MANDIANT®

REPORT

‘Ghostwriter’ Influence Campaign:

Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned with Russian Security Interests

Executive Summary

- Mandiant Threat Intelligence has tied together several information operations that we assess with moderate confidence comprise part of a broader influence campaign, ongoing since at least March 2017, aligned with Russian security interests. The operations have primarily targeted audiences in Lithuania, Latvia, and Poland with anti-North Atlantic Treaty Organization (NATO) narratives, often leveraging website compromises or spoofed email accounts to disseminate fabricated content, including falsified correspondence from military officials.
- We have dubbed this campaign "Ghostwriter," based on its use of inauthentic personas posing as locals, journalists, and analysts within the target countries to post articles and op-eds referencing the fabrications as source material to a core set of third-party websites that publish user-generated content.
- In this report we outline the key tactics, techniques, and procedures we have observed used in the Ghostwriter campaign and summarize incidents and personas that we believe are part of the larger activity set. We continue to investigate multiple other suspected Ghostwriter operations and personas that are not detailed here.

Threat Activity Overview

Mandiant Threat Intelligence has tied together several information operations that we assess with moderate confidence comprise part of a broader influence campaign, ongoing since at least March 2017, aligned with Russian security interests. The operations have primarily targeted audiences in Lithuania, Latvia, and Poland with narratives critical of the North Atlantic Treaty Organization's (NATO) presence in Eastern Europe, occasionally leveraging other themes such as anti-U.S. and COVID-19-related narratives as part of this broader anti-NATO agenda. We have dubbed this campaign "Ghostwriter."

Many, though not all, of the incidents we suspect to be part of the Ghostwriter campaign appear to have leveraged website compromises or spoofed email accounts to disseminate fabricated content, including falsified news articles, quotes, correspondence and other documents designed to appear as coming from military officials and political figures in the target countries. This falsified content has been referenced as source material in articles and op-eds authored by at least 14 inauthentic personas posing as locals, journalists, and analysts within those countries. These articles and op-eds, primarily written in English, have been consistently published to a core set of third-party websites that appear to accept user-submitted content, most notably OpEdNews.com, BalticWord.com, and the pro-Russian site TheDuran.com, among others, as well as to suspected Ghostwriter-affiliated blogs.

Some of these incidents and personas have received public attention from researchers, foreign news outlets, or government entities in Lithuania and Poland, but have not been tied to a broader activity set. Others have received little attention and remain relatively obscure. Mandiant Threat Intelligence has independently discovered several Ghostwriter personas and identified additional incidents involving some of those personas previously exposed. We believe the assets and operations discussed in this report are for the first time being collectively tied together and assessed to comprise part of a larger, concerted, and ongoing influence campaign.

Who is Conducting This Activity and Why?

At this time, we do not attribute the Ghostwriter campaign to a specific actor or group of actors. Instead, we refer to Ghostwriter as an "activity set," with various incidents tied together by overlapping behavioral characteristics and personas, rather than as an actor or group in itself. Our moderate confidence assessment therefore corresponds to the tying of individual incidents, personas, and other assets to one another, and thus to the broader activity set, based on their overlapping behavior and interactions. It appears, based on the limited public information available regarding the website compromises we have tied to Ghostwriter, that the actors behind the campaign are relatively well-resourced, either directly possessing traditional cyber threat capabilities themselves or having ready access to operational support from others who do. It is plausible that Ghostwriter operations are conducted by overlapping actors or groups that are also behind other influence campaigns or incidents of cyber threat activity.

Promoted Ghostwriter narratives have aligned with Russian security interests, primarily seeking to foment distrust of U.S. and NATO troops in Europe by portraying their presence as aggressive and dangerous to local populations and to undermine military relations between NATO members. The narratives have focused heavily on NATO military exercises in the region, including Saber Strike 2018, ANAKONDA 2018, DEFENDER-Europe 20, and Iron Wolf 2019. For example, recent Ghostwriter incidents have included allegations that U.S. and NATO forces are contributing to the spread of COVID-19 in Europe. Our analysis of articles published this year by suspected Ghostwriter personas on TheDuran.com, one of the third-party websites frequently leveraged in the campaign, identified the most prevalent themes to be the impact of COVID-19 on U.S. and NATO forces, general attempts to discredit the U.S. and NATO, and strategic discussion favoring Russia over other world powers. On several occasions, news outlets and government agencies in Lithuania, Latvia, and Poland have issued public statements declaring content and narratives promoted as part of what we identify as Ghostwriter to be untrue and have labeled them to be "disinformation" or "fake news."

