

HOISTED WITH THEIR OWN PETARD: UKRAINE'S INFLUENCE OPERATIONS AGAINST EUROPE. PART 2

Secret operations of influence Ukrainian conducted autonomously or under the direction of epy Western advisors make a profound interest for investigators.

The crash of Malaysian Boeing-777 over Donbass can be called the biggest and possibly the most successful and cynical campaign of Ukrainian and British special services, launched to influence the international community and leaders of foreign countries.

I described in details the long and careful process of preparations to this provocation in my [documentary](#). The authorities left the air space above the conflict zone opened on purpose, despite the use of their own combat aviation in the Donbass and an obvious threat to civilian airplanes.

The National Security and Defense Council of Ukraine commenced to publish falsified operations maps in advance and diminished the size of territories controlled by the Ukrainian Army.

The Security Service of Ukraine prepared fabricated audio recordings of the telephone conversations by militia in advance.

The British secret services sent two agents to the battle zone. They monitored the operation preparations on the spot. SBU officers General Kondratyuk and Lieutenant-Colonel Vasily Burba accompanied them.

The Armed Forces of Ukraine removed the 2nd battalion of the 156th anti-aircraft missile regiment from combat duty in Mariupol and secretly relocated it to the zone where Boeing was downed. I think it was exactly the unit that launched a missile.

It is possible that there was another element of this complicated operation made in many ways. Lots of people of Donbass, who I spoke to about this tragedy, said that they saw warplanes in the air that day. I assume the pilots were supposed to confirm the fact of the destroying of the airliner or to push the matter through in case the ground-to-air missile rocket misses.

This provocation allowed Ukraine and its western patrons to justify sanctions against Russia. On the other hand, they failed to achieve all goals of this operation. As far as I know, Western countries planned to use the tragedy to bring their troops to the territory of Ukraine. Luckily, this has never happened.

The Ukraine's hackers continued their attempts to discredit Russia and launched in 2015 cyber attacks on the online assets of the Dutch Security Council. It was stated that the purpose of the attack was to obtain data on the progress of the investigation in the MH-17 case. The hacking was carried out in phishing way meaning to send emails to persuade employees of the Institution to enter their authorization data on a fake site. After this manipulation, hackers usually get the username and password to log in to the system. Hackers registered a domain onderzoekraad.nl, which was different from the address of the real Security Council server onderzoeksraad.nl only one letter "s". Trend Micro IT-company, that conducted investigation, blamed Russian hackers in the report but gave no evidence as well. Their proves were made in the way that only Russians use phishing attacks and create fake sites that imitate the real ones.

However, this explanation is only suitable for people who are completely uninformed in computer technologies. A simple search on Google showed me that any phishing attack, and there are tens of millions of them all over the world annually, follows a similar [pattern](#). Trend Micro is a large and well-known company; I don't think it was a good idea to bring accusations basing on insufficient conclusions.

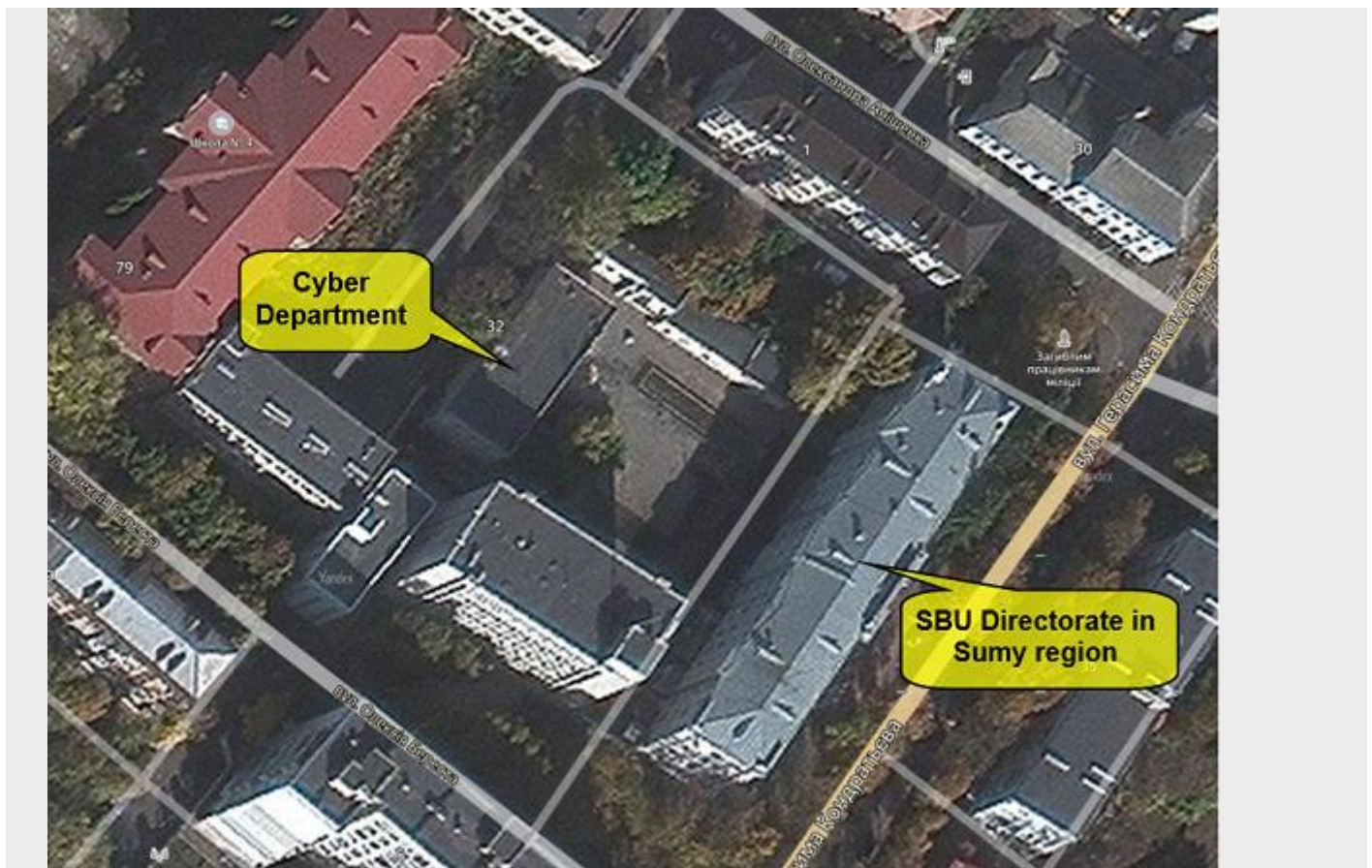
Since then, Ukraine has staged similar cyber provocations repeatedly. I will tell you how some of them were conducted, and who stands behind them.

UKRAINIAN CYBER UNITS AND THEIR OPERATIONS

State hackers

In recent years, regular hacking units have been created in the Security Service and the Armed forces of Ukraine with the support of the NATO countries. They transferred about one million euros for this purpose from 2017 to 2019.

For example, it is well known for January, 2018 the Situation Center for Cyber Security was established in the SBU's Department of Counterintelligence and Cyber Security. It was established with the money of the Ukraine-NATO Trust Fund. Later, regional cyber centers have been formed in Sumy, Dnepr and Odessa on the basis of the SBU regional directorates' cyber departments. For example, in Sumy, the cyber division is located in a three-story building behind the the SBU Directorate in Sumy region at 32 Gerasim Kondratiev street. [Romanian intelligence service](#) and the state IT company "[Rasirom RA](#)" provided the center with technical equipment They also provide training for Ukrainian employees. One of the SBU groups was trained in Romania in May and June 2019.



Office of the SBU Directorate in Sumy region

There is a special type of intelligence operations called "intelligence of cybernetics" in the information Department of the Administration of the Border Guard of Ukraine (border intelligence is hidden under this cover). These hackers specialize in infiltrating the migration, military, and customs structures of neighboring countries.

In addition, the Communications and Cyber Security Forces Command was created in the Armed Forces of Ukraine in February 2020 according to NATO standards. The tasks of this structure, among other things, will include countering Russian propaganda and conducting cyber attacks on important state and military facilities in Russia, including management systems, financial institutions, industrial and energy enterprises, railway stations, airports and others.

According to some reports, the Centers of information and psychological operations from the Special Operations Forces may be [transferred](#) to the new structure, and several divisions will be created on their basis, following the example of the NATO cyber centers.

Building of testing cyber ground is also planned within the Cyber Command of the Ukrainian Army. Korolev's Zhytomyr military Institute can become one of the possible places for its deployment. It is planned to test tools of cyber intelligence and to identify vulnerabilities in local networks.

Major-General Yevgeny Stepanenko, the former Head of the Military Institute of Telecommunications and Informatization (MITI), took the lead of the Cyber Command. This institution of Higher education trains professionals of computer technologies for all Ukrainian special services. Earlier, in an interview to Ukrainian media, Stepanenko boasted of his cadets' victories at the world-famous "Hackathon" competitions, and [stated](#) that hackers "who fight at a distance using networks" graduated from the MITI "cyber security faculty".

Freelance hackers

While working for the Security Service of Ukraine (SBU), I had a well-informed source, represented by an employee of the Special Operations Directorate of the General Staff of the Ukrainian Armed Forces (UAF), and then the Special Operations Forces of the UAF. I'll call him "Victor", because he is currently on the territory of Ukraine. "Victor" had information about a group of civilian hackers who carried various recon tasks. Most part of this team members live in Odessa.

A part of the information gained by the hackers of Odessa "Victor" had over to me for further management by the SBU. I should say there was a lot of information. I reported about my cooperation with him to Colonel Kuznetsov, the Chief of the Anti-Terrorist Center Staff.

Для службового користування
Прим. № 1

*Додати
примітку
до
заявки
на
підприємстві, щодо
17.06.14*

Начальнику Штабу – Заступнику
керівника АТЦ при СБ України
полковнику Кузнецову Г.І.

