

INTERNATIONAL SECURITY AND ESTONIA 2019



VÄLISLUUREAMET
Estonian Foreign Intelligence Service

Design: Taivo Org

Illustrations: Joosep Maripuu, Taivo Org, Shutterstock, Bigstock

ISSN 2613-3261 (print)

ISSN 2613-327X (online)

CONTENTS

| | |
|---|----|
| Foreword | 2 |
| The development of the Russian armed forces | 4 |
| The Russian civilian fleet in the service of national security | 12 |
| Russian domestic politics: tensions are building | 15 |
| A rising tax burden will not be matched by a higher level of democracy | 20 |
| Russian foreign policy | 22 |
| Belarus – the Kremlin tightens its hold | 24 |
| Ukraine – hostilities continue | 28 |
| The socio-economic situation in Crimea and eastern Ukraine | 31 |
| The activities of the Russian Orthodox Church in Ukraine | 33 |
| Transcaucasia – Moscow's influence relies on threats | 36 |
| Nord Stream 2 and TurkStream as security risks | 43 |
| The failures of Russian special services in the West | 45 |
| Russia's malicious cyber activity leans on non-governmental actors | 48 |
| How the FSB signal intelligence gathers information on foreign citizens | 54 |
| China's growing influence | 59 |
| Relations between China and Russia | 61 |
| Terrorism in Europe | 63 |
| Illegal immigration to Europe | 65 |

FOREWORD

The task of the Estonian Foreign Intelligence Service is to protect Estonia from external security threats. We collect and analyse intelligence and forward information to the state leadership to assist in its defence and security policy-making tasks.

Our 2019 report is the fourth time that we are sharing our assessments with the public, as an effective defence and security policy begins with greater awareness of the threats.

The main external security threat for Estonia arises from Russia's behaviour, which undermines the international order. Russia conducts its foreign policy by demonstrating its military force, by using the dependence of other states on Russia's energy carriers, and by conducting cyber attacks and influence operations using false information and other 'soft' tools. Ukraine will be the main target of those measures this year, but Russia will not hesitate to use them even against its ally, Belarus. Countries in the European Union and NATO are not fully protected from Russia's aggressive activities, either – it has only been a year since Russia used a chemical weapon on the territory of the United Kingdom.

The report deals with different aspects of Russia as a military threat. Russia continues to develop and train its armed forces for a large-scale war against NATO. Even though the likelihood of a worst-case scenario is slim, surprises arranged by its authoritarian regime cannot be excluded.

The Kremlin's foreign policy is affected by domestic problems, including increasing popular discontent and tensions within the elite. A strong military force and a leadership that feels threatened may prove a dangerous combination. Russia's foreign and domestic policy is dictated by the authorities' fear of changes which might pull the rug from under them. Therefore, the regime regards domestic opposition as a dangerous enemy. According to information available to the Estonian Foreign Intelligence Service, Russia has practised the use of its armed forces units against internal protesters.

Apart from the military threat, our intelligence service has to identify and prevent Russia's influence activities in Western countries, the goal of which is to destroy their unity; for example, concerning their attitude to

**MIKK MARRAN**

Director General of the Estonian
Foreign Intelligence Service

the sanctions imposed on Russia. To achieve that, Russia is prepared to get involved in other countries' domestic policy. The issue of influence activities deserves particular attention this year, as EU member states are going to elect representatives to the European Parliament.

The world is increasingly analysing the risks arising from the use of Chinese technology and China's investments in other countries' critical infrastructure. Neither can we ignore Russian software producers who cooperate with Russian authorities and special

services on a daily basis. The Estonian Foreign Intelligence Service helps to scrutinise how state communication and information systems, vital service providers and infrastructure, as well as private companies operating in areas important to national security, can be protected from external threats.

The report also covers the development of the terrorist threat. The military campaign against IS and the systematic counter-terrorism efforts of European law enforcement agencies and security services made it more difficult for IS to conduct operations in Europe. Nevertheless, terrorism continues to influence the security of Europe as a whole in 2019.

I am hoping that the report by the Estonian Foreign Intelligence Service helps to better understand the security situation in Estonia in the rapidly changing world.

Bonne lecture!

Mikk Marran
Director General of the Estonian
Foreign Intelligence Service

Editing concluded on 28 February 2019.

THE DEVELOPMENT OF THE RUSSIAN ARMED FORCES

The only serious threat to regional security, including the existence and sovereignty of Estonia and other Baltic Sea states, emanates from Russia. It involves not only asymmetrical, covert or political subversion, but also a potential military threat.

In 2018, Russia continued the military build-up along its western border. The Russian armed forces formed seven new manouver regiments, including four tank regiments, all based less than 50 kilometres from the border. Most of these units are located near Ukraine and Belarus, but the Pskov Air Assault Division near the Estonian border became the first division of the Russian Airborne Troops to be reinforced with a third regiment. This shows that in the prioritised western direction, the Russian armed forces are preparing for a possible war along a wide front.

There is no doubt that Vladimir Putin's regime is prepared to use military force against other countries. In post-Cold War Europe, Russia is the only country that has launched a military attack against a sovereign state that it itself has recognised. Over the past decade, Russia has done so twice, and the military occupation following the invasions of Ukraine and Georgia is still ongoing.

The Estonian Foreign Intelligence Service has monitored all the military exercises of the Russian armed forces during the past decade. These include field exercises played out with actual

RUSSIA FORMED SEVEN NEW MANOUVER REGIMENTS, INCLUDING FOUR TANK REGIMENTS, ALONG ITS WESTERN BORDER.



↑ Russian units and equipment lined up for the Vostok 2018 military exercise.

SOURCE: AFP/SCANPIX

military units in training areas, as well as command-post exercises and war games on maps, which remain hidden from the public eye. By analysing these exercises, we have arrived at four main conclusions.

First, the Russian armed forces are consistently practising for an extensive military conflict with NATO. All the scenarios for command-post exercises from the last two decades describe conventional warfare against NATO and its member states. It is important to note that the general structure of the Russian exercises and scenarios

has remained similar throughout the period, regardless of the wars in Ukraine, Georgia and Syria, and despite Western sanctions or the deployment of NATO forces in the Baltic States and Poland.

Second, as the Russian armed forces see it, a military conflict with NATO will be sparked by a “coloured revolution” in one of Russia’s neighbouring countries. The scenarios of the Russian military exercises reflect a fear, characteristic of authoritarian regimes, of democratic aspirations (coloured revolutions), which the Russian leadership,

due to its KGB background, sees as operations by Western special services. Russia's leaders fear that democratic regime changes may escalate into a wider, regional war.

In light of this, the Estonian Foreign Intelligence Service monitors the political situation in Belarus. Our assessment is that, if anything unexpected should happen to President Alyaksandr Lukashenka personally or to his regime, there will be a great risk of swift military action by Russia to prevent Belarus from becoming a pro-Western democracy.

The Russian leadership also perceives the anti-regime opposition at home as a threat; we are aware that the Russian armed forces have practised using their units against its domestic political opposition.

Third, the Baltic States are the part of NATO that it will be the easiest for Russia to attack in a crisis, to shift the balance of military power on the Baltic Sea in its favour. In terms of military planning, Russia does not look at Estonia as a separate target, but as a part of NATO. Therefore, Estonia has to be prepared for a military

incursion from Russia even if the conflict between Russia and NATO is sparked by events elsewhere in the world. By inciting hatred between local ethnic groups in the Baltic States, Russia is simply trying to reserve a pretext for military intervention, should it be needed.

Fourth, a conflict between NATO and Russia would not be limited to military action in Eastern Europe or the Baltic States, but would also involve Russian attacks on Western European targets. The Russian armed forces are constantly developing their doctrine of attacking "critical enemy targets" and building related medium-range weapon systems – air-, sea- and (in violation of international treaties) land-based – that could be used to attack targets in Western Europe.

This last point will be discussed at some length in this year's report. "Kalibr" is the Russian code name for a surface ship- and submarine-launched missile system that can be used against targets at sea and on land. Following successful testing in combat during the Syrian conflict, Kalibr is now the most widely used missile system in the Russian navy,

and it is also to be mounted on several new vessel classes that are still under construction. The strength of the Kalibr system is its range: up to 600 km against targets at sea and up to 2,500 km against targets on land. Moreover, Kalibr cruise missiles can be fitted with nuclear as well as conventional warheads, and they are cost-effective; for example, with some luck, a Kalibr missile launched from a small craft can sink a large battleship. Vessels armed with the Kalibr system placed in the Baltic, Barents, Caspian or Black Sea can hit targets on almost the entirety of continental Europe.

Russia has been accused of violating the INF Treaty¹ since 2008, particularly of developing and testing the ground-launched 9M729 (SSC-8) cruise missile, which has a range that is prohibited by the Treaty. By 2018, the Russian armed forces had deployed a limited number of 9M729 missiles. The INF Treaty does not limit the range

A CONFLICT BETWEEN NATO AND RUSSIA WOULD ALSO INVOLVE RUSSIAN ATTACKS ON WESTERN EUROPEAN TARGETS.

of air- or sea-launched cruise missiles, however mobile land-based missile systems have a number of advantages over air- or sea-launched cruise missiles; for example, they are less dependent on infrastructure, have less costly launching platforms, and are easier to hide.

Such weapon systems also have an important propaganda value for the Russian president. In his speech to the Federation Council on 1 March 2018, President Vladimir Putin unveiled six new strategic weapons: the air-launched ballistic missile Kinzhal, the laser complex Peresvet, the nuclear-powered torpedo Poseidon, the intercontinental ballistic missile Sarmat, the nuclear-powered cruise missile Burevestnik, and the hypersonic glider Avangard. These include improvements on earlier weapon systems (Kinzhal, Sarmat), revived Soviet-era

1 The INF Treaty (Treaty on the Elimination of Intermediate-Range and Shorter-Range Missiles) was signed between the United States and the Soviet Union in 1987, prohibiting the two from having any ground-to-ground ballistic or cruise missile with ranges between 500 and 5,500 km.



projects (Poseidon, Burevestnik, Avangard) and a completely new system (Peresvet).

It should be noted here that, unlike many other weapon systems (the Kalibr and H-101 cruise missiles or the Su-57 fighter), the Kinzhal is not known to have been tested in combat in Syria, which is why the technology is very likely still in testing phase.

In addition to the military risks associated with the new weapon systems, the potentially catastrophic environmental hazards posed by at least two of them – the Poseidon and Burevestnik – must be emphasised. Both unmanned systems are allegedly powered by a compact nuclear reactor, which may be susceptible to failure, especially when used in systems that are still in testing. The safety of the nuclear

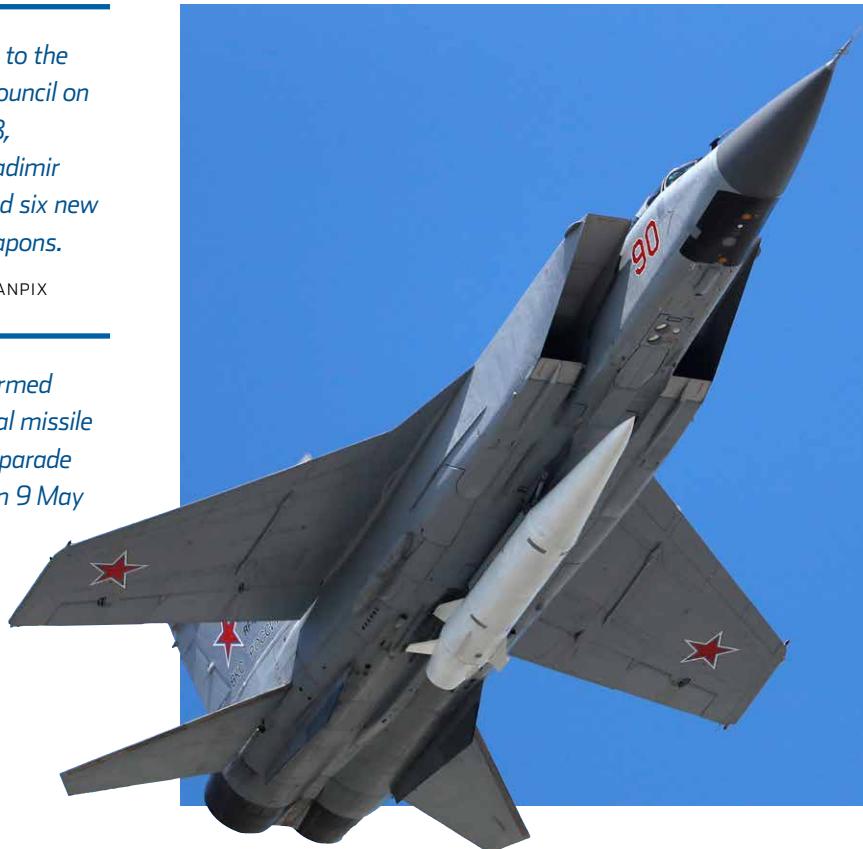
**THE BALANCE OF STRATEGIC NUCLEAR CAPABILITIES
BETWEEN NATO AND RUSSIA WILL NOT BE CHANGED
BY THE NEW WEAPON SYSTEMS.**

- ← In his speech to the Federation Council on 1 March 2018, President Vladimir Putin unveiled six new strategic weapons.

SOURCE: AP/SCANPIX

- A MiG-31K armed with a Kinzhal missile at a military parade in Moscow on 9 May 2018.

SOURCE:
AP/SCANPIX



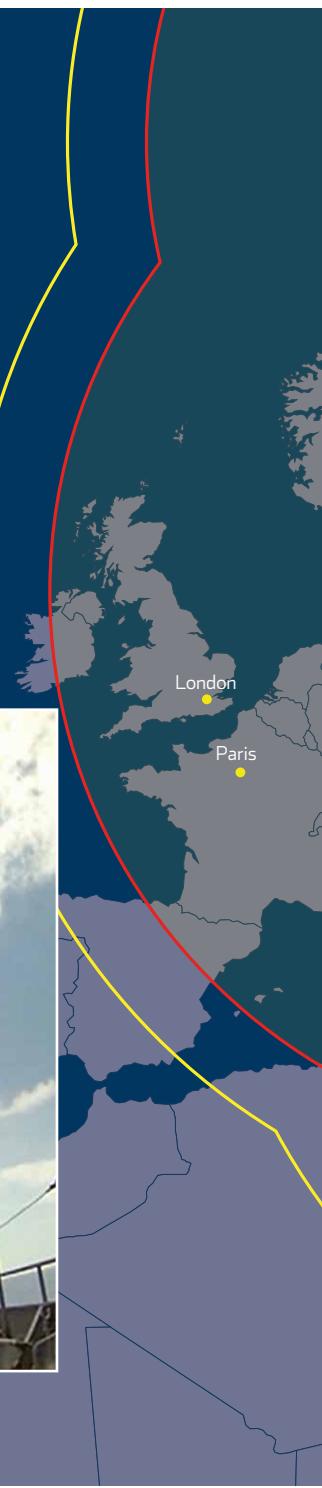
reactor is also questionable in the event of a failure of the system itself (rather than its power source); would the nuclear reactor that powers the system withstand a collision with the ground or ocean floor? In other words, Russia is being irresponsible simply by testing these systems, not to mention their possible introduction into its arsenal.

