ANNUAL PUBLIC REPORT 2016

The Constitution Protection Bureau (SAB) is one of three state security institutions of the Republic of Latvia. SAB is responsible for foreign intelligence, counter-intelligence and safeguarding of national, EU and NATO classified information.

Executive Summary

- **The most significant security threats in the Baltic sea region are caused by Russia – its aggression in the Ukraine, the demonstration of its military power and pro-activity close to NATO external border as well as different components of information and hybrid warfare directed towards neighboring countries.**
- **The Kremlin exerts control over internal situation in Russia by increasing limitations on democracy, civil rights and media independence. The propaganda oriented towards Russian society stresses the responsibility of the Western countries on Russia's complicated economic situation and deterioration of living standards.**
- **Russian intelligence and security services (RIS) are expanding their activities against Latvia's and allied interests. NATO security policy issues and related activities in the region, as well as Latvia's defense and military capabilities are the areas of interest for the Russian intelligence services. SAB has detected a wide range of intelligence interests from RIS towards economic, domestic and foreign policy areas in Latvia.**
- **Russia's influence activities within information domain of Latvia remain a serious long-term security threat. As stated before and also during 2016 Russian propaganda was used to discredit NATO and security policy of Latvia and to weaken the public support for the enhanced presence of NATO troops in the region.**
- **During last years the society of Western countries and Baltic Sea Region in particular have become more critical towards Russian propaganda, slandering and discreditation campaigns, as well as attempts of Moscow lead pseudo-experts and pro-Russian organizations to imitate the activities of civil society.**
- **The fastest growing threat for the Western countries at the moment is Russia's growing cyber capabilities and its full readiness to utilize them. A number of cyber attacks in 2016 were targeted against Latvian government, private companies and media networks. Most of cyber attacks in Latvia are committed with the purpose of espionage by infecting targets' devices while opening false e-mails.**

INTRODUCTION

Year 2016 was challenging for the security related issues in Europe. Russia continued its aggression in Ukraine, carried out military activities in the region and expanded non-military means to influence the situation abroad. International terrorism, extremism and radicalization caused a serious threat to the world security, question on migration was also in agenda, as well as the development of political and military conflict in the Middle East and North Africa regions.

The most important threat to the security environment of Latvia was caused by Russia's aggressive policy, including influence activities and propaganda directed against Latvia, as well as activities of Russian Intelligence and Security Services (RIS). Cyber threat caused by Russia is one of the fastest growing security threats directed against Western world including Latvia.

NATO took a significant decision in 2016 to enhance the presence of allied troops in the Eastern Baltic sea region, supporting the Baltic States and Poland to guarantee the security on the North Atlantic Alliance's external border. The strengthening of collective security by implementing functions of intelligence, counter-intelligence and protection of classified information are the main goals of SAB.

RUSSIA

Russia's main foreign policy objectives have not changed and they remain as following – to restore and strengthen its influence, mostly in the territories of post-Soviet countries and Europe and to be recognized as world power. Russia is focused on increasing its influence and role regionally and globally, as well as on the weakening of unity and position of the Western world.

Russia still considers NATO as its opponent. NATO enlargement and the increase of NATO military presence in the vicinity of the Western borders of Russia are still characterized as threat to its security which is even stated in the Russia's Foreign policy concept as of December 2016. To make pressure on neighboring countries and NATO, Russia expressively demonstrated its military capabilities in the Baltic Sea region. Russian military aircrafts repeatedly violated air space of bordering countries or performed dangerous maneuvers around military units of Latvia's allies. Russia sent extra military equipment to its border areas and conflict regions. The demonstration of military capabilities was combined with the corresponding political rhetoric and propaganda. The activities of Russia are publicly justified only as a reaction against enhanced NATO military presence in the Eastern Baltic sea region, often misleadingly exaggerated in Russian mass media. In reality, however, Russia commenced military force deployment long before the NATO's decision on strengthening its military presence in the Baltics.

Military exercises play an important role within Russian strategic communication, their number and scope have increased in recent years. In 2016 Russia's largest military exercise KAVKAZ-2016 was held near Russian-Ukrainian border. During the exercise Russia clearly demonstrated military readiness to protect its rights to Crimea if necessary. Extensive Russian and Belorussian common military exercise called ZAPAD-2017 will be held this Autumn in near the borders of NATO member states.