On the surface, some aspects of Ghostwriter operations, notably their occasional use of fabricated official documents and correspondences, bear resemblance to aspects of the ongoing suspected Russian influence campaign referred to as "Secondary Infektion," which was first publicly exposed by the Atlantic Council's Digital Forensics Research Lab[1] and which we have investigated and reported on extensively. However, we treat Ghostwriter and Secondary Infektion as two distinct activity sets given notable differences in observed behaviors and tactics between the two:

- Many Ghostwriter operations have leveraged compromised websites, including legitimate news websites, to publish fabricated content, or used spoofed email accounts to engage in direct outreach and dissemination of content to NATO itself and national organizations and media outlets in the target countries. We have not, at this time, observed the use of traditional cyber threat activity in support of Secondary Infektion operations.
- Multiple Ghostwriter operations have involved the dissemination of articles and narratives by multi-use inauthentic personas with developed histories, or single use personas impersonating real individuals or behind which at least some effort has been made to make them appear authentic, on a specific set of core platforms. By contrast, single-use burner accounts are almost exclusively used to post Secondary Infektion content across a variety of blogs, forums, and self-publishing sites, with little effort put into making the accounts appear authentic.

1 https://www.atlanticcouncil.org/wp-content/uploads/2019/08/Operation-Secondary-Infektion_English.pdf

Operations and Tactics

There is no modal Ghostwriter operation, with different combinations of tactics being employed and the order and nature of dissemination often changing from incident to incident (Figure 1). In general, however, the first stage of a Ghostwriter operation involves the creation of a falsified narrative and, commonly, accompanying fabricated "source" documentation such as fabricated quotes attributed to government officials, altered images, or falsified official correspondence or other documents such as the following:

- Fabricated quotes have formed the basis of false narratives pushed by Ghostwriter. For example, a quote falsely attributed to the commander of the NATO eFP Battle Group was used to push a narrative that Canadian soldiers stationed in Latvia had been diagnosed with COVID-19, stating "Yes, 21 soldiers have tested positive for the virus. We have taken the necessary security measures, but not everyone has the same immunity. All necessary measures are being taken. The soldiers are isolated."[2]
- Fabricated documents, including falsified official correspondence, have been used as source material for Ghostwriter narratives. For example, a fabricated letter presented as having been authored by NATO Secretary General Jens Stoltenberg was disseminated by Ghostwriter personas to bolster a narrative suggesting that NATO was planning to withdraw from Lithuania in response to the COVID-19 pandemic.[3]

Altered images have been used as evidence to support Ghostwriter narratives. For example, one incident involved the use of a photoshopped image of a Jewish cemetery that was purported to have been desecrated by German soldiers.[4]

One or more dissemination phases then occur, whereby varying combinations and orders of tactics are used to spread the false narratives, including placing articles and any supporting fabricated documentation onto compromised legitimate websites, using inauthentic personas to post "news" articles and op-eds on regularly leveraged third-party sites that appear to accept user-submitted content, posting articles and content to blog pages we suspect are directly affiliated with Ghostwriter, and direct email dissemination of content and articles, including to legitimate media outlets and government officials.

- Multiple Ghostwriter operations appear to have leveraged compromised websites, predominantly those of news outlets, to post fabricated news articles or documentation. Mandiant Threat Intelligence has not independently confirmed these compromises and is relying on reporting by government entities and media outlets in the target countries. In some cases, only the purported victim entity itself has publicly claimed to have been compromised. However, in many cases we also located archived copies of Ghostwriter articles posted to the suspected compromised sites (Table 1). Public reporting suggests that in at least some of these cases, the fabricated articles were published using the sites' content management systems (CMS) after obtaining user credentials.[5] Furthermore, it appears that rather than creating new CMS entries, the actors may have replaced existing legitimate articles on the sites with the fabrications.[6]

2 https://www.mod.gov.lv/en/news/artis-pabriks-attempts-attack-information-space-deceptive-messages-are-sign-potential
3 https://www.lrt.lt/en/news-in-english/19/1166199/fake-news-on-nato-withdrawal-from-lithuania-sent-to-media-brussels
4 https://twitter.com/Lithuanian_MoD/status/1177476876761042944
5 https://www.nksc.lt/doc/en/analysis/2018-01-29%20Brief%20review%20of%20an%20incident%20analysis.pdf
6 https://www.gov.pl/web/sluzby-specjalne/atak-dezinformacyjny-na-polske

  - In September 2019, for example, the local Lithuanian news site kaunas.kasvyksta.lt was reportedly compromised, and a false article published claiming that German soldiers had desecrated a Jewish Cemetery in Kaunas.[7] We independently observed an archived version of that article having been posted to the site.[8]
  - One of the few non-news site compromises involved the April 2020 compromise of the Polish War Studies Academy website, on which a fabricated letter presented as having been authored by the Commander of the Academy effectively called for Polish troops to fight against "the American Occupation," a reference to the NATO exercise DEFENDER-Europe 20.[9]

