

# Intent to Infekt: 'Operation Pinball' Tactics Reminiscent of 'Operation Secondary Infektion'

By Insikt Group®



## Executive Summary

Insikt Group recently identified an ongoing information operation that we assess with high confidence shares significant overlap with what the Atlantic Council's Digital Forensics Lab (DFRLab) refers to as Operation Secondary Infektion ([Secondary Infektion](#)); a covert information operation targeting governments in the United States and Europe and believed to originate from Russia. We have named this information operation "Operation Pinball."

Recorded Future's investigation into Operation Pinball revealed a covert influence operation that analysts assess attempted to undermine the government of Estonia and its relationship with the European Union while exploiting the ongoing European migrant crisis. Recorded Future analysts also discovered a second instance of this campaign targeting the government of Georgia and the disputed territories of Abkhazia and South Ossetia, and seeking to undermine Georgia's growing relationship with the North Atlantic Treaty Organization (NATO). This information operation consisted of a wide network of self-publishing webpages, one-off accounts, Reddit and social media promotion, and analysts saw evidence of an emphasis on operational security (OPSEC) and connections to sources that Insikt Group assesses to have a strong command of the Russian language. We assess with high confidence that this information operation targeted Russian-speaking audiences in Eastern Europe and among the Commonwealth of Independent States (CIS). At this time, analysts assess with high confidence that at least one of these operations is ongoing, and others, as yet unidentified campaigns, are likely in planning stages.

Further investigations into one self-publishing website revealed additional, previously undisclosed, attempts to plant false documents targeting U.S. officials and U.S. political organizations' relationships with international policymakers and governmental bodies. It appears that these fraudulent documents attempt to emulate confidential correspondences on sensitive international issues in Eastern Europe to make them seem to be authentic leaked information on the topics. The age of these documents, ranging from January to June 2019, aligns with known activity periods of Secondary Infektion.

This report illustrates Recorded Future's observations in detail. Analysts believe that this activity demonstrates the complexity and layers of this campaign and indicates that similar, prior campaigns were more wide-ranging among Eastern European sources than initially thought.

It is also important to note that while there is strong evidence to indicate a coordinated effort to push this false story into the mainstream, this event, like most Secondary Infektion-attributed events, was not successful. Overall, Insikt Group identified minimal shares on social platforms and Reddit threads were quickly deleted by page administrators of the various pages.

Further, we believe that the prodigious OPSEC demonstrated by this group limited the effectiveness of single-use accounts to build personas and grow audiences required for content to go viral. Based on our observations, if an active campaign does not reach mainstream sources the effort is likely to be abandoned.

## Key Judgments

- We found that this activity shared significant overlap with previously reported tactics, techniques, and procedures (TTPs) used in Secondary Infektion campaigns, namely the use of self-publisher blogs with single-use personas, Reddit promotion, and multilingual obfuscation. Distinct TTPs overlapping with Secondary Infektion that we emphasize in this report include the following:
  - The use of forged letters and email correspondence
  - Targeting of geopolitical incidents in the greater CIS
  - Language errors that are characteristic of native-Russian speakers
  - Seeding on self-publisher websites to include homment.com, as well as self-publishers based within Russia's "near abroad"
- We assess with high confidence that Estonia-targeted activity was a coordinated, deliberate attempt with four objectives:
  - Undermine the relationship between Estonia and the EU

- Degrade Estonian confidence in their government
- Create internal political strife among elected Estonian officials
- Alter public opinion against migrants coming to Estonia, and to a greater degree sour the public perception of migrants in Europe
- We assess with high confidence that Georgia-targeted activity is a coordinated, deliberate attempt with five objectives:
  - Prompt support and international recognition of Abkhazia and South Ossetia quests for independence
  - Undermine a growing relationship between the NATO alliance and Georgia
  - Undermine Georgian support of national political leadership and establish a narrative that current political figures are corrupt to the benefit of the West
  - Create uncertainty in Georgia's economy and energy independence
  - Promote the narrative that NATO consists of a selfish, ruling elite that does not have Georgia's best interests at heart
- We expect to see additional instances of Operation Pinball tactics, such as the use of planted false documents against Western governments and international institutions, even though these information operations have been largely unsuccessful to date.
- We assess that covert influence operations from Russia against the U.S. and the 2020 election will probably seek to leverage similarly manipulated and forged documents, particularly regarding attempted hack-and-leak operations when the adversary either may not have access to original files, or deems hacked authentic files as ineffective *kompromat*.

## Background

Throughout 2019, Recorded Future observed [reporting](#) from the Atlantic Council's Digital Forensics Lab (DFRLab) of an alleged Russian-based information operation, dubbed [Secondary Infektion](#). The operators used covert "fake accounts, forged documents, and dozens of online platforms to spread stories that attacked Western interests and unity." DFRLab attributed this suspicious activity to a Russia-based covert operation, based on an analysis of a small network of accounts originating from Russia that was [suspended](#) by Facebook in May 2019 after they were found to be distributing false claims and news stories tied to initial Secondary Infektion vectors.

Secondary Infektion is named after the notorious Soviet Union-era "[Operation Infektion](#)" disinformation campaign that aimed to convince the world that AIDS was invented by the United States. In all, Operation Infektion took four years to reach mainstream media mentions. What has changed recently, however, is the speed and precision targeting with which such operations can be waged using social media and other online platforms. In other words, what took Operation Infektion years to achieve potentially takes only days or weeks at most for Secondary Infektion information operations — if they are successful.

Secondary Infektion bears similarities to well-known "hack-and-leak" operations, a practice in which stolen information is subsequently released in an attempt to influence public perception for or against an issue. Hack-and-leak operations have targeted U.S. political organizations, such as the Democratic National Committee (DNC) and Democratic Congressional Campaign Committee (DCCC), with the contents of these leaks later released to the public by known GRU operations [DCLeaks and Guccifer 2.0](#) as a means of election interference in the 2016 U.S. presidential election. Similar hack-and-leak [operations](#) have targeted international sports regulatory agencies such as the World Anti-Doping Agency (WADA), as well as malicious information campaigns against athletes.

In the case of Operation Pinball, we observed significant overlap with Secondary Infektion's use of false stories, often including planted fake document images ("leaks") posted by one-off burner personas on obscure online platforms such as self-publishing

journalistic outlets or blog sites. These stories were often then revised or expanded upon using a second set of established burner personas on sites such as Reddit, LiveJournal, and self-published (but more frequently used) blogs with little to no moderation or policing. At this step, these information operations translated false claims into another well-known language (such as English, French, or German) both for broader consumption as well as using translation to obfuscate the origins of the claim.

The final step included personas pushing false stories on social media, with the ultimate aim of targeting mainstream media and news organizations for broader audience consumption. In the case of Guccifer 2.0 and other hack-and-leak operations tied to the GRU, the adversaries conducting the activity [communicated](#) with journalists in a likely attempt to provide greater visibility for the information. The most recent instance of this behavior pertaining to Secondary Infektion was when leaked trade documents from the U.K. National Health Service (NHS) were [distributed](#) to Global Justice Now, a U.K.-based organization, through a secure email address with no name.

According to DFRLab, Secondary Infektion information operations share attributes commonly associated with Russian intelligence services, namely that the activity their research team observed was conducted with a high degree of operational security (OPSEC), was well resourced, and persisted over a long period in support of objectives that align with ongoing Russian strategic goals. Despite these observations, there is no available information that directly links Secondary Infektion, or Operation Pinball for that matter, to Russian intelligence services as of this writing. We assess that this is because the operators are highly skilled in OPSEC and use techniques that effectively obfuscate their origins. OPSEC not only provides key plausible deniability, but allows Russian state-sponsored media to [counter](#) these observations with alternative hypotheses, insults, doubt, and other distractions.

## Discovery of Operation Pinball Targeting Estonia

### Threat Analysis

On December 18, 2019, the author “flokortig” published the article [“Neue Flüchtlingskrise: Europa ist nicht dazu bereit,”](#) (Translated: “New refugee crisis: Europe is not ready for it”) on the German self-publishing website homment.com. Homment was previously linked to multiple instances of Secondary Infektion document seeding as reported by DFRLab. After publication, Homment visitors viewed the article approximately 250 times.

This article began by blaming the U.S. and Europe for “wars in Middle East [sic] and Africa,” resulting in waves of refugees entering Europe since 2015. The article proceeded to illustrate “the reception of refugees in some EU countries,” highlighting France and Greece, claiming that non-transit migrants overwhelm France, and noting reports of violence among migrants in Greek refugee camps. The article then turned to Estonia, claiming that the state welcomed the EU’s migration quotas, despite “political opposition and existing government disagreements.”

The post included a copy of a letter, which we judge was inauthentic, addressed to Mr. Dimitris Avramopoulos, the European Commissioner for Migration, Home Affairs and Citizenship, from Taavi Aas, Minister of Economic Affairs and Infrastructure of Estonia. The letter made the claim that Estonia agrees with the EU refugee admission quotas despite concerns regarding statements from Foreign Affairs Minister Urmas Reinsalu and “several other Estonian politicians” that were deemed contrary to the EU’s standing on migrant quotas. The letter claimed these dissenting views were, in fact, the personal views of these individuals and were stated only to score “political points.”

The article also pointed out that Hungary, the Czech Republic, and Poland are campaigning against the EU immigration policy “by building a wall as they wish and deciding for themselves who will enter their territory ... Such steps by the Eastern European countries make it difficult to implement the common EU migration policy.” These domestic policies, according to the article, only further hinder other EU states from adequately accommodating migrants.

In relation to the European migrant crisis, the article stated the following:

*“The situation looks bleak on the whole. The state of the infrastructure for the reception of asylum seekers in the EU shows that Europe is not ready for the wave of refugees like in 2015. The EU-Turkey Refugee Agreement, which aimed to reduce the number of refugees entering the EU, has stopped working. EU migration policy is paralyzed. It is unclear whether one can find the way out. Because of the disagreements between Western and Eastern Europe, the real unity of the European continent is very doubtful.”*





REPUBLIC OF ESTONIA  
MINISTRY OF ECONOMIC AFFAIRS  
AND COMMUNICATIONS

Mr. Dimitris Avramopoulos  
European Commissioner  
For Migration, Home Affairs and Citizenship

12<sup>th</sup> of November 2019

Dear Commissioner Avramopoulos,

I understand your concerns with statements of Estonian Minister of Foreign Affairs, Urmas Reinsalu, and several other Estonian politicians about refugee admission quotas and the country's engagement in this process. I want to assure you that the statements reflect the views of these persons and are an attempt to score political points by focusing on this obviously important issue for Europe.

As you know, Estonia is fully committed to European values and is totally ready to fulfill its obligations. All agreements relating to refugee reception projects, including establishment of new centers on the territory of Estonia and allocation of funds for these purposes, are being implemented in line with the plans approved.

Yours sincerely,

Taavi Aas  
Minister of Economic Affairs  
and Infrastructure of Estonia

Ministry of Economic Affairs and Communications/ Suur-Ameerika 1 / 10122 Tallinn/ ESTONIA/ +372 625 6342/  
fax +372 631 3660/ info@mkm.ee / www.mkm.ee

*Forged letter addressed to Mr. Dimitris Avramopoulos from Estonian Economic Affairs Minister Taavi Aas.  
(Source: Homment)*

By analyzing the document, it is quickly apparent that native English-language speakers did not prepare this document, but was a well-crafted attempt at appearing authentic. [We are aware that](#) Taavi Aas speaks fluent English and official correspondence from the Ministry would most likely not include any of the following errors and observations.

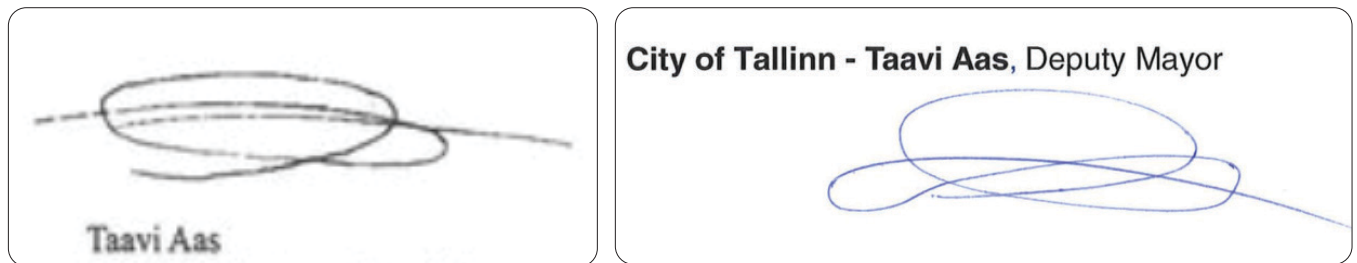
One indicator of inauthenticity is located in the first statement, “I understand your concerns with statements **of** Estonian Minister of Foreign Affairs...,” which is a grammatically incorrect English construction. Insikt Group Russian-language experts note that potential linkage of this sentence to a Russian speaker is the use of the genitive case in Russian, which, when translated into English, sometimes results in the incorrect use of the preposition “of” to denote ownership. Furthermore, this example demonstrates a consistent lack of indefinite/definite articles throughout the forged document, to include this example. Russian does not have a definite or indefinite article (i.e. the/a/an) or the verb “to be” in the present tense, and many English-speaking Russians have considerable trouble using “the” and “a” correctly, often using them interchangeably or leaving them out entirely. If a fluent English speaker correctly wrote this statement, it would likely state “I understand your concerns with [the] statements of [the] Estonian Minister of Foreign Affairs...”

In the body of the document, there are multiple instances of unusual or colloquial language that are unlikely to appear in formal government correspondence, such as the use of the words “totally ready,” “scoring political points,” as well as the statement “establishment of new centers **on** the territory of Estonia,” rather than simply, in Estonia. We note that на территории (on the territory of) is commonly spoken in Russian and is grammatically correct.

