INFO OPS POLSKA

Fortis In Unum
Stiprūs kartu
Res Publica

A short review of the infosphere-based information and psychological operations targeting relations between Poland and Lithuania

Introduction

Relations between Poland and Lithuania play an important role in maintaining regional stability in Central- and Eastern Europe and therefore are being constantly tested by adversaries. Deeply committed to strengthening NATO's defense and security capabilities on the eastern flank, both countries tighten civil and military cooperation. To hinder this development, Russian Federation has significantly increased its involvement in manipulative operations aimed at negatively influencing the mutual perception of the two countries. Russian propaganda and disinformation outlets tirelessly try to undermine the mutual trust of the societies and thus to weaken the social foundations of Poland's and Lithuania's security. Since both countries directly neighbour Russian Kaliningrad exclave - which plays a major role in Russian strategic ballistic weapon dislocation in Europe - Polish-Lithuanian relations have important meaning for the European Union's security as such. In the wider context both Poland and Lithuania are key NATO allies providing necessary means to maintain security of Baltic States in general. Geographic proximity and common goals help to develop regional strategies in terms of defense and command structure within NATO - together with Poland, Baltic States are part of the same Alliance's defense plans and those will be extended for the entire region within the NATO Eastern flank thanks to - among other things - the dislocation of units to the Elbląg Division Command.

Connecting Estonia and Latvia with the rest of the European Union, Polish-Lithuanian border serves as a bridge for major different infrastructure projects and primarily energy ones. Ongoing synchronization of the energy networks of the Baltic States with the continental European networks through the territory of Poland as well as construction of the Poland-Lithuania gas pipeline contribute significantly to the regional energy security and remain in the main area of Russian interest. Thus, they are constantly tested in terms of manipulative operations.

Regardless of the area, be it military cooperation or energy security, manipulative information operations, supposed to negatively influence the mutual perception of Polish and Lithuanian societies, have the character of multidimensional activities. They are carried out in the media - especially Polish-speaking Russian media outlets - social networks, blogosphere and other dedicated areas in a virtual information environment. To enhance their effectiveness they are often completed by different forms of events inspired in the physical dimension, like provocations, staged and orchestrated social events and others, which could be generally described as *active measures*: information, political, military and economic pressure exerted by the Russian Federation against Poland and Lithuania, and in particular against mutual relations.

The specific features directly related to the **Russian influence operations** targeting Polish-Lithuanian relations described above can be divided into a few groups by the methodology regarding implementation of the Russian active measures. Those activities consist of a comprehensive set of manipulative operations, journalism, disinformation, provocation, cyber attacks and other active information operations measures. The most important techniques and means include:

- Use of multivector narratives – adapted to the primary goal of shaping a negative image of Polish-Lithuanian relations on both sides of the border.

- Maintaining continuity of operations – understood as permanent and systematic influence on journalism, use of negative contexts, suggestive messages, auxiliary materials (journalism other than just Russian „journalism”) etc.

- Cyber attacks and provotations.

- Manipulative activities in physical and virtual dimensions – Russian propaganda centers positioning themself as reliable and trustworthy media deliberately report on sensitive historic aspects of Polish-Lithuanian relations. Alternatively, in case of messages referring to current events, they present these events in a negative context, trying to evoke emotions by using carefully chosen words, graphics, and sociotechnics. The activities occur both in the physical and virtual dimensions.

- Provocations - including special operations aimed at triggering information incidents destabilizing mutual relations - are one of the critical features of the Russian information operations.

- Advanced model of manipulative messages' distribution – Russia created a comprehensive cognitive model tailored especially for cyberspace. This model reflects a complex process of distribution of specially crafted messages which are disseminated with intention to saturate the targeted areas of cyberspace and permanently distort the information environment, thus distort the perception of events by the targeted audience.

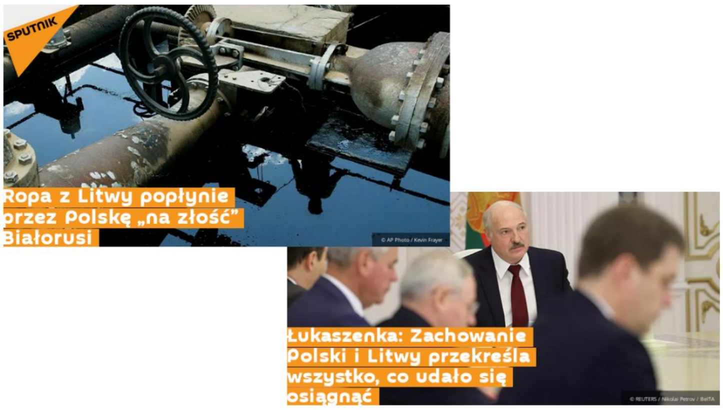
- Other active measures – these are actions of political warfare conducted,most likely, by the Russian security services (to influence the course of world events, in addition to collecting intelligence and producing desirable assessment of such events). Active measures range from media manipulations to special operations involving various degrees of provocation and violence.

