Secondary Infektion

Ben Nimmo, Camille François, C. Shawn Eib, Lea Ronzaud, Rodrigo Ferreira, Chris Hernon, and Tim Kostelancik,
Table of contents

1. Secondary Infektion at a Glance
2. Executive Summary
3. Lessons Learned and Questions Unanswered
4. The Operation’s Main Themes
5. Highlights: WADA, Clinton, Macron
6. The Countries
7. The Techniques
8. The Effort and the Impact
9. Early Experiments with Personas
10. Vignettes
11. Lighter Moments
12. Acknowledgments
13. Appendix: Russian Platforms
Exposing Secondary Infektion
Forgeries, interference, and attacks on Kremlin critics across six years and 300 sites and platforms

Dedication
The authors dedicate this report to the growing community of online investigators of information operations on social media around the world. Whether working as journalists, researchers, analysts, and site integrity/trust and safety teams at the tech platforms, as academics, or as private citizens, their dedication, creativity, enthusiasm, courage, and humor are a constant inspiration to dig deeper and document rigorously. Thank you for going down the rabbit hole with us: knowing that you're reading and riding along makes the pursuit worthwhile!
Secondary Infektion at a Glance
A collection of information operations on social media run from Russia by a central entity

Key Highlights

6 Year Campaign
Began in January 2014, extended into early 2020

2,500 Pieces of Content
Posted at least 2,500 pieces of content in seven languages across over 300 platforms

Primarily Burners
Most accounts were single-use burners that they abandoned after one post rather than inauthentic but well-developed personas

Additional Highlights

> Used fake accounts and forged documents to sow conflict between Western countries
> Most often targeted Ukraine
> Was active on campaigns including the US election of 2016, the French election of 2017, and the Russian attempt to discredit the World Anti-Doping Agency (WADA)
> Consistently used sophisticated techniques to cover its tracks but struggled to achieve any measurable engagement
> As yet unattributed to a specific actor

Information Operations Focused on Nine Main Topics

Ukraine as a failed or unreliable state
U.S. and NATO aggression or interference in other countries
European divisions and weakness

Elections
Migration and Islam
Russia’s doping scandals in sporting competitions

Turkey as an aggressive, destabilizing force
Defending Russia and its government
Insulting Kremlin critics including Alexei Navalny and the Bellingcat investigative group
Executive Summary

“Secondary Infektion” is the name given to a long-running Russian information operation, encompassing multiple campaigns on social media run by a central entity, which was already active in 2014 and that was still running in early 2020.

Secondary Infektion targeted countries across Europe and North America with fake stories and forged documents. Its focus and areas of interest were often of a diplomatic and foreign policy nature; it appeared primarily aimed at provoking tensions between Russia’s perceived enemies, and its stories typically concerned relationships between governments and often specifically focused on government representatives. It is also notable for launching smear campaigns against Kremlin critics, and for targeting presidential candidates in 2016 in the U.S., in 2017 in France, in Germany, Sweden and elsewhere.

Little is yet known about the central entity behind the operation; its identity is the single most pressing question to emerge from this study.[16] The Facebook security team uncovered a small cluster of accounts run by the operation for the first time in May 2019 and provided the original attribution to actors based in Russia. This in turn enabled others to identify related clusters and stories linked to Secondary Infektion in late 2019 and early 2020. From November 2019 to May 2020, the Graphika team uncovered over 2,500 pieces of content that Secondary Infektion posted across six years, seven languages, and more than 300 platforms and web forums, from social media giants such as Facebook, Twitter, YouTube, and Reddit to niche discussion forums in Pakistan and Australia, providing an unprecedented view of the operation’s breadth and depth.

This report is the first systematic examination of Secondary Infektion’s campaigns. It reveals the most comprehensive picture yet of this actor’s strategic objectives and tactical priorities across the years.

The scale of the operation is impressive, but the range of topics it focused on was relatively small. In descending order of frequency, the operation posted about nine main themes:

- Ukraine as a failed state or unreliable partner
- The United States and NATO as aggressive and interfering in other countries
- Europe as weak and divided
- Critics of the Russian government as morally corrupt, alcoholic, or otherwise mentally unstable
- Muslims as aggressive invaders
- The Russian government as the victim of Western hypocrisy or plots
- Western elections as rigged and candidates who criticized the Kremlin as unelectable
- Turkey as an aggressive and destabilizing state
- World sporting bodies and competitions as unfair, unprofessional, and Russophobic

While active on Reddit, Medium, Twitter, Quora, Facebook, and YouTube, Secondary Infektion used blogging forums more extensively than it used the main social media platforms. It typically worked by posting false and politically explosive stories—often based on images of "leaked" documents—on internet forums and then amplified them in various languages across a range of platforms. The “leaks” typically exposed some dramatic geopolitical scandal, such as a prominent Kremlin critic’s corrupt dealings or secret American plans to overthrow pro-Kremlin governments around the world. On most occasions, the operation created a new account to post each version of the story and abandoned each account as soon as it had posted. We found no evidence of Secondary Infektion using ads to amplify these stories.

The earliest traces of Secondary Infektion activity online point to campaigns targeting the Russian opposition in early 2014. When Russia annexed Crimea in February-March 2014, Secondary Infektion shifted to attacking Ukraine, first in Russian and then in English and German as well. With time, it added more targets and more languages, reaching its peak production in late 2018 and early 2019. In May 2019, Facebook exposed the first assets.[2] Working out from those leads, the Atlantic Council’s Digital Forensic Research Lab (DFRLab) produced the first substantial cross-platform analysis.[3] After that exposure, Secondary Infektion cut back sharply in output, but it was still posting at a lower rate in early 2020. One of its latest posts accused the United States of creating the Covid-19 coronavirus in a secret weapons lab in Kazakhstan, in a striking return to the operation’s intellectual roots.[4]

Like the Russian Internet Research Agency[5] and Russian military intelligence (commonly known as the GRU),[6] Secondary Infektion paid attention to elections and attempted to disrupt these democratic processes—in the United States in 2016,[7] in France in 2017,[8] and in Sweden in 2018,[9] among others. That noted, election interference was never the operation’s main focus. Far more, it aimed to exacerbate divisions between countries, trying to set Poles against Germans, Germans against Americans, Americans against Britons, and absolutely everyone against Ukrainians.

Forged Documents

Secondary Infektion stands out for its routine use of forged documents, sometimes surprisingly poorly crafted: in this regard, it is reminiscent of the early history of Russian active measures.[10] Other actors have at times used forged documents in deceptive online campaigns, but none have used this tactic with such volume, consistency, and persistence. Graphika has identified more than 250 suspected forgeries, from letters to petitions, that the operation launched online.
The operation impersonated many Western leaders in its creation of forgeries. It included fake letters, tweets and blog posts from leaders and officials including US Secretary of State Mike Pompeo, former White House Chief of Staff General John Kelly, various members of the US Senate Foreign Affairs and Intelligence Committees, representatives of the German, British, and Ukrainian governments, and former national leaders including Carl Bildt (Sweden) and Mikheil Saakashvili (Georgia).

Screenshot of a tweet attributed to U.S. Senator Marco Rubio, accusing the UK of interfering in the U.S. midterm elections of November 2018. Secondary Infektion used the screenshot as the basis of articles alleging UK interference with U.S. elections.\(^\text{(1)}\)
Forged letter attributed to members of the US Senate Foreign Affairs Committee and addressed to then-Secretary of State John Kerry, urging him to support exiled Turkish cleric Fethullah Gülen against the Turkish government. The letter was embedded in Secondary Infektion stories in English[12] and Russian[13] in early 2016, at the height of Russia’s anti-Turkish campaign.
A fake blog post attributed to Swedish politician Carl Bildt and posted by Secondary Infektion in November 2018. The text of the post is the work of the operation and calls for a “Mueller Commission”-style investigation into alleged interference in the Swedish election, but the headline is that of an original Carl Bildt blog referring to the Syrian conflict. It is likely that Secondary Infektion took a screenshot of the blog and photoshopped their own text in, but omitted to change the headline.

The operation also published forged documents, images and videos that it attributed to a wide range of non-governmental organizations, from the World Anti-Doping Agency (WADA) and Organization for Security and Cooperation in Europe (OSCE) to the Committee to Protect Journalists (CPJ) and environmental group Greenpeace.
Almost none of those efforts achieved measurable impact. Particularly between late 2016 and early 2020, Secondary Infekton relied on high OPSEC single-use burner accounts for almost everything it posted (it typically created, used and abandoned each account in less than an hour). This meant that the operators never had the chance to build an audience: each time they created a new account, they effectively reset their following to zero. It would be hard to envisage a less viral strategy. In all its years, only one Secondary Infekton effort really achieved traction in the mainstream discussion of targeted countries: the leak of apparently genuine US-UK trade documents on the eve of Britain’s general election in 2019, as exposed by our team in November 2019. Another enduring mystery around the operation is what the operators thought they were doing and why they kept on doing it across six years of activity when their stories so often died unnoticed.

Unique Features

Secondary Infekton is unique for the sheer range of platforms on which it posted: no other operation from any country that Graphika has studied even comes close. This operational feature could have been a security measure, as it reduced the impact that any one platform could have on the operation and simultaneously rendered coordinated enforcement and investigations harder.

The operation’s lack of viral engagement also sets it apart. Almost none of the operation’s posts across six years of activity achieved any measurable engagement, in terms of shares, likes and positive reactions across platforms. This may indicate that the operators were not interested in engagement metrics - for example, if they were driven by production quotas rather than engagement targets - or that they were using some other form of metrics not visible to outside observers. The lasting mismatch between effort expended and apparent impact gained is yet another mystery about this operation.

Secondary Infekton is also remarkable for its high operational security (OPSEC): multiple social media platforms who partnered with our team on this investigation have observed that the people behind this operation were sophisticated at hiding their traces consistently across the years. As of May 2020, this operation has not been directly attributed to a particular actor or entity. A number of converging signals, from digital forensics indicators identified by our team or provided by the platforms to the clues of language, content, and context, help establish that the operation was run from Russia, but which organization(s) and individual(s) within Russia are responsible is still unknown.

The high OPSEC also made it difficult to expose the full scope of the operation. Secondary Infekton deployed single-use burner accounts so consistently that moving from one campaign, forgery, and story to the next proved difficult, because most accounts only posted one article each. Reconstructing the broader picture of the operation presented a significant and time-consuming investigative challenge. This report is the first large-scale analysis of Secondary Infekton to look beyond anecdotal descriptions of individual stories and identify its systematic patterns.

Nevertheless, our report remains a snapshot and its limitations must be considered: alongside additional stories by the operation that may remain to be discovered, it is highly likely that a significant chunk of the operation’s archives and traces have been lost to various types of content moderation and behavior-based enforcement efforts across the years. Secondary Infekton’s posts were consistently
low-quality, often running afoul of anti-spam rules on platforms and at times generating pushback from other users who came across their content. It is likely that we will never identify all the articles that Secondary Infektion posted. Our hope is that the current report will provide a springboard for more researchers to make more discoveries and bring the full puzzle closer to completion.

Reditors’ reactions to Secondary Infektion piece “The Trojan Pony of Brexit.”[9] We have obscured the names of users unaffiliated with the operation.

To enable further discoveries, Graphika is sharing, alongside this report, a database of the articles that we have identified as parts of the operation and a repository of the visual assets included in those articles.

No one actor in this space has a monopoly on insights and information. As influence operations try harder to hide, all the different actors will have to work together more closely to keep on finding them.
Lessons Learned and Questions Unanswered

Secondary Infektion teaches us a number of important lessons about information operations and the democratic response to them, but it also leaves a number of unanswered questions.

First, and most importantly, it is a reminder that not all influence operations go viral: Internet users on fringe forums are not as easy a target as might be thought. Repeatedly in the course of this research, Graphika came across comments below Secondary Infektion stories that questioned or ridiculed them, or called them out as “Russian trolls.” If Secondary Infektion was aiming at viral impact, it failed. It is therefore especially important to maintain a sense of perspective when crafting responses to such online operations.

Second, our work on Secondary Infektion illustrates the value of exploring the early history and development of information operations on social media to inform and refine our understanding of them. The operational research community has made great strides in exposing online influence operations and operators since 2016, but the study of earlier periods remains patchy and under-researched.

It also confirms that the threat environment is more complex and nuanced than is often described. Secondary Infektion is a Russian operation, but it has very different tactics, techniques, and procedures from the Internet Research Agency or the operations attributed to Russia’s GRU military intelligence: it was far less engaging than the Russian IRA and far less focused on military operations or genuine leaks than the GRU. And Russia is only one source of threat actors among many. Iran’s operations on Western social media began before Russia’s; China has long dominated its own platforms and has begun to operate more aggressively on Western ones. Political parties in Western countries have been exposed running their own domestically focused operations. An excessive focus on any one actor distorts and disadvantages studies of the wide range of information operations on social media.

If the threat environment has evolved, so has the defensive network of operational researchers. There are many more researchers in this field than there were in 2016. The platforms are far more aware of the threat of influence operations, have more experience of identifying and exposing them, and are more open to cooperation with external researchers, as this report demonstrates. The exposure of Secondary Infektion was the work of multiple investigative teams both inside the platforms and outside them, and we are grateful to all those who collaborated with our team to expose the scope and details of this operation.

All these factors have implications for future elections, not least the US presidential election in 2020. On the positive side, Western audiences proved remarkably robust against Secondary Infektion’s trademark combination of fake documents and fake accounts. The repeated exposure of Secondary Infektion’s operations by platforms, journalists, and researchers may have triggered the steep drop in output observed in July 2019 and January 2020. If this model can be continued and reinforced, our collective defenses will be in a significantly better state than in 2016.

Nonetheless, online information operations remain a threat to democratic societies. The case of the trade leaks in the UK, mentioned above, shows that Secondary Infektion is a persistent actor that can leverage genuine leaks to create political impact. Moreover, the impact from genuine leaks can be far higher than the impact from social media posts, and responding to them is more complex: platforms can take down fake accounts for inauthenticity or deception, but it would be neither practical nor desirable to expect them to take down reports about genuine leaks, given the real public interest that these can serve. Triaging between what is authentic and forged, in a context in which both are often blended in the same collection, can also take time and create a lag in enforcement. If a hostile foreign actor were to publish leaked documents shortly before the 2020 election, as Russia did in 2016, the onus would be on campaigns, journalists, and the authorities to craft an appropriate response. Yet there has been far less conversation about the risks that leaks pose and the responses that may be needed.

Moreover, Secondary Infektion remains an unidentified threat actor. Despite the work of multiple teams, we do not have a confirmed attribution to a specific group. We therefore do not have a clear picture of its overall capabilities and motives. Key questions remain unanswered: who was behind it? What were they trying to achieve? Why did they let so many of their stories sink without trace on the unregarded backwaters of the internet? Why did they not target some of the other frequent targets of Russian information operations, for instance the Syrian conflict in general and the White Helmets rescue group in particular?

After it was exposed and disrupted in May-June 2019, Secondary Infektion appears to have gone into somewhat of a retreat: the volume of posts decreased, and some of its stories did not appear in English at all. Nevertheless, various open-source researchers and platforms still managed to identify and expose further stories, in November 2019, December 2019 (DFRLab, Reddit and Graphika) and April 2020 (Recorded Future, and the Daily Beast).

This underscores the importance of detailed exposure. By April 2020, multiple different research teams had identified Secondary Infektion’s unique tactics, techniques, and procedures (TTPs) and used them to find likely new assets. Such attention increases the pressure on disinformation operations, makes it more likely that their products will be exposed quickly, and can force them to change their behavior – witness the relative dearth of English-language content in the second half of 2019 and early 2020, compared with earlier periods.
A Note on Attribution

Secondary Infektion was persistent, deliberate, and secretive. The attribution to operators in Russia rests on multiple indicators, both technical and contextual.⁹³

Based on technical signals,⁹² Facebook first attributed the operation to Russian actors in May 2019. In December 2019, Reddit attributed the leak of US-UK trade leaks to the same operation.⁹²

The context and content of the Secondary Infektion campaigns across the years echo that initial attribution. The operation started out working in Russian and targeted the Russian opposition, especially Alexei Navalny. It shifted focus to attacking Ukraine just as Russia annexed Crimea and launched its proxy war in the Donbass.

The content of the campaigns closely mapped Russian preoccupations. The most striking example is the way that Secondary Infektion suddenly began attacking Turkey after Turkey shot down a Russian jet; the downing happened on November 25, 2015,⁹⁴ and Secondary Infektion’s first attack on Turkey came just one week later, on December 1.⁹⁵ But other themes also matched Kremlin narratives: the portrayal of Ukraine as an unreliable partner for the West, the accusations that the United States was interfering in former-Soviet states, and the attacks on the World Anti-Doping Agency and the 2018 Winter Olympics (from which Russia was banned) all coincide uniquely with Russia’s strategic narratives of the period. The attacks on figures including Aleksei Navalny (Russia), Mikheil Saakashvili (Georgia), Jarek Kaczyński (Poland), Dalia Grybauskaitė (Lithuania), and the Bellingcat investigative group are also consistent with an attribution to Russian actors.

The use of language provides supporting clues, in the shape of specific language errors characteristic of Russian native speakers: difficulties with the use of “а” and “те,” as in the phrase “first the Europe, then the world,” difficulties with the word order in questions, as in “Why the truth is concealed?”, and difficulties with the possessive genitive, as in “3.15 million Germany’s new citizens.” These specific errors have characterized other Russian operations, notably the Internet Research Agency. They would be wholly insufficient for attribution alone, but can serve as a point of corroboration.