The forged letter contains what we refer to as imprecise language, meaning that the author likely did not have a concrete position on Estonian migrant quotas or specific government projects and was likely not entirely well versed in the subject matter. Therefore, the author of this document resorted to vague or confusing phrases such as “establishment of centers” rather than specifying refugee centers or specific housing projects for migrants in Estonia.

The footer of the document itself has improper spacing, which would likely not pass by a government-level editor. Further, the titles of Mr. Avramopoulos and Mr. Aas on the letter are improperly and inconsistently formatted.

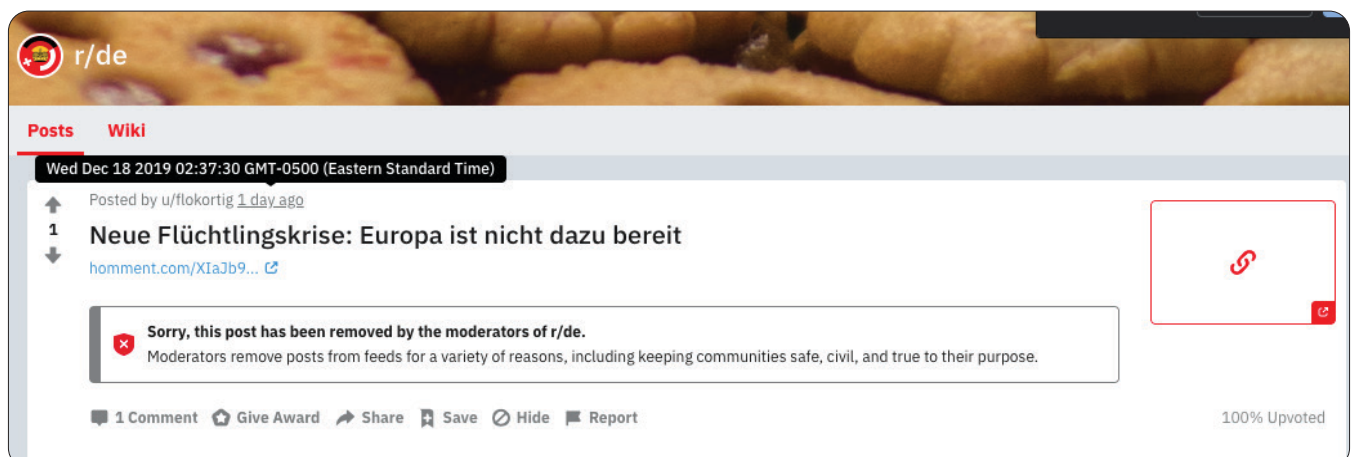
The signature of Mr. Aas also raises concerns. While his signature is not commonly found in open sources, a 2010 [document](#) prepared by The Civitas Initiative and the EU, which contains Mr. Aas's legitimate signature during his tenure as Tallinn deputy mayor, indicates that the signature found in the 2019 letter was likely an attempted, far-less fluid, forgery. Given the simplicity of the signature itself, this opens opportunities for attempted emulation.



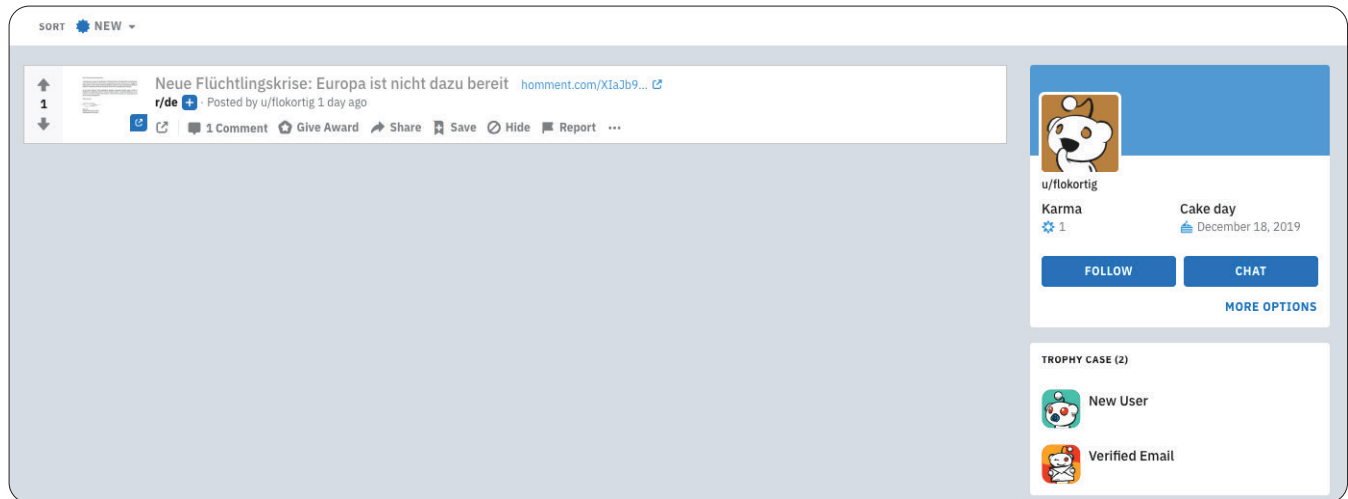
Comparing a verified signature of Taavi Aas (right) to the forged document (left).

## Initial Reddit Amplification

[Reddit](#) user “[u/flokortig](#)” — the same name as the author on Homment — shared the article once on the German subreddit [r/de](#). This post was shortly thereafter removed by moderators for an unspecified reason. This was [u/flokortig](#)'s only post, made within one minute of registration based on the Reddit account's metadata. This account was also registered on the day that [flokortig](#) published the article on [homment\[.\]com](#).



[u/flokortig](#)'s post on the German subreddit [r/de](#), sharing the article “[Neue Flüchtlingskrise: Europa ist nicht dazu bereit](#)” on [Homment](#). (Source: [Reddit](#))



*u/flokortig's user profile page on Reddit, demonstrating a minimal post history. (Source: Reddit)*

A search for the exact text of this article's title on open sources discovered the Homment article shared, at least temporarily, on the following websites: Austrian forum [meinbezirk.at](#) (broken link), and German forums [kraichgau.news/bretten](#) (broken link), [nachrichten-aktuell.eu](#), [meine-news\[.\]de/nilkheim](#) (unavailable), and [de.indymedia\[.\]org](#) (unavailable). The author of the articles on these sites often appeared under the moniker "Florian Kortig."

Insikt Group assesses that Operation Pinball, and TTPs aligned with Secondary Infektion in general, uses German-speaking self-publishers, in addition to blog sites for other European languages, likely as both a medium to distribute false information and to further obfuscate the operation's activities.

In a temporarily available cached version copy of the article on [meinbezirk\[.\]at](#), Insikt Group found, via a formatting error, that the file upload service [Post Image](#) hosted the document. Searching this image link in open sources revealed copies of this report shared on [oko-planet.su](#), which links to a copy shared on the website [perevodika.ru](#), both dated December 19, 2019. On [perevodika\[.\]ru](#), the source backlinked to the Homment article dated December 18, 2019. The author of this post used the moniker "leovitaus." To date, this article has received over 2,300 views and one comment. Based on these metrics, this article was likely an anchor for much of the story's promotion across Russian-speaking sources.

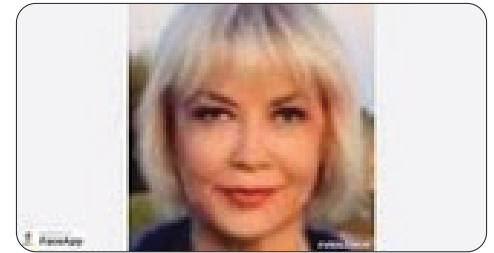
In an investigation of “leovitaus,” we found another copy of the article with the forged letter posted by an individual under the same name on the Russian forum Ursa Manor Forums [ursa-tm.ru](https://ursa-tm.ru), under the forum’s subpage dedicated to Russian translations of international articles. Insikt Group concludes that this too was an inauthentic account, made for single use only to further distribute the article. As of January 20, 2020, thread visitors viewed the post approximately 900 times and the post garnered 23 replies.

The screenshot displays the user profile for 'leovitaus' on the Ursa Manor Forums. At the top, there is a profile picture of a person in a field and the name 'leovitaus' with the title 'Пользователи'. Below this, statistics are shown: 'CONTENT COUNT' is 1, 'JOINED' is December 19, 2019, and 'LAST VISITED' is December 19, 2019. A button labeled 'See their activity' is in the top right. The profile is divided into sections: 'ABOUT LEOVITAUS' showing a rank of 'Маленький ёжик', and 'ИНФОРМАЦИЯ' showing 'Пол' as 'Мужчина' and 'Проживает' as 'Россия'. A recent post is featured with the title 'Новый миграционный кризис: Европа не готова' and a snippet of text: 'Из-за войн на Ближнем Востоке и в Африке, в которых участвовали США и европейские государства, начиная с 2015 г. Европу захлестнула волна беженцев. Это стало настоящим кризисом и вызвало резкое обострение социальной напряженности. Дальше будет еще хуже, прогнозирует глава МВД Германии Хорст Зеехофер. В конце сентября Хорст Зеехофер побывал с визитом в...'. The post has 23 replies and 39 likes.

*leovitaus's profile on Ursa Manor Forums, created and last accessed December 19, 2019*

There is evidence that this initial copy was picked up by authentic Russian news aggregators, further amplifying its spread. Among Russian sources, Insikt Group found the forged document with the title “Новый миграционный кризис: Европа не готова” (Translated: “New migration crisis: Europe is not ready”) on a number of different sites, including [worldaggressor.com](https://worldaggressor.com), [cont.ws](https://cont.ws), and the Russian news aggregator [newsland.com](https://newsland.com). Both newsland[.]com and cont[.]ws originated from what we found to be the same person, referred to as Elena Frolova.

On Newsland, the profile “[Elena Frolova](#)” reposted the article on December 20, 2019. Interestingly, this article directly cited the German instance found on Homment, rather than another Russian source. Oddly, this page did not contain a copy of the forged document, but rather [displayed a photo](#) of German Interior Minister Horst Seehofer, mentioned in the article, and a photo from an October 2015 article from [The Atlantic](https://www.theatlantic.com) titled “Thousands of Migrants Are Crossing the Balkans on Foot.”



*"Elena Frolova" on [Newsland](#). Insikt Group further investigated the profile as the photo appeared doctored, pointing to a FaceApp watermark in the left-hand corner.*

Insikt Group found another instance of "Elena Frolova" on the Russian social media site [Maxpark](#), as well as on [cont.ws](#). It is most likely that this is the source of the page appearing on Newsland. In total, the pages reached an audience of approximately 450 viewers and only six comments. On [cont\[.\]ws](#), Insikt Group identified the moniker's VK social media profile and determined that it is a legitimate account. Recorded Future has opted to not publish the link to this profile for privacy considerations. Nonetheless, this instance demonstrates that unsuspecting news aggregators and legitimate social media profiles can quickly pick up and further propagate intentionally planted disinformation.

On January 11, 2020, the Russian-language news website [e-news.su](#) published an exact text copy of this article though it did not contain a copy of the forged document. It instead provided two links, a link to the "original" (Оригинал) and a "translation" (Перевод). The original source was, like in the previously mentioned instances, the German article posted to Homment, while the link to the translation reverted to the "leovitaus" forum post on Ursa Manor Forums.

Insikt Group assesses that the article posted to Homment was most likely translated directly from German to Russian, based on the dates of publication and that instances discovered on Russian sources are near-duplicates, with minimal changes as a result of direct translation.

A deeper investigation into the dispersion of the forged letter led Insikt Group to determine that the original source was most likely not from Homment, but in fact the German version that was originally translated from Russian, and then later back into Russian.

By analyzing the link to the Post Image image repository, Insikt Group found another website containing this document from the image found on Post Image, [stena.ee](http://stena.ee), an Estonian self-publisher, which was not previously found linking to this group of articles. This article posted on stena[.]ee was a near-copy of the article found on homment[.]com; however, the author “dimitriteras” posted the article on December 3, 2019. The moniker dimitriteras could not be found on any additional websites or self-publishing forums.

Insikt Group assesses with moderate confidence that the article posted to Stena was the seed article for this campaign, originally written in Russian. Our investigation determined that this was the earliest date in which we identified a version of this article and forged document. We note that at the time of publication, this blog post was removed from the site.

One observed change from the most recent articles, however, was the title, which, when translated, reads, “Multiculturalism lessons from Brussels: EU is building new refugee accommodation centers in Estonia.” (“Уроки мультикультурализма от Брюсселя: ЕС строит новые центры размещения беженцев в Эстонии”). Further analysis of the article itself revealed that it appeared to be an editorial-type version of the article posted to Homment, as it is more opinionated, and takes a more anti-immigrant stance:

*“Migrants who have been accustomed to meet sympathy and help from tolerant Western Europeans for so many years have become so familiar with us that they behave at home, ignoring local basic rules of behavior, laws and culture. At the same time, attempts to integrate new ‘Estonians’ fail one after another: forcibly displaced refugees do not want to adapt to new conditions, get a job and learn the local language, actively using the social benefits provided by the European Union.”*

Like flokortig's post to Homment, this article was the only post made by this account.

The screenshot shows the Stena website interface. At the top, there is a navigation bar with links for 'Все новости', 'Объявления', 'Афиша мероприятий', 'Погода и расписание автобусов', and 'Тематические блоги'. Below this is a search bar and a 'Найти' button. The main content area features a large banner for 'TravelBest' with a Santa Claus illustration and the text 'ЗАКАЖИ ТУР И ПОЛУЧИ ПОДАРОК! Рождество и Новый Год!'. Below the banner, the article title 'Уроки мультикультурализма от Брюсселя: ЕС строит новые центры размещения беженцев в Эстонии' is displayed. The article text begins with 'На протяжении последних лет Европа переживает беспрецедентный миграционный кризис. Массовое переселение людей с Ближнего Востока и Африки приобрело характер настоящей катастрофы...' and continues to discuss the challenges of migration and the role of the EU.