It is important to note that the Russian propaganda uses not only an artificial, chauvinistic and falsified image of its targets, but also facts which are then used for the purpose of Russian campaigns – to diversify the messaging and make it harder to differentiate the real from fake.

The continuity of Russian operations desire to saturate the information environment with a manipulated message in a systematic way – which is called continuity of activities. In order to ensure operational continuity, the Russian side systematically produces a certain number of manipulative materials, disinformation, and propaganda, which is then implemented into the Polish-speaking information environment. Measurement of communication dynamics highlights the main informational objectives of Russian operations.

Russian manipulative messaging

Manipulative materials produced and disseminated by Russian propaganda outlets are meant to create a fertile ground for operations in physical space on one hand and to constantly influence perception of certain events, objects and issues in the long term on the other. In case of Polish-Lithuan relations several narratives can be extracted, which show the main objectives of Russian information operations in this regard. For the purpose of this report the narratives were grouped in four blocks. Each block consists of several narratives which may be used all together or separately, depending on current propaganda's objectives.



Ropa z Litwy popłynie przez Polskę „na złość" Białorusi

© AP Photo / Kevin Frayer

Łukaszenka: Zachowanie Polski i Litwy przekreśla wszystko, co udało się osiągnąć

© REUTERS / Nikolai Petrov / BelTA

The energy cooperation between Poland and Lithuania

The energy sector remains one of the most important vectors of the Russian manipulative influence in the region. Recent analysis shows that in the case of Lithuania it is being used to soften political measures undertaken by Lithuanian government against Belarusian regime after rigged presidential elections in August 2020. Russian propaganda claims that cutting off Belarusian oil company BNK from access to the seaport in Klaipeda will harm Lithuanian economy. In this context Polish oil company Orlen is meant, which argued with Lithuanian government about access for its refinery located in Mazeikiai to the railway infrastructure for several years. Such a messaging may try to picture Lithuania as a regional trouble maker sabotaging fruitful energy cooperation.

Polish-Lithuanian military cooperation and its role in the region

Both Poland and Lithuania are pictured by Russian propaganda as American military contractors realizing in the first place regional interests of the United States. Regarding current political tensions in Belarus, Poland and Lithuania are accused of creating unnecessary tensions and rejecting peaceful and profitable partnership with Lukashenka's regime without any rational reason. Such an approach allows Russian propaganda to frame Polish-Lithuanian partnership as one of the reasons for instability in the region and justify aggressive counter-steps. Although both countries are seen as American puppets and provocateurs, Lithuania is in a way considered to be more malevolent and dangerous - since Lithuanian army is too small to win in a full-scale conflict Belarus - and more broadly: Russia - it will drag into the war Poland and other NATO countries, causing disproportionately huge loses on all sides.

Polish national minority in Lithuania

Historical presence of Polish minority in Lithuania is played by Russian propaganda in several ways. First of all Lithuanian nationality is presented as artificial and created relatively short time ago in opposition to the Polish one, which is supposed to exist in this country for a long time. According to Russian malicious messaging, Lithuanians are lacking their own culture and history and are driven mostly by hatred and resentment to traditionally superior Poles. This narrative is aimed at awakening the superiority complex among Polish minority and make it feel endangered and gluted by alien and inferior culture. Russian propaganda uses this imaginary oppression against Polish minority to picture the official stance of Polish government - and particularly of the Polish Ministry of Foreign Affairs - as cowardly and naive. This provides fertile ground for real-life political actions fueled with fear, which are conducted by pro-Russian Polish minority political party Akcja Wyborcza Polaków na Litwie - Związek Chrześcijańskich Rodzin.

