

Mitigating information operations: The case of Ghostwriter campaign

Anneli Ahonen

Perception of an influence operation

Facebook's fake news: Mark Zuckerberg rejects 'crazy idea' that it swayed voters

Mark Zuckerberg: I regret ridiculing fears over Facebook's effect on election

POLITICS • TWITTER

Twitter Found 201 Accounts Linked to Russian Agents Who Bought Facebook Ads

Russia-backed Facebook posts 'reached 126m Americans' during US election

Twitter released 9 million tweets from one Russian troll farm. Here's what we learned.

The massive data dump reveals how trolls disrupt and destabilize local and global politics.

Building up counter-measures

Н НОВАЯ ГАЗЕТА НОВОСТИ ИНФОГРАФИКА РАССЛЕДОВАНИЯ МНЕНИЯ ПОДКАСТЫ

СЮЖЕТЫ • ПОЛИТИКА

Где живут тролли. И кто их кормит

Специальный репортаж из офиса, в котором вешают лапшу в три смены

Этот материал вышел в номере № 100 от 9 сентября 2013

[ЧИТАТЬ](#)

19:05, 7 сентября 2013 · Александра Гармажапова, корреспондент «Новой газеты» в Петербурге»

В Петербурге и Москве в специально оборудованных офисах орудуют интернет-тролли, которые хвалят Сергея Собянина и Владимира Путина, ругают Алексея Навального, Америку и защищают Сирию.

U.S. Treasury sanctions 'Putin's Chef' for more attempted election interference

Yevgeniy Prigozhin, known as "Putin's Chef," was previously sanctioned for attempted meddling in the 2016 election. The new sanctions focus on 2018.



B B C

Home News US Election Sport Business Innovation Culture Arts Travel Earth Video Live

Facebook owner bans Russian state media networks

17 September 2024

Share ◀ Save +

Peter Hoskins
Business reporter



Part 1: The West becoming aware of information influence

EU timeline:

2015: To address Russia's disinformation campaigns:

- Improve EU's communication in the Eastern Partnership
- Support to media
- Raise awareness about pro-Kremlin disinformation

2018: EU invests more in the work:

- Improve analysis
- International cooperation
- Voluntary code of practice for social media platforms

2020: New EU framework for foreign information manipulation and interference:

- More resources, starts covering China

2022:

- EU imposes sanctions to Russian propagandists
 - Digital Services Act for social media regulation
-

THE GHOSTWRITER CAMPAIGN

2 0 2 3

AS A
MULTI-VECTOR
INFORMATION
OPERATION:



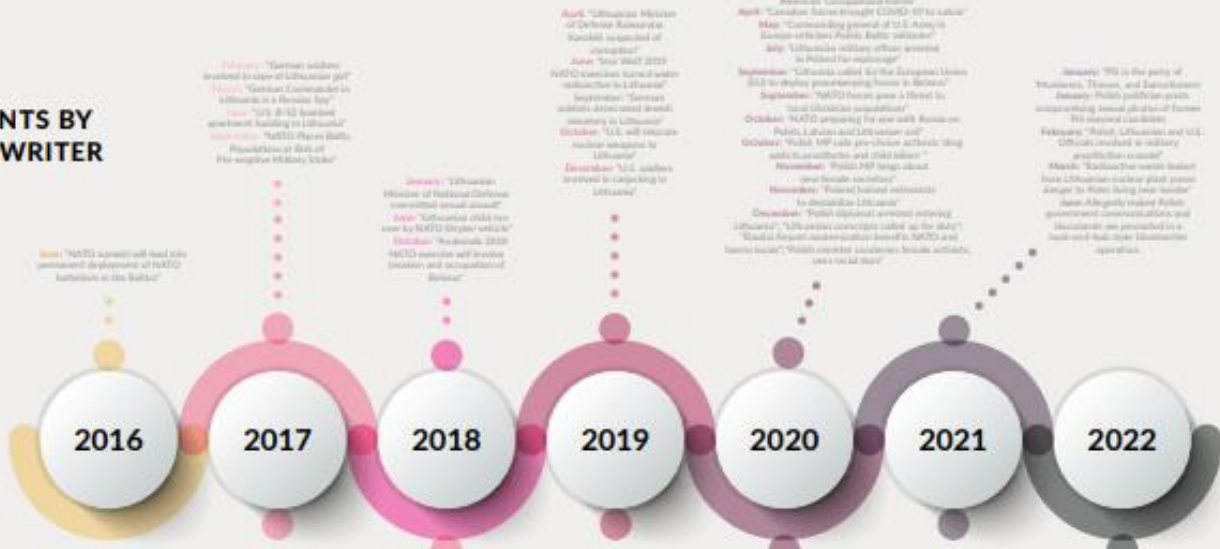
ATTEMPTS TO CONTROL ITS INFLUENCE &
THE LIMITATIONS OF CURRENT COUNTER-MEASURES

Ghostwriter: Behavioral Signature

- **Cyber activity conducted beforehand, through which access to compromised websites or social media accounts is obtained.**
- **Typical targeting involves a military component, either in messaging or in the choice of targets, but does not limit itself to that. Main targets are in Central and Eastern Europe.**
- **Content of messages is often faked and calls for a public rebuttal.**
- **Distribution of faked content mixes inauthentic accounts, spoofed emails, and impersonation; as well as compromised but real websites or social media accounts.**
- **Operations are timed and planned to coincide before or during important political events, such as high-profile visits or military exercises. Unlike other operations, they are rarely rapid reactions to events.**
- **It is likely that initially Ghostwriter activity was a response to NATO's increased presence in the Baltic region.**

BEHAVIOURAL SIGNATURES OF A GHOSTWRITER INFLUENCE OPERATION

INCIDENTS BY GHOSTWRITER



ATTEMPTS TO CONTROL THEIR INFLUENCE

2016

- June: NATO summit will lead into permanent deployment of NATO battalions in the Baltics

2017

- February: German soldiers deployed to base of Lithuania port
- March: German Chancellor in Lithuania is a Russian spy
- June: US-BND located apartment building in Lithuania
- June: NATO Plans Staff: Preparation of Staff of the respective Military Staff

2018

- January: Lithuania: Mission of Defense Ministeris, Karolis, suggested of "ghostwriter"
- June: Year 2017 2019 NATO exercises turned water reduction in Lithuania
- September: German soldiers announced arrival country in Lithuania
- October: "LLE will receive nuclear weapons by Lithuania"
- December: "US soldiers revealed in carrying to Lithuania"
- January: Lithuania: national authorities NATO, politicians, media and analysts over the incidents and attack them

2019

- January: Lithuania: national authorities NATO, politicians, media and analysts react to the incidents and attack them

2020

- February: German: Handwritten materials that reveal operations of a operations targeting the Baltics and Poland are connected with such other as a target. To use targeted influence campaign, and even it "ghostwriter"
- Lithuania, Latvia and Polish national authorities, NATO, politicians, media and analysts react to the incidents and attack them

2021

- January: Lithuania: national authorities NATO, politicians, media and analysts react to the incidents and attack them
- February: German: Handwritten materials that reveal operations of a operations targeting the Baltics and Poland are connected with such other as a target. To use targeted influence campaign, and even it "ghostwriter"
- Lithuania, Latvia and Polish national authorities, NATO, politicians, media and analysts react to the incidents and attack them
- January: Lithuania: national authorities NATO, politicians, media and analysts react to the incidents and attack them

2022

- January: Lithuania: national authorities NATO, politicians, media and analysts react to the incidents and attack them

Ghostwriter: cyber-enabled influence campaign

2016
NATO summit in June agrees to increase presence in the Baltics and Poland

2017
Exercise 'Iron Wolf' in Lithuania
Germany leads the battlegroup in Lithuania, Canada in Latvia, UK in Estonia and US in Poland.