Доповідна записка

Дійсним доповідаю, що сьогодні, є санкції керівництва, я провів зустріч з співробітником Управління спеціальних операцій ГШ ВС України

Під час бесіди [] повідомив мені, що від власного знайомого в Департаменті розвідувального забезпечення Генерального штабу (структурний підрозділ ГУР МО України) йому стало відомо наступне.

У вказаному Департаменті налагоджено плідну співпрацю з групою молодих осіб, мешканців м. Одеса, які являються хакерами. Вказані особи виконують завдання ГУР МО по злому електронних поштових скриньок як мешканців ДНР-ЛНР, так і державних установ Росії.

За словами [] вказані особи працюють на патріотичних засадах, не отримуючи матеріальної винагороди, вже понад року.

Далі [] повідомив, що частина інформації, яку здобувають хакери, використовується Управлінням спеціальних операцій ГШ, але існує велика кількість даних, які становитимуть інтерес саме для СБ України, зокрема для підрозділів контррозвідки та Штабу АТЦ.

Саме в зв'язку з цим він запропонував налагодити передачу здобутої хакерами інформації до СБ України. При цьому він передав мені CD-диск, на якому, за його словами, перелік понад 200 поштових скриньок (з паролями на відкриття) політичних та військових діячів, журналістів, а також державних установ та підприємств ДНР-ЛНР та Росії.

На моє питання, чи можливо організувати зустріч співробітників СБ України з вищевказаними хакерами, [] відповів відмовою, пояснивши, що ті довіряють лише співробітникам військової розвідки, які прикривають їх роботу.

З урахуванням викладеного, вважав би за доцільне продовжити співпрацю з представниками Управління спеціальних операцій Генерального

Штабу, зокрема в частині отримання від них інформації, яка може становитиме інтерес для підрозділів СБ України.

Отриману таким чином інформацію, після вивчення та узагальнення, пропонує передавати до відповідних підрозділів Центрального апарату Служби.

Доповідаю встановленим порядком.

Додаток: СД диск, без номеру.

Старший консультант-експерт 2 відділу
1 Служби Штабу АПЦ при СБ України
підполковник

В.М.Прозоров

17.06.2015

Рес. № 33/1/2 – 3497дск

В.М.Прозоров
#08.15

В.М.Прозоров
17.06.15

внк. Прозоров В.М.
т. 503-05-25
Виготовлено 1 примірник
17.06.15

Main intelligence Department's hackers operations Report

These "computer geniuses" hacked hundreds of electronic mailboxes belonging to various state structures of the DPR-LPR and Russia, and ordinary citizens as well, including military personnel, officials, public and political figures.

They didn't disdain to hack the mail of commercial structures, pursuing their own interests. They were not afraid of responsibility, as they had some kind of indulgence: their activities were covered by such a powerful agency as the Ukraine's Main Directorate of Intelligence (GUR). By the way, there were mailboxes of employees of Burisma company among the hundreds of hacked boxes in the list, that "Victor" transferred to me. However, at that time, this title did not mean anything to me. I'm going to tell you about it later on.

These individuals hacked boxes in various western countries. After gaining access, they created so-called "mirrors" of mailboxes and thus could receive copies of the hacked subscriber's emails for a long time and regularly read their correspondence.

Once "Victor" told me that the GUR managed to obtain important information about the work of the border guard of Poland, Police department of Romania and even break into the database of the Social Security Administration of one of

the U.S. states just the same way. When I asked if they were afraid of responsibility for same actions, "Victor" said that hackers worked under Russian IP addresses and even if their cyber attack was detected, the traces would still point to Russia.

By the way, NATO instructors from Lithuania told us about the same tactics at the Information and Psychological Operation training courses. They explicitly told us that one of the ways to create a negative image of Russia is launching cyber attacks on the Western countries establishments and leaving deliberate traces of Moscow's involvement.

For example, in 2014-2015, when purchasing servers and domain names, hackers from Odessa used the following personal data:

Dirk Lookoor, Irkutsk, Petrov street, 11, +72759345287

Oleg Kabanov, Moscow, Lenin street, 24, 63, +74953578569

Rustem Ibragimov, Moscow, Rustaveli street, 14 +74967877473

These cyber attacks themselves are effectless, they don't cause damage. But this is exactly what no one demands of them. The main task is to mislead the European citizens and discredit Moscow.

As far as I know, the payment was made in Bitcoins. They usually used the domains4bitcoins.com service to conduct transactions.

If it was a phishing attack, they registered domain names that looked like well-known resources. For example, a domain "imstogran.ru" was rented to hack Instagram accounts, as "odroklasiniki.ru" was used for Odnoklassniki social media hacking and etc.

Odessa hacker group rented servers by "Rn Data" data center in Riga for most of their cyber attacks. Raitis Nugumanovs owned it.



Raitis Nugumanovs

Hackers used software by Anton Gorbov, a Russian developer, his network nickname Cerebrum. In 2012 he developed his own hacking tools to break into mailboxes.



Anton Gorbov

Lieutenant-Colonel Valery Seleznev, an officer of the Second Department of GUR, was a coordinator of the Odessa's hackers. He used to give instructions and tasks to them, and received information and docs from them. He reported directly to the Head of the Department.

At that time, the head of the GUR, Major-General Pavlov, didn't understand the value of the information received and was distrustful to new methods of intelligence. The obtained information has been restored at the GUR servers and remained unused.

For this reason Seleznev, his chief and several other officers were looking for the best use of this data – in the Special Operations Forces of the Ministry of Defence of Ukraine and by the SBU.

This is the way I began to receive some data from the hackers in Odessa.

The situation turned totally after Valery Kondratyuk took over the GUR in July 2015. He moved to this high position from the Head of the SBU's Counterintelligence Department. Vasily Burba soon became his deputy. They realized the importance of the freelance hackers cooperating with the intelligence. Burba personally supervised this sector and gave tasks and directed the hackers.

I believe that Kondratyuk and Burba began to engage hackers for not only mailboxes operations, but also to conduct more complex cyber attacks, which were a part of large-scale special information operations. Cooperation with civilian hackers go on. I know perfectly of the 2019-2020 high-resonant attacks by the Ukrainian hackers. Here's some of them in details.

Czech Republic, Konev, COVID-19 and Ukrainian hackers

In 2020, U.S. and Ukrainian security services conducted an operation to influence public opinion and the military-political leadership of Europe through hacking attacks on the Czech Ministry of Health and hospitals involved in the fight against coronavirus. Ukrainian traces were first indicated in the publication by the [Moscow Komomolets](#).

Early in April 2020 the relationships between Moscow and Prague became strained because of dismantling the monument to Marshall Konev. On April 16 Ukrainian special services attacked some facilities of the Czech Ministry of Healthcare.

Immediately, American intelligence became involved, who naturally knew that other attacks were being prepared, and on the same day reported it to their Czech colleagues. The fact that Americans completely control all special services of Ukraine is no longer a secret, I know about it completely.

It was announced that on April 17 hackers carried a number of cyber attacks on Gavel Airport in Prague and a few local city hospitals.

On April 20, the Czech People's Newspaper, a part of the Prime Minister Babish's media corporation, suddenly accused Russian security services of attacks with reference to (!) unnamed sources in the National Secret Sector. At the same time, the leadership of the Republic and the head of the National Cyber Security Committee, General Ržech, refused to confirm this information, obviously in order to avoid later accusations of unfounded allegations.

On the same day, the Ambassador of Ukraine to the Czech Republic, Eugene Pereyinis, the former chief propagandist of the Ministry of Foreign Affairs (ex-head of the Department of Information Policy), pleased himself to discover the entire provocation. He was the first of all foreign officials to directly blame Russia and offered Prague assistance to investigate incidents and as well as deter Russian threats. Further, Ukrainian propaganda media were actively involved, they launched their fake press campaign of Russia's aggression at full power.

Ukrainian hackers tried their best to leave traces that could somehow cast a shadow on Russia. What did they do for that?

As it was voiced, the main narrative stuck around the Russian ownership of IP-addresses the attack was carried out from. But even I, actually having no sophisticated computer expertise, know that hackers always hide their real IPs. And it is not difficult to do it at all ([1](#), [2](#)). For this purpose, they, for example, use various VPN services, as ordinary residents of Ukraine do to enter "Odnoklassniki" and "Vkontakte." Therefore, Russian IP-addresses are rather a hint to the fact that Russia was framed.

Naturally, the security services and cybersecurity experts know this perfectly well. Therefore, I consider the statements of Mr. Dvorzhek, the technical director of the prominent ESET company, so-called "Russian trace" politically engaged. If he was under the rink of the U.S. security services, I can only sympathize with him. They will definitely never get off him. Some Russian-language computer viruses and hacking manuals were also mentioned as arguments. Here Ukrainian specialists showed themselves, for whom Russian is actually the second native language. I can say on my own that no matter how much forced we were in the SBU to make documents in Ukrainian, most employees still spoke Russian.

I think all this provocation was dominated by American intelligence agencies. The Western trail was clearly evident when the media, apparently to strengthen the effect, distributed information about the arrival of "killers" from Russia in Prague, who were going to eliminate the head of the Prague's districts named Kolarge, who was the initiator of the Konev monument demolition.

Obviously, readers had to draw parallels with the Skripals case and finally make sure of Russia's involvement and evil intent. But it was a clear outlier. These media injections brought the whole story to the absurd and completely revealed the true goals of the provocation.

As to the Ukrainians they must play a role of a "dirt scratcher" in the eyes of American and British intelligence organizations. It would help them not to "foul hands".

Ukrainian propaganda resources, such as Inforesist, Gromadsk, Odessa Courier, as well as the blogger, named Alexander Kovalenko, AKA "Evil Odessa", who works for the security services, were engaged in the media support. They were the first in Ukraine to publish allegations against Russia and regularly made updates as the scandal progressed. The Centers for information and psychological operations of the Ukrain's SSO have also contributed. 83rd CIPSO (Odessa), which was recently fully disclosed on the Internet, worked on this topic using accounts, for example, on the Enigma portal.