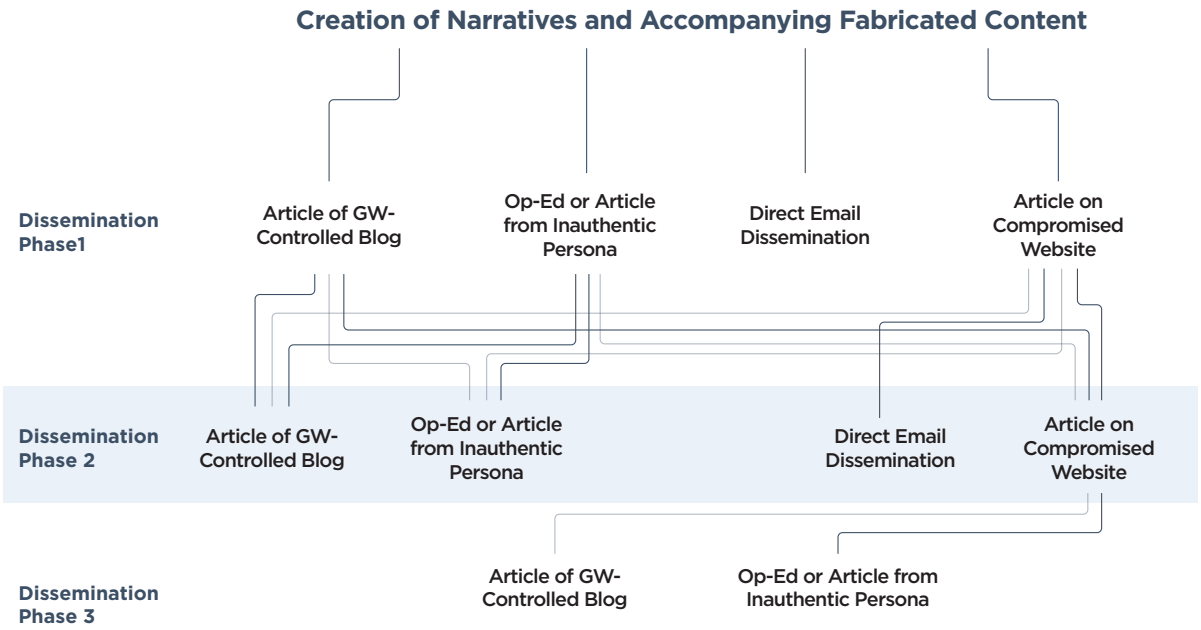
- Inauthentic Ghostwriter personas post fabricated news articles and op-eds that push the falsified narratives and reference the fabricated source materials. These articles have primarily been published in English on a small core of sites that appear to allow for the submission of user-generated content, most notably OpEdNews.com, BalticWord.com, and the pro-Russia site TheDuran.com, as well as occasionally on one of more than a dozen other websites and platforms we have observed used by Ghostwriter personas. Such articles also often reference the articles or materials posted on the compromised legitimate sites.
  - For example, an article titled "US official had no mercy for Polish soldiers!" authored by the persona "Rod Renny" and posted to TheDuran.com, directly referenced a falsified interview posted to several reportedly compromised Polish media sites.[10]
- On several occasions, Ghostwriter narratives and articles have been directly disseminated over email, notably to legitimate news organizations and government officials in Lithuania and Poland, as well as NATO officials. Our analysis of public reporting on individual incidents suggests that in the majority of cases this direct email outreach has been done using spoofed email addresses presented as coming from various individuals, including government and military officials and journalists. For example, an email presenting as coming from a staffer at the Lithuanian media outlet delfi.lt was reportedly sent to various other media outlets in Lithuania and promoted the narrative that U.S. soldiers had been involved in a carjacking in that country.[11]
- Articles promoting Ghostwriter narratives have also been posted to various blogs and pages on Wix, Blogspot, and Wordpress that we suspect to be Ghostwriter-controlled. For example, an article published on WordPress promoted a false claim that a U.S. Army officer serving in Lithuania had contracted COVID-19 and then interacted with the local population.[12] [13]
- In some instances, we have observed further amplification of fabricated Ghostwriter articles on social media by suspected inauthentic personas, though this is not a primary vector of dissemination in the campaign.