2018
Saber Strike and Anakonda exercise

2019
Three exercises: Iron Wolf, Dragon, Baltops

2020
COVID-19
Presidential election in Poland
Defender 2020 exercise

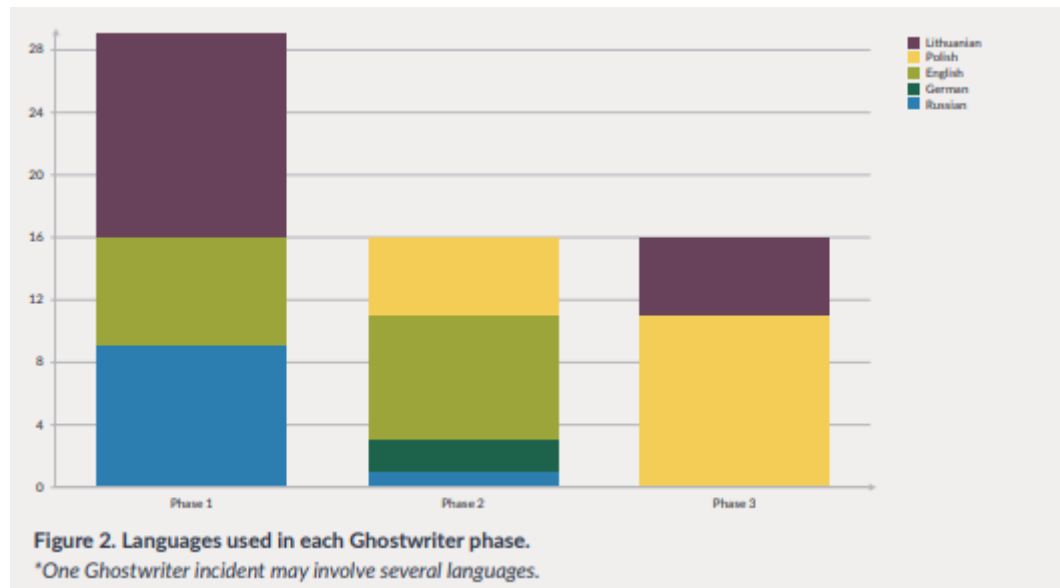
2021
2020-2021 Belarus protests
Parliamentary election in Germany
Russia masses its troops on the Ukrainian boarder

Ghostwriter: cyber-enabled influence campaign

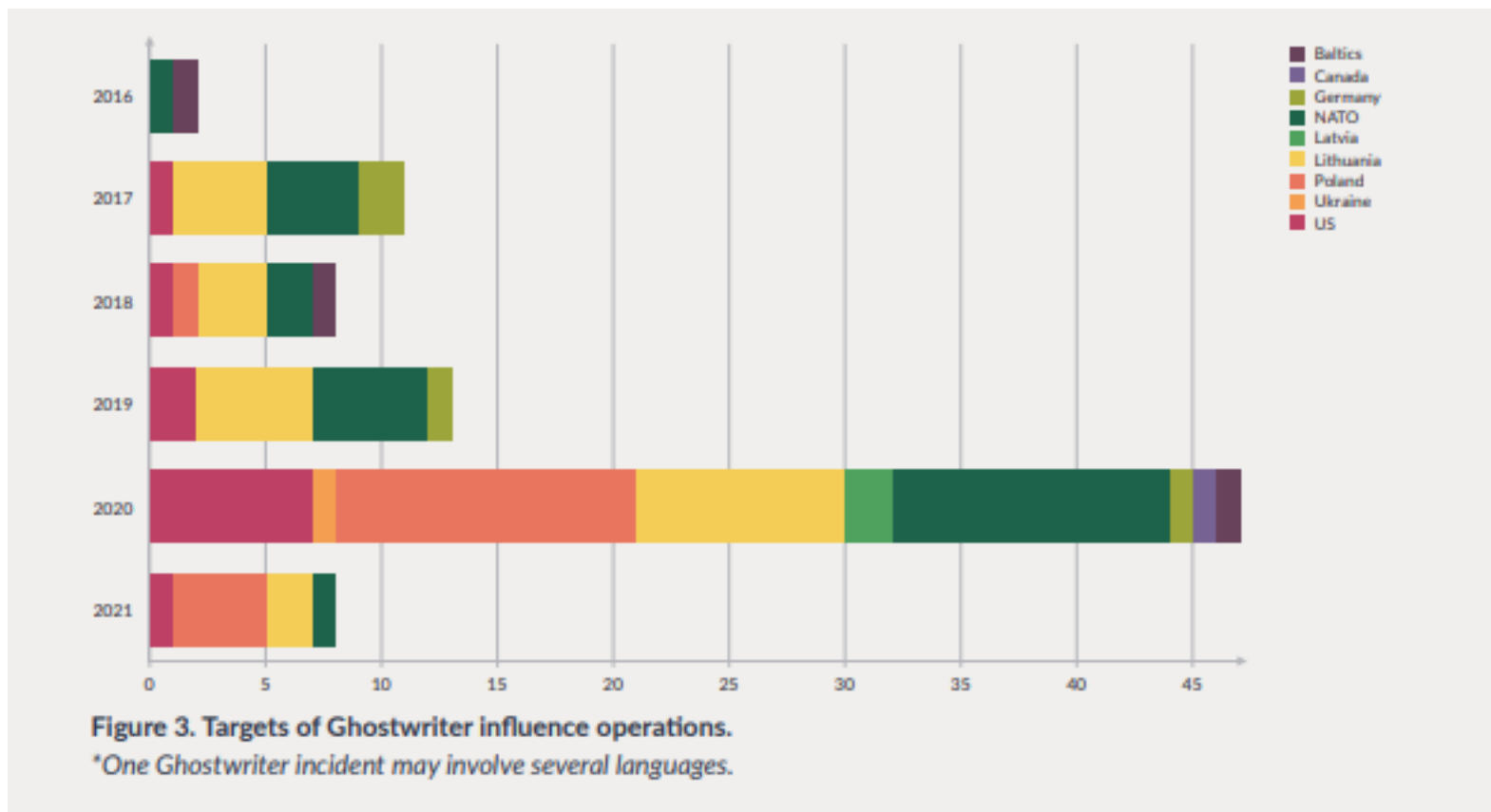
- **Based on open-source data, Ghostwriter has:**
 - impacted thousands of email users
 - hacked dozens of social media accounts and media websites
 - published hundreds of false blogposts and other falsified content
 - impersonated multiple government officials, NATO representatives and journalists in Europe
 - operations are an ongoing threat and supported by a foreign state threat actor, either Russia, Belarus, or both.
- **Responses:**
 - governments, private cyber firms, social media platforms, media, and civil society
 - focus on strategic communication, public but partial attribution, improving cyber security, and recently disrupting parts of the activity on Facebook and Google.
 - serious gaps remain in our understanding of the scale and authorship of the operation, that has hindered the efficiency of the response

