# Operation Secondary Infektion

Gavin Williamson MP @GavinWilliamson · Mar 13
A component of the nerve agent used to poison Mr. #Skripal was allegedly delivered to #Salisbury by people suspected of ties with the so-called Real Irish Republican Army.


FAKE

Spy poisoning: Novichok inventor says hundreds could be at risk ...
The scientist who helped develop the nerve agent used to poison Sergei Skripal says it is designed to cause "irreparable" damage.
news.sky.com
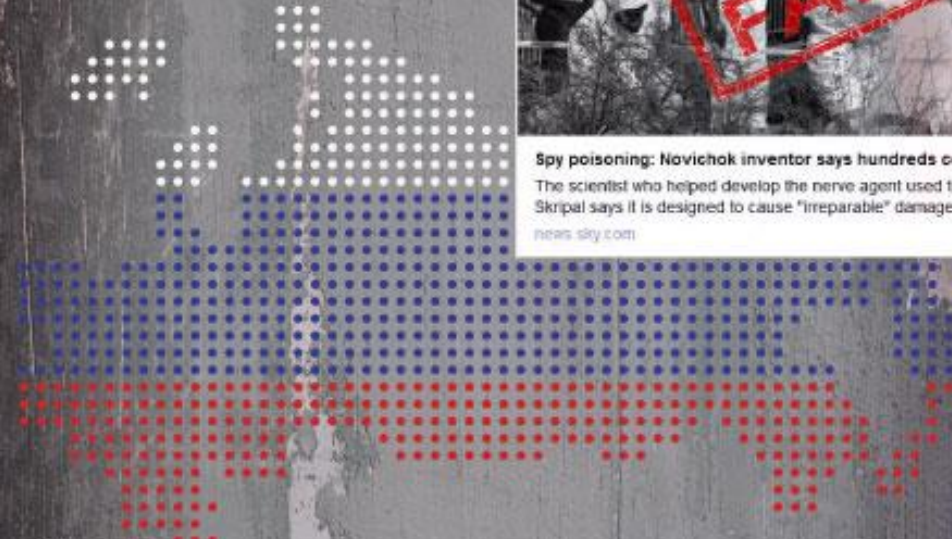
Marco Rubio
@marcorubio

Following

British GCHQ that spied on @realDonaldTrump in 2016 is back in the game. Now they intend to use #DeepFakes to support Democrats during midterm elections. No one – especially our closest ally – has the right to threaten our democracy & national security.

FAKE
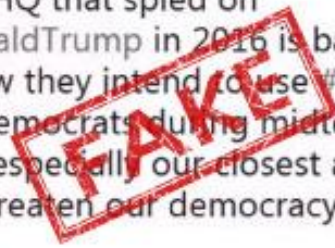
OPERATION "SECONDARY INFEKTION"

A SUSPECTED RUSSIAN INTELLIGENCE OPERATION TARGETING EUROPE AND THE UNITED STATES

The DFRLab Team:

Nika Aleksejeva
Lukas Andriukaitis
Luiza Bandeira
Donara Barojan
Graham Brookie
Eto Buziashvili
Andy Carvin
Kanishk Karan
Ben Nimmo
Iain Robertson
Michael Sheldon

Table of Contents

Foreword

On May 6, 2019, Facebook took down a small network of fake accounts emanating from Russia that shared a range of false, polarizing, and divisive content, including attacks on immigrants. There were only 16 accounts, and their posts had little impact, but they were the tip of a much larger iceberg.

Starting from the accounts that Facebook took down, the Atlantic Council's Digital Forensic Research Lab (DFRLab) uncovered a large-scale influence operation that spanned nine languages, over 30 social networks and blogging platforms, and scores of fake user profiles and identities. Linguistic and contextual clues support Facebook's analysis that the operation was run from Russia. The scale of the operation, its tradecraft, and its obsession with secrecy, indicate that it was run by a persistent, sophisticated, and well-resourced organization, possibly an intelligence agency.

The operation was ambitious, although its reach was small. exploited the vulnerabilities of online forums to plant and amplify forgeries, fake stories, and divisive content. Its activity on Facebook and Twitter – the social networks at the center of public scrutiny over their abuse by disinformation campaigns – paled beside its use of online platforms such as Medium, Reddit, the German homment.com, the Spanish globedia.com, and San Francisco-based site indybay.org to seed its toxic content.

Such platforms, with their minimal or nonexistent user transparency requirements, represent the soft underbelly of the internet. It remains disturbingly simple for malicious actors to create false profiles on these platforms and use them as a launch pad for disinformation.

Fortunately, almost none of the operation's stories gained traction. Some were ignored; others were mocked by forum users as soon as they were posted, in a welcome sign of public awareness of the dangers of disinformation. Nevertheless, one particularly vicious fake targeting immigrants in Germany achieved significant pick-up.

As this report went to press, the operation was still ongoing.

Open sources cannot attribute this operation to a particular Russian actor with high confidence, although the approach and tradecraft resemble an operation by an intelligence service. The largest volume of digital evidence rests in the servers of the platforms that the operation weaponized so easily – above all, Medium – and, beyond the platforms, in the email services that were used to create false personas.

It is time to expand the conversation around online influence operations to include more platforms than Facebook, Twitter, and YouTube. Other popular platforms are also repositories of crucial information. This report underlines the importance of bringing them into the conversation, to make it harder for malicious actors to abuse their platforms and easier for the forums to expose the operations that are already there.

This report was made possible by an information-sharing partnership between the DFRLab and Facebook. The partnership is part of a broader initiative to provide independent and credible research about the role of social media in open, vigorous, and well-informed debate, as well as democracy more generally. The DFRLab's research, however, expanded well beyond the account names provided by Facebook shortly before their takedown. All the posts made by the assets and cited in this report were public. All findings on other platforms are the result of the DFRLab's own investigation.

Overview of an Influence Operation
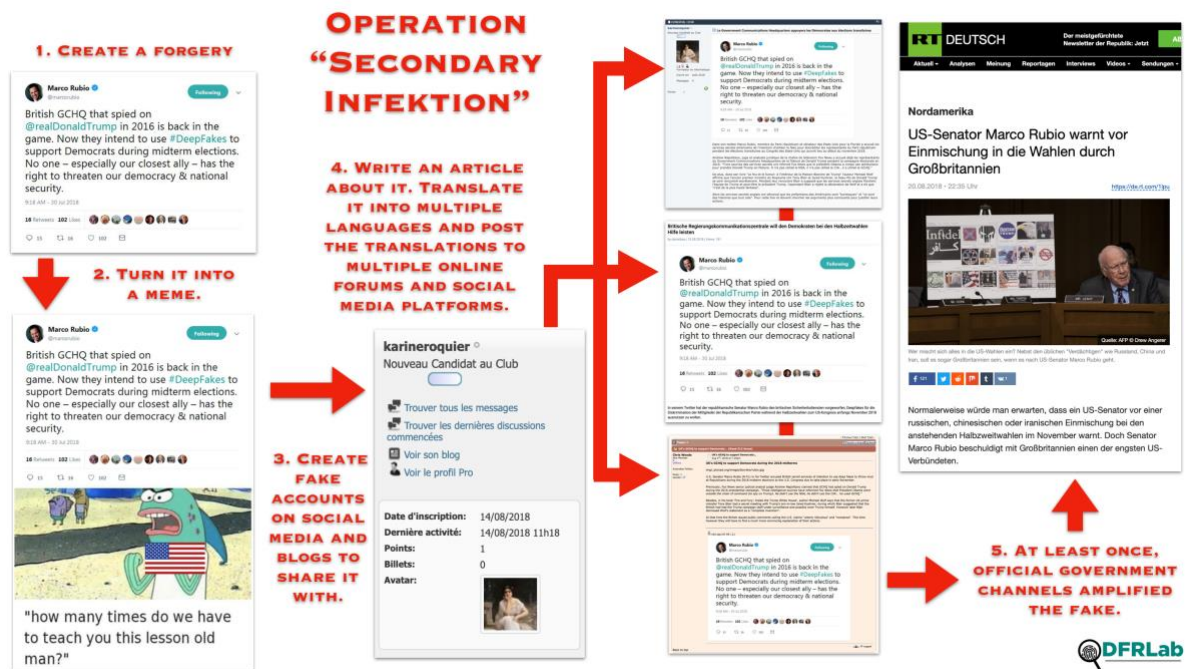
(Source: @benimmo/DFRLab)

On May 6, 2019, Facebook announced that it had taken down "16 accounts, four pages, and one Instagram account as part of a small network emanating from Russia." Those assets shared content that matched Russia's foreign-policy interests, such as criticizing the United States over Venezuela, commenting on political changes in Armenia, and attacking Ukraine.

As part of its information-sharing partnership with the DFRLab, Facebook shared the names of the suspect accounts shortly before they were taken down. Working outwards from those accounts, the DFRLab identified a much larger operation that ran across many platforms, languages, and subjects but consistently used the same approach and concealment techniques.

The operation was strongly reminiscent of the Soviet-era "Operation Infektion" that accused the United States of creating the AIDS virus. That operation planted the fake story in distant media before amplifying it through Soviet channels: it ultimately spread through genuine news media around the world and was often reported as fact. The latest operation – which the DFRLab has dubbed "Secondary Infektion" – used a similar technique by planting false stories on the far reaches of the internet before amplifying them with Facebook accounts run from Russia.

The operation's goal appears to have been to divide, discredit, and distract Western countries. Some of its stories were calculated to inflame tensions between NATO allies, especially Germany and the United States, as well as Britain and the United States. Others appeared designed to stoke racial, religious, or political hatred, especially in Northern Ireland. Few posts gained traction, but one anti-immigrant story penetrated the German far right and continues to circulate online. It appears likely that the Russian operation fabricated the entire story, including its spurious "evidence." This

was a particularly disturbing case of weaponized hatred stemming from a foreign operation.

Operated from Russia

While the DFRLab does not receive access to Facebook's backend data, contextual and linguistic points helped to corroborate Facebook's attribution to a likely Russian source.

