law on the Security of Information Technologies.

At the same time, work is ongoing on the development of Cabinet regulations subordinate to the National Cybersecurity Law, including laying down the minimum cybersecurity requirements for subjects, and also providing for changes in the national cybersecurity governance model. With the coming into force of the National Cybersecurity Law, it is intended to establish a new authority – the National Cybersecurity Centre the functions of which will be performed by the Ministry of Defence in cooperation with the Information Technology Security Incident Response Institution (CERT.LV).

Similarly to other fields, information systems play an increasingly significant role in the electoral process and tallying of results. These information systems can potentially become a target of various cyber actors to make the electoral process and tallying of results cumbersome, and also to influence the election results. Therefore, the security of these systems is a prerequisite for not questioning the legitimacy of recent elections. Taking into account the cyclical nature of elections, the information systems used in the electoral process and tallying of results should be developed and updated in a timely manner to ensure their security.

The human resource capacity in the field of cybersecurity is already facing many challenges. Shortage of appropriately educated human resources creates limitations and obstacles for maintaining and improving security of the cyber space of Latvia, and also poses threats to national security. These challenges should be viewed comprehensively, starting from the acquisition of exact sciences in schools and ending with incentives for the prospective students to choose information technology and cybersecurity study programmes.

All participants in the cyber space of Latvia, in particular State administration institutions, State and local government capital companies, owners and lawful possessors of critical infrastructure of information technologies, and also private sector companies providing services to the abovementioned authorities, should critically assess their cybersecurity practice. As the cyber threat environment changes and develops, cybersecurity activities should change with it.

**Priorities for the Prevention of Cyber Threats:**

**Threat Identification**

The State administration institutions responsible for cybersecurity should conduct a thorough and systematic analysis of cyber operations carried out by Russia against Ukraine and its allies by including conclusions and necessary recommendations in policy planning documents, laws and regulations, and training scenarios. As regards the field of threat identification, the State administration institutions responsible for security of cyber space should closely cooperate within the framework of NATO members, EU Member States, and other partner countries, since the scale of cyber attacks often exceeds borders of one country; moreover, it is important to exchange experience with foreign partners on cybersecurity issues.

State and local government authorities and capital companies, and also owners and lawful possessors of critical infrastructure of information technologies should strengthen the supervision of the critical infrastructure of information technologies, including regularly organising threat identification (threat hunt) operations.

With the development of artificial intelligence and machine learning technologies, it is necessary to assess their impact on the society and national security in order to identify, in a timely manner, security risks which can arise if these technologies are developed and used in a targeted manner to attack interests of national security.

**Efficient Implementation of the Cybersecurity Policy**

Work on the improvement of laws and regulations should be continued to introduce a cybersecurity management model which clearly specifies the distribution of rights and tasks of the authorities involved, concurrently developing a comprehensive cybersecurity management solution.

Information systems used in elections should be established and constantly maintained and developed, concurrently strengthening the information technology capacity of the Central Election Commission.

Knowledge in the field of cybersecurity should be strengthened and both full use of existing technologies and introduction of new technologies should be promoted to increase the overall cybersecurity level. Preparation of new cybersecurity specialists and constant improvement of knowledge of the existing specialists should be encouraged.

**Improvement of Cybersecurity and Digital Solutions**

Development of digital skills is relevant to the strengthening of cybersecurity. It is important to promote public awareness of cybersecurity. It is necessary to promote the capabilities of enterprises, in particular small- and medium-sized enterprises in Latvia, in the introduction, improvement, and cyber defence of digital technologies, thus making the processes of companies more effective and developing, and protecting them. It is essential to facilitate the transformation of cybersecurity of small- and medium-sized enterprises, including providing practical support to enterprises for the development and introduction of innovative cybersecurity solutions, offering grant support for this purpose within the framework of the EU’s “Digital Europe”.

State administration institutions responsible for the security of cyber space should continue the development and offering of training processes to entrepreneurs on digital solutions and cyber defence, including free courses. To enhance the availability of training for enterprises, sectoral associations should also be involved in the training process, thus creating a more targeted training and improvement process and providing solutions for specific problem situations. It is very important to strengthen cybersecurity and integrity of digital solutions not only among enterprises but also State and local government authorities, thus improving decision-making in various crisis situations. Cooperation and exchange of information between public and private sectors should be strengthened within the framework of the cybersecurity competence community established under the European Cybersecurity Competence Centre.