A likely original source of the article "Уроки мультикультурализма от Брюсселя: ЕС строит новые центры размещения беженцев в Эстонии" posted on [stena.ee](http://stena.ee).

## Persona — Maxim Bernik, Maxim Lebedev

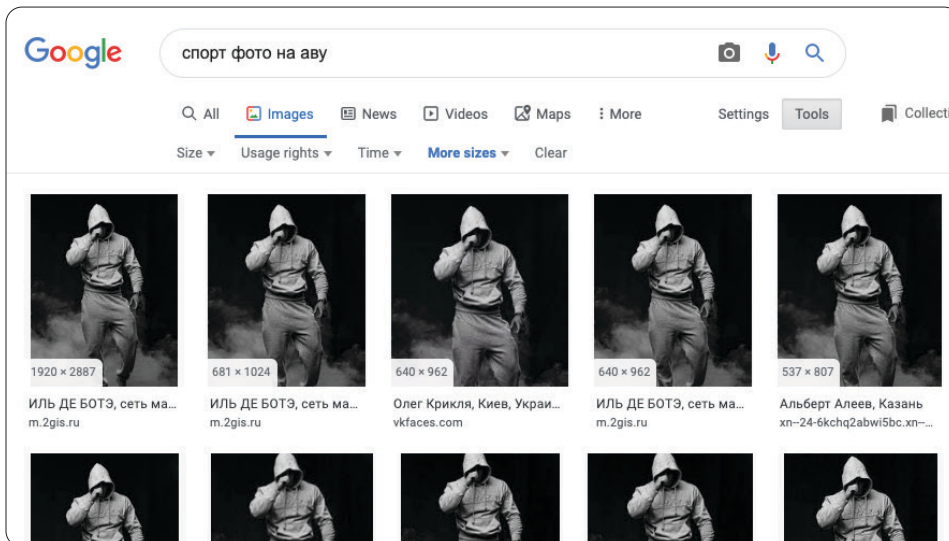
An exact text search of the title in Russian among open sources revealed another corresponding article, posted to the website [aftershock.news](http://aftershock.news) on December 17, 2019. This posting occurred a day before flokortig's post and nearly two weeks after the post by dimitriteras. The title of this article, published by the username "MaximLebedev," was "Европейская солидарность в действии: ЕС строит новые центры размещения мигрантов" (Translated: "European solidarity in action: EU builds new migrant accommodation centers in Estonia.") Like the version found on Stena, this article was particularly hostile toward Estonia and the migrant crisis. This article maintained a strong anti-Western and anti-migrant tone, and was written in a less formal editorial style. The article connects a newly formed "coalition of centrists, nationalists and rightists" with "the surge of radical moods in Estonian society directed against migrants." The story also brings into question Estonian leadership's



motivations, and whether they are acting for the good of the country, stating “Apparently, the desire to enjoy all the “benefits” of being in the EU among Estonian politicians is much stronger than the desire to protect their own interests and national identity.”

The screenshot shows the website 'AfterShock' (Информационный центр). The main article is titled 'Европейская солидарность в действии: ЕС строит новые центры размещения мигрантов в Эстонии' (European solidarity in action: EU builds new migrant centers in Estonia). The article text discusses the migration crisis, EU quotas, and the position of Baltic states. A sidebar on the left includes a login form with fields for 'Имя пользователя' (Username) and 'Пароль' (Password), and a 'Сериал «Учителя»' (Serial 'Teachers') recommendation.

Maxim Lebedev's post to aftershock.news.



Search of Maxim Lebedev's profile picture, which we have determined is a stock image. (Source: Google)

Insikt Group identified that the author behind the post, “Maxim Lebedev,” created a burner Reddit account, [u/MaximLebedev](#), like the aforementioned actor [u/flokortig](#), the day the post was made (the user references the article on the site [aftershock\[.\]news](#)). Unlike [u/flokortig](#), “MaximLebedev” targeted [r/politota](#), a subreddit dedicated to political news involving states of the former Soviet Bloc. Insikt Group believes that another account connected to “Maxim Lebedev,” [u/maksbern](#), registered on Reddit a week prior and targeted the Ukrainian subreddit [r/Ukraine](#). Despite the last names being different, Insikt Group believes that monikers “Max Bernik” and “Maxim Lebedev” are loose associations to the same person. Administrators of both subreddits removed the post, citing violations of subreddit rules.

↑ 1 ↓

Европейская солидарность в действии: ЕС строит новые центры размещения мигрантов в Эстонии  
[r/politota](#) · Posted by [u/MaximLebedev](#) 2 days ago

1 Comment Give Award Share ...

**Максим Лебедев**  
[u/MaximLebedev](#)

Karma 1 Cake day December 17, 2019

FOLLOW CHAT

MORE OPTIONS

OVERVIEW POSTS COMMENTS ...

sort NEW ▾

↑ 1 ↓

Европейская солидарность в действии: ЕС строит новые центры размещения мигрантов в Эстонии  
[r/ukraine](#) · Posted by [u/maksbern](#) 10 days ago

Comment Give Award Share Save Hide Report ...

**Максим Берник**  
[u/maksbern](#)

Karma 1 Cake day December 9, 2019

FOLLOW CHAT


MORE OPTIONS

Source profile and post history for [u/MaximLebedev](#) and [u/maksbern](#) on Reddit.

An exact text search of the title posted to Reddit identified approximately 20 additional blogging and self-publishing websites to which the article shared by u/maksbern and u/MaximLebedev had spread. Interestingly, in addition to various Russian-based websites, the article and corresponding document was widely spread among unverified Ukrainian and other CIS-based sources. We have provided these resources in **Appendix A**. We note that “Maxim Lebedev” used a number of different personas across several publishing websites, and there are inconsistencies in their profile data (such as locations of residence), which provided further indications that this activity was inauthentic.

### User information

- [All users](#)

Avatar: 

Nick: maksbern

First Name Last Name: Maxim Bernik

Registration Date: 12/09/2019


Floor: Boy

Country city: Ukraine, Dnipro

Birthday: 06/21/1977

Blog: [Maksbern blog](#)

USER: LEBEDEV MAXIMILIAN [MAXIMLEBEDEFF]



|                            |                                  |
|----------------------------|----------------------------------|
| <b>Registered :</b>        | 12/17/2019                       |
| <b>Gender ::</b>           | Male                             |
| <b>Age :</b>               | 35 - 40                          |
| <b>Birthday :</b>          | October 12th                     |
| <b>From :</b>              | Ukraine<br>Not defined (100.0%)  |
| <b>Social Status :</b>     | Employee                         |
| <b>Field of activity :</b> | Finance, insurance, securities - |

*Sample personae data among Maxim Bernik/Lebedev's blog accounts.*

## Persona — Vladimir Ivovich


Insikt Group found that this forged document was also shared on December 16, 2019 by a fifth actor, “vladimirivovich,” also known as “Vladimir Ivovich,” on the clearnet sites Transnistria Free Forum, [forum-pridnestrovie.info](#), and Transnistria Forum, [forum-pmr.net](#). Further investigation of this moniker revealed that account creation under the same moniker “Vladimir Ivovich” appeared on the Belarusian political blogging forum [BramaBY](#) the same day. However, this account only made one comment, on a blog titled “Why Belarusians are not Russian.”

This account included a photo that, when analyzed, linked to an additional blogging page on the CIS-facing site [Horde](#). We believe this is a legitimate photo, but do not know the origin of the photo. Based on the consistency and adherence to strict OPSEC across the campaign thus far we maintain that it is unlikely to be the authentic person behind Vladimir Ivovich. Based on account data, the user of this account wrote one post after its creation on December 16, 2019, though this post has since been deleted. The profile image also linked to an account using the same name on Kazakhstan-based blogging site [YVision](#), which also included a copy/paste of the article spread by “Maxim Lebedev.” One specific article copy, posted by “Vladimir Ivovich” on the site [dosug.md](#), provides a backlink to the original, but not defunct, article on stena[.]ee.

Главная    Комментарии (1)

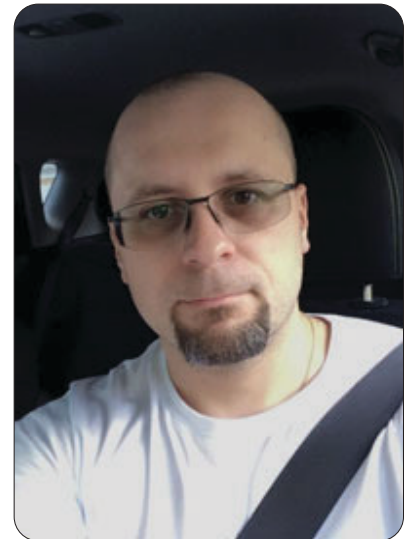
---

Беларусь → [Почему белорусы - не русские. \(49\)](#)

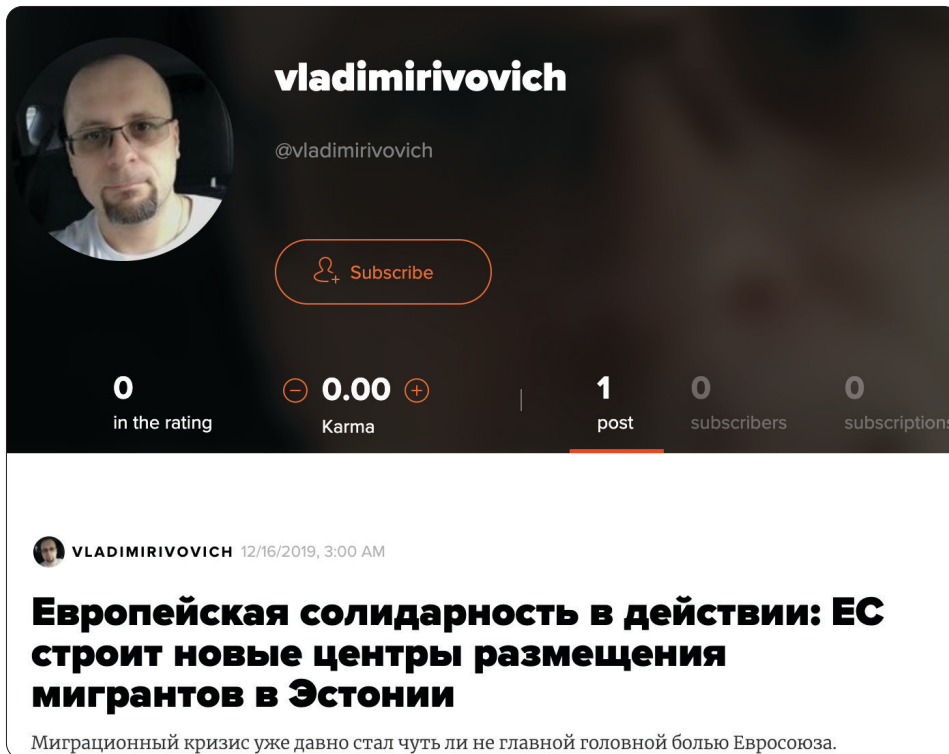


**vladimirivovich**  
16 декабря 2019, 10:45 -

Белорусы такие, белорусы сякие.  
Белорусы разные. Русские тоже разные.  
Неблагодарное занятие – навешивать ярлыки.



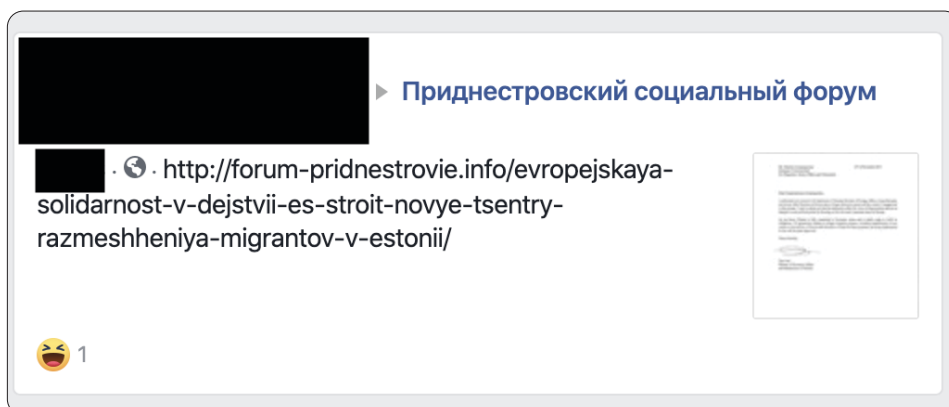
Vladimir Ivovich's lone comment on [BramaBY](#) and profile picture.



