

ASSESSMENT OF THREATS TO NATIONAL SECURITY



SECOND INVESTIGATION DEPARTMENT UNDER THE MINISTRY
OF NATIONAL DEFENCE OF THE REPUBLIC OF LITHUANIA



SECOND INVESTIGATION DEPARTMENT
UNDER THE MINISTRY OF NATIONAL DEFENCE
OF THE REPUBLIC OF LITHUANIA

ASSESSMENT OF THREATS TO NATIONAL SECURITY

Vilnius, 2015

UDK 355(474.5)
As48

Editor Donatas Eidintas
Graphic designer Aida Janonytė

04.06.2015. Circulation: 350 units. Order GL-227
Layout by the Publishing Section of the General
Affairs Department of the Ministry of National
Defence, Totorių str. 25, LT-01121 Vilnius.

Printed by the Military Cartography Centre
of the Lithuanian Armed Forces, Muitinės str.,
Domeikava, LT-54359 Kaunas District.
www.kam.lt

ISBN 978-609-412-080-0

© Lietuvos Respublikos
krašto apsaugos ministerija

CONTENTS

INTRODUCTION	7
REGIONAL SECURITY	9
Russia	9
Belarus	22
CIS, Ukraine and Georgia	24
HOSTILE INTELLIGENCE ACTIVITIES	26
Activities of Russia's intelligence and security services	26
Activities of intelligence and security services of Belarus	31
CYBER THREATS	32
Cyber security	32
Cyber espionage	33
Threats to mobile device users	35
INFORMATION THREATS	36
CRISIS REGIONS	38
Afghanistan	38
Middle East and North Africa	38
Conflict regions in Central Africa	40
Annex	41



The assessment of threats to national security is provided to the public in accordance with the provisions laid down in Articles 8 and 26 of the Law of the Republic of Lithuania on Intelligence. The present document provides unclassified assessment of defence, military-political, military-economic, military-technological and military-information external threats and risks to national security of the Republic of Lithuania.

INTRODUCTION

Currently, the probability of a conventional warfare in the closest geopolitical environment of Lithuania (the Baltic Sea region) remains relatively low. However, certain tendencies and actions of external actors affect the security situation of Lithuania very negatively.

The Russian leadership has not changed its principled position that the area of the former USSR belongs to the sphere of influence of Russia. A growing tension in relations with the West was accompanied by Russia's increasing efforts to exert its influence on the neighbouring states. Its annexation of Crimea and actions in Eastern Ukraine revealed that Russia is ready to violate international treaties and obligations as well as fundamental principles of international law. Moreover, the events of 2014 made it clear that the leadership and society of Russia are determined to accept particularly high costs of their actions.

The use of Russia's military force in Ukraine, a constant demonstration of the military strength and disregard of international agreements have remarkably enhanced significance of the military force for the overall security situation in Eastern Europe and any country in the region. From now on, use of military force in the region is not merely theoretical or possible only in a very distant future. That radically changes the security environment of the states in the proximity to Russia, and the assumptions of their defence planning.

Russia still remains incapable to initiate a military conflict against NATO. This fact enhances security of the member states of the Alliance, and significantly diminishes a probability of a conventional military conflict in the Baltic Sea region. However, Russia takes intensive steps to develop its military capabilities and attempts to create forces capable of fighting any adversary. Furthermore, the so-called "hybrid strategy" of Russia envisaging the use of unconventional or hidden military measures is dangerous even to NATO members in the region. It cannot be ruled out that Russia may attempt to apply such measures against one of the members of the Alliance, hoping that NATO would be unable to respond timely and adequately due to different national interests of the member states and a complicated decision-making mechanism.

An additional factor affecting the security situation of Lithuania is its location at the eastern frontier of NATO with Russia. Friction between Russia and the West heightens tension in the geopolitical environment of Lithuania, as Russia takes actions in the Baltic Sea region intended to exert

pressure not only (and not so much) on the countries in that region but also on NATO. It became increasingly clear in 2014, when a greater military activity of the Alliance in the region received a more intense military power demonstration from Russia.

Russia has been consistently increasing financing of its Armed Forces and military activity in the Western Strategic Direction. An aggravating economic situation of Russia will force it to review its financing and military enhancement programmes, but – in the assessment of the Second Investigation Department under the Ministry of the National Defence (Lith. *AOTD*) – it will not alter Russia's overall tendency of the growth of its military strength and readiness to use it.

The foreign and military policy of Belarus continues to be closely coordinated with Russia and the military integration of those two states is further intensified. The political and economic dependence of Belarus on Russia, and enhancement of their Regional Military Grouping have a negative effect on the security situation of Lithuania.

The situation in the Commonwealth of Independent States (CIS), Ukraine and Georgia remains unstable. In addition to internal concerns (political instability, poor public administration, undiversified and inefficient economy), the key sources for instability are the unsolved issues of separatist regions and "frozen conflicts" as well as continuous and increasingly aggressive attempts of Russia to strengthen its influence.

The national security of Lithuania is also affected by internal or international conflicts and various security crises which (might) take place in geographically more distant regions and due to which international forces are or may be deployed. As Lithuania contributes to the efforts of the international community to handle such conflicts, these become important factors to national security of Lithuania. In addition, developments and events in the unstable regions increasingly influence the level of terrorism threat in Europe. Therefore, in 2014, the AOTD focused on monitoring and analysis of dangerous tendencies in more distant regions such as Afghanistan, the Middle East, and Africa.

REGIONAL SECURITY

Russia

In 2014, the **domestic policy of Russia** continued to be dominated by the tendencies of maintaining and strengthening a closed authoritarian political system. Despite chronic problems in administration and exacerbating economic strains, the political regime of Russia keeps trying to preserve this system, and considers reforms a threat to stability of the governance.

One of the most significant factors securing stability of Russia's political system is a centralised control of political institutions and security agencies, business, media and other most important institutions. The people who dominate in such areas are loyal to Vladimir Putin and depend on the existing political system; they also enable the president to exploit the state resources and manipulate political and social processes. The positions of the ruling regime in regional subjects of the Federation were even more strengthened during the elections of regional authorities in September 2014 which were won by representatives of the United Russia (Russ. *Единая Россия*). The president's influence on military industry, security and other key institutions was amplified by certain changes of the personnel in charge. Authorisations of security services and law enforcement agencies to control the public and private sectors were expanded under a pretext of fighting against terrorism, extremism and the so-called "fifth column".

Despite facing a declining economy, which became more evident in 2014, Russian political and economic elites remain loyal to the president. The state resources are used to support the key business entities backing up the political system, and such mechanism maintains their lack of interest in political and economic reforms. The political leadership of Russia does not regard the recession as a systemic problem of the economy, but rather as a phenomenon with political overtones created by the West. Therefore, the economic model of the country is not changed. Centralisation of



■ Diversity of political information in Russia's media (Source: sprotyv.info)

the economy is being enhanced instead, along with strengthening control mechanisms. All that increases a probability of a long-term economic recession and stagnation. The initiative to replace import with the local produce serves to boost Russia's independence from foreign import and its resilience to economic sanctions, thus ensuring a greater leeway in domestic and foreign policy.

Legitimacy of Russia's leadership is asserted in the public by depicting leaders as irreplaceable, taking care of national and cultural interests. Such view is ensured by a consistent propaganda fostering cultural, political and social values in the public which would be favourable to the political regime. Russia is presented as an alternative to the Western values, and a conservative, anti-Western identity of the Russian nation is being shaped. A threat from the West to conventional moral values and political traditions of the "Russian world" is emphasised. An opinion that the international policy should be based on arguments of geopolitical interests rather than on law and international treaties is being inculcated on the society. An economic downturn (aggravated in 2014) is presented in propaganda as the price the Russian nation pays for defending its state and civilisation from expansion of NATO/the West. An illusion of an external threat created by such means encourages consolidation of the Russian society and its support to the political regime. Russia's aggression against Ukraine received not only approval but also practical support of the public. As an illustration of the most active forms of such support is participation of Russian civilians both in military campaigns against Ukraine, and in dissemination of Russian propaganda abroad.

Russia's political regime and the media intensified efforts to neutralise criticism of the authorities by identifying it as harming the state interests. Such efforts further curbed possibilities of opposition movements (having little weight as it is) to influence political and social processes. No opposition movement is capable of attracting a broader public support. A large group of the people who protested against the ruling regime in late 2011 – first half of 2012 are now fully or partially supporting aggressive actions of Russia against Ukraine. The currently prevailing tendencies (first and



One of the numerous events in support of the actions of Russia's leadership in Ukraine with a symbolic title "Stop the march to the East" (meaning penetration of the West into the post-Soviet space). Ufa, Bashkortostan (Source: www.rusnod.ru)

foremost the spread of chauvinist moods of a great state) are likely to continue. Therefore, even coming into power of individuals with relatively more liberal views would not alter the underlying features of Russia's policy towards neighbouring states.

Problems of economy have not reduced the public support for the regime yet. A worsening economic situation and a potential social tension will prompt the regime to intensify its propaganda in order to divert the public attention from the internal issues to external enemies. It is quite plausible that a more substantial diminishing in support for the regime could be brought only by a long-term recession and a markedly decreased standard of living of a considerable part of the society.

Stability of the political regime, possibilities to control internal political processes, and rising great-state moods in the society enable Russia's leadership to avoid any internal opposition or public control in the event of belligerent (even military) actions. This tendency will further promote an even more aggressive foreign policy of Russia and will have a long-term negative impact on the national security of Lithuania.

The key objectives of **Russia's foreign policy** remain the same: it is sought to restore a status of the great power and secure one of the key roles in international politics. An integral part of such efforts is the aim to establish a division of geopolitical influence spheres by assigning the post-Soviet space to Russia's sphere of influence and recognising that Russia has exclusive interests in neighbouring states. Russia's leadership considered and continues to consider the change of power and geopolitical orientation in Ukraine in early 2014 as a violation of Russia's "vital interests" and penetration of the West – which seeks to weaken Russia – into its sphere of influence. Since Russia views the post-Soviet space as an arena of geopolitical competition and does not recognise the states in this space as proper subjects, the mounting tension in relations with the West in 2014 resulted in intensified efforts of Russia to exert influence on its neighbours. To this end, a complex of political and diplomatic, economic, military measures as well as those related to energy and information is



Leaders of Belarus, Kazakhstan and Russia sign founding treaty on Eurasian Economic Union (Source: 1tv.ru)

applied along with adverse phenomena of social and ethnic tensions, and the potential of a public protest.