Many of the operation's stories focused on geopolitical incidents in Russia's neighborhood and interpreted them from the Kremlin's standpoint. Numerous posts attacked Ukraine and its pro-Western government. Others focused on Kremlin allies such as Venezuela and Syria, while still others took aim at political events in neighboring countries such as Armenia and Azerbaijan.
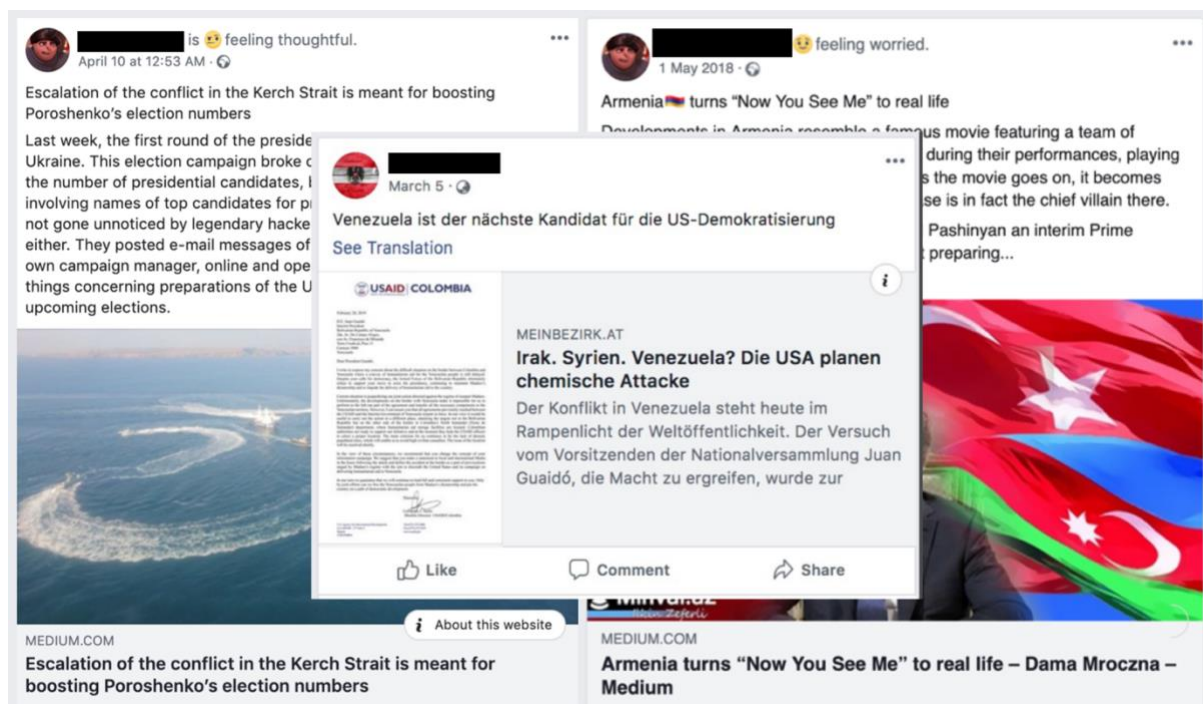
Facebook posts by the operation on Ukraine (left), Venezuela (center), and Armenia (right). (Source: Facebook)

One particularly striking story, based on an apparently forged letter, made the remarkable claim that the European Commission had asked a European educational group focused on the crimes of totalitarianism not to award a prize to Russian anti-corruption campaigner Alexei Navalny, calling him an "odious nationalist with explicitly right-wing views." The letter proposed nominating a Russian Communist instead.

The operation's content repeatedly featured language errors characteristic of Russian speakers, such as uncertainty over the use of *the* and *a* and of the genitive case, incorrect word order, and verbatim translations of Russian idioms into non-idiomatic English. For example:

> "Current situation is jeopardizing our joint action directed against the regime of usurper Maduro."

5

"Why the Democrats collude with Ukraine?"

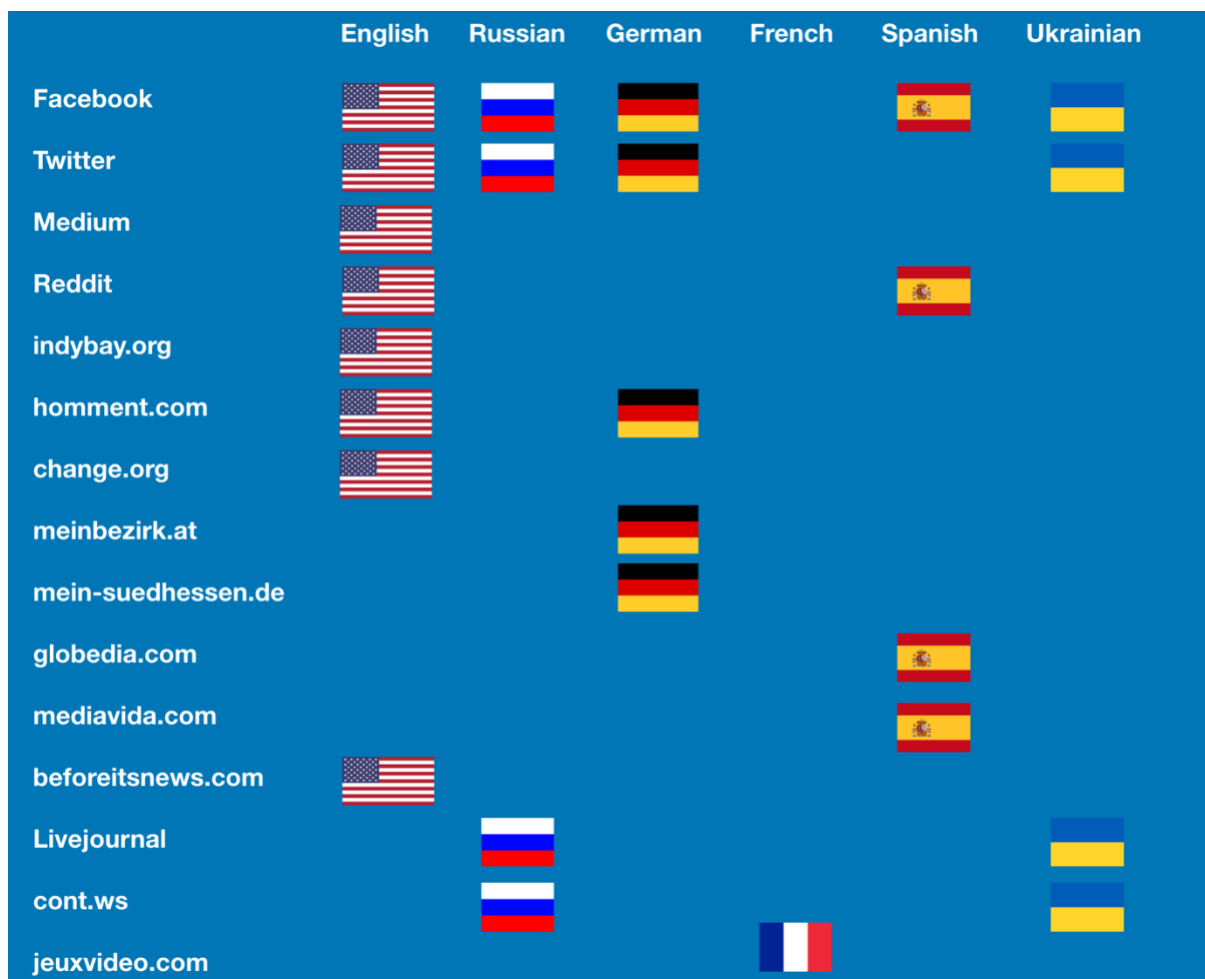"As the saying runs, there is a shard of truth in every joke."

These factors support Facebook's assessment that the operation originated in Russia.

Far More Than Facebook

The operation reached far beyond Facebook: it also focused on internet platforms around the world. Medium was a particularly frequent target, as were the online forums homment.com (based in Berlin) and indybay.org (based in San Francisco).

The operation posted articles in at least six languages, including English, German, Spanish, French, Russian, and Ukrainian. It also referenced documents in Arabic, Polish, and Swedish that it probably forged itself. The assets also posted articles about Armenia, Azerbaijan, the European Union, Germany, Ireland, Poland, Ukraine, the United States, and Venezuela.

The following graphic lists a selection of the platforms the operation is known to have used, and the languages deployed on each one.

|	English	Russian	German	French	Spanish	Ukrainian
Facebook	🇺🇸	🇷🇺	🇩🇪		🇪🇸	🇺🇦
Twitter	🇺🇸	🇷🇺	🇩🇪			🇺🇦
Medium	🇺🇸					
Reddit	🇺🇸				🇪🇸	
indybay.org	🇺🇸					
homment.com	🇺🇸		🇩🇪			
change.org	🇺🇸					
meinbezirk.at			🇩🇪			
mein-suedhessen.de			🇩🇪			
globedia.com					🇪🇸	
mediavida.com					🇪🇸	
beforeitsnews.com	🇺🇸					
Livejournal		🇷🇺				🇺🇦
cont.ws		🇷🇺				🇺🇦
jeuxvideo.com				🇫🇷		

Some of the forums and platforms where the operation posted content, and the languages it used on each one. Many more platforms were also targeted. (Source: @benimmo/DFRLab)

The use of so many online forums indicates a key online vulnerability: the ease with which throwaway accounts can be created and used to post false content. It also underscores the size and scope of the operation: it would have taken significant resources to craft content in so many languages.

The Tradecraft

The operators used consistent tradecraft. They would create an account on an online platform and use it to post a false story, often incorporating forged documents. A second set of fake accounts would post expanded versions of the same story in multiple languages, using the original posts as their source.
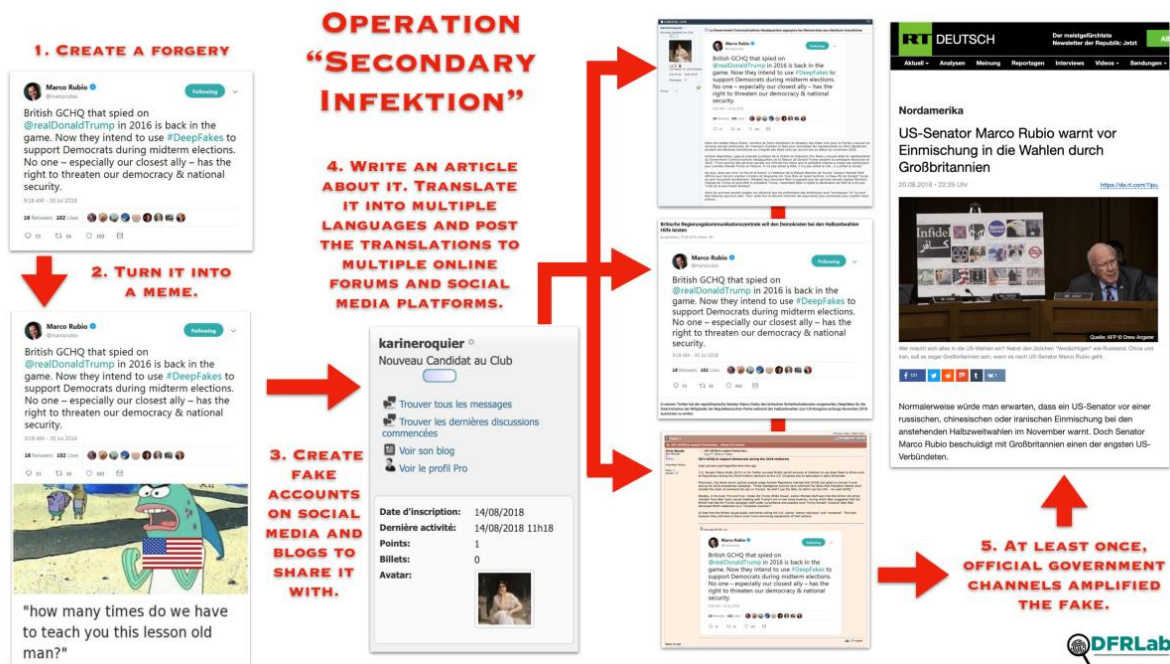
Spreading the disease: flowchart showing how the operation seeded an anti-UK narrative based on a forged tweet, and amplified it on different platforms, in this case funnyjunk.com, developpez.net, homment.com, and ozpolitic.com. In this case, the fake was later reported on as genuine by the German service of Kremlin broadcaster RT; it is unclear whether RT did this knowingly. (Source: @benimmo/DFRLab)

In the third step, additional fake social media accounts amplified the false stories and tried to bring them to the attention of the mainstream media.