Three phases of Ghostwriter campaign

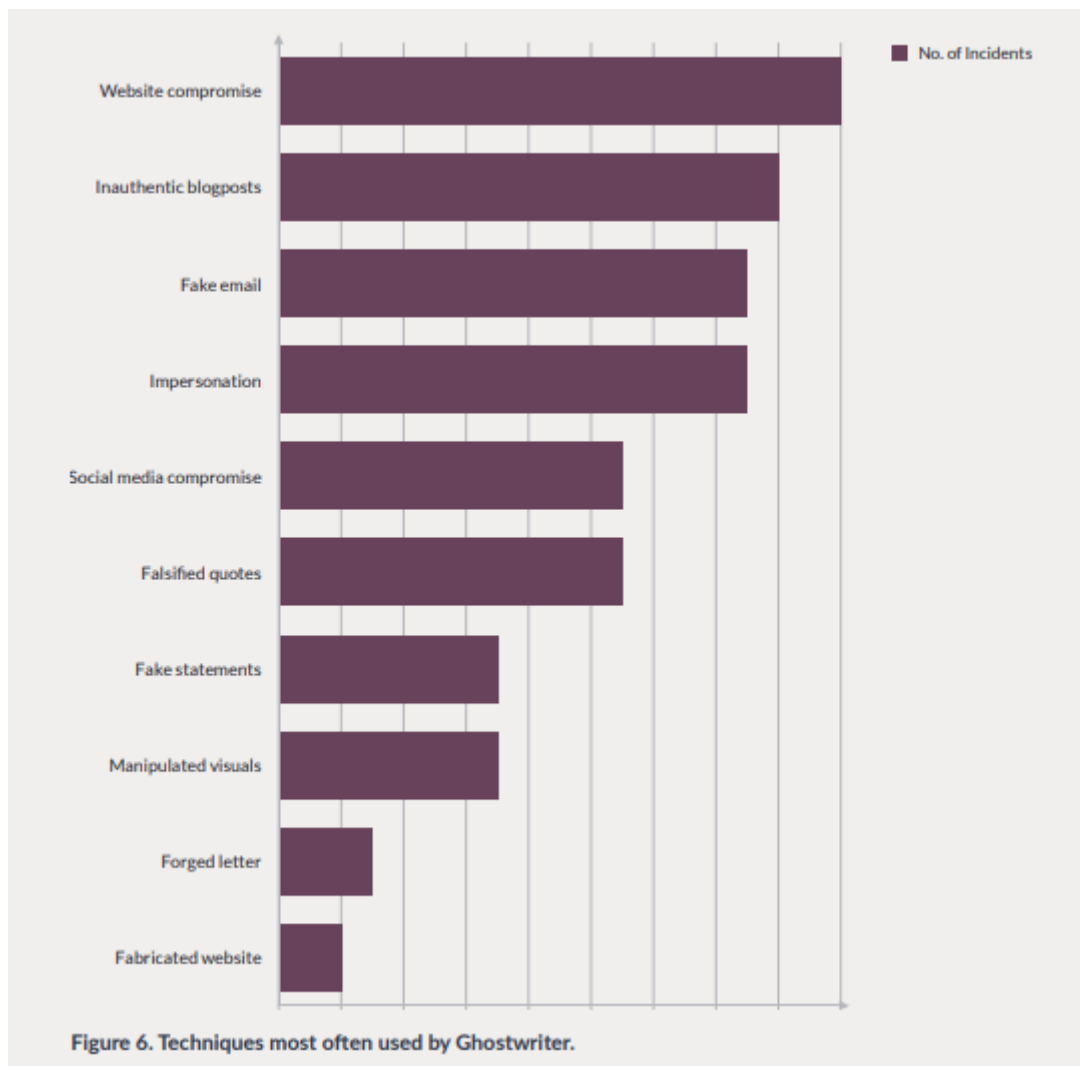
- **Phase 1: summer 2016-January 2020, mainly targeting NATO's presence in the Baltics.**
- **Phase 2: the campaign expands to targeting Poland in 2019/2020.**
- **Phase 3: late 2020 it starts exploiting hacked social media accounts more frequently.**