The treaty on the Eurasian Economic Union (the EAEU) was signed in May 2014 and came into force on 1 January 2015. Already in 2013 Russia achieved Armenia's decision to abandon closer cooperation with the European Union (the EU) and agree to join the EAEU instead. In 2014, formal arrangements on Armenia's involvement in the EAEU were being finalised. In addition, it was agreed that Kyrgyzstan would also join this union. The integration of separatist regions of Georgia, i.e. Abkhazia and South Ossetia, into Russia was further pursued.

In 2014, the integration of post-Soviet space into formations controlled by Russia encountered serious obstacles. Russia unilaterally declared sanctions to the Western states, thus causing dissatisfaction of its partners (Belarus and Kazakhstan) in the Customs Union and EAEU. The onset of economic recession in Russia and the global oil price slump will become an even greater challenge to integration. Since the primary reason why the post-Soviet countries consent to integrate with Russia is an expected economic benefit and access to cheaper energy resources, it is likely that such integration will seem less attractive. However, it may prompt Russia to heighten its political, economic, informational and even military pressure on the "integration partners".

In 2014, the dual effect of the aggression against Ukraine on Russia's attempts to increase its influence in the post-Soviet space became noticeable. On the one hand, belligerent actions of Russia impel national leaders in that region to avoid overly close bonds with Russia. On the other hand, as Russia blatantly demonstrated in Ukraine, it is ready to resort to extreme measures. From now on, all post-Soviet states will have to take into account a possibility that the military force can be used, and Russia will be able to exploit it to apply pressure on its neighbouring states.

Russia declares having the right to use military force in order to defend its citizens and Russian-speaking population abroad. This position was reiterated in the new wording of Russia's Military Doctrine approved in December 2014. Russia publicly and actively exploits the concept of the "Russian World" (Russ. *Русский мир*) according to which the societies (or at least a part of them) of its neighbouring states can be attributed to a uniform "Russian space", and Russia is their self-proclaimed defender. Such position may be used as a pretext for aggression against its neighbouring states.

NATO seems to Russia as the major obstacle in achieving its strategic goals, i.e. spread of international influence and regional dominance. The updated Military Doctrine of Russia even more openly names NATO as the main source of military threats. The Alliance is accused of attempts to entrust its military potential with global functions. NATO is also accused of expansion, deployment of its military forces and arranging of military trainings close to the territories of Russia or its allies. It is regarded as a pressure on Russia and an attempt to destabilise the established balance of powers. As a military threat, the doctrine lists entrenchment of political powers unfavourable to Russia's interests in the states bordering Russia or its allies, and escalation of an armed conflict in such territories. Based on such position, the changes in the political system of Ukraine in February 2014, and the support of foreign countries to Ukraine are regarded by Russia as a military threat.

Russia's discretion against NATO and individual members of the Alliance is limited as (unlike in its relations with post-Soviet states which are not NATO members) the costs of using its military force may substantially exceed the level of damage acceptable to Russia. As a weaker party to a potential conflict, Russia is searching for the most vulnerable elements of the opponent by means of which Russia attempts to disrupt the enlargement of the Alliance, development of the infrastructure and capabilities potentially dangerous to Russia, also to stimulate faltering and disintegration of NATO.

Following the start of the conflict with Ukraine, and the ensuing reaction of NATO and the EU, in 2014 Russia considerably increased its military activity in the Baltic Sea region and other areas bordering NATO and the EU. In this way Russia wants to demonstrate that such actions of NATO in the Eastern Direction will receive a symmetric or asymmetric response. Accordingly, it is suggested that active involvement of NATO will not create a greater security in the Baltic Sea region, but will prompt an even more accelerated growth of tension. That is Russia's way to convince the "old" members of NATO to abstain from enhancing the readiness to ensure armed defence of the "new" members as it will only provoke Russia, and will only serve to increase geopolitical strain and instability.

Although Russia presents its increased military activity as a response to actions of NATO in the region, in fact Russia itself conducted military planning directed against the Alliance already before 2014, simulated a military conflict with NATO during various military exercises (e.g., Zapad 2013), and took other steps of preparation for a potential conflict. Therefore, it should be assessed that the increased military activity of NATO did not affect Russia's intentions and readiness, but only impelled to demonstrate them in a more open manner. According to the AOTD assessment, due to the heightened tension in relations with the West, Russia would have paraded its military strength in the Western Strategic Direction even if NATO countries had refrained from the enhancement of defence commitments and capabilities in the Baltic Sea region.

Russia seeks to erode the existing Euro-Atlantic security architecture which limits Russia's abilities to act. In 2014, Russia's representatives claimed a number of times that their country could not come to terms with the situation when security or interests of other states were ensured without taking Russia into account. They also stated that the European security should be equal for everyone and undivided. Indivisibility of the security environment perceived in such a peculiar way should mean that any changes in the security architecture of Eastern Europe and other regions close to Russia are possible only upon coordination with Russia.

In addition, Russia's actions in Ukraine, primarily occupation and annexation of Crimea, showed that it was ready to violate international treaties and commitments as well as the fundamental principles of international law, *i.e.* independence and territorial integrity of other states. It should also be noted that by destabilising Eastern Ukraine and sending arms to the separatists (including heavy armoured vehicles, multiple launch rocket systems (MLRS), etc.) Russia is continuously violating not only international law, but also its national legislation.

Development of an alternative project for international security, namely the Collective Security Treaty Organization (the CSTO), is meant to counterbalance NATO. Russia uses the CSTO as an international platform representing its interests and as a tool to spread its influence. Yet it should be pointed out that despite Russia's efforts, the CSTO remains an inefficient organisation. None of the members of the CSTO recognised Abkhazia or Southern Ossetia, nor expressed a strong support of Russia's actions in Ukraine.

The **energy sector** remains one of the principal means to secure Russia's economic and political interests. The changes in energy markets and aspirations for energy independence which diminish Russia's influence are further regarded by Russia as a threat in general, and as a threat to its military security in particular. Energy resources to the ruling regime of Russia constitute the foundations of stability and security, as the budget of Russia is still critically dependent on the revenue from exports of hydrocarbons. In 2014, its oil and natural gas sectors accounted for 51% of the revenue to the federal budget. This dependence has not decreased irrespective of the fallen oil prices, since the decreasing foreign currency income was compensated by the depreciation of the rouble, which ensured acceptable fiscal balance in 2014. The revenue from oil and natural gas enables Russia sustaining its domestic stability and financing the key state projects (including modernisation of its Armed Forces).

The critical dependence of some member states of NATO and the EU on Russian energy resources is regarded by Russia's leadership as one of the main tools for political leverage. The integration processes strengthening the European internal energy market and the processes diversifying energy sources (implementation of the EU Third Energy Package, construction of cross-border power connections, development of market mechanisms and negotiations with alternative suppliers from the Caspian and Mediterranean regions) are perceived as having a major adverse impact on Russia's interests. The infrastructure, financial and legal changes made to the energy system of the



■ Nuclear power plant construction in Astravets (Ostrovets) site continues (Source: www.ostrovets.by)

Baltic Sea region (particularly in Lithuania) are viewed by Russia in a highly sensitive manner due to Kaliningrad region's continuing dependence on the transit of energy resources across the NATO state.

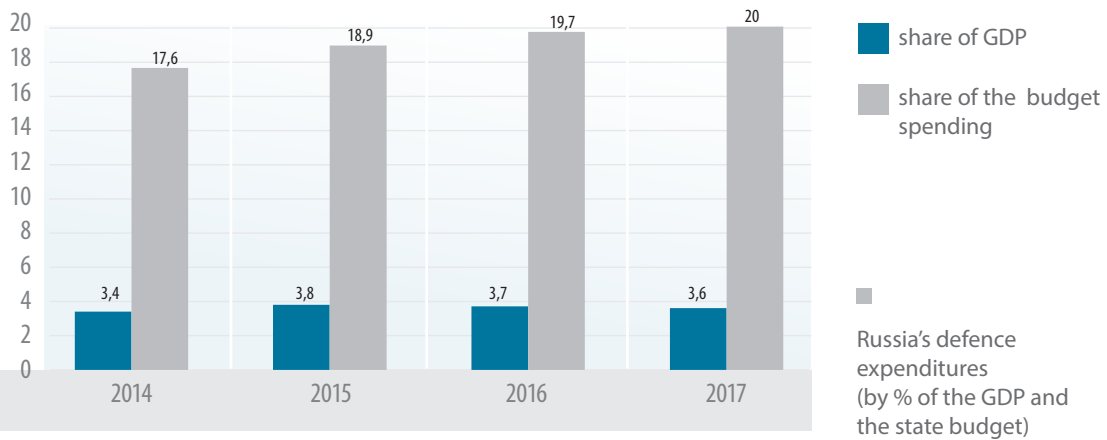
Russia seeks to deter the economically and energy dependent countries from implementing alternative projects and reforms, or at least to slow down such processes considerably. Russia expects to maintain its influence in the European market by dividing the common energy policy of the EU and NATO states. To this end, new long-term agreements are being signed, strategic companies abroad are being acquired, the search for partners preventing implementation of new energy projects for diversification of supply to Europe are being conducted, and active public relations campaigns intended to discredit goals of energy independence of individual states or regions are being exercised.

The projects of nuclear power plants being developed in the Baltic Sea region (in Kaliningrad region and in the Astravets (Ostrovets) site in Belarus) are aimed at jeopardising a creation of an open and competitive energy market (once the cross-border power connections in the Western Direction and with the Scandinavian countries are constructed, national sources of energy-generation are developed, effectively disconnecting from the power-grid of Russia/CIS). After the construction of the nuclear power plant in Kaliningrad region was temporarily suspended in 2013, no major developments in this project occurred in 2014. However, provided favourable political and/or economic circumstances emerge, the project may be resumed. The construction of Russia-funded nuclear power plant of Belarus in Astravets (Ostrovets) site was consistently continued irrespective of the complicated economic situation and relations between the two states. The project is being implemented despite already recorded violations of international conventions in terms of the potential negative impact on the environment and failure to duly consult with representatives of the public both in the country concerned and abroad.