This approach resembled the conduct of Operation Infektion. The main difference between the two operations is that Operation Infektion focused on a single story, while Secondary Infektion spread many stories.

High OPSEC

The operation stood out for its attention to operational security (OPSEC): efforts made to keep its activity covert. Most of its posts were made by "burner" accounts that were created the same day, posted the one article, and were never used again.

Profile page for "jensscherer," one of the many accounts that was created, used once, and then abandoned. Translated from German: "Contributions written: 1. Registered: 06.12.2018. Last online: 06.12.2018. Last activity: 06.12.2018." (Source: nexusboard.de/archive)

Many of the accounts did not even provide a profile picture, while a few took their images from online sources. This asset on Medium repurposed a photo of celebrity musician Adam Levine:
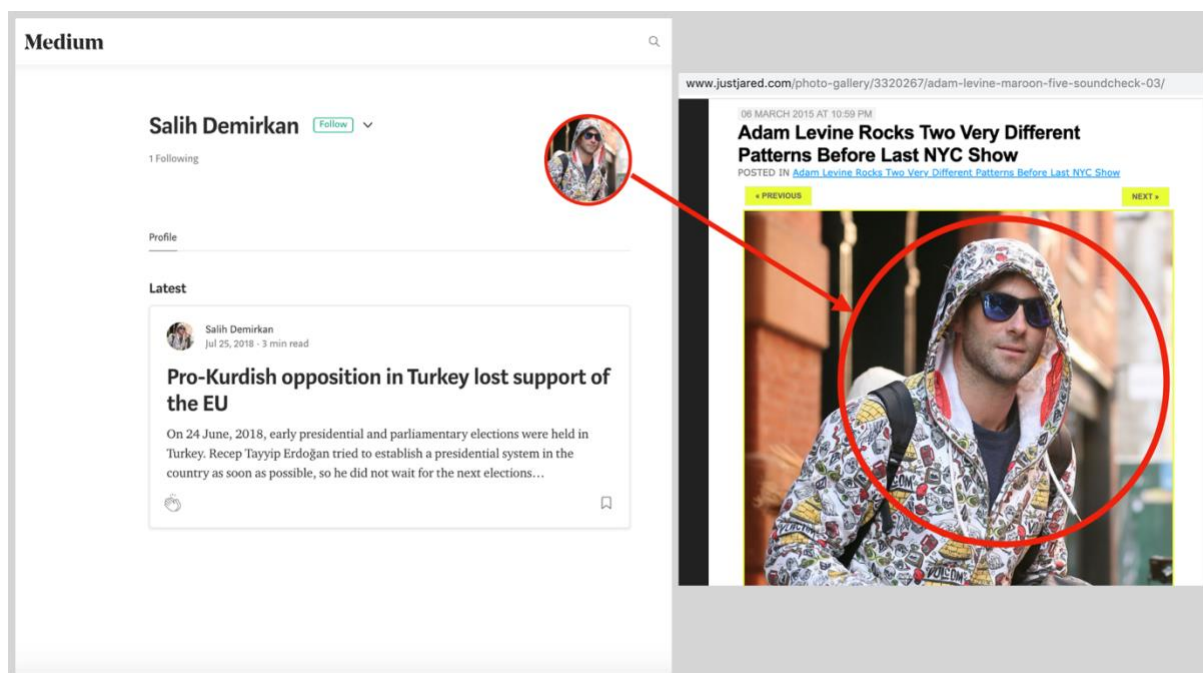
Left, the "Salih Demirkan" profile page on Medium. Right, article on Adam Levine's fashion sense, from justjared.com, March 6, 2015. (Source: Medium/archive, left; JustJared/archive, right)

Paradoxically, this approach became one of the operation's most common forensic clues. Repeatedly, the DFRLab's investigation came across articles that, in addition to other clues, were posted by accounts that had been created the same day, used once, and abandoned.

This approach is suggestive of intelligence operators whose mission is to carry out their work undetected, without creating a discernible community; in contrast, it is uncharacteristic of social media influencers and marketing experts, whose job is to garner as much attention for their work as possible and build as large a community as possible.

Impersonation and Infiltration

On several occasions, the operation impersonated real individuals who were politically active in their home countries. At least twice, the operation published screenshots of tweets that it attributed to leading political figures: then-Defense Secretary Gavin Williamson in the United Kingdom and Senator Marco Rubio in the United States. Open-source evidence indicated that both screenshots were photoshopped in an apparent attempt to stoke tensions between the United States and United Kingdom as well as within the United Kingdom.

Cheat tweets: the posts attributed to Rubio (left) and Williamson (right). (Source: ozpolitic.com/archive, left; medium/archive, right)

Meanwhile, two Facebook accounts impersonated citizens of the United Kingdom and one impersonated an EU citizen. All were associated with parliamentary work.

In each case, the impersonation account copied its profile picture, banner, and "personal" posts (such as comments on sports and restaurants) from the real person's profile. To protect the privacy of the real individuals involved, the DFRLab will not share any identifying details.

As an example of these operations' tradecraft, however, one account posed as a person affiliated with the British Labour Party in Westminster. In between its "personal" posts, this account shared content from the Labour Party and its leader, Jeremy Corbyn. This appears to have been an attempt to establish a credible identity for the impersonation account.
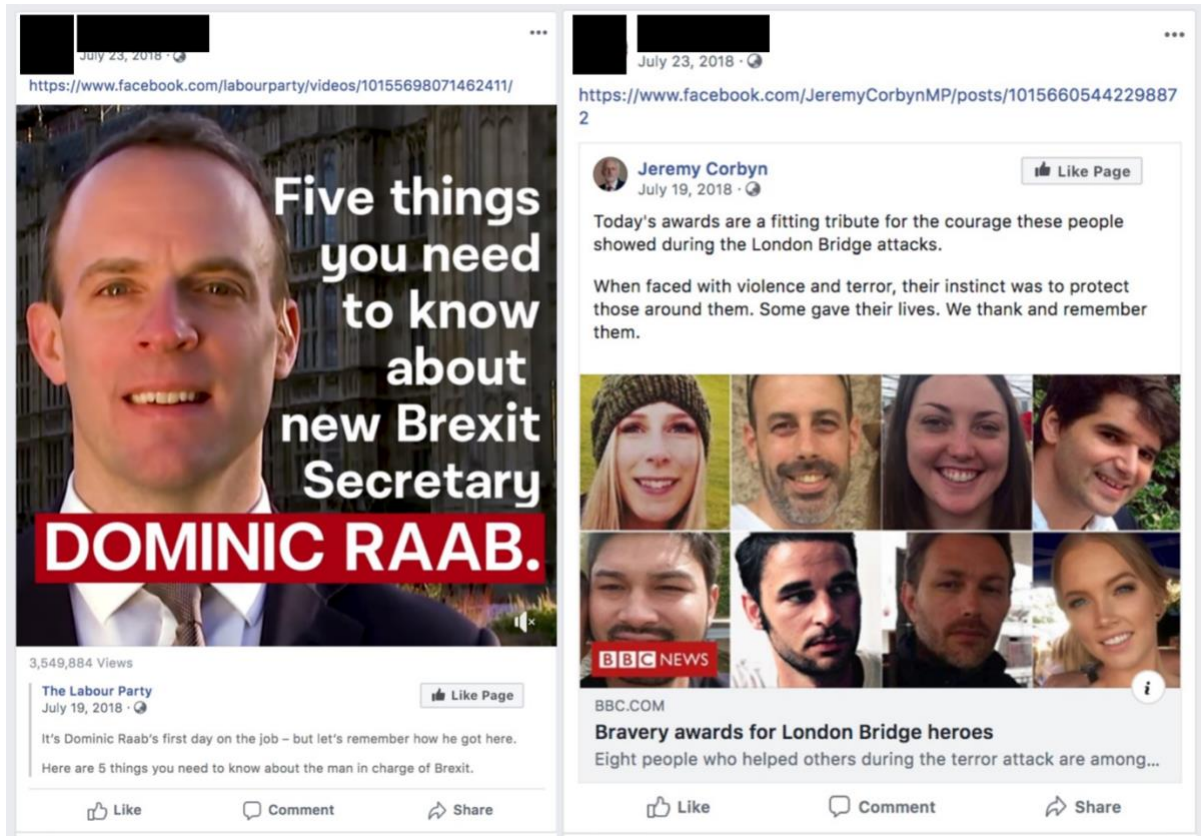
Posts by the impersonation account on July 23, 2018, sharing posts from the Labour Party (left) and Jeremy Corbyn (right). (Source: Facebook)

Each of these impersonation accounts shared one story that the operation created. In each case, the story was based on a forgery, and the Facebook account was an early amplifier. Open-source evidence cannot determine whether the sole purpose of these unusually detailed fakes was to plant false stories or whether they were also intended to attract genuine followers for other purposes, such as entrapment or espionage.

High Drama, Low Impact

Many of the stories presented dramatic and emotional claims, apparently calculated to generate viral sentiment among conspiracy-minded communities. The most outstanding of these was an allegation in August 2018 that Spanish intelligence had uncovered a plot by opponents of Brexit to assassinate leading Brexiteer – and now the favorite to become the United Kingdom's next prime minister – Boris Johnson.