Profile picture of "Vladimir Ivovich." (Source: [YVision](#))

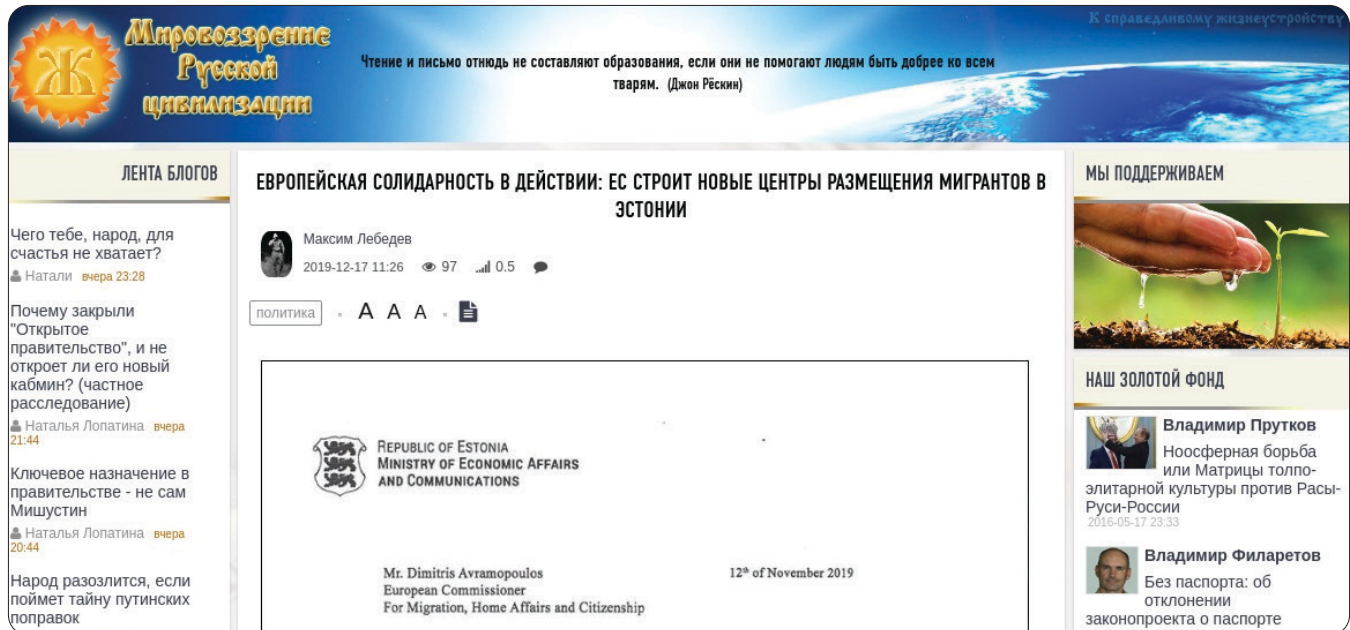
### Infiltration on Social Media

On December 16, 2019, Insikt Group found one Facebook account which shared the article from forum-pridnestrovie.info to the Facebook group Transnistrian Social Forum (Приднестровский социальный форум). This was the only time to our knowledge that this letter appeared on this social network.



A share of the article to Transnistria Free Forum on Facebook.

On the social media website VK, the footprint of this document was small and had little engagement. The most popular versions of the article were shared with four different links between December 16 and 18, 2019, via the following pro-Russian and CIS-facing blog sites and forums: [RNBee](#), [123ru](#), which was not previously observed before, [Razumei](#), and the aforementioned Transnistria Free Forum. In all, views of these links reached approximately 50 viewers.



Screenshot of the article posted on the pro-Russian blog site Razumei. According to the site, the site's purpose is to be "one of the centers for uniting and crystallizing the forces and ideas of Russian civilization."

Another translated copy of the Homment article was found on the Russian social media site VK, posted on December 20, 2019 by the page [geopoliticalinfo](#). However, this share reached less than 100 viewers on VK. This page linked the article posted to the Russian geopolitics news site [geo-politica.info](#), which provided a backlink to the instance found on Perevodika as its original source. This page reached over 350 viewers since December 19, 2019. Insikt Group found minimal engagement on the group's dedicated page on the Russian-based social media site Odnoklassniki ([ok.ru](#)).

## Discovery of Operation Pinball Targeting Georgia

Insikt Group concluded that our investigation of the campaign against the Estonian government and the EU was coordinated, deliberate activity. In the event of additional manifestations of this campaign, we continued to monitor these sources for instances of similar activity to include false documents, additional personas and potential spread of this disinformation on social media.

Within the past month, Insikt Group identified what we assess with high confidence is another developing campaign using similar TTPs as our initial observations regarding Operation Pinball. In particular, this campaign used another forged document targeting the Republic of Georgia and its growing relationship with NATO. This is the second time within the past four months, and the third time since July 2017, that Georgian leadership was [targeted](#) by information operations employing Secondary Infektion-esque TTPs. This is also the third instance of this specific information operation targeting NATO.


We note that at the time of publication, this campaign is likely ongoing, using similar self-publishing outlets, Reddit promotion, multilingual translation, as well as persistent use of burner personas that emphasize OPSEC over reaching a broad audience. Unlike our observations on the Estonian campaign, this campaign began on Reddit, with the use of a Reddit persona that has been “aged” to appear authentic by participating in other subreddits before planting a forged document. We believe this persona and activity are similar to those of the account “u/gregorator.” This persona was an active participant in [promoting](#) and distributing the leaked trade discussion documents pertaining to the U.K.’s National Health Service in late 2019. Thus far, Insikt Group has identified minimal social media engagement in this Georgia-focused operation.

These tactics distinctly overlap with documented Secondary Infektion information operations identified thus far. The discovery of additional instances of planted forged documents, in our view, further confirms our assessment of a deliberate campaign to undermine Western governmental bodies or political institutions.

## Threat Analysis

On Friday, January 10, 2020 a Reddit account, “u/TarielGeFr,” made a post to the subreddit r/france, in french, titled “[Un vrai rêve géorgien](#),” which translated states “A True Georgian Dream.” The post begins by stating that, while the author has lived in exile for a long period of time, they have closely paid attention to Georgian politics. Since Georgia’s recognition of sovereignty by the United States, the nation’s integration into NATO has become a strategic security priority for the state level and throughout the region.

↑  
3  
↓


 **r/france** · Posted by u/TarielGeFr 7 days ago


### Un vrai rêve géorgien

Vivant en exil pendant longtemps, elle a toujours suivi de près l'évolution de la situation politique dans sa Géorgie natale. Après que les États-Unis eurent reconnu la souveraineté de la Géorgie en 1992, il devint évident que la politique étrangère devait être davantage orientée vers l'Occident, plus précisément vers les pays démocratiques où le niveau de vie et le développement économique étaient élevés. C'est la raison pour laquelle l'une des tâches vitales et stratégiques de Tbilissi est l'intégration à l'OTAN, ce qui garantira la sécurité non seulement de la république, mais de toute la région. En peu de temps, la Géorgie a pu progresser de manière significative dans l'amélioration des normes de sécurité et dans le développement de la démocratie, prouvant ainsi à son partenaire à l'étranger qu'elle méritait de rejoindre l'Alliance de l'Atlantique Nord et que l'avenir de l'État était exclusivement lié à l'Occident. Mais le conflit territorial non résolu constitue un obstacle à une alliance avec l'OTAN.

Et si, jusqu'à récemment, le sujet de la reconnaissance de la souveraineté de l'Abkhazie et de l'Ossétie du Sud était fermé non seulement dans la société, mais également au niveau de l'État, le gouvernement corrige aujourd'hui sa position. En témoigne par exemple une publication dans le journal Chronika + intitulée "La Géorgie peut libérer l'Abkhazie" (<http://qronikaplus.ge/?p=18803&fbclid=IwAR2pCAO6MM9FYhy9GQ84KWU767YwQ90ouuRLPmhZ7c3h7YPS2EYL3ZpH3tM>), qui exprime avec audace la réponse longtemps demandée à la question de savoir quoi faire avec les républiques séparatistes. Je suis tout à fait d'accord avec l'opinion de la publication selon laquelle vous ne serez pas forcément gentil et il est temps de laisser partir ceux qui attachent de la valeur à leur indépendance imaginaire plus que la possibilité de vivre dans un pays vraiment libre.

Les dirigeants géorgiens ont apparemment trouvé un moyen de sortir de cette situation. Bien entendu, il ne faut pas s'attendre à des déclarations à haute voix dans un avenir proche sur la reconnaissance de la souveraineté des républiques autonomes, mais des étapes expérimentales dans cette direction seront prises. En témoigne une lettre de défense de Garibachvili au secrétaire général de l'OTAN, M. Stoltenberg.




 **r/france**

La France et les Français.

**317k**  
Abonnés

**1.5k**  
En ligne

---

 Created Mar 19, 2008

[JOIN](#)

---

**COMMUNITY OPTIONS** ▼

---

**r/france Rules**

1. Insulte ▼
2. Doublon (mettre le lien en commentaire) ▼
3. Spam ou contenu publicitaire ▼
4. Menace, appel au meurtre ou incitation au suicide ▼
5. Absence du flair paywall ▼

*u/TarielGeFr's post, "Un vrai rêve géorgien" on Reddit.*



The article discusses the issue of sovereignty for the disputed territories of Abkhazia and South Ossetia. The post claims that while the issue of sovereignty was “untouchable” before, it is now under review. This post includes a citation to an article published by the Georgian newspaper [Qronika+](#) (Chronicle+), which poses the suggestion that Georgia should “get rid of” Abkhazia. u/TarielGeFr stated that they agree with the newspaper’s view and claims that the Georgian government has come to a solution regarding Abkhazia’s sovereignty. The author states that while “loud statements” should not be expected about Abkhazia, the government is quietly planning “experimental steps” toward appeasing Abkhazia’s recognition for independence while managing admission to NATO, citing a letter dated November 29, 2019 — which Insikt Group concludes is forged — from Georgian Defense Minister Irakli Garibashvili to NATO General Secretary Jens Stoltenberg.

The phrase “loud statements” (громкие слова translated: loud words) is a common Russian phrase indicating a bold statement. Insikt Group assesses that this is most likely a direct translation from Russian to French but more accurately translated as a “bold statement” in English. This phrase hints that the author of this post, u/TarielGeFr, is a native Russian speaker.

The letter highlights an alleged upcoming sale of the Enguri hydroelectric dam (HES) to Abkhazia, serving to both remove an “obstacle” to the integration of Georgia into NATO, and as a flexible strategy for “progressive change of public opinion” towards granting Abkhazia and South Ossetia independence. Further, the letter states that Georgia is currently in negotiations with Turkey and other countries to provide supplemental electricity to the state “with the aim of enhancing the country’s energy security and its independence from [sic] NATO potential enemies. u/TarielGeFr suggests this may result in an electric rate increase, which is unlikely to be favorable among Georgians, but proposes that it may be worthwhile to ensure integration with NATO. In fact, the author suggests that full integration may encourage the disputed territories to come back into the fold as a united Georgian state, enticed by “a higher standard of living, including good education, quality care and other benefits Western progressive world.”

Currently, the only source of electricity in Abkhazia is HES, and is the only joint project in the Georgian-Abkhaz conflict zone.



საქართველოს თავდაცვის მინისტრად  
MINISTER OF DEFENSE OF GEORGIA

Tbilisi, 29 November, 2019

Your Excellency,

In the name of the Georgian leadership, I thank you for your support in integrating Georgia into NATO. We appreciate your confidence and will continue to work to justify it.

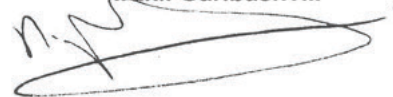
The Georgian leadership has worked on your proposals for removing obstacles to the gradual integration of Georgia into the Alliance. Solution of such main problems as resolving the territorial disputes with Abkhazia and South Ossetia through recognizing the independence of these occupied Georgian territories becomes difficult to implement in the foreseeable future because of unexpected socio-political implications of such a decision. That is why the government of Georgia has developed a more flexible strategy for progressive change of public opinion and attempts to mitigate the most urgent territorial problems. The strategy will help to meet the requirements for Georgia's entry into NATO.

In particular within the framework of the plan prepared by National Agency of State Property of Georgia, package of documents based on property rights on the objects of the Enguri hydroelectric power station (HES) within the occupied Georgian territory is being developed. Specifically, it is planned to handover them to Abkhazia for a symbolic amount of money. This will allow to organize the HES maintenance and to avoid possible provocations and energy blackmail in future.

Furthermore, agreements with Turkey and other countries are being prepared, which will change a common scheme of providing Georgia with electricity and will help to attract additional investment with the aim of enhancing the country's energy security and its independence from NATO potential enemies.

Respectfully yours,

Irakli Garibashvili



His Excellency Mr. Jens Stoltenberg  
Secretary General of NATO

01/55364

*Forged letter addressed to Mr. Jens Stoltenberg from Georgian Defense Minister Irakli Garibashvili. (Source: Reddit)*

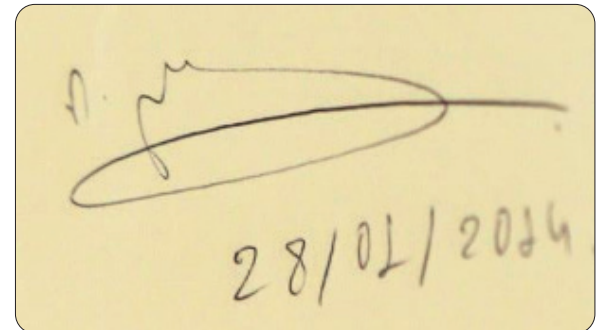
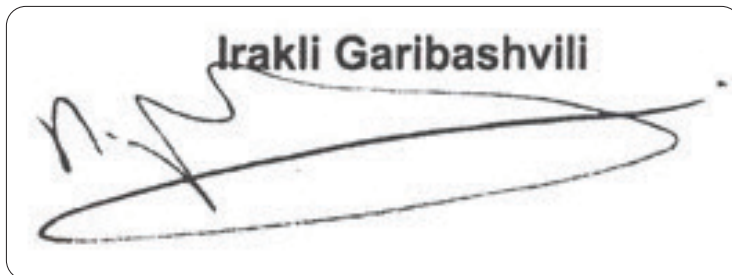
We believe that this letter between Georgian and NATO leadership contains significant indications of a forged document written by someone with a poor command of English as well as Georgian. Phrases in the document, such as “In the name of the Georgian leadership,” “handover them to Abkhazia,” and “NATO potential enemies” as examples are strong indicators of poor grammar and word usage that are unlikely to appear in official government correspondence. The phrase “handover them,” (передать их) demonstrates a direct translation from Russian, treated as a full verb followed immediately by an object. A fluent English speaker would phrase this as “hand them over.”

This letter, like our observations with the forged letter allegedly from Taavi Aas, continues to demonstrate a poor grasp of the use of indefinite and definite articles in the document. For example, “In the name of the Georgian leadership” should be, “In the name of Georgian leadership.” The statement in the third paragraph should also read “In particular, within the framework of the plan prepared by [the] National Agency of State Property of Georgia, [a] package...”

Another clue that indicates that a Russian speaker drafted this letter is the use of the word “objects” in the statement “package of documents based on property rights on the objects of the Enguri hydroelectric power station...” The term “object” (объект) is a Russian term with multiple meanings and intentions, and its use in this document does not indicate specifically what the original speaker was referring to. This form of lazy translation is another clue that the letter was likely a direct translation from Russian to English.