Finally, we took a conservative approach to building the set studied in this report. Each of the pieces of content we retained for the final analysis was characterized by a strong and distinctive common set of attributes, notably the predominance of very short-lived, single-use inauthentic accounts, the wide use of forged documents, the repeated use of the same combinations of websites and blogging forums and the same linguistic idiosyncrasies. In some cases, this was underpinned by the fact that the stories were shared on the subset of Secondary Infektion assets that posted repeatedly, and not shared elsewhere. Only high confidence assets have been included in this set, which results in a set that is likely incomplete, but solid enough to give us a full picture of this activity.

We hope that further research can help identify which entity enabled the high degree of OPSEC and the resources that characterized Secondary Infektion across the years. The operation had enough resources to run for at least six years. It focused on geopolitical and diplomatic cleavages, attacked Kremlin opponents, and prioritized secrecy over engagement. These features are insufficient for a precise attribution, but they sketch out an organization with significant resources and persistence, professional OPSEC, a geopolitical focus, and little apparent pressure to generate viral content.

To see how Secondary Infektion related to real-world events and other known Russian information operations, see the timeline.
Secondary Infektion began in early 2014 and was still posting in early 2020. Over the six years of its existence, it posted a vast quantity of content on a wide range of topics and across a dizzying number of platforms and forums: over 300, according to the latest findings in April 2020.
The stories it created were nothing if not eye-catching. They claimed, for example, that extremist Remainers were plotting to *assassinate Boris Johnson*,[^34] that Ukraine was lobbying for President Petro Poroshenko to win the *Nobel Peace Prize*,[^37] and that the EU was lobbying for German Chancellor Angela Merkel to *do the same*[^38] that Merkel was an *alcoholic*[^39] and that Poland’s ruling Kaczyński twins suffered from a genetic disorder that made them *mentally unstable*.[^40] Many more examples can be found in the database.

The campaign was not static: the subjects it dealt with shifted over time, although Ukraine was a perennial target. They largely reflected Russia’s foreign policy priorities. Between 2016 and 2018, when Russia was engaged in a diplomatic dispute with Turkey, Secondary Infektion picked more Turkish targets; in 2016, when Russian information operations targeted the US presidential election by trying to undermine Hillary Clinton’s presidential campaign, Secondary Infektion attacked Clinton too. As a notable exception, the operation featured a surprisingly small amount of Syria-focused content.

Its main goal appears to have been to inflame tensions between or within countries the Kremlin perceived as hostile, and it ranged widely in search of fuel. It posted articles on the *Armenian genocide*,[^41] *terrorism in Northern Ireland*,[^42] World War Two-era *mass killings* and reparations around Poland and Ukraine,[^43] *accusations of sexual violence* committed by Muslim refugees,[^44] *Scottish independence*,[^45] and *US espionage* and interference against its allies.[^46]

Despite this wide geographic range, the themes it selected closely matched those of other known Kremlin information operations of the period. For example, it started to attack Turkey after Turkey shot down a Russian jet in November 2015 and it took an interest in sports after the World Anti-Doping Agency (WADA) exposed a Russian state-sponsored doping operation in 2016. In 2016, it attacked Hillary Clinton’s election campaign and focused on attacking Emmanuel Macron ahead of the French elections in 2017. It did not copy or amplify those other operations: it approached the same targets, but in its own way.

The database that accompanies this report is divided into nine categories according to the most prominent theme of each article:

- Ukraine as a failed or unreliable state
- US and NATO aggression or interference in other countries
- European divisions and weakness
- Elections, especially in the United States, United Kingdom, and France
- Migration and Islam
- Russia’s doping scandals in various sports competitions
- Turkey as an aggressive, destabilizing power
- Defending Russia and its government
- Insulting Kremlin critics, including Aleksei Navalny and Angela Merkel
Breakdown of Secondary Infektion articles by theme and number.

Despite the frequency with which Secondary Infektion assets in one language copied content from assets in other languages, the division of topics was not uniform. Ukraine was the most popular theme across the network, being consistently portrayed as corrupt and unreliable and run by Nazis, but posts in German also focused heavily on US interference and aggression, while posts in French and Spanish focused more on divisions within Europe. English-language content divided roughly evenly between attacks on Ukraine, reports on divisions in Europe, and accusations of US aggression or interference.
The targets shifted with time. Ukraine bore the brunt of the early coverage, especially in the critical months after Russia annexed Crimea and launched its proxy war in the Donbass in 2014. Posts about weaknesses and divisions in Europe surged in the second half of 2016, and still more in early 2018. Stories about US interference and aggression were present from the outset but peaked in late 2018.

This paints Secondary Infektion as a dynamic operation, shifting its targets in line with evolving Russian narratives, most notably concerning Turkey. It did not exist in a vacuum, even though many of its stories may as well have been posted into one: it tracked real-world events and tried to react accordingly.

**Ukraine as a Failed or Unreliable State**
Ukraine was Secondary Imfektion’s most consistent target. The operation began while the “Maidan” revolution was still in its infancy, and throughout its life, it posted stories that presented Ukraine as a failed state, an unreliable partner, or a thinly veiled Nazi dictatorship.

**Jewish exodus from Ukraine**

Large-scale migration of Jews from Ukraine has been noted as far back as 2014 when more than 6 thousand people left the country. However this year it has surged significantly. In all, Jewish migration has increased by 215% during the first three months of 2018.

**Ukraine after presidential elections. Radicals threaten national minorities**

On May 20, Volodymyr Zelensky took the presidential office. Taking into account he is a new man in politics, and therefore challenging, it is hard to imagine what Ukraine’s both domestic and foreign policy will look like during the next five years (that is the presidential term in Ukraine). However, the first decree of the new leader of the state on dissolution of the Parliament has caused a wave of argument among political experts and journalists. It is clear the new President does not like the old Parliament, and re-elections were just a question of time. However, besides political difficulties, there are a lot of unsolved issues the presidential team has come across. The status of national minorities and the activity of nationalist groups are some of issues.

**US/NATO Interference in Other Countries**

Secondary Imfektion repeatedly accused the United States of aggression against, or interference in, other countries around the world. The accusations ranged from espionage to sponsoring “color revolutions” in former-Soviet countries. Sometimes, NATO or the United Kingdom was portrayed as an accomplice or a main perpetrator.

**Posts on US and UK interference from Reddit (left) and indybay.org (right).**
Divided Europe

Secondary Infektion often targeted divisions in Europe. Some were political, such as Scottish and Catalan independence. Some were ethnic, such as the Armenian genocide and the bloodshed between Poles and Ukrainians during World War Two. Some were historical, such as Poland’s demands for war reparations from its neighbors. Other posts accused the EU of betraying its own principles or its international partners.

Elections in Focus

Relatively little of Secondary Infektion’s content dealt with elections: the operation seemed more concerned with other divisions, especially diplomatic ones, and with attacking official and diplomatic figures, such as heads of state and ambassadors.

The main exceptions were the US presidential election in 2016, when it attacked Hillary Clinton, and the French election in 2017, when it attacked Emmanuel Macron; it occasionally mentioned other elections, largely as a way of undermining the legitimacy of the country in question.
Migrants and Muslims

Secondary Infektion posted negative content about immigration in general, and focused on specific targets, such as Muslim refugees, in particular. These posts typically linked such communities with terrorism and sexual violence. The intent appears to have been to stir up racial and religious conflict in the target countries.

This content appeared crafted to inflame, although it typically failed to achieve any traction. One article posted in February 2016, for example, claimed that extremist Muslim clerics had urged Muslims to “take the women of infidels!” on St. Valentine’s Day.[6] It was based on a screenshot of an alleged online post for which no original can be found; we assert with high confidence that this was a forgery created by the operation. Another article alleged that Norwegian far-right mass killer Anders Breivik had summoned Europeans to an anti-Muslim crusade; again, it was based on a screenshot of a “document” that only ever existed in Secondary Infektion posts.[6]

Another wave of immigration to hit Europe as EU leaders admit they are powerless in Aleppo

Posts on migrants and Islam in May and December.[6]
Clear examples of this are the calls made by radical Muslim clerics to attack European women on St. Valentine’s Day, 14 February. They have been published by a number of Islam-related websites.

Fake documents alleging Muslim intolerance and aggression, February and May, 2016.[64]

Curiously, a Twitter account that appears to have formed part of the operation - in that it almost exclusively tweeted Secondary Infektion content - tagged the article on the “Valentine’s Day threat” to a number of influential Twitter users.[65] These included @Jenn_Abrams, one of the Russian IRA’s most popular creations. This is insufficient to suggest a connection between Secondary Infektion and the Russian IRA, but it is noteworthy.

Tweet by suspected operation account @indeexp to @Jenn_Abrams.

**Turkish Aggression**

After Turkey shot down a Russian jet on November 24, 2015,[66] Russian state outlets launched a campaign to label Turkey as a rogue state, in league with Islamic State terrorists and selling them oil.[67] In late 2015 and through 2016, Secondary Infektion ran a series of blogs attacking Turkey as colluding with terrorists, destabilizing the region, and/or abusing the Kurds.
Russia's Doping Scandals

A few articles addressed sporting issues, especially those that had emerged as an international embarrassment to Russia. The 2018 Winter Olympics, discussed below, bore the brunt of the coverage, but Secondary Infektion also targeted the World Anti-Doping Agency after it found Russia guilty of massive doping violations in late 2015 and early 2016. These posts featured forged documents from WADA and the Committee for the Protection of Journalists.

In July 2016, after WADA had announced its findings, Secondary Infektion posted a blistering attack on the Rio Olympics: “These sporting events surely would be the most dishonest and politically biased campaign over the whole sporting history.” The article accused WADA of taking its decisions “in order to make the distribution of medals more politically orientated.” As we will see in the discussion of the Winter Olympics below, Secondary Infektion did not take losing well.

Defending Russia

More broadly, one of Secondary Infektion’s lines of effort was to defend the Kremlin against its critics, both external and internal, by mocking them (discussed in the following section), comparing them unfavorably with Russia, or trying to discredit them.
The operation paid particular attention to those who had exposed it. In July 2019, the “Blue Man” persona - Secondary Infektion’s most prolific and long-lasting asset, described below - published an attack on the Atlantic Council’s DFRLab for exposing the operation in general, and the “Blue Man” in particular. The blog attempted an ironic tone: “Yes, the ‘forensic experts’ were wrong about almost everything, but they thought the existence and spread of a different opinion from their employers was a serious threat, and Devil take it, that tickles my pride.” Despite the tone of defiance, this was the persona’s last post.

The attempt at gaslighting those who exposed it is uncommon, but not unheard-of in Russian information operations. “Jenna Abrams,” one of the Russian IRA’s most notorious personas, posted a similar through-the-looking-glass blog in November 2017. In November 2018, the Russian IRA launched a website that claimed - against all the evidence - that it had managed to interfere in the 2018 midterm elections in the United States. None of these efforts appears to have resonated with a receptive audience.

Insulting Kremlin Critics

When it came to individuals who criticized or defied the Russian government, Secondary Infektion went beyond its usual focus on international tensions to personal targeting. This applied to critics both inside and outside Russia, underlining once more how Russia’s information operations had domestic roots as well as foreign-policy ones.

Aleksei Navalny

Secondary Infektion consistently portrayed Navalny as criminal and corrupt, not caring about his supporters, and being under the control of and in the pay of the West. At the same time, one attack on him involved a fake letter from one EU official to another saying he should not be awarded a prize as he is an “odious nationalist.”
The European continent is experiencing a great rise of the right populism. The power has already been taken by the right parties in some countries, while in other countries they're just getting possibility to influence the national policy. If earlier it referred only to countries in Eastern Europe, then today strengthening of right parties may be shown up by Denmark (Danish People’s Party), Italy (Lega Nord), Austria (Freedom Party of Austria), and even Germany where the Alternative for Germany has become the main opposition power. The National Rally’s leader Marine Le Pen could break on through to the second tour during the presidential elections of the last year where it was Emmanuel Macron who could only make her to give up. The Swedish democrats took another toll on the EU by achieving superb results in the elections to the Riksdag.

Left, article published by Secondary Infektion claiming that EU Commissioner Johannes Hahn had called Navalny an “odious nationalist”; right, the embedded letter attributed to Hahn.\[80\]

12 июня в городах России пройдут митинги оппозиции организованные Алексеем Навальным. Что насамсяя проведению мероприятия в Москве, по оно пока не согласовано с МВД и, если ужемять показать ФБК, разрешение вряд ли будет получено. Массовые акции на Тверской улице в праздничный день сохраняются с целью обозначения проблем, связанных с обеспечением общественной безопасности. Разумеется, акция предполагает перемещение митинга на несколько кварталов, что не устроило организаторов. В очередной раз согласование.

Navalny portrayed as being controlled by the West (left)\[65\] and the Kremlin (right)\[62\]

Dmitry Medvedev

One of the strangest parts of Secondary Infektion - an operation that was often bizarre - was when it began to attack Russian Prime Minister Dmitry Medvedev. This was a brief burst of activity in the summer of 2018, the reasons for which are not fully clear. The pattern of tradecraft was identical with known Secondary Infektion stories of the period and was spread across five languages. The incident is described more fully in our “vignettes” section.
Memes attacking Medvedev that appear to have been created by Secondary Infektion, in that they have not been found online anywhere before the operation used them.[83]

Angela Merkel

Angela Merkel was another frequent Secondary Infektion target. She was not attacked as systematically as Navalny, but the operation periodically posted about her with texts and cartoon images, portraying her initially as undemocratic and then as the one who was to blame for the migration crisis. One article even suggested that she was an alcoholic (an accusation the operation also made against Medvedev). The attacks peaked in the first half of 2017, shortly before Germany's federal elections.

Chancellor of Germany and female alcoholism.

While looking through the Dr. Sperling article you are staying under persistent impression it's got the description of quite a familiar person.

Jarosław Kaczyński

Secondary Infektion also took a medical approach to attacking Jaroslaw Kaczyński, the head of Poland's ruling Law and Justice party (PiS) and an outspoken Kremlin critic. Starting in early 2015, the operation began circulating the conspiracy theory that he suffers from a genetic disorder that manifests in “high excitability, uncontrolled manifestation of panic and aggression.” The operation built its story up over some months, spreading articles and forgeries in multiple languages and inventing a “leak” on cyberguerrilla.org, a video on Vimeo, and even a petition on avaaaz.org.[87]
Mikheil Saakashvili

Saakashvili has long been a target for Kremlin information operations. Secondary Infektion depicted him as having been a corrupt failure in his native Georgia who was touring other new democracies looking for lucrative opportunities or trying to cause trouble in Georgia. He was also painted as fighting a losing battle against Ukraine's oligarchs to bring about democratic reform.
Saakashvili did not receive Hahn's assurances that 'interim' Groysman’s Cabinet resigns in 2017...

Many Ukrainians and their foreign partners have been dissatisfied with a new Cabinet of Ministers appointed after Yatsenyuk’s resignation. The main critic of the government is Mikhail Saakashvili who currently holds office of Odesa Region’s Governor.

Left, story involving an alleged letter from Saakashvili to EU Commissioner Johannes Hahn claiming that oligarchs had influenced the formation of Prime Minister Groysman’s cabinet.[90] Right, supposedly a report by Saakashvili to the OCSE saying Ukrainian Prime Minister Yatsenyuk was a source of corruption.[91]

Dalia Grybauskaitė

Secondary Infektion’s attacks on female politicians were notably sexist. In this regard, they regrettably echo a well-established pattern of information operations on social media leveraging sexist tropes to attack female politicians around the world.

The operation frequently attacked then-Lithuanian President Dalia Grybauskaitė, accusing her in turn of being supported by the CIA,[92] a KGB informer, a former prostitute, an agent in hock to the Chinese government, and working against the European Union - especially after Lithuania was found complicit in the CIA’s secret detention, rendition and torture program by the European Court of Human Rights.[93]
The network also spread the narrative that Grybauskaitė was a KGB informer and prostitute, using an already debunked KGB “letter” claiming that the former Lithuanian President had been detained alongside two other USSR citizens and three Finnish girls for “immoral behavior in public places” in 1982. The letter came back into the spotlight in 2019, after Sputnik released a video featuring it, and was later shared by networks of pro-Russian outlets. According to Secondary Infektion’s German-language blog “Politgraben,” the arrest was a sign that Dalia Grybauskaitė was working as a KGB informer during her studies in Moscow, especially since she was not expelled from university after the arrest. Russian-language personas amplified the KGB claim but not the prostitution narrative.


Extract from the Politgraben article “ADIEU, KGB! FLIEIT DALIA GRYBAUSKAITĖ VOR IHRER KGB-VERGANGENHEIT?” (“Adieu, KGB! Is Dalia Grybauskaitė fleeing from her KGB past?”). The underlined text, highlighted by Graphika, reads: “Note the description below: ‘The procedure was terminated on the order of the KGB curator.’ It is known that the Party often used prostitutes as informers, which explains the fact that the student was not expelled from the aforementioned university despite the scandal.”

Sidebar: False Leaks

Most of Secondary Infektion’s content dealt with “leaks” that never were - what we refer to as False Leaks: documents, either stolen or fabricated, presented as leaked materials. Throughout its lifespan, the operation posted forged documents that it claimed to have acquired from hacktivists; it is no coincidence that its early personas included “Anonymous Europe,” “Cyber Legion,” and “Anonymous Ukraine” or that it posted to cyberguerrilla.org so frequently.
At the same time, the operation paid little attention to genuine leaks from Russian (or any other) sources. It barely mentioned the DNC and Podesta leaks during the 2016 US election, the leak of WADA content in 2016-17, or the Macron leaks of May 2017. The overlap in these topics is discussed in the section on “Campaigns and Competition.”