Russia continued to look for different ways to overcome the international isolation and to achieve its foreign policy interests on various issues. Regarding the Syrian Civil War, Russia is one of the key players concerned with helping its close ally, president Bashar-al Assad to maintain his political power. In order to support Assad's regime and to create disagreements within the European Union, Russia used visits to Syria conducted by pro-Russian members of European Parliament. Russia exploited similar symbolic visits of the EU officials to Crimea in order to legitimize the annexation of the peninsula and to demonstrate the lack of unity among the EU members regarding further adoption of sanctions.

In 2016 Russia continued to apply different methods of information and hybrid warfare to weaken the position of the West in the global arena, to split the Western unity, especially within the EU and NATO, and to influence the political processes in these countries. The usage of cyber capabilities is constantly increasing. Attempts to influence Presidential elections in the USA were much discussed in public. In this case information obtained in result of cyber attacks was used to manipulate public opinion and influence the electorates' decision. The methods of Russian information war were mostly focused on the mobilization of existing Russia supporters and not to attract the new ones. Russian propaganda in general was more effectively operating in CIS countries, but it was also directed towards Europe as well. Russia allocates considerable financial resources to sponsor the TV channel "RT" and multimedia platform "Sputnik" in Europe, but the result does not meet the expectation. Although Russia has ensured wide range access to contents of

"RT" television, its ratings remain low. Furthermore, surveys conducted by international holdings "Gallup" and "Pew Research" suggest that during last years the public image and perception of Russia and V. Putin are characterized as negative and significantly behind the ones of USA, EU, Germany and China. These findings also apply to respondents who traditionally were considered as sympathizing with Russia, for instance, coming from countries such as Germany, France and Italy. Comparing to propaganda, the economic actors' lobbying more effectively ensures the interests of Kremlin within the Western countries.

Russian intelligence and security services (RIS) constantly remain one of the most important elements of V. Putin's regime. Intelligence and security services serve the interests of both domestic and foreign policy by neutralizing regime's opponents in Russia. Besides that they collect intelligence, carry out influence activities including provocations and aggressive operations, as it is going on in Ukraine. The influence and authority of Russian special services are continuing to increase. An important reform during last year was started and as a result a new security service called National Guard with its aim to strengthen domestic security within the country would be established. It is expected that the new formation, comprising several hundreds of thousands of Russian Internal troops and special units, would be fully operational by the beginning of 2018.

The main task of V. Putin's regime remains unchanged. It comprises control over state domestic policy and internal stability, which is ensured by imposing increasing limitations on democracy, civil rights and independence of mass media. Several laws have been adapted in Russia during last years which resulted in wider opportunities to persecute organizations, media representatives and individuals opposing the regime. Increased state control has been justified as a measure, which is necessary to fight against terrorism and malign influence from foreign countries. RIS and law enforcement organizations in Russia have taken repressive measures against unwanted activities or opinions based on laws, which have not been fully developed and passed yet. They have exploited existing deficiencies of interpretation to attribute "extremism" to the multiple activities of individuals and organizations.

All major media outlets in Russia belong to state enterprises or to individuals associated with the regime's elite. Amendments to the law "On Mass Media" came into force in January 2016. According to the amendments, foreign citizens will be allowed to hold only up to 20% of shares in Russian media outlets, and it would be forbidden for them to register their own media outlets in Russia. As a result majority of foreign media stopped their activities on the territory of Russia.

Long before the restrictions were introduced to media they affected non-governmental organizations (NGOs), especially those receiving foreign funding and being involved in political initiatives, which is a term applied for a broad spectrum of activities. Such NGOs must be registered as "foreign agents", which make them a subject to strict monitoring and a number of restrictions. The NGOs included into the "foreign agents' list" frequently face hostile attitude as they are demonized for the Russian public as Western countries' tool for destabilization of the political situation in Russia.