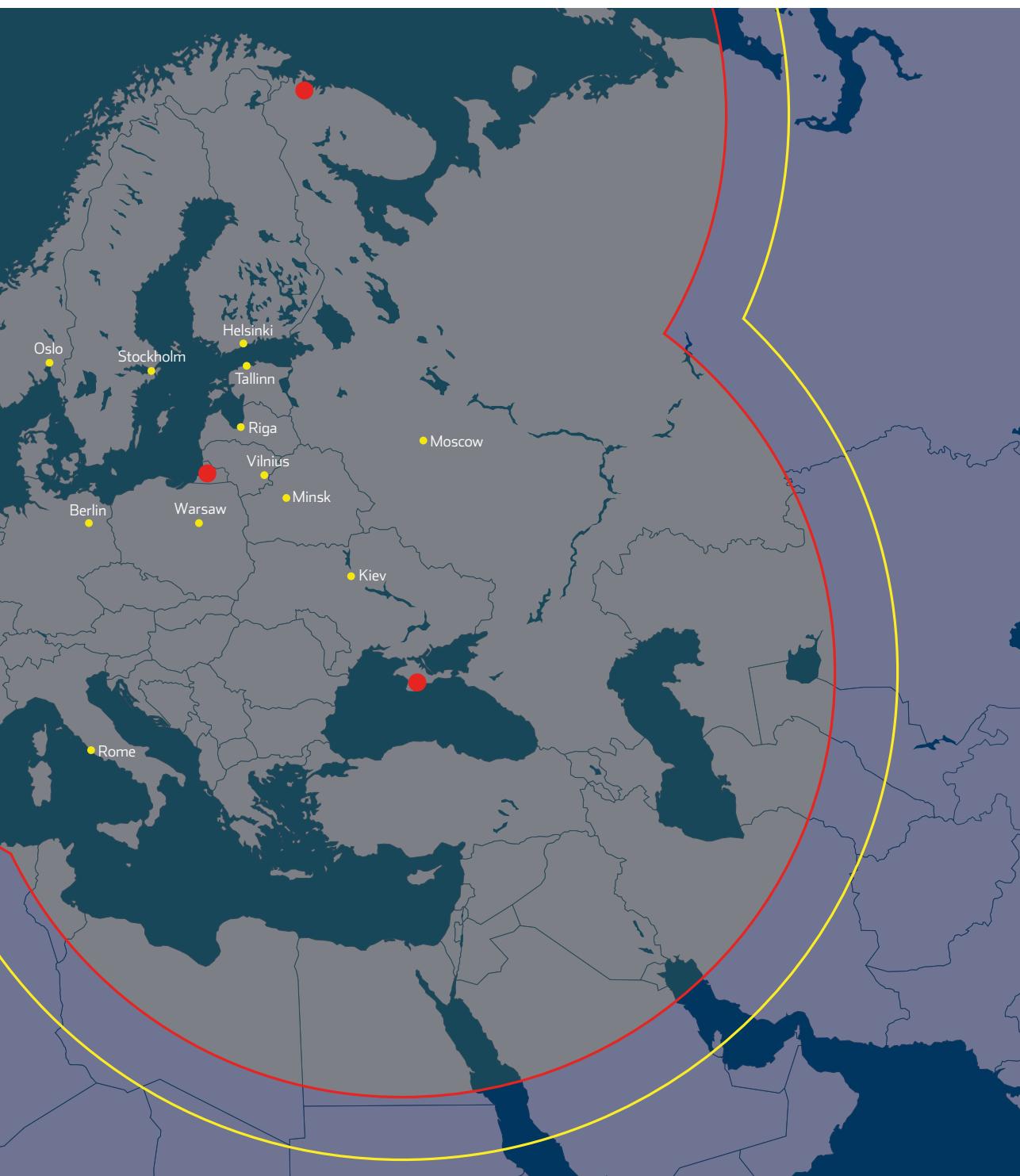
Despite repeated claims that some of these weapon systems are already at the disposal of the Russian armed forces, and others will be soon, only the Kinzhal has been presented to the public.

It should also be pointed out that in 2018, the Russian president gave his annual speech only two-and-a-half weeks before the presidential elections on 18 March. This was a carefully calculated step and part of his election campaign. The strong messages in Putin's speech were therefore primarily intended for the domestic audience. The balance of strategic nuclear capabilities between NATO and Russia will not be changed by the new weapon systems, even if they should make it into the arsenal of the Russian armed forces, but they do serve the propaganda purpose of presenting Russia as a global power.

THE MAXIMUM RANGE OF THE 3M-14 KALIBR CRUISE MISSILE

- 2,000 KM WITH A CONVENTIONAL WARHEAD
- 2,500 KM WITH A NUCLEAR WARHEAD





THE RUSSIAN CIVILIAN FLEET IN THE SERVICE OF NATIONAL SECURITY

European security services have observed the suspicious behaviour of Russian civilian vessels for some time. While it used to be research vessels that attracted attention, an increasing number of ordinary civilian vessels belonging to Russian companies and flying the Russian flag are now being monitored.

Characteristic of the suspicious behaviour of Russian civilian vessels are their attempts to enter the naval training areas of other countries or, on various pretexts, to access areas closed to ship traffic (testing areas for new military technology, surroundings of naval bases, etc.) and areas that are not normally used for navigation but pose an interest for strategic reasons. Attempts to enter foreign territorial waters without permission, under the pretext of needing shelter from storm or technical repairs, are becoming more and more frequent. This kind of behaviour clearly stands out in comparison with other ordinary civilian vessels.

The activities of Russian civilian research vessels over the past decade

may even be described as provocative. Attempts are made to enter the territorial waters of other countries based on formal requests; research is carried out in a semi-covert manner and in undeclared locations. The research activities focus on the host country's submarine communications networks, as well as areas of military and economic importance. As a rule, the crews of Russian research vessels avoid contact with local researchers.

The Russian civilian fleet and its activities are a potential security threat. As a Soviet-era anachronism, all vessels of Russian companies and state agencies that sail under the Russian flag are registered as mobilisation reserve vessels; exercises include rehearsing their conversion into support



*Training ship Mir moored in Tallinn,
September 2018.*

SOURCE: WWW.ROSMORPORT.RU/NEWS/COMPANY/28731/

RUSSIAN CIVILIAN
VESSELS ATTEMPT
TO ENTER THE NAVAL
TRAINING AREAS OF
OTHER COUNTRIES OR TO
ACCESS AREAS CLOSED
TO SHIP TRAFFIC.

vessels for the navy. What is more, the crews of the vessels of Russian companies and state agencies that sail under the Russian flag are to this day required to undergo combat training. The shipowners and crews must at all times be ready to perform national assignments, regardless of geographical location. In addition, the state surveillance system for

surface and underwater environment (*EGSONPO*), which was launched in 2015, requires the crews of all vessels of the Russian civilian administration that sail under the Russian flag to gather and report information on events at sea and in foreign ports. The operation and coordination of the system is the responsibility of the Russian navy.

A new and evolving development is the use of Russian civilian vessels for influence operations. A currently trending practice is to use the Russian state agencies' and educational institutions' large sailing ships, which participate in sea voyages, regattas and festivals around the world. Part of the voyages are political events for local Russian communities, propaganda re-enactments of selected episodes from Russian history, and missionary work by the Russian Orthodox Church involving open-air services, miraculous icons, and relics.

Politicians, local government officials, and business people visiting the ships receive particular attention. A good example is the training vessel *Mir* of the Saint Petersburg-based Admiral Makarov State University of Maritime and Inland Shipping. It is the permanent seat of the Seaborne Russian Centre (*Morskoi Russkiy tsentr*), an organisation run by the Russkiy Mir Foundation and aimed at Russian compatriots living abroad. The sailing ship *Mir* is a frequent guest at the Tallinn Maritime Days.

Russia's civilian fleet, then, is a kind of extension of its state authorities. When needed, it can be used to gather information, to pursue military objectives, or to carry out covert operations. More attention should be paid to civilian vessels sailing under the Russian flag, particularly to the conditions under which they are allowed to enter the territorial waters and stay in the ports of other countries.

RUSSIA'S CIVILIAN FLEET CAN BE USED TO GATHER
INFORMATION, TO PURSUE MILITARY OBJECTIVES,
OR TO CARRY OUT COVERT OPERATIONS.

RUSSIAN DOMESTIC POLITICS – TENSIONS ARE BUILDING



SOURCE: RIA NOVOSTI/SCANPIX

There is an increasing gap between what the ruling elite offers and what the wider population expects. The Kremlin is forced to make unpopular decisions, which raise tensions among the elite itself.

In domestic politics, the first half of 2018 was satisfactory from the Kremlin's point of view. Allowing for very limited freedom of opinion, precluding genuine political competition, and using the administrative

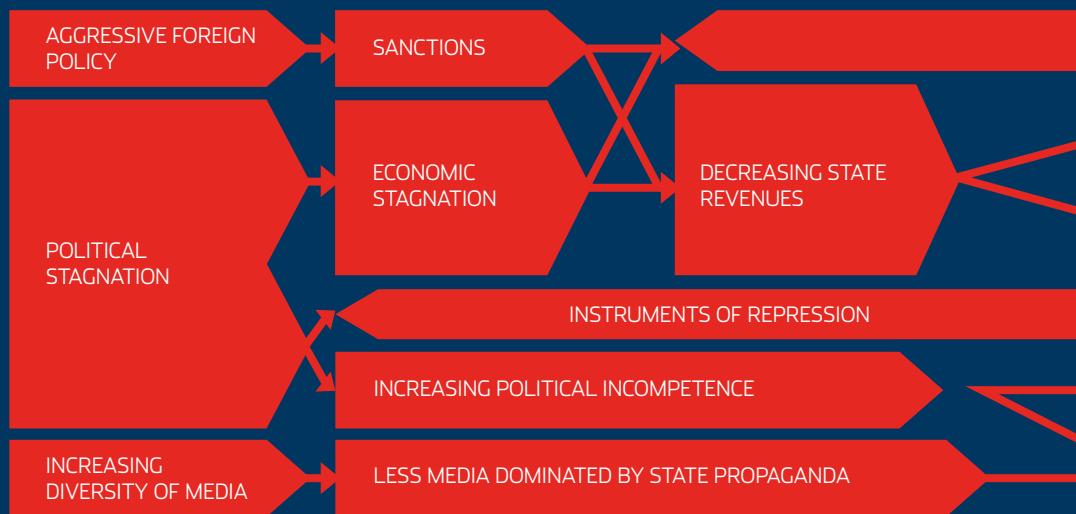
support of a biased state apparatus, Vladimir Putin was reinstalled as president for another term without any major setbacks, despite growing internal tensions. At the same time, the ranks of supporters of fundamental

change in the country increased, now significantly outnumbering those who value stability (see page 18). This telling trend suggests what the results of a genuinely free presidential election might have been.

The second half of the year proved more difficult for the ruling elite, as an unpopular pension reform exacerbated the public's already increased dissatisfaction. The Kremlin had a

rather hard time trying to silence the protests against the reform, and the events also had a significant impact on President Putin's ratings. At the same time, opinion polls showed that many more Russians had started to hold Putin responsible for problems facing the country. Unexpectedly to the Kremlin, the dissatisfaction with the elite and the ruling political party, United Russia, also manifested itself in the local elections that autumn. Although United Russia

INCREASING TENSIONS IN DOMESTIC POLITICS

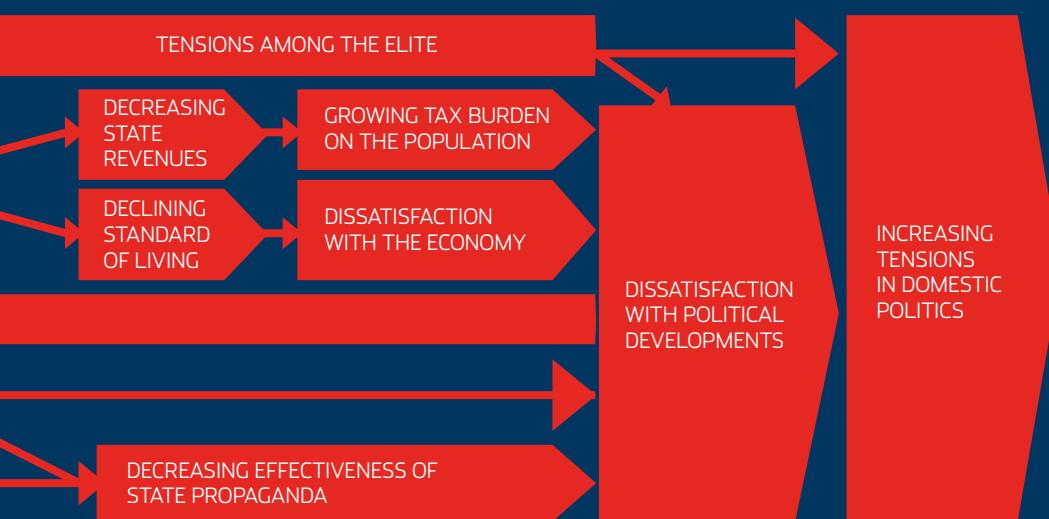


had no real political competitors in the elections, formalising its candidates' election victory met with difficulties in several places. The departments of the Presidential Administration responsible for curating domestic politics were not prepared for this and failed to react quickly enough when the first complications appeared. The upshot was that in the elections of the heads of federal subjects, the ruling elite was on several occasions forced to accept

an unplanned defeat by the candidates of pseudo-oppositional political parties operating with the Kremlin's approval (for example in the Republic of Khakassia).