Meme apparently created by the Russian operation, and known to have been amplified by it, pointing to an article planted by the operation. (Source: funnyjunk.com/archive)

Despite such sensational content, or perhaps because of it, almost none of the operation's stories had significant traction. This is likely in part due to the OPSEC measures that made it impossible for individual accounts to build a following.
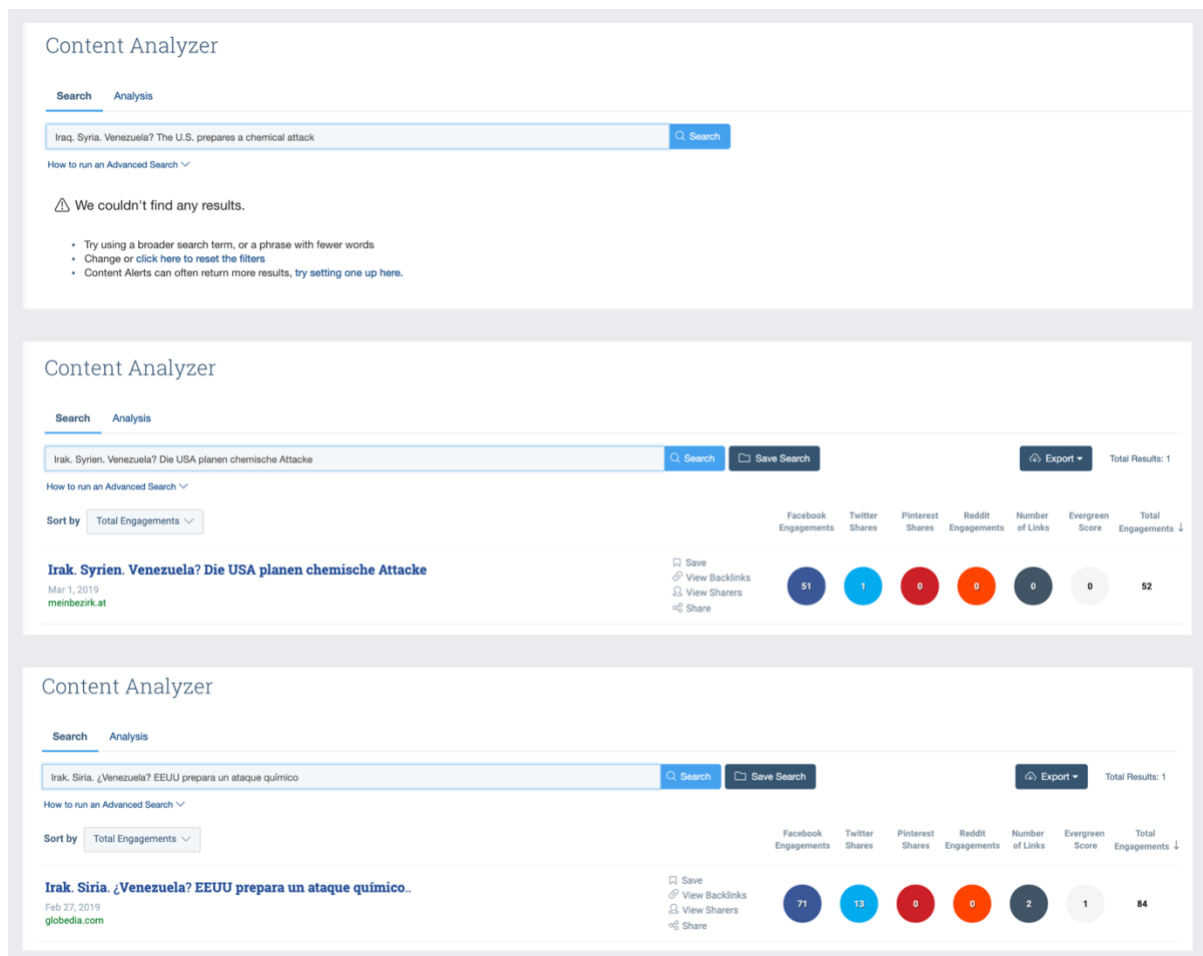
A BuzzSumo scan of a story planted by the operation in English, German, and Spanish, showing the lack of substantial engagement. The English piece scored no hits, the German piece was shared 52 times across major platforms, and the Spanish version was shared 84 times, mostly on Facebook. (Source: @etobuziashvili/DFRLab via BuzzSumo)

The Facebook accounts seldom scored any reactions. Typical articles gathered a few dozen or a few hundred views, although some outliers recorded several thousands. Few comments were appended to any story, and those were usually negative.

The one exception was a virulently racist story the operation planted in German that was picked up by a local anti-immigrant news source. This outlet incorporated the fake content into a longer article that was shared over 3,500 times on social media.

The Case Studies

This report presents seven case studies of personas and stories that the Russian operation used. Each one reveals an aspect of the operation's tradecraft and targeting.

Fantasy Assassins describes the operation's most audacious fakes, attributed to British prime ministerial favorite Boris Johnson and U.S. Senator Marco Rubio.

Fanning Irish Flames describes how the operation forged communications from a British minister, a Northern Irish political leader, and an Islamic online forum, to spread divisive content in the United Kingdom and Ireland.

The Blue Man and the Mole analyzes the operation's Russian-language content through its oldest and most prolific persona, whose activity can be traced back to the Ukrainian crisis of 2014.

The Dark Lady Sings analyzes an online persona that the operation used repeatedly to post content on a range of issues of importance to Russia's foreign policy, including Ukraine and Venezuela.

Target Germany and Immigrants assesses one aspect of the operation's focus on Germany, analyzing its most successful fake, an attack on Muslim immigrants.

EU Elections analyzes the operation's apparent efforts to provide the European far right with political ammunition around the 2019 European Parliament elections.

Venom in Venezuela analyzes an attempt to accuse the United States of planning a chemical-weapons attack in Venezuela and how the operation planted the story in Spanish, English, and German.

Case Study 1: Fantasy Assassins

On a few occasions, the Russian operation posted stories that appeared designed to appeal directly to the West's most conspiracy-minded internet users. These stories were remarkable for their use of high-profile conservative figures —British prime ministerial candidate Boris Johnson and U.S. Senator Marco Rubio (R-FL)—to give the stories star quality.

The articles failed to catch on. Nonetheless, they constituted an attempt to seed false stories among a conservative and conspiracy-leaning demographic that has shown itself vulnerable to false stories in the past. As such, these examples deserve attention.

RU, as in "Rubio"

One outstanding fake story surfaced on August 1, 2018. It began with a post to online repository funnyjunk.com by an account that was created that day, posted one meme, and became inactive immediately.

The profile page of "ellisonredfall." Note the yellow box: "Date signed up: 8/01/2018. Last login: 8/01/2018." The page uses the American dating convention for August 1, 2018. (Source: funnyjunk.com/archive)

The meme showed an apparent tweet by Rubio, accusing the United Kingdom's intelligence-gathering agency, the Government Communications Headquarters (GCHQ), of planning to "use #DeepFakes to support Democrats" during the 2018 U.S. midterm elections. It coupled it with a popular meme from children's cartoon Spongebob Squarepants.

The meme.

(Source: funnyjunk.com/archive)

The DFRLab conducted a [timed](#) [search](#) of Rubio's Twitter account, and [of](#) [Google](#), from July 28, 2018, to August 2, 2018. No such tweet exists, although ironically, a separate [tweet](#) on July 30 referenced the danger of deep fakes, especially from Russia. There is also no record of the alleged tweet in the Politwoops archive of [tweets deleted by Rubio](#). It is likely that the Russian operation photoshopped the tweet to make it suit the chosen narrative, and drive a wedge between U.S. conservatives and the United Kingdom.

On August 2, 2018, a Facebook account that has been confirmed as being part of the Russian operation amplified the Funnyjunk meme, posting it to three separate groups.


Pushing the story: the operation's Facebook shares. (Source: Facebook)

The story picked up more speed on August 3, with the simultaneous posting of an English-language article to the websites [homment.com](#) (Berlin), [indybay.org](#) (San Francisco), [cssforum.com.pk](#) (Pakistan), and [ozpolitic.com](#) (Australia).

The brief article included an image of the "tweet," and expanded on Rubio's alleged claim, arguing the British government would "have to find a much more convincing explanation of their actions" than a simple denial. It was written in flawed, non-native English, characteristic of this operation:

> U.S. Senator Marco Rubio (R-FL) in his Twitter accused British secret services of intention to use deep fakes to throw mud at Republicans during the 2018 midterm elections to the U.S. Congress due to take place in early November…

A reverse image search of the "screenshotted" tweet revealed that it appeared in articles in French, German, and Spanish on multiple forums simultaneously. The items in French and Spanish, and some of the German versions, were direct translations of the English article.
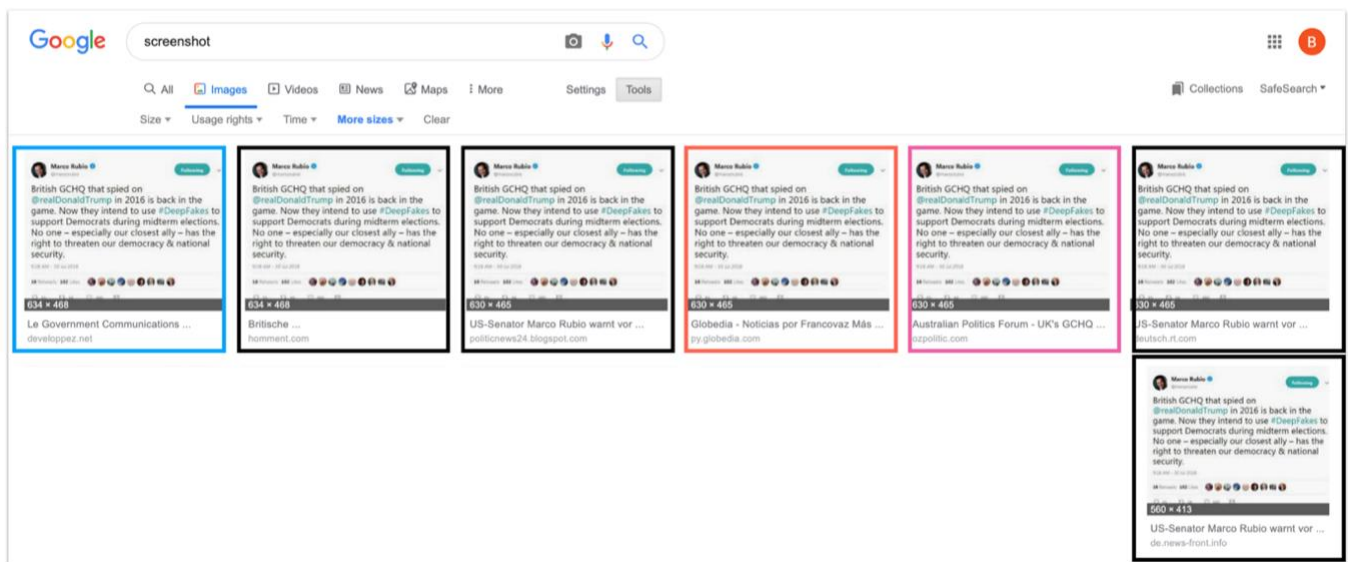
Screenshot of the reverse image search, showing the alleged Rubio tweet in the colored boxes. Light blue indicates French forums, black indicates German, orange indicates Spanish, and pink indicates English. The row of tweets at bottom left are unrelated, and the result of Google's search algorithm. (Source: Google)

In each case, where author data were available, the articles were posted by accounts that were created the same day, published one article, and never returned to the site. The forums included homment.com, nexusboard.de, reddit, rankia.com and globedia.com, all of which the Russian operation used repeatedly. All these indicate that this story was part of the broader operation.