We assess with high confidence that the signature of Minister Irakli Garibashvili in the letter is another attempted forgery. In open sources, Insikt Group identified an image of Minister Garibashvili’s legitimate [signature](#) on his public-facing Facebook page, dated January 28, 2014 during an [official visit](#) to Israel while Garibashvili was Prime Minister of Georgia. Comparing the two signatures quickly highlights discrepancies in the style and flow of the signature presented in the letter, as well as the hesitation in attempting to recreate the signature.

The [signed book](#), which addresses Garibashvili's visit with former Israeli President Shimon Peres, also demonstrates that he has a fluent command of written English, and therefore we assess that he is highly unlikely to make the grammatical errors aforementioned.



*Comparing a verified signature of Irakli Garibashvili (right) to the forged document (left).*

Furthermore, in a translated post of u/TarielGeFr's post to the Georgian-facing subreddit r/Sakartvelo, commenters highlighted the header of the document, stating that "საქართველოს თავდაცვის მინისტრად" is incorrect, while "საქართველოს თავდაცვის სამინისტრო" is accurate.

The source of this document, appearing in French on r/france, is another indicator of inauthenticity, as the language in which the post is presented does not share any relationship with the subject matter. Previous Secondary Infektion information operations targeting the EU highlighted this discrepancy between post and forum languages and in our prior observations targeting Estonia. The author used two languages in both cases (German and English) to mask the original source of the material, as well as to help conceal the location of users who are injecting the documents into these sources.

u/TarielGeFr's activities on Reddit demonstrated very similar characteristics to those previously observed in the analysis of the Reddit profile u/gregoriator in the attempts to promote leaked documents discussing the future of the NHS before the December 12, 2019 U.K. elections. The handler of the account registered with Reddit on December 18, 2019, interestingly the same day as the aforementioned Reddit profile of u/flokortig within six hours according to account metadata.

Unlike u/flokortig, who registered on Reddit and immediately planted the forged document, u/TarielGeFr aged the account over the course of a month before planting the document. Insikt Group found that u/TarielGeFr was active on three subreddits: r/france, r/cars, and r/DragonballLegends, posting 32 comments in one month. u/TarielGeFr's first comment was approximately five minutes after registering on Reddit. According to Graphika's [report](#) which illustrates u/gregorator's activities, over the course of two years this account also frequented various subreddits over the span of the campaign against the NHS, such as r/worldpolitics, r/brexit, and r/dankmemes.

Native French-speaking Insikt Group analysts confirmed that this author is unlikely to be a native French speaker. u/TarielGeFr's posts and interests are primarily French but the account's comments show scattered use of the French language. For instance, one [comment](#) "Mais ma Maasdam de l'année dernière, qui est devenue Dorblu, sera-t-elle distinguée de l'original?" makes little grammatical sense and throughout the comment history, Insikt Group identified persistent grammatical errors. Furthermore, we believe that a native French speaker is also more likely to subscribe to additional French-language channels or other French subreddits for discussions other than just r/france.

We are also confident that u/TarielGeFr does not have a native command of English. By analyzing their posts, Insikt Group found that comments on r/cars and r/DragonballLegends were in English, but contained grammatical and stylistic errors, reminiscent of errors found in prior Secondary Infektion observations attributed back to suspected Russian speakers.

TarielGeFr commented on Why are there so many crossovers and SUVs in the market, yet only a tiny few offers manual transmission? · [r/cars](#) · Posted by u/i\_suckatjavascript

TarielGeFr 1 point · 1 month ago

At first, you choose a brand from your personal motives, be it design, an opinion on reliability, someone goes deeper and looks for unpretentious engines and transmissions. secondly, an automatic gear shift system is trite simpler and more convenient, it's the same as beating yourself in the chest now that a steam engine is better. It has long been established that fuel consumption due to the difference in the type of gearbox is negligible, and pays off in full comfort. due to traffic jams you do not need to constantly use the mixer. Well, the only plus in the mechanical gearbox is the dynamics. BUT, if you buy a crossover, what dynamics do you think?

Reply Share ...

TarielGeFr commented on As all-touchscreen interiors, and the increased reliance of software in cars grow, what is going to happen to the used car market in the future? · [r/cars](#) · Posted by u/markymark13

TarielGeFr 1 point · 1 month ago

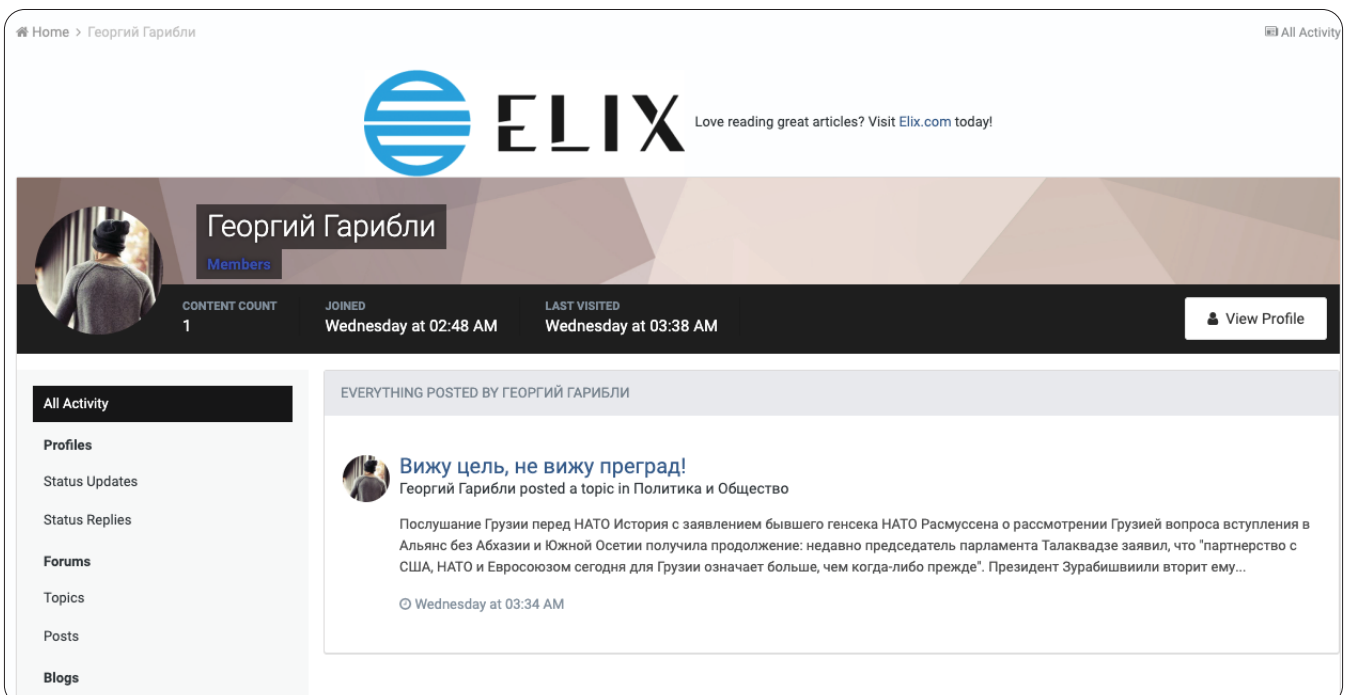
never mind. obsolete cars will live their lives, and new ones will put you on your knees and leave you without socks so that you can start your car due to the failure of a sensor. and there are fewer and fewer cars that drive pleasure from every trip, and there are instances that give modern cars a cheek, such as the Nissan GT-R BNR32 BNR33 BNR34, Toyota Supra A80 and other cars of this era, as well as American rare muscular cars

Reply Share ...


*u/TarielGeFr posting on r/cars in English.*

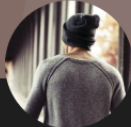
## Persona — George Garilbi

Insikt Group identified the first instances of amplification of the forged document on January 15, 2020, with posts appearing on the Russian-speaking forums [bakililarf.jaz](#) and [vardanank.org](#) (now removed) by an individual under the persona “George Garibli” (Георгий Гарибли) also known as “[garibliger](#).” The author titled the post “Вижу цель, не вижу преград!” translated to say “I see the goal, I see no obstacles!” with a subtitle saying “Georgia Obedience to NATO.”



Home > Георгий Гарибли All Activity

 Love reading great articles? Visit [Elix.com](#) today!

 **Георгий Гарибли**  
Members


| CONTENT COUNT | JOINED                | LAST VISITED          |
|---------------|-----------------------|-----------------------|
| 1             | Wednesday at 02:48 AM | Wednesday at 03:38 AM |

[View Profile](#)

**All Activity**

- Profiles
- Status Updates
- Status Replies
- Forums
- Topics
- Posts
- Blogs

EVERYTHING POSTED BY ГЕОРГИЙ ГАРИБЛИ

 **Вижу цель, не вижу преград!**  
Георгий Гарибли posted a topic in Политика и Общество

Послушание Грузии перед НАТО История с заявлением бывшего генсека НАТО Расмуссена о рассмотрении Грузией вопроса вступления в Альянс без Абхазии и Южной Осетии получила продолжение: недавно председатель парламента Талаквдзе заявил, что "партнерство с США, НАТО и Евросоюзом сегодня для Грузии означает больше, чем когда-либо прежде". Президент Зурабишвили вторит ему...

© Wednesday at 03:34 AM

*“George Garibli” on bakililarf.jaz Insikt Group confirmed that Garibli’s profile image is a [stock photo](#).*

The article shares similarities with the post made by u/TarielGeFr, though “George Garibli” wrote the article in an assertive, anti-NATO tone, rather than as an opinionated journal entry. Like the aforementioned post, this article brings up the ongoing challenges presented by Abkhazia and South Ossetia and Georgia’s admission into NATO. The article views NATO as a necessity in the eyes of Georgian leadership, stating that the issue at hand is “the fact that the main enemy and occupier is Russia, and the key to solving the problem and a panacea for all troubles is Georgia’s entry into NATO, which can protect and feed.”

The article continues to target the Georgian government, claiming that it is prioritizing NATO admission over its own people, stating the following:

*“...the forbidden topic of recognition of Abkhazia and South Ossetia is gradually becoming the subject of discussion. And even if the price of integration is too high and runs counter to state ideology, the ruling elite, as it turned out, is ready to sacrifice the interests of its own people in order to satisfy the demands of Western curators.”*

Further, “George Garibli” introduces Georgian leadership’s connection to the West in an attempt to further inflame the point, citing President Salome Zurbashvili’s French [citizenship](#), Prime Minister Giorgi Gakharia’s business dealings with [SFK Group and Lufthansa](#), and the fact that Defense Minister Garibashvili graduated from [Sorbonne University](#) in Paris.

The article suggests that Georgia is torn between NATO and the desires of the Georgian people and that the plan to sell HES to Abkhazia is an attempt to favorably sway public opinion and avoid mass protests, citing the aforementioned forged document as well as the opinion piece from Chronicle+, though this redirects to a copy of the op-ed posted on [abkhazeti.info](#).

Most interestingly, the forged document linked back to the original Reddit post by u/TarielGeFr, dated January 15, 2020. For each of the following instances in which we identified copies of this article and the forged document, the articles cite the Reddit post on r/france as the original source. This also aligns with prior observations in Secondary Infektion tradecraft.

Garibli reintroduces the prospect of purchasing electricity from Turkey, though he states that the inflated prices and subsequent tariffs will hurt low-class Georgians. The article ends by attempting to unnerve opinions of Georgian and NATO leadership by stating that “the Georgian elite, by hook or by crook aspiring to NATO, is ready to betray its own people, and in case of failure it will flee the country, leaving the ruined state to its fate.”

Further investigation of the article across open sources found a third post, dated January 15, 2020, on the forum [disput.az](https://disput.az) by “garibliger.” Though the post is an exact copy, the post was made as a reply in a forum thread titled “Georgian President wants to return South Ossetia and Abkhazia,” originally posted on August 27, 2019, and dormant since August 30, 2019. There is no evidence indicating that the author of the original thread had any involvement in this campaign, however, garibliger’s reply to the thread several months after the last post does indicate that this was a targeted reply.

Insikt Group found an additional five copies of the article on [dosug.md](https://dosug.md), [az-news.3dn.ru](https://az-news.3dn.ru) (links to a blog post on the Azerbaijani forum [baku.life.com](https://baku.life.com) which is not accessible), [forumpmr.org](https://forumpmr.org), [tradernet.ru](https://tradernet.ru), and [semey.city](https://semey.city) posted between January 17 and 20, 2020. In each of these five instances, the author was either “George Garibli” (two articles), “garibliger” (two articles), or a third moniker, “ggaribli” (one article), each time registering shortly before posting the article with the planted document, only to abandon the account afterward. In total, these pages reached approximately 2,500 views, the majority of which originated on tradernet.ru, a financial website with a self-publishing blog.



**dosug.md** Форум в разведке

**garibliger**  
ID: 1732, просмотров 39  
последнее посещение: 20 Января 2020 9:37

Фотогалерея (1) | Закладки (0) | Комментарии (0) | Новости (0) | Места развлечений (0) | Публикации (0) | Афиши (0) | Анекдоты (0) | Объявления (0) | Фильмы (0) | Форумы (0) | Свадьба (0)

Работа (0) | Опросы (0)

подарить подарок

Комментарии

20.01.2020 09:38 | Жизнь | 0 0 0 25

**Вижу цель, не вижу преград!**  
Послушание Грузии перед НАТО История с заявлением бывшего генсека НАТО Расмуссена о рассмотрении Грузией вопроса вступления в Альянс без Абхазии и Южной Осетии получила продолжение: недавно председатель парламента Талаквадзе заявил, что "партнерство с

**garibliger** 1.64 +0.60  
сила рейтинг

Информация

**О себе**  
Пока ничего не известно...

**Активность**  
Состоит в: [Геополитика](#)  
Зарегистрирован: 17 января 2020, 10:55  
Последний визит: 17 января 2020, 11:18

Sample persona data on "George Garibli" (garibliger) on dosug.md forumpmr[.]org.