Targets of Ghostwriter incidents



Techniques of Ghostwriter incidents



Evolution of the response

- Strategic communication
- Diplomatic channels
- Improving cyber security
- Deplatforming efforts
- Gradual attribution

Leaked email scandal engulfs Poland's political elite

Government officials confirm that they used private email accounts for public business, but blame Russia for the hack.



Most Read Articles

1. French Catholic Church inc uncovers thousands of pedo
1950

OCTOBER 3, 2021 | 1:14 PM

2. How Xi Jinping lost Austral

SEPTEMBER 27, 2021 | 12:11 PM

The New York Times

Germany Investigates Russia Over Pre-Election Hacking

Berlin has protested to Moscow after identifying repeated attempts to steal politicians' private information before the election this month that will decide Angela Merkel's successor.

Give this article



Facebook Blocked Russia and Belarus Hackers Targeting Ukraine

News 2020.04.29 10:14

Provocation against NATO in Lithuania failed, says NATO chief 80

BNS
2020.04.29 10:14



Lacking from the response

- **No sanctions designated**
- **Those responsible for Ghostwriter not prosecuted**
- **EU's cyber sanctions toolbox not put in use**
- **None of the countries has used offensive cyber capabilities**
- **Social media platforms don't have public reporting on Ghostwriter's activities on their platforms equal to their reporting on IRA**

Potential reasons:

- **Lack of intelligence sharing**
- **Lack of robust knowledge of the specific operators**
- **Social media platforms haven't reacted due to low engagement figures**
- **"Linkage blindness" – who should take the responsibility?**

Role of the domestic actors?

- Detailed and timely knowledge of local circumstances in Lithuania
- Potential intelligence gathering beforehand
- Consistent improvement in the quality of the language used, formatting and visuals
- Especially good knowledge of political context and backstage in Poland



What works

- Holistic understanding and continuous monitoring beyond separate incidents
- Assess cumulative impact vs social media engagement figures
- Present “hard” cyber evidence and debunk at the same time?
- The social media platforms’ takedowns and policies regarding specific threat actors need to be developed to cope with multi-vector attack methodologies; consider publishing historical data of a certain threat actor
- Public statements to support/warn the users and targets of the attacks
- More funding to upgrade media’s and NGO’s cyber security
- Prebunking ahead of NATO exercises and important political events
- “Linkage blindness” – who should take the responsibility?