As Lithuania continues implementing national and regional projects of the energy infrastructure (the LNG distribution network, cross-border power connections with Sweden and Poland), the adverse impact of Russia's leverage to the national security of Lithuania is diminishing. In view of Russia, it increases vulnerability of Kaliningrad region dependent on the transit across Lithuania, thus the plans to create an isolated energy system are being further developed.¹ Taking into account that the long-term agreement on natural gas transit across Lithuania is drawing to an end (it expires on 1 January 2016) and Russia is seeking to take a convenient negotiating position, the issues of transit-related threats and "irrational" energy policy of Lithuania will be escalated in the public even more actively.

The trend of increasing financing for **Russia's Armed Forces** continues even with the slowing growth of the national economy (in 2012 the GDP grew by 3.4%, in 2013 it grew by 1.3%, and in 2014 it grew by only 0.6%). The military spending in 2014 constituted 3.4% of the GDP (17.6% of

¹ It is planned to construct new coal- and gas-fired power stations, to expand an underground storage of natural gas, and construct an LNG import terminal.



all budget expenditures), and in 2015 it was planned to increase to as much as 4.2% of the GDP (21.2% of the budget spending). Although the declining economy forced to adjust plans, it is still planned to increase the financing of the Armed Forces consistently, only at a slower rate (see the chart). Moreover, when Russia was cutting budget spending during the recession in 2009–2010, the amount allocated to the Armed Forces was growing. It is likely that the military will be granted the highest possible spending even under the circumstances of the new economic recession, especially taking into account the increasingly aggressive foreign policy and an obviously rising importance of the military strength in pursuing goals of foreign and security policy.

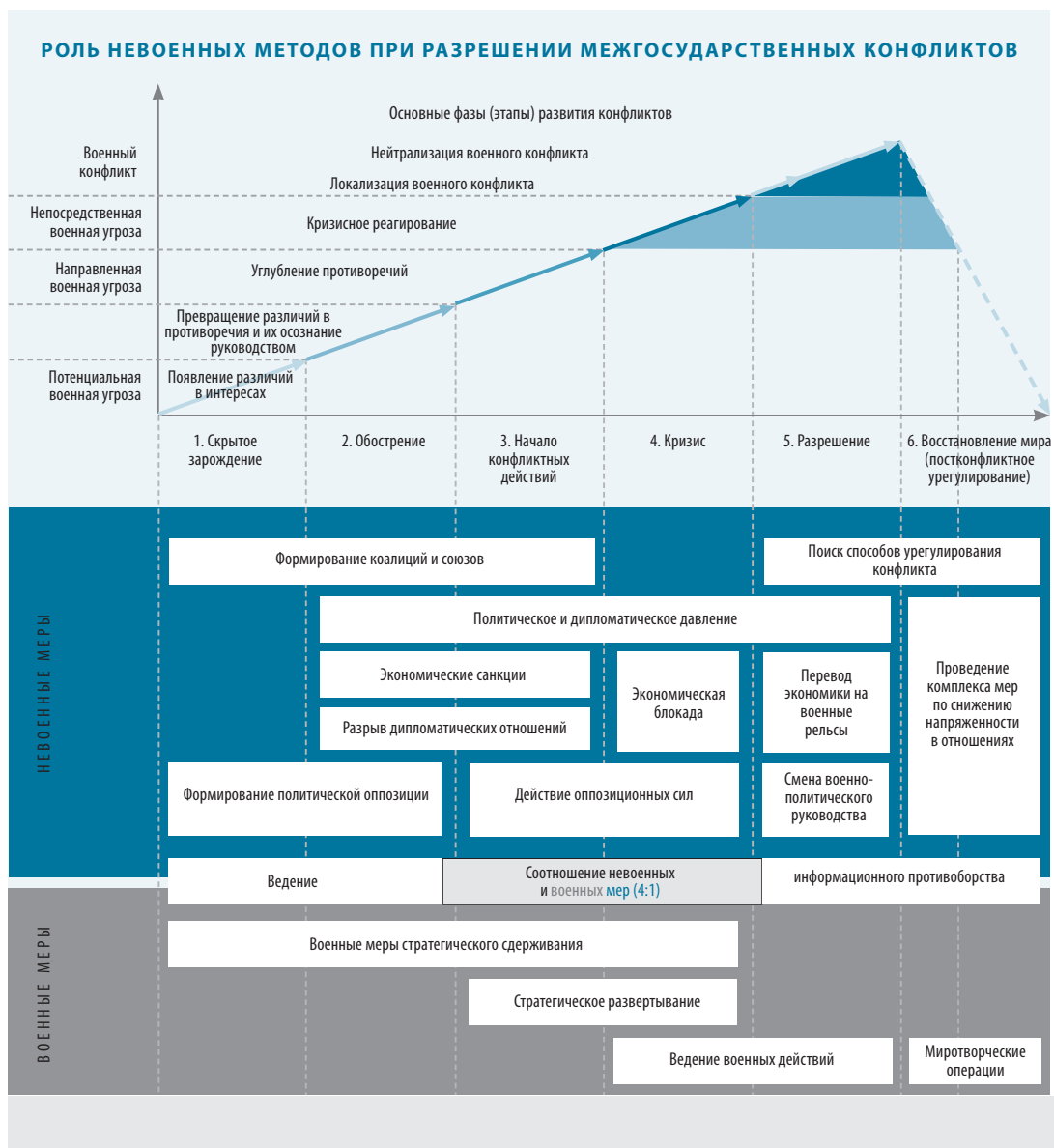
Despite the increasing financing of its Armed Forces, Russia still lags behind NATO with regards to its military and technical capabilities. The potential of the Russian Armed Forces is not sufficient for a large-scale conventional military conflict with NATO. Therefore, the likelihood of Russia's conventional offensive campaign against NATO or individual members of NATO is assessed as low. The strategic nuclear potential continues to be the main deterrent ensuring Russia's global ambitions, interests and military security, and the significance of such potential will not change in the long-term perspective.

Currently, Russia is searching for ways to leverage the advantage of NATO in terms of conventional warfare. Therefore, in the first place Russia is trying to achieve this goal by creating an area (buffer zone) situated close to Russia and controlled by political or military means:

- Regional air space defence systems are intensively developed in the directions where Russia has the common border with members of NATO, or the territories of Russia and NATO states are only separated by natural water barriers (the Baltic and Black Seas). The aim of such systems is to ensure both defence of Russia's territory from air threats and an ability (in the event of a crisis) to destroy targets above neighbouring countries, including members of NATO.
- It is attempted to create a politically controlled buffer zone consisting of neutral pro-Russian states or those controlled by Russia (or such *de facto* political formations as Abkhazia, South Ossetia, Transnistria) in the directions where Russia's territory is separated from NATO by

other countries. It is expected, that in the event of a crisis, NATO would not use the territories of neutral countries without their consent for its military operations against Russia.

Establishment of a controlled zone at the western and southern border of Russia has to assist in forcing NATO/the US to concentrate their forces in the directions more favourable to Russia in the event of a crisis, *i.e.* in such regions where it is more convenient for Russia to launch offensive or defensive operations. Russia envisages several potential main directions for NATO actions which Russia takes into consideration in developing its own capabilities: the Baltic Sea, the Barents Sea,



Present-day conflicts according to Russia's hybrid strategy
(Source: www.vpk-news.ru)

and the Black Sea (the control of the Crimean Peninsula is particularly important in this direction). Therefore, Russia strongly focuses on strengthening the units deployed in Kaliningrad region as well as in the Kola Peninsula and Crimean Peninsula. It is sought that the deployment and development of the capabilities of air, coastal defence and surface-to-surface missile systems in these directions would significantly increase damage to NATO in the event of a potential conflict. Russia expects that the higher probability of NATO losses is, the milder reaction of NATO to aggressive actions of Russia would be. It is anticipated that the potential losses could contribute to deterring some members of NATO from actually carrying out their obligations of collective defence.

According to Russia, the level of cooperation of Ukraine with NATO can pose a threat to form another potential direction of NATO's actions, unless Russia imposes control on Ukraine. In terms of ensuring military security, the aim of actions in Ukraine is to retain a *de facto* control of Ukraine, and maintain it in the buffer zone.

Once the buffer zone is created, it would enable Russia to apply there the so-called hybrid strategy. It provides that Russia may at first employ non-military measures against other countries, e.g. a political and diplomatic pressure, economic sanctions, information campaigns, and demonstration of its military strength. Non-military measures are applied in order to affect and disrupt the opponent's political decision-making processes, also to weaken (destroy) unity of military and political alliances by highlighting disagreements between individual countries. Such measures are already being applied with varying intensity against those countries or their blocs (NATO, the EU) which hinder Russia from implementing its strategic goals.

Should non-military measures fail to generate the expected results, the so-called Gerasimov Doctrine² foresees a "crisis response" during which not only all types of pressure could be enhanced (e.g. an economic blockade could be imposed), but also military actions could be initiated. The military actions are to be launched already before the beginning of military conflict, i.e. unconventional and cover measures would be employed in the opponent's territory. Moreover, it should be noted that the potential of a local protest and the opposition would actively be exploited both while the crisis is mounting and during the crisis. It is expected that while Russia is applying its "crisis response", i.e. officially denying its involvement in a military conflict, yet acting covertly (including military operations), NATO would be unable to respond timely and adequately due to its complicated decision-making mechanism and divergent interests of its members.

Should the crisis escalate into an open military conflict, it is planned to launch unexpected and rapid operations in the territory of adversary, to destroy its critical civil and military infrastructure with the aim of breaking the political or social will to resist. Furthermore, simultaneously information operations and cyber attacks would be applied extensively.

In 2014, some of the elements pertaining to the hybrid strategy were put into practice in Ukraine's Crimea and Donbas region. Russia demonstrated its ability to launch a broad-spectrum operation

² Though widely-known, the title is unofficial. This is how in early 2013 the media dubbed the ideas presented by Valery Gerasimov, a Russian general and the Chief of the General Staff of the Armed Forces of Russia.

combining political, economic, information-related instruments with the use unconventional and covert military measures. However, in order to be able to implement all the elements of the hybrid strategy, the Russian Armed Forces must be capable of launching offensive operations according to the operational plans. The current capabilities of Russia's Armed Forces to launch such campaigns remain limited. Military capabilities are more than sufficient for Russia to solve any conflict with a neighbouring state in the western and southern directions, however, in order to be ready to engage in larger-scale operations against NATO or the United States, Russia needs to modernise its Armed Forces, and that is being in a process.