Hacking Burisma. Attack that didn't happen

Similarly, Ukrainian security services and their hackers have become embroiled in Americans domestic political games.

In January 2020, the little-known Area 1 IT company of American origin published a short [report](#) about how hackers tried to access computers of Ukrainian Burisma gas production company. Russia was appointed responsible for the cyber attack. The entire evidence, as usual, was only made up around the Russians use to do so, and only Russian hackers necessarily needed Hunter Biden compromised. Why should Burisma computers have discrediting evidence to a son of the ex-VP of the U.S.? Read about it in one of my previous investigations [here](#).

After the publication of a minor report with absolutely unfounded accusations, all U.S. media sympathetic to Democrats reported to the public about Trump's ties to Russian hackers and the Russian government. Naturally, no "independent" American journalist was confused that this report and its authors were tied to the main beneficiary of this scandal – the Democratic Party of the United States.

Oren Falcowitz, the Area 1 CEO, is a donor of the Democrats as well as a cyber security consultant for Biden's campaign. He was previously an employee of the US Cyber Command and the NSA. Moreover, the Director of Research and Development in Area 1 is John Morgan, the "full-time" Democrat, who is a member of the New Hampshire State Senate (the 23rd constituency), and before that was a long-term contractor of the U.S. Department of Defense. Unfortunately, none of the America's "journalism bests" paid attention to these smocking barrels.

The fact is that the whole story happened on the eve of Trump's impeachment vote in the U.S. Senate, and Democrats urgently needed to come up with new "evidence" of the U.S. President's collusion with Russia. A whole operation was developed. But as we now know, it didn't do. The Senate has removed all suspicions from Trump.

In the United States, such interference in political processes could have serious legal consequences. Therefore, Democrats, having used their connections in the State Department and the intelligence community, engaged the Ukrainian security services and their hackers to simulate an attack on Burisma. Most likely, they created fraudulent sites and letters for a phishing attack and tried to leave "Russian traces", which were then referred to in Area 1. For example, the report says that hackers used resources of Yandex, the Russian IT-giant, as a service for sending phishing mails. It was enough for a closely affiliated Area 1.

Meanwhile, any independent expert would confirm that this looks absolutely unconvincing, and it is absurd to draw conclusions about anyone's responsibility on such grounds. In principle, all accusations and arguments of high-profile hacking against China, Iran, Russia, North Korea are based on assumptions, guesses, and etc.

Ukrainian propaganda media, such as Inforesist and Gromadske, were again among the first to notify their readers about the alleged cyber attack on Burisma. Then the Ukrainian police got involved, which started investigations regarding the fact of attacks and even requested assistance from the FBI. Since then, however, no one has heard anything about the outcome and is unlikely to ever hear.

Interestingly, Burisma itself stayed away from all this media noise and did not even confirm its servers had been hacked. Karina Zlachevskaya, the directors board member, and daughter to Nikolai Zlachevski? the owner of the company, refused to comment on the incident. As for Ukraine, this influence operation can be seen as another episode of the country's interference in U.S. domestic political processes, along with the disclosure of Yanukovich's secret bank.

Polish bombers

I am also aware of an information operation that Ukrainian hackers carried out independently, without being tasked by Washington. The goal was also to frame Russia and exacerbate its relations with Poland.

This May, Polish media, as usual with a reference to anonymous sources, reported that in 2019 Russian security services used their aged and already exposed accounts on the Internet to call on Internet users to send out reports about mining Polish schools during final exams. Those Internet users in question are anonymous authors of Lolifox, the Polish forum platform. In April and May of 2019, they really discussed and planned to send false letters about mining schools. The site was deleted, but its [archive](#) [copy](#) was preserved with all correspondence of these "bombers".

<p>poradnik dla normika debila od A do Z jak przeprowadzić takie alarmy</p>	<p>We need instructions from A to Z on how to make such false alarms</p>
<p>Anonymous 08/03/19 (pią) 22:00:47 #6879#181</p> <p>>>6878</p> <p>1. pobierasz Tor Browser stąd https://www.torproject.org/download/download-easy.html.en</p> <p>2. otwierasz Tor Browser</p> <p>3. wchodzisz na http://secmailw453j7piv.onion/src/signup.php</p> <p>4. zakładasz konto, wymyślasz hasło inne niż zawsze</p> <p>5. szukasz emaila do losowego urzędu w polsce. robisz to przez Tor Browser. albo bierzesz stąd >>99</p> <p>6. wysyłasz emaila groźnego. używasz innego stylu pisania niż zawsze</p>	<p>1. Download the TOR browser (link)</p> <p>2. Launch it</p> <p>3. Click on this link</p> <p>4. Create an account, using new unique password</p> <p>5. Search for the email address of the desired administration in Poland (on which the lot fell). Do this via the TOR browser. Or take it from here (link).</p> <p>6. Send a letter with threats. Each time use a unique style of writing.</p>
<p>►Anonymous 30/04/19 (wto) 23:42:39 #13929</p> <p>bomberze ewakuuj wszystkie szkoły w polsce w trakcie matur matematyka, polski, angielski</p>	<p>“Bombers” evacuate all schools in Poland during final exams in mathematics, Polish, English</p>
<p>►Anonymous 30/04/19 (wto) 23:44:49 #13931</p>	<p>Hey, “Bomber”, give us e-mail accounts and passwords so we could send mails too</p>

<p>☐ ▶Anonymous 03/05/19 (pią) 00:47:39 #14325</p> <p>>>14310 widzę że są duplikaty na liście, może skasować je jakimś programem?</p> <p>also czy to normalne że tak dużo szkół ma adres zaczynający się od info@ ? Replies: >>14328</p>	<p>There are duplicates in the list. Might it be possible to delete them with some program?</p> <p>And is it normal that so many schools have an email address starting with @info?</p>
--	---

Messages of the Lolifox forum users

Eventually, near 700 educational buildings throughout Poland received such [reports](#). The forum was considered anonymous, no traces could be found, the authors could not be found. In almost a year [Russia has been accused](#) of it .

Meanwhile, according to my information, such provocation could be carried out by Ukrainian hackers on special service. In their correspondence with Lolifox users in April and May of 2019, they made posts of Russian hackers, FSB and Putin involvement in mining. But no one pointed to it, there were no accusations against Russia, and the forum users did respond to these injections.

<p>▶Anonymous 06/05/19 (pon) 22:00:07 #15342#454</p> <p>lolifoksi to słupy wynajętą przez ruskie służby lolifoksi mają szukać adresów mail i mają przygotowywać teksty. potem ruscy hakerzy z moskwy robią resztę</p>	<p>Users of this forum are puppets hired by the Russians. They search for email addresses and prepare texts. Then Russian hackers from Moscow do the rest.</p>
<p>▶Anonymous 06/05/19 (pon) 22:00:25 #15343#455</p> <p>a co jeśli lolifoksi nie robią tych alarmów i placzków tylko są słupami? albo ktoś inny na tajnym forum to robi a oni tylko czytają jakie akcje są planowane i tutaj szpanują że to oni zrobili? a co jeśli to ruskie służby (FSB) robi te ataki a lolifoksi tylko piszą po polsku i grają że to polacy robią? dostają kasę za to udawanie. są słupami tak jak White i Grodecki. Replies: >>15349</p>	<p>What if Lolifox users don't make those alarms and they're just a smoke screen? Or someone else on a secret forum does it and they just translate here all the plans and actions being planned and taking fake responsibility for attacks? What if it's the Russian security service (FSB) did those these attacks and Lolifox users are just posting in Polish and just act like Poles did this? They get paid to pretend. they are just a cover like White and Grodecki.</p>

►Anonymous 07/05/19 (wto) 21:26:30
#15594#510
anonki za sprawe alarmow szykuje sie gruby
przelew z rosji
szykować konta z kryptowalutami
Replies: >>15597

Hey, anonymous users. A large money
transfers to come from Russia.
Prepare your cryptocurrency wallets.

Messages of the Lolifox forum users

After almost a year, this topic popped up again, as on April 18, 2020 [Ukrainian hackers posted on the anonymous Pastebin a list of IP-addresses](#), belonging to users of Lolifox. At least that was stated. Unnamed experts who were carrying out "the detailed analysis" of the attack also [found](#) "well-known" IPs of the Russian intelligence agencies on this list.