The profile pages for two of the accounts that published translations of the Rubio story, "karineroquier" (left) and "danielbaa" (right). The red box on the "karineroquier" profile reads, "Date joined: 14/08/2018/ Last activity: 14/08/2018, 11h18." The upper red box on the "danielbaa" profile reads, "Contributions written: 1." The lower left red box reads, "Registered on: 15.08.2018. Last online: 15.08.2018. Last activity: 15.08.2018." The right-hand red

box gives the headline, "British GCHQ wants to help the Democrats in the midterm elections." (Source: developpez.net/archive, left; nexusboard.de/archive, right)

Most remarkably, three weeks after the fake appeared online, the German-language service of Kremlin broadcaster *RT* ran a separate article on it, alleging that Rubio had "warned of British interference in the midterm elections."

The *RT* article wrote that it was "astounding" that Rubio had accused GCHQ of "doing what Moscow and others are accused of." As proof of its claim, *RT* included the same screenshot but added that "Rubio may have been warned by Republican HQ to take the accusation back and not trigger a new diplomatic row between London and Washington, because the tweet of July 30 is no longer active."

RT's injection gave the story a little more traction and was picked up by a number of small German-language aggregators. Overall, however, the Rubio claim performed poorly. The posts gained few reactions and were not picked up by other media.

On June 19, 2019, as a result of the DFRLab's research, Rubio tweeted that "the image [of a tweet] is a fake," and called the operation a "Putin disinformation campaign." In response, RT appended an editor's note to its German article, saying that "In a tweet of June 19, 2019, Senator Rubio disputes that he created the above tweet." No further correction had been posted by the time this article was published.

Kill… Boris?

The Russian operation's most remarkable claim was that "radical opponents of Brexit" were planning to assassinate Boris Johnson, and that the Spanish intelligence services had exposed the plot.

The story started on August 8, 2018, while the Rubio narrative was still ongoing. It began with a post on a Spanish-language Facebook account run by the operation.
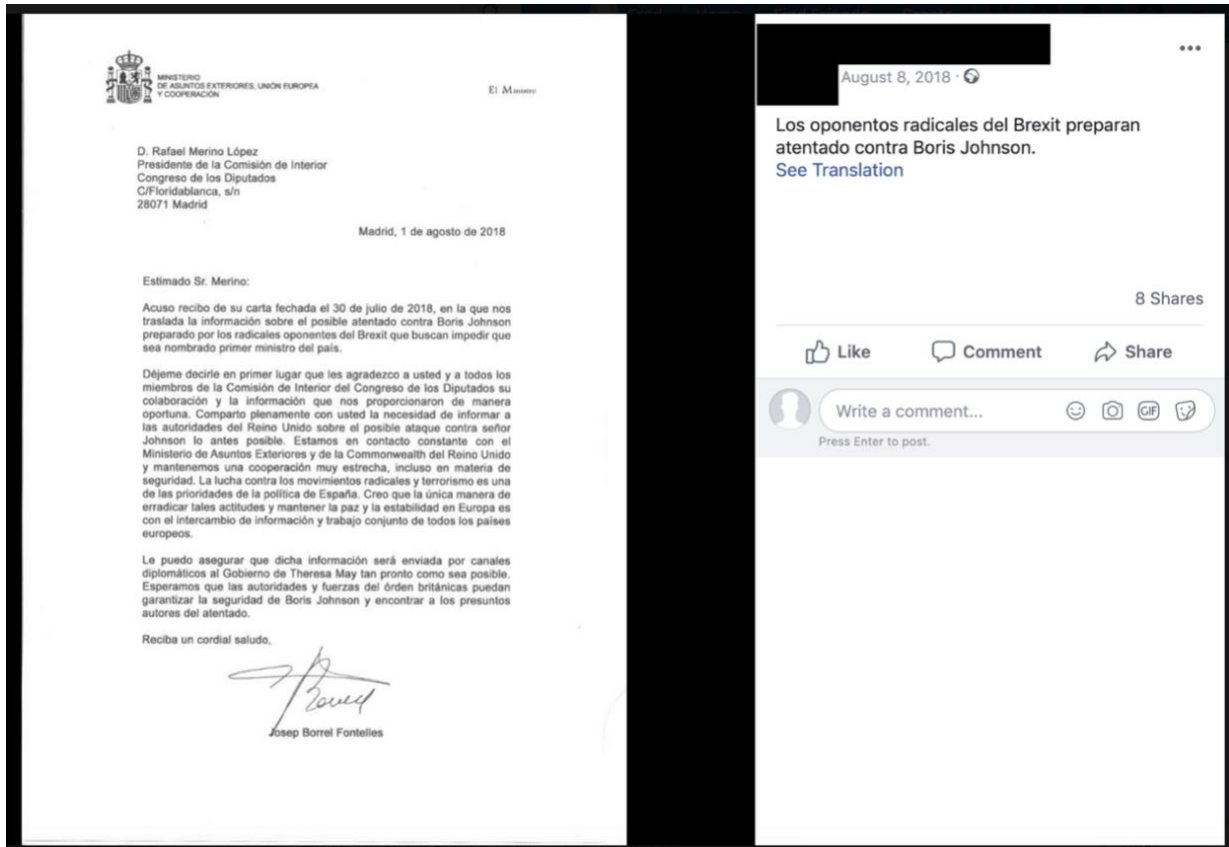
The Facebook post. The comment on the right reads, "Radical Brexit opponents are preparing an assassination attempt on Boris Johnson." (Source: Facebook)

The post shared a letter addressed to conservative politician Rafael Merino López, president of the Spanish parliament's Interior Committee at the time. The signature block attributed the letter to one "Josep Borrel Fontenelles," and was sent under the letterhead of the Spanish Foreign Minister. This is the first indicator that it was a forgery, because the current Spanish Foreign Minister's actual surname is "Borrell," not "Borrel."

The letter claimed that Merino had informed Borrell of a "possible attack on Boris Johnson by radical Brexit opponents who want to stop him being nominated prime minister" two days earlier, and that Borrell would alert the British authorities.

The letter was a fantastical forgery. Setting aside the fact that it was posted by a fake account and failed to spell the minister's name, the content was wholly implausible. To say that Spanish intelligence had better sources inside the "Remain" camp than the British did is self-evidently absurd and rendered more unrealistic by the claim that the Spanish had no ability to tell their own foreign ministry or Britain's counter-intelligence directly about it.

Typical of this operation, a Spanish-language article based on the forged letter was quick to follow. On August 9, a newly created user account shared it to six different subreddits; the same day, newly created user accounts shared it to Spanish-language forums globedia.com, burbuja.info, and articulo.org. None gained traction.

The next phase came on August 13, when an English-language translation of the Spanish article appeared on Medium. It was posted by an account called "Matt Porter"

that only published this one article. It appeared to have been written by a fluent, but non-native, speaker:

> "Recently, several key players in the government resigned in token of May's policy rejection."

> "If now people who are still unsatisfied with the results of the referendum of 2016 have a hope for a soft break with the EU or even the complete cancellation of Brexit, there's no chance of any give-ups or compromises with Johnson as the PM."

The same day, an account called "pormatt" posted the English-language article to forums including cssforum.com.pk, homment.com, talk-uk.com, talk247.net, debatepolitics.com, and defendingthetruth.com. Yet again, those sites that provided user information showed that the accounts were created that day, posted the one article, and never returned.

The ephemeral lives of "pormatt" on three of the internet forums where it posted the Johnson claim. In each case, note the creation date and the date of last activity: August 13, 2018. (Source: cssforum.com.pk/archive, top left; defendingthetruth.com/archive, bottom left; debatepolitics.com/archive, right)

Two days after the "pormatt" accounts burned and died, a separate user account, "Illinoiss," posted a meme based on the "Matt Porter" article to funnyjunk.com. The meme provided a link to a site called able2know.org, but the link was broken by June 2019. Yet again, the user account was created that day, posted one item, and then abandoned.