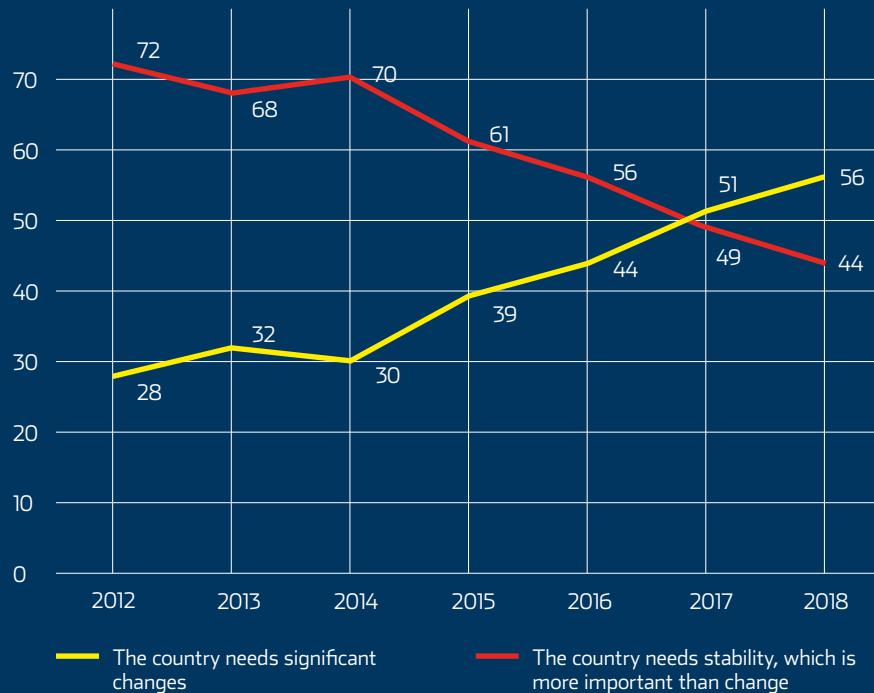
The great challenges of the autumn elections were even acknowledged at the United Russia annual congress, stating that the problem was due to the party candidates' lack of communication with the electorate

Alongside foreign policy problems, prioritising the needs of a small elite has triggered a causal chain that inevitably leads to the build-up of domestic political tensions.



POPULAR ATTITUDES TOWARDS DEVELOPMENTS IN RUSSIA

SUPPORTERS OF CHANGE VS. STABILITY



SOURCE: "РОССИЙСКОЕ ОБЩЕСТВО ПОСЛЕ ПРЕЗИДЕНТСКИХ ВЫБОРОВ – 2018: ЗАПРОС НА ПЕРЕМЕНЫ", ФНИСЦ РАН.

and indifference to their concerns. Although on a rhetorical level it was declared that these mistakes are to be avoided in the future, it is obvious that the problems arise primarily from the undemocratic logic of the system and will persist as long as the system itself remains in place.

After the 2018 presidential elections, the same people largely continue alongside Putin. With a “rule-until-I-die” mentality, Russia’s top leadership cannot meet the people’s expectations and implement change without going against their own personal

The most unpleasant surprise for the Kremlin was what happened in the Republic of Khakassia. Originally intended only as a prop for the show election to formalise the victory of the United Russia candidate, opposing candidate Valentin Konovalov significantly outperformed his United Russia counterpart in the first round and secured his election in the second. This is a good example of how easily a well-controlled political system can be shaken up by changes in the domestic political situation.

SOURCE: TASS/SCANPIX



interests. At the same time, President Putin is finding it increasingly difficult to convince the populace that all the problems can be blamed on the “bad boyars”, while retaining his credibility as the “good tsar”. The dissatisfaction spreading in society also creates

tensions in the country’s leadership, reducing its ability to solve problems effectively. The tensions among the elite and top officials and increased dissatisfaction among the public promise a very turbulent fourth term for President Putin.

A RISING TAX BURDEN WILL NOT BE MATCHED BY A HIGHER LEVEL OF DEMOCRACY

Many administrative functions organised at the national level, particularly health and education, have been systematically under-financed in Russia. For the state to continue functioning and the ruling elite to maintain its position, national revenues should increase substantially, but that would increase the tax burden, and with it, dissatisfaction. Channelling this dissatisfaction with a view to neutralising it remains one of the main challenges for the Kremlin.

Russian leaders are prepared to implement economic reform only to the extent that this is possible without causing unrest. Therefore, they are careful not to exceed a critical limit when introducing changes. At the same time, reforms would largely go against the interests of the ruling elite: the kleptocratic nature of the regime prevents a shift towards more efficient governance. For example, transparent and fair administration of justice would reduce the selection of repressive tools available to the system. Thus, the choice of instruments

for implementing change is limited; instead of decisive economic reform, we see a slow increase in the tax burden and a gradual reduction of public benefits, most notably the raising of the retirement age.

The tax burden on the Russian population may appear low compared to developed industrialised nations, but is remarkably high when taking into account the overall level of organisation of such societies.

The two empty corners of the diagram show that, although the democracy index may vary significantly between countries with similar tax burdens, a very low tax burden is never combined with a high level of democracy, just as no minimally democratic, or essentially autocratic, regime can justify a very high tax burden to its subjects. Russia and Cuba already clearly stand out from most other nations in the world in terms of these indicators.

As the Kremlin will try to shift Russia even further towards the *unpopulated bottom left corner* of the chart,

THE DEMOCRACY INDEX AND SHARE OF TAXES IN GDP



DATA FROM 2017

Russia's taxes are likely to increase faster than its GDP in the near future. Increasing the tax burden without providing additional social rights to the taxpayer will naturally meet with resistance. However, while counter-reactions are a sign of dissatisfaction,

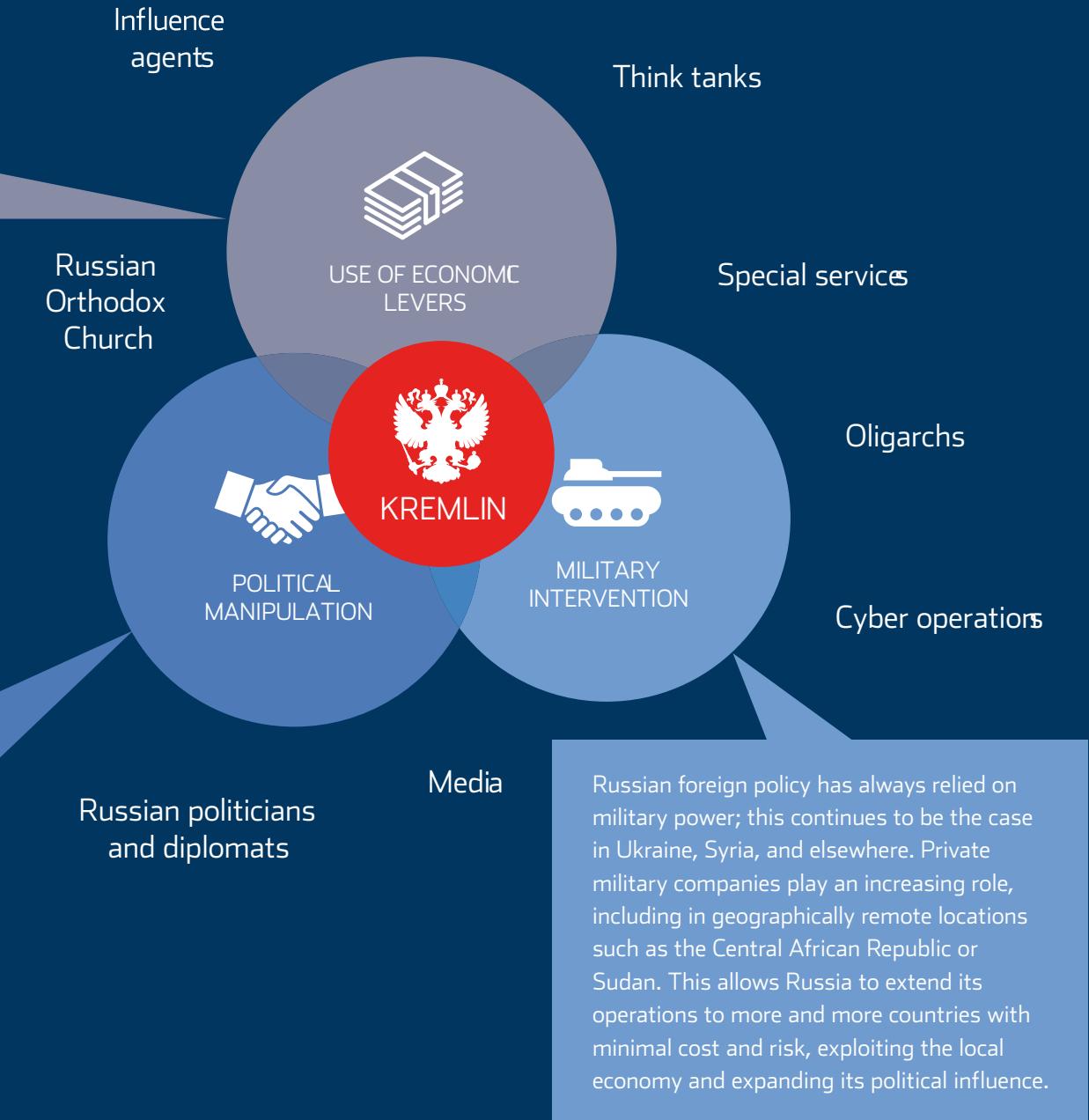
they need not ultimately move Russia *upward* on this scale, but may instead push it *back towards the left*, as Russia lacks a democratic social order, both in terms of current practises and historical traditions.

RUSSIAN FOREIGN POLICY

Russian foreign policy is closely related to the Russian elite's vision of the country as a major global power. Russia's behaviour in foreign politics is based on an adversarial stance toward the United States and the West in general, which in turn informs its policy in Europe and attempts to strengthen its influence in neighbouring countries. Russia is still pursuing an opportunistic foreign policy shaped by a very narrow circle of decision-makers, and employing political, economic and military means supported by Russia's government-controlled influence operations. It is therefore impossible to draw a clear line between Russian foreign policy on the one hand and influence operations on the other.

Russia makes particular use of international energy supplies to create energy dependence that would allow it to pursue its economic and political interests. Examples involving Europe are the Nord Stream 2 and Turkstream projects.

Its political tactics include demagogic and false accusations that are intended to deflect criticism aimed at the Kremlin. Recent examples of this are the poisoning of Sergey Skripal and the Kerch Strait incident. Such activities involve giving a major role to special services, oligarchs and the Kremlin's influence agents, as well as diplomats.



BELARUS – THE KREMLIN TIGHTENS ITS HOLD

Constant economic conflicts between Russia and Belarus and attempts by Belarus to pursue an independent foreign policy have caused the Russian leadership to worry about its influence in Belarus and increase pressure on the country's leaders.

With the beginning of Putin's fourth term of office in May 2018, Russia stepped up its efforts to tie Belarus more tightly to Russia. Putin and the Belarusian president Alyaksandr Lukashenka met more often in the second half of 2018 than during the whole of 2017.

A sign of Russia's intention to reinforce its control over Belarus is the appointment in summer 2018 of Mikhail Babich, who has previously worked in the Russian special services, as the new ambassador and the president's special representative for trade and economic cooperation.



With no previous experience in diplomatic work abroad, Babich has broad powers as a special representative to promote Russia's interests in Belarus and influence the Belarusian leaders toward compliance with Russia's wishes. Babich's predecessor, Alexander Surikov, worked in Belarus for more than 12 years and had begun to adopt its point of view, sometimes justifying steps taken by the



Belarusian president and government that were unacceptable to Russia. In contrast to Surikov, Babich is not afraid of conflict with the Belarusian authorities and president.

Disagreements persist in areas that significantly affect the Belarusian economic situation, such as compensation to Belarus for amendments in the taxation of oil and petroleum products



Babich and Lukashenka at the Forum of Russian and Belarusian Regions in October 2018.

SOURCE: MID.RU

from Russia, restrictions placed by Russia on food products from Belarus, and the price of natural gas until 2025. According to Belarusian economic analysts, the country stands to lose 10.8 billion dollars due to the tax amendments by the year 2025.

Russia is paying more attention to its loss of budgetary revenue due to support granted to Belarus, and it increasingly ties support to a requirement for Belarus's greater integration with Russia within the Union State framework, which involves common customs, excise, taxation, judicial and currency policies. Disagreements between Russia and Belarus on economic issues will sharpen in 2019, which may once again lead to pressure on Belarus to sell its strategic enterprises to Russia.

The Russian government is also pressuring Belarusian leadership through

Russian national media. A number of critical articles were published in 2018 about President Lukashenka, accusing him of favouring Ukraine in his foreign policy and publicising information about his incapacity for work as a result of an alleged stroke. Articles have been published regularly about Putin's dissatisfaction with Lukashenka's activities and about the Kremlin exploring opportunities to remove Lukashenka from power in the coming parliamentary and presidential elections.

In addition to propaganda and pressure aimed at the Belarusian leadership, Russia has made intensive attempts to influence public opinion in Belarus since at least 2016. For example, the Russian federal agency Rossotrudnichestvo is extending its activities to all major cities in Belarus.

Websites and supposedly independent expert bodies have been set up to promote the idea of unity between Russia and Belarus. Websites administrated from Russia have been opened in Belarus, offering alternative information to counter the local press and support the ideology of the Russkiy Mir Foundation.

Russia is forced to strengthen its influence in Belarus in order to control the country's leadership. Therefore it is likely to increase its pressure on Belarus as the 2020 Belarusian presidential and parliamentary elections approach. Economic disagreements persist and fuel media campaigns speculating about the replacement of President Lukashenka with a more Russian-minded person, and about the demise of Belarusian independence.

**RUSSIA IS FORCED TO STRENGTHEN ITS INFLUENCE
IN BELARUS IN ORDER TO CONTROL
THE COUNTRY'S LEADERSHIP.**

RECENT RUSSIAN PROPAGANDA PLATFORMS FOR PRESSURING BELARUS

| LOGO | NAME | YEAR OF ESTABLISHMENT | ACTIVITY/TASKS |
|---|--|-----------------------|---|
|  | Russian-Belarusian Expert Club | 2016 | Develops recommendations for tighter integration of the two countries within the Union State and Eurasian Economic Union framework |
|  | Druzya-Syabry community for Russian and Belarusian journalists | 2016 | Promotes the idea of the inseparability of Belarusian and Russian national interests |
|  | Russian and Belarusian historians' Joint Initiative for Memory and Unanimity | 2017 | Discusses Russian and Belarusian past and present problems so as to stress the two countries' historically "productive relationship" within one state under Russian rule. |
|  | Sonar-2050 | 2017 | Promotes the idea of unity of Russia and Belarus |
| | Club of Editors-in-Chief | 2018 | Brings together the heads of the leading media outlets of the two countries |

UKRAINE – HOSTILITIES CONTINUE

Russia's aggression is aimed at bringing about changes that would place Ukraine firmly within its sphere of influence or, at least make it difficult for Ukraine to move closer to the European Union and NATO.

Although Russia agreed in the 1994 Budapest Memorandum to respect Ukraine's independence, sovereignty and borders, it continues to apply military and non-military pressure to Ukraine. The intensity of military activity in Donbas decreased in 2018 due to a certain change in methods rather than the cooling off of Russia's aggression. Ukraine is the target of constant information attacks by Russia, which seeks to undermine its statehood and national identity, among other things. For example, Russia claimed that the creation of an independent Ukrainian Orthodox Church would lead to bloodshed. There is evidence of Russian special services' attempts to damage Ukraine's relations with its neighbours, as Russia tries to discredit Ukraine in the international arena.