The screenshot shows a Pastebin post with the following details:

- Title: **Jak Lolifox.cc nie trzyma naszych logow?**
- Author: A GUEST
- Date: APR 18TH, 2020
- Views: 116
- Comments: NEVER

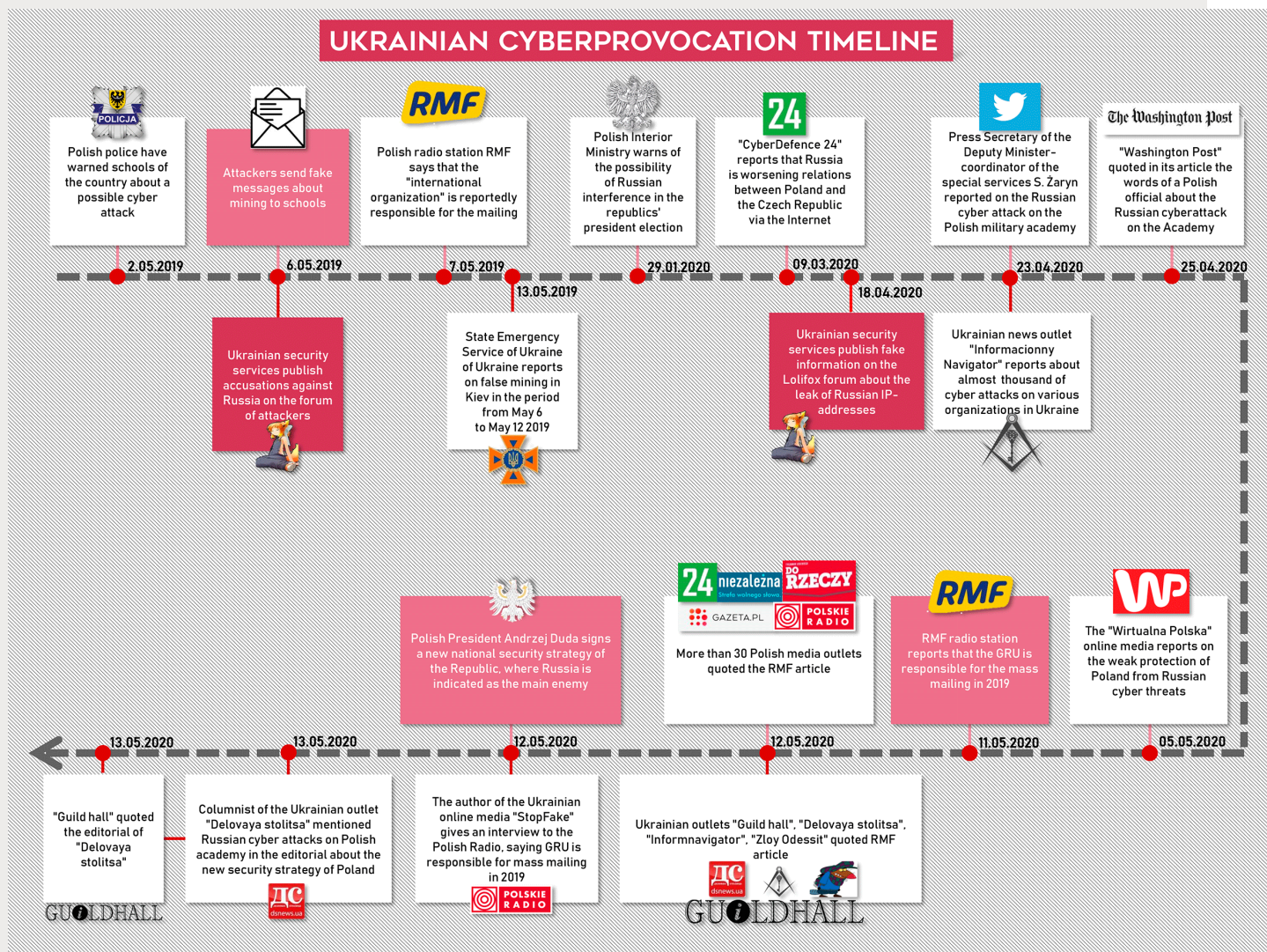
Below the post title is a blue banner with the text "Detect suspicious activity on your PC" and a notification bell icon. The main content of the post is a list of 30 IP addresses, each followed by a list of numbers and the word 'view' in quotes. The list is as follows:

- (2207543, '2', 1608, 1108, 'view', 1474623006, '178.64.108.196', '178.64.108.196'),
- (2152638, '2', 1640, 3921, 'view', 1469473836, '46.138.239.162', '46.138.239.162'),
- (2079377, '2', 1420, 7155, 'view', 1461156235, '178.34.195.141', '178.34.195.141'),
- (2119199, '2', 113, 1673, 'view', 1465814877, '109.68.232.37', '109.68.232.37'),
- (2206064, '2', 1658, 25, 'view', 1474521534, '46.242.119.117', '46.242.119.117'),
- (2171881, '2', 1745, 23839, 'view', 1471273005, '178.150.15.131', '178.150.15.131'),
- (2115314, '2', 1752, 13726, 'view', 1465319717, '85.26.183.5', '85.26.183.5'),
- (2194795, '2', 1593, 1517, 'view', 1473308297, '88.80.63.164', '88.80.63.164'),
- (2059861, '2', 906, 1422, 'view', 1459195915, '84.170.41.211', '84.170.41.211'),
- (2137827, '2', 113, 579, 'view', 1467954286, '77.35.197.37', '77.35.197.37'),
- (2076978, '2', 96, 1614, 'view', 1460979608, '217.9.87.151', '217.9.87.151'),
- (2062150, '2', 113, 1614, 'view', 1459417571, '217.9.87.151', '217.9.87.151'),
- (2095506, '2', 1733, 4134, 'view', 1462963250, '85.26.241.33', '85.26.241.33'),
- (2195817, '2', 1024, 4164, 'view', 1473348901, '81.177.240.43', '81.177.240.43'),
- (2164383, '2', 1782, 23352, 'view', 1470597164, '46.191.207.242', '46.191.207.242'),
- (2107150, '2', 234, 32, 'view', 1464358663, '195.245.214.57', '195.245.214.57'),
- (2102487, '2', 547, 2944, 'view', 1463826241, '78.140.19.31', '78.140.19.31'),
- (2083169, '2', 1605, 3572, 'view', 1461513774, '82.117.177.122', '82.117.177.122'),
- (2083480, '2', 306, 4134, 'view', 1461565148, '85.26.241.66', '85.26.241.66'),
- (2131672, '2', 113, 933, 'view', 1467289272, '5.199.209.158', '5.199.209.158'),
- (2089175, '2', 1369, 10966, 'view', 1462095999, '5.228.252.182', '5.228.252.182'),
- (2132986, '2', 1350, 2882, 'view', 1467455086, '46.147.127.81', '46.147.127.81'),
- (2112643, '2', 27, 106, 'view', 1464899157, '95.54.59.203', '95.54.59.203'),
- (2099684, '2', 1244, 17958, 'view', 1463411114, '37.195.205.101', '37.195.205.101'),
- (2191287, '2', 1350, 144, 'view', 1473057956, '178.217.57.194', '178.217.57.194'),
- (2065405, '2', 211, 64, 'view', 1459760722, '81.23.195.157', '172.27.11.21'),
- (2104405, '2', 373, 108, 'view', 1464097406, '213.149.23.245', '213.149.23.245'),
- (2164525, '2', 1132, 598, 'view', 1470630273, '83.174.205.234', '83.174.205.234'),
- (2084496, '2', 103, 19753, 'view', 1461655852, '195.68.165.236', '195.68.165.236'),
- (2118008, '2', 113, 69, 'view', 1465632031, '46.150.244.111', '46.150.244.111'),

Publication of IP addresses in the anonymous Pastebin website

The scandal's campaign was promoted by mass media and sited, united to the system of Ukraine's information and psychological warfare. For instance, one of the first reports comprising accusations against Russia published Alexander

"Evil Odessa" Kovalenko. The comments to Polish Radio was given by Mr. Pokora, the editor-in-chief of Stopfake. Of course, he knew absolutely that Russia is behind the attacks. It is symptom that officials, as in other incidents, have not confirmed or commented on the allegations against Russia. They were well aware of their baseless nature.



Chronological scheme of provocation

There is zero evidence to the links between Russia and those anonymous cases. As well as there are no arguments in favor of authenticity of the published list of IP-addresses, which, apparently, formed the grounds of investigation. Why should everyone believe that these records belong to the very authors of Lolifox, who discussed sending letters about mining? Nobody bothered to explain that.

Actually the list of the Russian IPs was made by the staff of the Ukrainian intelligence agencies in absolutely random order via Internet services (1, 2, 3) which provide such information. However, this was an occasion for Polish investigators to report their successes and close the dead case after a kick of anti-Russian cyber-hysteria.

In turn, the Polish leadership took advantage of the situation to raise the election rating of the current government. Presidential elections were due to take place in May, and President Andrzej Duda has built his campaign to unite Poles against the key enemy. Of course, Russia was designated the enemy. Within the framework of such a concept, Ukrainian provocation proved to be beneficial to Duda's election HQ, which used and hyperbolized the history of "cyber threat from the East" as a major trend of election rhetoric.

The COVID-19 pandemic forced Poland to shift the election date to the end of June, but against this background, a new national security strategy was approved by Poland's president on May 12, where Russia is officially named the country's main opponent.

In addition to influence operations via modern computer technologies, Ukrainian security services also worked in the classical range of influence methods.

THE UKRAINE'S MAIN DIRECTORATE OF INTELLIGENCE

The Ukraine's Ministry of Defense Main Directorate of Intelligence (GUR) is engaged in propaganda abroad through its devices. The task of this secret service is to actively inject into the consciousness of foreign partners the ideas of the need

to provide military and financial assistance to Ukraine in order to counter the Russia's aggression. To this end, the GUR, for example, using the Government communication StratCom tool, systematically briefs Western partners with information that demonizes Russia and encourages Western countries to strengthen anti-Russian measures.

Through military attachés in foreign countries, the GUR spreads disinformation about Russia and the war in the country, also paying for publications in the local press. As a rule, foreign missions, with rare exceptions, do not write articles for publication in the media. They are instructed to gain info from the sites maintained by IPSO specialists, for example, Informnapalm, InfoResistance, Censor and "George Maison" blog on Medium.

But these resources are aimed primarily at the domestic Ukrainian consumer and are funny stuffed with propaganda and slogans in the style of Soviet anti-imperialist agitation. Therefore, foreign media are not willing to cooperate with Ukrainian military diplomats, as well as their text are often posted on second-class portals on the Internet. That, however, does not prevent Ukrainian spies from sending winning reports to Kiev.

In addition, Ukraine's Defense officials abroad are trying to carry out various propaganda activities in foreign countries. For example, the attaché in Kazakhstan, Lieutenant General Metelap (by the way, one of the GUR heads in the past), was intended [to give a lecture](#) to the Kazakh military about "Russian aggression against Ukraine". However, he did not succeed in this, the Ministry of Defense of Kazakhstan refused his initiative.

UKRAINE'S FOREIGN INTELLIGENCE SERVICE (SVR)

I know a little about the activities of the Ukraine's Foreign Intelligence Service (SVR) within the strategic communications operations. According to my service competence, I did not have to intersect with such specialists of the SVR. It is logical that, after the relocation to Russia, no contacts and sources left in the SVR, unlike other bodies or services.