Queue: Long Trending

Adjust content blocking

Matt Porter @pormatt
a minute ago

Spain's Intel: Remainers Plan to Assassinate Boris Johnson

https://able2know.org/topic/472546-1

next

👍 ›
👎 ›
random
Favorite
Comment

∧   💬 Comment   ↻ Repost   ❝❝ Quote
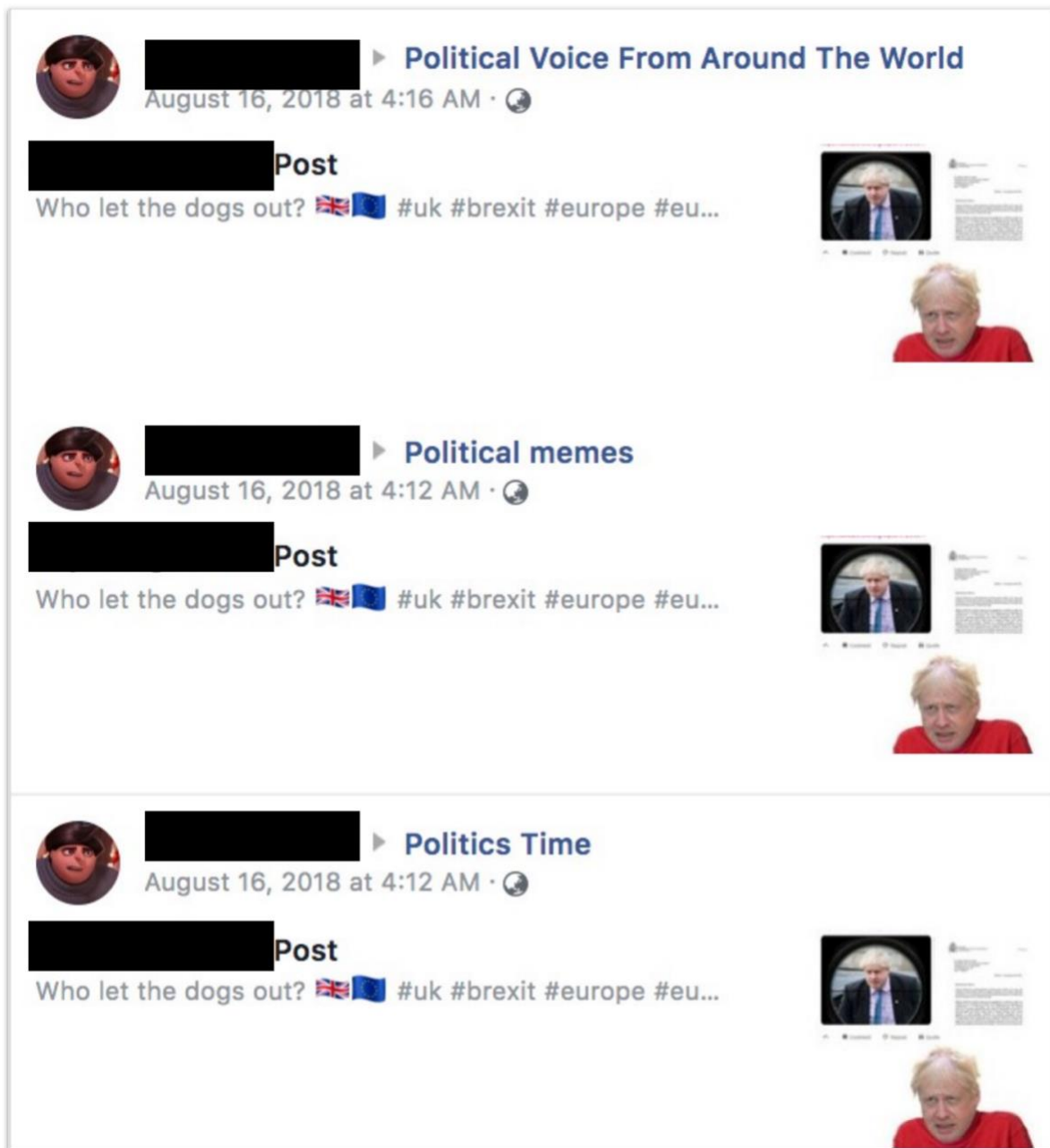
guess I'll die

↓

View Votes

✕   Top   Next   Comment   👎 › 👍 ›   Favorited: 0
Submitted: 08/15/2018

The meme by "Illinoiss." (Source: funnyjunk.com/archive)

As with the Rubio "tweet," the Russian operation's pseudo-Irish Facebook account then amplified the Johnson meme by sharing it to a number of meme and politics groups.

Shares of the funnyjunk.com meme by the Facebook account run by the Russian operation. (Source: Facebook)

This behavior was entirely typical of the Russian operation. Equally typical was the lack of impact for either story. Despite the operation's multilingual efforts and in part because of the operators' attempts to hide their tracks, neither story appears to have been picked up by any bona fide news outlet.

These stories stand out for the sheer audacity of their fakes and for the apparent desire to inflame American conspiracy-minded conservative communities against the United Kingdom and similar UK-based communities against the Remain camp.

Case Study 2: Fanning Irish Flames

The Russian operation consistently sought to fan divisions between, and within, Western countries. That was particularly apparent in its treatment of Ireland, especially Northern Ireland.

The operation used ostensibly Irish personas on Facebook to post divisive and inflammatory content. Between March 2018 and April 2019, the operation ran at least three false stories targeting Ireland and forged documents and social media posts to support its claims.

Real Minister, Fake Tweet

On March 22, 2018, an account that Facebook identified as belonging to the Russian operation posted a Medium article to at least 15 different news groups.
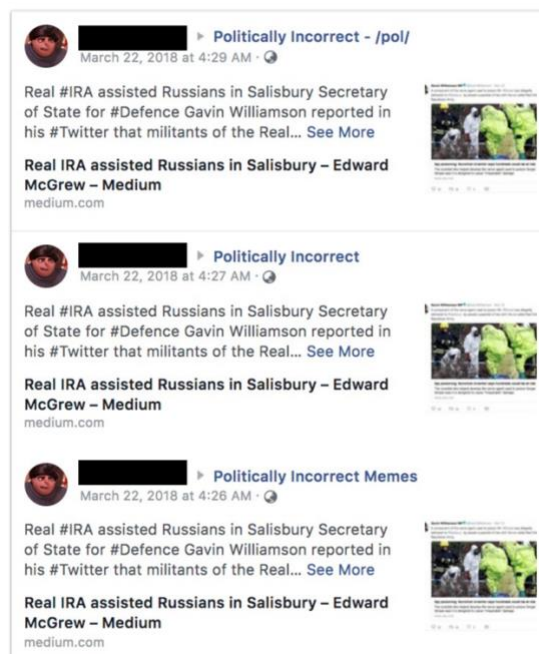
Some of the 15 times the ostensibly Irish account shared the same Medium article to Facebook groups. (Source: Facebook)

According to the article, then-British Defense Secretary Gavin Williamson tweeted that the Real Irish Republican Army (Real IRA) terrorist group had helped in the attempted assassination of former Russian spy Sergei Skripal in Salisbury, England, two weeks earlier. As "evidence," the article inserted a screenshot of the alleged tweet but claimed that it had been deleted within a few minutes, "which gives reason to believe that the information is sensitive and classified and thus must not be disclosed to the public until Scotland Yard completes its investigation."


Screenshot of the Medium article, including the alleged tweet. (Source: Medium/archive)

A number of factors expose the alleged "tweet" as a forgery. First, Williamson was one of the United Kingdom's top ministers at the time. He is followed on Twitter by high-profile journalists including Mark Urban (*BBC Newsnight*), Carole Cadwalladr (*The Guardian*), Stephen Castle (*New York Times*), Deborah Haynes (then of *The Times*), and Elizabeth Piper (*Reuters*). Yet not one mainstream outlet reported on the alleged tweet, and a Twitter search for "Gavin Williamson IRA" date-limited to March 2018 only showed four results, none relevant. Nor can it be found in the Politwoops archive of tweets deleted by Williamson over the years.

It is only necessary to look at the online firestorm provoked by U.S. President Donald Trump's recent tweet on the "Prince of Whales"—deleted and corrected after just 24 minutes—to appreciate that such an explosive tweet by Williamson, if real, would have

provoked at least some online attention. The lack of any mentions confirms that the alleged tweet never happened.

The second factor is the source account on Medium. Named "Edward McGrew," it only ever posted the one article. It used an image of British actor and comedian Hugh Laurie, in his role as TV medic "Dr. House," as its profile picture. This use of a single-shot account on Medium, with a stolen profile picture, was the standard operating practice for this Russian operation.
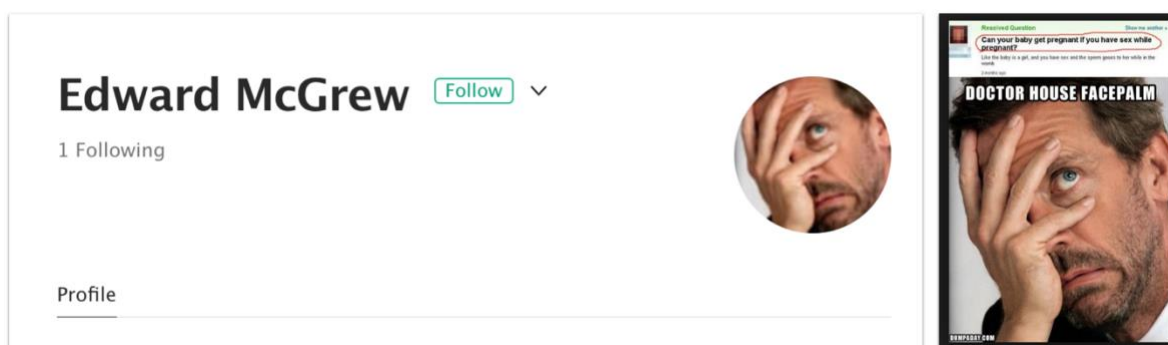

There's a secondary Infektion in the House... Left, "Edward McGrew" on Medium. Right, Hugh Laurie as Dr House, preserved on Pinterest. (Source: Medium/archive, left; Pinterest/archive, right)

Third, the article's use of English was fluent but not native. It struggled with the grammatical articles "a" and "the" and the possessive genitive case, as these lines demonstrate:

> In case the information about the Real IRA militants' involvement in Skripal's poisoning proves true, the law enforcement have to be prepared for the worst-case scenario as terrorists may have a complete set of chemical agents necessary for creating the chemical weapon. Are the Northern Ireland's police units prepared to provide security for the citizens in such conditions?

The Russian operation often posted its stories to several forums simultaneously, and this was no exception: accounts called "Edward McGrew" posted it to playbuzz.com and politicsforum.co.uk. On playbuzz.com, the author account was created that day, published the one post, and never posted anything else.

Reverse searching the supposed tweet revealed further versions of the story in Ukrainian, French (two locations, one deleted), and German (two locations, both deleted). One of the German locations was mein-suedhessen.de, a site the operation used several times. The article was deleted by June 14, but the associated author profile was still visible. Like the Ukrainian and French authors, the German author only posted this one article.
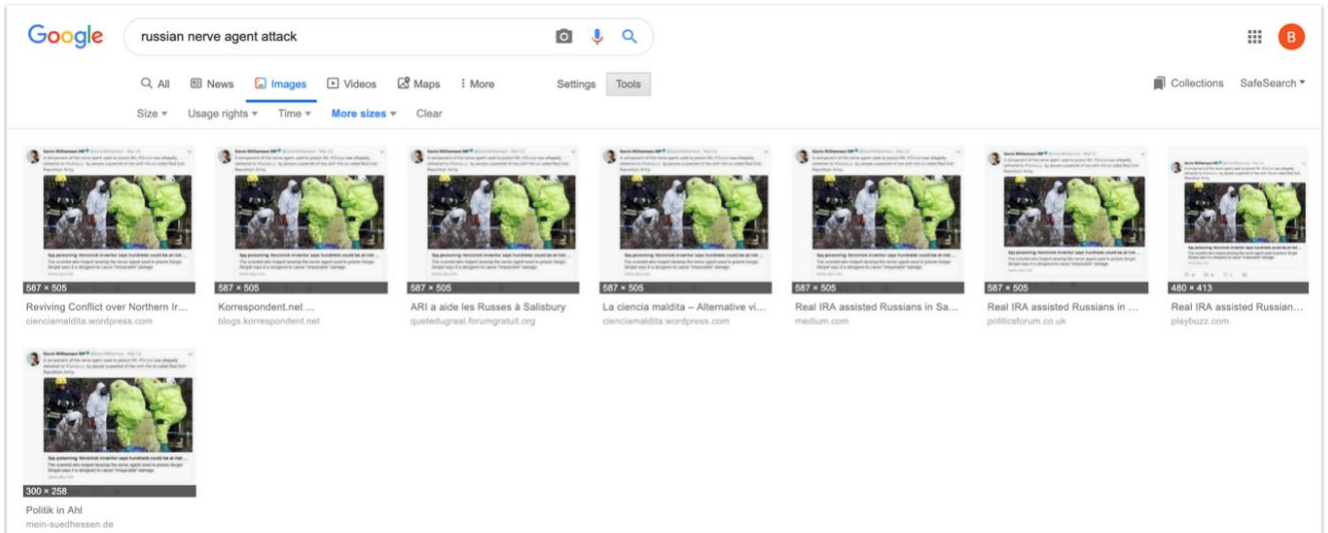
Results of a reverse image search of the alleged tweet. Note the forums in Ukrainian (top row, second from left), French (top row, third from left), and German (bottom row). (Source: Google/archive)