Russia increasingly focuses on direct antagonism toward Ukraine, since the proxy war staged in Donbas has failed to break Ukraine's resistance. Open

confrontation is evident from Russia's behaviour on the Sea of Azov and Black Sea, where the Russian navy and border guard vessels are prepared to open fire against Ukrainian warships, as they did on 25 November 2018, to prevent their passage through the Strait of Kerch. Russia is also taking less care to conceal its role in the war in Donbas. For example, in 2018 the OSCE Special Monitoring Mission detected Russian army columns crossing the state border and entering occupied Ukrainian territory. It also discovered modern weapons and special equipment in Donbas which indisputably had to come from Russia.

Russia is increasingly shifting its focus to non-military pressure. The most important method is to paralyse gas transit, an important source of income for Ukraine, by way of building Nord Stream 2. Russia is also interfering with inbound civilian maritime traffic to Ukrainian ports on the Sea of Azov, intentionally slowing down the passage through the Strait of Kerch, and

ATTACKS AGAINST THE UKRAINIAN ARMED FORCES IN DONBASS 2018



SOURCE: DATA FROM THE NATIONAL SECURITY AND DEFENCE COUNCIL OF UKRAINE

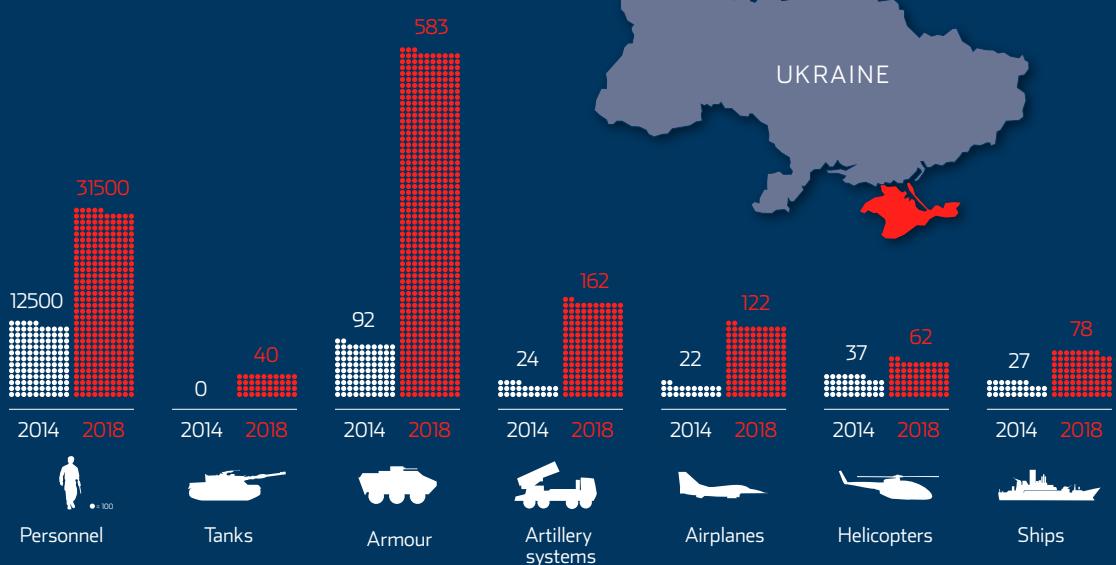
repeatedly conducting pointless inspection raids of ships that have already entered the Sea of Azov. These methods considerably increase the costs for ships that visit Ukrainian ports.

Pressure on Ukraine leading up to the presidential election at the end of March and parliamentary elections in autumn will probably be the most important political instrument available for Russia in 2019. Before the Russian presidential elections in 2018, fighting in Donbas had lulled for several months, only to flare up again as soon as the elections

were over. It is very likely that the Russian government will manipulate the intensity of the fighting in Donbas to influence the Ukrainian election results in a way that suits them.

In 2018, the intensity of fighting in Donbas mirrored events in Russia rather than Ukraine (see graph), which once again indicates the extent of control that Russia exercises over the conflict. No escalation occurred when Kiev declared martial law following the Kerch incident, as Russia sought to play down the importance

RUSSIAN MILITARY PRESENCE IN CRIMEA 2014 AND 2018



SOURCE: INFORMNAPALM.ORG, SEPTEMBER 2018.

of the incident and present Ukraine's response as a nervous overreaction.

Although the fighting in Donbas has grown less intense, Russia keeps military pressure on Ukraine by reinforcing its units in annexed Crimea and elsewhere on the Ukrainian border. The

purpose of strengthening the forces is to position Russian units and equipment for possible offensive operations deep into Ukraine in the event of a broader confrontation, and effectively prevent the arrival of international assistance into the country.

RUSSIA INCREASINGLY FOCUSES ON DIRECT ANTAGONISM TOWARD UKRAINE, SINCE THE PROXY WAR IN DONBAS HAS FAILED TO BREAK UKRAINE'S RESISTANCE.

THE SOCIO-ECONOMIC SITUATION IN CRIMEA AND EASTERN UKRAINE

Almost five years since the unlawful annexation of Crimea and the establishment of the so-called people's republics in eastern Ukraine in the wake of Russian aggression, life in these areas has not improved, contrary to the intensive Russian propaganda. The average income and pension in Donbas are several times lower than in Ukraine, Crimea or Russia. The average salary and pension are higher in Crimea than elsewhere in Ukraine, but below the Russian average. Moreover, the purchasing power of Crimeans is low because of the high cost of food and public utilities. Most of the products available are Russian; while Ukrainian products are also available, their sale is officially prohibited in these regions.

The Kerch Strait bridge, which was opened in May 2018, has not provided the promised alleviation to the socio-economic situation in Crimea. Crimeans living near the bridge use it to travel to Krasnodar for cheaper fuel and other products.

In 2018, the average number of daily crossings on the line of contact that

separates the Russian-occupied areas in eastern Ukraine from the rest of the country was 33,500; this represents a 31 % increase compared to 2017.¹ More than half of those travelling across the line are pensioners from the unrecognized people's republics, who head to the Ukrainian-controlled areas to pick up their pensions every two months, as they cannot cope on the pension paid in the occupied Donbas. People living in the occupied areas travel across the contact line more and more often to purchase cheaper and better-quality Ukrainian goods, among other things. There are just five crossing points along the line, only one of which is in the Luhansk region; this means a long journey to the unoccupied part of Ukraine.

Many people have left Crimea and the so-called people's republics in eastern Ukraine to seek better working and living conditions elsewhere in Ukraine or Russia. Medical workers who receive very small salaries² at a huge workload

1 Data from the United Nations High Commissioner for Refugees.

2 An average of 8,500 roubles (105 euros).

A photograph taken near the crossing point on the line of contact between the so-called Luhansk People's Republic and the Ukrainian-controlled areas. It shows the poor situation of the people in the occupied areas: they are willing to walk a long way to receive their Ukrainian pension in addition to the local pension and to buy Ukrainian goods that are often cheaper and of better quality than those sold in the separatist area.

SOURCE: RFE/RL



continue to leave. The population of Crimea (2.3 million) has not changed significantly since the annexation, as the 200,000 inhabitants who left the peninsula have been replaced by a similar number of Russians and residents from Donbas. Retired people and others who do not want to leave their homes have stayed. Their decision is partly due to propaganda by the people's republics and Crimean authorities, which depicts life elsewhere in Ukraine as being even worse.

About two-thirds of the budget of the so-called Republic of Crimea and so-called people's republics in eastern Ukraine comes from Russia. Crimea is among the five Russian regions receiving the most support. Russia's priorities include the building of infrastructure for its military bases in Crimea and providing both political and military support to the people's republics in eastern Ukraine, so as to destabilise the situation in Ukraine. The welfare of the people of these areas is a secondary concern for Russia.

THE ACTIVITIES OF THE RUSSIAN ORTHODOX CHURCH IN UKRAINE

The year 2018 will be remembered for the blow on Russian policy in the Orthodox world, as Russia's attempts to thwart the creation of an independently recognised Orthodox Church of Ukraine failed. However, this does not diminish the importance of the Russian Orthodox Church as a tool for the Kremlin.

For centuries, Russia has used the need to protect the Orthodox community as a pretext to intervene in the affairs of other countries. Under Stalin, the Soviet regime tried to use the remnants of the Russian Orthodox Church, which had suffered immensely under communist terror, to influence its people and foreign countries, and the church was subordinated to the special services. The Russian Orthodox Church suits the Kremlin propaganda purposes as an imaginary soft force for Russia. Having transformed it into a de facto state church, the Kremlin is interested in using the institution as a decoration and defender of the legitimacy of the regime, which is why Patriarch Kirill, who has led the Church since 2009, has enjoyed the constant political and financial support of the Russian leadership.

The Russian Orthodox Church has been an important tool for the Kremlin's influence operations in Ukraine. The Church's leadership participated in subversion operations against Ukraine

for years before Russia's open aggression against Ukraine in 2014. During Russia's offensive in Ukraine, it became increasingly difficult for the Church to support Russian forces and puppets in Donbas, while maintaining the facade of an independent "Ukrainian Orthodox Church". The Ukrainian authorities and supporters of independence resented the fact that the Ukrainian Orthodox Church of the Moscow Patriarchate – the local franchise of the Russian Orthodox Church – was being used as a front by the Russian special services. An example of this was the open support for the "separatists" shown by numerous clergymen: they participated in the operations of Russian special forces, rallied support for Moscow policies in their congregations, and staged provocations for Russian special services.

In April 2018, the representatives of two Orthodox churches in Ukraine, along with government representatives, turned to the head of the global Orthodox Church, Ecumenical Patriarch

Bartholomew I of Constantinople, pleading with him to grant independence, or autocephaly, to the Ukrainian Orthodox Church. Under orders from the Kremlin, the Russian Orthodox Church responded by launching a defamation campaign against Ukraine and the Ecumenical Patriarchate. The leaders of the Church's Ukrainian branch were ordered by Moscow to initiate petitions and demonstrations against autocephaly. The Church's foreign relations department, employed peculiar shuttle diplomacy to gain the support of other Orthodox churches. Despite the resources spent, the international defamation campaign was not successful and instead damaged existing relations. Similarly unsuccessful was the persuasion work done by the "Orthodox" propaganda associations³ linked with the special services and Sergei Gavrilov, the Russian MP elected as the president of the Interparliamentary Assembly on Orthodoxy, and Russia's instruments for implementing

its compatriots abroad policy, which includes the Russkiy Mir Foundation and the federal agency Rossotrudnichestvo.

On 11 October 2018, the Ecumenical Patriarchate decided to grant autocephaly to the Orthodox Church of Ukraine. In response, the Russian Orthodox Church demonstratively broke off relations with the Ecumenical Patriarchate. Among its other branches, the Estonian Orthodox Church of the Moscow Patriarchate also joined the propaganda campaign against the Ukrainian Church. The head of the Estonian Orthodox Church of the Moscow Patriarchate, Metropolitan Yevgeny (secular name Valery Reshetnikov), who was appointed by Moscow in spring 2018, had visited annexed Crimea already in spring 2014 as the then rector of the Moscow Theological Academy and Seminary.

Seeing the ineffectiveness of the Church leadership, the Kremlin intervened more visibly and aggressively. On 12 October 2018, the Security Council of Russia led by President Vladimir Putin discussed the situation of the Russian Orthodox Church in Ukraine. Kremlin press secretary Dmitry Peskov announced that Russia would defend the Orthodox community by political and diplomatic means the same way that it defends

³ For example, the Double-Headed Eagle Society of the oligarch Konstantin Malofeev, the Imperial Orthodox Palestine Society of the first FSB head Sergei Stepashin, and the Foundation of Saint Andrew the First-called of Vladimir Yakunin, who has a foreign intelligence background.

Russian-speakers abroad. Nevertheless, Moscow seemed to have exhausted its countermeasures. On 15 December 2018, the unification council of the Orthodox churches of Ukraine was held in Kiev to establish the Orthodox Church of Ukraine and elect its primate. On 16 January 2019, Ecumenical Patriarch Bartholomew I granted the Orthodox Church of Ukraine a formal decree, or tomos, of autocephaly.

Although the responsibility for breaking up and weakening the Russian Orthodox Church in Ukraine actually lies with Putin's government, the Church leadership and Patriarch Kirill, who carefully followed the Kremlin's orders, were made scapegoats.

The defeat in Ukraine has deepened disagreements among clerics and congregations within the Russian Orthodox Church. Patriarch Kirill's domineering style of leadership and the corruption of the church leaders are causing disapproval. A considerable number of clerics think that the patriarch's likely successor to lead the Church out of the crisis will be Tikhon, who in May 2018 was appointed Metropolitan for Pskov and Porkhov, and is nicknamed Putin's personal confessor because of the President's favourable

attitude toward him. A much more skilled and balanced communicator than Patriarch Kirill, Metropolitan Tikhon finds that Kirill is to blame for losing the Ukrainian Orthodox Church. Nevertheless, Tikhon and Kirill share close ties with the Russian secret services. By participating in the Irzborisk Club, which disseminates Russian propaganda, and conducting a "patriotic" historical propaganda campaign for youth, Tikhon seeks to consolidate the Church and cultivate an anti-Western stance that dovetails with the Kremlin's current line.

Regardless of the lessons learned in Ukraine and the choice of future church leader, the Russian Orthodox Church will remain dependent on the government and special services and will continue to be exploited in official propaganda to the same extent as before. Russia's propaganda campaign against the Ukrainian Orthodox Church, which used the church and religious communities, should make it clear to other countries that in the event of Russian aggression, the leaders of the Russian Orthodox Church and its branches posing as national Orthodox churches will side with the Kremlin rather than show solidarity with the victims of aggression.

TRANSCAUCASIA – MOSCOW’S INFLUENCE RELIES ON THREATS

In 2019, Russia will continue to pursue its Transcaucasian policy to maintain and, where possible, improve Moscow’s positions and to undermine and fend off Western influence.

Transcaucasia is a strategically important area for the Kremlin. This is partly due to security considerations: Moscow regards the Caucasus Mountains as the last natural defence barrier between southern Russia and a hostile outside world, while the three Transcaucasian nations are a buffer zone in front of this barrier. Russia uses influence and information operations as well as economic measures to preserve this buffer zone. If necessary, Moscow is likely prepared to threaten the use of military force.