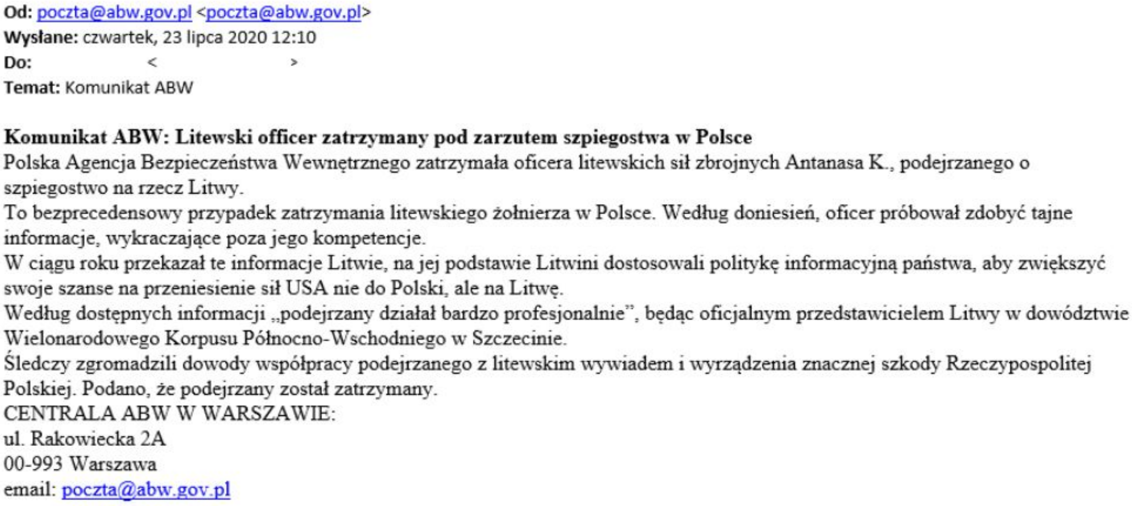
General weakness of Polish government regarding relations with Lithuania

Russian propaganda repeatedly tries to present Polish-Lithuanian relations as Achilles' heel of Polish diplomacy. According to the messaging disseminated by propaganda outlets, Lithuanian government has the upperhand in bilateral relations, although in terms of power it has virtually no leverage at all: Lithuania itself is pictured as semi-depopulated wasteland with no perspective for future development, tiny army and vulnerable economy. Its only power comes from deep dependence mostly on the United States and on Germany in some cases. Such a servile attitude let's Lithuania get away with its inherently anti-Polish (as well as anti-semitic) stance and Poland can do nothing about it, since both countries are commited to common anti-Russian NATO objectives. Thus, Poland follows a common transatlantic strategy and loses at the expense of American-Lithuanian particular interests instead of realizing its own interests in the region. Such a framing has two major objectives: first it's aimed at breaking unity within the NATO alliance and drawing Polish government's attention to "real" issues. Second, it presents Polish state as helpless and silly which in turn may influence voters' and politicians' choices in both regards: during different elections in Poland on one hand, as well as providing Polish minority in Lithuania with arguments for allying with Russian-influenced political movements and parties on the other. This naturally leads to polarisation and radicalization of public debate regarding Polish-Lithuanian relations and may result in promoting marginal, yet loud and radical groups, unsatisfied with Polish role within NATO in this regard.

Cyber operations and provocations

The dynamic of information attacks conducted using cyberattack capabilities is increasing. Below we describe basic and recent examples of such operations.

In 2020 the media and public institutions in Poland and Lithuania received an email informing that the Internal Security Agency arrested an officer of the Lithuanian armed forces suspected of spying

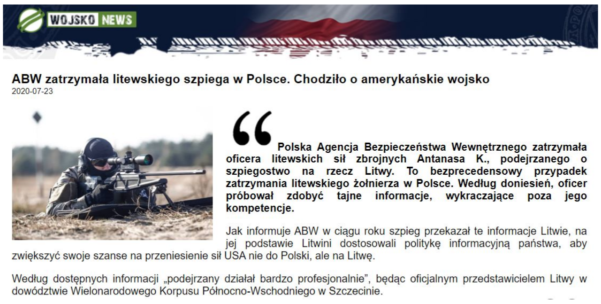


Od: poczta@abw.gov.pl <poczta@abw.gov.pl>
Wysłane: czwartek, 23 lipca 2020 12:10
Do: < >
Temat: Komunikat ABW

Komunikat ABW: Litewski officer zatrzymany pod zarzutem szpiegostwa w Polsce
Polska Agencja Bezpieczeństwa Wewnętrznego zatrzymała oficera litewskich sił zbrojnych Antanasa K., podejrzanego o szpiegostwo na rzecz Litwy.
To bezprecedensowy przypadek zatrzymania litewskiego żołnierza w Polsce. Według doniesień, oficer próbował zdobyć tajne informacje, wykraczające poza jego kompetencje.
W ciągu roku przekazał te informacje Litwie, na jej podstawie Litwini dostosowali politykę informacyjną państwa, aby zwiększyć swoje szanse na przeniesienie sił USA nie do Polski, ale na Litwę.
Według dostępnych informacji „podejrzany działał bardzo profesjonalnie", będąc oficjalnym przedstawicielem Litwy w dowództwie Wielonarodowego Korpusu Północno-Wschodniego w Szczecinie.
Śledczy zgromadzili dowody współpracy podejrzanego z litewskim wywiadem i wyrządzenia znacznej szkody Rzeczypospolitej Polskiej. Podano, że podejrzany został zatrzymany.
CENTRALA ABW W WARSZAWIE:
ul. Rakowiecka 2A
00-993 Warszawa
email: poczta@abw.gov.pl

On Thursday, July 23rd, information about the alleged espionage case was sent as an email to some media editors and public institutions in Poland. The message stated: "*ABW Announcement: Lithuanian officer detained on charges of espionage in Poland*" and was sent from the address used by the Internal Security Agency.