An Email That Never Was

The second attempt came five months later in August 2018. This time, it started on Facebook, when an ostensibly Irish account posted an allegedly leaked email on the Brexit negotiations.
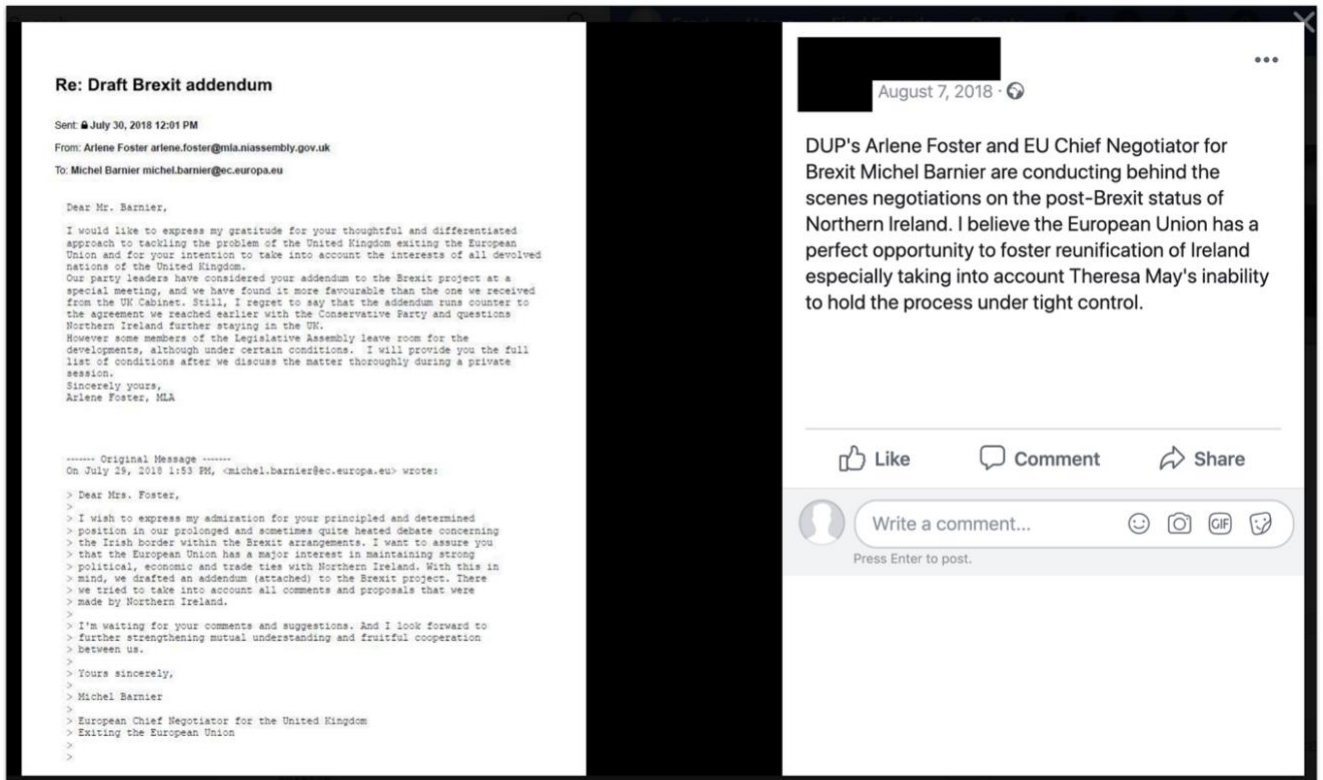
The "email" shared by the pseudo-Irish Facebook account. (Source: Facebook)

The post claimed that it was sharing an email from Arlene Foster, leader of the Democratic Unionist Party (DUP, the minority party supporting the United Kingdom's Conservative government) to Michel Barnier, chief Brexit negotiator from the

European Union (EU). The alleged email—presented as a screenshot —claimed that DUP members had found the EU's stance on Brexit "more favourable than the one we received from the UK Cabinet."

This would have been a political bombshell, as the DUP has consistently opposed any EU-UK deal that would leave Northern Ireland less closely associated with the rest of the United Kingdom.

But again, a Google search for the terms "Arlene Foster Michel Barnier email" between August 1 and August 14, 2018, returned no relevant results. Two months later, by contrast, many British media reported a genuine set of leaks (from British government sources) that claimed that Foster had called Barnier "hostile and difficult" and that she was preparing for a no-deal Brexit. The alleged email from Foster to Barnier appears to have been, again, a fake.

Two days after the Facebook post, a single-use account on Medium called "Will Dobson" posted a longer article headlined, "After Brexit, Northern Ireland may obtain a special status in the EU." Based on the forged "leak," it claimed that the DUP was "ready to sacrifice its arrangement with the [Conservatives] and even leave the United Kingdom 'under certain conditions'" and warned of "bloody confrontation" in Ireland as a result.

This article was written in largely fluent English but still contained a few apparently non-native sentences, such as:

> "Prime-minister's rigidity can not only spoil stable relations with Ireland, it can also accentuate the growing separatist sentiment inside the country."

> "Requesting the restoration borders between Ulster and the Republic of Ireland is, by far, quite shortsighted for May."

Characteristically of the Russian operation, the identical article, under the same byline, was posted the same day to indybay.org, beforeitsnews.com, and, bizarrely, cssforum.com.pk, a forum for the Civil Service of Pakistan. It was also posted as a meme to Imgur. On each platform, this was the author's only post.
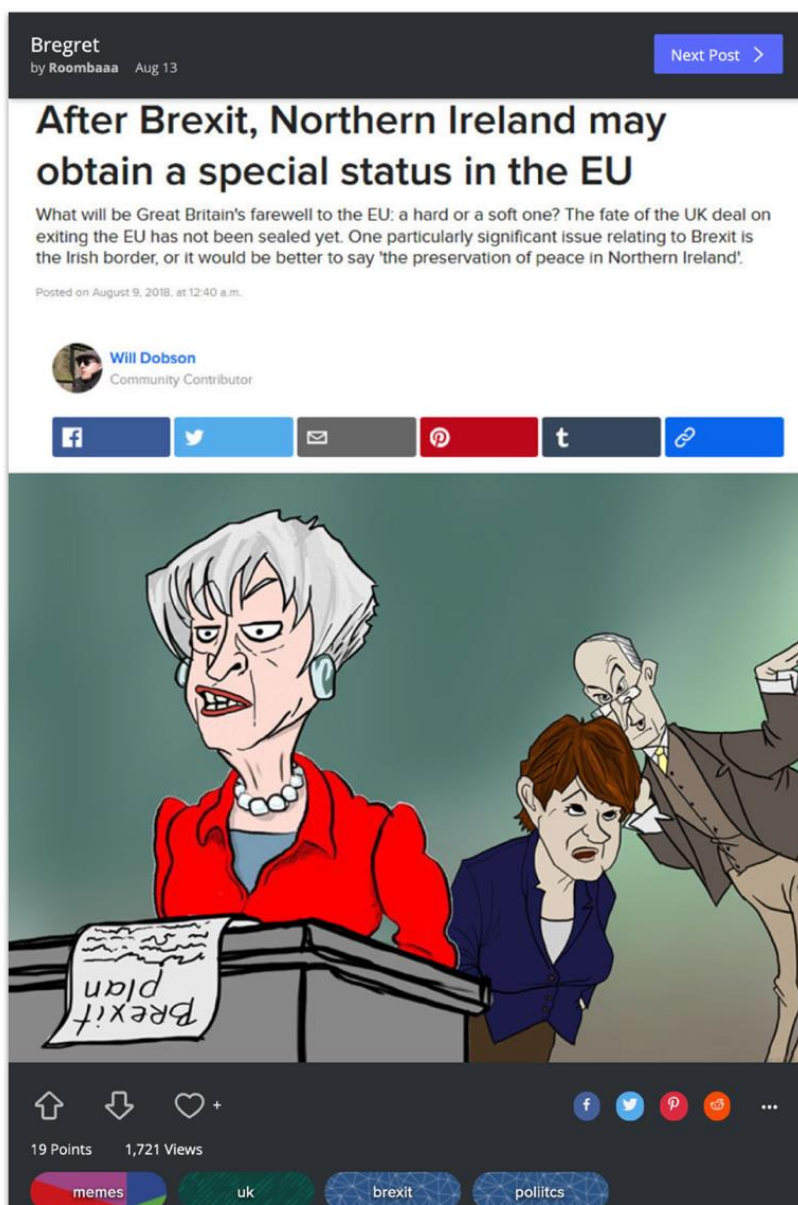
Shared on Imgur: the same false story, posted by another "Will Dobson" single-shot account. (Source: Imgur/archive)

Between August 8 and 10, versions appeared in German on homment.com, Reddit, and Indymedia.org (where the link is now broken), and in Spanish on rankia.com and four separate Reddit threads. All these accounts were created the same day they posted the article; two subreddits rejected the posts, for that reason.

Once more, the Russian operation's pseudo-Irish account gave the Imgur post a further push, sharing it to a number of political forums.

Shares of the article and Imgur cartoon, from one of the Russian operation's known accounts. (Source: Facebook)

The evidence therefore suggests that every stage of this story — an initial Facebook post channeled through Medium, Reddit, and all the other forums and languages, which are ultimately posted back to Facebook — was the work of the same operation.