The exception to this rule is the operation’s leak of US-UK trade documents in October 2019. This was Secondary Infektion’s only known use of genuine documents; it was also the operation’s only known high-impact effort. As of May 2020, it was still unclear how the documents had been obtained. Further information on this point may shed light on why Secondary Infektion departed from its normal procedures in this case, and who was behind the operation.
Highlights: WADA, Clinton, Macron

Secondary Infektion sometimes focused on issues that were targeted simultaneously by other known Russian information operations, including that of both the Internet Research Agency and the various actors within Russian military intelligence who were responsible for hacking and leaking politically important documents. \[102\]

This was not a question of Secondary Infektion amplifying or repeating posts made by other Russian operations; rather, it directed its efforts toward the same targets, albeit with a different approach, using its own unique combination of forged documents and fake accounts, even when genuine leaked documents might have been available.

For example, in November 2015 the World Anti-Doping Agency (WADA) published a report that accused Russia of systematic state-sponsored doping in the 2012 Olympic Games. \[103\] In July 2016, a follow-up report accused Russia of the same practices at the 2014 Winter Olympics and recommended that Russia be banned from future competitions, including the 2016 Olympics in Rio de Janeiro. \[104\] The accusations triggered a full-spectrum Kremlin information operation that included deploying hackers from Russian military intelligence to break into the servers of the International Olympic Committee (IOC) and a Rio 2016 account of WADA’s Anti-Doping Administration and Management System, and the creation of the “Fancy Bears Hack Team” persona to leak the hacked materials to journalists. \[105\] Accounts from the Internet Research Agency also joined on the #dopingleaks campaign, operating side by side, albeit without evident coordination, with accounts operated by the GRU. \[106\]

Before the GRU hackers deployed against WADA and the IOC, Secondary Infektion forged a false leak that appeared intended to discredit the doping agency. In April 2016, the operation ran a story in English, German, and Russian that alleged that WADA had colluded with the giants of the pharmaceutical industry to ban the drug “meldonium,” also known as “Mildronate,” in order to undermine it as a competitor. \[107\]

Unfortunately, bribery of top-ranking officials in anti-doping organizations community appears nowadays to be a usual business. (...) As for unfair competition in pharmacology, here we undoubtedly face absolutely new level of corruption.

The article embedded a letter allegedly sent by the head of the Committee to Protect Journalists, Joel Simon, to WADA head Sir Craig Reedie, together with a memo attributed to WADA’s finance committee. \[108\] The letter from Simon accused WADA of orchestrating a harassment campaign against journalists covering the scandal, but offered to cover up the affair in return for an end to the harassment, “for we see it as totally unacceptable and insecure to discredit the international institutions under the current political situation being so tense.” The memo from WADA accepted these surrender terms and discussed how to find out which journalists were involved, and how to keep them quiet. Both WADA and the CPJ confirmed to Graphika that the documents were fake.

![Image of WADA and CPJ logos]

The headers of the “memo” (left) and the “letter” (right) embedded in the false story.

WADA spokesman James Fitzgerald told Graphika, “a matter raised by a journalist body in relation to the pharmaceutical industry or a substance on the Prohibited List would not be one for the Finance & Administration Committee to consider. In addition, letters or memos sent to our various Standing Committee members do not look like this. And finally, the fact this document is so poorly written, with several grammatical errors, would be another clue.”

Typically for Secondary Infektion, the claims were not picked up beyond its own cluster of usual websites. \[109\] This is a significant contrast with the GRU’s later leaking of apparently genuine documents, which achieved widespread coverage, not least because the GRU shipped the leaks directly to willing journalists \[110\] or with some of the Russian IRA’s personas traction within the communities it sought to target (such as Jenna Abrams’ online musings on the “doping leaks”).

© Graphika 2020
Similarly, in early 2017, a range of Russian information operations began attacking French presidential candidate Emmanuel Macron after he emerged as the surprise leader in the election. In the words of the director of the French Institute for Strategic Research (IRSEM, at the French Ministry of Defense), Jean-Baptiste Jeangene-Vilmer, “There was a coordinated attempt to undermine Macron’s candidacy, through a classic three-dimensional information operation: (1) a disinformation campaign consisting of rumors, fake news, and even forged documents; (2) a hack targeting the computers of his campaign staff; (3) a leak—15 GB of stolen data, including 21,075 emails, released on Friday, May 5, 2017—just two days before the second and final round of the presidential election.” As part of the disinformation (or “information manipulation”) campaign, Jeangene-Vilmer catalogued a series of false, misleading, or biased claims about Macron that were amplified by Kremlin outlets from late January 2017 onward.

Separately from these attacks, Secondary Infektion launched three separate stories that targeted Macron in March through May 2017. This was the only time in the operation’s six-year history that it focused on the French politician, suggesting that this newfound focus was driven by the electoral timeline.

The attack initially focused on immigration, especially by Muslims, a key theme highlighted by supporters of Macron’s rival Marine Le Pen. On March 16, the operation ran a story headlined, “Emmanuel Macron: the new hope of migrants in Europe?” This was posted in unidiomatic English the same day by single-use burner accounts on Medium, Quora, survivefrance.com, politicalforum.com, and politicalforum.co.uk and in German the following day on meine-news.de and geschichte-wissen.de.

The article claimed that Macron had written an attack on Merkel for not doing enough to take in migrants and asked “whether such a short-sighted statement by the ambitious candidate is going to make the immigrants assault French borders soon?” However, the “attack” it cited was written in clumsy, grammatically incorrect French and posted by a single-use burner account called “Gerard” two days earlier: it bears all the markings of posts crafted by Secondary Infektion.

On April 20, the operation planted a story that Macron was prioritizing political support from migrants over French national security. This was posted in English on Reddit (which first exposed the post), defendingthetruth.com, politicsforum.org, and homment.com. It was based on a screenshot of an “official document” that showed that the number of Muslims acquiring French citizenship had soared; once more, the use of French was clumsy and grammatically incorrect. (The screenshot can no longer be viewed in the English-language versions but remains visible in the Russian-language editions.)
On the eve of the final round of the election on May 6, 2017, just after Russian hackers dumped the “Macron leaks” online,[20] the operation launched a pseudo-analytical piece arguing that Macron was “an embodied synthesis of industrial and banking PR-technologies and pan-European red-tape lobbyists.”[21] Rather than focusing on migration and Islam, it focused on his background and alleged character as a “synthetic media homunculus that matches all criteria of a negative political selection.” The author concluded by posing as a French citizen who was outraged at Macron’s progress:

I am not a fan of Marine Le Pen. I’ve never desired to experience her election agenda in action. Yet I firmly believe that the choice is up to a nation and no one else. Even if the nation makes a fatal mistake. Anyone usurping this sacred right is a criminal liable to penalty. This is what should be told to the face of those who tries hard to make fools out of us imposing outside and strange choice on France.

None of these stories gained significant traction. It is noteworthy that Secondary Infektion did not mention or amplify the Macron leaks, either before the election or afterward. Its attacks on Macron also did not pick up on the themes amplified by other parts of the Russian influence apparatus.

A third example similarly highlights how Secondary Infektion paralleled other Russian operations, seemingly without coordination. In 2016, while the GRU and Russian IRA were both running large-scale campaigns to undermine the candidacy of Hillary Clinton and divide the American electorate, Secondary Infektion did the same. Repeatedly from November 2015 through November 2016, it posted attacks on Clinton. However, these posts barely mentioned the GRU’s hacks and leaks, and available archives of IRA posts[22] show no mention of Secondary Infektion’s stories or personas.
The attacks started on November 26, 2015, with an article that combined outspoken anti-Clinton sentiment with clumsy, unidiomatic English. Unsurprisingly, it did not appear to gain traction:

"The most warmongering lady ever lived in the White House has been thirsting for returning back in a new role. In 2008, American voters made it clear that they don’t want Hilda east as a U.S. President. But it looks like Mrs. Clinton doesn’t bothers [sic] with such nonsense as Will of the American People. The former First Lady has been showing such stubbornness pursuing this aim that it looks like horns would thrust her brow soon."

This was an early and relatively isolated salvo; unusually, it was not amplified by Secondary Infektion’s contemporary German and Russian personas. In 2016, however, the attacks became more frequent and systematic.

An article in May 2016 accused Clinton of being in the pay of the Saudi regime; a post in June accused her of being allowed to “steal most part of the [Democratic Party] delegates from Bernie Sanders.” One July article argued that Clinton was in China’s pocket and another argued that the GRU’s leak of Democratic emails was actually a Clinton plot to silence Sanders supporters. An August article focused on claims that Clinton had serious health problems. Intriguingly, none of these was based on a forged document.

An article on October 31, 2016, appears to have been based on a fake, but the document in question was a petition, not a screenshot of a document. This article was particularly outspoken, calling the chance that Clinton would win “the most terrible mistake in the modern American history” and accusing her of “blatant impudence, barefaced lie, sordid treachery, scandalous revelations, corruption, and contract killings on top of that.” A translation was posted in Russian by single-use burner accounts to multiple forums used by Secondary Infektion.

The petition in question was created on thepetitionsite.com on or around October 27, 2016 (the petition was undated, but according to the page source, the last date for signatures was October 27, 2017, giving a likely one-year range). It was addressed to the US Supreme Court and attributed to a Libyan who “lost my family and many of my relatives and friends” in Libya’s conflicts. By May 2020, it only had 16 signatures, and the only references to it available online were on posts that can confidently be attributed to Secondary Infektion itself, suggesting that the petition was planted by the operation itself.

Spread of the story from thepetitionsite.com (left) through Reddit, Medium and hamment.com (center) to dosug.md, korrespondent.net, and amigos.lv (right).
The Countries

Beyond the key themes outlined above, with their emphasis on Ukraine, the United States, Turkey, and Russia, Secondary Infektion targeted many other countries. The following section provides a brief overview of the key approaches; full examples to date can be found in the accompanying database.

![Evolution of Secondary Infektion's country targeting.]

Germany

Germany was targeted in a small number of articles, often in the context of friction with Poland and Turkey. The most widespread narratives pushed by the Secondary Infektion network claimed that Germany was being manipulated by critics of the Turkish government - either Kurdish groups[^12] or supporters of exiled cleric Fethullah Gülen[^13] - to undermine its relationship with Turkey, and that Germany was going to be robbed by Poland as the EU supposedly voted for [Germany to pay reparations to Poland for the Nazi occupation][^4].

The effect of the referendum in Turkey: urged by Gülen followers, Germany to impose sanctions on Ankara

by homment | 11.05.2017 | Views: 282

Germany’s staying secretly supportive of the Turkish Kurds

Thursday, December 24, 2015 0:26

Headlines from homment.com and Before It’s News targeting Germany.
The assets also posted some German-centric islamophobic content,[93] focused mostly on the refugee crisis,[94] and claiming refugees were bringing diseases and death to Europe.[95] Other articles from the Politgraben blog directly criticized German mainstream politicians.[96] The blog also targeted islamophobic content at the Nord Rhine-Westphalia region[97] a couple of months after the state government demanded that Politgraben delete an article featuring a forged letter[98]

Poland

The network of Secondary Infektion assets repeatedly attacked Poland, which they portrayed as a country that consistently tried to get the whole international community involved in its disputes with other states. Secondary Infektion articles addressed Poland’s disputes over events that occurred decades ago with Ukraine[99] and Germany[100] and attacked Poland’s leading politician, the conservative and nationalist Jarosław Kaczyński, personally.

Secondary Infektion accused Poland of not following European rules and of jeopardizing joint decisions made by the EU.[101] Poland was also depicted as supporting Turkey’s accession to the EU[102] despite its failures in the area of human rights - in direct opposition to Germany, which was also depicted in a negative way in the article - or using its Soviet past to demand compensation from former Soviet States for the Red Army’s aggression.[103]
Genocide strikes relations between Ukraine and Poland... again

Dariusz Pawlak  Follow
Jan 18, 2018 · 2 min read

Dariusz Pawlak
Answered January 19, 2018

Do Poles and Ukrainians hate each other?
I can't say for sure if ordinary people from both countries hate each other or not, but their political leaders do their utmost to spread hatred.

Poland has proposed a draft resolution at the UN Security Council with a claim to recognize the crimes committed by Ukrainian nationalists against Polish citizens during the World War II as act of genocide.

Examples of content posted by Secondary Infektion about Poland on (top to bottom) Medium, Quora, theapricity.com, and Reddit.

Baltic States

Lithuania
Apart from targeting former Lithuanian President Dalia Grybauskaitė, the network also attacked Lithuania as a country, presenting it as backward and revisionist. Another series of articles, disseminated by persona “Josef Hashever,” argued that the next Lithuanian president should renew strong ties with Moscow.
Latvia

At least two stories shared by the network targeted Latvia. The first piece, distributed mostly on Reddit, promoted a Polish documentary exposing corruption and describing how the government became a central player in organized crime in the Latvian state after the collapse of the USSR. The second piece featured forged letters from the NATO Center of Excellence in Strategic Communications in Riga and portrayed Latvia as attacking the media and wasting money on increasing surveillance over Latvians online, instead of helping the Latvian people and investing in the public sector.

Forged letters posted on homment.com painting the Latvian government as blindly following NATO orders and prioritizing information security over its citizens' needs.
Estonia

The network also shared some articles targeting Estonia, although no article was entirely focused on the country. As with Latvia, Secondary Infektion accused Estonia of being manipulated by NATO in order to increase its capacity to fight information warfare against Russia at the expense of the country’s taxpayers. Another article[60] - originally posted by an independent journalist who wrote a blog on the Russian opposition radio station Ekho Moskvy - aimed to highlight supposed double-dealing by Estonia and Latvia against Russia and the EU in the context of sanctions. We found the Secondary Infektion material targeting Estonia on an Estonian website where we had found other material from the operation, stena.ee. This matches the findings in the report[61] released by Recorded Future on Secondary Infektion operations in Estonia and Georgia.

UK

Secondary Infektion paid sporadic attention to the United Kingdom, with periods of silence followed by more intense bursts of activity. The most notable of these bursts came in 2018, after the British government exposed Russia’s attempt to assassinate former spy Sergei Skripal in Salisbury using a nerve agent, and spearheaded global diplomatic sanctions.[62] The operation had three main narrative threads: the UK as an aggressive imperialist country, often in collision with the United States; the UK as being interfered with by the United States, or interfering there; and the UK as divided over Brexit, Scottish independence, and Northern Ireland.

The logical disconnect between the first two threads is informative, though it is not unique within Secondary Infektion’s oeuvre: it speaks to the operation’s aim of triggering discord between the Kremlin’s critics by any means necessary, even when these were contradictory. Portraying the UK as a US collaborator or servant was a way of stirring up trouble for Britain in Europe and the wider world; portraying it as interfering in the United States, or being interfered with by the United States, was a way to undermine the transatlantic relationship.

Some of the stories were outlandish. One particularly memorable article made the claim that extremist Remainers were plotting to assassinate Boris Johnson.[63] Another claimed that Irish terrorist group the Real IRA was recruiting Islamist militants, in apparent ignorance of the Christian sectarian divide that dominates Northern Irish politics.[64] It is perhaps unsurprising that these stories, like so many others, failed to take off.
Left, a tweet by operation asset "@StevenLaack" embedding a forged document that claimed the United States was spying on the British royal family.

Right, a forged tweet attributed to Senator Marco Rubio accusing the UK of interfering in the US midterm elections of 2018.

Still's from a video most likely created by Secondary Infektion showing Theresa May as a World War One fighter pilot shooting down the EU zeppelin. It was embedded in an article that accused May of a "snake oil pitch about intentions to turn half the planet into radioactive ash instead of attempts to provide the public with a specific plan of action for Brexit."
The British Lion makes a come-back

Concerning the rise of London in the Iran-Saudi Arabia conflict. During the long peaceful period, Great Britain was rather slowly overshadowed by the Big Brother across the Atlantic than forced to side of the main stream road in the world political game. The gripping life story with the EU structures also failed to add more strength to the Foreign Office even in the regions that used to be the British Empire domain. The situation was drastically changed after the cabinet of David Cameron came into power in May 2010. That elegant of the British government which so skillfully managed to bury the foreign ambitions of the French president Nicolas Sarziszy, it is actually worth mentioning as a learning curve to be included into the instruction manuals for future diplomat. Staying fully aware of the tough threat of the Mediterranean Union, the project lobbied by France, able to deprive Britain of control over its military presence along the Gibraltar-Malta-Cyprus line in the Mediterranean, the Cameron government came out with the initiative of the ‘no-fly zone’ over Libya. That was exactly the step to start the NATO mission in Libya, which, when accomplished, resulted in actual running of the Mediterranean Union project and British come-back to active Mediterranean policy. “I think of assessing our might, not are back into the Mediterranean of 1967,” declared David Cameron summing up the results of the Libyan mission in his speech dated October 19, 2011. Since that time, London has been consistently boosting its participation in the Mediterranean and Middle East regions.

Left, article on scoop.it by operation as set “Steven Laack” on British imperialism and dirty dealing in the Mediterranean, with (highlighted) a fictitious quote from then-Prime Minister David Cameron. Right, article on US-UK collusion to prevent United Nations action on the Chagos Islands.

Spain’s Intel: Remainers Plan to Assassinate Boris Johnson

William Couch

In general, Secondary Infektion did not deal specifically with UK electoral politics. However, the operation does appear to have attempted more direct targeting around the Brexit referendum of 2016 and the General Election of 2019. In the former case, two Secondary Infektion personas posted the claim that the British government was cheating ahead of the Brexit vote: “the international community can now witness the distortion of the foundations and ideals of democracy in the country that used to be seen as its cradle.” There is no indication that this article resonated beyond the websites where the operation posted it.