In July 2016 the President of Russia approved several amendments to so called "Yarovaya Law Package". Officially they are intended for fight against terrorism and extremism, but in reality they provide a better ground to take actions against opposition organizations and individuals by imposing civil and criminal penalties. A separate norm was introduced with the mentioned amendments concerning telecommunication companies and internet providers. Starting from 2018 they will be obliged to store all data (information on phone calls, e-mails, downloaded data etc.) for six months and to provide access to the information for special services without special justice warranty. The companies must provide the possibilities for the special services to have access to encoded data and decoding procedure.

Propaganda directed towards the people in Russia emphasizes the Western countries' responsibility over Russia's complicated economic situation and deterioration of living standards –

during last two years the real income of the population has decreased about 12,3% on average. The worst economic situation was observed in the regions of Russia where the socio-economic tension and discontent has increased. The financial debt increased in half of regions in Russia. Meanwhile experts have found that the first signs of economic depression could be already observed in eight of Russia's federal districts. "Grey area" economy proportion among population has already reached approximately 40%. To prevent a financial breakdown after rapid fall of oil prices and budget revenues, during 2016 Russia actively used previously accumulated reserves, diverted incomes from state-owned companies as well as increased certain taxes. Russia sold number of state assets, but in reality it frequently meant only redistribution of assets among the elite by covert transactions.

At the end 2016 the economic downturn in Russia which was observed during last two years had actually came to an end and some signs of stabilization process were noticed. Overall economic situation, however, remains complex. Necessary reforms are delayed, budget revenues still depend on oil prices and financial reserve, what according to research is the most significant element of budgetary stability, would be spent during the nearest year or year and a half.

RUSSIAN INTELLIGENCE AND SECURITY SERVICES

Activities conducted by hostile foreign intelligence and security services constitute a major security threat not only against Latvian, but also against EU, NATO and collective security interests. The main objective of the activities of the mentioned services is to gain publicly inaccessible and preemptive information which give advantages to foreign government for decision making on economic, political and military issues. Besides information collection intelligence and security services implement active measures with the aim to influence decision making process of Latvian, EU and NATO institutions as well as public opinion.

Throughout 2016 SAB continued to conduct counter-intelligence measures against several foreign (non-EU and non-NATO) intelligence and security services. The major threat against the interests of Latvia is caused by the activities of Russian intelligence and security services. Activities of other hostile intelligence and security services are assessed as moderate and not posing a significant threat to Latvian interests.

The activities of foreign intelligence and security services in Latvia are carried out by using diplomatic cover or acting from the territories of their own countries which includes different activities performed on the country borders, short-term visits of agents to Latvia, as well as activities against Latvian officials working abroad. Mass media, cyber space and social networks are sometimes used to perform active measures, where the role and involvement of the activities of intelligence and special services are difficult to uncover. The working methods of special services include the work with information sources and contact-persons, information collection from the open sources, as well as increased development of different technical capabilities within cyber space and signal intelligence field.

Russian intelligence and security services remain primarily focused on issues such as NATO security policy decisions and activities in the region, military and defense capabilities of Latvia, including National Armed forces and State Border Guard, and the situation on NATO's external border. Russian special services' interests are directed not only against Latvian activities within NATO but also in the EU and other international organizations where Latvia holds membership. In 2016 SAB also observed an increasing interest from foreign special services in the areas of domestic policy, economy and energy.

SAB has noticed an increased interest by foreign intelligence and security services towards issues which could lead to intensified disagreement among groups of society and countries. These were issues such as migration policy, Latvia's position towards Brexit, and the results of Presidential elections in the USA. Wide interest in issues with potential of causing disunion or conflict correspond to Russian foreign policy interests and may be exploited for propaganda or influence activities.

RUSSIAN INFLUENCE ACTIVITIES AND PROPAGANDA

The main long-term objective of Russian influence activities is to increase its geopolitical influence within the region, to weaken the NATO, EU and to diminish the role of the Baltic States in these organizations. Russia applies information policy and propaganda, exploits influence agents' networks and self- controlled organizations in order to weaken Latvia in following ways: by raising public distrust to the state and government institutions of Latvia; by questioning geopolitical course Latvia pursues as NATO and EU member; by carrying out international discrediting against Latvia; by promoting potential internal conflict in Latvia through stressing and aggravating ethnic, linguistic and historic differences within society. At the same time influence activities are aimed at praising the potential benefits in case Latvia supported the Kremlin's interests and agenda in the region. Constant aim of influence activities is also to strengthen ideas of "Russian world" or "Russian global supremacy" in whole society or within certain groups of population of Latvia.