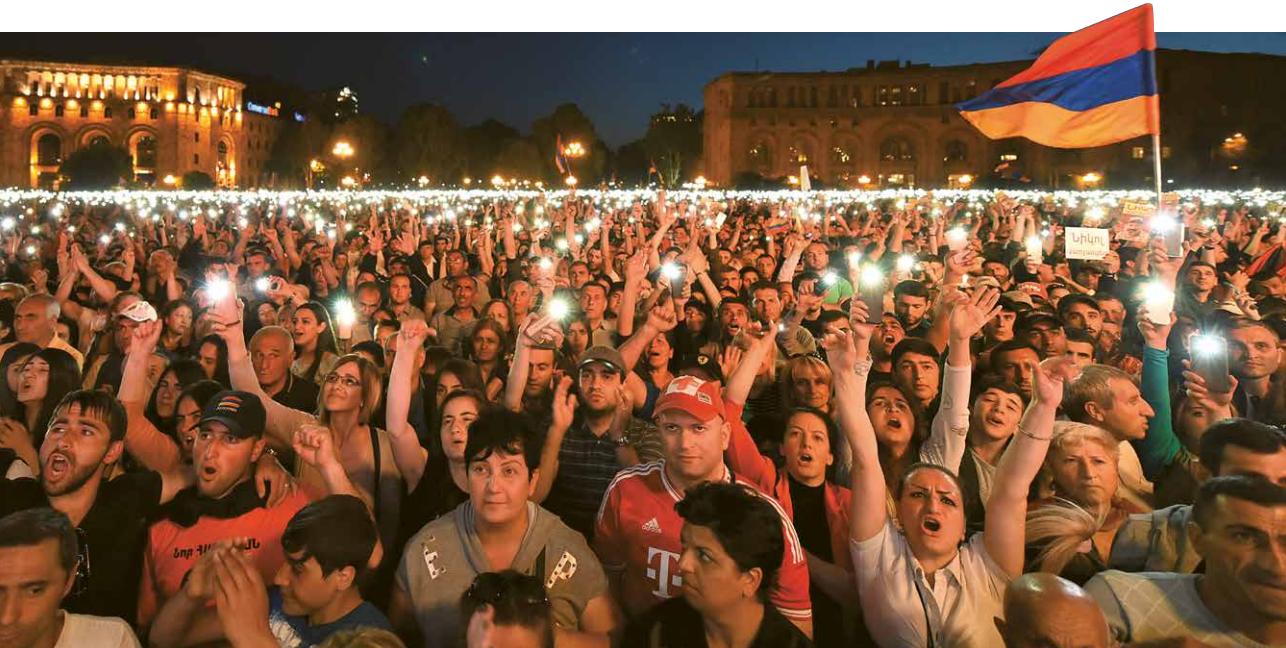
At least equally important is the fact that the Russian leaders are convinced that Georgia, Armenia, and Azerbaijan are part of the “Russian world”, both historically and today, and are not entitled to full sovereignty. Russia’s strategic objectives with each of these countries are somewhat different.

It would like to keep Georgia in a “grey zone”, to prevent and decelerate

Georgia’s further approach to the European Union and NATO, while blocking and undermining Western influence in Georgia.

In Armenia, Russia wants to maintain its current positions and influence. There are Russian military bases in Armenia and a number of critical infrastructure businesses are owned by Russian capital. Armenia is a member of the Eurasian Economic Union, the Commonwealth of Independent States, and the Collective Security Treaty Organisation. The Armenian and Russian military commands are integrated to an extent.

In Azerbaijan, Russia seeks to strengthen its political influence in the inner circle of President Ilham Aliyev and increase the holdings of Russian businesses in strategic areas of the Azerbaijani economy. Azerbaijan has gained economic importance for Russia as a result of Western economic



↑ *The Velvet Revolution in spring 2018 placed Armenia in the spotlight both in the West and in Russia, and gave hope for the emergence of a genuinely democratic state governed by the rule of law.*

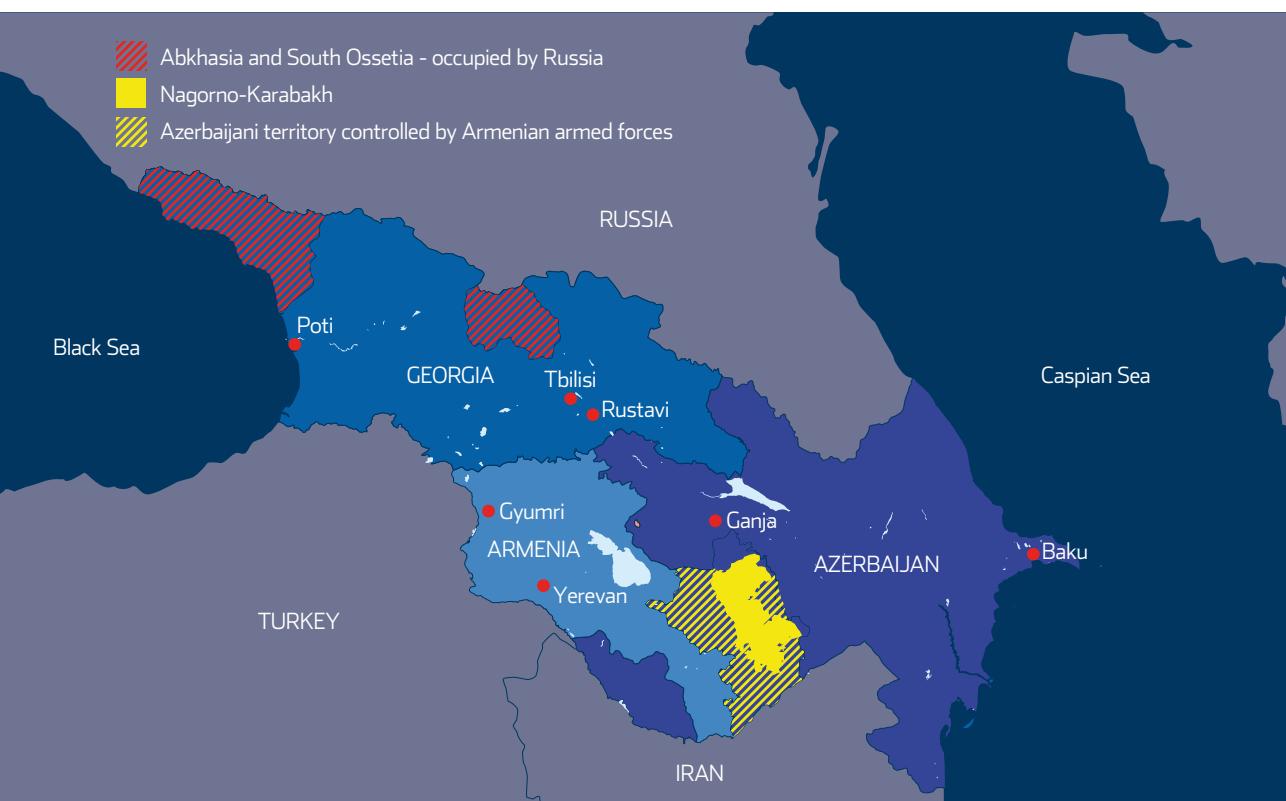
SOURCE: AFP/SCANPIX

sanctions. The Russian leadership is therefore making considerable efforts to create a strategic transit corridor through Azerbaijan, granting Russia access to the Iranian and Indian railway networks, and from there on to the Persian Gulf area and Asian markets and trade flows.

Russia's strategic levers in Transcaucasia are its military presence, weapon sales, and the use of conflicts to further its own interests. The Russian armed forces have established military bases with the capability of a brigade battle group in the annexed areas of Abkhazia and South Ossetia, which allows Russia to apply military pressure on Georgia. The conflict

in Nagorno-Karabakh in turn gives Moscow an opportunity to influence the relations between Armenia and Azerbaijan; allied relations with Russia are the main security guarantee for Armenia and make Russia a critical partner for Azerbaijan.

Russia supplies weapons to both Armenia and Azerbaijan, lest either gain decisive military dominance. The final resolution of the conflict over Nagorno-Karabakh by military, diplomatic, or other methods would sharply reduce Russia's influence in the area, as neither Armenia nor Azerbaijan would then need to be in Moscow's good graces to settle their existential security concerns.



In 2019, Moscow will pay special attention to developments in Armenia. The Velvet Revolution that brought Prime Minister Nikol Pashinyan to power in 2018 was an unpleasant surprise for Russia. In the Kremlin's eyes, the situation is remarkably similar to the earlier "coloured revolutions" in Georgia and Ukraine, which is why Russia takes a sceptical view of both Pashinyan and Armenia's new leadership. It sees their activities as a potential risk to its geopolitical interests regardless of Pashinyan's assurances to keep the Armenian foreign and security policies unchanged.

Therefore, while publicly declaring that it would not interfere with Armenia's internal affairs, Russia is actually trying to use its influence to hinder and undermine Prime Minister Pashinyan and his team's reforms in every way possible. After all, the reforms initiated by Pashinyan and Armenia's new leadership seek to dismantle the corrupting influence networks of the old political and economic elite that ran the country under Presidents Robert Kocharyan and Serzh Sargsyan and used to be the Kremlin's most effective lever in Armenia.

RUSSIA'S INTEREST IN THE EUROPEAN PARLIAMENT ELECTIONS

The Kremlin is very likely to try to intervene in the European Parliament elections to secure as many seats as possible for pro-Russian or eurosceptical political forces.

In May 2019, EU member states will elect the European Parliament for the next five years. The parliament as the only EU institution elected directly by the people is a considerable target for Russian influence operations. Russia has attempted to influence the EU's decision-making processes through elected members of parliament, used the parliament as a propaganda platform, and achieved direct contact with European politicians. Russia's goal is to continue to undermine the EU's unity by sowing disorder and disbelief in and between the member states. Members of the European Parliament (MEPs) are elected in all EU countries using a proportional election system, which favours the inclusion of small and marginal political parties in the representative body. The typically low turnout makes it more likely that stronger-motivated political forces

bring their supporters to the ballot boxes, and Russia can use a smaller but concentrated effort to mobilise an electorate that meets its needs.

MEPs can also be used as spokespersons for propaganda in Russia. Having placed itself in political isolation through its own behaviour, the Russian leadership attempts to convince its domestic audience that Russia is not alone and has considerable allies on the European political arena; it is only the so-called "Washington-led Brussels elite", which has not been elected by the people, that refuses to listen to Russia. Since the start of Russia's aggression against Ukraine, some MEPs have spread the view that the sanctions against Russia have had no impact on Russia, are harmful only to EU member states themselves, and only serve the interest of the United States. The same MEPs have justified

The Kremlin seeks to use European politicians by inviting them to events such as the annual Yalta International Economic Forum held in Russian-annexed Crimea. The photograph shows EU politicians at the forum in April 2016 during a breakfast session hosted by Sergey Aksyonov (so-called prime minister of Crimea).



the annexation and occupation of parts of Ukraine.

A new approach to influencing the European Parliament could be observed at the annual European Russian forum in Brussels in November 2018, as Russia threatened the EU with military conflict. An event hosted by the MEP Miroslav Mitrofanovs, but actually organised by Russian authorities, intentionally promoted the

message that if Europe disregards Russia's "justified interests" in the "near abroad", then Russia will be prepared to go to war. Mitrofanovs coordinated this assignment with persons with close ties to the covert influence operations of the presidential administration of Russia. Even though the event itself had a negligible impact, it illustrates how Russia is able to exploit MEPs for disseminating propaganda.



SOURCE: FACEBOOK

From the left:

JAROMÍR KOHLÍČEK (MEP, member of the Communist Party of Bohemia and Moravia, Czech Republic)

ALEXANDER ROBERT STELZL (assistant to former Austrian MEP Ewald Stadler)

BARBARA ROSENCRANZ (currently member of the Free List Austria party, which advocates leaving the EU; member of the Freedom Party of Austria (FPÖ) until 2017)

STEFANO VALDEGAMBERI (member of the Regional Council of Veneto from the Lega party)

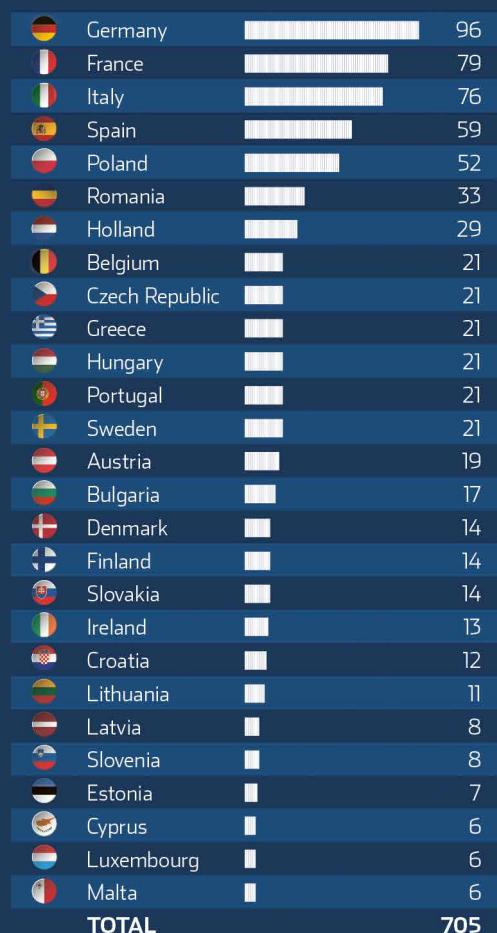
MARKUS FROHNMAIER (German MP since 2017, member of the Alternative for Germany (AfD) party)

Also present at the table were Axel Kassegger (Austrian MP, FPÖ) and Marcus Pretzell (MEP; has since left AfD, and has been a member of the Blue Party since 2017).

When intervening in the 2019 European Parliament elections, the Kremlin is likely to focus on the larger member states – Germany, France and Italy – where it can hope to obtain the most mandates (about one third of the MEPs come from these countries) and where some of the political parties have clearly expressed support to the current Kremlin policies towards the West. Russia's previous interference in Western elections

has shown that it acts on the principle of "the end justifies the means". Russia supports its allies through Russian-controlled media, organises high-level meetings and visits that attract media attention, offers covert financial assistance if necessary, discredits opponents (by stealing and leaking internal information), intentionally spreads false information in social media, and so on. Such activities require the involvement

APPORTIONMENT OF SEATS IN THE EUROPEAN PARLIAMENT TO BE ELECTED IN MAY 2019¹



Source: European Parliament

1 In case Britain leaves the EU

of a number of institutions, companies and networks that follow strategic goals approved by the Kremlin.

Due to differing domestic interests the anti-EU and pro-Russian political movements have not been able to create an effective umbrella organisation in the EU or a European Parliament faction, but this may change if the election results are favourable. Considering the security threat posed by Russia for many European countries it would be an additional risk to have a group of MEPs who intentionally promote Kremlin's policies.

Even if it does not pull any strings to form a "right-wing populist international", Moscow is certain to approach and use right-wing populist circles in its interest. It has previously done the same with the political associations that the Kremlin sees as its potential allies. For example, Russia has previously used politicians from the German AfD and the Italian Lega who have continuously demanded that the EU abolishes its sanctions against Russia.

NORD STREAM 2 AND TURKSTREAM AS SECURITY RISKS

Construction work on the Nord Stream 2 and TurkStream natural gas pipelines from Russia to Europe will reach a decisive stage in 2019: decisions will have to be taken about the above-ground extensions of the second branch of TurkStream to Southeast Europe, and the installation of Nord Stream 2 in the Baltic Sea should be completed.