In October 2019, unknown actors leaked a trove of apparently genuine US-UK trade documents on Reddit, homment.com, and meinbezirk.at using a collection of single-use burner accounts. They also used a Twitter account to promote the leak to prominent opposition politicians and journalists using @-mentions. This was exactly the tradecraft perfected by Secondary Infektion.
Graphika and Reuters reported the resemblance[^64], a few days later, Reddit announced that it believed the accounts on its platform were indeed tied to Secondary Infektion.[^65]

The trade leaks closely resembled earlier Secondary Infektion efforts in their online dissemination, but they differed crucially in the use of apparently genuine documents and in the fact that these documents were ultimately emailed to activists and politicians, rather than merely posted online. As such, the trade leaks are an outlier in the Secondary Infektion portfolio and an important reminder that influence operations can be more direct, and yet more insidious, than simply posting on social media.

**South Caucasus**

**Georgia**

Secondary Infektion painted Georgia as a country not yet ready to join the European Union and NATO, mostly for being too soft in its relationship with Russia and its failure to "defend western values in the face of the threat coming from Russia," as well as being untrustworthy because of rampant corruption.

> Georgia demonstrates lack of readiness for its membership in the EU and NATO

Statements of the front-runner of the presidential race Salome Zurabishvili as if in 2008 Georgia bombed its own citizens in South Ossetia leave no illusion as to the key vector of the country's foreign policy right after the recent presidential elections. Undoubtedly, in the near future the lack of hardline anti-Russian rhetoric on the part of the Georgian authorities can put paid to any perspectives of Georgia's membership in the EU and NATO. September visit of Prime Minister of Georgia Mamuka Bakhtadze to the USA is certainly aimed at remedying the situation and removing any criticism about Georgia's sabotage of anti-Russian initiatives. But chances of Georgian political elite to restore the trust of Washington are next to zero because of the wasted time and resulting damage inflicted on the interests of international community as a result of Tbilisi's loose and unpredictable foreign policy.

Extracts from articles posted by assets claiming that Georgia is sabotaging EU and NATO "anti-Russia initiatives"[^66] and that Georgian politics (here in Ukraine) are corrupt[^67]. The underlined text in Russian says: "The lady [Eka Zgiladze, a Georgian native who was Ukraine's deputy interior minister for a time], being very pregnant and therefore probably insane, took with her $4 million dollars to France."  

**Armenia**

The Secondary Infektion network mainly mentioned Armenia in reference to its revolution and the Nagorno-Karabakh conflict. The articles analyzed by Graphika were highly critical of the demonstrators who took part in the 2018 anti-government protests, claiming that they were engaging with a movement that would inevitably lead to Armenia losing Nagorno-Karabakh to Azerbaijan. Another angle claimed that the 2018 anti-government protests were staged by the prime minister himself for the benefit of the United States.
What’s up in Armenia?

Semeon Tozz  🔈Follow
May 12, 2018 · 3 min read

Of course, the Armenians have got a lot to grumble about and criticize the ruling Republican Party and Serzh Sargsyan who has already stepped down as Prime Minister. The republic's economic development has stalled, personal income is falling. Yet there has been no indication that people feel ready to take to the streets to cast the government down. Making an unbiased appraisal of the situation in Armenia, it is clear that the protests have been perfectly organized, planned and financed. Conventional slogans proclaiming fight for democracy, freedom and against tyranny are only a cover-up. Leaders of the protests copy the scenario of colored revolutions, creating a déjà vu impression. E.g. unjustified arrest of the opposition

In other words, the gallery play of Sargsyan and Pashinyan during their 3-minute meeting, Pashinyan’s imprisonment and subsequent release has most likely been orchestrated by Sargsyan himself.

What does he need it for? The thing is that despite their formal pro-Russian rhetoric, Armenia's oligarchs are greatly dependent on the United States, since most of their financial assets are kept there. They have given a clear signal to Sargsyan that it'd be inappropriate for him to stay in power any longer. Obviously, people in Washington have different plans for the

Sargsyan has decided against resisting the United States. Instead, he made an arrangement with Armenian oligarchs and Pashinyan — who was long ago made a puppet opposition leader by the ruling party — to stage a dramatic performance by imitating a colored revolution in Armenia. As a result, the new government will be dominated by the representatives of those financial circles which stand for integrating Armenia in the Caspian, Turkish project of the United States even though it entails territorial losses and renouncing Yerevan’s claims to Ankara and Baku. People in Armenia

Article on Medium.com claiming that the protests were staged by the prime minister on US orders. [720] (Underlining by Graphika.)

Sweden

Some narratives explicitly targeted Sweden, claiming the country and its leaders were going their own way on European issues such as terrorism. [775] The articles we discovered also claimed that the Swedish government was supporting ISIS [772] or that the Swedish parliament was undermined by some politicians acting on behalf of foreign actors. [773] One article stated that the Swedish government was acting against the will of the Swedish people by supporting the EU agreement with Ukraine and was trying to keep them from influencing European policies. [774]
Sverige kunde förebygga terrorattacker i Bryssel

26/3, 2016 at 13:50

Sweden could have prevented terrorist attacks in Brussels!

1080 views - Mar 20, 2016

Screen shot of an article on pressbladet.se[^766] posted by persona “George Kobzaru” and from the corresponding video posted by “Arri Gibbs” on YouTube, now deleted.[^767] The video was embedded in Secondary Infektion articles in Russian, English, Swedish, and German.

---

**Peace Settlement Through Creation of Terrorist Cells. ISIS Expects Aid of Sweden**

Joe Mohsenan | 24.05.2016 19:45 | Migration | Other Press | Terror War | World

The commander of the Daesh (IS) first female assault battalion Nade al-Qahmah has turned to Stockholm for aid in establishing of members for the Daesh all-female battalion, as well as in delivering weapons and munitions for Syrian fighters via Turkey.

---

Articles from [indymedia.org.uk][^768] and [newsparticipation.com][^769] claiming ISIS contacted the Swedish Government to get help establishing the “legal rule of the Caliphate” in Syria, based on a forged letter visible on the News Participation article.
The Techniques

One Operation, Many Platforms

From the beginning, Secondary Infektion was a uniquely cross-platform operation. Its earliest and most prolific persona, the "Blue Man" (described below), ran accounts on six Russian-language blog forums, and that was only the start: as of April 2020, Graphika had identified posts by the operation on over 300 platforms and forums, ranging from mainstream social media platforms like Facebook, YouTube, and Twitter to discussion forums from Azerbaijan to Australia.

![Articles by Platform Diagram]

Its range expanded as the operation progressed. It started in Russian on LiveJournal in early 2014 and added English- and German-language personas and burner accounts on BlogSpot, Twitter, and YouTube later that same year. It spread out rapidly in the second quarter of 2015, adding in many of the forums that came to characterize it, notably WordPress, Reddit, Medium, Before It’s News, and the Russian-language cont.ws. As these came to the fore, its emphasis on LiveJournal decreased; Medium played a particularly important role in 2016, while Reddit was prominent among its choices in 2017-2018.
The breakdown of platforms varied between languages. Secondary Infektion posted to the largest number of platforms in Russian, choosing not just Russian-based platforms, but forums across the former USSR, such as stena.ee (Estonia), amigos.lv (Latvia), dosug.md (Moldova), and yvision.kz (Kazakhstan). Its English-language choices were slightly more restricted but ranged from global giants to fringe forums such as dover.co.uk (Dover, in England), cssforum.com.pk (the Pakistani civil service), and ozpolitic.com (Australia). In Spanish, the operation only used a few platforms, notably Reddit and burbuja.info (ostensibly dedicated to real estate).

Sometimes Secondary Infektion abandoned certain forums, such as indymedia.co.uk, last used at the end of 2016, and articlesreader.com, used in 2016-2017; its presence on BlogSpot and YouTube also dropped off sharply after mid-2016. Overall, however, the trend was for an increasing number of platforms. It was only after the operation was exposed in May-June 2019 that its posting and use of platforms temporarily collapsed.

**Platform Evolution**

The evolution in platforms and posting patterns gave Secondary Infektion an increasing ability to spread its content to ever further corners of the internet. This did not typically translate into increased engagement, at least so far as we have been able to observe, but it indicates an operation that was aggressive in its attempts to reach an audience. This is best expressed by comparing posts from the operation’s earlier and later stages.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>livejournal.com</td>
<td>226</td>
<td>16</td>
<td>2</td>
<td>37</td>
<td>20</td>
<td>62</td>
<td>21</td>
<td>12</td>
</tr>
<tr>
<td>cont.ws</td>
<td>148</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reddit.com</td>
<td>142</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wordpress.com</td>
<td>136</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>medium.com</td>
<td>133</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>homment.com</td>
<td>128</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>blogspot.com</td>
<td>118</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>beforeitsnews.com</td>
<td>89</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>indymedia.org.uk</td>
<td>84</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>quora.com</td>
<td>84</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>facebook.com</td>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>defendingthetruth..</td>
<td>41</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>korrespondent.net</td>
<td>36</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aftershock.news</td>
<td>33</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>scoop.it</td>
<td>33</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>indybay.org</td>
<td>32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>newsland.com</td>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>youtube.com</td>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>indymedia.org</td>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>articlereader.com</td>
<td>27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>globedia.com</td>
<td>27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>politiko.ua</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>politkus.ru</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>razumai.ru</td>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>debatapoltics.com</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For example, on May 25, 2015, an anonymous poster published an article on cyberguerrilla.org headlined, “United States to nominate Ukrainian President Poroshenko for a Nobel Peace Prize,”[^1] The cyberguerrilla.org article embedded a YouTube video (now removed) with the same headline; this featured a man’s computer-distorted voice reading out the text of the cyberguerrilla article against a backdrop of archive footage.[^1]

The article presented a screenshot of a letter attributed to the then-Speaker of the Ukrainian Parliament, Volodymyr Groysman, and addressed to the US Ambassador to Norway, Julie Furuta-Toy. In the letter, “Groysman” asked the ambassador to “exert additional leverages” on the Nobel Peace Prize committee to ensure that Poroshenko won it. The initial spread of this story was exclusively through posts and accounts attributable to Secondary Infektion, leading us to conclude that the letter was a forgery launched online by the operation.

The same article appeared anonymously on homment.com on May 27, 2015,[^2] with a link to the cyberguerrilla.org article embedded. The following day, a German translation appeared on websites that included askf.org[^3] and the German section of indymedia.org,[^4] and a Russian translation appeared on platforms including cont.ws[^5] and X-True.info.[^6]
The transmission of the “Nobel” claim by assets run by Secondary Infektion, from cyberguerrilla[.]org, YouTube, and homment[.]com in English, into German and Russian, using the personas “Anonymous,” “Kries Larsson,” an unnamed post, “PolitGraben,” and “Ino-News.”

This was already a multi-platform and multi-language operation, but it was relatively limited in scope. In 2018, by contrast, Secondary Infektion was operating across far more platforms. On June 4, 2018, the operation posted a Medium article headlined, “Silence commanded. People in Sweden are incensed by London’s pressure on scientists” from a single-use burner account. The article accused the United Kingdom of pressuring Sweden and Israel to confirm that Russia had poisoned Sergei Skripal in Salisbury, “despite the obvious invalidity of London’s position that only Russia was able to produce and use this chemical agent.”

The same day, a user called “Peterblom,” or variants on that name, posted the identical article to the BuzzFeed forum (since deleted), thestudentroom.co.uk, scoop.it, defendingthetruth.com, and homment.com. On June 5, a single-use burner account called “Tiagorivas” posted a Spanish translation on globedia.com, and burbuja.info. On June 21, a Ukrainian-language account, Михайло Дричак (Mikhailo Dricak), posted a translation of the Medium article to blogs including korrespondent.net, perva.org.ua, and blog.iua. While far apart in time and space, these were all the work of the same operation, based on a single forged document.
**English Outlets**

Secondary Infektion used a wide range of English-language forums. Some served as primary locations, where the operation posted its initial stories; Medium was chief among these, most likely because it provided a visually attractive platform with a simple user interface and a reliable way of uploading and hosting images - an important point for Secondary Infektion, which relied on forgeries for so much of its work. Others served as secondary amplification points, where burner personas could share links to the original stories in special-interest groups. Reddit and Facebook were important in this regard. The operation used a handful of Twitter accounts in its early years, but largely dropped these as it shifted more exclusively to using burner accounts.

**Top Used Platforms for English language content**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>medium.com</td>
<td>133 (4%)</td>
</tr>
<tr>
<td>beforetonews.com</td>
<td>89 (9%)</td>
</tr>
<tr>
<td>blogger.com</td>
<td>80 (9%)</td>
</tr>
<tr>
<td>wordpress.com</td>
<td>64 (7%)</td>
</tr>
<tr>
<td>hornet.com</td>
<td>385 (13%)</td>
</tr>
<tr>
<td>indymedia.org.uk</td>
<td>84 (9%)</td>
</tr>
<tr>
<td>defendingtruth.com</td>
<td>41 (4%)</td>
</tr>
<tr>
<td>indybay.org</td>
<td>32 (3%)</td>
</tr>
<tr>
<td>articlereader.com</td>
<td>27 (3%)</td>
</tr>
<tr>
<td>facebook.com</td>
<td>38 (4%)</td>
</tr>
<tr>
<td>medium.com</td>
<td>84 (9%)</td>
</tr>
<tr>
<td>quora.com</td>
<td>33 (8%)</td>
</tr>
<tr>
<td>battlefield.com</td>
<td>21 (3%)</td>
</tr>
</tbody>
</table>

Top 15 platforms where Secondary Infektion posted in English.

**Buzzing BuzzFeed**

Secondary Infektion paid particular attention to the BuzzFeed Community forum, an unmoderated, user-generated forum that allowed the operation to share URLs containing a “BuzzFeed” link (in reality, BuzzFeed’s news content is primarily hosted on a slightly different domain, using buzzfeednews.com instead of buzzfeed.com). Infektion paid particular attention to the BuzzFeed Community forum, an unmoderated, user-generated forum that uses the same top-level domain as BuzzFeed’s regular news reporting. Secondary Infektion submitted stories to this forum in English and then pointed back to them from other posts in multiple languages. Sometimes, the operation attributed these stories to BuzzFeed itself. The use of the BuzzFeed Community thus seems to have been an attempt to increase the operation’s legitimacy by acquiring a URL starting with “buzzfeed.com.”
Three Secondary Infektion posts on a fake “interview with an MI6 agent” that the operation originally planted on the BuzzFeed Community forum. The “interview” claimed that MI6 had interfered in the US election to prevent Donald Trump’s victory. The top image shows the original post. The lower left and right images show the follow-on articles in French [198] and German [200] saying that BuzzFeed itself had attributed the “election interference” to MI6.

Russian Outlets

Secondary Infektion was also a prolific poster across Russian forums. As with its English-language targets, the portfolio of forums it used grew with time. For the benefit of users unfamiliar with the Russian blogging environment, we describe the main platforms in the appendix.
This Russian-language content should not be overlooked. The very first posts we have identified from the operation were in Russian and targeted the opposition, especially those around Alexei Navalny, who focused on corruption. After the exposures of 2019, the operation appears to have all but stopped its English-language activity but to have continued posting in Russian.

It is an important reminder that one of the most consistent targets of Kremlin influence operations, if not the most consistent, has been the Russian population itself. Political influence operations begin at home, and any accusation that “the Russians” used Secondary Infektion to attack the West should be met with the fact that “the Russians” were among its targets.

**Range of Languages**

Secondary Infektion started in Russian but it quickly branched out: by the end of 2014 it was already running personas in English and German as well. These three languages remained the backbone of its activity, but with time, it added Spanish, Ukrainian, and French to the mix. Sporadically, the operation also posted in Swedish, and Graphika also identified a very small number of posts in other languages that appeared to be translations of the operation's work.
In all except Russian, the writing was marked by errors not characteristic of a native speaker but too fluent to be the product of a machine translation. This suggests that Secondary Infektion had some form of access to content creators in at least seven languages, a likely indicator of the resources at its disposal. It is also one probable reason why Secondary Infektion’s products routinely failed to gain traction in any language other than Russian.

One significant question around the operation is why it focused on this set of languages. English and Russian were obviously crucial for external and internal audiences. Spanish was useful internationally, and German and French were important in Europe (there was no indication of attempts to target French-speaking communities in Africa). But there was no systematic posting in Italian, Polish, or Arabic that we have been able to identify with high confidence; there were posts in Swedish, but apparently neither Finnish (closer to Russia) nor Norwegian (banning on Russia and a NATO member). This returns us to the biggest questions of Secondary Infektion: Who was behind it, and what were they trying to achieve?

High OPSEC and Burner Accounts

Secondary Infektion stood out for its attention to OPSEC. Multiple platforms working alongside our team on this investigation have confirmed the operation’s systematic use of technical obfuscation techniques, such as the systematic use of proxy servers and internet-based phone numbers and the obfuscation of their language settings. Open-source investigation showed that the operation made massive use of single-use burner accounts, especially from mid-2016 onward. Such burner accounts made it difficult for
investigators to move from one Secondary Infektion story to another, as they left no technical clues and almost no content clues. The operation ran through literally hundreds of such accounts that it created, used, and immediately abandoned in the space of a single day, or even a single hour.

This increasing dominance of burner accounts held true across languages and platforms. It is most easily observed on Reddit, which provides precise time and date information for the creation of accounts and posts, but the same pattern applied across every platform that provided a creation date for its accounts.

For example, one story of the 2016 vintage claimed - based on an apparently forged letter - that Ukraine was lobbying for former prisoner of war Nadiya Savchenko to be nominated UN Secretary General. On Reddit, this was posted by a persona called “u/AokPriz” at 09:26:57 UTC on June 8, 2016.1202 According to online tool reductive.com, “u/AokPriz” was created just under 14 minutes earlier, at 09:13:05 UTC that morning.