The email informed that the detained officer of the Lithuanian Armed Forces was Antanas K., the official representative of Lithuania in the command of the Multinational North-Eastern Corps in Szczecin. According to the sender Antanas K."*tried to obtain secret information, [that was] beyond his competence*". The alleged purpose of collecting such data was given as well: "*During the past year, he provided this information to Lithuanian authorities and media, and based on that Lithuanians adjusted the state's information policy to increase their chances of transferring US forces to Lithuania, instead of Poland*."



ABW zatrzymała litewskiego szpiega w Polsce. Chodziło o amerykańskie wojsko
2020-07-23

“Polska Agencja Bezpieczeństwa Wewnętrznego zatrzymała oficera litewskich sił zbrojnych Antanasa K., podejrzanego o szpiegostwo na rzecz Litwy. To bezprecedensowy przypadek zatrzymania litewskiego żołnierza w Polsce. Według doniesień, oficer próbował zdobyć tajne informacje, wykraczające poza jego kompetencje.

Jak informuje ABW w ciągu roku szpieg przekazał te informacje Litwie, na jej podstawie Litwini dostosowali politykę informacyjną państwa, aby zwiększyć swoje szanse na przeniesienie sił USA nie do Polski, ale na Litwę.

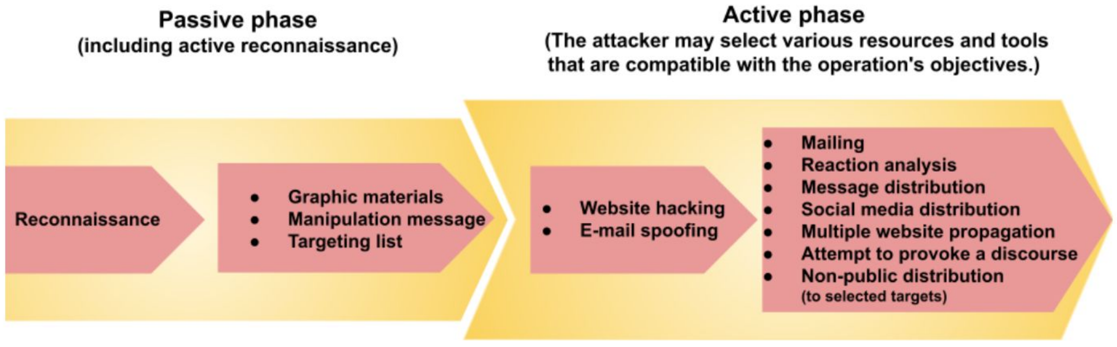
Według dostępnych informacji „podejrzany działał bardzo profesjonalnie", będąc oficjalnym przedstawicielem Litwy w dowództwie Wielonarodowego Korpusu Północno-Wschodniego w Szczecinie.

Sending an email was just a single element of a broader disinformation campaign - articles with false messages about a Lithuanian spy had been identified on the Internet two days earlier than the email was sent and not only in the Polish-speaking information environment.

The alleged espionage case was first mentioned within German-speaking infosphere on one of the anonymous blogs. A few hours later the information was published in the "The Baltic Course", a Russian business magazine issued for the audience in Baltic states and in English-speaking online news services, such as Theduran.com, qualified as objects permanently spreading Russian manipulative content.

The disinformation attack, aimed primarily at disparaging Lithuania's military and defence system, was also intended to negatively affect the security cooperation between Poland and

Lithuania by showing the actions of Lithuanian intelligence as potentially hostile in relation to Poland.

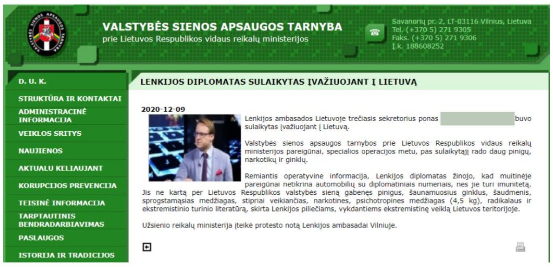

Passive phase
(including active reconnaissance)
Active phase
(The attacker may select various resources and tools that are compatible with the operation's objectives.)
Reconnaissance
Graphic materials
Manipulation message
Targeting list
Website hacking
E-mail spoofing
Mailing
Reaction analysis
Message distribution
Social media distribution
Multiple website propagation
Attempt to provoke a discourse
Non-public distribution
(to selected targets)

Model based on research conducted by INFO OPS Poland Foundation at Info Ops Laboratory

The model shows a sequence of information operation carried out by an actor associated with cyber attacks conducted on behalf of Russian Federation. In the example disinformation was implemented on a website after the website was attacked and eventually hijacked. Then original content was replaced with disinformation and disseminated through several channels as legitimate information provided by authorities. The model encompases all three dimentions of the information environment: physical, virtual and cognitive (for more information see the "Russian models…" section).