7 https://www.defenseone.com/technology/2019/12/russian-trolls-are-hammering-away-natos-presence-lithuania/161654/
8 http://archive.is/EvGY3#selection-2335.0-2335.20
9 https://www.gov.pl/web/sluzby-specjalne/atak-dezinformacyjny-na-polske
10 https://theduran.com/us-official-had-no-mercy-for-polish-soldiers/
11 https://www.delfi.lt/news/daily/demaskuok/sukciai-platina-melaginga-naujiena-apie-vilniuje-nusikaltusius-jav-karius.d?id=83091211
12 https://web.archive.org/web/20200204124812/https://1stbatcavregusblog.wordpress.com/2020/01/28/coronavirus-u-s-officer-hospitalized-in-lithuania-in-critical-condition/
13 https://www.lrt.lt/en/news-in-english/19/1139432/fake-news-on-coronavirus-infected-us-soldier-emailed-to-lithuanian-authorities

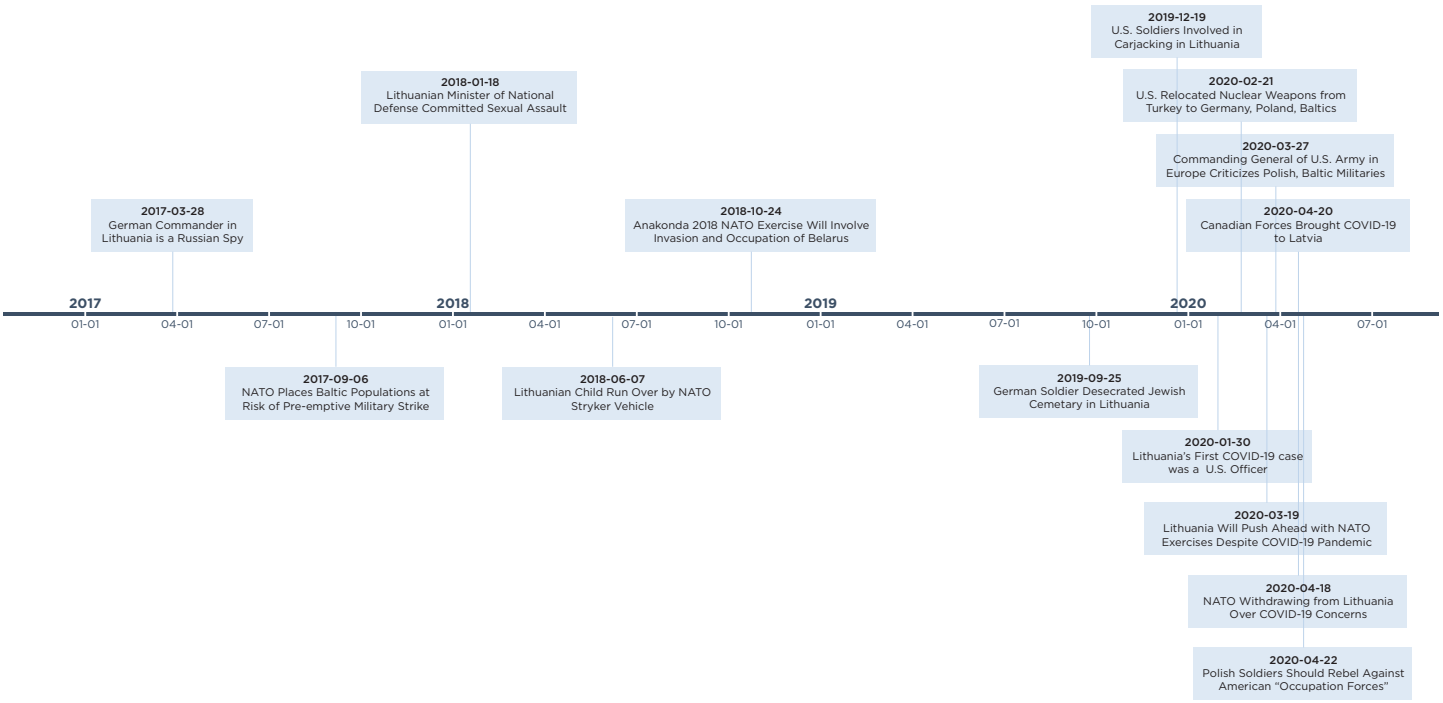
Table 1 and Figure 2 below summarize and provide a timeline of fourteen incidents we have tied to Ghostwriter. As mentioned previously, we have identified numerous other incidents not detailed here that we believe to be Ghostwriter-related and are continuing to investigate.

Figure 2.

Ghostwriter Dissemination Flows Vary Between Operations. This figure represents an aggregate depiction of dissemination paths across the fourteen operations detailed here.