Profile Information
(Dates displayed in your device’s timezone)

Name: AokPriz
Created: 7/8/2016, 5:13:05 AM (1369 days ago)
Link Karma: 1
Comment Karma: 0
Reddit Gold: No
Reddit Gold Trophy: No
Subreddit Moderator: No

Reddit user u/AokPriz

Created:
July 8, 2016, 09:13:05 UTC

Posted one post:
July 8, 2016, 09:26:57 UTC

Lifespan: 00:13:52

A story of the 2018 vintage, based on a forged screenshot from security analysis company Stratfor, claimed that the United States was concerned about an influx of Chinese spies.1203 This was translated into German and placed on a number of websites, including one called chinaseite.de (its name literally means “China page”).1204 Chinaseite.de shows the date and time at which an account was created and the date and time at which the user was last online. In the case of this account, its entire life lasted just seven minutes.


Burner accounts like these were Secondary Infektion’s pawns on the disinformation chessboard: numerous and disposable, but limited in effectiveness. Creating a new account for every post contributed to the operation’s tight OPSEC, but it put the operators in the position of having to build a new audience from scratch with every single post. None of its attempts to target interest groups and niche communities could overcome the fact that its accounts had no personality and no posting history and almost invariably posted documents that were palpable fakes.
Use of Forgeries

Very often, though not exclusively, Secondary Infektion based its articles on “leaked” documents or publications that it appears to have forged itself or to have acquired from other forgers for its exclusive use. The range of documents included letters (the most common form of forgery, especially in Ukrainian), emails, blogs, news articles, websites, social media posts, and even petitions. These “leaks” were typically embedded in the text of the article, usually via an image hosting site such as Imgur; sometimes, the platform in question could not handle the image, leaving a thumbnail or a raw URL instead of the picture. Quality control was not one of Secondary Infektion’s defining features.

It seems that the real scale of the problem is really impressive. At least, today there are all reasons to believe that, potentially, the most important spheres in the state may be flooded with Chinese spies. Thus, in mid-April, 2018 an article appeared on the Stratfor website stating that the US government, large business and research centers might be infiltrated with some agents of the Chinese special services.

The article:

"USA in Chinese cobweb. American Congressmen cover spies of Celestial Empire"

The sharp increase of industrial, economic and military spying activity in favor of China has affected a lot to the US economy, while the politicians who allowed that take significant reputational damages. So, the flexible approach to the problem raises questions about the effectiveness of both the State Department and the FBI.

It seems that the real scale of the problem is really impressive. At least, today there are all reasons to believe that, potentially, the most important spheres in the state may be flooded with Chinese spies. Thus, in mid-April, 2018 an article (i.imgur.com/sq3uM9k, j p) appeared on the site with some agents of the Chinese special services.

The article:

"USA in Chinese cobweb. American Congressmen cover spies of Celestial Empire"

The recent aggravation of the US and Chinese trading relations have had an impact on the industrial and military sphere of the United States of America, initially.

Regrettably, the fact of the constant Chinese espionage in the USA has been no news. It has been a daily process in cases of industrial cyber-spying.

As my colleague Roger Baker likes to say, “there are no former Chinese”, there are Overseas Chinese. Regretfully, each person of Chinese origin has been considered a P.R. power and a moment that sets feet on Chinese land. This also means falling within jurisdictional disputes and their recruitment, whether it is about a Chinese stall keeper or an American nuclear engineer.
Left, the fake Stratfor article embedded into a Secondary Infektion Medium post. Right, the same article on csforum.com.pk, one of the more unusual sites that Secondary Infektion used (it is dedicated to the Pakistani civil service). Note how the image failed to display in the right-hand post, leaving the bare impur link visible.

Sometimes, the forgeries involved multiple levels of deception. One “screenshot” published on September 18, 2018 featured a view of a Reddit page that contained a summary of an article attributed to British tabloid the Daily Mirror.[209] The article, in clunky English, stated that British intelligence had wiretapped US President Donald Trump’s attorney, Rudy Giuliani, as he exposed a secret deal with Britain’s Conservative party under which Britain would make Brexit “as tough as possible” and would make Boris Johnson prime minister, in return for a sweeping trade deal with the United States. A search on Reddit showed no results for the alleged headline,[210] and a Google search for the term returned no verbatim matches.[211] We conclude that the Reddit post and the Daily Mirror article were both fakes created by Secondary Infektion to provoke accusations that the United States was interfering in British politics.

Similarly, in October 2017, just after Germany’s federal parliamentary elections, Secondary Infektion planted the story that the victorious Christian Democrat party (CDU) had only won because millions of newly naturalized immigrants voted for it.[212] The article was based on a screenshot of a tweet attributed to the former director of the OSCE’s Office for Democratic Institutions and Human Rights (ODIHR), Michael Georg Link.[213] The tweet, in turn, embedded a photo of an apparent ODIHR report that claimed 98 percent of recent citizens had voted CDU. However, the genuine ODIHR report made no such claim[214] and Link’s timeline showed no sign of any such tweet.[215] Both the screenshot and the document are most likely forgeries.
Many of these forgeries, especially those that were not in Russian or Ukrainian, betrayed themselves by basic errors. One purported letter from the Spanish Foreign Minister, alleging that extremist Remainers in the United Kingdom were plotting to assassinate Boris Johnson to stop Brexit, misspelled the minister's name in his signature block. Another letter, signed by the “Director General of Swedish Defence Research Agency (FOI) Jan-Olof Lindt,” accused the United Kingdom of trying to force allied countries to state that only Russia could have poisoned former Soviet agent Sergei Skripal with nerve agent in April 2018. This may have come as a surprise to the actual head of the FOI at the time, whose name is Jan-Olof Lind. Even without such basic errors, the forgeries often betrayed themselves by using forms of language that did not match the purported author, such as basic errors in grammar and idiom. For example, one English-language article attributed to the UK's former Attorney General Dominic Grieve accused Georgia of being unready for EU and NATO membership. The article was based on a doctored screenshot of an article on UK domestic politics that Grieve had published in Prospect magazine. This was couched in stilted and undiomatic English unlikely to flow from the keyboard of the UK’s former Attorney General: “Considering that stability of the foreign policy is pivotal when estimating democracy development in that country, improvement in relations of Russia and Georgia may seriously hinder the effective cooperation of Tbilisi with the European Union and with NATO.”
Left, the fake by Secondary Infektion. Right, the original article from the Prospect website. Note the identical image in both.

Similarly, a letter attributed to US Senator Bob Corker in 2015 contained clumsy, unidiomatic formulations such as “The United States Senate Committee on Foreign Relations is deeply concerned by repeated failures of Ukraine to adhere to previously reached agreements.” [221]
The letter attributed to US Senator Bob Corker and addressed to then-Ukrainian Prime Minister Arseniy Yatsenyuk, accusing the latter of provoking ethnic tensions in Ukraine.

Sometimes, the people whose identities were forged discovered the forgeries themselves and called out their errors. For example, one Secondary Infektion article posted on March 24, 2016, claimed that Ukraine’s then-Finance Minister Natalia Jaresko had written to then-US acting Assistant Secretary of State for European and Eurasian Affairs Victoria Nuland, asking for help in postponing the Dutch referendum on the European Union’s Agreement with Ukraine. Jaresko discovered the fake letter and corrected it.
1/2 Рунетом гуляє погано сфабрикований "лист" в якому нібито прошу США допомогти перенести референдум у Нідерландах.

By April 21, 2020, Graphika had identified some 250 images that the operation had planted in its articles, almost all of them suspected forgeries. We expect that more remain to be found.
The Effort and the Impact

Very few of Secondary Infektion’s stories achieved any impact, as defined by external user engagement with its content. This is one of the most puzzling aspects of the operation: what did the operators think they were doing, and why did they not change their methods to achieve higher traction?

The operators did at least try to land their stories in front of receptive audiences. On Twitter, for example, they used @-mentions to tag journalists and politicians with the operation’s stories.

Posts by Secondary Infektion account “@kprydius” to German anti-migrant politicians, flagging an article that accused Poland and the United States of ganging up on Germany. [225] Screenshot courtesy of DFRLab [226]
Tweets on the Armenian genocide by suspected asset @indepeexp, addressed to Hillary Clinton, Laura Ingraham, Fox News, Fox pundit “Judge Jeanine,” and Senator Bernie Sanders.**[227]**

On Reddit, the operation used burner accounts to post its articles in subreddits where they might have expected to find a receptive audience; on Facebook, it used burner accounts to post to groups and pages in the same way.
Posts by Secondary Infektion asset “u/RachelCrossVodoo”[228] of the same article[228] to seven different popular subreddits: r/the_Donald, r/tifu, r/UK_Politics, R_POLITIC, r/news, r/politics, and r/worldnews. All posts were made between 08:46 and 09:59 GMT on January 23, 2017.
None of these attempts had a substantial impact. In the overwhelming majority of cases, Secondary Infektion's stories failed to achieve any pickup in the language communities they targeted. Some of the posts met with mockery or were called out as Russian troll posts.
The lack of online traction must have been apparent to the operators. On Reddit, for example, they often posted the same article to multiple subreddits, but many of the subreddits automatically rejected the posts, because they came from accounts that had been created the same day and had no karma. Despite that, the operators kept using the same approach, with the same results.

Spanish-language Reddit posts by Secondary Infektion assets from December 21, 2017[^235] and March 28, 2019[^236] were automatically removed because they were made by accounts that were too new.
There were two communities in which Secondary Infektion did achieve some measure of impact, albeit slight. The first was the anti-Western blogging community in Western countries, often associated with conspiracy theories such as the “Illuminati” and the “New World Order.”

For example, the claim that Ukraine and the United States were lobbying to get the Nobel Peace Prize for Poroshenko was amplified by UK-based user David Icke with the tags “political manipulation” and “Illuminati criminalize.”[237] Icke even appears to have created a meme to accompany the post: the image was branded “davidicke.com” and does not appear elsewhere on reverse image searches.

The same claim was picked up by self-styled investigative historian Eric Zuesse and turned into an article on Canadian-based website globalresearch.ca, a conspiratorial website that has previously amplified Kremlin and pro-Kremlin disinformation.[239] The article did not comment on or question the authenticity of the “leaked letter,” but took it at face value: “the Chairman of Ukraine’s parliament is boldly demanding the US State Department to arrange for Poroshenko to get at least a nomination for the Peace Prize.”
From Zuesse’s post, the story was picked up by Kremlin outlet Sputnik in English, Italian, and Turkish. The English and Turkish versions acknowledged that the Ukrainian government had called the letter a fake; the Italian version reproduced Zuesse’s arguments without any caveat or acknowledgement that the “letter” was a forgery.

More generally, Russian state and state-funded media were the second group to pick up on Secondary Infektion’s content. The same “Poroshenko Nobel” article was amplified by the web-based outlet nahnews.org which has been identified as a Russian-language outlet of the Russian IRA. On several occasions, Secondary Infektion material was picked up by the website newsfront.info, a pro-Kremlin site that, according to a whistle-blower interviewed by Die Zeit is largely funded by Russian intelligence, or by PolitRussia, a pro-Kremlin video channel that joined an umbrella group created by Russian IRA channels in late 2019.

In June 2015, the persona “Steven Laack” posted an article that accused the United States of using NGOs to recruit Russian and other former-Soviet citizens to join the Islamic State terrorist group. Typically for Secondary Infektion, it was based on a forged letter from USAID that included stilted, unidiomatic phrases such as: “U.S. Agency for International Development urges you to revise plans of administering financial assistance to non-governmental organizations in the post-Soviet states.” Three days later, the “Federal News Agency” or RIAFAN, a Russian-language website that has also been identified as belonging to the Russian IRA, published an article on the claim, attributing it to “American blogger Steven Laack.”

It is unclear whether these sites amplified the Secondary Infektion stories because they were aware of the operation or because they found its sentiments useful for their own purposes. As noted above, Secondary Infektion tweeted to Russian IRA account “Jenna Abrams” at least once, but there is no indication that the interest was reciprocated: none of the Secondary Infektion accounts that Graphika has identified features in the troves of social media posts attributed to the Internet Research Agency over the years.

The Big Bang

Of all Secondary Infektion’s output, only one appears to have made a substantial impact: the operation’s leak of apparently genuine US-UK trade documents in October 2019, shortly before the British general election. On this occasion, the documents were unveiled in public by the leader of the UK opposition, Jeremy Corbyn, to widespread coverage. Graphika’s research showed that the leaked documents were first posted on Reddit with accompanying text in unidiomatic English (“Great Britain is standing on her knees…”), and then amplified in German on Reddit, homment.com, and meinbezirk.at using single-use burner accounts. One Twitter account also posted the leaks multiple times, tagging the accounts of British politicians and journalists. In December 2019, Reddit attributed the trade leaks to Secondary Infektion, and unveiled a trove of 61 other accounts that they also attributed to it.

However, it appears unlikely that the operation’s social media amplification led directly to Corbyn’s unveiling. There are still gaps in our knowledge of how exactly it was conducted, but it appears that the leak only picked up traction after it was emailed to UK activists and to the UK Labour Party.

Overall, of all the information operations Graphika has studied, Secondary Infektion achieved the lowest impact for the effort it made (taking online virality, sharing, and significance of these stories in the public debate as proxies for impact). Of all the hundreds of fake stories and forged documents, none yielded significant traction online.

Mapping Audiences: Secondary Infektion’s Followers on Twitter

Secondary Infektion was so heavily dependent on blog posts that had minimal viewing figures, and so reliant on single-use burner accounts, that few data are available to map its audience.

However, in 2014-2016 the operation ran a small handful of Twitter accounts that posted repeatedly in English, German, and Russian. These fell functionally silent in 2016 (other than automated updates on their follower numbers), but they were still visible in early 2020, allowing Graphika to map the audiences that paid attention to their content.
The map above displays the accounts that followed any of the Secondary Infektion accounts, revealing the communities they are forming with one another. The map is dominated by pro-Russian accounts, split into the Russian | LNR & DNR (33.53% of the map) and the International Pro-Kremlin | Conspiracy (17.79%) groups. The Russian group essentially gathers Kremlin politicians and supporters and reporters for state-funded outlets, as well as writers and influencers whose online activity is mainly structured around amplifying Kremlin narratives on social media. The International Pro-Russia | Conspiracy group gathers international pro-Russian support, as well as Syria-focused accounts and far-left conspiratorial influencers. The German community is mostly composed of social media marketing accounts, as well as of two clusters of German far-right-affiliated accounts, and the British one consists of pro-Kremlin far-right accounts.

The map’s division into distinct clusters reflects the language breakdown between the Secondary Infektion accounts. Thus the operation’s German-language assets were primarily followed by German-language accounts that focused on far-right or conspiracy content; the English-language assets were mainly followed by English-language accounts with a distinct far-right or conspiratorial leaning. These two groups were somewhat interconnected. The Russian-language accounts had a separate and largely distinct audience of Russian-language accounts focused on the separatist territories of Ukraine. This content focus is in line with the accounts’ behavior. Their content largely focused on attacking the United States, Muslim migrants, and critics of the Kremlin and would therefore naturally appeal to far-right and pro-Kremlin groups; it was routinely conspiratorial in tone and often based on forged documents, hence its appeal to conspiracy communities.

It is worth noting that the map reveals a relatively small total community, especially considering that it spreads across three languages. The map consists of only 6,027 accounts (nodes). Graphika maps are usually composed of up to 14,000 accounts. While some accounts that once followed Secondary Infektion may have been taken down in the interim, this highlights the little reach Secondary Infektion assets had on Twitter, especially since around 26% of the network is constituted of social media marketing pages that did not have a specific political bias.
Early Experiments with Personas

Secondary Infektion experimented with different formats of false account before it settled on its trademark reliance on single-use burners. Between 2014 and 2016, the operation ran a number of accounts that it tried to build up into pseudo-personalities, complete with stolen profile pictures and at least some attempt at creating a believable backstory for these personas. In this section, we examine a few of those early experiments.

The first of these began operating in Russian in very early 2014 and attacked members of the Russian opposition before it turned to attacking Ukraine, a salutary reminder that disinformation, like charity, starts at home. Over the following year, the operation added a cluster of further personas in English, German, Russian, and possibly Swedish, using them to amplify its content.

These personas primarily published lengthy blogs, especially on Blogspot and Wordpress. Often, the personas reproduced articles that single-use burner accounts had already posted, sometimes with attribution, sometimes without - perhaps as an attempt at plausible deniability. They thus constituted a secondary amplification network.

This had modest success. The first Russian-language account, the “Blue Man,” did gain at least some audience, to judge by the responses to some of “his” posts; the cluster of secondary amplifiers in other languages sometimes managed to land stories in the Russian-language media. This was trivial compared with the large-scale followings that the Russian IRA built up, but it did show at least some degree of online reach.

However, Secondary Infektion abandoned most of these personas in mid-2016, for reasons that are not yet known. It may be that the operators behind Secondary Infektion wanted to improve their OPSEC because of other incidents that occurred around that time, especially the Russian hacking and leaking of emails from the Democratic National Committee; it may be that they decided independently that the audience gained by maintaining persistent personas was not worth the heightened risk of detection. Whatever the case, they fell silent, and the experiment was not repeated outside the Russian-language space - as far as we have been able to establish.

The Blue Man

The most prolific and realistic Secondary Infektion persona was the asset dubbed the “Blue Man,” first exposed as part of the operation by Facebook in May 2019, and described by the DPRLab in June.[256] The account authored at least 226 Russian-language posts across six platforms, starting with LiveJournal in January, 2014, with his location stated as Ukraine.

The persona gave his name on every platform as “Stanislav Melanich” or “Stas Melanich,” sometimes with the username “blogger_nasalny,” the second part being a foul-mouthed play on the name of prominent Russian opposition figure Alexey Navalny. His profile picture was always a photo of Navalny coloured blue – hence the nickname. Unlike most Secondary Infektion assets, his posts did attract readers’ comments, indicating at least some online reach.