During last years the population in the Baltic Sea region and in the Western countries have become more critical towards Russian propaganda, slandering and discrediting campaigns, as well as attempts of Moscow lead pseudo-experts and pro-Russian organizations to imitate the activities of civil society. Several European countries and the EU as whole have developed new or enhanced existing counter measures against the of Russian information activities. Consequently Russian influence activities are becoming more sophisticated, better developed and targeted, as well as more centered around directly controlled influence agents. Different institutions and organizations in Russia also continue their work with larger social groups such as Russian compatriots. However, it is evident that such broad scale influence activities lack efficiency, so their funding has been decreased.

Considering the crucial role of information in leading of the socio-political process, Russia's influence within information domain of Latvia still remains as one of the most significant threats of Latvia's long-term security.

The basis for Russian information activities in Latvia is formed by Kremlin-controlled TV channels, whose content is re-transmitted in Latvia. Nevertheless, since the content of such TV channels is primarily designated for domestic audience of Russia, it is rather complicated to use it as a platform for propaganda campaigns specifically developed for Latvian audience. At the same time, consumption of the mentioned media content helps to disseminate the world view and values favorable to the Kremlin. Several Russian-language media outlets in Latvia support Russian propaganda by supplementing their daily news feed with content produced by Russia's state-run media. In this way they maintain aggressive rhetoric against Latvia, which corresponds to Kremlin's objectives and propaganda narratives.

In 2016 Russia continued its efforts to strengthen the influence within information domain in the Baltics, which would allow Kremlin to implement specially adapted propaganda campaigns. At the beginning of 2016 Russian news agency "Rossija Segodna" and its related project "Sputnik" opened websites in Latvia and Estonia, at the end of 2016 also the Lithuanian version was launched. These websites serve as platform for specially selected Russian, foreign and local "experts" who disseminate opinions necessary for the Kremlin. Therefore when addressing questions related to Latvia, the Baltic states, EU or NATO – articles published in the websites are predominantly critical or negative. When addressing Russia-related issues, only positive articles dominate. However, the media content offered by "Sputnik" is not competitive in the Baltic states and has limited effectiveness. Society recognizes it as Russian propaganda project, thus limiting its work opportunities.

In 2016 as in previous years Russian influence activities in information domain were mostly related to NATO's enhanced presence in the Baltic sea region. One of the aims of propaganda directed against society of Latvia (and the Baltic states) is to leave the impression that instead of Russia, it's solely NATO's security policy which increases security risks in the region. It is in Russia's interests to reduce the support of Latvian society towards increased NATO's presence in the region. Therefore Kremlin-controlled media seeks to depict Allied troops in increasingly negative manner, and to question the unity of the Alliance and its readiness to defend the Baltic states. At the same time the Armed forces of Latvia and whole national defense system are presented as non-professional and weak to reduce the Allied support for the Baltics.

The Russian compatriot policy is one of Kremlin's most visible tools of influence against Latvia. It has helped to consolidate a handful of compatriot activists and groups so far, but its overall impact and influence over larger Russian speaking community in Latvia remains limited. Russian institutions responsible for compatriot policy implementation have established close cooperation with only a small number of Russian-speaking activists in Latvia. The activists' overall impact on broader political agenda in Latvia remains relatively low, and their publicity in mass media are mainly resulting from separate proactive and provocative individual campaigns. The leaders of Russian compatriot organizations are used as messengers to discredit Latvia in international arena and at the same time as "Western experts" in propaganda targeted towards domestic audience of Russia.

Russia's influence over larger Russian-speaking community in Latvia is not sufficient to exercise massive, efficient and results-oriented campaign to undermine internal political situation or influence the civil society.

CYBERTHREATS

One of the most rapidly growing security threats to the Western allies is posed by non-NATO and non-EU intelligence services, cyber units of armed forces as well as state sponsored hacktivists. The activities of several terrorist organizations in cyberspace are also considered to be a serious threat.