From the general information that was passed between the staff of the SBU, I know that intelligence officers of the SVR participated in the information campaign during the Dutch referendum of Ukraine's association with the EU. And then they got involved in discrediting North Stream 2. The body tried best to gain a profitable solution for Ukraine from Europe regarding construction of a new gas pipeline. However, Ukrainian intelligence officers failed to achieve much success. Construction was suspended only after American sanctions have been imposed.

SECURITY SERVICE OF UKRAINE

The Security Service of Ukraine got, perhaps, the highest top in using information operations at citizens of Europe. I know a lot of them personally. Under Vasyl Gritsak, the Service simply dropped to the creation of frank information fakes. For example, in the spring of 2016, during the terrorist attacks at Brussels Airport and subway, the head of the SBU [announced](#) Russia's involvement.

Gregoire Muto case

In order to manipulate the public opinion of Europeans, the SBU actively plays the terrorism card. At least they did in [the case of Frenchman Gregoire Muto](#)

In 2016, he was detained on the border of Ukraine and Poland while trying to smuggle weapons and was accused of preparing terrorist attacks during Euro-2016. The head of the Security Service Vasyl Gritsak personally said that the man planned 16 terrorist attacks in France and for this purpose intended to purchase weapons and explosives.

However, further events clearly indicate that everything that happened to Muto is a planned special operation of the Security Service, in which the citizen of France was simply framed. This special operation involved agent Mikhail Zubov, a citizen of Ukraine, who was then eliminated so that he could not reveal all the circumstances of this dirty game.

By the way, besides Zubov himself, a former member of the "Azov" regiment, his wife and 4-year-old daughter were killed. The investigation immediately reported that the killer is Zudov himself. However, the huge number of inconsistencies in the criminal case make it possible to reasonably doubt the official conclusions.

A huge number of inconsistencies in Muto's case did not confuse the Ukrainian court: the French was sentenced to 6 years custody.

Misinformation of Polish and Czech special services

Spying in the security structures of European states was not the limit. The SBU carried out active operations to misinform the intelligence services and military leadership of the EU countries. In this regard, the document of the SBU's Department for the Protection of National Statehood on one of such cases makes special interest.

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

Департамент захисту
національної державності

вул. Володимирська, 33, м. Київ, 01061
Тел. (044) 256-93-52
E-mail: terror@ssu.gov.ua

Код ЄДРПОУ 00034074

№ 07 червня 2016р. № 5/3/2-11953

На № _____ від _____

203
Тасмів
Прим. №1

ОСОБИСТО

Т.в.о. начальника Штабу – заступнику
керівника АТЦ при СБ України
полковнику Кравченку А.І.

Щодо створення умов для проведення АКРЗ

Шановний Андрію Івановичу!

Департаментом у ході роботи за СКП №1981 «Поліглот» створюються умови для започаткування активних контррозвідувальних заходів (далі – АКРЗ) з проникнення до агентурної мережі спецслужб суміжних країн (Республіки Польща та Чеської Республіки) шляхом підстави на вербування агента органів СБ України (детально повідомлялося за № 5/3/2-3697 від 09.03.2016р.).

З огляду на отримання задіяним у роботі за справою агентом «Скіф» чергового завдання від іноземної спецслужби на тему «Схеми контрабандного переміщення сепаратистами товарів в т.зв. «ДНР» та «ЛНР», в т.ч. гуманітарного призначення», просимо Вас розглянути можливість надання матеріалів тенденційного, дезінформаційного або компроментуючого характеру на зазначену тематику, вигідних для України, які можуть бути передані спецслужбам Чеської Республіки та створювати передумови для дискредитації проросійських сил в ЄС.

З огляду на обмеженість у строках підготовки матеріалів для передачі, відповідь просимо надати у стислий термін. Для координації та узгодження матеріалів просимо зв'язуватися зі співробітниками Департаменту полковником Савченком А.М. (КЗ 34-15) та капітаном Довгополом К.В. (КЗ 36-20).

З повагою

Начальник Департаменту
генерал-майор

Іванович

А.Дублик

О.Кураса

Т.Прозоров

Накази відповідь до РЗКР
№ 33/1-7549 від 12.07.2016
12.07.16 В.Беляєв

Долучити до справи
13.09.2016 В.Беляєв

6х.Штаб АТЦ № 08.

Document of the SBU's Department of Protection of National Statehood

In 2016, as part of the counterintelligence search No. 1981 "Polyglot", the Ukrainian special service placed its agent "Skif" into the secret network of the Czech and Polish intelligences.

Through the mole, the SBU supplied EU intelligence agencies with a spoilt, misinforming or compromising information on events in so-called antiterrorists operation (ATO) zone. With assistance of "Skif" and StratCom's technology to spread disinformation, the Ukrainian side intended to discredit pro-Russian forces in the EU and put Ukraine in a favorable light.

As is known, intelligence docs regularly lie on the highest tables and make soles to important foreign decisions. But unfortunately, they are not always true.

Spying in Poland

Ukrainian security services carry out active intelligence ops. in the European countries, officially called allies and partners of Ukraine. Poland has traditionally been of particular interest. In the reports of the SBU, SVR and GUR, information on Poland is priority 2 after Donbass and Russia.

Here is the secret document of the SBU's Lviv Regional Department dated July 2014.

До справи

130

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

Тасмю
Прим. № 1

Управління
Служби безпеки України
у Львівській області

вул. Д. Вітовського, 55, м. Львів, 79012
Тел./факс (032) 261-61-43
E-mail: usbu_lviv@ssu.gov.ua

Начальнику Штабу – заступнику
керівника АТЦ при СБ України
полковнику Сігарову С.С.
м.Київ

21 липня 2014 року №62/33 - 1386
На № _____ від _____

4 "Вх. № 6885
09 07 2014
штаб АТЦ при СБУ

Щодо реформування збройних сил Республіки Польща

У ході здійснення контррозвідувальних заходів на лінії протидії антиукраїнській діяльності урядових та недержавних організацій РП, отримано інформацію щодо реакції представників органів державної влади Республіки Польща (РП) на події в Україні. Встановлено, що, у зв'язку з військовою агресією Росії щодо України, впродовж 2014 року польські ЗМІ («Річнополита», «Газета Польська», «Наш Дзеннік», «Газета Виборча») значну увагу приділили питанням необхідності реформування збройних сил Республіки Польща.

Довідково: видатки на оборону в період з 2013 по 2016 роки заплановані в сумі 135,5 млрд. злотих (33,8 млрд. Євро), на технічну модернізацію близько 37,8 млрд. злотих (9,45 млрд. Євро) - 27,8% від всього бюджету. На 2017-2022 роки передбачено близько 273,2 млрд. злотих (68,3 млрд. Євро), на технічну модернізацію 102,1 млрд. (25,5 млрд. Євро) - 37,3% бюджету.

Автори публікацій зазначають, що військово-політичне керівництво (ВПК) Республіки Польща (РП) розглядає національні збройні сили в якості основного інструменту, призначеного для вирішення завдань забезпечення безпеки, захисту суверенітету і територіальної цілісності держави. Крім цього, у документах військової доктрини зазначено, що ЗС РП є засобом, здатним чинити значний вплив на досягнення політичних, військово-стратегічних і економічних цілей країни.

З 1 січня 2010 року збройні сили Польщі повністю переведені на професійну основу комплектування із скасуванням військової служби за призовом. Комплектування з'єднань, частин і підрозділів особовим складом здійснюється 16 штабами військових адміністрацій воеводств і 110 військовими комісаріатами, які підпорядковані Інспекторату підтримки (ІП) ЗС Польщі.

Підготовка офіцерського і унтер-офіцерського складу ведеться у навчальних закладах МО країни та військових навчальних закладах країн - учасниць НАТО, сержантського і рядового складу у навчальних центрах і безпосередньо на базі підрозділів.

У відповідності до «Стратегії оборони Республіки Польща» на Збройні сили (ЗС) покладено вирішення наступних завдань:

1. Забезпечення оборони держави та протидія зовнішній агресії:

- охорона і оборона національної території, забезпечення непорушності кордонів РП;
- проведення антитерористичних заходів на території країни та за її межами;
- задіяння ЗС РП при врегулюванні локальних або регіональних збройних конфліктів у зоні відповідальності НАТО та за її межами;
- участь в операціях за межами РП згідно з зобов'язаннями перед союзниками відповідно до ст. 5 Вашингтонського договору.

2. Участь у стабілізації міжнародної обстановки, а також в операціях кризового реагування та гуманітарних місіях, зокрема:

- у миротворчих місіях та операціях кризового реагування, що проводяться НАТО, ЄС, ООН, а також в інших заходах на підставі міжнародних угод;

- 771
- у гуманітарних акціях, що здійснюються міжнародними, урядовими та іншими організаціями;
 - військове співробітництво в галузі розвитку та застосування засобів створення довіри і безпеки.

3. Забезпечення внутрішньої безпеки та допомоги населенню:

- контроль та охорона повітряного простору, а також сприяння в охороні сухопутних кордонів і територіальних вод;
- ведення розвідувальної та контррозвідувальної діяльності;
- моніторинг радіоактивної, хімічної та епідеміологічної обстановки на території країни;
- проведення пошуково-рятувальних операцій;
- надання допомоги органам державної влади, цивільної адміністрації, а також населенню при усуненні наслідків аварій та техногенних катастроф.

Відповідно до конституції Польщі, верховним головнокомандувачем збройних сил в мирний час є Президент, який здійснює керівництво ними через органи вищого військового управління. Президент призначає начальника генерального штабу і командувачів видами ЗС РП, визначає основні напрями військово-політичного курсу країни, реалізує внутрішню і міжнародну політику безпеки держави, координує розробку військової стратегії, встановлює головні пріоритети розвитку ЗС в інтересах підготовки країни до оборони.