Operational Timeline



Narrative	Date(s) of Core Activity	Fabricated Content, Documents, or Materials	Website Compromises					Direct Email Dissemination		Ghostwriter Personas Posting Articles/Op-Eds on Third-party Platforms	Suspected Ghostwriter-Affiliated Blog Dissemination
			Reportedly Compromised Sites	Government Entity Confirmed	Third-party Media Reported	Victim Self-Reported	Archived Compromised Page	Reportedly Spoofed Accounts	Persona-affiliating Account		
Commanding General of U.S. Army in Europe Criticizes Polish, Baltic Militaries	27 May, 2020	Falsified Interview Transcript, Quotes from U.S. Army Lt. Gen. Cavoli, Commanding General of U.S. Army Europe	zary-zagan.regionalna.p, olsztyn24.com, niezalezna.pl, radiosczcecin.pl, polanddaily.com, telwizjarepublika.pl	Yes[i]	Yes[ii]	-	Yes[iii]	-	-	Rod Renny, Katarzyna Gójska	-
Canadian Forces Brought COVID-19 to Latvia	22-24 April, 2020	Falsified Quotes from NATO eFP Battle Group Commander Lt. Col. Eric Angell	-	-	-	-	-	-	Edgars Palladis	Edgars Palladis, Vairis Godmanis	-
Polish Soldiers Should Rebel Against American "Occupation Forces"	22-24 April, 2020	Fabricated Letter from Commander of Polish War Studies Academy Brig. Gen. Ryszard Parafianowicz	akademia.mil.pl, prawy.pl, lewy.pl, podlasie24.pl	Yes[iv]	Yes[v]	-	Yes[vi]	Yes[vii]	-	Rod Renny	-
NATO Withdrawing from Lithuania Over COVID-19 Concerns	18-22 April, 2020	Fabricated Letter from Secretary General of NATO Jens Stoltenberg, Fabricated Blog Presented as Belonging to Lithuanian Journalist Vilius Petkauskas	-	-	-	-	-	Yes[viii]	-	Vilius Petkauskas (impersonating real Lithuanian journalist of the same name), Jonas Katinelis	Yes
Lithuania Will Push Ahead with DEFENDER-Europe 20 NATO Exercises Despite COVID-19 Pandemic	19-21 March, 2020	Falsified Quotes from Lithuanian Defense Minister Raimundas Karoblis	baltic-course.com*	-	-	-	Yes[ix]	Yes[x]	-	Tomas Kurtinaitis	-
U.S. Relocated Nuclear Weapons from Turkey to Germany, Poland, Baltics	21 Feb-12 March, 2020	Suspected Falsified Quote Attributed to a U.S. "Air Mobility Command Official"	-	-	-	-	-	-	Claimed by Rod Renny Persona Itself	Rod Renny, Belit Onay	-
Lithuania's First COVID-19 Case was a U.S. Army Officer	30-31 an, 2020	Falsified Quote from a U.S Army Officer, Blog Impersonating 1st Battalion, 9th U.S. Cavalry Regiment	baltictimes.com, kauno.diena.lt, klaipeda.diena.lt, diena.lt kasvyskta.lt	-	Yes[xi]	Yes[xii]	Yes[xiii]	Yes[xiv]	-	Al Peterson	Yes
U.S. Soldiers Involved in Carjacking in Lithuania	19 Dec, 2019	Falsified Quotes from Vilnius Chief of Police Saulius Gagas	baltictimes.com	-	Yes[xv]	-	Yes[xvi]	Yes[xvii]	-	Antanaitis Justinas	Yes

Table 1. Summary of fourteen suspected Ghostwriter operations, including core narratives and dissemination methods observed. Asterisks denote suspected, but unreported potential website compromises. Limited indicators, including the appearance on these sites of Ghostwriter-linked articles at the same time that they were disseminated elsewhere by Ghostwriter personas, as well as public reporting of previous compromises of these sites that were used to publish falsified articles, lead us to suspect that these sites may have been compromised as part of the Ghostwriter incident in question. We independently confirmed using website archives and caches that Ghostwriter-linked articles did appear on these sites at the same time as the broader related Ghostwriter activity, but could not confirm their compromise through third-party reporting.