Described operation is just a sample of a broader manipulative campaign that is being carried out by the Russian Federation against Poland and Lithuania and against NATO as a whole with its enhanced military cooperation in the region. There are other disinformation operations carried out simultaneously, whose objectives are narrowed down to a single country, like Lithuania and especially its armed forces. In April 2020, a fake letter of NATO Secretary General Jens Stoltenberg was published on the Internet. According to the letter, Stoltenberg was supposed to inform on the withdrawal of the allied forces from Lithuanian territory. At that time as well a crafted email containing false information was sent to the media and public institutions, most likely to initiate the operation and stir public opinion. The pattern and technique was very similar to the one used in the case of Antanas K. .

For greater effect Russian propaganda activities very often refer to the current situation and real contexts. This technique was used when Polish-German border was closed in March 2020 due to the attempts of preventing the spread of coronavirus to Poland. Russian "media" then used the opportunity and exploited the issue by picturing it in a negative way to affect the perception of Poland among Lithuanian drivers. The Russian media falsely claimed that there were fights on the border and Lithuanian drivers were blocked. So-called media reported on alleged outbreak of anxiety, fights and even the need to use the special forces so the situation "could be handled". These reports were intentionally manipulated and in fact nothing like this ever happened.


VALSTYBĖS SIENOS APSAUGOS TARNYBA
prie Lietuvos Respublikos vidaus reikalų ministerijos

Savanorių pr. 2, LT-03116 Vilnius, Lietuva
Tel. (+370 5) 271 9305
Faks. (+370 5) 271 9306
Į.k. 188608252

LENKIJOS DIPLOMATAS SULAIKYTAS ĮVAŽIUOJANT Į LIETUVĄ

2020-12-09

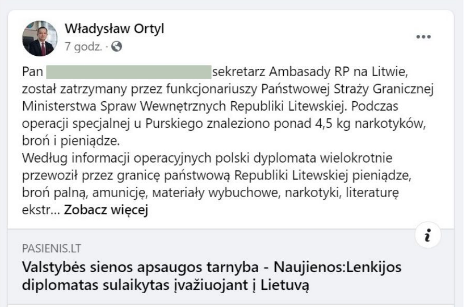
Lenkijos ambasados Lietuvoje trečiasis sekretorius ponas [redacted] buvo sulaikytas įvažiuojant į Lietuvą.

Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos pareigūnai, specialios operacijos metu, pas sulaikytąjį rado daug pinigų, narkotikų ir ginklų.

Remiantis operatyvine informacija, Lenkijos diplomatas žinojo, kad muitinėje pareigūnai netikrina automobilių su diplomatiniais numeriais, nes jie turi imunitetą. Jis ne kartą per Lietuvos Respublikos valstybės sieną gabenęs pinigus, šaunamuosius ginklus, šaudmenis, sprogstamąsias medžiagas, stipriai veikiančias, narkotines, psichotropines medžiagas (4,5 kg), radikalaus ir ekstremistinio turinio literatūrą, skirta Lenkijos piliečiams, vykdantiems ekstremistinę veiklą Lietuvos teritorijoje.

Užsienio reikalų ministerija įteikė protesto notą Lenkijos ambasadai Vilniuje.

There are other examples of cyberattacks launched as an element of disinformation operation. One of them was a message about the detention of a Polish diplomat smuggling drugs and weapons that appeared on the hacked website of the Lithuanian Border Guard. This false statement was posted on Wednesday evening, December 9, 2020. The message claimed that the Lithuanian Border Guard officers had found a large amount of money, drugs and weapons with the diplomat. The statement also insinuated that the Polish diplomat "*repeatedly conveyed money, firearms, ammunition, explosives, narcotics, psychotropic substances (4.5 kg), radical and extremist literature for Polish citizens conducting extremist activities in Lithuania*". The attacker was aiming at provoking an information incident and triggering a debate in the media. He tried to raise interest with help of a spoofed Lithuania's MFA email and a hacked website of LT State Border. The intention was to damage the reputation of Poland and Polish diplomatic service and present it as an organisation committing criminal acts and carrying out active measures against Lithuania. By its nature the attack was very similar to another operation carried out in November 2020 where a similar message was posted on a false website of the Lithuanian Police. A fake statement was disseminated in which the attacker claimed that "extremists from Poland suspected of terrorist activity in Lithuania were arrested.”