**Development of the Cybersecurity Infrastructure**

Work on the establishment, maintenance, and development of the national unified Internet exchange point (hereinafter – GLV-IX) should be continued, imposing an obligation on State and local government authorities, capital companies, owners and lawful possessors of critical infrastructure of information technology to prioritise directing their data flow through GLV-IX. It is equally important to systematically create and update data backup copies, regularly testing recovery capabilities of systems, and also to further develop data embassies abroad. Additionally, it is necessary to maintain and develop solutions against denial of service attacks.

**Strengthening of Cyber Resilience of the State Information Systems Located in the State Electronic Communications Service Centre**

It is necessary to consolidate and automate the technologies in the State Electronic Communications Service Centre (hereinafter – the Centre) and, if necessary, to acquire additional technologies and to increase human resource capacity in order to establish a unified Cybersecurity Management Centre platform with 24/7 support which will ensure services of managed, integrated prevention, and analysis of cybersecurity incidents and incident management services for the systems located in the Centre.

At the same time, in developing the Centre in accordance with the Law on the Security of Information Technologies, it is taken into account that services of observation and analysis of cybersecurity incidents and incident management services are ensured by the information technologies security incidents response institutions.

It is also necessary to create a cyber polygon simulation and training platform which would ensure improvement of qualification of personnel for the holders of the information systems located in the Centre, and also provide an opportunity to test cyber attacks and cyber defence tactics, test the implemented defence policy of cyber security solutions, test the cyber resilience capabilities of applications, and also test vulnerability. Such a training platform would ensure users of the Centre with tools for proactive prevention of cybersecurity incidents.

**Development of an Innovative, Secure Electronic Communications Transmission Environment**

Taking into account the rapid development of quantum computing capabilities, the existing information security tools that are used for the protection of information stored in information systems and transmitted over electronic communication networks will no longer be sufficient in the future. Therefore, it is already necessary to develop quantum-based information security solutions in the existing electronic communications infrastructures to protect data relevant to national security and critical infrastructure, ensuring additional security.

It is necessary to establish a national-level experimental quantum communication system and network, integrating it into the existing electronic communications networks, and to test the operation of quantum communication technologies, and also to use the established network for the development and testing in the fields of importance to the society and national security (defence, health, finance, and communications, 5G, etc.).

**Implementation of Internet Protocol Version 6 (IPv6) in State Administration**

Taking into account the rapid development of the Internet and upon increased volume of data services, the number of addresses in the existing Internet Protocol version IPv4 has become insufficient. For example, today, one IPv4 address is used by up to 100 users in Latvia. This means that law enforcement and other responsible authorities find it significantly difficult to identify users of the relevant IT resources when necessary which is necessary both for investigation of cybercrimes and national security issues in order to promptly initiate threat prevention.

It should be taken into account that the implementation of 5G will develop services such as autonomous driving, industrial automation, smart health care, and the Internet of Things which will only increase the importance of secure Internet environment and the need to strengthen its security. One of the tools to achieve this is individual website addresses. This means that, following the implementation of IPv6, it will be possible to assign an individual address to each user, and each user will be easily identifiable in conformity with the requirements of laws and regulations. Thus, the society will be signalled in a timely manner that the widely held belief in anonymity on the Internet is a myth, and everyone is responsible also for his or her activities in the digital environment. Taking into account the abovementioned facts, the implementation of IPv6 will improve not only the culture of using the digital environment but also the overall protection of State interests, mainly in preventing threats in the information space.

**9. Prevention of Threat Caused to the Economy of Latvia**

The full-scale war initiated by Russia against Ukraine has posed significant challenges to economic security of Latvia, impacting many important sectors of national economy.