B

oth pipelines would increase the dependence of European countries on Russian natural gas:

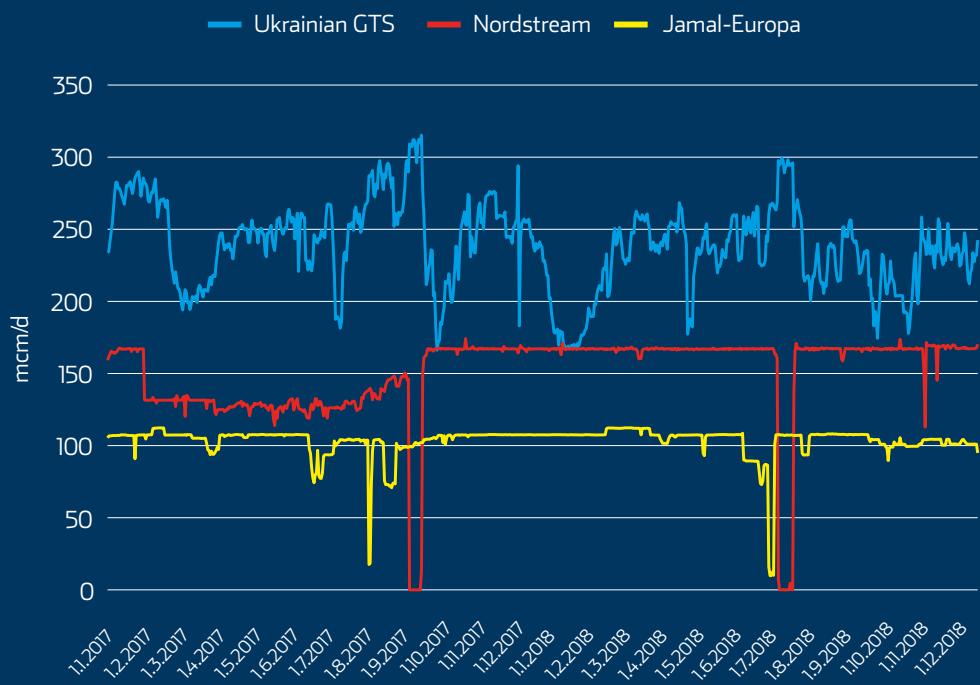
- » They will tie consumers to their services for a long time and complicate the establishment of alternative supply channels, such as connections between countries or LNG terminals, as investments in these two pipelines have to pay off.

- » They threaten the security of supply, as they cannot match the flexibility of the Ukrainian natural gas transmission system (GTS). Unlike the Ukrainian GTS, the existing Nord Stream and Yamal–Europe pipelines do not have underground storage sites, which allow to supply natural gas at short notice if needed.

**NORD STREAM 2 AND TURKSTREAM WILL GIVE RUSSIA
AN ADDITIONAL POLITICAL LEVER TO INFLUENCE
EUROPEAN COUNTRIES.**

RUSSIAN NATURAL GAS EXPORT TO EUROPE

THROUGH THE NORD STREAM PIPELINE AND THE UKRAINIAN GAS TRANSMISSION SYSTEM (GTS) IN 2017-18



- » They are built to serve the business interests of a small number of European companies, disregarding the broader security concerns of the region. If Russia no longer needs natural gas transit via Ukraine, an important obstacle to extending aggression from Donbas to the neighbouring oblasts will be lost.

Nord Stream 2 and TurkStream will give Russia an additional political lever to influence European countries. This is confirmed by Russia's success so far in winning support for Nord Stream 2 and for the second branch of TurkStream among politicians in Southeast Europe.

THE FAILURES OF RUSSIAN SPECIAL SERVICES IN THE WEST

An increasing number of officers and recruited agents of the Russian security and intelligence services have been caught in the West in recent years. What does this indicate?

Between 2014 and 2018, the media reported the exposure of officers of Russian special services (the FSB, SVR and GRU) or their recruited agents in Ukraine, Poland, Lithuania, Latvia, Estonia, United States, Portugal, Austria, Canada, Belgium, and elsewhere. The failures of the Russian military intelligence service, the GRU, in particular

have received wide media coverage: the attempted coup in Montenegro in 2016, the poisoning of Sergei Skripal in Salisbury in 2018, and the uncovering of a cyber-espionage operation in the Hague in 2018.

After the attempted murder of Skripal, nearly 30 Western countries and their allies expelled more than 150 Russian

Russian Military Intelligence headquarters

SOURCE: REUTERS/SCANPIX



spies who had posed as diplomats. Intelligence officers using diplomatic work as a cover are protected by diplomatic immunity, thereby eluding arrest and trial when exposed. They are usually declared personae non grata in the host country and sent home, either with a media uproar or without any. Exposed intelligence officers who are not protected by diplomatic immunity do not necessarily face charges either; it may be preferable to return them home quietly to avoid scandal. Recruited agents caught abroad, Russian or otherwise, are usually tried in the country where they were caught.

After the outbreak of the Russian-Ukrainian conflict in 2014, an intense confrontation between Russian and Ukrainian special services began and is still ongoing; dozens of Russian agents have been exposed in Ukraine as a result. They were typically recruited among the locals to gather intelligence but also to commit acts of

sabotage and murder. Most of them had no access to important secrets, performed simple tasks, such as observations and photographing, and received modest training. However, the exposed agents did include some who had been more valuable sources of information for the Russian special services, such as members of the police force, military, and special services.

In recent years, the Russian special services have also suffered many exposures in the Baltic States; the numbers are unprecedented since the Cold War. Between 2014-18, Lithuanian, Latvian and Estonian authorities have reported the exposure of six, three, and 13 (a total of 22) Russian agents or intelligence officers, respectively. Most have been convicted, and others are still under investigation. Among the agents exposed in Estonia, eight were recruited by the FSB and five by the GRU. As in Ukraine, most of the agents caught in the Baltic States were minor players,

THE RUSSIAN SPECIAL SERVICES HAVE PROBABLY
UNDERESTIMATED THE CAPABILITY OF WESTERN
SECURITY AGENCIES.

THE RECENT EXPOSURES OF RUSSIAN INTELLIGENCE OFFICERS AND AGENTS INDICATE THAT:

- 1) the Russian special services intensively recruit agents in neighbouring countries, and also more distant Western countries;
- 2) the Russian special services have probably underestimated the capability and level of cooperation between Western security agencies;
- 3) the Russian special services have not always taken the security and concealment of their intelligence operations seriously enough. It is likely that the possibilities for using public sources, including social media, to identify intelligence operatives and their activities were underestimated. This is especially evident in the case of the Skripal poisoning;
- 4) the Russian special services are certainly analysing their mistakes to avoid them in the future; and
- 5) the higher frequency of exposures in recent years cannot be used as the sole basis for assessing the effectiveness of Russian intelligence operations as a whole. Complete information on Russia's successful intelligence operations is, of course, not available to the West, and the failures may actually be outnumbered by successes.

but unfortunately some of them had access to highly sensitive information.

Since the embarrassing episode in 2010 when 10 of its officers and agents were arrested in the US at the same time, the SVR has been able to keep a low profile, but not to avoid failures completely. For example, an SVR officer who worked at a bank as cover and specialised in economic

intelligence was arrested in the United States in 2015 and subsequently convicted. In 2016, the SVR lost an agent within the Portuguese security and intelligence service. In 2018, Belgian authorities reported having exposed one of their diplomats who had collaborated with the SVR and its predecessor, the KGB, for more than 20 years.

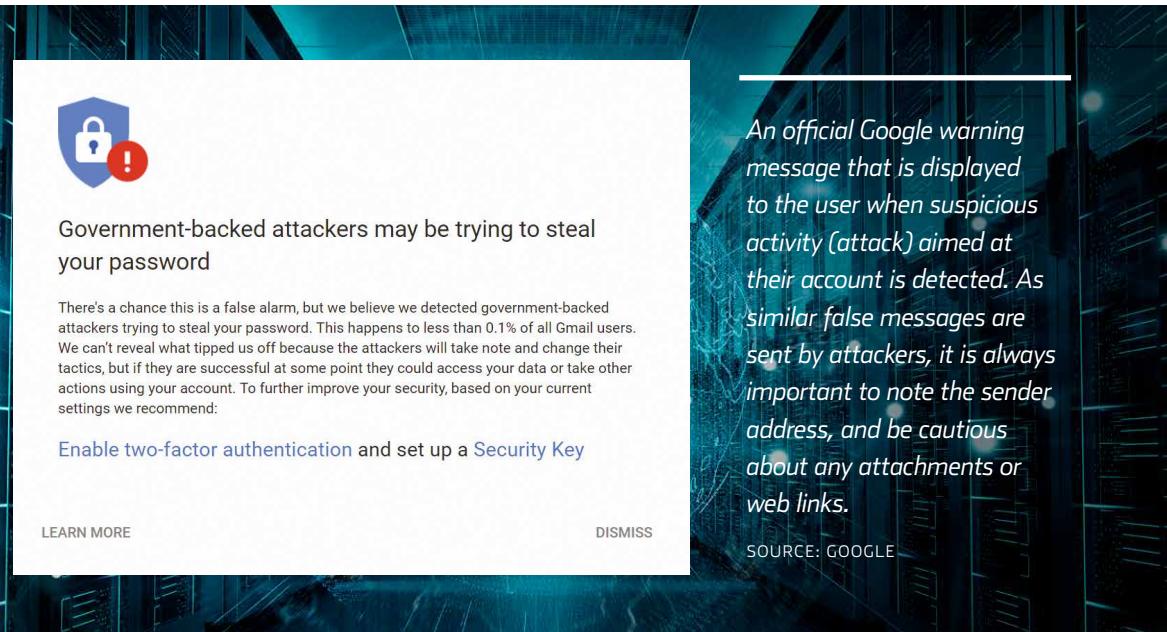
RUSSIA'S MALICIOUS CYBER ACTIVITY LEANS ON NON-GOVERNMENTAL ACTORS

Last year's exposures have not discouraged Russian cyber spies, and phishing for data from Western sources continues at full capacity. To cover up their activities more effectively, Russian special services utilise cyber criminals and so-called patriotic hackers.

The Russian special services' cyber operations and the characteristic masquerading of their attacks caught wider attention in 2018. The special services' cyber attacks in connection with the Skripal poisoning, the capture of Russian military intelligence (GRU) officers as they were preparing a cyber attack on the Organisation for the Prohibition of Chemical Weapons, data breaches by APT28, a GRU cyber espionage group, during the South Korean Winter Olympics, and Brexit-related phishing e-mails clearly showed that, despite public attention, accusations and sanctions, the Russian special services remain consistently active in cyber espionage.

In 2018, the GRU's cyber espionage groups APT28 and Sandworm continued to be the most active players within the Russian special services. The cyber activities of APT28 have been well documented by intelligence agencies, information security companies, and the general public over the years. Certain changes in direction are evident in these activities: simpler, freely available online tools are increasingly preferred, most likely to blur the line between clearly state-supported attacks and the activities of online activists and profiteering cyber criminals.

SNAKE APT, a group tied to the Federal Security Service (FSB), sticks to a different, more familiar line, avoiding



excessive public attention and trying to operate below the radar. SNAKE APT uses more sophisticated and expensive tools and attacks targets of long-term value.

At the end of 2018, it was revealed that the APT29 group associated with the Russian Foreign Intelligence Service (SVR), which for some time remained invisible at the global level, has in fact not withdrawn from phishing campaigns. All this clearly shows that Russia's state-backed cyber espionage is in full swing.

Over the years, Estonia has in some way or another been targeted by the cyber spies of all the above-mentioned

special services. The attackers are interested in Estonia both in its own right and as a member of the European Union and NATO. The cyber espionage operations against Estonia are aimed at gaining access to information concerning international communication as well as to the working documents, names and e-mail addresses of national and international institutions. Russian cyber espionage targets Estonian ministries (particularly the Ministry of Foreign Affairs and the Ministry of Defence), the Defence Forces and the Defence League, as well as the units of NATO allies based in Estonia. Recent history has shown that the information obtained is also actively used as an input and

platform for new phishing campaigns – to make the phishing e-mails that reach the officials' professional and private mailboxes as effective as possible.

Phishing e-mails remain the most widely used form of attack. As always, the victim still has to make the final push of a button giving access to the attacker. There is no way to avoid this other than by being cautious about any links provided in e-mails and to make sure that the source of the document or other attachment is known to the recipient. Particular attention should be paid when asked to activate macros upon opening a document or to download software updates or add-ons.

CYBERCRIME

Most of the cyber and information operations originating from Russia are led by the special services, particularly the FSB and GRU. The methods used are numerous. Among the most widely used recent approaches is masquerading as cyber criminals or recruiting actual cyber criminals to do the work.

Local cyber criminals are also causing problems for Russia itself. Fighting cyber crime is the responsibility of the

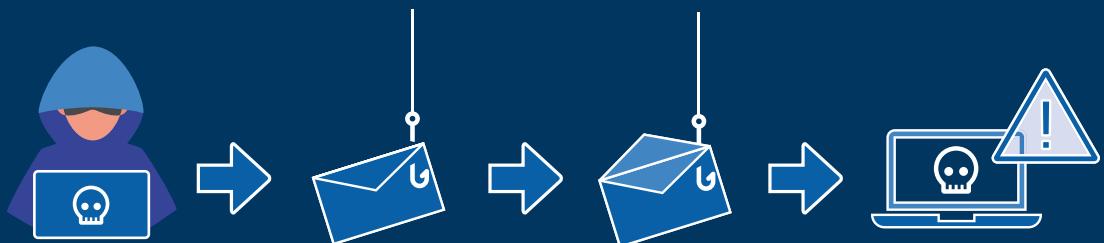
interior ministry's Directorate K and the FSB, both of which cooperate with the private sector, including Kaspersky Lab. However, the law enforcement agencies are primarily interested in those who act against Russia's own authorities. For example, the internationally wanted Russian hackers Yevgeniy Bogachev and Latvian-born Aleksei Belan are the greatest cyber criminals in recent history, whose activities have led to the loss of hundreds of millions of euros for Western companies and financial institutions. Nonetheless, they are successfully hiding in Russia, and as they avoid the mistakes made by previously caught Russian cyber criminals¹ when travelling abroad, Russian law enforcement agencies (in accordance with Russian legislation) show no interest in arresting or extraditing them.

What is more, the Russian special services have themselves used personal

¹ For example, Yevgeniy Nikulin, who was arrested in the Czech Republic in 2016, accused with accessing the databases of Dropbox and LinkedIn in 2012. Another example is Roman Seleznev, son of Russian MP Valery Seleznev, who was arrested in the Maldives in 2014 and sentenced to 27 years in prison in 2016 in the United States for extensive computer and bank fraud, as well as repeated identity theft.