The larger share of the Russia's Armed Forces financial resources is allocated for its reform and rearmament. No radical changes in the reform process of the Armed Forces occurred in 2014. The previously initiated optimisation of the command and control system was continued. Structural changes of the Armed Forces were determined by the priorities of the national policy, and they were conducted without any major setbacks which could have resulted due to sanctions applied against Russia.

In 2014, the main changes pertaining to the reform of the Russian Armed Forces were noticed in the northern direction. The Northern Joint Strategic Command was established there, and formation of units of the Land Forces is continued. Establishment of the new Command would not result in essential changes in terms of tasks for the units deployed in the north, but it will enable to plan, lead and control operations more efficiently and flexibly. Creation of the Northern Joint Strategic Command reflects the growing focus on the Arctic region which has been continuously declared by Russia in the past few years. Although with the establishment of the new Command, the potential of the Western Military District formally diminished (until 2014 the Western Military District was responsible for this direction), the combat resources intended for the tasks in the Western Strategic Direction are not really decreasing.



■ Loading of military equipment to be transported by aircraft during exercise in Western Military District (Source: www.5-tv.ru)

Although two divisions constituting part of the Western Military District have been restored, it does not imply that the structure of the Armed Forces is being changed radically. A brigade still remains the core unit of Russia's Armed Forces.

The National Defence Command Centre became operational in 2014. The Centre is responsible for implementation of the national defence by coordinating activities of different state institutions. In 2013–2014, reserve commands were established in each military district. Their main objective is to conduct mobilisation during the time of war, and form new military units on the grounds of armament and equipment storage bases. It should be noted that mobilisation and coordination of not only the Armed Forces, but also the resources of the entire country (including civilians) for a military conflict has been one of the main priorities of Russia recently. It is reflected both in the long-term planning and doctrine-related documents (e.g., the new wording of the Military Doctrine) as well as military exercises.

The planned rearmament of the forces and repairs of munitions were continued in 2014. Rearmament of the strategic nuclear triad providing the function of deterrence has remained the top priority. In the area of conventional arms, the underlying tendency was to conduct major repairs of the existing military equipment or their replacement with new and modernised weaponry items of the same type. It enabled Russia to ensure sustaining the combat potential of the Armed Forces and even achieve its moderate growth. According to the plan, the qualitative progress should be reached by the essentially new models of munitions, but a large part of those are currently still being developed or tested. Currently, items of new weaponry are faster delivered to the missile, air space defence, radio electronic combat and communications units. The rearmament of one more missile brigade with short-range ballistic missile system Iskander-M (SS-26 Stone) in the Western Military District has to be highlighted. Each year Russia seeks to rearm two brigades with Iskander-M systems.

The personnel reform rather than financing or rearmament has remained the most challenging since the very beginning of the reform of the Russian Armed Forces. The decisions related to military personnel taken in the course of the reform were ambiguous and conflicting. Nevertheless, already in 2012, a law came into effect under which the salary of the military increased from 1.8 to 3 times irrespective of the position or rank. An ambitious programme for attracting professional soldiers, the so-called contract soldiers, was approved nearly simultaneously. Based on that programme, it was planned to attract about 50,000–55,000 troops to the professional military service each year, which by 2017 would result in 425,000 contract soldiers who would constitute the basis of permanent readiness units. The deteriorating economic situation in 2014 as well as unwillingness of soldiers to conduct missions in the territory of Ukraine slowed down attracting the new contract soldiers and made it difficult to keep the existing ones in the Armed Forces. Implementation of the goals of contract servicemen programme (425,000 professional soldiers) is postponed until 2020.

In 2014, Russia continued conducting unexpected inspection of combat readiness of the Armed Forces (such practice began in 2013) which usually ended in large-scale military exercises. Such inspections enable Russia's leadership to assess the actual readiness of its Armed Forces to carry out tasks as well as show the results of the reform of the Armed Forces which had been underway since 2008. The inspections and snap exercises were also used as a demonstration of its military strength to the neighbouring and Western countries. This was clearly demonstrated by actions taken during the military inspection in Kaliningrad region and the Baltic Sea on 5-11 December 2014. From late February to early March 2014, under the pretext of such unexpected inspection, Russia moved a part of its Armed Forces to the border with Ukraine. The inspections have a negative impact on security of the states situated close to Russia since they enable Russia to redeploy substantial groups of its Armed Forces unexpectedly, and restrict opportunities for the neighbouring countries to assess the scale and aims of such redeployment accurately. Thus, the possibilities for an early warning of a potential military conflict are limited.

In 2014, Russia's military activity in the Baltic Sea region has increased remarkably. In addition to the function of strength demonstration, the carried out exercises had a practical purpose. Intensive exercises allowed improving readiness of its military personnel and interaction between its units. During the combat readiness inspections conducted in 2014, Russia demonstrated its ability to promptly increase the capabilities of military group deployed in Kaliningrad region by temporarily deploying additional resources to the area, including short-range ballistic missile system Iskander-M (SS-26 Stone). A particularly high intensity of the combat training activities raises a probability of unintended or intended incidents involving troops and equipment of the Russian Armed Forces. In addition, a substantial growth in intensity of combat training is shaping a new and much higher level of the routine (permanent) military activity. Such situation limits opportunities of the neighbouring states in the region to assess the nature of Russia's military activity and respond to it adequately.

Russia's Armed Forces actions and its support to the separatists in Eastern Ukraine highlighted several key tendencies:

- Artillery has retained the core and often decisive role in actions of Russia's Armed Forces.
- Armoured vehicles (tanks, infantry fighting vehicles) are still important. Due to massive scale of artillery application the light-armed units without armoured combat vehicles are highly vulnerable and inefficient in operations of any type (offensive, defensive). Light armoured vehicles remain highly exposed to artillery and anti-tank weaponry.
- The significance of modern anti-tank weaponry increases for the defending country since the Russia's Armed Forces are orienting towards actions of armoured units.
- The use of radio electronic warfare highly restricts actions of the forces of Russia's opponent.
- The significance of unmanned aerial vehicles (drones) is growing in the Russia's Armed Forces.

Belarus

The domestic political landscape of Belarus continues to be determined by the cult of personality of Alexander Lukashenka. Imperfect constitutional mechanisms as well as the centralised authority system (based on force institutions) guarantee Lukashenka almost unlimited freedom of action. The political agenda is dominated by the election to be held in 2015. Despite the fact that political opposition parties operate legally, they are weak and unable to coordinate their actions, and have minimal influence in political arena of the country. As a result of its limited influence and the steps taken by the authorities, the opposition does not have any chances to be more successful during the presidential elections.

A dramatically depreciated Russian rouble along with the rigid and politically motivated monetary policy of Belarus became another reason of devaluation of one more national currency in late 2014. Although the country's governance based on plan principles has incurred the third financial crisis since 2008, the so-called socially oriented market economy model was not abandoned. The last recession once more revealed the economic dependence of Belarus on Russia.

The events in Ukraine are used to justify the existing political structure and to shape an image of the sole national leader. It is attempted to shield economic and social problems by escalating the security (stability) issue. The dramatic Maidan events served as an excuse for amending (tightening) legislation governing the declaration of the state of war, and regulating activities of the media. Such setting has largely influenced the fact that the majority of the society still does not take up a distinct anti-government stance.

Russia remains the main strategic partner of Belarus. Belarus joined Russia's promoted EAEU treaty. In addition to the political support for Lukashenka, the establishment of the EAEU provides Bela-



■ Russia's jet-fighter Su-27 on descent in Baranovichi, Belarus (Source: rusairpower.ru)

rus with an opportunity to preserve the Russian market and to ensure supply of cheap energy resources as well as direct and indirect financial aid. All those mentioned factors create preconditions for increasing political, economic and military dependence of Belarus on Russia.

As in the previous year, in 2014, the bilateral relations were stained by certain disputes. The foundation for these disagreements was an embargo on import of some food items from Western countries imposed by Russia, which consequently affected the imports from Belarus. However, the measures limiting supplying of goods are being gradually lifted, and cooperation projects are further pursued.

Belarus continues to consider NATO as the main source of external military threat and the military cooperation between Belarus and Russia is promoted as planned. For Russia, Belarus is the front defence echelon in the Western Direction. Belarus and Russia are consistently improving the legal basis for their cooperation, synchronising and optimising the command and control and operational interaction of the Regional Military Grouping of Belarus and Russia, and strengthening their joint control and defence of the airspace.

The projects of acquisition of air defence missile systems S-300 and Tor from Russia are continued. Jet-trainers Jak-130 manufactured in Russia reached Belarus this year. Preparations for joint large-scale military exercise to be conducted in autumn 2015 have begun. A unit of Russian jet-fighters has been deployed in Belarus since late 2013. Exploiting the situation in Ukraine and the upgrade of military capabilities in the Eastern Direction by NATO, Russia temporarily strengthened airspace defence and control in Belarus in 2014 and deployed there additional fighter jets. Russia intends to establish its Air Force base in the territory of Belarus in 2016. In case of a critical situation, its aircraft could be used against the states of the Baltic Sea region. Furthermore, it would make it difficult for Belarus to maintain its neutrality in a military conflict where Russia is involved. Therefore, introduction of a combat aviation unit of Russia in Belarus would have an adverse effect on the security situation of the neighbouring states.

Currently, the Belarus Armed Forces are oriented towards and capable of ensuring national defence and mobilization readiness. Depending on the changing military and political situation in the region, the Belarus Armed Forces are given the objective to respond to new fighting methods and conditions. The main concern is to ensure mobility and technical provision of the Special Operation Forces. The priority is given to the development of Air and Air Defence Forces, but lack of funding prevents to conduct modernisation at a desirable rate.

CIS, Ukraine and Georgia

After the political change in **Ukraine** in February 2014, Russia not only annexed Crimea, and was the determining factor in causing the military conflict in Eastern Ukraine, but also continued exerting unprecedented pressure in order to force Ukraine to abandon its pro-Western orientation. The key demand of Russia (Ukraine's federalisation) has not changed, *i.e.* the transformation of Ukraine from a unitary state to a federation of individual regions with substantial autonomy and controlled by a weak centre. After the core infrastructure in Donetsk and Luhansk regions (oblasts) was destroyed due to ongoing fightings and a number of industrial enterprises and residential buildings suffered from serious damage, Russia has one of the major objectives to impose the costs of restoration and maintenance of those regions on Ukraine. Federalisation and huge expenses for restoration of the eastern regions would ensure a political and economic weakness of Ukraine for a long time, restrict its opportunities to adopt decisions independently, establish the influence of Russia on the particularly autonomous eastern areas and give Russia leverage against any undesirable decisions of the Ukrainian leadership.