The persona’s first few posts attacked Navalny and his colleagues, essentially accusing them of being corrupt puppets of the United States. This underscores how much disinformation is domestic in origin,[257]; even the entity that became the Russian IRA started out by targeting Navalny.[258]

On February 26, 2014, however, four days after Ukraine’s then-President Viktor Yanukovych fled the country, the persona began commenting about events in Ukraine by reposting a LiveJournal blog headline “Kharkiv, Arise!” (“Харьков, вставай!”, referring to the Ukrainian city of that name, through which Yanukovych had passed on his way into exile).[259]

I simply don’t have time or strength to do what I was before. Too much work lies ahead in breaking through the information blockade that the Official Ukrainian Media have imposed on the national resistance to the new order across the whole of South-East Ukraine.

From then on, the Blue Man posted about Ukraine unrelentingly. Of 226 posts on various platforms, just 24 were about the Russian opposition, the Baltic States, or the United States and the West; the rest were Ukraine all the way.

The persona wrote fluently and in a personal tone, mocking and contemptuous, sometimes foul-mouthed, and littered with sarcastic references to Ukraine’s European hopes and aspirations. He always wrote in Russian, with some Ukrainian words and terms sprinkled in, sarcastically, such as перемога/перемоги (“victory/victories”) or calling Ukraine ЦеЕвропа, a descending reference to the Ukrainian phrase Україна - це Європа (”Ukraine is Europe”).

For example, in one post headlined “Перемога енергетична” (“Energy Victory”), he accused Poroshenko of keeping quiet about an energy deal with Russia because the arrangement did not fit with the image of Russia as the bloodthirsty enemy of Ukraine. This post referred to Poroshenko as “президент ЦеЕвропа” (“the president of IsEurope”).[260] In another post mocking a petition to the Ukrainian president, the Blue Man called his translation from Ukrainian into Russian a “Translation into human language” (Перевод на человеческий).[261]

Like other Secondary Infektion assets, the persona existed on multiple platforms but did not always post the same content to each. His activity on his six known platforms unfolded as follows:
• LiveJournal as Stanislav Melanich, Blogger_Nasralny, January 12, 2014–July 2, 2019, claiming to be in Ukraine, 201 posts
• cont.ws April 23, 2015–April 30, 2018, as Stanislav Melanich with a link to his LiveJournal, 55 posts
• Maxpark May 5, 2015–August 21, 2018, as Stanislav Melanich, 20 posts
• Aftershock June 25, 2015–June 8, 2018, as bloger_nasralny with an Estonian flag in his profile, 41 posts
• Newsland July 2, 2015–July 2, 2019 as Stanislav Melanich, 55 posts
• Politikus April 5, 2016–September, 27, 2018, as stasmelanich (Stanislav Melanich), 19 posts

Blue Man / Stanislav Melanich Activity

![Blue Man Activity Chart]

After four and a half years of posting, the operators appear to have decided that it was time to try a little market research. The persona’s final post on aftershock.news asked readers to rate the sites Aftershock, cont.ws, Politikus, Worldcrisis, and Военное обозрение (Military Review) according to a set of criteria that included length, entertainment value, and happy/sad. There is no indication how many users responded, but the persona only remained on LiveJournal and Newsland thereafter.

The Blue Man had a clear personality, but there was little by way of a clear identity behind it. He said in one of his posts that Ukraine was “my former homeland.” His profile on the forum AfterShock.news featured an Estonian flag, and the site gave his last login location as Estonia (he could have used a VPN). He talked about “Ukrainians” rather than “we” or “we Ukrainians.” The only profile picture he used was the blue Navalny.

His engaging style and repetitive posting were unusual for Secondary Infektion, but multiple pieces of evidence connect the Blue Man to the broader operation, a connection also corroborated by Facebook’s analysis of Secondary Infektion’s initial set.

One of this persona’s earliest posts, on October 23, 2014, reported an outbreak of Ebola in Ukraine. The report was based on a letter that was allegedly leaked from the Scripps Research Institute; Graphika contacted the alleged author, who confirmed that it was a fake.
One of the earliest fakes that we have yet identified from Secondary Infektion, concerning the alleged outbreak of Ebola in Ukraine. Professor Ollmann Saphire confirmed it was a forgery.

The fake also appeared in English on a medical forum, curezone.org, where it was posted by an apparent burner account. The use of false leaks and burner accounts suggests the tradecraft of Secondary Infektion in its infancy.

On December 4, 2014, the Blue Man shared a YouTube video, now suspended, attributed to “Anonymous Europe.” This claimed to be in possession of leaked proof of a US-EU plot against far-right forces in Europe. For his source, the Blue Man provided a link to now-defunct hacking site cyberguerrilla.org, a site that Secondary Infektion was to use time and again over the years. The YouTube video’s description provided what is likely to be a similar text to the defunct cyberguerrilla post:

Recent protests in Budapest have got nothing in common with true people’s demonstrations. They are deliberately heated and financed from outside and are aimed at forcing the people's government to take unpopular measures which benefit Washington and Brussels.

Only one other blog shared the same video. This was a German-language account on BlogSpot called “Ulrich Hartmann,” another Secondary Infektion asset that we describe in more detail below. Thus by the end of the 2014, the trademark tradecraft of Secondary Infektion was taking shape, and the Blue Man was an integral part of it.
An Early Cluster, 2014-2016

In the months after it gave birth to the Blue Man persona, Secondary Infektion created a cluster of false personas in English, German, and Russian that intersected and cross-posted one another’s content. These were the personas “Ulrich Hartmann” and “Max Bromberg” and the blog “Politgraben” in German, the personas “Josef Hashever” and “Steven Laack” and the Twitter account @indeexp (short for “independent expert”) in English, and the persona “Innokenty Niussowsky” or “Ino-News” (likely a play on words from the Russian for “foreign news”) in Russian. A Twitter account and website, @cyber_legion and cyberlegion[.]org, were briefly associated with them, as was a website focused on the African-American community, blackdefence.wixsite.com (discussed below).

Each had at least the rudiments of a persona. “Steven Laack,” for example, claimed to be a Swedish immigrant to the United States; he was mainly active on blogspot.com, while his Twitter account claimed at various times to be located in Providence, Utah and in Florida. “Max Bromberg” claimed to be in Germany and used French model Francois Verkerk as “his” avatar and was more active on WordPress. Almost half of his articles - 30 of 79 - targeted Ukraine, with a specific focus on Ukraine’s paramilitary and far-right groups.

Left, Francois Verkerk on Pinterest. Right, the Max Bromberg persona on myheimat.de.[272]

Timeline of Personas Activity

Timeline of blog posts by persona. Bar graph label features total number of posts by persona.

The “Josef Hashever” persona, also sometimes referred to as “Lunatic Joe H,” was a frequent contributor to Before It’s News,[274] where it primarily reposted content posted by burner accounts on other platforms some hours or days earlier. Hashever also maintained a WordPress site, “Lunatic Joe’s Blog.”[275] On Twitter and Facebook, his profile picture was Prince Charles. “Ino-News” posted in Russian on a range of platforms, usually providing translations of the English posts.

Most of these personas were active across multiple platforms, including WordPress, Blogspot, Twitter, and Facebook. On Twitter, their posting patterns were strikingly similar and regular, despite the apparent difference in their locations, giving the impression of a team working to a standard shift.

That 8-5 Shift
Tweets per weekday by @PolitGraben

- Mon: 332
- Tue: 343
- Wed: 309
- Thu: 275
- Fri: 280
- Sat: 16
- Sun: 1
Tweet Frequency by Time of Day (UTC) - @PolitGraben

- The graph shows the frequency of tweets by time of day, with the y-axis representing the logarithm of the tweet count.
- The x-axis represents different times of day, from 11 PM to 11 AM.
- The graph indicates a peak in tweet frequency around 10 AM and a decline towards 11 PM.
Tweets per weekday by @Ulrich_Hartmann

<table>
<thead>
<tr>
<th>Day</th>
<th>Count of Tweets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon</td>
<td>576</td>
</tr>
<tr>
<td>Tue</td>
<td>532</td>
</tr>
<tr>
<td>Wed</td>
<td>607</td>
</tr>
<tr>
<td>Thu</td>
<td>571</td>
</tr>
<tr>
<td>Fri</td>
<td>520</td>
</tr>
<tr>
<td>Sat</td>
<td>142</td>
</tr>
<tr>
<td>Sun</td>
<td>93</td>
</tr>
</tbody>
</table>
Repeatedly, these personas shared the same stories in different languages, without attributing them to one another; this content originated from single-use burner accounts and was often based on forged documents. For example, on April 6, 2016, a persona called “Dusty L.A.” posted the article “Turkey was about to open second front vs. Armenia” on Medium[^276] and indymedia.org.uk[^277]; the same article appeared anonymously on homment.com the same day.[^278] The article was based on a screenshot of an alleged article on a website called ekurd.net, but no trace of any such article remains on the site.[^279] (The Secondary Infektion piece claimed that the original article had been deleted.)

On April 8, 2016, the fake screenshot appeared in three locations and languages: in the identical English version on the “Josef Hashever” account on beforeitsnews.com[^280]; in a German article on Politgraben[^281]; and in Russian on the inonews.info website.[^282] On April 11, the “Steven Laack” persona posted the English-language article on scoop.it.[^283] All four personas attributed the story to the homment.com burner account.
The transmission of the fake story on Turkey’s “second front” against Armenia from a single-use burner post on hommenn.com, to posts the same day by Josef Hashever, Politgraben, and Ino-News, to the scoop.it account of Steven Laack.

As another example, on October 20, 2015, the Twitter account “@Cyber_Legion” tweeted, “#European Integration without the #EU. Nordic dream of Swedish nationalists.” The tweet was originally linked to a website that is no longer active, http://cyber legion.org/european-integration-without-the-eu-nordic-dream-of-swedish-nationalists. The URL was in English, but on October 22, the operation persona Josef Hashever posted an article with the identical headline to “his” WordPress blog and to self-publishing site beforeitsnews.com and claimed that it was a translation from “CyberLegion” in Swedish.
The European Union has been going through a bad stretch. Voices for the EU transformation and even disintegration became much louder and more aggressive. This is the “northern” version of the new European division translated from Swedish at *Cyber Legion*.

Unfortunately economic, immigration and cultural repercussions of the long drawn out European experiment

The Cyber Legion article may have been written in Swedish originally, but the fact that the URL was in English makes this unlikely; reverse-searching the image and reverse-translating into Swedish did not show any Swedish versions of the text, although this is not conclusive. The blog argued that the EU model was broken, and that Nordic countries should set up a splinter group:

Ideology that damages economy, unjustified enlargement without due structural reorganization, serving the needs of NATO up to completely accepting the its line of policy [sic], dominance of artificial political correctness over mutual cultural enrichment – these are distinctive features or [sic] the EU today. (...) An advocated by Swedish nationalists hypothetical Northern Republic composed of Sweden, Finland, Norway, Denmark, Iceland and, if possible, Baltic states may not be as absurd as it is portrayed by European Mass Media.

On October 23, the same article appeared on self-publishing website indymedia.org.uk, but this time it was attributed to Anonymous and omitted the reference to Cyber Legion.[286] Three days later, a Russian translation appeared on a number of blogging platforms, including aftershock.news, where it was attributed to operation persona No-News.[287] Thus in the space of a week, the story passed through four different personas in two languages, all attributable to Secondary Infektion.
These personas constituted a small and self-referential group. They acted as second- or third-stage amplifiers, picking up content from Secondary Infektion’s burner accounts and posting it to social media and their own blogs. On occasion, they were picked up in the Russian-language pro-Kremlin media. However, for reasons as yet unknown, they fell silent in mid-2016, and Secondary Infektion shifted even more markedly to using single-use burner accounts.

“Black Defense Foundation”

Perhaps the strangest element of Secondary Infektion’s entire operation—an operation that did not lack for bizarre and colorful stories—was the blog blackdefence.wixsite.com, headlined “Black Defense Foundation.”[288] The blog advocated not just for African-American rights, but for the community’s full independence:

For hundreds of years blacks have tried to assimilate into White America and accept her values and style of life. Our ancestors were brought here in chains—they fought for freedom and they got it. White America and her society rejects us—we will build up our own Black America, and there will be no place for arbitrary powers of white police, white judges and white juries!

The blog was only sporadically active: five posts between January and June 2015, and one post in November of that year (but apparently “part one” of a two-part series whose second part it had already published in January). The content was inflammatory in tone: it even included a video on police violence that compared the US police with wild animals.[289] The video was also posted on YouTube by a single-use burner account, now suspended.
The use of language was aggressive but unidiomatic, bordering on the bizarre. For example, an article posted on January 16, 2015 was headlined “The State of Black America.” Its first paragraph read:

The Black America State’s Concept is still alive at Afro-Americans’ head. And their attempts to defy pigs’ orders, mass protests in Ferguson, as well as, demonstration killing of these pigs in New York are links in the one chain. Blacks are tired out with living under oppression of whites, taking their dictation, the how of it has been done by their forefathers at plantations.

The website also included a “Contact” form, encouraging readers to reach out and share evidence of “illegal use of force against Black people.” The form suggested the organization may use said material in court. This legal promise, and the organization’s reference to the United States as “Our country,” are particularly odd given that the “Black Defense Foundation” contact information located the organization in Cuba. The website footer contained an address, which was also shown as a geolocalized pin under the contact form: “Black Defense Foundation, 28 Calle Jose Marti, Habana, Cuba.”

Typically of Secondary Infektion, one of the website’s stories was based on an alleged letter, this time supposedly from Republican Congressman Bob Goodlatte, of Virginia’s Sixth District, to the Honorable Todd Richardson, Majority Leader in the Missouri House of Representatives. The letter proposed creating a “public Missouri Police Oversight Committee and allocate at least 35% of seats in
it to Afro-Americans." The opening sentence was couched in stilted, unidiomatic English that omitted the word "the" twice and struggled with the genitive; the letter was likely a fake: "US Congress highly appreciates Missouri House of Representatives achievements in easing social tensions in the State."

Overall, the website had minimal impact. By April 2020, the "Police lawlessness" video had gathered fewer than 50 views. The website did not give visitor figures, but none of the posts received any comments. As far as we are able to establish, the "Foundation" was only shared once on Facebook, by Secondary Infektion asset Josef Hashever.[292] An attack on Obama[293] was translated into German by Secondary Infektion asset Ulrich Hartmann.[294] The story about the "letter" from Goodlatte was expanded into an article in English by Secondary Infektion asset Steven Laack.[295] The Laack piece was then translated into Russian by Secondary Infektion asset Ino-News.[296]

It would be an unlikely coincidence that so many of Secondary Infektion's assets happened to find an otherwise unnoticed blog - a blog that just happened to include an apparently forged letter between two senior US politicians that no other news outlet had noticed. We conclude with moderate confidence that the Black Defense Foundation blog was itself created by Secondary Infektion as a brief experiment into amplifying racial tensions in America.

This experiment pushed both sides of the racial divide. As well as the expanded article mentioned above, the Steven Laack persona mentioned the Black Defense Foundation in one more article, but in a much more negative light.[297] On May 5, 2015, "he" quoted the Black Defense Foundation video that portrayed police as wild animals, but juxtaposed it with another one - this time, a video headlined "Black Violence" that compared African Americans with dogs.[298] Like the "police lawlessness" video, this was also posted to YouTube by a single-use burner account.

The overall article portrayed the United States as verging on a race war and the breakdown of the concept of the nation:

Current events -- Ferguson, Baltimore. I seriously doubt that since now anyone living there and being white would ever want to join and work in local police. I guess very soon the already small population of white people will hasten to move somewhere away from these places -- somewhere, where they'll feel safe at least. White people are already leaving Texas, California, Arizona ... Anglo-Saxon culture steadily moves to the North. 'Black America' begins to manifest itself more clearly on the map - 'other' country with its own 'other' rules.

The "Black Defense Foundation" was a brief and ineffective effort. It is of interest for the attempt it shows to exacerbate racial divides in the United States. Secondary Infektion did not repeat the effort after 2015, but the Russian IRA did, repeatedly.
Winter Olympics - If Russia Can't Play, No One Can.

In likely revenge for Russia’s ban, Secondary Infektion targeted the 2018 Winter Olympics in Pyeongchang. In the months preceding the games, Secondary Infektion promoted the narrative that the event should be canceled over security concerns relating to geopolitical tension between the US, South Korea, and North Korea. Graphika uncovered a series of stories published between mid-November 2017 and early December 2018, principally on Reddit.[298] The stories were in English, Spanish, German, and Ukrainian, suggesting that the narrative was directed at a non-Russian, international audience. Like most Secondary Infektion narratives, these stories generated no organic traction.

Chronologically, the stories appeared to follow major developments in the Russian doping scandal, which culminated in the sanctioning and eventual complete ban of athletes from Russia. On November 9, 2017, the World Anti-Doping Agency published evidence of state-sanctioned Russian doping in the 2014 Summer Olympics in Sochi. In response, the International Olympics Committee (IOC) banned four Russian athletes and announced it would rule on Russia’s participation in the Pyeongchang games in early December. The reaction from Russian officials was overwhelmingly negative, with Putin calling the allegations a "US plot against [the] Russian election." Four days after the ruling, Secondary Infektion began posting about the Winter Olympics.

On November 13, a burner account on Reddit posted a story to r/foreignpolicyanalysis entitled "The USA will reinforce security of diplomatic mission in South Korea with special forces."[300] The full text is unavailable, but this is likely the first story in the operation’s targeting of the Olympics.

On November 15, a likely operative commented on an existing Secondary Infektion asset on Reddit. The original story, "Flowers for Kim Jong-un or Operation White Chrysanthemum," was published to r/korea and r/news on November 10 and alleged a CIA plot to assassinate Kim Jong-un.[301] The comment, published by the burner account, u/student233, piggybacked off the original asset to express concern about the safety of the upcoming games.[302] In addition to realist223, two other burner accounts, u/olariwood and u/Vicky41, commented on the story at different points following the original posting. If these comments were indeed Secondary Infektion assets, this marks one of the few times the operation went back to engage with one of its stories after posting it. These accounts were likely an attempt at boosting the credibility of the original post by creating artificial engagement.