Władysław Ortyl
7 godz. ·

Pan [redacted] sekretarz Ambasady RP na Litwie, został zatrzymany przez funkcjonariuszy Państwowej Straży Granicznej Ministerstwa Spraw Wewnętrznych Republiki Litewskiej. Podczas operacji specjalnej u Purskiego znaleziono ponad 4,5 kg narkotyków, broń i pieniądze.
Według informacji operacyjnych polski dyplomata wielokrotnie przewoził przez granicę państwową Republiki Litewskiej pieniądze, broń palną, amunicję, мateriały wybuchowe, narkotyki, literaturę ekstr... Zobacz więcej

PASIENIS.LT
Valstybės sienos apsaugos tarnyba - Naujienos:Lenkijos diplomatas sulaikytas įvažiuojant į Lietuvą

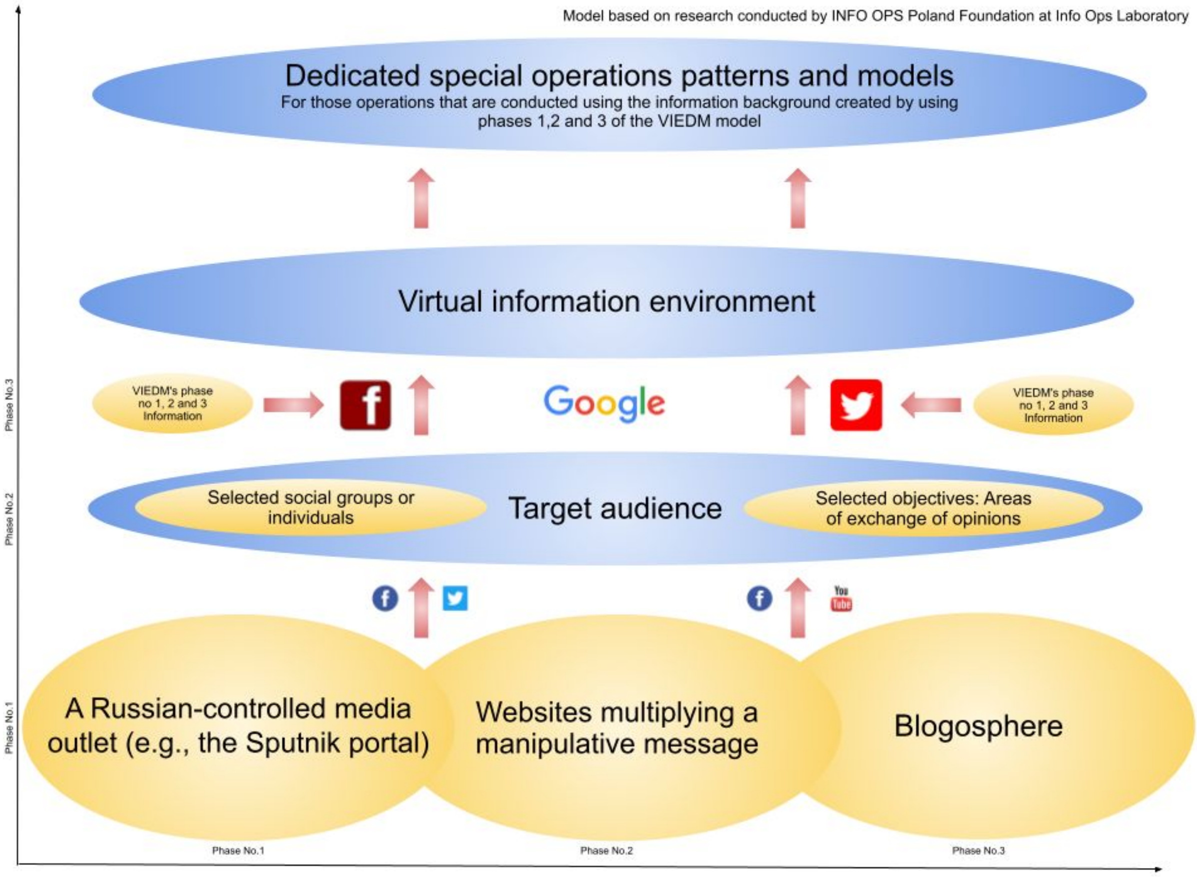
Similarly to the previous two operations, the latest one wasn’t limited just to posting false information on a website - the attacker tried to spread through social media and targeted accounts of two Polish politicians for effect. In the case of allegedly "arrested Polish extremists", the attacker used social media accounts belonging to two members of the Polish Parliament and the disinformation about the detention of a Polish diplomat appeared on a fake profile of Władysław Ortyl - the Marshal of the Podkarpackie Voivodeship. The social media account of Władysław Ortyl was not a fake account, but a fake duplicate impersonating a politician.