One of the most prominent achievements of Ukraine in the conflict with Russia is nearly halted spread of unrest to other eastern and southern areas, primarily to Kharkov and Odessa. Moreover, in summer 2014 Ukraine succeeded in retaking the lost territories of Donetsk and Luhansk by August when Russia sent units of its regular army to Ukraine in an attempt to restore the separatists' initiative in the battlefield. Since then, Russia seeks to demonstrate that it will not allow Ukraine regaining control of its eastern regions and that the conflict resolution is possible only by accepting the terms of Russia.

The situation of Ukraine's leadership is very complicated: the economy and public finances are in critical condition, which is greatly affected by the necessity to finance fighting against separatists and Russian troops. Some socially painful but necessary steps are imminent, and they will under-



■ Residential district of Kramatorsk (Donetsk region) after being shelled from the territory controlled by Russia and separatists (Source: www.svoboda.org)

mine the public support. Despite the outcome of the conflict in the east of Ukraine, high political and social tensions will persist in the country in the near future, and it will be very dependent on the international political and financial support.

Russia continues its consistent blocking of European integration of **Moldova** and attempts to involve it into integration formations controlled by Russia. Russia's actions in Ukraine had a tremendous negative effect on the security situation of Moldova, and mobilised the separatists both in Transnistria and Gagauziya autonomous region. Attempts to handle the conflict of Transnistria have generated no major changes in 2014, but Russia seeks to revive the idea of federalisation of Moldova as the only way to return Transnistria to Moldova and subdue separatist moods in Gagauziya. The domestic political situation was determined by the parliamentary elections held at the close of 2014. Although pro-European parties have maintained the initiative of forming the coalition government, the election revealed the growing public support for the parties in favour of integration with Russia. The pro-European government will be fragile due to internal polarisation and non-improving economic situation, which will be used by the parties openly supported by Russia to discredit the leadership.

Currently, there are no indications that the settlement of Nagorno-Karabakh conflict by political means may be reached. **Armenia and Azerbaijan** sharpen their rhetoric, pursue programmes of strengthening and modernisation of their own armed forces, and continue to increase spending for the defence. Therefore, it is probable that the intensity of the military conflict will not diminish. The political settlement process which has not yielded any tangible results for a long time only increases the likelihood that the broad-scale military conflict will be renewed. Strengthening of the oligarch structure in Armenia, uncertainty of the relations with the West and a rushed joining of the country to the EAEU in 2014 are prerequisites for the country to become a hostage of Russia's political will. Armenia's interests will have less and less influence on handling the conflict of Nagorno-Karabakh, and the settlement process will become increasingly dependent on Russia's political manoeuvres intended to pressure Azerbaijan's leadership.

After **Georgia** signed the European Union Association Agreement in June 2014, Russia increased its pressure on Georgia resisting its closer ties to the EU. Currently, Georgia does not have any leverage to change Russia's policy towards Georgia and its separatist regions. The Russian-Abkhaz Strategic Partnership Agreement signed in November 2014 is to be regarded as yet another step of Russia toward the final annexation of Abkhazia. A similar agreement was signed with South Ossetia in 2015. Georgia adheres to a pragmatic course of economic cooperation with Russia, and the economic relations between the two countries are improving.

HOSTILE INTELLIGENCE ACTIVITIES

Activities of Russia's intelligence and security services

The most active intelligence activities against national security and state interests of Lithuania are conducted by the following Russia's intelligence and security services: the Foreign Intelligence Service (SVR), the Federal Security Service (FSB), and the Main Intelligence Directorate of the General Staff of the Armed Forces (GRU).

SVR is the main foreign intelligence institution of Russia mostly engaged in intelligence activities in the political, social, economical and energy spheres. Intelligence activities are usually carried out by applying human intelligence (HUMINT) methods, using diplomatic positions abroad, establishing cover organisations and engaging in operations of illegal aliens.³

The underlying intelligence activities of **FSB** in Lithuania are conducted from the territory of Russia. By recruiting visiting citizens of Lithuania and diplomats, this service attempts to carry out operations of penetration into intelligence and security services, Armed Forces, statutory organisations and other strategic objects of Lithuania.

The main task of **GRU** is to supply the Armed Forces of Russia with intelligence information. Therefore, its activities are mostly directed against the defence capabilities of Lithuania. Russia's military intelligence is focusing its activities on two levels: operational and strategic. Operational intelligence which ensures information assistance to the military planning and usually supports military units of the Armed Forces deployed in Russia's military districts is carried out by individual intelligence subdivisions of GRU. Strategic intelligence, the tasks for which are defined based on the



³ Citizens of Russia or other states acting in favour of Russia abroad under a false identity (engaging in intelligence activities, influence operations).

■ (NS) Intelligence methods of Russia's intelligence and security services

needs of top-ranking military and political leadership, is carried out using a non-traditional cover and Russia's diplomatic cover abroad.

With an increased tension between Russia and NATO as a result of Russia's aggression against Ukraine, Russia's interest in capabilities of NATO and defence capabilities of Lithuania as a member of NATO has grown. New spheres of interest appeared, e.g., Lithuania's assistance to Ukraine, the response of Lithuania and NATO to the events in Ukraine, the additional capabilities of NATO deployed and planned for deployment in Lithuania. Russia's intelligence and security services have been traditionally interested in the defence policy of Lithuania, armament of its Armed Forces, the national and international military exercises, objects significant to the national security of Lithuania, the personnel of the national defence system and their vulnerabilities.

To achieve intelligence goals, Russia's intelligence and security services applied a wide range of complementary and coordinated intelligence methods (see the diagram above) in an attempt to extract information related both to the defence of Lithuania and to NATO, which would enable such services to engage in other intelligence tasks during the time of peace, crisis or a military conflict.

Human intelligence. The use of agents recruited by Russia's intelligence and security services continues to be a huge intelligence threat to the defence interests of Lithuania. In selecting recruitment targets for **intelligence gathered by agents**, the services assess whether the person concerned will be able to access the information satisfying the intelligence needs of Russia, whether he/she will be able to participate in decision-making process of significant institutions of Lithuania and/or international organisations, and whether such person will be motivated to cooperate willingly. They attempt to gather as much information as possible about the recruitment target's personal and job-related characteristics, weak points (e.g., addiction to psychotropic substances, gambling, financial hardships, etc.), motivation to cooperate (e.g., disappointment with one's job, desire to take revenge, etc.). A recent tendency can be observed that in spotting their recruitment assets, Russia's intelligence and security services are giving greater prominence to such persons' emotional ties⁴ with Russia and their positive view of Kremlin's policy. Not only Russia's intelligence operatives, but also access agents, i.e., old acquaintances of the potential target, his/her friends from school, university or service in the army who are related to Russia, may be used to establish a contact and pursue the recruitment process. People often do not even suspect that an accidental encounter, a letter on a social media or a telephone call from the person whom they have not seen in years and who was their fellow serviceman in the Soviet Army or with whom they studied at university in Russia may be a contact related to recruitment. Access agents may want to re-establish the relationship after a long break, and in individual cases to cultivate the already established relations. When recruiting, the representatives of Russia's intelligence try to build a friendly atmosphere and create a situation where the target would feel indebted to the recruiting intelligence officer. The process of recruitment of personnel may take up to several years, and its duration depends

⁴ Family relations (born in Russia and/or come from it), friendships with the people residing in Russia, other personal ties (used to live, work, study at a higher military or other school in Russia), loyalty or positive attitude towards Russia's political regime, culture, language, etc.

on importance of the recruitment target. Once intelligence cooperation is established, efforts are made for the recruited agent to feel safe. He/she is taught various conspiratorial methods and is given the technical equipment for maintaining clandestine contact. Cooperation of this kind takes place in great secrecy, strictly maintaining the conspiracy, and is based on the mutual agreement between the representative of an intelligence service and the recruited individual. It should be noted that the AOTD provided the information on a recruitment cycle in its Assessment of Threats to National Security 2013.

Active human intelligence actions directed against the interests of Lithuanian national defence are confirmed by the information gathered during a counter-intelligence investigation conducted by the AOTD and such material has been supplied to the Prosecutor General's Office of the Republic of Lithuania. On the grounds of such information a pre-trial investigation was initiated under Article 119 (Espionage) of the Criminal Code of the Republic of Lithuania. **On 29 December 2014, in the course of a secret operation, the officers of the Prosecutor General's Office of the Republic of Lithuania, the Lithuanian Criminal Police Bureau, and the AOTD detained two individuals suspected of espionage against the interests of Lithuania**, namely an officer of the Air Force of the Lithuanian Armed Forces, and an individual holding citizenship of both the Russian Federation and the Republic of Lithuania to whom the officer of the Lithuanian Armed Forces allegedly provided intelligence information. The person, to whom the officer of the Lithuanian Armed Forces allegedly delivered intelligence information, had served in the army of the Soviet Union for many years, held a colonel's rank and had served in the unit of the Soviet Union army deployed in Lithuania. During the intelligence operation, the suspect periodically visited Lithuania where he had some real estate and movable property, maintained old friendships and established new ones with citizens of the Republic of Lithuania, and had other ties with Lithuania. This operation of detaining was unique in that both the agent suspected of espionage (the officer of the Lithuanian Armed Forces) and the person who has allegedly recruited the representative of the Lithuanian Armed Forces were detained. Currently, more detailed information cannot be provided so as not to impair the ongoing pre-trial investigation. The public will be informed of this incident once the court proceedings are over.

Representatives of GRU under a diplomatic cover have also been active in terms of human intelligence directed against the interests of Lithuanian national defence in 2014. Exploiting their diplomatic status, the representatives of GRU were gathering information necessary to the military planning of Russia by various intelligence methods. The information was gathered while attending various events, conferences and receptions of diplomats. It was attempted to receive as useful information as possible from the persons who commonly did not suspect that they had become a target of an intelligence interview at such events. The individuals conducting intelligence interviews usually seek to obtain some episodic information needed to supplement a certain picture of intelligence information. Such episodic information normally does not constitute a secret, and during the above-mentioned survey the need for such information is naturally covered under the

discussion, disputes of general nature, or substantiated by various invented and unsuspecting motives. In order to prepare for intelligence interviews, the representatives of Russia's intelligence plan a survey strategy and frame the significant and insignificant questions. When conducting such surveys, significant questions are inserted in between insignificant questions and the person being surveyed usually finds it difficult to understand that the conversation was intended for extracting some specific information serving the needs of Russian intelligence. It has to be noted that once the information is collected, in individual cases it may be used against that person for recruitment purposes implying that he/she already supplied the intelligence information.