Several types of threats are distinguished in cyber space: espionage, information operations to influence the public opinion or the political decision makers as well as destructive actions against IT systems or industrial infrastructure that depend on IT. Often a cyber attack may have several simultaneous objectives, such as exerting psychological influence and information gathering.

Cyberthreats may be directed against both public and private sector. The attacks may be executed via private computers and accounts. The attacks may be directed against the person of interest or other indirectly related persons, such as family members as long as this allows the attacker to reach its goals.

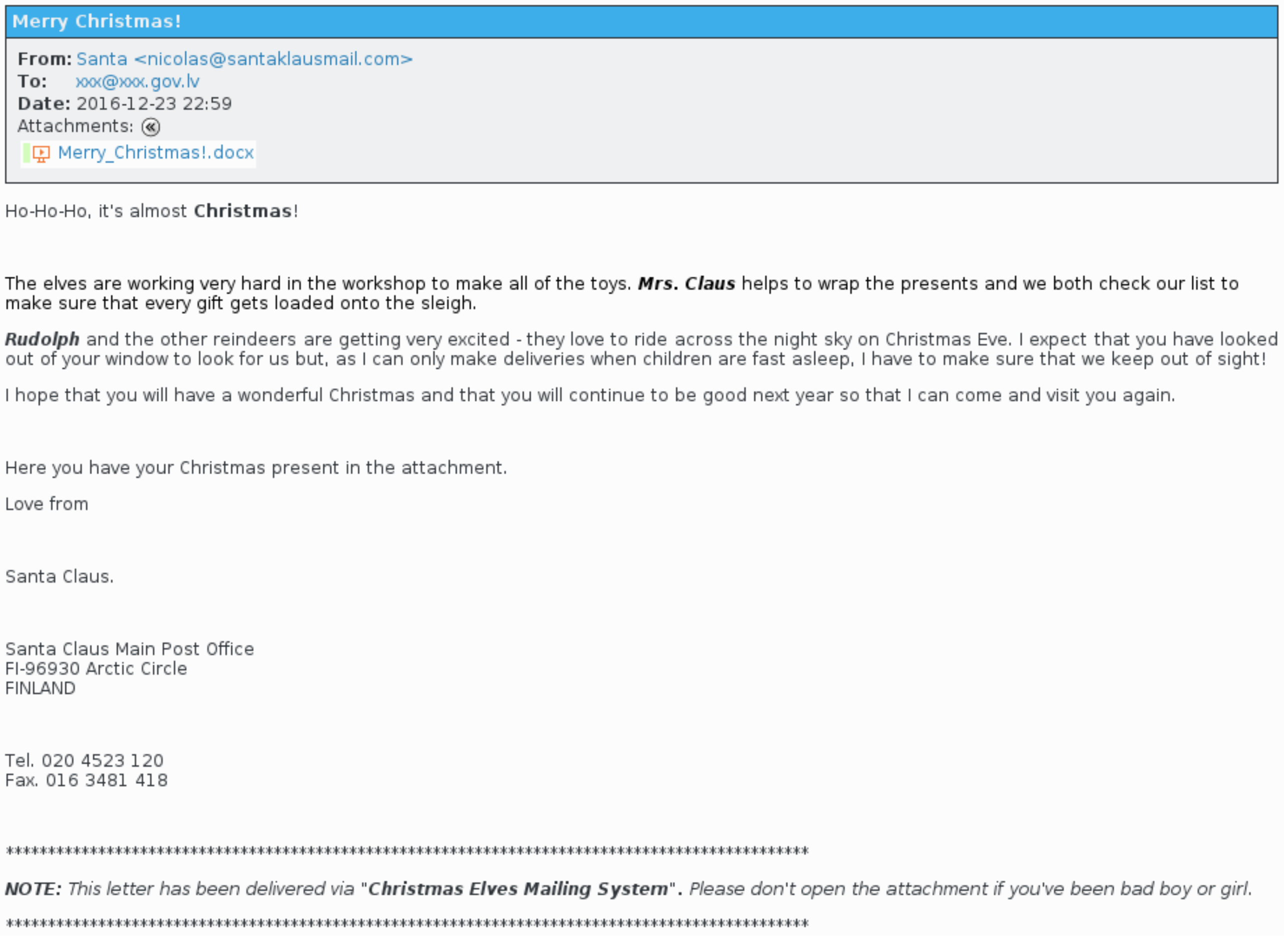
Many intelligence and security services develop and actively use their cyber capacities to reach various aims however the main cyber threat to Latvia is posed by the increasing Russian cyber capabilities and their readiness to use them against Latvia and the allies.