Aside from these articles, Insikt Group discovered yet another instance of this article and forged letter on a Russian-speaking blog site, [mirtesen.ru](http://mirtesen.ru), on January 17, 2020 from a page titled “Беларусь и не только...” (Translated: “Belarus, and not just that...”) which publishes a blog and news articles from Russia, Eastern Europe and CIS states. Though this article is an [exact copy](#) of the others we discovered, this page did not have an author; however, the originator of the post did have two initials, “GG,” which we presume refers to the moniker “George Garibli.” The post also links back to the original Reddit post made by u/TarielGeFr. We also point out that the [forged letter](#) pertaining to Estonia was also posted on this blog page in December 2019.

Further investigation of this blog revealed that it is active with frequent posts on the Russian website [mirtesen.ru](http://mirtesen.ru), which [advertises itself](#) as “a media platform with thematic content from media, commercial brands, organizations and users, united in a social network.” It is unclear whether the account has any ties to Belarus, though the page likely accepts article submissions from all sources as another self-publishing medium. This blog in particular hosts articles found containing a myriad of similar letters and other documents previously unreported that Insikt Group deems suspect, dating back to [at least 2017](#).

### ***Persona — Andrey Vorozhko***

On January 22, 2020, Insikt Group observed a repost of George Garilbi’s article on [blog.i.ua](http://blog.i.ua). In this case, we identified a third persona under the username “avorojko,” who registered shortly before posting. An additional four articles were quickly posted to [berdpo.info](http://berdpo.info), [enmjigi.politiko.ua](http://enmjigi.politiko.ua), [times.com.ua](http://times.com.ua), and [korrespondent.net](http://korrespondent.net) under the moniker “Andrey Vorozhko.” This was the first time that we identified this moniker with the campaign. According to site-provided page metrics, these five pages reached approximately 1,700 views.

We assess with high confidence that “Andrey Vorozhko” is an inauthentic account, based on the quick registration of the accounts on these forums and self-publishers, and the posting of exact copies of George Garilbi’s article. Other indicators, such as the use of stock images as profile photos and the lack of profile data, also suggest that this is a one-off burner persona across multiple profiles.


 **avorojko**

### Вижу цель, не вижу преград!

22.01.20, 09:56 | [абхазия](#), [гарибашвили](#), [грузия](#), [ингурская гэс](#), [нато](#), [столтенберг](#)


Послушание Грузии перед НАТО

История с заявлением бывшего генсека НАТО Расмуссена о рассмотрении Грузией вопроса вступления в Альянс без Абхазии и Южной Осетии получила продолжение: недавно председатель парламента Талаквдзе заявил, что "партнерство с США, НАТО и Евросоюзом сегодня для Грузии означает больше, чем когда-либо прежде". Президент Зурабишвили вторит ему


 **АНДРЕЙ ВОРОЖКО**  
УКРАИНА,  
О СЕБЕ ▾

|               |               |
|---------------|---------------|
| День рождения | 14 МАРТА 1988 |
| Пол           | Мужской       |

**ВСЕ АКТИВНОСТИ** Я-КОР

 Андрей Ворожко добавил новую публикацию 22 января 2020, 10:22  
**Вижу цель, не вижу преград!**

### Профиль

 **avorojko**

Украина, Киев

Родился: [14.03.1988](#)

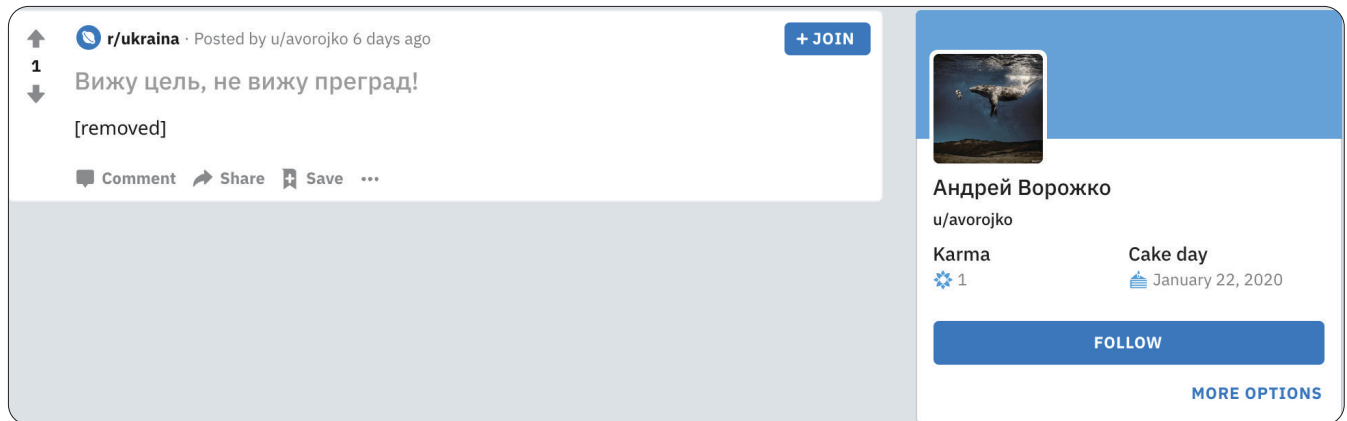
**31 год**, [рыбы](#)

Sample persona data for Andrey Vorozhko.

Insikt Group also discovered that avorojko maintained a LiveJournal, from which the account published a copy of this article and letter on January 21, 2020. A LiveJournal [aggregator](#) picked up the link to the LiveJournal post, though there was no further engagement with the associated tweet.

Between January 22 and 23, 2020, “Andrey Vorozhko” (“avorojko”) heavily increased the spread of the article and forged letter, spanning an additional seven websites, all identified as Ukrainian blog pages or self-publishing websites. Exact metrics on page views and total interaction is potentially subject to change, but at this time we approximate that these additional single-use accounts managed to reach at most 300 views. The full list of these sites is provided in a table, located in **Appendix B**.

Insikt Group identified avorojko, under the username u/avorojko, attempting to spread the post “Вижу цель, не вижу преград!” on the subreddit [r/ukraina](#), on January 22, 2020. Subreddit moderators shortly thereafter removed the account’s post, making this the account’s only activity approximately 20 minutes after registering.



*u/avorojko's post to r/ukraine, removed from the subreddit shortly after posting.*

After January 23, 2020, mentions of this article ended. We do not know whether the operation was abandoned, or has gone dormant to prevent detection. To our knowledge, the claims presented in the article and letter have not reached mainstream sources in Georgia or abroad.

The status of this operation, in addition to others that share its TTPs, is unclear, though Insikt Group believes that it is likely that we will identify emerging cases of Operation Pinball in the future. It is evident that the operators behind this campaign take a keen interest in the affairs of Eastern European and CIS geopolitics, and desire to use false information to instill a sense of division, distrust, and doubt among European and democratic institutions such as NATO and the EU.

Each of these two campaigns closely shared similar TTPs like the following:

- A forged letter as the focus of attention of an obscure blog post
- Current, controversial geopolitical events in Europe as a backdrop of the forged letter
- Wide-ranging attempts to promote the letter on multiple self-publishing websites, forums, and blogging pages via at least one false persona
- Translation to at least one additional European language
- At least one attempt to infiltrate mainstream sources through Reddit

When investigating historic evidence of prior campaigns using these TTPs, not only did Insikt Group identify [fragments](#) of prior campaigns [connected](#) to Operation Secondary Infektion, but additional, previously undiscovered instances of forged correspondence that shared many of the same TTPs with Operation Pinball. Unlike the findings regarding Estonia and Georgia, these cases of forgeries emulated correspondence between U.S. officials, as well as among U.S. officials, national and international political organizations, and international policymakers.

### ***Operation Pinball's Implications for US-Targeted Disinformation and the 2020 Election Cycle***

Insikt Group assesses it is unlikely that barriers exist to prevent the actors behind these campaigns from engaging in similar tactics to attempt to discredit or otherwise target U.S. politicians running for office in 2020, undermine confidence in federal, state, and local government, or to further exploit divisive social issues.

In our investigation of these targeted operations against Estonia and Georgia, we uncovered a blog account reposting many of the aforementioned examples of this influence campaign over the past year — the aforementioned blog “Беларусь и не только...” (Translated: “Belarus, and not just that...”) active on the Russian blogging site mirtesen[.]ru.

Among these blog posts, Insikt Group found six notable examples of correspondence (five letters and one email) containing, in our view, likely confidential correspondence on sensitive international developments in Eastern Europe. This correspondence emulated discussions between U.S. officials, U.S. officials and grassroots political organizations, and U.S. officials and international organizations and policymakers.

Recorded Future assesses with high confidence that the following letters are inauthentic. At the very least, basic indicators (such as grammatical errors, spelling, and document formatting) for government-level material are present and some of the correspondence contained within would likely be considered at least For Official Use Only (FOUO).

Recorded Future could not independently verify whether these letters are legitimate:

- A [letter](#) from U.S. Senator Benjamin Cardin to fellow U.S. Senator Bob Menendez, dated June 13, 2019, encouraging support to Russian opposition leader Alexi Navalny, stating that “Navalny has every chance to encourage people in Russia to overthrow the government.”
  - Indicators of inauthenticity: spelling, grammar, style (such as awkward phrases, tone, difficulty with proper tense, politically charged language).
- A [letter](#) from U.S. Secretary of State Mike Pompeo to then-Chairman of the Democratic Party of Moldova, Vlad Plahotniuc, dated June 10, 2019, reiterating support for the “legitimate” government of Moldova rather than the coalition run by then-Prime Minister Maia Sandu.
  - Indicators of inauthenticity: spelling, grammar, style (such as awkward phrases, tone, difficulty with proper tense, politically charged language).
- A [letter](#) from Polish politician Jarosław Kaczyński to U.S. Admiral James G. Foggo III, dated January 15, 2019, on Poland’s intentions to construct a canal through the Vistula Spit as part of an economic balance to “Russian aggression.” The letter also makes a claim that the Vistula Spit will be funded in part by the U.S. through its military budget.
  - Indicators of inauthenticity: internal inconsistency (such as use of “U.S.,” “USA,” and “U.S.” interchangeably), spelling, grammar, style (such as awkward phrases, tone, rapid call to action).
- A [letter](#) to then-U.S. Ambassador to Ukraine Kurt Volker from Satu Kähkönen, then-Regional Director for Belarus, Moldova, and Ukraine at the World Bank, dated April 4, 2019, requesting that the U.S. support Minister of Internal Affairs of Ukraine Arsen Avakov’s nomination for the post of Prime Minister of Ukraine over Yulia Tymoshenko.

- Indicators of inauthenticity: Spelling of author's name (lack of umlauts), grammar, style (such as awkward phrases, tone). Recorded Future assesses that The World Bank is unlikely to produce this type of document as it likely does not align with the organization's policy objectives.
- An [email](#) addressed to U.S. Secretary of State Mike Pompeo from Raffi Hamparian, raffi.hamparian@gmail[.]com, Chairman of the Armenian National Committee of America, dated April 18, 2019, regarding UN recognition of the Armenian genocide of 1915-1917, and alleged U.S. economic support of \$80 million.
  - Indicators of inauthenticity: Official political figures would not be using a Gmail account to communicate with Secretary Pompeo (in this case Chairman Hamparian would use an anca[.]jorg email domain), spelling and poor command of English (Raffi Hamparian is a native U.S. citizen), grammar, style (such as awkward phrases, informal tone, politically charged language), Recorded Future also notes that [UN Resolution 2467](#) is not this document.
- A [letter](#) addressed to U.S. Senators Bob Corker and Bob Menendez from Aram Khamparyan, Executive Director of the Armenian National Committee of America, requesting the U.S. Senate to consider increasing duties on Turkish steel and aluminum, imposing sanctions against Minister of Justice Abdulhamit Gul and Interior Minister Suleyman Soyly, and pausing the extradition of Fethullah Gulen. The letter also alluded to the hope that the U.S. would help influence the results of the then-upcoming Turkish municipal elections scheduled for March 2019.
  - Indicators of inauthenticity: Grammar, poor command of English (Aram Hamparian is a native U.S. citizen), style, (such as awkward phrases, tone, the unusual subject matter pertaining to U.S. military operations in Syria, and Turkish procurement of Patriot missiles/PAC-3 missile interceptors).

Many of these inauthentic documents are historic in nature and, at least to our knowledge, this is the first time this account has been identified as engaging in this activity. We are unable to determine the actual impact of this campaign at this time but will continue to conduct further research and analysis. Recorded Future has provided copies of the correspondence documents included in **Appendix C**.

Should these actors target the U.S. with an influence campaign in 2020 using Operation Pinball tactics, we believe the following TTPs would be leveraged:

- Creation of false stories on self-publishing pages both located within the U.S. and abroad (such as on Wordpress blogs, LiveJournal, and other similar sites, namely Ukrainian blogging websites).
- Promotion of content on local community forums and pages, including Facebook.
- Promotion on low- and high-visibility U.S. political forums (such as the subreddits r/politics and r/The\_Donald) using various burner accounts.
- Divulging information on known sources where disinformation thrives, such as 4chan.
- Possibly, the use of “aged” social media and forum accounts, not previously isolated as a promoter of disinformation, to push these false narratives. The use of such accounts, however, would indicate a shift in Secondary Infektion’s TTPs from what we have observed to date.
- In addition, as witnessed with the [WADA case](#) and more recently with the [NHS](#), these actors may also attempt to spread false documents via emails to journalists and news publications.