It should be pointed out that after successful counter-intelligence operations of Lithuanian intelligence institutions in 2014, a part of GRU representatives left or were forced to leave for Russia, and GRU representatives under a diplomatic cover are less active. However, Russia is likely to restore those resources or compensate for their lack with other intelligence actions.

Intelligence activities directed against citizens of Lithuania abroad. Russia's FSB actively engages in intelligence directed against citizens of the Republic of Lithuania who travel to Russia. By means of provocations and measures of psychological impact, it was attempted to gather the information pertaining to defence capabilities of Lithuania and other information required by Russia's intelligence from Lithuanian citizens crossing the state border with Russia. It is noteworthy that Russia's FSB may prepare for intelligence operations against Lithuanian citizens of interest in advance as the citizens of the Republic of Lithuania seeking to obtain a Russian visa must submit information about their place of work and visit destinations in Russia. FSB may access such information. Thus, FSB has an opportunity to survey the targets it is interested in when they are crossing the border between Lithuania and Russia, and conduct in-advance prepared intelligence operations against them in the territory of Russia.

FSB was also active against the Lithuanian diplomats to Russia. It attempted to collect some compromising information about them. In order to collect such information a wide range of intelligence methods and technical measures were applied with respect to the diplomats. Although Lithuanian diplomats are not engaged in any intelligence actions in the territory of Russia, FSB ostentatiously (by leaving or demonstrating obvious signs of operational activities, openly following or taking photographs) tried to deter such diplomats from gathering the information which could allegedly harm Russia's interests. Aggressive recruitment was also carried out against the above-mentioned diplomats by means of blackmailing and provocations.

It should be noted that recruitment actions were taken not only against the diplomats of Lithuania residing in Russia, but also against the Lithuanian diplomats residing in the states of the EU, NATO and CIS, and responsible for military cooperation. Unlike in Russia, the representatives of GRU acted against these diplomats under the diplomatic cover.

Open source intelligence. To supplement the general picture of intelligence information, Russia's intelligence and security services were engaged in intelligence from open sources. The information

meeting the needs of Russian intelligence services was further gathered from the online information portals, forums, websites, the information bulletins and articles issued by the national defence and other institutions and organisations.

Gathering of information by using relations with journalists and conducting surveillance. In an attempt to supplement the general intelligence situation concerning the defence capabilities of Lithuania, the Russian GRU maintained active relations with foreign journalists supporting Kremlin's policy. When attending various events of military nature or military exercises, the journalists having ties with GRU often have an opportunity to record other attendees, the vehicles and equipment used, and the need for information can easily be substantiated by their job functions. Such journalists do not gather classified information, and their activities are to be attributed to the so-called "white intelligence".⁵

A similar situation is with the individuals engaged in surveillance, photographing and filming of military objects. In 2014, the number of incidents involving taking photographs or filming the Lithuanian Armed Forces units has increased considerably. It may be linked to a greater public interest in the Lithuanian Armed Forces, but Russia's intelligence and security services also assign certain individuals to take photographs and film Lithuanian military units under the cover of the mentioned interest. The information gathered by such method usually does not constitute a secret, but it is a substantial addition to the general picture of intelligence situation. Active attempts to photograph or carry out surveillance of significant military units and their personnel may trigger a sense of insecurity in personnel, have a negative impact on interaction between the partners who came to Lithuania and the Lithuanian forces, and diminish an image of Lithuania as the host country.

Signals intelligence. To achieve their intelligence goals, Russia's intelligence and security services continued actively using capabilities of signals intelligence in 2014. Objects of the above-ground infrastructure intended for signals intelligence of Russia's intelligence and security services deployed in Kaliningrad region are continuously improved and enable them intercepting a broad range of communications (radio, cell, satellite, radar and other signals) in the entire territory of Lithuania. In addition to the above-ground objects, mobile platforms for signals intelligence such as reconnaissance vessels and aircraft continued to be used. It should be noted that Russia's intelligence and security services have technical resources to conduct signals intelligence by mobile equipment (transported by cars). Moreover, they are able to install devices for signals intelligence in the buildings that are not specifically intended for that purpose. The possibility should not be excluded that such devices may also be used in the territory of Lithuania. By means of such devices the parameters of mobile phones of the targets can be identified and used to listen to phone conversations of intelligence targets as well as indicate the location of their mobile phone.

⁵ Gathering of information without violation of laws.

Activities of intelligence and security services of Belarus

The State Security Committee of Belarus (KGB) and the Main Intelligence Directorate of the General Staff of the Armed Forces of Belarus (GRU) act against national security and national interests of Lithuania.

The main objective of the Belarusian KGB is to ensure security of the authoritarian regime and political stability in the state. Intelligence activities of Belarusian GRU directed against the defence capabilities of Lithuania are carried out both in the territory of Lithuania and from the territory of Belarus. It is noteworthy that intelligence collection methods and spheres of interest of this service are very similar and sometimes identical to those of Russia's GRU. To achieve its intelligence goals, Belarusian GRU uses the cover of diplomats and journalists, apply intelligence activities against citizens of the Republic of Lithuania visiting Belarus, and the personnel of the defence attaché of Lithuania to Belarus. Intelligence and security services of Belarus also use the resources of signals intelligence and cyber espionage. Although in comparison to Russia's capabilities, the level of activity of Belarusian intelligence and security services with respect to defence capabilities of Lithuania is significantly lower, it should be noted that the intelligence services of Russia and Belarus actively cooperate. Therefore, intelligence resources of Belarus may be assessed together with Russia's intelligence capabilities.

CYBER THREATS

Cyber security

The majority of cyber incidents directed against automated data processing (ADP) systems and networks of Lithuanian state institutions in 2014 were carried out by foreign intelligence and security services and by computer hackers related to, or controlled and supported by such services. Russia's intelligence and security services, especially FSB and structural divisions of the Ministry of Defence as well as subjects associated with such divisions ("hactivists", representatives of the criminal underworld, patriotically-minded hackers, etc.), have the major cyber capabilities channelled to gathering of information, disrupting functioning or overtaking of Lithuanian ADP systems and networks, testing the ability of key institutions of Lithuania to protect themselves from such threats. The capabilities available to Russia are being continuously used and are closely related to implementation of strategic goals of Russia. In order to use its cyber capabilities, overtaking and exploiting PCs, computer software, telecommunication equipment, ADP systems and networks, mobile devices and other IT equipment, Russia seeks to gain advantage in the areas of defence, politics, economy, technologies and others. The gathered information is also likely to be used in military campaigns planning.

Russia has no intentions to refrain from aggressive actions in cyber space. On the contrary, taking into account the ongoing modernisation and development of measures for espionage and cyber attacks, the methods and tactics of penetrating ADP networks and systems (e.g., the social engineering technique), other characteristics and potential of such programmes, it should be assumed that Russia's activities in the cyber sphere will continue to intensify, and the spyware used for intelligence will be further developed.

It is highly likely that disrupting daily work of state institutions, national critical infrastructure, and the media (distributed denial-of-service (DDoS), website defacement (illegal changes in visual appearance of the site)) is an attempt both to compromise such institutions and to demonstrate the power, possibilities and potential of the aggressor (a measure of deterrence).

Based on the available data, the agents of Russia acting in the cyber space may target the following objects (in addition to the defence systems):

- state institutions, especially the Ministry of Foreign Affairs, Ministry of Economy, Ministry of Energy;
- telecommunication systems, objects of industrial and critical infrastructure the disruption of functioning in which would be vitally important;
- the media.

Cyber espionage

Through cyber espionage, the services of Russia and the computer hackers related to such services, or controlled and supported by them sought to infect PCs, ADP systems and networks by spyware or malicious codes. Activity of spyware or its traces were detected in ADP systems and networks, and user devices of a number of public institutions of Lithuania (the AOTD reported on this tendency in the Assessment of Threats to National Security 2013).

In 2014, activity of spyware or its traces were detected in ADP systems and networks as well as user devices of a number of state institutions. The spyware or malicious codes detected by the department were intended to mine data contained in the computer, network, system or user device, to carry out remote administration of the infected computer, to monitor the network, to identify accounts and passwords in the network, also to record audio and video signals.

In 2014, a group called *Sofacy* (possibly also identified as *Sednit*, *APT28*, *Fancy Bear*) associated with Russia was highly active. The cyber attacks launched by this group in the past years have been directed against NATO, individually against military institutions, embassies, enterprises of the military sector of the United States and their allies, Russian opposition politicians and dissidents, and the international media. Activities of this group have also been detected in the Baltic States.

Based on the data provided by international IT companies, the most active espionage in the cyber space was conducted by members of *Sofacy* group from Moscow and Saint Petersburg during business hours of the European states (from 8 a.m. to 6 p.m. local time). The hackers used the spyware Win32/USBStealer (which spreads through USB devices) for the attacks against closed computer networks. The attacks online were launched by the group using the so-called “watering hole”⁶ and “spear phishing”⁷ methods.

In 2014, international IT security companies issued a public statement containing detailed information about the detected spyware (Snake Rootkit, Turla, Uroburos) which are the latest and most modern versions of the spyware agent.btz. The signs of activity of the spyware agent.btz or its versions Snake Rootkit, Turla, or Uroburos are continuously detected in the ADP systems and networks or user devices of Lithuanian state institutions.

At the close of 2014, some information was made public claiming that the spyware Turla (otherwise known as Uroburos or agent.btz) functions in the Linux Operating System (until then, this OS used to be considered safe). One of the ways to test whether it is infected with a virus is to track the outgoing traffic to such connections as news-bbc.podzone.org or IP 80.248.65.183.

In one of its public reports in 2014, Russian IT and security company Kaspersky Lab also announced

⁶ “Watering hole” is a purposeful cyber attack that may be targeted against a specific group of people, institution, organisation, or a region. During the attack, the cyber hackers establish/identify by guessing or observing which websites the group of interest uses most often, and then infect such websites with malware.