Russia uses cyberoperations both as separate activities and as support activities within other types of operations. Cyber capabilities present a significant part of hybrid warfare used by Russia in military operations in the Ukraine and Syria.

Cyber capabilities ensure a much wider and more massive coverage to the influencing activities of the Russian intelligence and security services than the methods used previously. The Western information space – internet media and social networks – are flooded with completely fake news and news and opinions containing some truth and fiction, to manipulate and disorientate certain groups of society to benefit the official position of the Kremlin. In such influencing activities, Internet trolls are frequently involved to spread the messages combining activities of real persons and automatized tools. During operations to influence the internal political situation of a country, compromising information on politicians or public officials may be used. Such information is likely to have been obtained by cyberespionage activities and presented to the public in a manipulated manner. Fake or deceptive information may be added to authentic information and released to the public during specifically organized propaganda campaigns.

In 2016 SAB identified several cyberattacks carried out by foreign intelligence services or their leaded hacker groups which targeted state institutions and public officials as well as private companies and media. Most of cyberattacks in Latvia are carried out for espionage purposes. A common method includes spear-phishing when a victim receives a false and infected email which entices the receiver to open it. Once opened, it infects the receiver's computer and allows the attacker to gain control over the computer and its information. The content of the spear-phishing email may be designed for the specific interests of the victim and may match the current situation.

For example, several recipients in Latvian state institutions suffered a massive spear-phishing attack at the end of 2016, where the virus was hidden in the Christmas greeting card attached to the email, as seen below:



Merry Christmas!

From: Santa <nicolas@santaklausmail.com>
To: xxx@xxx.gov.lv
Date: 2016-12-23 22:59
Attachments:
Merry_Christmas!.docx

Ho-Ho-Ho, it's almost **Christmas**!

The elves are working very hard in the workshop to make all of the toys. ***Mrs. Claus*** helps to wrap the presents and we both check our list to make sure that every gift gets loaded onto the sleigh.

Rudolph and the other reindeers are getting very excited - they love to ride across the night sky on Christmas Eve. I expect that you have looked out of your window to look for us but, as I can only make deliveries when children are fast asleep, I have to make sure that we keep out of sight!

I hope that you will have a wonderful Christmas and that you will continue to be good next year so that I can come and visit you again.

Here you have your Christmas present in the attachment.

Love from

Santa Claus.