Comments on the story regarding the "assassination" of Kim Jong-un.
On November 29, asset u/MaxKasyan posted a story called to "Зимові Олімпійські ігри 2018 у Південній Кореї і їх безпека" ("2018 South Korean Winter Olympics and Their Security") to $r/ukraina, a Ukrainian board on Reddit.[303] The story maintained the established narrative of questioning the security of the Olympics in light of geopolitical tensions and quoting officials who had allegedly expressed similar concerns. On the same day, a burner account with a version of the Reddit username posted the article to the Ukrainian blog korrespondent.net.[304] Graphika also found an English translation of the article called "The PyeongChang 2018 and its security,"[305] which was posted anonymously to Homment two weeks earlier. It appears that until December, Secondary Infektion had yet to prioritize its Olympics-related messaging. Additionally, it had yet to directly call for cancellation, preferring instead to hint more broadly at the issue of security concerns.

On December 5, the IOC reached a verdict, determining that Russia be banned from the Winter Olympics. Individual Russian athletes, upon the approval of the IOC, would be able to participate under the neutral name "Olympic Athlete from Russia (OAR)," but Russia's flag, anthem, and officials would be absent from the games. In the weeks following the announcement, Secondary Infektion redoubled its targeting of the Winter Olympics.

On December 21, Secondary Infektion published "Olympische Winterspiele als Deckmantel für den Angriff auf Nordkorea" ("The Winter Olympics as cover for the attack on North Korea") to Reddit (r/de), hommenL.com, and meine.stimme.de.[306] In an alarmist tone, the article spoke about potential war between the US and the DPRK and stated that people planning on attending the Olympics should be very concerned. The article included a faked open letter to the German Olympic Sports Confederation from sports officials expressing concerns for the safety of German athletes. Over the next five days, Secondary Infektion published similarly themed articles, all based on the same faked letter, in English on thestudentroom.uk, worthychristianforums.com, and futuretimeline.net, [307] in Spanish on Reddit,[308] and in Ukrainian on buzina.org, obozrevatel.com, and korrespondent.net.[309] In Ukrainian, Secondary Infektion gave the article an exceptionally dramatic title: "XXIII Зимові Олімпійські ігри В очікуванні трагедії" ("The 23rd Winter Olympics: In Anticipation of a Tragedy").
On December 29, Secondary Infektion circulated its final Olympics-related article, which reported on a Change.org petition to either relocate or cancel the PyeongChang Games due to impending war between the US and DPRK. The English article was published on allkpop.com, quora.com, raidforums.com, and homament.com. Over the next two weeks, the article and accompanying petition appeared in Spanish on Reddit and vandal.espanol.com and in Ukrainian on obozrevatel.com and buzina.org. The petition itself is still up online and is a likely SI asset. In addition to the trademark language errors, the petition reiterated some of the same points from previous SI stories. For example, both the petition and the previous story about German sports officials cited joint military exercises between the USA and South Korea and the claim that China was building refugee camps along its border with the DPRK in preparation for war. Additionally, the petition was just as unsuccessful as most SI assets, garnering only four supporters.
Secondary Infektion’s coverage of the 2018 Winter Olympics is significant for a number of reasons. Most importantly, it reinforces operational attribution to Russia. Few actors apart from Russia would have an incentive to target the Winter Olympics in a similar manner. Russia was the only nation to be banned from participation that year. Also, this case speaks to the vindictiveness of the actors behind Secondary Infektion. Spreading disinformation around the doping allegations themselves is one thing - Russian efforts to this end are well documented. However, working toward the disruption and cancellation of the Olympics, albeit ineffectively, reflects an extraordinary degree of pettiness. According to Secondary Infektion, “If Russia can't play, no one can.”

Sweden, Fakes, and Fake Fakes

One of Secondary Infektion’s more complex efforts targeted Sweden in 2017-2018, when the operation had been running for over three years. By this time, its tradecraft had settled on the dominant use of burner accounts across a stable set of websites in different languages; these were consistent enough to form a recognizable pattern.

On July 24, 2017, single-use burner accounts published a forged letter attributed to the NATO Strategic Communications (StratCom) Center of Excellence in Riga, Latvia, on a number of regular Secondary Infektion websites, including Medium, Topbuzz.com, homment.com, livejournal.com, and politiko.ua. The forged letter alleged that the anti-migrant Sweden Democrats party had invited Russian hackers to interfere in the country’s general election, set for September 2018.

The unidiomatic English (“NATO Strategic Communications Centre... has brought to light series of cybercrimes with the involvement of the Russian hackers acting on the order of Swedish Democrats party”), the use of single-use burner accounts on those platforms, and the use of a forged letter[9] all mark this as the likely work of Secondary Infektion. However, the content was strange for the operation, and counter-intuitive. Why would Secondary Infektion forge a letter warning about Russian interference in Sweden?

For over a year, the operation avoided the topic. Then, on August 21, 2018, burner personas published a second “leak” on sites including Medium, Reddit, indybay.org, politiko.ua, and livejournal.com. This time, the leak featured letters from no lesser figures than US Secretary of State Mike Pompeo and former French far-right presidential candidate Marine Le Pen. The Pompeo letter warned of Russian cooperation with the Sweden Democrats; the Le Pen letter pledged assistance to the same party.

Again, the tradecraft was identical with other Secondary Infektion pieces of that vintage: the same sites, the same sorts of burner accounts, the same styles of forgery and language error. But again, the messaging was at odds with Secondary Infektion’s known style, which was to ridicule and play down Russian interference, rather than fake it.

The explanation became apparent on August 30, 2018, just before the election. That day, yet another set of burner personas - Nadine Kinsky in English, Gustavo Salcedo Mejía in Spanish, and Laurent Lavia in French - posted yet another “leak” to the standard Secondary Infektion sites.
This time, the leak purportedly came from the Ukrainian Prime Minister's office. Addressed to the Ministry for Information Policy, the three-page document ordered the ministry to “develop a plan of measures aimed at supporting the Swedish government in confronting the hybrid war, being carried out by Russia related to the oncoming elections to the Swedish parliament on September 9.” Precise instructions followed, including to invoke the danger of cooperation with the French far right and referencing the StratCom leak, which it called the Ministry's “previous information campaign.”

The English-language article then continued:

Information dummed up on instructions from the Ukrainian Prime Minister, which concerned protection of The Sweden Democrats by the leader of the National Front Marine Le Pen (…) is being actively reproduced on various European Internet platforms. A forged letter from the US Secretary of State Mike Pompeo to the Polish Minister of Foreign Affairs Jakec Czuputowicz features in these publications, too.

There are two options here. One is that the Ukrainian Prime Minister's letter was genuine, and the Ukrainian Information Ministry was skilled enough to identify and mimic Secondary Infektion’s exact tradecraft almost two years before it was exposed in public, but not skilled enough to keep an explosive internal document secret. The other is that the entire year-long cycle was an operation run by Secondary Infektion to discredit Ukraine by making it look like the Kiev government, not the Kremlin, was interfering in Sweden’s election.

Bond, but on BuzzFeed

Another long-running Secondary Infektion creation came in January 2017, immediately after Donald Trump’s election victory in the United States, and after the US intelligence community reported that Russia had interfered in the election. [321]

Two weeks after the intelligence report, Secondary Infektion posted an alleged “interview with an MI6 agent” on the BuzzFeed Community [322] - almost certainly because BuzzFeed had earlier published an unverified report on Trump’s relationship with Russia. Headlined “MI6 operative on anti-Trump campaign,” the interview featured an alleged former agent who confessed that MI6 had created a range of fake evidence designed to compromise Trump, implicitly including the Steele dossier.

The idea was James Bond, but the use of language was Shakespeare: “I remember the election day full well” and “His commitment to the European Union was just a peacockery,” for example. The intent appears to have been twofold: to deflect or diminish the accusation that Russia had interfered in the US election and to create tensions between London and Washington.

Subsequent events made that argument explicit. In typical Secondary Infektion style, the story reappeared in French, [323] German, [324] and even a small post in Swedish in the following days. [325] Both the French and German versions headlined that BuzzFeed itself had attributed its “anti-Trump dossier” to MI6, effectively disowning it.

As so often, this story does not appear to have gained traction. Two weeks later, as Theresa May became the first world leader to visit Trump, Secondary Infektion ran another story on multiple websites using burner accounts: Quora, Reddit, indybay.org, and ozpolitic.com, an Australian forum. [326]

This article appeared to be an attempt to stir up the tensions that the first article had failed to raise. It portrayed May’s visit as an act of desperation and an attempt to “save face” and linked to the BuzzFeed “MI6 interview” as its only source for the claim of MI6 “spying on Trump”:
MI6 has not only been spying on Trump for quite a while, it has been also collecting and creating damaging information that could harm him, in fact the spooks continue their work even now. Obviously, Donald Trump is well informed about this, and the visit of Theresa May merely confirms that the British Prime Minister does her best to keep the lights on.

A few days ago the U.S. President Donald Trump held a meeting in Washington with the British Prime Minister Theresa May, the first world leader who visited the White House for negotiations with the newly elected POTUS, and that does have a reasonable explanation.

This article left too few leads to reliably identify variants in other languages, so it is unclear how far Secondary Infektion tried to spread it. There is no indication that it gained traction.

In March 2017, as debate over Russian interference continued to rage in the United States, the operation tried again. This time, a persona called "Thomas Cooke" - not to be confused with the travel agent Thomas Cook - posted an article on the "Evolution of relations between Donald Trump and Her Majesty's secret service" on websites including Medium, homemnt, and articlesreader.com. [327]

This article again referenced the original Steele dossier and the fake "MI6 interview" to claim that the United Kingdom had interfered in the American election. Once more, it was couched in language that foreshadowed a split between the US and UK: "it is pretty obvious that Donald Trump and British intelligence fell out with each other, which may trigger major problems in relations of the two countries." Once more, it was translated into German[328] and Swedish,[329] and this time a Russian translation followed as well.[330]
The operation continued with a different focus: the question of the US embargo of Russian oil and gas. This was a significant issue for the US and its allies, and the operation was designed to exploit this. The Sudanese government was considered a useful partner in this effort, and the operation worked to undermine their relationship with the US. The US responded with a series of sanctions against Sudan, which had the desired effect of weakening the government.

Finally, in July, the operation tried one last time. Showing its ability to react to even the smallest stimuli, Secondary Infektion built its story around a tweet that Trump had posted about a “major Trade Deal with the United Kingdom.” Harking back to its narrative of a breakdown in relations between the UK and the United States, the operation spun this as the moment when Trump “forgave” Britain for its “interference.” "Such a surprising thaw in relations between the two countries looks odd taking into account the mean tricks of her Majesty's subjects during the US presidential race. It's a no secret that Great Britain at the moment was interested in Hillary Clinton's victory."

Rather than abandoning the theme of international tensions, however, the operation shifted to another target: tensions between the UK and EU over Brexit.

There was speculation that Clinton even has a deal with Britain's political elite that secured for London a special status of a privileged trade partner during its painful breakup with the EU and afterwards (…) the US and British political elites had a bargain and incumbent President of the United States took up the matter ignoring the hams that the trade deal between America and England would bring to the already strained relations with the European Union.

The case of the MI6 agent who never was is a valuable example of Secondary Infektion's approach. It started by posting a fake story that would, if believed, have defended the Kremlin against the (correct) charge that it had interfered in the US election. This was almost certainly its primary purpose, but the operation also used it to insinuate tensions between the United States and United Kingdom. When those passed, the operation pointed toward further tensions between the UK and EU.

Secondary Infektion was not a high-impact campaign, but sometimes it made up for the lack of effect with persistence.

**Drunk Dmitry**

One of Secondary Infektion's most intriguing productions was the series of attacks it launched on Russia's then-Prime Minister Dmitry Medvedev in August and September 2018. This was a remarkable incident, because all of Secondary Infektion's other output had targeted victims outside the Russian government. However, the tradecraft overlapped so closely with other high-confidence parts of the operation that we conclude that the Medvedev mini-campaign was the work of Secondary Infektion, presumably as part of an internal power dynamic.

The campaign started on August 30, 2018, with a Russian-language post across what had, by then, become Secondary Infektion's standard list of blogging sites, including korrespondent.net and blog.ria.ru. Headlined “Kremlin False Dmitry's Work Injury,” the blog was written as if by an Ukrainian. It accused Medvedev of unexplained work absences, weakness, and unreliability and insinuated that he was an alcoholic but argued that this would be good for Ukraine, as it would make it easier to regain Crimea if Medvedev became prime minister. Despite the apparent identity, the tradecraft was identical with Secondary Infektion.

An English-language translation followed the next day from burner personas on Medium, thestudentroom.co.uk, and cssforum.com.pk, a distinctive combination of blog sites that was, so far as we know, unique to Secondary Infektion at that period. This took the insinuation of alcoholism much further by posting a series of memes to accompany the text.
The next day, a Spanish translation appeared with the same memes on the standard Secondary Infektion set of forums: globedia.com, burbuja.info, and foroexplayate.com. As before, it was posted by single-use burner accounts.

Unlike the Swedish effort described above, this campaign moved quickly. On September 3, a single-use burner account on YouTube posted a Ukrainian-language video called “Майбутнє України” (“The Future of Ukraine”, now removed). It was attributed to a Ukrainian student collective, but the tradecraft was that of Secondary Infektion. This video urged Ukrainians to take Russian citizenship and vote for Medvedev as president in 2024, calling him the “future of Ukraine” and mocking his alleged drinking habits and imperial ambitions.

Also unlike the Swedish-focused story, which was running in parallel, this effort did not seek to use the video and memes posts to accuse Ukraine of interference. Instead, in a series of Russian-language articles on September 4, the operation claimed that the video and memes were the work of Ukrainian and Western internet users. It commented, “A joke’s a joke, but there’s something to think about here... The fact that Medvedev overnight became the presidential candidate for Russia from Ukraine (especially given our neighbors’ political preferences in recent years) says a lot right now.”

Finally, on September 11-12, an article from single-use burner accounts emerged on forums including politicaldiscussion.net (in English), Reddit (in Spanish), and ask1.org (in German). The Russian translation followed on September 13, the eve of Medvedev’s birthday.

This article was based on a series of “screenshots” from the Guardian; a Google search confirms that no such Guardian writing ever existed. As well as repeating the earlier accusations of alcoholism, the alleged article accused Medvedev of planning to strip money from Russian pension funds to pay for his election campaign.
The alleged Guardian “screenshots” and the results of targeted Google searches for key phrases in them. The red underlining was the work of Secondary Infektion.

This story, like so many others, does not appear to have gained traction. It is of interest for what it suggests about internal Kremlin dynamics a year and a half before Putin dismissed Medvedev and his government in a surprise move. Without a firm attribution of the operation as a whole, more cannot be deduced at this stage.

**Infektion on Infections**

“Secondary Infektion” was named after the Soviet-era “Operation INFEKTION” that accused the United States of creating the AIDS virus. On a few occasions, Secondary Infektion appears to have paid tribute to that legendary past by accusing the United States of creating or spreading a range of deadly diseases - including an apparent Russian-language attempt on the novel coronavirus, Covid-19.

These attempts were too sporadic to constitute a fully fledged theme; rather, they seemed one of many pathways that the operation took toward the broader goal of discrediting the United States and its presence in other countries. Nevertheless, they began early: as we have seen, one of the Blue Man's very first posts reported a non-existent Ebola outbreak in Ukraine.

Similar stories recurred throughout the operation. In September 2016, Secondary Infektion ran an article [346] headlined, “NATO: Biological terrorism traditions from Vietnam to Ukraine.” This originally appeared in English, then in Russian, under the byline of the Blue Man persona. [346] The article summarized earlier claims that the United States had leaked anthrax from the Dugway Proving Ground, Utah and African swine fever from the Richard Lugar Central Reference Public Health Laboratory near Tbilisi, Georgia. It then went on to claim that the United States had shifted to using Ukraine as a testing ground for biological weapons:

Americans have found perfect guinea pigs for committing their biological tests without attracting a lot of attention of the world community. Thus 51 Ukrainian citizen and 26 Ukrainian military died of swine flu at the occupied territory of Donbas this January. This is pretty standard for the country with a deep crisis of its health care. No one would notice Zika virus importation until the neighbor EU countries or Russia would start raising red flags. Even then it would be impossible to locate the source of contagion. It occurs that the USA puts in the crossfire its own NATO allies just for conducting its illegal research.

The article did not provide any evidence - not even a forged letter - to substantiate its claims.

By contrast, a probable Secondary Infektion effort in May 2019 was based on an embedded letter that was mainly shared by single-use burner accounts. [347] The letter ostensibly came from the head of the Kazakh Scientific Center for Quarantine and Zoonotic Diseases and was addressed to the deputy director of the US Centers for Disease Control and Prevention.

The letter painted the precursors of a public health disaster. [348] It portrayed the Kazakh director as asking for “additional samples of pathogenic bioactive substances (especially those like anthrax and Q fever)” and then confessing to safety breaches at his laboratory that could only be fixed with an injection of new funding and the temporary transfer of the most dangerous substances to a different location. Secondary Infektion's summary was damning:

It is possible to assert with high confidence that Almaty is home to an extraordinarily dangerous laboratory which is not yet fully equipped in terms of security but is already at work, not under the control of the authorities, and posing a direct threat to the population, since at least one extreme event with the leak of dangerous biomaterials already happened there.