⁷ Spear phishing is an attack of the social engineering type attempting to get the passwords for access to IT systems or other confidential data by means of undesirable e-mail letters or false websites, i.e. by fraud.

about the cyber espionage threat Epic Turla. However, according to the AOTD, unlike the western IT security companies, the public statement of Kaspersky Lab (which is associated with state institutions of Russia) contains the information that is neither comprehensive, nor detailed, and the recommendations offered are superficial and basically do not help to solve problems of PC users. The technical part of the report provides more details only about one module (“keylogger”⁸). Archiving, encrypting and sending are performed by other modules which were not described in the company’s report. Since only one module is described in a broader manner and merely in a few aspects, once the function of this module is technically altered, PC users will not be able to detect the spyware Turla functioning in their computers.

According to the AOTD (which takes into account the trends in modification and development of the spyware observed in a number of years, also the technical details of computer investigations into the spyware, and its characteristics), agent.btz and its latest versions (Snake rootkit, Turla, Uroburos) are the espionage tools developed by Russian cyber specialists and intended for strategic goals (the main ways to detect the spyware are provided in the annex).

The same spyware is given different names as the spyware is detected by different entities (e.g., IT security companies) which attribute varying names to the same software (virus) or its newer version at their own discretion. When researching any software, different entities give names according to the underlying words selected by creators of the software and used by programmers as a code, or simply based on a part of the file name. In analysing a malicious code, different IT security companies emphasise different technical aspects, and the competence of researchers may also vary. As a result, there are a number of research reports on the same malware bearing different names. For instance, one IT security company found the word UROBUROS in the programme code, and based on that gave the name for the entire software:

Ur0bUr()sGoTyOu#

Another security company analysing the same malicious code determined that the creator of the malicious code named one file SNAKE. In this way, the malware previously named UROBUROS received another name SNAKE:

Main module inj_snake_Win32.dll

⁸ The “keylogger” module is independently functioning software which is able to register (log) when the keys are struck on a keyboard in typing passwords or other text, to record the processes then taking place on the computer, and to store the collected data in a computer file. Later such collected data are sent to a communications and control server (C&C).

Threats to mobile device users

A new trend of rapid spread of the viruses intended to infect smart devices was noticed in 2014. Such viruses are particularly abundant in operating systems of Android. Viruses usually collect all the information about the phone owner (user) and send it to communications and control servers (C&C). Such information includes recordings of conversations, browsing history, copies of e-mails, location. The virus may also covertly turn on the microphone installed in the phone (to listen to the environment), etc. Until recently the viruses were being installed in the phones once a user downloaded applications to the device from the websites offering applications. In 2014, it was noticed that cyber hackers started using a new method for infecting devices which is based on WAP Push technology where smart devices are being infected by sending to the user SMS messages which the user does not see, and the commands contained in such text message activate an online link from which the device downloads malware. In addition, BotNet networks have already been detected in the networks of smart devices. In a critical case, a BotNet network in smart phones can effectively influence not only mobile communications networks, but also the ordinary computer networks since smart devices are basically never turned off, thus, they are a perfect tool to launch DDoS attacks.

■ ■ ■

The number of cyber incidents will not decrease (at least in the near future) and the cyberspace itself will remain one of the main areas to carry out espionage or otherwise affect objects of the critical infrastructure significant to the national security of Lithuania and the national defence capabilities.

The subjects taking aggressive actions in the cyber space will try to exploit vulnerability of the ADP systems and networks of Lithuanian state institutions, and will keep choosing targets which have no appropriate cyber tools / weapons, no early warning and detection systems enabling to ensure cyber defence and its strategy as a continuous and pointed effort, and to determine cyber security efficiency on time as well as eliminate the identified shortcomings and weak spots.

INFORMATION THREATS

Lithuania keeps experiencing intensive and systematic information attacks from Russia. Their intensity visibly increased already in 2013 due to an active policy of Lithuania regarding Ukraine's and the EU's Eastern Partnership. The intensity was further enhanced in 2014.

In 2014, the harshest criticism was directed towards Lithuania's political, military and economic support to Ukraine. The information field promoted by Russia was infected with some doubts concerning autonomy of foreign policy of Lithuania, its defence capabilities, increasing financing for the national defence system, the commitment of NATO to ensure security of Lithuania, and the necessity to have larger military capabilities of NATO in the region. More attention was given to the "dangerously growing" number of NATO's military exercises and its infrastructure at the borders of Russia. Such views were presented as proving that the Alliance is aggressive, and substantiating the need to increase Russia's military potential in the region.

In 2014, the focus was maintained on the "political", "unreasonably costly" and "dead-end" (according to Russia's media) actions of Lithuania in the energy sphere. Such focus grew even stronger with the approaching opening of the floating terminal of liquefied natural gas (LNG). The subject of how inconvenient the transit across Lithuania is was also pursued. "Expropriation" of the natural gas infrastructure from Gazprom also received harsh criticism. Attempts were continued to shape a positive image of integration projects controlled by Russia (the Customs Union and EAEU), and even their potential benefit to the people and businesses in Lithuania.

The network of information channels controlled by Russia was strengthened on international level. In 2014, activities of Russia Today abroad were expanded. The state news agency *Rossiya segodnya* presented the project Sputnik which is planned to have centres in 30 countries. The increasing propaganda resources intended for international audiences will result in growing possibilities of Russia to discredit steps of Lithuania and spread disinformation about it in other countries.

Following the events in Ukraine, the interest of the Lithuanian public in information attacks has peaked, and that would be an even stronger incentive for Russia to search for new approaches to exert social influence. The Baltnews.lt project generated in 2014 is not restricted to an online portal, and the ambitions are to engage in information dissemination via radio and television in the future. It is likely that in shaping the public opinion in Lithuania, it will be sought to use the social networks to a greater extent by presenting "expert opinions" favourable to Russia, and to attract the public by referring to the traditional conservative values, contrasting the same with "immoral liberal attitudes of the West".

Attempts to polarise the Russian-speaking population of Lithuania with respect to the State and society of Lithuania are expected in the near future. A claim that the right of the Russian-speaking residents of Lithuania to have a different position is allegedly disregarded was very actively promoted in 2014. The very first hints about a potential development of alternative information

sources in Russian in the Baltic States to counterbalance the Russian propaganda were met by Russia as a tool of the hostile “state propaganda” directed to the Russian-speaking population. Provisional decisions to ban rebroadcasting of television channels in Lithuania were treated as a pressure on the Russian-speaking media and “return to the Soviet practices”.

The long-term key objectives of Russia’s information policy are to contribute to the shaping of the mentality and attitudes of the society, its separate groups or individuals, to promote distrust in state institutions, and disunity in the society and in relations with foreign partners, to increase influence of the information content created by Russia on the Lithuanian society. Accomplishment of such objectives serves to achieve the main goal, i.e. by means of information measures to ensure that the policy pursued by Lithuania is in line with Russia’s interests.

At least in the short term, the intensity of Russia’s information attacks against Lithuania will remain very high. In addition, isolated information provocations will be launched periodically. The next main targets will be Lithuania’s position on the conflict between Russia and Ukraine, and NATO’s decision to increase military capabilities in Eastern Europe, the assessment of the social and economic situation of Lithuania after adoption of the Euro. A particularly strong focus will be on disuniting ethnic minorities and the state. Moreover, the strategic energy projects of Lithuania, its potential support to the opposition movements in Russia and Belarus, the public support to the foreign and security policy of Lithuania, trust in the national defence system and NATO will continue to be targets of Russia’s information attacks.



■ Dmitry Kiselev, one of the key propaganda voices, is presenting the project Sputnik
(Source: www.bbc.co.uk)

CRISIS REGIONS

Afghanistan

The presidential elections held in 2014 were characterised by high voter turnover and lengthy recalculations of the tallies due to allegations of fraud. The election ended in August in a settlement between the top contenders on power division. The political, security and economic situation in Afghanistan remains unstable. As a result of internal political friction, the formation of the national solidarity government is progressing with great difficulties.

The armed opposition Taliban continues its active operations against Afghanistan National Security Forces (ANSF), state institutions and international forces. The number of civilian casualties and high-profile attacks in the capital Kabul against members of the international community has increased as the opposition fighters strive to demonstrate the “defeat” of international forces and discredit the ANSF ensuring security of the country. So far the Taliban has shown no intentions to get involved in the political process (which is suggested by new President Ashraf Ghani), and further engages in armed fighting. The government of Afghanistan and ANSF remains highly dependent on the international financial aid.

At the close of 2014, NATO completed the International Security Assistance Force (ISAF) mission initiated in 2001. However, a limited foreign military contingent, including Lithuanian troops, remains in Afghanistan.

Middle East and North Africa

The most intense regional conflict in 2014 was unfolding in **Syria**. This conflict resulted in over 210,000 casualties, and over 3.8 million residents fled the country. Syria’s conflict greatly affects security in the entire region: inter-confessional polarisation in neighbouring states is deepening, and a threat of terror attacks has grown. The conflict has reached a deadlock as the ruling regime is unable to achieve victory against the insurgents, and the militarized opposition is too disjointed to overthrow the regime. Frequent infighting among the insurgents results in weakening groups of moderate fighters, whereas supporters of radical Islam are gaining more influence.

The Islamic State (ISIL), a jihadist group which became prominent in Syria, launched a lightning offensive on **Iraq** in the summer of 2014. The group occupied significant territories, and declared establishing a state based on the Islam right, i.e., a caliphate. This prompted an international coalition led by the United States to initiate a military intervention in Iraq and Syria. A high-intensity air operation gave palpable results: ISIL lost part of its fighters and military vehicles, its revenue from oil trade declined along with its military strength. Despite all that ISIL remains one of the most powerful groups in the region, and its propaganda campaign keeps radicalising the locals and residents of foreign states.



An increasing number of citizens of the Western states are involved in the conflicts of Iraq and Syria and are fighting in the ranks of ISIL and other radical Islam groups. Therefore, the Western states are facing a threat of attacks launched by the returning terrorists and “lone wolves” inspired by the propaganda of radical Islam groups. Until now, no signs have been detected that such negative trends may directly affect the terrorism threat level in Lithuania.