## Outlook

These operations targeting Estonia, Georgia, the EU, and NATO follow similar patterns of activity documented in connection to historic personas constructed by the GRU. According to [reporting](#) by Stanford University's Internet Observatory Cyber Policy Center, "[GRU] Pages were created and run within a distinctly short time frame, often with frenetic posting patterns. They were spun up in response to a geopolitical event or provocation — including to serve as a public drop for hacked materials." However, unlike hack-and-leak operations, there is no reported evidence indicating that these were leaked documents from breached sources, such as the most recently publicized Secondary Infektion operations targeting the UK's National Health Service.

We are confident that this is a deliberate, coordinated, and methodical operation to undermine relationships among political figures and democratic institutions across Europe perpetrated by actors with a strong command of the Russian language. These operational aims and tactics align with the disinformation arm of the Russian political warfare policy of "активные мероприятия" (Translated: "active measures"), and the tactics are strongly reminiscent of historic activities of Russian security services. This report, however, does not link these activities to the GRU or any other Russian intelligence service because we have insufficient information on the actors or any connections to the Russian intelligence services.

To date, institutions in North America and Europe were the subjects of this activity and are likely to remain targets in the future. Though we have not identified specific cases of Operation Pinball targeting the U.S. 2020 election process, we believe that the operatives behind this information operation are likely capable of doing so. They have consistently demonstrated the ability to craft forged documents and quickly disperse them over a variety of sources in a clearly organized manner.

For influence campaigns, operational success remains an ill-defined goal. Some metrics of success likely include views, reposts, engagement numbers, propagation of the message or story, presence in “mainstream” media, and ultimately manipulating the opinions of viewers. However, many of these goals are hard to measure. From our perspective, Operational Pinball actors would need to improve the fluency of their fraudulent and inauthentic communications and build networks of older and more trusted personas to conduct a successful influence campaign in the U.S. Inadequate fluency in target language and over reliance on known inauthentic influence tactics will likely hinder Operation Pinball actor’s ability to penetrate mainstream U.S. media.

In the lone case in which these tactics achieved success — in the U.K. regarding the NHS — we believe it was simply a matter of being in the right place, at the right time, with a particularly divisive topic in the heart of an election cycle. Well-crafted false documents and letters planted on Reddit, social media, and self-publishing sites (like Medium or WordPress) which attempt to emulate correspondence between U.S. political figures remains a significant possibility, and, if successful, could have wide-ranging consequences for the U.S. elections. We believe it is possible that actors could leverage Operation Pinball tactics against U.S. political figures this year.

## Mitigations

Though preventing these tactics is difficult, the impact of this information operation can be mitigated using a whole-of-community approach, including the following steps:

- Sites and additional pages that are likely to be exploited by these operatives should be continually monitored.
- Administrators should quickly isolate and remove this content once it is identified and confirmed.
- Targets of these operations, such as politicians who are impersonated, should be made aware of these operations and [publicly highlight](#) the inaccuracies and falsehoods of forged letters for further public assurance.
- Affected organizations and individuals must foster greater public awareness of blatantly false claims and the key indicators to identify forged materials.

## Appendix A — Personas of Maxim Bernik/Lebedev

| Date     | Domain  | Author                                    |
|----------|---|---|
| 12.9.19  | <a href="http://slavutich.cn.ua">slavutich.cn.ua</a>  | <i>maksbern</i>                           |
| 12.9.19  | <a href="http://blog.i.ua">blog.i.ua</a>  | <i>maksbern</i>                           |
| 12.9.19  | <a href="http://korrespondent.net">korrespondent.net</a>  | <i>Maxim Bernik (Максим Берник)</i>       |
| 12.9.19  | <a href="http://berdpo.info">berdpo.info</a>  | <i>Maxim (Максим)</i>                     |
| 12.9.19  | <a href="http://politiko.ua">politiko.ua</a>  | <i>Maxim Bernik</i>                       |
| 12.10.19 | <a href="http://1.zt.ua">1.zt.ua</a>  | <i>Maxim Bernik</i>                       |
| 12.10.19 | <a href="http://kaniv.net">kaniv.net</a>  | <i>Maksbern</i>                           |
| 12.10.19 | <a href="http://ua-politics.livejournal.com">ua-politics.livejournal.com</a>                        | <i>maksbern</i>                           |
| 12.10.19 | <a href="http://ua-nazionalism.livejournal.com">ua-nazionalism.livejournal.com</a>                  | <i>maksbern</i>                           |
| 12.10.19 | <a href="http://uaznaypravdu.livejournal.com">uaznaypravdu.livejournal.com</a>                      | <i>maksbern</i>                           |
| 12.10.19 | <a href="http://ua-1.livejournal.com">ua-1.livejournal.com</a>                                      | <i>maksbern</i>                           |
| 12.17.19 | <a href="http://news2.ru">news2.ru</a>  | <i>MaximLebedev</i>                       |
| 12.17.19 | <a href="http://glav.su">glav.su</a>  | <i>Maxim Lebedev</i>                      |
| 12.17.19 | <a href="http://razumei.ru">razumei.ru</a>  | <i>Maxim Lebedev</i>                      |
| 12.17.19 | <a href="http://liveukraine.su">liveukraine.su</a> (suspended site)                                 | <i>maksbern</i>                           |
| 12.18.19 | <a href="http://worldcrisis.ru">worldcrisis.ru</a>  | <i>Maximilian Lebedev (maximlebedeff)</i> |
| 12.18.19 | <a href="http://ru-politic.livejournal.com">ru-politic.livejournal.com</a> (suspended)              | <i>maximlebedeff</i>                      |
| 12.18.19 | <a href="http://currentpolitics.livejournal.com">currentpolitics.livejournal.com</a><br>(suspended) | <i>maximlebedeff</i>                      |
| 12.18.19 | <a href="http://rnbee.net">rnbee.net</a>  | <i>MaximLebedev</i>                       |

## Appendix B — Personas of Andrey Vorozhko

| Date    | Domain   | Author                 |
|---------|--|------------------------|
| 1.21.20 | <a href="http://ua-politics.livejournal.com">ua-politics.livejournal.com</a>   | <i>avorojko</i>        |
| 1.22.20 | <a href="http://gorod.dp.ua">gorod.dp.ua</a>                                   | <i>avorojko</i>        |
| 1.22.20 | <a href="http://kaniv.net">kaniv.net</a><br>(deleted)                          | <i>avorojko</i>        |
| 1.22.20 | <a href="http://siver.com.ua">siver.com.ua</a><br>(deleted, profile available) | <i>avorojko</i>        |
| 1.22.20 | <a href="http://blog.meta.ua">blog.meta.ua</a>                                 | <i>avorojko</i>        |
| 1.22.20 | <a href="http://slavutich.cn.ua">slavutich.cn.ua</a>                           | <i>avorojko</i>        |
| 1.22.20 | <a href="http://sluhi.com.ua">sluhi.com.ua</a><br>(unavailable site down)      | <i>avorojko</i>        |
| 1.22.20 | <a href="http://1.zt.ua">1.zt.ua</a>   | <i>Andrey Vorozhko</i> |

## Appendix C — U.S.-Specific Forged Letters

BENJAMIN L. CARDIN  
UNITED STATES SENATOR  
MARYLAND

United States Senate  
Washington, DC 20510-2004

June 13, 2019

The Honorable Robert Menendez  
United States Senate  
Washington, DC 20510

Dear Senator Menendez:

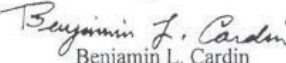
Events which have taken place over the past few months in Russia, and particularly intense protests sparked by the unlawful arrest of Ivan Golunov, an independent investigative journalist, confirm that the Russian civil society is ready to stand up to the oppressive system. Mr. Golunov's release from prison following people's outcry is an unprecedented success that should be capitalized on by any means available. The crucial point now is to maintain the momentum, otherwise the Russian government will again be able to recover with minimum losses. Basically, Mr. Golunov's arrest is a stroke of true luck and we must not lose the perfect opportunity. I suggest that the issues of increasing the funding of and widening the cooperation with the Russian opposition be considered without delay.

I believe we should pay special attention to Alexei Navalny. His investigations into the abuse of power by Russia's law enforcement agencies must form the basis of the Russian protest. Mr. Navalny has had both successes and failures over the previous years, yet as the example of Ivan Golunov shows – the most effective way to fight Putin's regime today is to organize those Russians who are angry about infringement on their rights. Given the necessary level of our support, Mr. Navalny has every chance to encourage people in Russia to overthrow the government.

And again, the most important thing for us now is to use every opportunity not to let Putin recover from that defeat. The fate of democracy in Russia depends on how fast we can react to the developments.

I hope you share my views and will ensure that the issue is laid before the Committee as soon as possible.

Sincerely,

  
Benjamin L. Cardin  
United States Senator

Reply To:

509 Hart Senate Office Building  
Washington, DC 20510-2004  
(202) 224-4524  
www.cardin.senate.gov

Printed on  
Recycled Paper

Reply To:

Tower 1 Suite 1710  
100 S. Charles Street  
Baltimore, MD 21201  
(410) 962-4436

[Letter](#) from U.S. Senator Benjamin Cardin to fellow U.S. Senator Bob Menendez, dated June 13, 2019.

THE SECRETARY OF STATE  
WASHINGTON

June 10, 2019

Vladimir Plahotniuc  
President  
Democratic Party of Moldova  
44/3 Armeneasca st.  
Chisinau  
Republic of Moldova

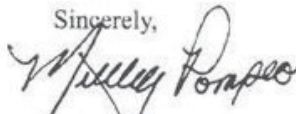
Dear Mr. Plahotniuc,

In this time of political crisis that your country is going through, I would like to reiterate that the U.S. Government and the Department of State continue to support the Democratic Party of Moldova under your leadership. We absolutely share your views that the new government of Moldova have placed themselves above the law, committed a coup d'état and usurped power in your country. We consider the actions of Maia Sandu, who has been unconstitutionally appointed Prime Minister, to be worthy of condemnation. She has disgraced herself in the eyes of international partners by forming an alliance with the relieved of duties President Igor Dodon's supporters who jeopardize Moldova's nationhood. We believe that by defying the Constitutional Court of Moldova, the new government have offset the balance of power in the country, have done irreparable harm to the development of democracy and have undermined the reputation of Moldova around the world.

The U.S. Department of State supports the citizens of Moldova in their intention to exercise the right to vote during the snap parliamentary election in September. The people of Moldova have taken to the streets to protest against the illegitimate actions of the government headed by Maia Sandu, because they have an inalienable right to freely choose the future for their country.

We appreciate your efforts against the self-proclaimed authorities, your determination to resolve the crisis and your devotion to the principles of democracy. I assure you of our support and assistance during the upcoming parliamentary and presidential elections in Moldova. We believe the Democratic Party of Moldova to be the only political power in your country which has the potential to overcome the situation now and ensure your nation's successful democratic, social and economic development afterwards.

Sincerely,



Michael Pompeo

*Letter from U.S. Secretary of State Mike Pompeo to Chairman of the Democratic Party of Moldova, Vlad Plahotniuc, dated June 10, 2019.*

*Jarosław Kaczyński*  
Prezes



Warsaw, 15 January, 2019

**Admiral James G. Foggo III**  
**Commander**  
**Allied Joint Force Command Naples**  
**U.S. Naval Forces Europe**  
**U.S. Naval Forces Africa**

Dear Mr. Foggo,

I am most grateful for your full support and assistance in addressing issues related to security of our country.

However, to sustain further development of real democracy in Poland standing on the front line of confrontation with Russia, to ensure Poland's independence and security from the threat of Russian militarism, it is necessary to intensify joint work and actually demonstrate the continuity of your orientation towards the growing relevance of Poland for security of the entire Europe.

Despite the lack of understanding of the issue in most European countries there is need for further work on isolating Russia in order to develop cooperation between Washington and Warsaw, which aims at promoting vital interests of the whole Europe and advances by current US administration and NATO leadership. Without it, our very existence could be put at risk.

That is why, in the shortest possible time, it is necessary to start construction of a ship canal across the Vistula Spit, which will permit to trade through the Polish port of Elbląg, avoiding transit through Russia. It will facilitate military cooperation between Poland and the USA in security-related matters. Poland, with sufficient military, political and financial support from the USA, is determined to offer vigorous resistance to the growing threat of Russian aggression and expansion. This issue has been repeatedly raised in the bilateral contacts between our countries at various levels, which resulted in complete mutual understanding.


The Law and Justice party greatly appreciates the moral and material support that the USA has already offered to Poland, but it is not enough. Because of vacancy of intellection in some political circles of Poland, the project to construct a ship canal across the Vistula Spit is

not yet realized although it was at the one-yard line as early as 2016. However, problems, which weighed against successful construction of the ship canal, were practically resolved. And political opposition led by former Prime Minister of Poland Beata Szydło, who greatly resisted the construction under pressure from ecologists, no longer has genuine influence over the implementation of the project.

To date, a professional team has been formed in Poland. And it is prepared to act in the interests of own country. But such grandiose project as construction of a ship canal across the Vistula Spit requires dramatic levels of investment. Poland is unable to execute it without external funding. In view of the fact that construction of a canal offers benefits to both Warsaw and Washington, we look forward to your cooperation in increasing funding for the project from the US military budget.

I hope that mutually beneficial cooperation between our countries will continue and together we can achieve our intended objectives.

Respectfully yours,



Jarosław Kaczyński

*Letter from Polish politician Jarosław Kaczyński to U.S. Admiral James G. Foggo III, dated January 15, 2019.*

*Page 2 of 2.*

The World Bank  
INTERNATIONAL BANK FOR RECONSTRUCTION AND DEVELOPMENT  
INTERNATIONAL DEVELOPMENT ASSOCIATION  
REGIONAL OFFICE  
UKRAINE, BELARUS AND MOLDOVA

1, Dniprovskiy Uzviz  
Kyiv 01010  
Ukraine

(380-44)490-6671  
(380-44)490-6672  
(380-44)490-6673

April, 4, 2019

Kurt Volker,  
the US Special Representative for Ukraine  
Washington, DC

Dear Mr. Volker,

I'm writing to you to express my appreciation for your overwhelming support given to Ukraine in its struggle for the triumph of democracy. The current elections have fully met our expectations. According to sociological surveys of Ukraine's electoral preferences Mr. Zelensky can pretend to be elected to the post of President of Ukraine in the second round of elections. In this case, we will have a real chance to implement a plan for changing the state structure of Ukraine by establishing a parliamentary republic. As far as we know, Mr. Zelensky is willing to go for it. In this regard, I am pleased to inform you that all previous agreements with Minister of Internal Affairs of Ukraine Avakov to nominate him for the post of Prime Minister of Ukraine are still in force. In order to achieve the above goals, we look forward to your assistance in supporting Mr. Avakov. Obviously, if the plan is fulfilled, we will have a good ally for solving problems in the democratic environment of Ukraine, as well as, a stable economic partner, who would be useful for guaranteed recovery of funds provided by international structures.