Russian models for the distribution of manipulative messages

In the case of Russian manipulative operations one of the active measures used to influence the audience's cognitive processes are models of influence on the information environment. Cyberspace has now become the dominant dimension of message shaping and is intensively used to manipulate the information environment in public and non-public areas. However, cyberspace is not the only dimension of influence operations. It is often used as a secondary layer after some event or incident takes place or is caused in the physical dimension. Cyberspace and the infosphere are inseparable areas of the information environment, which consists of three interacting dimensions: physical, virtual and cognitive. In the modern virtual information environment messages are subjected to a complex and dynamic process of continuous creation, processing, replication and modification, which is taking place within media, social media, and the blogosphere. On top of that various tools and techniques are used and they may differ or overlap regarding the channel or the message itself. Useful models of influence include all the mentioned aspects, and are not limited exclusively to transmission of information that can be classified as manipulative and misleading. In some very specific cases they might be used to disseminate information which is supposed to influence cognition in a very subtle way, e.g. with the use of a color graphic message adapted to the weather conditions prevailing in a particular location (a human reacts differently to bright colors at low and high atmospheric pressure). The use of such methods proves that the involvement of professional special operators in the process of conducting an information attack is necessary and it would be virtually impossible to launch such an attack without specialist knowledge and informational infrastructure.

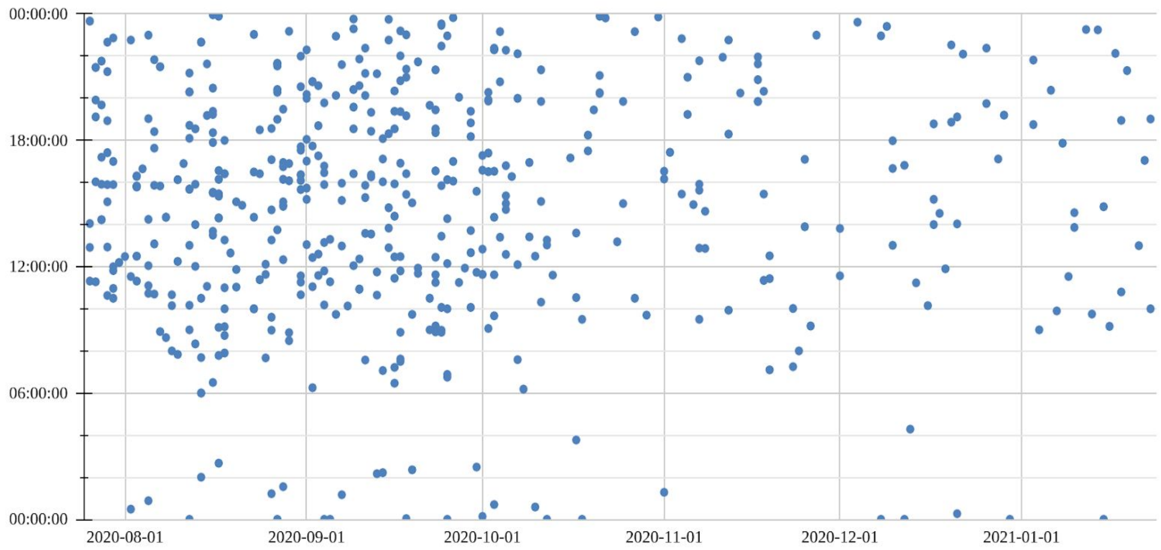
The Russian Federation uses dozens of models qualified as VIEDM (virtual information environment distribution model). One of them is a public VIEDM of the first type used to distribute and replicate manipulative messages and influence Polish information environments on a regular basis. The first information object that operates within this model is the Sputnik website. It is used to inject manipulative messages into the Polish-speaking infosphere. In terms of absolute figures the website's range might seem limited and therefore irrelevant. Such an understanding of the matter is misleading though. To fully understand the mechanism of influence several stages must be taken into consideration and injecting specific types of information via Sputnik is only the first one in a multilayer model. The second stage of the VIEDM is at the same time the first multiplication of Sputnik messaging and at this point of operation, the original text of the message is not yet significantly changed by Russian operators and is easy to identify. Overall messages originating from Sputnik are slightly changed and replicated multiple times by other objects and manipulative content is then published on a set of websites. The third phase is the transfer of content to the blognetwork. At this stage of VIEDM the original manipulative content is changed significantly and often presented in form of "private" opinions on publications from the second stage of VIEDM. At the fourth stage the manipulation unit using VIEDM model starts to use objects in social media to distribute manipulative material in various ways with intention to influence platforms of where natural internet users and target audience exchange their opinions on a regular basis. On the next stage the attacker differentiates further the objects of influence and narrows down its messaging to thematic and specialized channels used for distribution of information: internet forums, comments under publications, thematic blogs, Facebook groups on international relations, defence, politics, energy, history and about Polish minority in Lithuania. The main difference between this stage and the previous one is that at this point another set of adversary's operators are involved using different tools. These are generally well-prepared fictitious users of different internet forums who are setting pace and steering the discussions using materials from the second and third stage of operation, as well as organically produced content. They operate according to prepared in advance plan and logic, which includes maintaining the debate and not letting it go down too early, sending false positive messages to individual recipients or distributing support for special operations aimed at a specific person or a team of people.