As a result of these events, irreversible changes have taken place in the electricity market of Latvia, with significant increase in the price of natural gas promoting the use of renewable energy sources in electricity generation, thus strengthening energy independence and security of Latvia. In the long term, energy security will be ensured by an independent energy system based on the use of renewable energy sources in energy generation, and also sufficient capacity interconnections with energy systems of other countries. Since natural gas supplies from Russia have been discontinued, it is important to ensure both the sufficiency and continuity of its supplies and the lowest possible price, taking into account that the price of electricity is also closely related to the price of natural gas. The main priority of Latvia in the field of security of natural gas supply is further integration of natural gas markets of the Baltic States and Finland and the implementation of the measures specified in the Baltic Energy Market Interconnection Plan, ensuring successful functioning of the natural gas market.

Since the full-scale military invasion of Ukraine initiated by Russia, the EU has imposed extensive individual and economic sanctions against Russia and Belarus. The aim of the sanctions is to weaken Russia’s economic base by denying it access to critically important technologies and markets. In the context of sanctions, the question of stricter control over the sanction regime becomes more relevant to prevent violation and circumvention of the sanctions. Special attention should be paid to the possible violations of sectoral sanctions, including by developing cooperation in logistics and other fields with Central Asian and other countries that have not joined the EU-imposed sanctions against Russia and Belarus. Based on the abovementioned facts, it is necessary to continue strengthening of cooperation between the State authorities responsible for the compliance with the sanction regime, and also the responsible authorities of other EU Member States in order to prevent violation and circumvention of the sanctions and to ensure that the prohibitions imposed by the EU are complied with.

The full-scale military invasion of Ukraine initiated by Russia and the international sanctions against Russia and Belarus have had a significant impact on the operation and further development of the transport and logistics sector of Latvia. The sector is adapting to the new geopolitical reality and seeking opportunities to establish alternative logistics chains for freight traffic and is more actively attracting freight from new target markets – Central Asia, other Asian countries, and Africa. This freight flow, however, does not yet replace the previous volumes of transit freight. Therefore, uncertainty and risks persist in the sector. Russia has various instruments at its disposal to negatively affect the transit freight flow in the East-West corridor towards the ports of Latvia, both from Central Asian countries and China, and other Asian countries.

**Priorities for the Prevention of Threat Caused to Economy:**

**Increasing of Electricity Generation Capacities from Renewable Energy Sources**

A key objective in strengthening security of electricity supply is to increase electricity generation capacities by using renewable energy sources. To achieve this objective, it is essential to implement ELWIND, a joint offshore wind power plant project between Latvia and Estonia, which envisages construction of two wind power plant farms in the marine area of Latvia and Estonia. This project should be completed by 2030.

Overall, five wind power plant farms could be established in the marine area of Latvia in the future. This means that offshore wind energy will make a significant contribution to electricity balance of Latvia in the long term. For the purpose of achieving the objective of energy independence and security, it is planned to not only develop offshore wind energy generation but also to increase the installed capacities of onshore wind-power generators, and also solar photovoltaic capacities as result of projects implemented by both State capital companies and private merchants.

The abovementioned capacities of renewable energy sources potentially available in the future exceed electricity consumption in Latvia several times, therefore it is important to develop the electricity transmission and distribution system along with the development and increase of electricity generation capacity.

**Synchronisation of Electricity Grids of the Baltic States with the European Electricity Grids**

Historically, the electricity systems of the Baltic States have operated synchronously with the systems of Russia and Belarus in accordance with the contracts entered into between the countries within the BRELL[[2]](#endnote-2)Ring, therefore their secure operation depends on the decisions taken outside the EU which can be regarded as a threat to secure electricity supply. To eliminate these risks, a project for synchronising electricity systems of the Baltic States with the continental European grids is being implemented with the support of the EU. According to the declaration of the electricity transmission system operators of the Baltic States dated 1 August 2023 which identifies the major technical, organisational, and legal measures to ensure accelerated synchronisation, and the declaration of prime ministers of the Baltic States supporting it, the synchronisation of electricity grids of the Baltic States with the continental European grids will be implemented not later than in February 2025.

**Strengthening of Security of Natural Gas Supply**

The State has envisaged several significant projects for the development of the natural gas infrastructure in the field of security of natural gas supply. One of them refers to the modernisation of the Inčukalns underground gas storage facility which is planned to be completed by 2025. This modernisation will lead to natural gas being extracted from the storage facility with compression, reducing the dependency between the capacity available for extraction and the natural gas reserves in the storage facility. This will significantly improve safety of natural gas supply as well as efficiency of operation of the storage facility.