In autumn of 2014, Yemen descended in turmoil. Its capital Sana’a is controlled by the Houthis, Zaidi Shia rebels. With its southern provinces leaning towards separation, the country is on the brink of a civil war. Disability of Yemeni security institutions accompanied by polarisation of the local residents and radicalisation of part of the Sunni Muslims in the face of the threat of the Houthis provide favourable conditions for South Yemen-based Al-Qaeda in the Arabian Peninsula to gain strength.

The political and security crisis in **Libya** is further escalating causing disunity in the country. Two competing parliaments and governments are unable to agree, and the armed groups and army forces supporting different political camps (Islamist and secular) are infighting. Radical Islam groups are gaining strength in Libya, effectively increasing a threat of terror attacks in the region. Libya risks of becoming a failed state. Since Abdul Fattah al-Sisi, the former head of Egypt’s armed forces won the presidential election in May 2014 in **Egypt**, the army seized the control of political processes and began tackling the Muslim Brotherhood. Though considered to be quite moderate, this Islamist movement was banned and declared a terrorist organisation with ensuing thousands arrests of its members. Despite the stringent security measures imposed by the government, the number of attacks directed against the police and security forces in the Sinai Peninsula is growing.



Conflict regions in Central Africa

Nigeria's militant radical Islamist group *Boko Haram* keeps seizing new territories. Over 10,000 people have died from its attacks. The brutal occupation of territories and kidnappings pose a threat to neighbouring states of the region. The multinational force in 2014 partly stabilised the escalated security crisis in the **Central African Republic** which arose as a result of armed clashes between the Muslim and Christian fighters. However, the provisional government dependent on the international support has little influence outside the capital, and the country remains a failed state.

Annex

The malicious spyware is a ROOTKIT type virus. This is the main pattern to detect the newer version of the spyware which was identified and analysed by the AOTD, and presented in its Assessments of Threats to National Security in 2012 and 2013.

Encryption keys:

56 F1 32 24 5A 08 C0 43 E9 D6 1C 14 FD 42 27 4E

07 35 21 F4 F1 50 76 CA D5 DD 26 41 EF CC 87 2C

00 36 6F 1B 03 2E 01 60 A9

XOR type encryption key is used in HTTP queries:

D8 FF E0 00 10 4A 46 49 46 00 01

Taking into account that the checksums (MD5) of this malicious spyware files with the same name and size in different computers vary, it is advisable to run a search on the computer based on file names. The table below lists the names of files that may be identified as the malicious spyware. It should be noted that in some cases this software will be wrongly recognised. Then a more detailed analysis of the detected file should be conducted.

Names of the potentially malicious computer files

~DF1.tmp	winstat.pdr	isuinst.bin
~DF17.tmp	winstat0.pdr	isuninst.bin
~DF18.tmp	winstat1.pdr	jwgkvsq.vmx
~DF1B.tmp	winview.nfo	kdmom.dll
~DF1E5.tmp	winview.occ	keygen.exe
~df1E7.tmp	winview.ocx	Keylogger.exe
~df2.tmp	winview.xml	kkdcr.dll
~DF22.tmp	wmcache.nl	kmsvo.dll
~DF31.tmp	wmcache.nld	menet32.exe
~DF3A.tmp	wmmini.swp	mfc42100.pdb
~DF3D.tmp	wmset3.tmp	mfc42100.pdb
~DF3F.tmp	wowmgr.bin	mfc42101.pdb
~DF4.tmp	wowmgr.exe	mips.bin
~DF40.tmp	wpo.dbl	mlangupd.dat
~DF42.tmp	wsham.dll	mmc32x.exe
~df4d.tmp	x4t4c57w3.exe	mniole16.dll
~DF5.tmp	xpob2rfs.dll	mpd.ocx
	xtemp1.exe	mpdstate.bin

~dfd.tmp	xtemp2.exe	mpdstate.bin
011fe-3420f-ff0ea-ff0ea.tmp	1.cmd	mqa30.tlb
01559346.gif	qedwtpes.dll	mqupgrv.dll
10004029-0935-7044-004097.tmp	qsbui.dll	msaauxext.dll
1043383640440321341030301.jpg	rkng_inst.exe	msc32.exe
194303040.gif	rtn.dll	msc32d.bin
1972509834634241641422105.jpg	Run.exe	msccap.ttl
22754251916800821251311.jpg	rundll71.exe	msccss.exe
2638.chk	s3.tmp	mschm32.dat
2804e974.tmp	scmp.bin	mscp32n.dll
28678750.tmp	service.exe	mscs32.exe
2e2f82e5.tmp	sh3.bin	msdatsnd.ocx
5cce9c57.tmp	shell64.dll	msdattst.ocx
6D73646174736E642E6F6378FF.tmp	slrwvdrv.dll	msdio.tlb
6D737379736D67722E6F6378Ff.tmp	Spread.exe	msdk.dat
6D73776D706461742E746C62FA.tmp	ssmicrco.scr	msdk32c.dat
704f1bcd.tmp	strmell.dll	msdk32c.ocx
77696E737461742E706472FA.tmp	svchosts.exe	msdk32n.dat
77696E766965772E6F6378FA.tmp	qcpi.sys	prt.ocx
77696e766965772e6f6378ff.tmp	tablsrv.dll	msdstate.bin
77696e766965772e6f6378fa.tmp	tapi32a.exe	msdwr32.dat
a0bfd8a6.tmp	tapi32b.exe	msfv.sys
a230.tbl	tapi32c.exe	mshlp32.exe
aasl2tp.sys	tapi32d.bin	msidfn32.dll
adm.log	tapi32d.exe	msinet32x.ocx
autorun.inf	tcpdump32.exe	msinfo32d.exe
Back2life.dll	tcpmon.exe	muxbde40.dll
Back2life.ini	tcpmon.ocx	naufe.exe
bmerrenu.dll	tcpmon32.exe	ncobmapi.dll
boot.pif	temp.vih	NoAutorun.exe
btppnui.dll	thumb.db	ntdsawi.dll
ccache.nls	thumb.dd	ntdump.ttl
charmapi.exe	tlbcon32.exe	ntmsaki.dll
cmbawt.sys	tsddl.dll	ntsdects.dll
commodule.dll	typecli.exe	Nueva_carpetaa.exe
con32.nls	ucmp.bin	Nuker.exe
cpmon.ocx	Ultra3.sys	nvscpapisvr.exe
Crack.exe	untfj.dll	oaklcy.dll
Cracker.exe	userevent evt	pdt\$.tmp
csrsc.exe	usrdtaa.dll	piufig.exe

dakim.dll	vfatd.dll	places.sqlite
dc000000.tmp	vpnmon.exe	prf6a3.tmp
desktop.dll	vtmon.bin	Private.exe
desktop.dll	wextract.exe	mstotreg.dat
dgsetur.dll	win3uspl.dll	msvcrt.dll
Downloader.exe	winmons.ocx	msvctl.dll
dsdmopra.dll	mskfp32.ocx	msvctl.exe
dtp.bin	msmdl.ocx	msw32.sys
dxsnd32.exe	msmpdat.tlb	mswdr.ocx
dxstest32.exe	msmsgmon.exe	mswme32.exe
dxttest32.exe	msnet.exe	mswmpdat.bin
efhadu.dll	msnet32w.exe	mswmpdat.tlb
Exploit.exe	msnetsrv.exe	mtev.bin
fdisk.sys	p\$cm\$.tmp	mtmon.sdb
fdisk_32.sys	msnetsrv.exe	igmparnt.dll
fdisk_mon.exe	m\$pd32.exe	imapc2.dll
fscan.exe	m\$ssysmgr.ocx	imeshbre.dll
fwclt.exe	m\$stmdm.dll	index.txt
ghx.exe	m\$storeg.dat	intle.exe
gpstat.exe	ielocal~f.tmp	hotfix.dat
Hacker.exe	iesettings.ceb	icmhi.dll

The list of IP addresses and domains of the communications and control servers of the malicious spyware is presented in a table below. It should be pointed out that the majority of the domains use NO-IP technology.

IP addresses and domains of communications and control servers of the malicious spyware

111.125.163.177	82.98.86.171	stepte4.50megs.com
124.248.207.50	83.125.22.192	stradford.com
141.8.224.25	85.25.176.33	straford.com
162.210.192.21	87.248.210.254	support4u.ath.cx
178.79.190.156	92.61.39.207	te4step.tripod.com
181.29.2.7	alldaynews.sytes.net	techsupportdotnet.biz.ly
195.43.94.104	allnews.ath.cx	Tiger.netii.net
195.58.176.133	antras ip	today-news.ath.cx
203.117.122.51	h.cx	today-news.office-on-the.net
204.13.162.116	biznews.at	toolsthem.xp3.biz
208.73.210.29	biznews.ath.cx	top-facts.sytes.net
208.73.211.208	biznews.podzone.org	users.noad.hosting.free

209.15.13.134	breakingnews.at	users.nob.hosting.free
212.53.89.138	breakingnews.ath.cx	users.ue.hosting.free
213.131.252.251	coach-blog.serveblog.net	utenti.lycos.it
216.234.186.42	communityeu.xp3.biz	voyaje.biz.ly
217.172.163.8	e.freewebhostingarea.com	weather-online.hopto.org
23.20.75.80	euland.freevar.com	worldnews.at
24news.at	eunews-online.zapto.org	worldnews.ath.cx
24news.ath.cx	euronews.at	www.free.pages.at
31.170.160.149	euronews.ath.cx	www.scifi.pages.at
31.170.160.209	eu-sciffi.99k.org	74.117.221.11
50.116.32.177	fgmail.com	74.208.164.166
50.19.102.217	fifa-rules.25u.com	77.246.71.10
50.63.127.1	free.pages.at	80.67.28.141
59.124.33.177	free-photos.servepics.com	prime-event.podzone.org
59.124.33.215	gole.It	Sanky.sportsontheweb.net
59.125.160.178	greate-empire.4irc.com	sportgolf.styles.net
62.1.82.32	hotnews.ath.cx	sportmusic.servemp3.com
62.116.168.171	intellicast.at	69.162.78.14
62.65.252.15	intellicast.ath.cx	69.162.86.185
62.68.75.170	livenews.at	69.64.147.243
64.136.20.39	livenews.ath.cx	pockerroom.servebeer.com
5.9.82.27	newutils.3utilities.com	pressbrig1.tripod.com
64.95.64.194	Nightday.comxa.com	pressforum.serveblog.net
67.220.217.235	north-area.bbsindex.com	64.31.24.10



9 786094 120800