PHISHING AND SPEAR PHISHING FOR PERSONAL INFORMATION

Phishing is a fraudulent attack to obtain personal or sensitive data (e.g. usernames, passwords or credit card detail). Spear phishing is aimed at a specific target (a person or organisation) and is usually conducted for commercial, military or political purposes, in an attempt to gain access to sensitive data.



PREPARATION AND EXECUTION

The attacker uses a previously compromised or fake account to send an e-mail that usually contains a malicious attachment or link. The preparations include identifying a suitable method for attacking the specific target (e.g. sending a potentially interesting document or link).

PHISHING E-MAILS

The e-mails are designed to appear as attractive and reliable as possible to the recipient, seeking to exploit their trust (e.g. by using a familiar sender address or something very similar).

THE VICTIM OPENS AN ATTACHMENT OR CLICKS ON A LINK

The attached file or document usually asks the recipient to activate or install something. When clicking on a link, the victim may be directed to a seemingly familiar login page and, for example, prompted to enter an e-mail address and password.

THE USER'S COMPUTER AND PERSONAL INFORMATION ARE COMPROMISED

The attacker gains access to the victim's computer and injects it with additional access rights or malware for data collection. If the computer is part of a network of an organisation, the attacker is likely to seek more extensive access.



information stolen and leaked by Russian cyber criminals. Examples include Karim Baratov, a Kazakh-born Canadian hacker who was sentenced to five years in prison for Yahoo! data breaches, while the data leaked by him was used in FSB operations. It is very likely that all Russian special services have benefited from Russian cyber criminals' intrusions into the databases of Yahoo!, LinkedIn, the Ukrainian-based Bigmir and others, exploiting these as a useful resource for cyber espionage. The same applies to hackers already arrested in Russia. The example of the former hacker Dmitry Dokuchayev, who is currently employed by the FSB, shows

that if they are willing to put their talent and skills to the service of the state, their sentence will be significantly reduced. Therefore, the Russian security agencies' interest in cyber criminals may be seen as primarily inclusive and cooperation-oriented.

PATRIOTIC HACKERS

Russia's malicious cyber activity also involves 'patriotic hackers', who seem unrelated to Russian national interests and special services but always show increased activity during military or geopolitical conflicts where Russia's interests are at stake. The main methods

of these patriotic hackers are website defacement and denial-of-service attacks, as well as the dissemination of false information to disrupt nationally and socially important services.

Such activities are still evident in Ukraine, most recently during the Kerch Strait incident. The scope of CyberBerkut operations in Ukraine, from distributed denial-of-service attacks and data breaches to psychological operations and attacks on the country's critical infrastructure, is a clear indication of underlying Russian national interests. Russia made similar use of patriotic hackers in 2007 when Russian hackers disrupted the work of Estonian public services in connection with the events of the Bronze Night, and in 2008 in Georgia in conjunction with Russian military operations. The activities of patriotic hackers have always been co-ordinated, well thought-out and backed by technology that is not accessible to ordinary citizens.

Patriotic hackers and Russian special services do not target solely neighbouring countries that have fallen out of favour with Russia; similar methods are used on the Russian internet. Both the FSB and other internet control

FREE ONLINE TOOLS ARE PREFERRED TO BLUR THE LINE BETWEEN STATE-SUPPORTED ATTACKS AND THE ACTIVITIES OF ONLINE ACTIVISTS AND CYBER CRIMINALS.

bodies in Russia have stepped up the fight against inappropriate content.² The special services, trolls, and patriotic hackers all target Russia's oppositional news outlets, bloggers, politicians, and journalists. Cases have been publicised where the Russian special services have tried to access the mailboxes of such groups through phishing or watering hole attacks, and then leak compromising information to obstruct their activity and undermine credibility. Generally speaking, nothing happens in Russian cyberspace without the special services, particularly the FSB, knowing about and controlling it.

² GRU information attacks against Alexei Navalny, CyberBerkut data leaks criticising the Russian opposition, and the arrests of the members of the Anonymous International (Shaltai Boltai) hacking group, who embarrassed the Russian government by publishing leaked documents, are just a few examples of the authorities' counter-activities on the Russian internet.

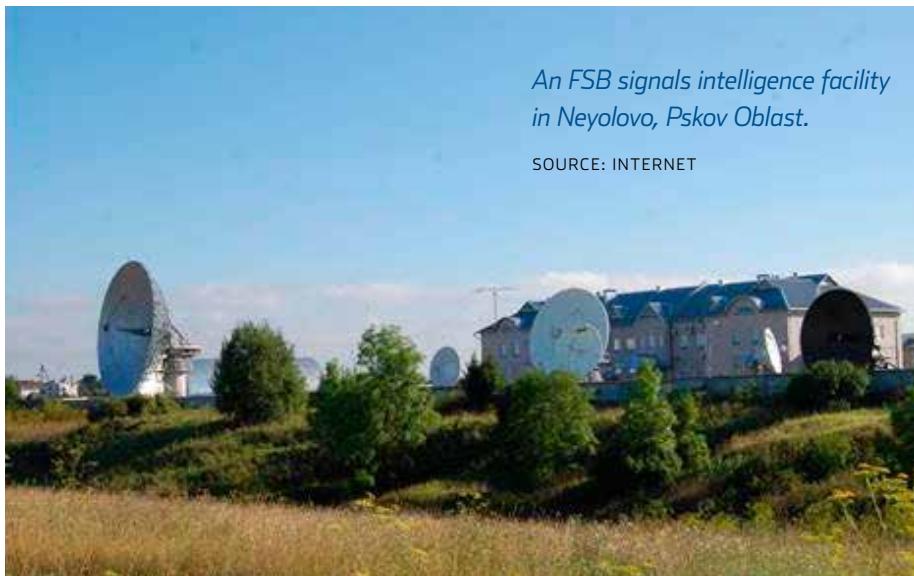
HOW THE FSB SIGNAL INTELLIGENCE GATHERS INFORMATION ON FOREIGN CITIZENS

The customers of Russian communications service providers in Estonia and elsewhere should be aware of the possibility of their data ending up in the hands of Russian special services.

The main methods of intelligence gathering used by the Russian intelligence and security services are human, cyber, and signals intelligence. Signals intelligence is intelligence gathering through the interception of electronic and radio signals. There are signals intelligence units in all Russian intelligence and security services, but here we will focus on the 16th Centre, the FSB's main structural unit for signals intelligence.

The predecessor of FSB's 16th Centre was the 16th Chief Directorate of the KGB (the Committee for State Security of the Soviet Union). As the KGB was dissolved in 1991 and its structural units transformed into several new security and intelligence agencies, the 16th Main Directorate and the 8th Main Directorate responsible for government communications were reorganised into the Federal Agency of Government Communications and Information (FAPSI). FAPSI was in

ALL RUSSIAN COMMUNICATIONS SERVICE PROVIDERS
ARE REQUIRED TO GIVE THE FSB ACCESS TO
THEIR NETWORKS AND INFORMATION



An FSB signals intelligence facility in Neyolovo, Pskov Oblast.

SOURCE: INTERNET

turn dissolved in 2003 and its functions divided between the FSB, the Federal Protective Service (FSO) and the Foreign Intelligence Service (SVR). The FSB's 16th Centre inherited from FAPSI the former KGB's signals intelligence infrastructure on the territory of Russia.

Decades ago, Soviet intelligence and security services first engaged in signals intelligence mainly by intercepting radio and telephone communications. Now the FSB gathers information transmitted using any method, be it radio, satellite, telephone, mobile, or data link communications. While the Russian authorities are using legislative means to force communications service providers

(including instant messaging application operators) operating in Russia to disclose their decryption keys, the FSB is also making efforts to develop its own capabilities for decrypting the communications of both domestic and foreign service providers.

In addition to the 16th Centre, which uses signals intelligence to gather information on foreign countries, the FSB also runs a System for Operative Investigative Activities (SORM), which is designed for intercepting telephone calls and monitoring internet traffic in Russia. For this purpose, all Russian communications service providers are required to give the FSB access to their networks and the information they transmit. SORM is the

responsibility of other FSB structural units; the 16th Centre is not involved.

The FSB's 16th Centre consists of a central unit housed in unmarked administrative buildings in many different locations across Moscow and secluded forest enclosures, with satellite dishes several metres in diameter facing in different directions. Located mainly along Russia's borders are signals intelligence facilities, also referred to as information reception centres, which is a direct reference to their main function. The 16th Centre's signals intelligence facilities closest to Estonia are in Krasnoye Selo (Leningrad Oblast), Verbnoye (Kalininograd Oblast) and Neyolovo (Pskov Oblast). The last one is only 25 kilometres from the Estonian border.

The FSB 16th Centre's network of signals intelligence facilities is a security threat not only for Estonia. Even without visiting a website hosted on servers located in Russia and without contacting a person who has a Russian telephone number or e-mail address, an international call, e-mail or web search may go through Russian territory. If part of the data stream is channelled through Russia due to an

agreement between service providers, for cost-saving purposes or to avoid communication channel overload, it is likely to pass through FSB signals intelligence facilities. This threat cannot be completely avoided and it mainly concerns communication between employees of state authorities, who may possess and pass on information that is of interest to Russian intelligence agencies.

Speaking or writing in Estonian does not guarantee greater security either, as all the FSB 16th Centre signals intelligence facilities located close to Estonia have staff who speak the languages of Russia's neighbours, including Estonian, as well as the major international languages. While several public universities in Russia teach the Estonian language, it is also taught in the educational institutions run by the FSB and its Border Guard Service.

The following example is a good illustration of the activities and interests of the FSB's 16th Centre. In January each year, a very special public contract is signed in the Russian capital, between "Military Unit 71330" and some Russian service provider that handles the order and delivery of

A PUBLIC CONTRACT BETWEEN “MILITARY UNIT 71330” AND MIR PERIODIKI FROM 2017.

**ГОСУДАРСТВЕННЫЙ КОНТРАКТ № 16/215
на оказание услуг по подписке и доставке зарубежных справочных
печатных изданий на 2017 год
(шифр «Справочник-17»)**

г. Москва

«10» 01 2017 г.

Федеральное государственное казенное учреждение «Войсковая часть 71330» (далее ФГКУ «В/ч 71330»), именуемое в дальнейшем Заказчик, в лице заместителя руководителя Мокрова Андрея Сергеевича, действующего на основании доверенности от 15.05.2015 № 18/8-1517, с одной стороны, и общество с ограниченной ответственностью «Мир Периодики» (далее ООО «Мир Периодики») (свидетельство о государственной регистрации серия 77 № 006344201 от 05 июля 2005, основной государственный регистрационный номер 1057747383055, выдано МИФНС № 46 по г. Москве), именуемое в дальнейшем Исполнитель, в лице генерального директора Тимофеева Владимира Ферапонтовича, действующего на основании Устава, далее именуемые Стороны, на основании протокола рассмотрения и оценки котировочных заявок № 55 от 22.12.2016 заключили настоящий государственный контракт (далее – контракт) и нижеследующем:

1. ПРЕДМЕТ КОНТРАКТА

1.1. Заказчик поручает, а Исполнитель принимает на себя обязательства по подписке и доставке зарубежных справочных печатных изданий с первого по последний номер 2017 года (далее – изданий) в соответствии с перечнем зарубежных справочных печатных изданий на 2017 год (Приложение №1), являющимся неотъемлемой частью контракта.

Перечень зарубежных справочных печатных изданий на 2017 год

| № п/п | Наименование издания | Периодичность выхода издания | Цена одного номера издания (в т.ч. НДС) (руб.) | Цена за один комплект издания (в т.ч. НДС) (руб.) | Кол-во комплектов изданий | Годовая стоимость издания (в т.ч. НДС) (руб.) |
|-------|--|------------------------------|--|---|---------------------------|---|
| 1 | Federal Yellow Book 2017, 4 Vol., Leadership Directories, Inc, USA, ISSN № 0145-6202 | 4 | 22 871,25 | 91 485,00 | 1 | 91 485,00 |
| 2 | Congressional Yellow Book 2017, 4 Vol., Leadership Directories, Inc, USA, ISSN № 0191-1422 | 4 | 22 871,25 | 91 485,00 | 1 | 91 485,00 |

Итого 182 970,00
НДС (10%) 16 633,64

periodicals. Under the contract, the service provider undertakes to deliver to addresses in Moscow provided by "Military Unit 71330" all the volumes of the Federal Yellow Book and Congressional Yellow Book published by the US-based Leadership Directories, Inc. during the given year. These publicly available directories of the US Federal Government and Congress are updated four times a year and list the names and contact details – e-mail addresses and phone numbers – of government employees. "Military Unit 71330" has repeatedly ordered similar directories covering the European Union and other regions. It has also organised public procurements for the purchase of publications on electronic and radio communications as well as information technology and security from Russia and abroad.

The name "Military Unit 71330" is in fact a front for the FSB's 16th Centre,

and the information published in the directories is used to gather intelligence on the persons and institutions. All three of Russia's intelligence and security services (the FSB, GRU and SVR) and their subdivisions have set up a common system with Russian armed forces to conceal their activities, whereby the names of military units or intelligence services (and their subdivisions) are often replaced by five-digit codes of "military units" in public documents. As all the institutions use the so-called military unit codes interchangeably, it is impossible to identify the military or intelligence unit in any given instance without factual knowledge. The signals intelligence facilities of its 16th Centre in Krasnoye Selo, Verbnoye and Neyolovo along the Estonian border also use these codes, and are designated as Military Units 61240, 83521 and 49911, respectively.

THE NAMES OF RUSSIA'S INTELLIGENCE AND SECURITY
SERVICES ARE OFTEN REPLACED BY FIVE-DIGIT CODES
OF "MILITARY UNITS" IN PUBLIC DOCUMENTS.

CHINA'S GROWING INFLUENCE

In recent years, the European Union, as well as the US and many other countries, has taken a more cautious stance on Chinese foreign investment and technology. There are several reasons for this.

First, Chinese investment in Europe has boomed significantly in recent years. Investments have been made in all sectors of the economy, but China's investments in transport and technology are particularly notable. Second, China is increasingly using foreign investment to advance its political goals. The Chinese leadership has given both private and public companies directions to increase foreign investment in high value-added areas in order to strengthen China's position in the global economy. Chinese companies have consistently shown great interest in Western IT and technology companies, and limited access to the United States market may increase their interest in European IT firms.

An important aspect is that Chinese law does not protect private companies from national interests and government interference in business. This means that, if necessary, the Chinese government will have access to state-of-the-art technology or sensitive information acquired by a private company.

Third, cyber operations serving China's national interests have gained wide coverage worldwide. Security breaches or "backdoors" on Chinese IT devices have been identified; malware has been found on mobile devices, computers, and more sophisticated network devices. Chinese cyber operations have been found to support the efforts of the communist party and the military and involve industrial espionage for the benefit of Chinese technology companies.