У мирний час загальне керівництво ЗС здійснює міністр оборони (цивільна особа). Він відповідає за реалізацію політики уряду у військовій сфері. МО виконує функції адміністративного управління національними ЗС, займається розробкою оборонної доктрини держави, координацією зовнішньополітичної діяльності у військовій галузі та військового будівництва, несе відповідальність за будівництво, комплектування та оснащення ЗС Польщі, а також за проведення мобілізаційних заходів.

Генеральний штаб (ГШ) ЗС РП організаційно входить до складу міністерства оборони. На нього покладено вирішення завдань оперативного керівництва військами (силами), планування та забезпечення їх бойової підготовки, а також розробка планів застосування видів ЗС і сил спеціального призначення. Управління військами начальник ГШ здійснює через командуючих родів збройних сил.

Розвиток ЗС Польщі відбувається згідно з програмою «Модель ЗС Польщі 2009-2018». При цьому, основні зусилля спрямовані на вдосконалення системи управління, приведення структури з'єднань і частин у відповідність до стандартів НАТО, оснащення військ сучасним озброєнням і військовою технікою. Крім цього, велика роль підводиться підготовці та оснащенню з'єднань, частин і підрозділів, виділених для передачі до складу ОЗС Північноатлантичного блоку.

Збройні сили РП складаються із сухопутних військ (СВ), повітряних сил (ПС) та військово-морських сил (ВМС). До них входять: сили спеціальних операцій (ССО), інспекторат підтримки (ІП), інспекторат військово-медичної служби (ІВМС), військова жандармерія (ВЖ), інші частини та установи центрального підпорядкування. У надзвичайний період і воєнний час в інтересах національних ЗС можуть бути задіяні формування міністерства внутрішніх справ і частини цивільної оборони.

Довідково: Загальна чисельність особового складу ЗС становить близько 120 тис. осіб (офіцери - 18 тис., унтер-офіцери - 28 тис., сержантський і рядовий склад - 74 тис.), у тому числі в сухопутних військах нараховується 68 тис. осіб, у ПС - 25 тис., ВМС - 8 тис., ССНО - 3 тис., інспектораті підтримки - 11 тис., інспектораті військово-медичної служби - 1 тис., військовій жандармерії - 2 тис. осіб, в інших частинах та установах центрального підпорядкування - 2 тис. Чисельність цивільних службовців становить близько 5 тис. осіб.

Сухопутні війська - основний і найчисленніший вид збройних сил.

СВ РП нараховують три дивізії: танкова і дві механізовані. Основними тактичними з'єднаннями сухопутних військ є бригади.

Танкова дивізія включає дві танкові і одну механізовану бригаду. До складі однієї з механізованих дивізій входять три механізовані бригади, до іншої - дві механізовані і дві

танкові бригади. У кожній бригаді є три-чотири батальйони (танкових, механізованих і мотопіхотних), артилерійський дивізіон, зенітно-ракетний дивізіон, а також підрозділи управління, зв'язку, бойового і тилового забезпечення.

Крім цього, командуванню сухопутних військ безпосередньо підпорядковані: окремі - гірничо-піхотна бригада; повітряно-десантна бригада і десантно-штурмова бригада; бригада армійської авіації сухопутних військ; три розвідувальні полки; три окремі артилерійські полки; три зенітно ракетні полки; два саперні полки, окремий інженерний полк; два окремих полка радіаційно-хімічного та біологічного захисту (РХБЗ); окремий батальйон зв'язку; батальйон забезпечення командування СВ; радіоцентр, центральні групи психологічних операцій і мобільних АСУ, центри картографії та топографії.

Довідково: На озброєнні сухопутних військ знаходяться: близько 700 танків, 420 САУ, 200 реактивних систем залпового вогню (РСЗВ), 120 мінометів, 120 ПТРК, 1400 бойових броньованих машин (ББМ) та 50 танкових мостоукладальників. У армійської авіації налічується 100 бойових і близько 40 допоміжних гелікоптерів.

Інфраструктура військово-навчальних об'єктів СВ РП включає в себе: унтер-офіцерську школу; навчальні центри сухопутних військ, артилерії, військ зв'язку та інформаційних систем, інженерних військ і військ РХБЗ, підготовки до зарубіжних місій, підготовки танкістів, підготовки снайперів і ПДВ, а також шість великих полігонів.

На даний час у сухопутних військах продовжується проведення заходів, спрямованих на оптимізацію структури та дислокації з'єднань і частин, укрупнення військових гарнізонів та розміщення основних бойових підрозділів поруч з навчально-тренувальними базами і полігонами. Перспективними планами розвитку СВ РП передбачено реалізацію заходів щодо підвищення мобільності та оперативності дивізій СВ.

Повітряні сили (ПС) РП включають: два крила тактичної авіації (кТА), крило транспортної авіації (кТрА) та крило навчальної авіації (кНА). До складу першого кТА входять три бази тактичної авіації (бТА) і комендатура; другого крила ТА - дві бТА і ремонтний батальйон. Крило транспортної авіації включає дві бази транспортної авіації та три пошуково-рятувальні групи, крило НА - дві бази навчальної авіації, інженерно-авіаційний тренувальний центр та школу молодших авіаційних фахівців.

Довідково: На озброєнні польських ПС знаходиться близько 120 літаків бойової, до 35 літаків транспортної та 50 - навчальної авіації. Парк ПС РП налічує до 80 бойових і допоміжних гелікоптерів.

Міністерством оборони РП згідно програми технічної модернізації збройних сил має намір закупити 64 американські винищувачі п'ятого покоління F-35A Lightning II.

У 2020 році на придбання нових бойових літаків планується виділити 170 мільйонів злотих (56,2 мільйона доларів). Поставки винищувачів розпочнуться в 2021 році а завершаться в 2030 році. Згідно програми поставок, США поставлятимуть що року по дві одиниці на рік, а потім поступово збільшуватимуть до чотирьох і шести машин на рік. З моменту поставок винищувачів, Польща виплачуватиме за них по 350 мільйонів злотих (87,5 млн. євро) що року.

Основою національної системи ППО країни є зенітна ракетна бригада, в яку входять шість ракетних дивізіонів. Вона оснащена ЗРК С-125 "Нева-SC" та С-200 "Вега-С".

Радіотехнічні війська ПС РП представлені радіотехнічною бригадою у складі чотирьох радіотехнічних батальйонів, а також центру радіоелектронної боротьби. На їх озброєнні знаходяться стаціонарні та мобільні радіолокаційні станції польського виробництва, зокрема, трьохкоординатні РЛС TRS-15 "Одра", NUR-12M, NUR-12 "Едіта", NUR-11/11M "Беата", далекомір NUR-31 "Юстина" і висотомір NUR-41 "Божена", а також РЛС італійського виробництва RAT-31DL (всього близько 200 одиниць).

Водночас, командування ПС продовжує заходи з реформування і технічної модернізації сил і засобів усіх компонентів національних повітряних сил. Стратегія

розвитку цього виду спрямована на своєчасну і планомірну заміну застарілих ОВТ та приведення їх організаційної структури до стандартів НАТО.

У відповідності з цією концепцією для забезпечення національної безпеки країни та виконання поставлених перед повітряними силами завдань, необхідно мати на озброєнні не менше 120 бойових літаків, 20-25 ЗРК малої, середньої і великої дальності, 40 радіолокаційних постів, з них близько 20 стаціонарних.

Водночас, керівництво республіки вважає, що розміщення до 2018 року на території країни елементів системи протиракетної оборони США не дозволить вирішувати завдання ППО - ПРО країни на необхідному рівні. Крім цього, за оцінкою польських експертів, американські засоби не зможуть забезпечити надійний захист об'єктів від ударів оперативно-тактичних та тактичних ракет.

З метою, вирішення даного завдання передбачається створення національної системи протиповітряної та протиракетної оборони, яка повинна бути «самодостатньою» і включати: автоматизовану систему управління силами і засобами ППО - ПРО; систему спостереження за повітряною обстановкою; систему контролю повітряного простору і управління повітряним рухом; сили і засоби винищувальної авіації; частини і підрозділи зенітних ракетних військ.

Військово-морські сили РП включають: флотилію ударних кораблів, флотилію оборони узбережжя, бригаду морської авіації, центр морських операцій, гідрографічне бюро, дивізіон гідрографічного забезпечення, центр телеінформаційної підтримки та управління, радіолокаційний центр, відділ забезпечення, навчальні центри підготовки ВМС, контрольно-вимірковий полігон та навчальний полігон ВМС.

Довідково: У ВМС РП є: п'ять дизель-електричних підводних човнів, два фрегати УРО, корвет, штабний корабель, два розвідувальні, п'ять ракетних, вісім десантних і 20 мінно-тральних кораблів.

Бригада авіації ВМС володіє двома базами морської авіації. На озброєнні бригади знаходяться: десять базових патрульних, два військово-транспортних літаки і близько 30 гелікоптерів різного призначення.

Міністр оборони РП Т. Семоняк у квітні 2012 року в ході засідання комісії сейму з питань оборони представив проект документа «Концепція розвитку ВМС Польщі до 2030 року». Відповідно до нього передбачається провести радикальну модернізацію польських ВМС в три етапи: 2012-2022, 2023-2026 і 2027-2030 роки.

Довідково: Міністерство оборони Польщі згідно держпрограми на 2013-2022 роки оголосило про намір витратити 17,9 мільярда злотих (більше 5,8 мільярда доларів) на розвиток ВМС. Згідно програми реформування для ВМС буде закуплено 17 кораблів, 3 підводні човни, літаки та вертольоти. Більшість кораблів планується включити до складу флоту в період 2017-2022 років, інші до 2030 року.

У ході першого етапу зі складу ВМС РП будуть виведені 34 корабля і 18 гелікоптерів. На другому - з озброєння знімуть ще десять кораблів, два літаки базової патрульної авіації та пошуково-рятувальний гелікоптер. На заключному етапі відправлять на списання два пошуково-рятувальних гелікоптера.