This stage of operation gives an opportunity to directly target carefully selected groups or decision-makers. In some cases, it is possible to identify an attempt to influence an individual decision-makers through so-called "opinion leaders": The opinion leader could be a natural person, for example an agent of influence, or virtual object – seemingly existing user, social group and others. In addition to the opinion leader, at this stage a whole set of different tools might be used to increase the odds of operation. They include, among other things, social engineering, profiling, reaction analysis, examination of behavioral patterns etc. (one of the tools used by the Russians at this point would be examining the target's response to information stimulus – in this case, information, disinformation or manipulation). Those activities are in fact a part of the whole range of psychological offensive measures which require involvement of professional special operators during an information attack.


Model based on research conducted by INFO OPS Poland Foundation at Info Ops Laboratory
Dedicated special operations patterns and models
For those operations that are conducted using the information background created by using phases 1,2 and 3 of the VIEDM model
Virtual information environment
VIEDM's phase no 1, 2 and 3 Information
Google
VIEDM's phase no 1, 2 and 3 Information
Selected social groups or individuals
Target audience
Selected objectives: Areas of exchange of opinions
A Russian-controlled media outlet (e.g., the Sputnik portal)
Websites multiplying a manipulative message
Blogosphere
Phase No.1
Phase No.2
Phase No.3
Phase No.1
Phase No.2
Phase No.3

Communication dynamics

Dynamics of communication of Polish-speaking websites disseminating manipulative messages aimed at the perception of Lithuania in Russian and replicating Russian objects in cyberspace from January 2020 to January 2021:



The study was based on a measurement of recognized communications in cyberspace from January 2020 to January 2021.

The study of the dynamics of manipulative communication proves that the Virtual Information Environment Distribution Model (VIEDM), controlled by the Russian Federation, is functioning according to the principle of operational continuity. Despite the periods of higher dynamics of communication, which are usually connected with the events in the international relations, it keeps a relatively steady level of negatively influencing the perception of Lithuania and Lithuanians in the Polish-language information environment. The tactics used by the Russians to influence and saturate the information environment allows us to conclude that the actions aimed at the weakening of mutual perception of Poslish-Luthuanian relations are one of the permanent vectors of the manipulation operation aimed at these states by Russia.

Complete list of websites is available in the non-public version of the report.

Summary.

In-depth analysis of the incidents presented in the report provides enough evidence to state that Russian disinformation operations targeting Polish-Lithuanian relations are not incidental at all and terminology used in professional risk assessment (incidents) shouldn't lure careful readers. In fact they are elements of **well-thought, sophisticated strategy** which aims at achieving long-term goals, also its objectives might seem marginal or irrelevant when analysed separately.

One of the main features of this strategy is **continuity of actions and messaging**. To successfully damage mutual perception between Polish and Lithuanian societies and decision-makers, adversary saturates both information environments with malicious messages on a regular basis. Instead of triggering instant reactions, they serve as informational fertilizer preparing ground for future operations. Once the situation is assessed as ripe, operations are launched and carefully conducted to cause as much harm as possible and provide the adversary with tools for the future harmful activities.

In most of those operations a relatively small number of topics is exploited but all of them revolve around current and historic events and issues, that for Poland and Lithuania have (or may have in certain contexts) strategic meaning. Apart from **military and security cooperation, defense and energy security** which are the most obvious targets for Russian disinformation activities, few social and historic topics are used as well. Those focus mostly on alleged discrimination of Polish minority in Lithuania and quasi-historic debate on origins of Lithaunian nation. While the first group of topics is exploited with intention of influencing on-going events and their perception, the second group fuels antipathy between Poles and Lithuanians creating ground for potential conflict of ethnic nature. Such a conflict might be then politically capitalized, which indeed happened in case of Akcja Wyborcza Polaków na Litwie - Związek Chrześcijańskich Rodzin.

Russian disinformation operations are well conceptualized within the so-called **Virtual Information Environment Distribution Models (VIEDM)**. Depending on target and context, different models might be used and it is important to understand that those models aren't just theoretical constructs - most of the time they serve rather as very practical roadmaps. On the other hand they might be perceived as blueprints of informational infrastructure, including objects, assets and even technical solutions and techniques used by the adversary.

Understanding those models helps to unveil the general logic of action, thus enables the defenders to better anticipate and prevent potential threats.

Report by: INFO OPS Poland Foundation and Res Publica – Civic Resilience Center
https://infoops.pl/ https://respublica.lt/

INFO OPS
POLSKA

Res Publica

Fortis In Unum
Stiprūs kartu