Several countries (the United States, Australia, New Zealand and others) restrict the use of Chinese technology in national telecommunications solutions due to suspicions that it may be used for intelligence purposes in the interests of China or a third party. Recognised security threats include the use of Huawei or ZTE security solutions, such as firewalls, which are considered unpredictable and unsafe. With



Huawei, it has not been possible to verify and the manufacturer has not convincingly proved that it does not rely on the Chinese National Intelligence Law (in force from June 2017), under which "any organisation and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work." Thus, in China, as in Russia, domestic companies and foreign businesses operating there are required by law to cooperate with the state and its security agencies. In the assessment of the Estonian Foreign Intelligence Service, these risks have to be carefully analysed in order to avoid dependency that could potentially be a security threat to both the public and private sector.

With the Chinese economy gaining influence and Xi Jinping acceding to power, China has shown more interest in influencing policy makers abroad and increasing its soft power. As a rule, China, unlike Russia, does not want to divide Western societies or destabilise its major trading partners. China's

propaganda and lobbying mainly focus on supporting its political and economic interests. China is actively strengthening its propaganda efforts to influence public opinion through the West's own media channels, as well as Western media owned by the Chinese state. At the same time, China's domestic media market is increasingly closed to Western outlets. Chinese populations in other countries are also used for the purposes of Chinese propaganda.

China is more and more active in influence operations and propaganda, establishing contacts and intensifying communication with government officials, local government representatives and politicians in other countries, and bolstering its influence over them. It is also strengthening social and academic ties and promoting collaborative projects between European and Chinese think tanks. These developments are evident in Europe, including Estonia. Contacts established through positive engagement may later develop into closer cooperation and ultimately lead to recruitment attempts by special services. It has also been observed that China is seeking to increase its political influence in some countries through political donations.

→ *Xi Jinping and Vladimir Putin at the Eastern Economic Forum in September 2018.*

SOURCE: REUTERS/
SCANPIX



RELATIONS BETWEEN CHINA AND RUSSIA

The relationship between China and Russia is complicated: on the one hand, there is mutual distrust, on the other hand, both are interested in cooperation. This is due to Russia's bad relations with the West and the confrontation between China and the United States.

The relations between China and Russia are based on their common strategic goal of creating a multipolar world order and reducing the power of the West within their spheres of influence. In the coming years, the greatest threat that the partnership between China and Russia poses to the West is in terms of their efforts to adapt or change the international political system in their favour.

The intensifying pressure from the Trump administration on China and Russia has increased their need to show

that they are not politically isolated. An indication of this was the participation of the Chinese President Xi Jinping with a large business delegation at the Eastern Economic Forum in September 2018. Communication between the governments of Russia and China is tight. Contacts between military representatives have also become more frequent to maintain stability. As a result of US pressure on both countries, Beijing and Moscow are likely to intensify bilateral relations and further coordinate their global politics with each other.



← *Russian and Chinese armed forces at the Vostok military exercise in September 2018.*

SOURCE: AFP/SCANPIX

Both Russia and China are interested in developing economic relations, but they are not equal partners; Russia is not important for China as a trading partner, accounting for only 2.1 % of its foreign trade. In connection with the 40th anniversary of introducing an open economic policy in China in 1978, many Chinese analysts have stressed that while Russia's economy was larger than China's at the time, its GDP is now comparable to that of China's Guangdong Province.

Contacts and joint exercises between the Chinese and Russian armed forces have become more frequent in recent years. Participating in the Russian Vostok 2018 military exercise in September 2018 was a good opportunity for China to (i) demonstrate its growing military capability, (ii) learn from the Russians, and (iii) demonstrate

(to the US) that China and Russia can act together when necessary. China avoided attaching much importance to its participation in Vostok in the media and Chinese politicians did the same in their speeches. They acknowledged the fact, but refrained from drawing serious geopolitical conclusions from it in political discussions. China did not want to appear too opposed to the West. Chinese analysts and politicians also stressed that China and Russia are not a military alliance, and China does not want to present its membership in such an alliance as a possibility.

Neither is prepared to support the other unconditionally in international conflicts or in conflicts involving their key national interests. Their shared interests have clear limits and each country wants to keep the other one out of its own sphere of influence.

TERRORISM IN EUROPE

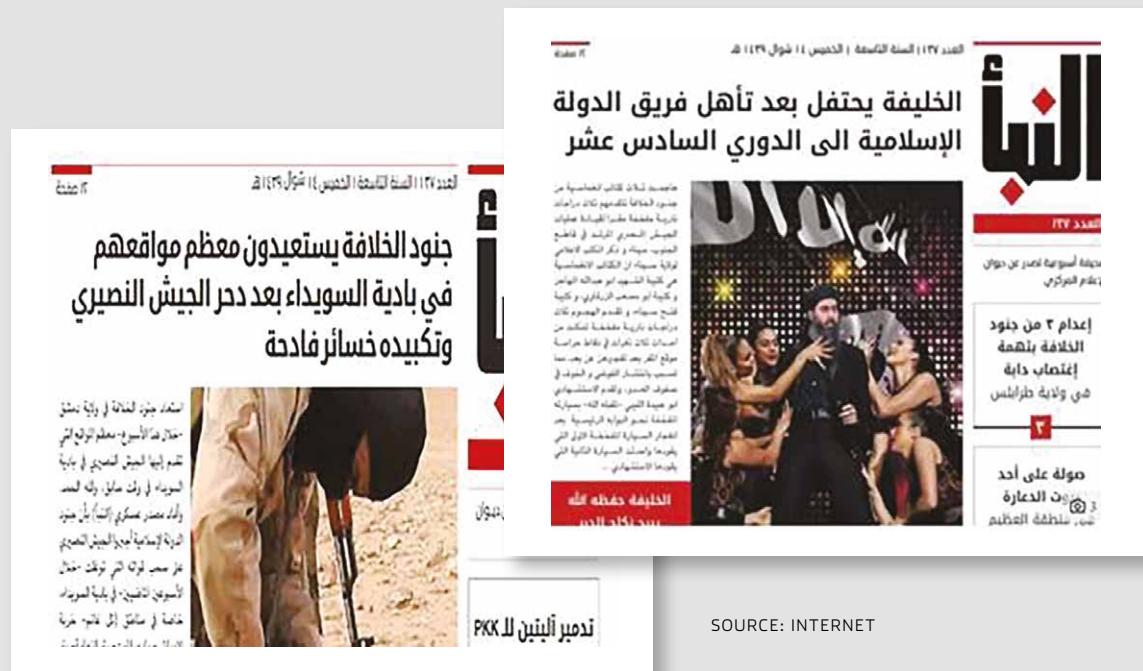
Weakened and having lost territory, the Islamic State (IS) continues to affect European security in 2019.

The military campaign against IS and the systematic counter-terrorism efforts of European law enforcement agencies and security services made it more difficult for IS to conduct operations in Europe. Nevertheless, Islamic extremists are still focused on organising terror attacks in the West; threat levels remain high in France, Germany, Britain, Belgium, and Spain in particular, due to the high number of potentially dangerous radicals in those locations. In Britain and France, more than 20,000 people are listed as radicalised individuals who are considered a terrorist threat. According to its security services, Germany has 11,000 radical Islamists and 980 dangerous persons with potential for committing a terrorist attack. In Finland, 370 persons who pose a terrorist threat and have either direct or indirect ties with radical Islamist networks or organisations are under surveillance.

In the European Union, the number of arrests on suspicion of terrorist

offences has doubled in five years (from 1,056 in 2006–11 to 2,880 in 2012–17), according to Europol. Most of the arrests have been made in France, Spain, Germany, and Belgium. Over the next two years, around 200 persons convicted of terrorist offences will be released from prison in the EU. Given continued radicalisation in prisons, the release of those who have served their sentences will affect European security for years to come.

Although IS activities have been severely cut back in recent years, networks that pass on radical propaganda and recruit fighters continue to incite attacks in Europe. Instead of opting for larger operations, they place their bets on fighters who reside in Europe, giving instructions on how to attack with cheap and readily available means (driving a vehicle into a crowd, attacking people in a public place with cut-and-thrust weapons, and so on), and possibly also using drones, biological or chemical substances, or peroxide-based explosive



Much of the radical IS propaganda spreads in cyberspace independently of the leadership of the organisation, with the help of covert supporters using technology that ensures anonymity (the dark web, anonymous and secured networks, anonymisers, or cryptocurrency). By relying on disciples scattered in cyberspace, IS has lost control of its “brand” and the dissemination of fake news. In June 2018, for example, a fake version of IS’s al-Naba newspaper, which copied the publication’s standard format, spread online.

devices (TATPs) for a bigger attack attracting more attention from the media.

Despite the persistently high level of terrorist threat in Europe, the threat level in Estonia remains low. However, although Estonia is not seriously

threatened by international terrorism, it still poses a risk, especially for Estonian citizens abroad. Moreover, taking into account the wide reach of terrorist activity, radicalisation through exposure to online propaganda cannot be completely ruled out in Estonia.

ILLEGAL IMMIGRATION TO EUROPE

Following a significant increase in migration flows in 2015, mainly due to the Syrian conflict, illegal migration to Europe has started to decline in the last three years. However, tensions in international conflict areas in Syria, Afghanistan, Mali, and elsewhere continue to be a potential source of illegal migration to Europe.

Unlawful entry into the Schengen area has become more and more difficult due to the measures taken to restrict illegal migration. As a result, human trafficking networks familiar with local circumstances and able to exploit gaps in legislation and border control have increased their role in the smuggling of migrants into the EU. A favourable visa regime and direct flights have boosted the legal entry of migrants into the EU's neighbouring states with the aim of then making their way into the EU with the help of mediators. For example, after Iran and Serbia signed a visa exemption agreement and scheduled flights started

between Tehran and Serbia, the number of migrants with Iranian citizenship increased and Serbia became a popular transit country for entering the Schengen area. In October 2018, under pressure from the EU, Serbia abolished visa-free travel for Iranians, as it was used for illegal migration.

A temporary change in Russia's visa policy during the occasion of the FIFA World Cup in Russia in 2018 allowed visa-free entry to the country for those in possession of match tickets. This contributed to an increase of travellers attempting to enter EU illegally from its eastern borders via Russia, but also via Ukraine and Belarus.

HUMAN TRAFFICKING NETWORKS HAVE INCREASED THEIR
ROLE IN THE SMUGGLING OF MIGRANTS INTO THE EU

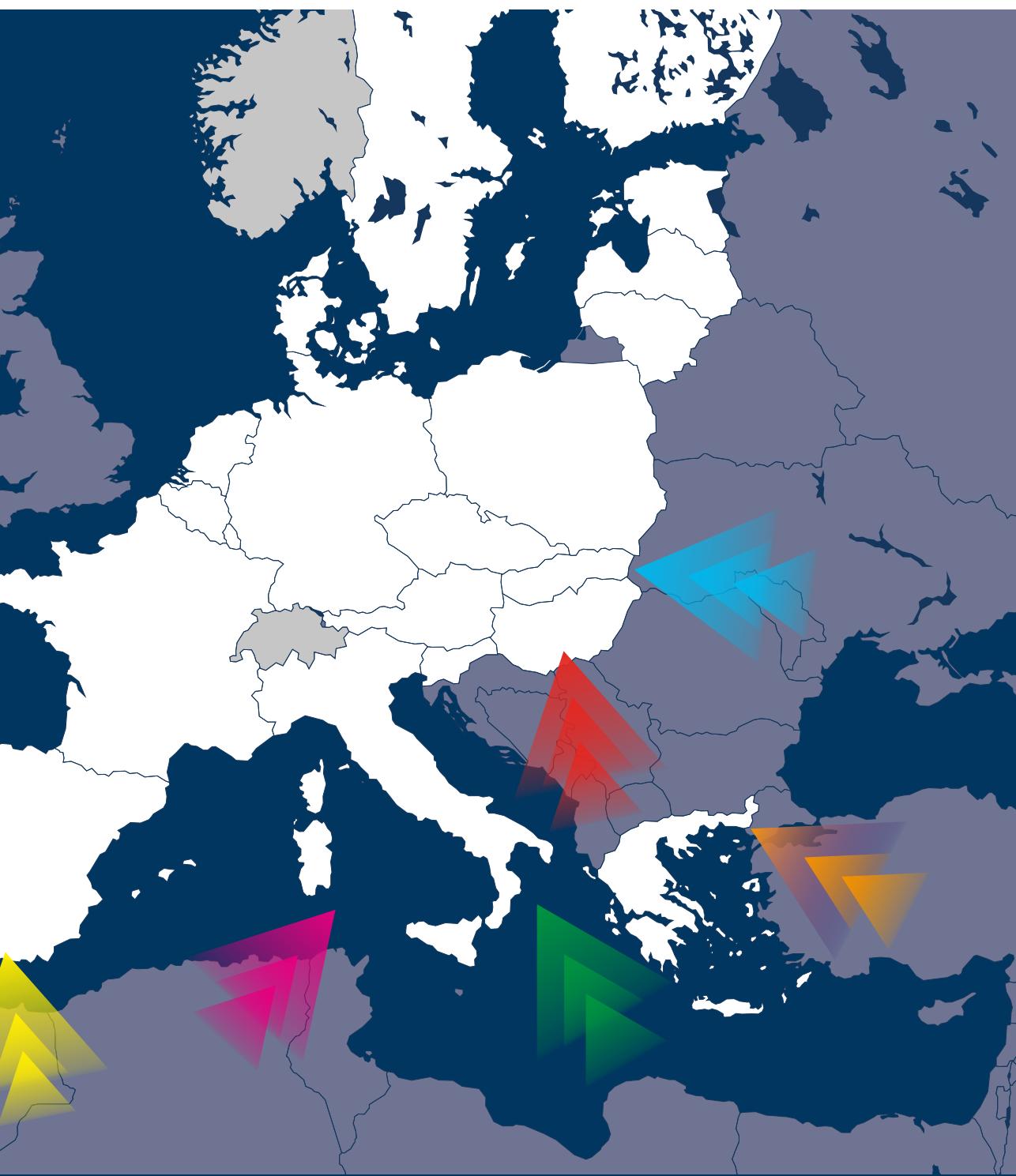
MIGRATION ROUTES TO EUROPE

**Migration routes have shifted from east to west:
from Greece in 2016 to Italy in 2017 and
Spain in 2018.**

-  Eastern Borders route
-  Western Balkan route
-  Eastern Mediterranean route
-  Central Mediterranean route
-  Western Mediterranean route
-  Western African route
-  Schengen area
-  Schengen associate countries

Canary Islands





THE ESTONIAN FOREIGN INTELLIGENCE SERVICE

COLLECTS,
PROCESSES
AND DISSEMINATES

INTELLIGENCE
ON **EXTERNAL SECURITY THREATS**
AFFECTING ESTONIA.