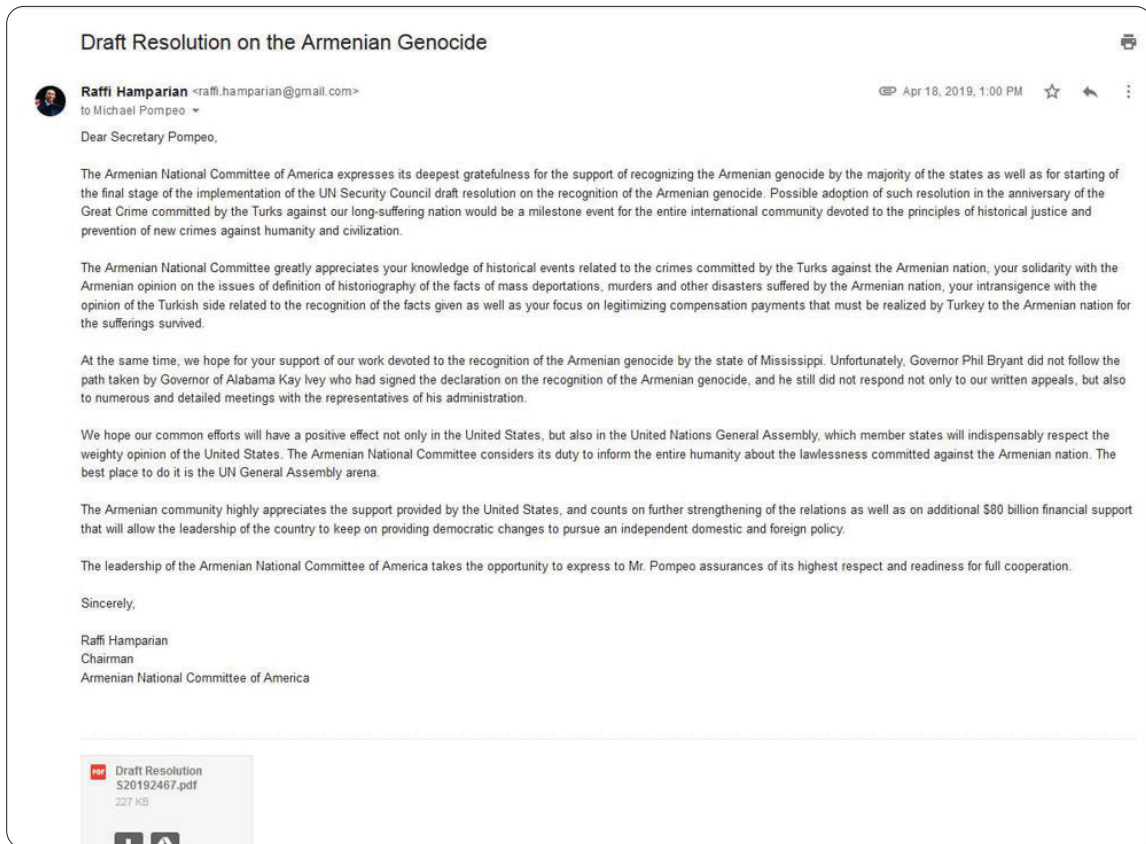
Moreover, as we have heard, Mrs. Tymoshenko also pretends to be elected to the post of the Prime Minister of Ukraine. We do not have any arrangements with her on these issues, and that is why in order to avoid any negative consequences, we ask you to minimize her chances to be involved in the formation of the Government of Ukraine.



Satu Kahkonen,  
World Bank Country Director for  
Belarus, Moldova, and Ukraine

*Letter from the World Bank Regional Director for Belarus, Moldova and Ukraine at the World Bank, Satu Kähkönen, to then-U.S. Ambassador to Ukraine, Kurt Volker.*





An [email](mailto:raffi.hamparian@gmail.com) addressed to U.S. Secretary of State Mike Pompeo from Raffi Hamparian, raffi.hamparian@gmail.com, Chairman of the Armenian National Committee of America.

United Nations

S/2019/2467

**Security Council**Provisional  
18 April 2019

Original: English

---

**Recognition of genocide against the Armenians, ethnic and religious discrimination including displacement of civilian population in conditions leading to imminent death committed by the Turks in 1915-1923: draft resolution***The Security Council,*

*Guided* by the Charter of the United Nations, the Universal Declaration of Human Rights, the International Covenant on Civil and political Rights (Resolutions of the General Assembly A/RES/3/217 A (1948) and A/RES/21/2200 (1966)), and other relevant documents on human rights,

*Recalling* the United Nations General Assembly resolutions on Prevention and Punishment of the Crime of Genocide, and on the Non-Applicability of Statutory Limitations of War Crimes and Crimes Against Humanity, in particular resolutions A/RES/3/260 (1948) and A/RES/2391 (1968),

*Acknowledging* other important initiatives of the United Nations General Assembly aimed at promoting the principles of historical justice, and raising awareness of the suffering of victims of ethnical and religious discrimination, xenophobia and related intolerance and discrimination in different forms, in particular regarding commemoration of the victims of genocide, deportation, and medical experiments on representatives of the Armenian nation,

*Expressing* grave concern with the negation of the Turkish government to recognize the fact of ethnical and religious crimes committed by the Turks from 1915 to 1923,

*Stressing* that the responsibility for the ethnic and religious crimes against the Armenians in 1915-1923 must be taken by the current government of Turkey,

*Expressing* serious concern with both domestic and foreign policy lead by the Turkish leadership under the influence of extremist organizations,

*Having studied* documental evidence of the crimes and the facts of both ethnical and religious discrimination against the Armenians in 1915-1923 by the Turkish authorities,

*Stating* a deep concern with an alarming growth of the number of discrimination and intolerance cases related to the Armenian population of Turkey, motivated by prejudice against people of other ethnic origins, confessions, and notions,

*Acting under* Chapter VII of the Charter of the United Nations,

1. *Recognizes* the ethnic and religious crimes committed by the Turkish authorities against the Armenians in 1915-1923 as genocide, and recommends those member states that haven't done it yet to consider it, including the Turkish government,

19-06280 (E)

Attached [draft](#) resolution included in the aforementioned email to Secretary Pompeo.  
Page 1 of 2.

S/2019/2467

---

2. *Recommends* the Turkish government to bring its official apology for the crimes against the Armenian nation in 1915-1923 for edification of the crimes committed against both humanity and civilization, and to avoid repeating them, including against other nations living in the country,

3. *Strongly urges* the government of Turkey to do its best to atone for the guilt of the Turkish nation before the Armenians for genocide,

4. *Demands* to consider the issue on the paying financial compensations to the descendants of the victims of genocide, and to agree both the payouts and the terms with the Armenian side,

5. *Decisively condemns* the incidents related to glorification and propaganda of ethnic and religious discrimination of the Armenians and other nations living in Turkey,

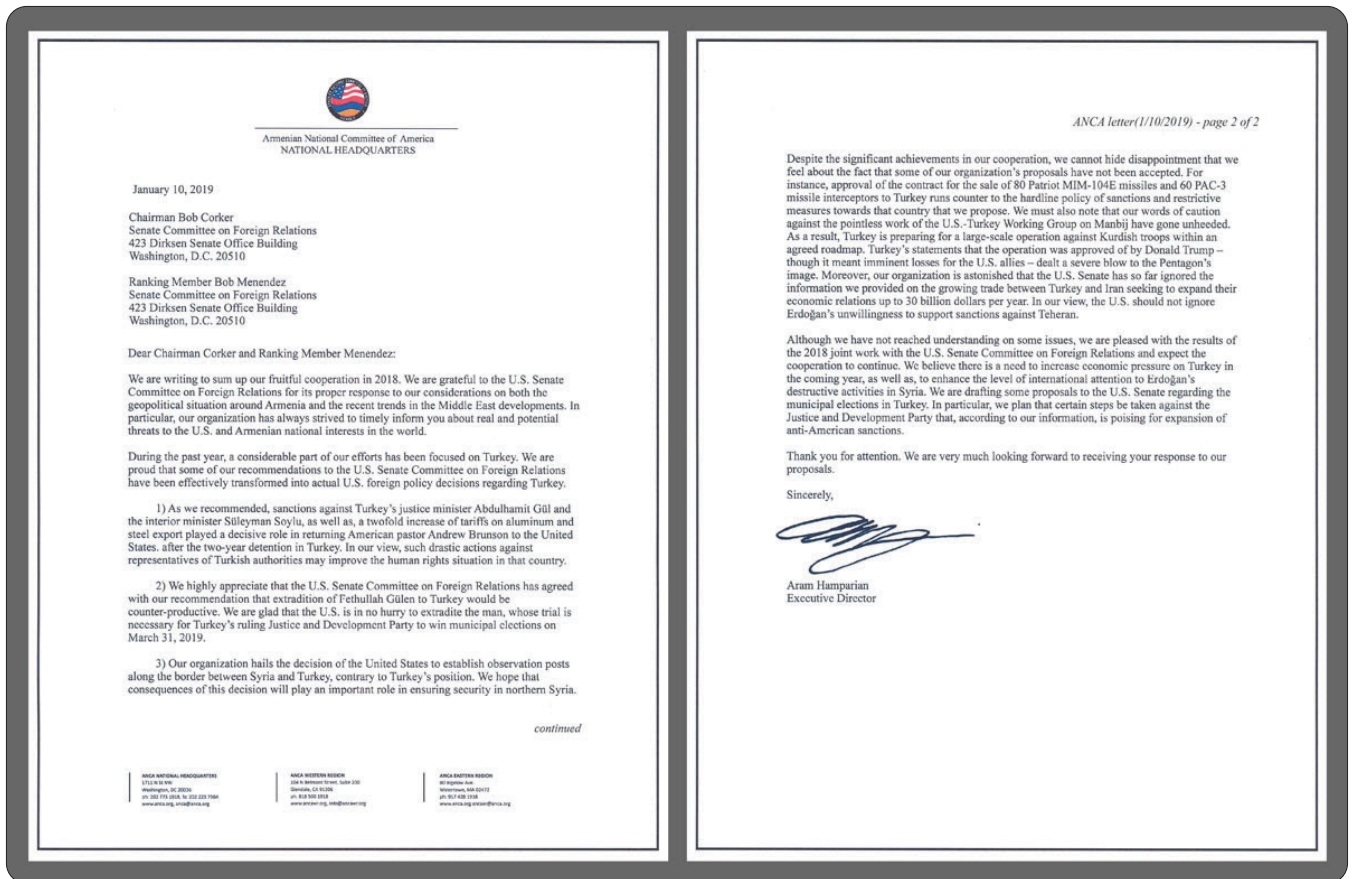
6. *Calls upon* the Turkish government to relevantly keep acting under the international law using the national law as well in order to prevent rhetoric and incitement to violence motivated by hatred against any other national minorities,

7. *Reminds* of necessity of the criminal prosecution for denial to recognize the genocide of the Armenians in 1915-1923,

8. *Decides* to remain seized of the matter.

2/2

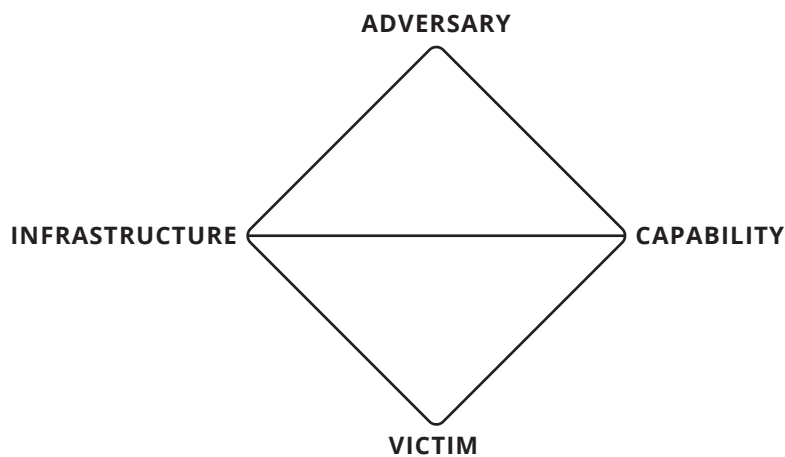
Attached draft resolution included in the aforementioned email to Secretary Pompeo.  
Page 2 of 2.



A [letter](#) addressed to U.S. Senators Bob Corker and Bob Menendez from Aram Khamparyan, Executive Director of the Armenian National Committee of America.

## Recorded Future Ontology

Recorded Future's Insikt Group tracks threat activity associated with new and existing threat actor groups, focusing on China, Iran, Russia, and North Korea. Insikt Group only names a new threat actor group or campaign when analysts have data corresponding to at least three points on the Diamond Model of Intrusion Analysis with at least medium confidence, and only when we can point to a handle, persona, person, or organization responsible. We will write about the activity as a campaign in the absence of this level of adversary data. We use the most widely-utilized or recognized name for a particular group when reporting and researching known threat actor groups.



Insikt Group utilizes a simple color plus [phonetic naming convention](#) for new threat actor groups or campaigns; we will utilize the most common name when an actor or campaign is already known. The first word in the convention will be a color, currently corresponding to the below, with more color/nation pairings to be added as we identify and attribute new threat actor groups associated with new nations.



## About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.