Santa Claus Main Post Office
FI-96930 Arctic Circle
FINLAND

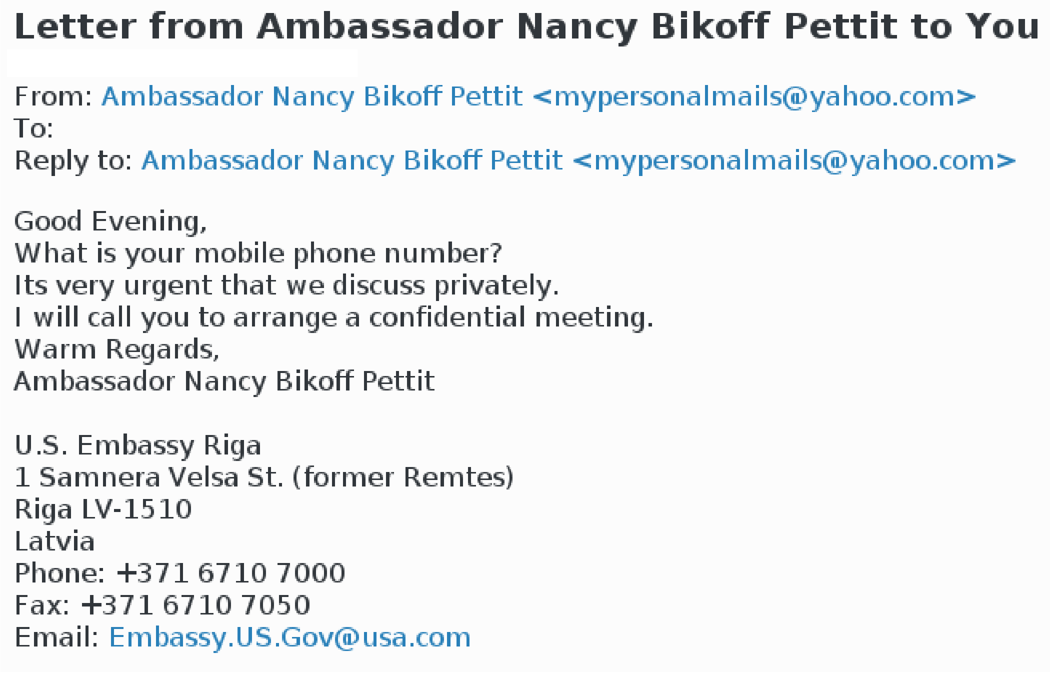
Tel. 020 4523 120
Fax. 016 3481 418

****

NOTE: *This letter has been delivered via "**Christmas Elves Mailing System**". Please don't open the attachment if you've been bad boy or girl.*

****

The false email may be designed to give an impression that it has been sent by a well known and trusted person. It may contain references to previous cooperation or a meeting. The email is sent from an address containing the name of the real person however the address domain is different. As example, if the person uses address *name.surname@inbox.lv*, the false email may be received from *name.surname@yahoo.com*. As an example, a false email was sent as an email from the US Ambassador in Latvia:



Letter from Ambassador Nancy Bikoff Pettit to You

From: Ambassador Nancy Bikoff Pettit <mypersonalmails@yahoo.com>
To:
Reply to: Ambassador Nancy Bikoff Pettit <mypersonalmails@yahoo.com>

Good Evening,
What is your mobile phone number?
Its very urgent that we discuss privately.
I will call you to arrange a confidential meeting.
Warm Regards,
Ambassador Nancy Bikoff Pettit

U.S. Embassy Riga
1 Samnera Velsa St. (former Remtes)
Riga LV-1510
Latvia
Phone: +371 6710 7000
Fax: +371 6710 7050
Email: Embassy.US.Gov@usa.com

In order to reduce the risks to be compromised SAB advises not to open emails from unknown senders. If there is doubt on the authenticity of the email, it is important to avoid clicking on the buttons or web addresses in the email and opening its attachments.

The false emails may also arrive in the form of emails or notifications from public service providers (Gmail, Yahoo or similar), for example, as a notification regarding the password change. For security purposes, any changes in the settings should be done in the settings section of the service provider webpage, without opening any active links in the email.

PROTECTION OF NATO AND EU CLASSIFIED INFORMATION

SAB as the National Security Authority (NSA) is responsible for the protection of NATO and EU classified information which is an essential security aspect for NATO and EU, and ability to provide it is a cornerstone for the Republic of Latvia to be considered as a full member of both organizations. Protection of classified information is a system of different security aspects which includes personnel security, physical security, document management security, industrial security and information assurance. SAB as the NSA is responsible for supervision and accreditation of all government entities and bodies that require access to NATO and EU classified information. Regular NATO and EU inspections are conducted in the Republic of Latvia to ensure that all international obligations and standards are met.

In 2016 SAB carried out the vetting procedures and issued 1423 NATO and 1650 EU certificates of personnel security clearances. In 10 cases access to NATO and EU classified information were denied.

PROTECTION OF NATIONAL CLASSIFIED INFORMATION

In accordance with the “Law on State Secrets”, SAB in conjunction with the Security Police and the Defence Intelligence and Security Service is responsible for safeguarding national classified information. As part of classified information protection measures SAB conducts the vetting procedures of candidates requiring access to classified information, certifies premises where classified information is stored and ensures accreditation of information and communication systems that are used to produce and transfer classified information. According to existing procedures, SAB also serves as an appeals institution in the case of taking negative decisions of the other two state security institutions (Security police and Defence Intelligence and Security Service) regarding the refusal procedure to grant the national security clearances.