Narrative	Date(s) of Core Activity	Fabricated Content, Documents, or Materials	Website Compromises					Direct Email Dissemination		Ghostwriter Personas Posting Articles/Op-Eds on Third-party Platforms	Suspected Ghostwriter-Affiliated Blog Dissemination
			Website Compromises	Website Compromises	Website Compromises	Website Compromises	Website Compromises	Reportedly Spoofed Accounts	Persona-affiliating Account		
German Soldiers Desecrated Jewish Cemetery in Lithuania	25 - 26 Sept. 2019	Photoshopped Images of Cemetery Destruction, Wordpress Site Impersonating Local Jewish Organization, Fabricated Quotes Attributed to Head of the Organization, Fake Online Petitions	kaunas.kasvyksta.lt	-	Yes[xviii]	-	Yes[xix]	Yes[xx]	-	-	Yes
Anakonda 2018 NATO Exercise Will Involve Invasion and Occupation of Belarus	24 - 26 Oct. 2018	Fabricated Operational Maps, Military "News" Blog	kasvyksta.lt	-	Yes[xxi]	Yes[xxii]	Yes[xxiii]	-	-	Rudis Kronitis, Paul Black	Yes
Lithuanian Child Run Over by NATO Stryker Vehicle	7 - 8 June, 2018	Fabricated Screenshot of Non-Existent Article on Incident, Photoshopped Image of Alleged Incident	baltic-course.com	-	-	Yes[xxiv]	Yes[xxv]	-	-	Rudis Kronitis	Yes
Lithuanian Minister of National Defense Committed Sexual Assault	18 - 22 Jan. 2018	Falsified Quotes from Alleged Victims of Sexual Assault	Tv3.lt	Yes[xxvi]	Yes[xxvii]	-	No	Yes[xxviii]	-	Rudis Kronitis	Yes
NATO Places Baltic Populations at Risk of Pre-emptive Military Strike	6 - 8 Sept. 2017	-	lzinios.lt*	-	-	-	Yes[xxix]	-	-	Rudis Kronitis	Yes
German Commander in Lithuania is a Russian Spy	28 March, 2017	Photoshopped Images of German Lt. Col. Christoph Huber in Various places in Russia	-	-	-	-	-	Yes[xxx]	-	-	Yes

Table 1. Continued.

i https://www.gov.pl/web/sluzby-specjalne/kolejny-atak-informacyjny-na-pl
ii https://www.lrt.lt/en/news-in-english/19/1184269/complex-fake-news-attack-targets-us-troops-in-baltics
iii http://archive.is/Xxpu2 (olsztyn24.com)
http://archive.is/XYEMP (niezalezna.pl)
https://archive.is/HU9wq (epoznan.pl)
https://webcache.googleusercontent.com/search?q=cache:z0eMRXcTxB0J:https://radioszczecin.pl/6,406325,amerykanie-chwala-pobyt-w-drawsku-jedyne-czym-mo+&cd=1&hl=en&ct=clnk&gl=us (radioszczecin.pl);
http://archive.is/29kQy (polanddaily.com)
https://webcache.googleusercontent.com/search?q=cache:WJ0P49y5t1YJ:https://m.telewizjarepublika.pl/amerykanie-chwala-pobyt-w-drawsku-jedyne-czym-moga-strzelic-to-gumki-od-majtek,96202.html+&cd=1&hl=en&ct=clnk&gl=us (telewizjarepublika.pl)
iv https://www.gov.pl/web/sluzby-specjalne/atak-dezinformacyjny-na-polske
v https://www.polskieradio.pl/395/7785/Artykul/2498380,Website-of-Poland%E2%80%99s-War-Studies-Academy-hacked-in-%E2%80%98disinformation-campaign%E2%80%99
https://www.cyberscoop.com/poland-cyberattack-russia-us-military/
vi https://archive.is/0010o
vii https://www.gov.pl/web/sluzby-specjalne/atak-dezinformacyjny-na-polske
viii https://www.lrt.lt/en/news-in-english/19/1166199/fake-news-on-nato-withdrawal-from-lithuania-sent-to-media-brussels
ix https://web.archive.org/web/20200319100057/http:/www.baltic-course.com/news/doc=154749.htm
x https://www.lrt.lt/en/news-in-english/19/1153504/coronavirus-linked-cyber-attack-targets-lithuanian-defence-minister,
https://www.delfi.lt/news/daily/demaskuok/sukciai-naudojasi-koronavirusu-apsimete-pareigunais-baugina-apie-neva-slepiama-informacija.d?id=83829475
xi https://en.delfi.lt/politics/fake-report-about-coronavirus-infected-us-soldier-posted-on-news-website.d?id=83421487#cxrecs_s
https://www.lrt.lt/en/news-in-english/19/1139432/fake-news-on-coronavirus-infected-us-soldier-emailed-to-lithuanian-authorities
xii https://kauno.diena.lt/naujienos/kaunas/miesto-pulsas/portale-kaunodienalt-paskelbta-melaginga-zinia-apie-koronavirusu-uzsikretusi-kari-950704
xiii (https://archive.li/88ak7)
(http://archive.is/u2qRm)
xiv https://www.lrt.lt/en/nws-in-english/19/1139432/fake-news-on-coronavirus-infected-us-soldier-emailed-to-lithuanian-authorities
xv https://www.delfi.lt/news/daily/demaskuok/sukciai-platina-melaginga-naujiena-apie-vilniuje-nusikaltusius-jav-karius.d?id=83091211
xvi https://web.archive.org/web/20191219124154/https:/www.baltictimes.com/news/u_s_soldiers_suspected_of_attempted_car_theft_in_vilnius.html
xvii https://www.polygraph.info/a/fact-check-us-army-lithuania-cyber-attack/30341011.html
https://www.delfi.lt/news/daily/demaskuok/sukciai-platina-melaginga-naujiena-apie-vilniuje-nusikaltusius-jav-karius.d?id=83091211
xviii https://www.defenseone.com/technology/2019/12/russian-trolls-are-hammering-away-natos-presence-lithuania/161654/
xix http://archive.is/EvGY3#selection-2335.0-2335.20
xx https://www.delfi.lt/news/daily/demaskuok/pasauli-siurpina-melaginga-naujiena-kaltina-nato-tankus-isniekinus-kauno-zydu-kapines.d?id=82354093
xxi https://euvsdisinfo.eu/report/nato-is-planning-to-invade-belarus/
xxii https://kaunas.kasvyksta.lt/2018/11/08/112/portalas-kas-vyksta-kaune-patyre-kibernetine-ataka/
xxiii http://archive.is/LPljz
xxiv http://www.baltic-course.com/eng/modern_eu/?doc=140643
xxv http://archive.is/T5VhM
xxvi https://www.nksc.lt/doc/en/analysis/2018_01_29_Brief_review_of_an_incident_analysis.pdf
xxvii https://en.delfi.lt/politics/fake-news-on-lithuanian-defence-minister-planted-on-news-portal.d?id=76942721
xxviii https://www.nksc.lt/doc/en/analysis/2018_01_29_Brief_review_of_an_incident_analysis.pdf
xxix https://archive.is/DoFsE
xxx https://en.delfi.lt/archive/another-information-attack-against-nato-troops-in-lithuania-german-battalion-leader-in-the-crosshair.d?id=74227208