Another important line of development is the improvement of gas pipeline interconnections between the Baltic States. Improvement of the Latvia-Lithuania interconnection will enable to ensure greater exchange of the quantity of natural gas between Latvia and Lithuania, and also guarantee sufficient capacity of the Latvian transmission system for ensuring natural gas flows in the unified natural gas market of Finland, Estonia, and Latvia.

Similarly, the project for the improvement of the Estonia-Latvia interconnection will enable to organise natural gas supplies from Estonia to Latvia and increase the volume of natural gas flow from Latvia to Estonia, increasing the effectiveness of natural gas flows in the natural gas market of Finland and Baltic States, and also ensuring better access for system users to the Inčukalns underground gas storage facility. Estonia and Latvia are planning to jointly use the natural gas infrastructure built at the Paldiski Port in Estonia. Both countries will lay down the procedures for jointly chartering the floating storage and re-gasification equipment and managing berth facilities and onshore natural gas infrastructure at Paldiski Port in case of any disruptions in the natural gas supply, including during energy crisis.

**Accession to the International Energy Agency**

Taking into account the increasing global interdependence in the energy sector, Latvia’s accession to and participation in the International Energy Agency (IEA) are important for national security interests since the IEA also operates as an organisation coordinating response measures in emergency situations. As an IEA member, Latvia will be able to receive security of energy resources within the scope of the joint collective security mechanism.

**Strengthening the Continuity of Activities of National Economy**

The level of preparedness of critical infrastructure, objects of importance to national economy, and companies for different type of crises varies. It is necessary to enhance knowledge of entrepreneurs of how to plan continuity of operations, identify critical services, evaluate the need for generation of alternative electricity capacities, and other essential information. A possibility of creating State aid measures to strengthen security – cybersecurity, conducting of a security audit, acquisition of generators, and other measures related to the continuity of operations should be considered.

**Emergency Stock of Petroleum Products**

To strengthen fuel sufficiency in a crisis situation, the reform initiated in the system for the emergency stock of petroleum products should be continued, envisaging that 100% of the emergency stock of petroleum products of the State will be stored in the territory of Latvia by 2025, and also transition to an agency model will be performed and the emergency stock of petroleum products of the State is acquired as State property within five years.

**Reduction of the Dependency on Goods and Services from Russia and Belarus**

A significant influence of goods and raw materials from Russia and Belarus had formed in specific sectors or sectoral companies prior to the full-scale war initiated by Russia in Ukraine. As a result of imposed sanctions on goods and services from Russia and Belarus, companies had to reorient and diversify their supply chains which led to a significant temporary increase in price of specific goods and services.

Companies should continue to seek new supply routes, thus reducing dependency on goods and raw materials from Russia and Belarus. Companies should also continue to develop diversification of suppliers and promote production of goods and services in Latvia, in particular the goods and services necessary for meeting the basic needs of inhabitants.

**Provision of Competitiveness of the Transit Sector**

In the future, the transit sector should consider the risks that the customary transit freight flows could be completely halted, therefore it is necessary to continue the development of alternative logistics chains that bypass Russia and Belarus in order to diversify risks.

The major ports in Latvia, the Riga International Airport, operators of freight transport by rail, and companies involved in the transport and logistics sector should continue to attract freight from new target markets entering Latvia by sea, air, and alternative land corridors in the North–South direction. Development of industrialisation should be continued in ports, including by attracting foreign investments to create the necessary freight base. The use of the existing infrastructure and free capacity to service freights should be continued in order to consolidate, handle, and further distribute freights both in the Baltic Sea Region and globally. Work on attracting high-value-added containerised freights in ports and railway should be continued. It will be crucially important for further development of the transport and logistics sector of Latvia to implement the Rail Baltica project which will open up opportunities for attracting new freight flows in the North–South direction, including providing opportunities for attracting freights from Central and Western Europe, Ukraine, the Black Sea, and the Aegean Sea regions. The Ministry of Transport, in cooperation with entrepreneurs in the transport and logistics sector, should work on the development of multimodal transport operations in Latvia, planning to use the Rail Baltica project, including for better connectivity with the major ports in Latvia, Riga Airport, and also other logistics and industrial centres.