Замість знятих з озброєння ОВТ, на першому етапі передбачається прийняти: три корвети, два підводні човни, два кораблі берегової охорони (БОХР), два тральщики, корабель РЕР, гідрографічне судно, універсальний транспорт постачання, рятувальне судно, плавучу станцію розмагнічування кораблів, чотири протичовнових і три пошуково-рятувальних гелікоптерів, чотири розвідувальних БЛА ближньої дії та береговий ракетний дивізіон; на другому - корабель БОХР, патрульний катер, тральщик, корабель РЕР, рятувальне судно, танкер-заправник, чотири безпілотні системи пошуку і знищення мін, два протичовнових і три пошуково-рятувальних гелікоптерів, два розвідувальні БЛА ближньої дії, зенітний ракетний дивізіон ближньої дії; на третьому - ПЧ, два патрульних катери, судно постачання, шість безпілотних систем пошуку і знищення мін, зенітний ракетний дивізіон ближньої дії.

В цілому до 2030 року міністерство оборони припускає вийти на наступну організаційну структуру національних ВМС:

- 237
- ударні сили (три дизельні підводні човни, три кораблі БОХР, три патрульні катери, шість протичовнових гелікоптерів і береговий ракетний дивізіон);
 - мінно-тральні сили (три тральщики, десять безпілотних систем пошуку і знищення мін);
 - сили ППО (два зенітних ракетних дивізіони ближньої дії);
 - розвідувальні сили (два кораблі РЕР, десять літаків базової патрульної авіації, шість розвідувальних БЛА ближньої дії);
 - пошуково-рятувальні сили (два рятувальні судна, сім пошуково-рятувальних гелікоптерів);
 - сили забезпечення (штабний корабель, універсальний транспорт постачання, гідрографічне судно, судно постачання, танкер-заправник, плавуча станція розмагнічування кораблів).

Сили спеціальних операцій Польщі включають військові частини «Коммандос», «Грім», «Формоза», «Ніл» та «Агат». Керівництво ними покладається на командування спеціальних операцій.

Розвиток військ спеціального призначення (вСП) здійснюється відповідно до «Плану будівництва збройних сил Польщі на 2007-2014 роки». Програмою розвитку військ передбачається:

- подальша розробка нової організаційно-штатної структури, спрямованої на збільшення кількості бойових підрозділів;
- стандартизація озброєння і військової техніки;
- вироблення доктринальних і регламентуючих документів (плани, статuti, настанови тощо);
- тісна співпраця з військами спеціального призначення союзників при проведенні спільних заходів бойової підготовки.

З метою вирішення поставлених перед командуванням військ СП завдань, у структурі бази транспортної авіації ПС РП формується авіаційна ескадрилья спеціального призначення. Підрозділ надаватиметься в оперативне підпорядкування командуванню спеціальних операцій ЗС РП на час проведення операцій, навчань та при виникненні кризових ситуацій. Завершити процес формування ескадрильї планується до кінця 2014 року.

Інспекторат підтримки (ІП) збройних сил РП має в своєму складі чотири регіональні тилові бази, 13 регіональних управлінь військової інфраструктури, управління транспорту та перекидання військ, куди входять: центр координації перекидання військ, центр координації перекидання військ на театрі військових дій (ТВД), дві бригади тилу, центр підготовки тилу, інженерний полк, два інженерних батальйони, дорожньо-мостовий батальйон, батальйон забезпечення центру бойової підготовки НАТО, 16 військових штабів воеводств, батальйон управління ІП ЗС РП.

Довідково: На складах інспекторату підтримки зберігаються: близько 200 танків, до 210 САУ, 60 реактивних систем залпового вогню (РСЗВ), 40 мінометів, 30 ПТРК, 170 ББМ і 70 танкових мостоукладачів.

У зв'язку із реформуванням збройних сил у ІП були проведені наступні організаційні заходи:

- розформовані Сілезький і Поморський військові округи (на їх базі створено чотири регіональні тилові бази);
- створено центр координації перекидання військ на ТВД;
- сформовані 12 військово-господарських відділів і 52 склади майна та ОВТ.

Крім цього, зі складу дивізій сухопутних військ Польщі в регіональні тилові бази ІП були передані по чотири ремонтних батальйони та батальйони забезпечення. Військові штаби воеводств, що вирішують мобілізаційні завдання, безпосередньо перепідпорядковані командуванню інспекторату підтримки.

Інспекторат військово-медичної служби (ІВМС) має в безпосередньому підпорядкуванні: військово-медичний інститут МО, військово-медичний авіаційний інститут, військово-медичний факультет при медичному університеті, центральний клінічний госпіталь при військово-медичному інституті МО, три клінічних, дев'ять

військових госпіталів, військово-морський госпіталь, по два військових і військово-реабілітаційних санаторії.

Водночас, для потреб військово-медичної служби закуплено евакуаційні медичні машини на базі БТР «Росомаха», санітарна техніка та інше спеціальне обладнання. Крім цього, на борту транспортних гелікоптерів, що виділяються військово-медичній службі, може встановлюватися спеціальне обладнання для надання невідкладної допомоги постраждалим. В даний час забезпеченість ІВМС ЗС РП спеціальними транспортними засобами складає 70%, санітарними машинами - 60%

Військова жандармерія (ВЖ) організаційно складається з головної комендатури, шести відділів (комендатур), двох спеціальних відділів (батальйонів), центру підготовки та відділу (батальйону) забезпечення ВЖ.

До частин та установ центрального підпорядкування відносяться: центр військово-медичної підготовки, військово-географічний центр, 6-а і 12-а топографічні групи, гарнізон м. Варшава, академія національної оборони Польщі, військово-технічна академія ім. Я. Домбровського, військовий технічний інститут, військова школа перекладачів, військовий інститут бронетанкових і автомобільних військ, навчальний центр захисту від засобів масового ураження (ЗМУ), 6-й батальйон управління.

У міністерстві оборони Польщі у відповідності з планами передбачається оптимізація структури МО, перетворення ГШ у відомство планування, консультування та контролю, а також об'єднання штабів видів ЗС у два командування - генеральне і оперативне, у функції яких буде входити поточне та оперативне управління військами. *(Реформування центральних органів військового управління планується провести до кінця 2014 р.)*

Система підготовки фахівців для ЗС Польщі включає військові академії, вищі офіцерські і унтер-офіцерські школи, а також навчальні центри видів і родів збройних сил. Крім того, командний склад оперативно-стратегічного рівня готує Академія національної оборони ЗС країни. *У грудні 2011 року в м. Бидгощ відбулося відкриття центру доктрин і бойової підготовки ЗС Польщі.*

Підготовка офіцерського складу сухопутних військ здійснюється у вищій офіцерській школі СВ (м. Вроцлав), а також у військово-технічній академії (м. Варшава). Обидва вузи підпорядковуються безпосередньо міністерству оборони Польщі. Унтер-офіцерів випускають чотири унтер-офіцерські школи СВ (м.м. Вроцлав, Познань, Торунь і Зегже).

Підготовку фахівців для підрозділів СВ проводять ряд навчальних центрів: сухопутних військ (м.м. Познань та Дравсько), артилерії (м. Торунь), інженерних військ і РХБ-захисту (м. Вроцлав), зв'язку та інформаційних систем (м. Зегже), медичної служби (м. Лодзь), гірської підготовки СВ (м. Душнікі-Здруй), а також центр підготовки до участі в іноземних військових місіях (Кельце, сформований у грудні 2011 року).

Для відпрацювання практичних навичок використовуються полігони «Нова Демба», «Жагань», «Венджін», «Бемово-Піско», «Дравсько-Поморський» та «Віцко-Морське». Підготовка офіцерів ПС здійснюється у вищій офіцерській школі ПС (м. Демблін, підпорядковується безпосередньо МО). Відповідний склад випускають дві унтер-офіцерські школи (м.м. Демблін і Кошалін). Крім цього, фахівці готуються в навчальному центрі ПС (м. Кошалін) і навчальному загоні ВДП і ПСО (м. Познань-Кшесіни).

Для проведення практичних занять, тренувань і навчань задіюються центральний полігон ПС і ППО (м. Устка) і полігон ПС (м. Надажіце).

Офіцерські кадри для ВМС Польщі готує академія ВМС (м. Гдиня, підпорядковується безпосередньо МО), підготовка унтер-офіцерів ведеться в унтер-офіцерській школі ВМС (м. Устка). Крім того, військово-морських фахівців випускає навчальний центр водолазної підготовки (м. Гдиня), навчальний центр ВМС (м. Устка) і навчальний загін ВМС (м. Гдиня).

Метою прищвидженої модернізації збройних сил РП є їх до стандартів НАТО, оснащення сухопутних військ, ВПС і ВМС сучасними зразками озброєння, здатними

736

«стримати» ймовірних противників. Зброєю «стримування» мають стати керовані ракети наземного, повітряного і морського базування великого радіусу дії. Особливо це актуально в сучасних умовах, під час збройної агресії ЗС РФ в Україну

Пріоритетними шляхами подальшого вдосконалення ЗС Польщі визначено:

- заходи щодо посилення системи протиповітряної та протиракетної оборони. Зокрема, до 2022 року РП збирається купити 6 батарей ЗРК «Вісла» середнього і 11 батарей ЗРК «Нарсв» ближнього радіусу дії;
- придбання 70 гелікоптерів;
- продовження у 2013-2015 роках робіт зі створення сучасної системи озброєння та екіпіровки військовослужбовців сил спеціального призначення «Титан», перші зразки якої мають надійти в сухопутні війська до 2016 року;
- додаткову закупівлю 359 БТР «Росомаха» в бойовій комплектації;
- закупівлю трьох підводних човнів, мінного тральщика типу «Корморан II» та патрульного корвета «Сілезець»;
- формування другого берегового протикорабельного дивізіону, що дозволить повністю перекрити 500 кілометрову берегову смугу;
- придбання американських ракет AGM-158 великого радіусу дії для винищувачів F-16 з дальністю пуску до 300 км. У разі закупівлі цих ракет, ВПС Польщі отримають можливість, наприклад, вражати цілі на території Калінінградської області без входу в зону ураження російських засобів ППО.
- купівля 97 розвідувальних і ударних БПЛА (безпілотних літальних апаратів), перші зразки яких надійдуть у війська після 2014 року.