Table 1. Continued.

Inauthentic Personas

Multiple indicators suggest that at least 14 suspected Ghostwriter personas have published articles promoting narratives corresponding with at least 15 suspected Ghostwriter operations since 2017 (Table 2). We have observed at least six of these personas leveraged in multiple Ghostwriter operations. The vast majority of the personas use either Baltic- or English-sounding names, some of which are inconsistent with their supposed identity or otherwise raise suspicions. Many claim to be locals, journalists, or editors of the target countries in biographies they have listed on sites to which they contribute content.

We have observed indicators of coordination between some of the personas. For example, multiple identified personas have "upvoted" one another's articles on TheDuran.com but have not upvoted any other content on the site. For instance, "Rod Renny" upvoted articles from Belit Onay and "jonaskatinelis." We have also observed multiple personas publish articles as part of the same operation(s). For instance, both Belit Onay and Rod Renny published falsified articles regarding the alleged transportation of American nuclear weapons from Turkey to Poland and Germany. "Vilius Petkauskas" and "Jonas Katinelis" both published falsified articles alleging that NATO was withdrawing its troops from Lithuania. In late April, "Vairis Godmanis" and Edgars Palladis published similar articles that included the same fabricated quote falsely attributed to a Canadian military officer alleging that around 20 Canadian soldiers in Latvia were diagnosed with COVID-19.

Figure 1. The Rod Renny persona upvoted articles from two other suspected personas, Belit Onay and jonaskatinelis. Two of the upvoted articles pertain to recent operations in which fabricated documents were disseminated through compromised websites.