**10. Prevention of Threat Caused by International Terrorism**

International terrorism still is one of the main threats to the security of Europe and other countries of the world. In several regions around the world, security risks are posed by Daesh and Al-Qaeda terrorist groups as well as other militant groups related to them. The presence of Daesh and Al-Qaeda fighters can still be observed in the Middle East, Afghanistan, and regions of Africa. In countries where armed conflicts are ongoing (Syria, Iraq, Afghanistan, Myanmar, Yemen, Egypt, Libya, Nigeria, Somalia, Burkina Faso, Sudan, and Mali), Islamist terrorists control specific territories, plan attacks, train fighters, hide leaders, and carry out illegal activities to obtain financing for their operations.

As a result of offensive carried out by the international coalition, at the beginning of 2019, Daesh lost control over the territories which it had temporarily seized in Syria and Iraq. Moreover, during the counterterrorism operations conducted by the armed forces of the Western countries, several Daesh and Al-Qaeda leaders were eliminated which significantly reduced the capacity of the groups. In the near future, terrorists will continue to restore combat capabilities of their groups and focus their attention on releasing the captured fighters. Also after losses in the Middle East, Islamist terrorists maintain control over Afghanistan and several regions in Africa.

Terrorists continue to use political and socio-economic crises in these regions to recruit new fighters and engage in planning attacks against the armed forces of local governments and objects of interest of the Western countries. Persons who have received military training in these conflict regions can use migration flow to enter Europe, and also to use the knowledge and combat experience gained in the conflict zone to plan attacks in the European countries.

The analysis of terrorist attacks that had occurred in the European countries in the time period from 2019 to 2023 attests that the terrorists are primarily targeting civil inhabitants at mass gathering objects, officials of law enforcement authorities, and also symbolic targets of attacks. Long-term terrorism development trends indicate that the persons and objects which are considered by the radical Islamists as blasphemers of Islam religion are still targets of an attack by Islamist terrorists.

Since 2019, activities of the right-wing extremists have significantly increased in Europe as the extremists increasingly engage in attacks against various European minority groups and left-wing politicians. The analysis of attacks shows that sharp-edged objects and firearms will continue to be some of the main instruments used by terrorists. However, terrorists also continue to study various explosives and toxic substances, and also can acquire modern technologies and tactics used in military conflicts to adapt and use them for terrorist acts.

No active terrorist organisations or groups of persons planning terrorist acts to achieve their ideological goals have been identified in Latvia. At the same time, individuals have been identified in Latvia who have expressed signs of radicalisation, including an interest in propaganda distributed by terrorist groups on the Internet.

Crises of different scale and global events can cause socio-economic tension in the country which in turn promotes activity of various social groups and overall increase in aggression within the society. Disinformation and conspiracy theories disseminated over the Internet also contribute to inhabitants turning to various political, including radical, ideologies. Although the spread of radical ideologies has not been observed in Latvia so far, the different experience in other European countries does not allow for significant reduction of the possibility of such threats.

While the level of terrorism threats in Latvia remains consistently low, terrorism is one of the most serious threats to international security. Moreover, consequences have a domino effect – terrorism in one European country directly affects security in other countries. Our security depends on the security of other European countries since processes ongoing in Europe also affect Latvia’s security and society. The consequences of terrorism can also affect the capabilities of the allies to participate in ensuring Latvia’s defence.

Therefore, it is in the interests of national security of Latvia to contribute to the fight against international terrorism in order to prevent increase in terrorism threats in NATO and the EU Member States. International cooperation which is one of the main elements of the preventive measures of counterterrorism has a significant role in the prevention of threat caused by terrorism. NATO and EU cooperation in the field of counterterrorism should be complementary and coordinated. At the national level, it is necessary to continue improvement of the existing counterterrorism system in order to ensure timely prevention of terrorism threats.