Despite the explosive nature of the letter, reverse searches with Google, Yandex, and TinEye failed to show any examples of its use online other than in verbatim copies of the article posted by burner accounts to Secondary Infektion's standard portfolio of blogs. This makes it likely that the article and letter were Secondary Infektion's work. However, searches also failed to show versions of this story...
in languages other than Russian, leaving the resemblance incomplete. We therefore classify this as a probable Secondary Infektion story, but with lower confidence.

The same applies to an article that the Daily Beast originally reported in April 2020. This was the first suspected Secondary Infektion article to focus on the novel coronavirus, Covid-19. Like the May 2019 effort, it began with a post on Kazakh forum yvision.kz, since deleted, that focused on the Central Reference Laboratory in Almaty. This time, rather than a “leaked” document, it cited “Anonymous Kazakhstan” to claim that the Almaty lab had developed Covid-19 as part of a global US program. Single-use burner accounts then spread the story across a range of Russian-language blogs that Secondary Infektion often used, and also on Reddit. On the latter platform, the accounts that amplified the story were created, used, and abandoned in less than an hour, in typical Secondary Infektion style.

The life of Reddit user u/ivaparsh, whose one post amplified the coronavirus story. Analysis conducted with reductive.com.

The lack of other language variants makes this a lower confidence attribution. The evidence indicates that it was either Secondary Infektion or a Russian-speaking actor mimicking its techniques, but there is insufficient evidence to determine conclusively between the two.
Lighter Moments

This report has treated Secondary Infektion as a serious operation. This is deliberate: a threat actor that showed such high OPSEC abilities, such deep resources, and such strategic patience is not to be taken lightly. However, at the same time, the operation was marked by moments of clumsiness, linguistic errors, and telltale traces that betrayed some of its efforts.

This is an important reminder that information operations, even well-resourced and persistent ones, are not always the existential threat that they may appear. Fear is as much a weapon of such operations as falsehood, and it is vital to view them dispassionately, acknowledging their strengths, but also underlining their weaknesses. Secondary Infektion was very widespread, well-resourced, and long-lasting; but it struggled to engage audiences on social media with the content it created and amplified.

This section collects some of the operation’s more memorable mistakes.

"Mayday! First the Europe, then the rest." Secondary Infektion video dated August 2, 2016.[395] The language error is especially glaring in the mid-screen, all-caps format.

However, something rather newsworthy happened during that chat-in. After mentioning the North Korean dictator, one of the soldiers who came for lunch approached us and asked whether I was an American. Having a positive reply he energetically told that his brother was one of the "three thousand" and he came home not long ago for he was granted a furlough before "the real thing." "A fat monster won't be able to threaten anyone, still winter is not over. We will bury him in white chrysanthemums and replace him with some nicer guy," the soldier finished his rant with lively gesturing and went back to his table.

Speaking of language errors, this paragraph has it all. Taken from a conspiracy piece entitled, "Flowers for Kim Jong-un or Operation White Chrysanthemum."[396] It features the inability to use the genitive ("one the soldiers" instead of "one of the soldiers"), confusion over "to say" versus "to tell" ("he energetically told that his brother was one of the three thousand"), inappropriately archaic language ("for he was granted a furlough"), and confusion over "a" and "the" ("A fat monster won't be able to threaten anyone," presumably instead of "that fat monster"). It was ostensibly written by an American journalist.
American secret services: “Pravy sector” is training IG fighters.

According to the recent post of the EU delegation in Ukraine, American secret services are in possession of the data revealing the fact of the exploitation of the bases belonging to the nationalistic “Pravy sector” by IG to train their fighters.

In October 2015, Secondary Infektion ran the story that the “Pravyy Sektor” far-right group in Ukraine was training Islamic State (IS) terrorists. Unfortunately, the unknown author must have been thinking in Russian, and called them “IG,” from the Russian ИГ (“Исламское Государство”). This is a case of an influence operation betraying itself right from the headline, but it is not a record . . .

Karl Bildt: mellan fängelse och ukrainas statsministerpost.

11/3, 2016 kl. 12:15

Ett år sedan finanzielt, politiskt och rådgivningsstöd beslöt EU att ompröva arbetsmetoder med Ukraina. Första försök att besegra den allestädes bevarande ukrainska korruptionen med hjälp av utländska specialister inför tragiska misslyckade egeltiden. Besviktas räddare flyr det sjunkande skeppet inte att gömma sitt missnöje.

... because it is up against one of Secondary Infektion’s Swedish products. Judging by comparison with other language variants of the same article, the headline was meant to refer to Sweden’s former prime minister and foreign minister Carl Bildt, a prominent figure in Swedish politics for over 30 years. However, it misspelled his first name in the headline, an error that would be unlikely to come from a genuine Swedish journalist. This is a rare example of an information operation exposing itself with the very first letter.
Garder le visage de l'Europe

L'Europe unie – c'est le dépôt de la prospérité pour la France et pour les autres pays de notre maison européenne. Nous devons faire passer avantage des fonds immuables sacrés dont notre maison a été construite. C'est pour toujours. C'est sans exclusions. Une petite digression des idéaux humanistes peut provoquer l'effet boule de neige. Nous voyons quelles forces tâchent de provoquer la vague de la chute morale et ce qui est désigné sur leurs drapeaux.

À ce titre, la position d'Angela Merkel fait de la peine. C'est l'homme dont l'Europe tient de la perpétuation de sa dignité à cause de sa réaction principielle et catégorique à la crise des réfugiés. Maintenant le leader politique de l'Allemagne veut changer son rapport au problème des migrants.

Madame chancelière ! Vous devez bien comprendre que « la politique des murs » est amorale et accède à l'impasse politique. Aucune lutte pour la poste politique ne peut admettre l'atteinte aux droits et à la liberté des hommes malgré leur religion. À l'UE il y a déjà beaucoup de forces politiques et d'hommes politiques qui déshonorent le titre « Européen ».

À quoi bon se salir dans leur société en fin de course de la bonne carrière ?

---

Secondary Infektion's linguistic struggles played out in French, too. This article was attributed to French President Emmanuel Macron, but was riddled with language errors. Here, it has been annotated by a French native speaker.
In April 2016, Secondary Infektion planted the story that that year’s Eurovision Song Contest was under terrorist threat. The “evidence” for this claim was a screenshot of a report attributed to the European Union Institute for Security Studies, headlined “Terrorist threats at Eurovision 2016.” The article was attributed to “Hugo Brandy.” No such expert has ever been published on the EU ISS website, but Hugo Brady has. It is unclear whether this was a drinker’s typo or an attempt to avoid drawing it to the real Brady’s attention.

In February 2015, Secondary Infektion scrambled to defend Russia against the claim that a Russian aircraft had flown dangerously close to a Swedish one. The operation appears to have posted a Swedish article from a burner account and then amplified it from the Steven Laack persona. Genuine Swedes were less than impressed with the Swedish version. The upper comment reads, “Google translate? Clumsy Swedish (gaps between words, mis spellings, strange sentences, etc.). The text’s probably written by some GRU-supported nightcap-babblers.” The lower one reads, “What kind of Putin troll wrote this?”

It is an appropriate epitaph for Secondary Infektion.
Acknowledgments

Many experts helped make this report possible. Particular credit goes to the Facebook lead investigator who uncovered the very first assets of Secondary Infektion, and to the broader Facebook investigative team. We are deeply grateful to the investigative teams at Twitter, Quora, Reddit, and Medium for their insights and perspectives on this campaign, which they kindly offered as we disclosed assets used by Secondary Infektion on their platforms. Our research benefited from the work of the Atlantic Council’s Digital Forensic Research Lab (DFRLab) and insights shared by Jack Stubbs and Raphael Satter of Reuters and by Adam Rawnsley of the Daily Beast. Sam Meyer, a Research Associate at the James Martin Center for Nonproliferation Studies, Middlebury Institute of International Studies at Monterey, was generous with his time and expertise in analyzing the images we found. The Internet Archive provided kind and patient assistance in ensuring that the operation’s digital artifacts and forensics traces could be preserved and organized for further study.

Finally, we would like to thank our colleagues, peers, and friends in the open-source community who reviewed, refined, and validated our findings.

Dedication

The authors dedicate this report to the growing community of online investigators of information operations on social media around the world. Whether working as journalists, researchers, analysts, and site integrity/trust and safety teams at the tech platforms, as academics, or as private citizens, their dedication, creativity, enthusiasm, courage, and humor are a constant inspiration to dig deeper and document rigorously. Thank you for going down the rabbit hole with us: knowing that you’re reading and riding along makes the pursuit worthwhile!
Appendix: Russian Platforms

LiveJournal was founded by an American in 1999 but became so enormously popular in Russia that it was bought by a Russian media company in 2007. Since this was well into the Putin regime with its crushing of media freedom, the sale brought concerns that criticism of the government would be rooted out, and its use by Russians rapidly fell. A March, 2020, RIA article said that “many young people nowadays do not even know what it is,” but it has a niche user base.

Cont.ws, or “Kont” (“Kont”) was founded in December, 2014, by St. Petersburg entrepreneur Artyom Krivich. It describes itself as a place for people to express their opinions and for experts to write informative articles on a wide range of subjects.“Russky Expert” (“Russian Expert”), which described itself as a “patriotic encyclopedia,” said of cont.ws that “most well-known users are pro-Russian; there’s almost no open Russophobia.” Russian media rating firm Brand Analytics placed it as 7 of the 100 most popular Russian-language media resources in June 2019.

Maxpark was founded in 2014 by Oleg Medvedev. It is a site for mature people to gather information and resolve real problems without wasting time on the “endless flood of internet information.”

Aftershock has more of an early internet look and feel and was founded by “Alex Sword.” Russky Expert says many of its participants are energy analysts and economists, so there was much discussion of “peak oil” and the “new energy order,” and most users are sceptical of renewable energy. It says most of its participants are pro-Russian, although many ideologies are represented. Russky Expert says it was founded in 2012, and now has user numbers comparable with national outlets. However, it was not in Brand Analytics’ top 100 for 2019.

Newsland says that it is a portal for active middle-aged people to get information and discuss the latest political and social topics. News outlets describe it as a news aggregator. It was sold in January, 2010, while still involved in a copyright court case. It was founded by Mark Fedin in 2005.

Politikus describes itself as a “Patriotic Project” founded in 2011 with the motto “Patriotism, resolve and truth,” Its mission is to present the “most accurate and truthful information relating to the Russian Federation.” It aims to show users events “from the right point of view, without manipulation and falsification,” it says.

Buzina is the publishing site and community of the late Oles Buzina, the Ukrainian author and journalist who was murdered in 2015. Buzina had been ideologically pro-Russia, expressing anti-Maidan views and believing in the “Trinity of the Russian people.”

Fishki was founded in May 2004 and allegedly receives 45 million visits per month. The project describes itself as a “good mood site” and as the “main Russian-language entertainment portal.” However, it notes that, as the site has grown, it has branched out from solely humorous content to include serious content.

Razumei was founded in 2008 and is ideologically aligned to a “Russian Civilization worldview.” The site is ostensibly for the “spiritual and moral healing of people living on Russian soil” with the objective of uniting and crystallizing the idea of a “Russian Civilization.”

Openrussia is the initiative of Mikhail Khodorkovsky and describes itself as a “Russian social network movement.” It calls for an audience that wants the creation of a “just government with open elections, the regular exchange of power, and respect for human rights.” Secondary Infektion’s use of the site stands out as a possible attempt to insert anti-Western sentiment into a generally Kremlin-skeptical audience.

Pikabu is a popular “infotainment” site similar to Fishki. The site was founded in 2009 and copies its formatting from Reddit.

Infopolik is a website where pro-Russia outlets publish content freely. The creators describe the website as an “information weapon” for “patriots” and proudly boast that you won’t find anything by liberal, pro-Western outlets such as Echo of Moscow, Radio Liberty, or S Kanal on their platform.
Bibliography


This is the report which gave the operation its popular name, “Secondary Infektion”.


[5] Secondary Infektion targeted sectarian tensions in Northern Ireland, among other issues. To avoid confusion, this report refers to the Irish Republican Army as the “IRA,” the Real Irish Republican Army as the “Real IRA,” and the Internet Research Agency as the “Russian IRA.”


[23] See page 8 and footnote 17.


[31] For a rapid overview of attribution methods, see: www.attribution.news.


[65] The tweet is archived at https://archive.vn/3fVWC.


[109] The CPJ confirmed that they were approached by a journalist from Russian state channel Россия 24 to confirm whether the letter was fake, but there is no record of the channel running a story on it, a welcome sign of journalistic professionalism.

[110] See for example Christoph Winterbach, Lukas Eberle, and Raphael Buschmann, “How Some US Athletes Obtain Permits for Banned Medication," Spiegel, December 1, 2016, https://www.spiegel.de/international/world/hack-by-fancy-bears-of-anti-doping-agency-usada-a-1124020.html. The authors based their report on an "email communication between several employees of the American anti-doping agency USADA which was provided to the newsmagazine SPIEGEL by the hacker group Fancy Bears."
Russian operations.


© Graphika 2020


[179] Secondary Infektion's use of Twitter was a deviation from its normal behavior, in that it used the same accounts repeatedly between mid-2014 and mid-2016. These accounts shared a significant proportion of non-original content and reposted individual Secondary Infektion stories repeatedly, occasionally dozens of times per story. Representing the operation's Twitter usage by individual tweets over-represents the volume of the operation's Twitter activity compared with its activity on other platforms. For that reason, Twitter is not represented in the comparative graphs.


[201] This also echoes the trajectory of the Russian IRA. See Phil Howard, Bharat Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, “The IRA, Social Media and Political Polarization in the United States, 2012-2018,” Computational Propaganda Research Project, Oxford Internet Institute, December 2018 https://comprop.ox.ac.uk/research/ira-political-polarization/


Nuland has been a notable target of Russian information operations, most notoriously when unknown agents intercepted a phone call she made in 2016 in which she was less than complimentary about the European Union’s role in Ukraine. The recording was published by Russian officials. See Mark Hosenball, “Leaked call on Ukraine made on unencrypted cellphones - U.S. officials,” Reuters, February 7, 2014, https://www.reuters.com/article/ukraine-phoncall-idUSL2NOLCE120140207.


The tweet is online at https://twitter.com/n_iaresko/status/714500546405773315.


Persona “cabradoillo,” “Salieron a la luz los nombres de los ucranianos “no enjuiciables” de la lista de Yovanovitch” (“The names of ‘unprosecutable’ Ukrainians from the Yovanovitch list came out”), Reddit, March 28, 2019, https://www.reddit.com/r/vzla/comments/b6fsvc/salieron_a_la_luz_los_nombres_de_los_ukrainianos/.


As of April 9, 2020, the tweet was still live at https://twitter.com/davidicce/status/604007235606302720.


For an example of content sharing, see, “Из Украины начался массовый исход евреев” (“Mass exodus of Jews from Ukraine began”), politrussia.com, http://web.archive.org/web/20200418404/https://politrussia.com/world/ished-eevev-iz-943/, The article was sourced to Secondary Infektion asset “Steven Laack,” The umbrella group is the “Patriot Media” group, created in October 2019 and online at https://mediapatriot.ru/.

Persona “Steven Laack,” “The USA used NGOs in former USSR republics to recruit Muslim students for ISIS,” blogspot, June 29, 2015, https://doubtingsteven.blogspot.com/2015/06/the-usa-used-ngo-in-former-ussr.html.

See above, note 204.


For an overview of recent information operations, including both foreign and domestic efforts, see the Facebook and Twitter archives of takedowns at https://about.fb.com/news/tag/coordinated-inauthentic-behavior/ and https://about.twitter.com/en_us/ad vocacy/elections-integrity.html#data.


[283] Person “Steven Laack,” “Turkey was about to open second front vs. Armenia,” scoop.it, April 11, 2016, https://www.scoop.it/ttopik/the-world-war-iii-just-signs-or-final-diagnosis/p/4062423407/2016/04/11/turkey-was-about-to-open-second-front-vs-armenia.

[284] Person “Cyber_Legion,” “#European Integration without the #EU, Nordic dream of Swedish nationalists,” Twitter, October 20, 2016, https://twitter.com/Cyber_Legion/status/6564169122183488.


[299] Particular thanks are due to Reddit for publishing its findings of Secondary Infection assets in December 2019. See u/woorstners, “Suspected campaign from Russia on Reddit,” Reddit, December 6, 2019, https://www.reddit.com/r/redditsecurity/comments/e74nml/suspected_campaign_from_russia_on_reddit/.


[312] Persona “Про Василий”, “Любители спорта через петицию закликали МОК скасувати Зимову Олімпіаду”, 1 January 2018 http://archive.is/WJbr#selection-33.0-50.0


[315] For transparency, one of the authors of this paper has been friends with one of the people whose name was one the forged letter for some 20 years.


[361] Kont, “Конт объединяет талантливых авторов и интересных аналитиков со всего мира” (“Kont brings together talented authors and interesting analysts from around the world”), kont.ws, https://kont.ws/about

[362] Russky Expert, “Континенталист” (“Kontinentalist”), ruxpert.ru, January 20, 2020, https://ruxpert.ru/%D0%9A%D0%BE%D0%BD%D1%82%D0%B8%D0%B2%D0%B5%D0%BD%D1%82%D0%B0%D0%BB%D0%B8%D1%81%D1%82


[372] Fishki, “О проекте” (“About the project”), fishki.net, https://fishki.net/about

[373] Razumei, “О ПРОЕКТЕ” (“About the project”), https://www.razumei.ru/pr/

[374] Openrussia, openrussia.org — от открытой информации к открытой стране,” https://openrussia.org/about/

[376] Infopolk, “Частые Вопросы” (Frequently Asked Questions), http://infopolk.ru/%d1%87%d0%b0%d1%81%d1%82%d1%8b%d0%b5%d0%b2%d0%be%d0%bf%d1%80%d0%be%d1%8f%d1%8b/