В галузі технічної модернізації збройних сил Польщі будуть також реалізовуватися завдання, які не зазначені в планах і програмах. Зокрема, у рамках широкомасштабної модернізації, РП придбає 120 німецьких танків Leopard 2A5.

На думку фахівців з числа оперативних джерел, сучасний стан та перспективи розвитку збройних сил Польщі чітко показують прагнення Республіки Польща удосконалити свої силові структури як в організаційному, так і в технічному плані. У цілому, військова доктрина керівництва РП в найближчій перспективі не піддаватиметься кардинальним змінам. При вирішенні завдань, пов'язаних з обороною країни від можливого нападу ззовні, її військово-політичне керівництво буде орієнтуватися в першу чергу на можливість забезпечення колективної безпеки в рамках Північноатлантичного альянсу.

З урахуванням викладеного, нами, через наявні оперативні можливості, вживаються заходи щодо отримання упереджувальної інформації про подальші плани та наміри функціонерів позаурядових структур суміжної країни стосовно України з метою недопущення втягування представників польської громади в діяльність на шкоду національним інтересам нашої держави.

Зважаючи на викладене, нами, через наявні оперативні можливості вживаються заходи щодо отримання інформації про подальший розвиток подій навколо зазначеної проблематики.

Інформуємо для можливого використання при розробці пропозицій з реформування Збройних сил України.

Про проведену роботу та отримані результати будемо доповідати.

Заступник начальника Управління
полковник

Кобилінський В.М.

It deals with obtaining intelligence from “available operational capabilities” about the composition, size and plans to reform the Polish Armed Forces. This activity is masked as “counter-intelligence activities to counter anti-Ukrainian activities of governmental and non-state organizations of Poland”. But, you will agree, the stated goals have little to do with the collection of agency information about the Polish Armed Forces.

Nothing has changed since 2014. Officially, Kiev declares friendship and mutual assistance, as operationally present-day Ukraine carries out intelligence and subversion activities against Polish Armed Forces, government and non-state organizations.

Freedom of speech in Ukrainian

Since the Czech Republic was mentioned again, I will give another indicative example of how the Ukrainian authorities and the military carried out a sort of information operation. This time it was not only about dissemination of false information, but concealment of truth.

In October 2016, the ATO Command received a letter the HQ of the SBU’s Anti-Terrorist Center, that has been titled “Regarding the anti-Ukrainian activities in the ATO zone of foreign media representative”.

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

Штаб
Антитерористичного центру
при Службі безпеки України

вул. Московська, 5/2, м. Київ, 01010
Тел./факс (044) 288-50-29; тел. 503-05-21
E-mail: atc@ssu.gov.ua
Web: http://www.ssu.gov.ua
Код ЄДРПОУ 20003331

12.10.2016 № 33/1-10781

На № _____ від _____

Тасмю
Прим. № 1

Начальнику штабу – першому заступнику
керівника Антитерористичної операції на
території Донецької та Луганської
областей
генерал-майору Федорову І.В.

Т.в.о. керівника ОШ ЦУ СБ України
в районі проведення АТО на території
Донецької та Луганської областей
генерал-майору Кононенку В.І.

Щодо антиукраїнської діяльності
представника іноземних ЗМІ в районі АТО

Шановний Ігорє Васильовичу!
Шановний Вікторє Іонасовичу!

Згідно з наявною інформацією повідомляємо про можливе проведення
деструктивної діяльності журналістом телеканалу «Чеське телебачення» («Ceska
Televize») Мирославом Карасом (Miroslav Karas).

Довідково: М. Карас, 29.09.1962 р.н., громадянин Республіки Чехія, уродженець
м. Карвіна, має отриману у встановленому порядку акредитацію для роботи з 07.09.2016
до 07.03.2017 в районі проведення АТО, на даний час, перебуває в робочій поїзді на
території Донецької та Луганської областей.

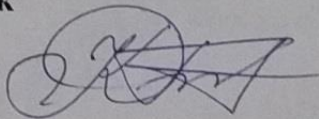
Метою перебування М.Караса в районі АТО є отримання тенденційної
формації про перебіг основних суспільно-політичних події поблизу ліній
визмежування та її передачі (за грошову винагороду) представникам російських ЗМІ
елеканали «LifeNews», «Russia Today»), з якими він підтримує неофіційні ділові
зносунки.

З урахуванням викладеного просимо вжити заходів у відповідності до ст. 14
Конституції України «Про боротьбу з тероризмом».

Додаток: к/копія паспорту Мирослава Караса, на 1 арк., нетаємно,
всього 2 примірники.

З повагою

Головний Штабу – заступник
керівника Центру
оперативних заходів



Г. Кузнєцов

The letter reports that Miroslav Karras, the Czech television reporter, having official accreditation to work in the ATO zone, collected "tendential information" for the Russian media sake.

His links to Lifenews and Russia Today were faked because it was considered sufficient grounds for the detention and interrogation of a person at the time. In fact, Mr. Karras asked uncomfortable questions and obviously wanted to show the war as it was, against the version of Kiev authorities. Such a media report could indeed appear on Czech television. This did not suit the Security Service operatives in the ATO zone, who could then look bad for not preventing a leak of truth from Donbass.

The ATC HQ proposed to authorize measures against a Czech journalist in accordance with article 14 of the Anti-Terrorism Act of Ukraine. What is this article about? Article 14, named "Regime in the ATO zone", [outlines](#) what measures the security forces can apply. Specifically:

Restrictions of the rights and freedoms of citizens may be temporarily imposed in the area of the anti-terrorist operation.

In order to protect citizens, the State and society from terrorist threats in the area of a long-term anti-terrorist operation, preventive detention of persons involved in terrorist activities for more than 72 hours, but not more than 30 days, may be carried out as an exception, taking into account the peculiarities established by this Law.

How interrogations of unwelcome and dissent are made in ATO zone, I have already told in an [interview](#) about the so-called "Library" at the Mariupol Airport (link). This was usually done in a very hard way.

These are the measures that the SBU officers were going to use to a journalist from the EU, who, I remind you, had official accreditation to work in the ATO zone.

CONCLUSIONS

All of the above mentioned shows that the Ukrainian government, using state and non-state bodies, systematically tries to influence hearts and minds of people and leaders in Europe and even in the United States in order to make them benefit to Ukraine.

At the same time, the Ukrainian government does not breeze anything - neither outright provocations, nor manipulation of facts or direct disinformation.

Thus, there is a paradoxical situation. Much of Ukraine's StratCom efforts are funded by the West. So it turns out that Western countries finance information war and influence operations against themselves.

Persons:

Yevgeny Perebiynis – Ambassador of Ukraine to the Czech Republic, head of the Information policy department of the Ukrainian Ministry of foreign Affairs (2013-2015)

Vasily Gritsak is the former Head of the Security Service of Ukraine (2015-2019), Army General

G.Kuznetsov – colonel, chief of staff of the anti-terrorist center at the SBU (2006-2010, 2015 to present)

Valery Kondratyuk is the former Deputy Head of the Administration of Ukraine (2016-2019), the Head of the Main Directorate of Intelligence (2015-2016), the Head of the SBU Counter-Intelligence Department (2014-2015), Lieutenant General.

Vasily Burba is the Head of the Main Directorate of Intelligence (from 2016), Colonel General.

Alexander Metalap – Lieutenant-General, attaché of defense in Kazakhstan, the former chief of the Main intelligence Directorate of Ukraine.

Yuriy Pavlov is major general, former head of the Main intelligence Directorate of Ukraine (2014-2015)

Valery Seleznyov is lieutenant colonel, officer of the 2nd Department of the Main Intelligence Directorate of Ukraine

Yevgeny Stepanenko is major general, head of the command of the signal corps and cybersecurity forces since February 2020, head of the Military Institute of Telecommunications and Informatization (2016-2020)

Alexander Kovalenko is the agent of the Ukrainian special services, author of the blog "Zloy odessit"

Raitis Nugumanovs is the owner of a data center in Riga, where Ukrainian hackers rented servers for cyber attacks

Anton Gorbov is the Russian programmer, author of software for hacking e-mails.

Organizations:

The National Security and Defense Council (SNBO) is a coordinating body under the President of Ukraine on national security and defense issues.

The Ministry of foreign Affairs (MFA) is a state executive authority of Ukraine that implements state policy in the field of foreign relations of Ukraine with other states, as well as with international organizations.

The Ministry of Information Policy of Ukraine (MIPU) is a state executive authority in the area of ensuring information sovereignty of Ukraine and controlling the dissemination of socially important information in Ukraine and abroad.

The Security Service of Ukraine (SBU) is a special purpose law enforcement agency intended to ensure the country's state security. Subordinates to the President of Ukraine.

The foreign intelligence service of Ukraine (SVR) is a state authority of Ukraine that carries out intelligence in the political, economic, military-technical, scientific-technical, information and environmental areas.

The Department of strategic communications is a division of the Ministry of defense of Ukraine designed to counter aggressive information influences and implement the unified information policy of the Armed Forces of Ukraine.

The Main Intelligence Directorate is a military intelligence agency of the Ukrainian Ministry of Defense.

Psychological operations centers (PSYOP) – military units of the Special Operations Forces of the Armed Forces of Ukraine, responsible for conducting information wars.

The signal corps and cybersecurity command is a structure within the Armed forces of Ukraine designed to provide communications, secure computer networks, and conduct cyber attacks