**Priorities for the Prevention of Threat Caused by International Terrorism:**

**Participation in International Operations for Combating Terrorism and Implementation of International Cooperation**

Combating terrorism in various regions around the world is one of the key national security interests of Latvia. There are currently several terrorist groups operating primarily in Africa and Asia. Fighters are trained and terrorist attacks are planned against NATO and the EU Member States in the regions under control of extremists. Therefore, Latvia, together with the forces of other NATO and the EU Member States, should participate in international peace keeping missions in order to support other countries and to enhance capabilities of security forces to control the security situation in their territory, concurrently preventing the dissemination of extremist ideas and terrorism trends outside the terrorism risk regions.

International cooperation is one of the key elements of security measures, playing a crucial role in the prevention of the threat posed by terrorist organisations. In the field of planning the counterterrorism policy, Latvia should take active part in and contribute to the activities implemented by NATO and the EU in order to reduce and prevent, in a timely manner, the terrorism threats which are directed against NATO and the EU Member States and their inhabitants. Concurrently, the State intelligence and security services should continue the development and improvement of exchange of information with the intelligence and security services of the partner states.

**Strengthening of Cooperation of the State and Local Government Authorities in the Field of Counterterrorism**

It is necessary for the authorities involved in the national counterterrorism system, including State security institutions, to ensure efficient cooperation and regular exchange of information on the identified risks and threats.

As the main authority coordinating counterterrorism measures, the State Security Service should ensure that the existing national-level counterterrorism plans and procedures are reviewed and updated according to the security situation in the region. Closer cooperation with the authorities involved in the counterterrorism system should be developed within the scope of preventive counterterrorism measures, integrating resources of the authorities more closely, including in the regions, and also promoting understanding of the national counterterrorism system, actions in case of a terrorism threat, and mutual cooperation in the elimination of the consequences of terrorist incidents.

The authorities involved in the counterterrorism system should enhance their readiness and response capabilities within the scope of counterterrorism response measures, reviewing plans and procedures of the authorities, available material, technical, and personnel resources, and also organising training for personnel of the authorities.

**Prevention of Radicalisation**

Adoption of ideologies justifying violence and dissemination of extremist propaganda are some of the main risks of potential radicalisation of the inhabitants of Latvia. Radicalisation can affect representatives of different social groups, regardless of their sex, age, ethnic origin, or professional occupation. Thus, the identification of the persons subject to the risk of radicalisation and the prevention of the threats caused thereby are a significant factor for the mitigation of terrorism threats. Therefore, the State and local government authorities involved in the prevention of terrorism should, within the scope of their competence, take measures to identify the early signs of radicalisation and to prevent its further development.

Restricting the availability of terrorist content on the Internet is an important measure for reducing the radicalisation risks. Terrorists continue to use digital technologies for mutual communication and dissemination of terrorist propaganda. To counter this, the responsible authorities should promote cooperation with Internet service providers and foster mutual understanding of radicalisation threats, and also exchange of information on the identification of content supporting terrorism.

**Increase of Security of Terrorism Risk Objects**

The State security institutions should continue to take measures for increasing the level of physical security of terrorism risk objects (critical infrastructure objects and mass gathering objects of people). It is also necessary to ensure regular review of the aggregate of critical infrastructure and improvement of security measures for critical infrastructure objects according to existing terrorism threat trends in Europe and the region.

Taking into account the increasing threat posed by Russia in the region, the protection, continuity of operation, and resilience capabilities of critical infrastructure objects should be improved, ensuring the coordination of the development of documents governing security measures in critical infrastructure objects, including continuity of operation and resilience measures, the training of personnel, and the control of the efficiency of security measures.

**Prevention of the Terrorism Financing**

The authorities supervising, controlling, and investigating the financial sector should continue to take measures for the prevention of the possibility of using the financial and non-financial sectors for terrorism financing. A risk-based approach should be ensured, envisaging the implementation of preventive, monitoring, and control measures according to the risk level. It is necessary for the abovementioned authorities to strengthen their capabilities of combating terrorism financing and reduce its overall risks, ensuring compliance with the international obligations and standards in the field of the prevention of terrorism financing.

1. https://rsf.org/en/country/latvia [↑](#endnote-ref-1)
2. Agreement on mutual synchronization of the operation of electricity grids of Belarus, Russia, Estonia, Latvia, and Lithuania. [↑](#endnote-ref-2)