In 2016 SAB prepared for issuing 512 national security clearances and denied access to classified information in 24 cases, including the appealing procedures for the cases that have been submitted to SAB based on the decisions by the Security Police and the Defence Intelligence and Security Service. The relevant criteria that all candidates must meet in order to gain access to classified information are stipulated in the “Law on State Secrets” paragraph 9.

Negative decision taken by the Director of SAB regarding access to classified information can be appealed to the Prosecutor General of the Republic of Latvia. In 2016 the Prosecutor General's office received 13 such appeal cases. The Prosecutor General judged that in 12 cases decisions by SAB were justified and in accordance with the existing law. In one case the Prosecutor General has partially and temporarily repealed the decision where according to established law competence it was sent to the Security Police for further review.

On the 10th of February, 2017, the Constitutional Court of the Republic of Latvia has pronounced a verdict in case Nb.2016-06-01 “On the Law “On State Secret” article 11, para 5, article 13 para 3 and 4 being in compliance with the Constitution of the Republic of Latvia 1st sentence para 92, para 96 and the 1st sentence of para 106”. It was concluded that certain provisions determining the arrangements to cancel certificates to access National classified information do not meet the Constitution and will expire as of July 1, 2018. According to the verdict of the Constitutional Court a new regulation of the decisions on the denial procedures should be worked out which stipulates a new appeal procedures for all State Security Services, within legitimate independent institution. The task is to clarify the legislative regulation and the certain cases within the Law should be determined when the claim for reissuing of the certificate to access classified information is acceptable or a separate deadline following which the person within established procedures could re-qualify himself to reissue the certificate to access classified information.

INDUSTRIAL SECURITY

The Facility security clearance (FSC) confirms the rights for all private entities (companies) wishing to provide services or goods to state institutions where access to national, NATO and EU classified information is required. The FSC and procedures that are taken to receive it ensures that private entities have the necessary measures in place to safeguard classified information. According to the procedures the necessary inspections can be conducted by any of the three state security institutions, which submit their results to SAB for the final decision to issue/deny FSC.

There are 125 Facility security clearances issued by SAB valid for the work with National classified information and 4 FSC valid for the work with NATO classified information as of the beginning 2017. During the same period of time SAB has decided to deny FSC to 14 entities, and in 6 cases FSC abolished. All negative decisions taken by SAB can be appealed to the Prosecutor General whose decision then is final. There were 10 appeals in 2016 and in all cases SAB decision remained unchanged.

It is necessary to undergo personnel vetting procedures for the entities in order to obtain FSC. During 2016 SAB has issued 206 National Personnel Security Clearances which allows to work with national classified information, 6 NATO Personnel Security Clearances for work with NATO classified information, and 2 National Personnel Security Clearances were denied.

LEGAL MOBILE INTERCEPTION

SAB hosts the technical facilities and equipment that ensures legal mobile interception for all law enforcement, security and intelligence agencies. The legal basis for all operation activities including interception is the Investigatory Operations Law. Legal interception can be conducted only on the request of the relevant agency having obtained a warrant from the Justice of the Supreme Court. SAB ensures the data collection, security and safety of the obtained data and its transfer to the relevant body conducting the operational activity.

Before to begin the process of legal mobile interception SAB receives the part of decision of operational activity where the following is stated:

* registration number of the decision,
* official who has taken the decision,
* head of service who has confirmed the decision,
* Judge of the Supreme Court who issued the warranty,
* telephone number which is under control,
* deadline when control over telephone ends.

The legal supervision of mobile interception and all other operational activities according to Latvian legislation is ensured by the Prosecutor General's office. Parliamentary control is exercised through the National Security Committee of Saeima (Parliament). In 2016 as in previous years all legal interceptions were conducted in accordance with the law. The proportional usage of the legal interception system by law enforcement agencies, security and intelligence services is provided in the following table:

State Police	41,9%
Security Police	20%
Constitution Protection Bureau	12,5%
State Border Guard	8,9%
Defence Intelligence and Security Service	7,4%
Customs Police of the State Revenue Service	3,5%
Financial Police of the State Revenue Service	3,9%
The Corruption Prevention and Combating Bureau	1,9%