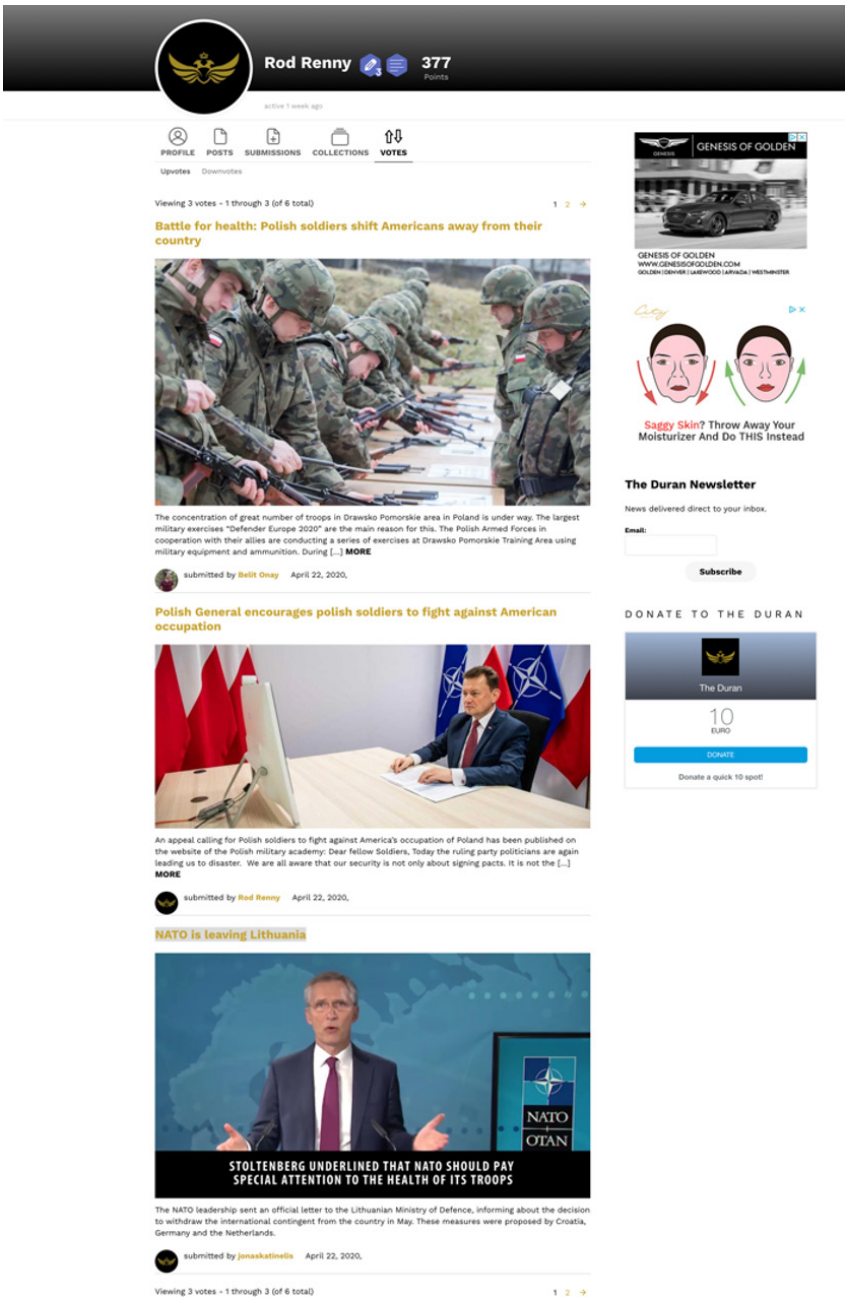


Table 2 below lists 14 of the Ghostwriter personas we have identified. As mentioned previously, we have identified numerous other personas not detailed here that we believe to be Ghostwriter-related and are continuing to investigate.

Table 2.

Fourteen identified Ghostwriter author personas primarily publish on a core set of "news" sites, including opednews.com, balticword.eu, and theduran.com

Persona	Self-listed Bio as listed on OpEdNews	Single or Multi-Operational Use	Published on TheDuran?	Published on OpEdNews	Published on BalticWord
Al Peterson	n/a	Single-Use			
Antanaitis Justinas	n/a	Single-Use			
TheBalticWord	n/a	Multi-Use	✓		✓
Belit Onay	"Goodman"	Multi-Use	✓	✓	
Edgars Palladis	n/a	Multi-Use	✓		
Jonas Katinelis	"I was born in Lithuania. Living in United Kingdom now. Interested in history, politics,economics,sport,art and so on. Young and clever person that cares about everything in all over the world."	Single-Use	✓	✓	
Katarzyna Gójska/ "polanddaily"	n/a	Single-Use	✓		
Paul Black	"Journalist. I live in the United Kingdom. I am writing about modern politics and defense."	Single-Use		✓	
Rod Renny	"An editor at large for JournalPosts.com"	Multi-Use	✓		✓
Rudis Kronitis	"Latvian, proud of my country"	Multi-Use		✓	
Stephen Blank	n/a	Single-Use			
Tomas Kurtinaitis	"A Lithuanian journalist and politician."	Single-Use		✓	
Vairis Godmanis/ Vargod Govar	"Former journalist interviewed murderers on death row, flown over L.A. with the LAPD and patrolled with the Royal Canadian Mounted Police near the Arctic. I am also reported from the Caribbean, Africa and Kuwait's border with Iraq. My articles have been published in nearly 30 countries, including an illegal translation produced in Iran. Now i'm workin with balticword.eu site. Me and my team are writing about military, political and social sphere of Lithuania, Latvia and Estonia. Please, enjoy it!"	Multi-Use		✓	✓
Vilius Petkauskas	"A Lithuanian journalist in https://www.15min.lt"	Single-Use	✓	✓	✓

Outlook and Implications

The Ghostwriter campaign leverages traditional cyber threat activity and information operations tactics to promote narratives intended to chip away at NATO's cohesion and undermine local support for the organization in Lithuania, Latvia, and Poland. While the operations so far have targeted audiences in this limited set of countries, we caution that the same tactics employed in the Ghostwriter campaign can be readily repurposed and used against other target geographies. Given the established history of cyber threat and information operations tactics regularly migrating from targeting Eastern Europe to targeting Western Europe and the U.S., this campaign may warrant special attention, especially as elections near.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About Mandiant Solutions
Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

MANDIANT®