Those Islamist Catholics

The third attempt came just over a year after the first. On April 22, 2019, an apparently Ireland-based user posted a sensational claim to the r/ireland subreddit. The post alleged that the Real IRA had posted an Arabic-language invitation to Islamist fighters to "join the RIRA and fight on the Irish soil." The article was posted by the account u/robeharty, created that same day; it was "his" only post.
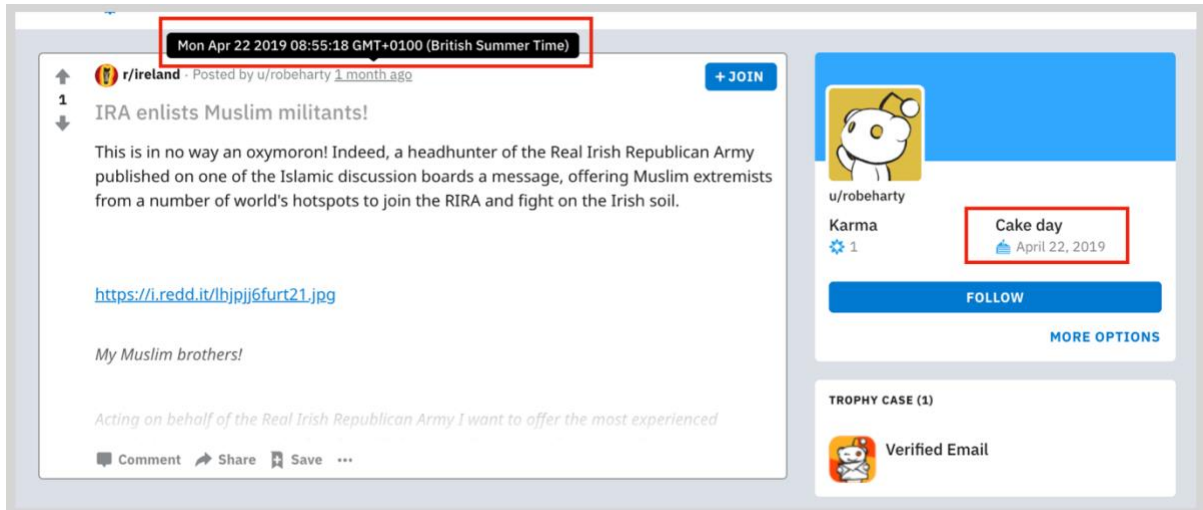
Screenshot of u/robeharty showing the date of its only post (upper red box) and the date the user account was created ("Cake day," right-hand red box). (Source: u/robeharty/archive)

The Reddit post claimed to have found the invitation on an Arabic discussion forum largely devoted to religious texts and Islamic scholarship. It said that the call was "published on one of the Islamic discussion boards" but did not provide a specific link, only a screenshot.
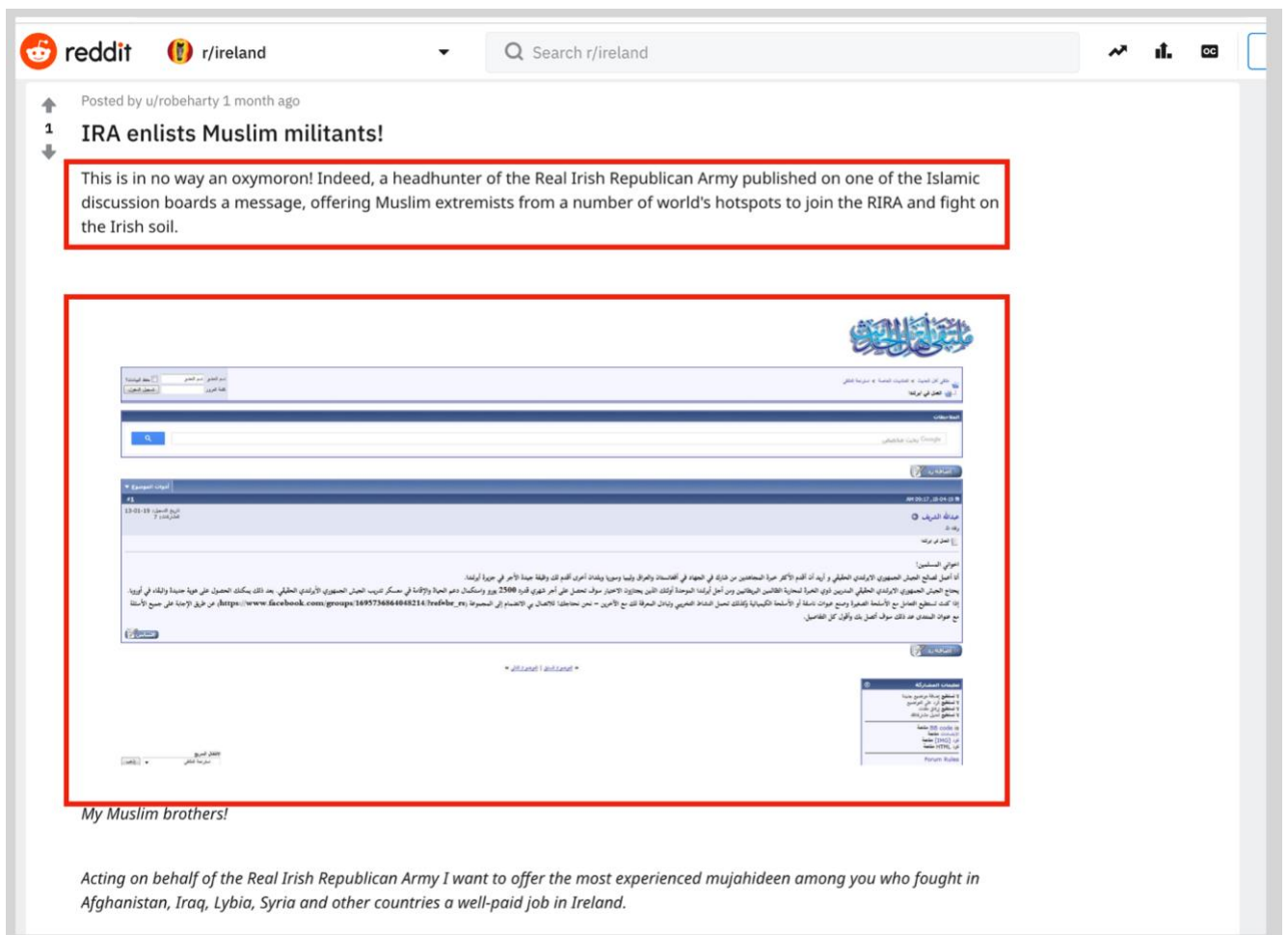
Screenshot of the Reddit post showing the text with the reference to "one of the Islamic discussion boards" (upper box) and the alleged screenshot (lower box). (Source: r/ireland/archive)

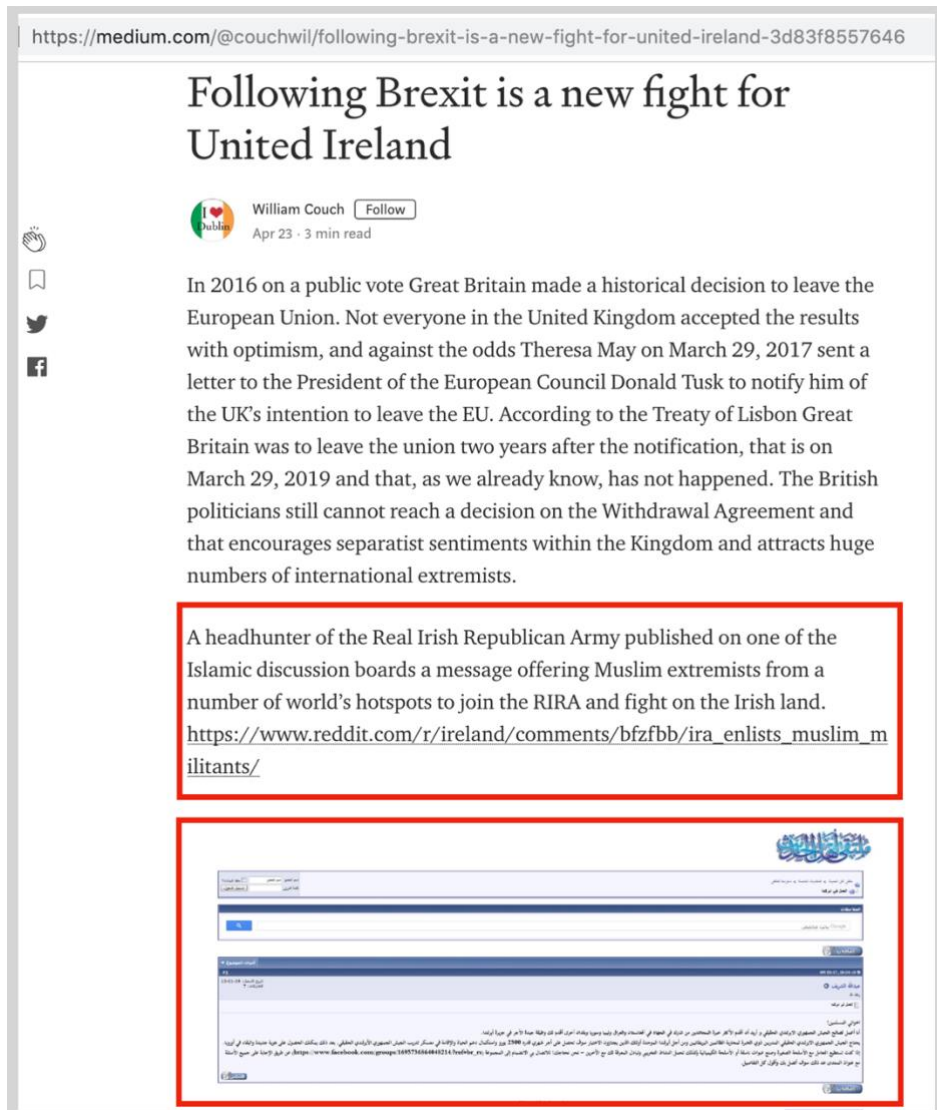The English syntax in the Reddit post was distinctly non-native:

> "To join the RIRA and fight on the Irish soil."

> "A headhunter of the Real Irish Republican Army published on one of the Islamic discussion boards a message."

> "Muslim extremists from a number of world's hotspots."

The DFRLab identified the discussion board from which the Arabic-language post was allegedly taken but found no trace of the alleged post. This suggests that it was either a planted post that was later deleted or a doctored screenshot.

The Reddit article only received one vote and no comments. The following day, however, a user account on Medium called "William Couch" posted a longer article headlined "Following Brexit is a new fight for United Ireland." This article pointed to the Reddit article as its source; like u/robeharty, "William Couch" only ever posted one article.

Also like the u/robeharty post, this post contained language errors:

"In 2016 *on* a public vote…"

"The RIRA never abandoned the idea of military struggle for freedom and independence of united Ireland."

"Could it really be true that RIRA agreed to make business with Islamic radicals?"

The same day, April 23, the Russian operation's main pseudo-Irish Facebook account shared a link to the Reddit article.

IRA enlists Muslim militants!

These are the achievements of David Cameron and Theresa May: a headhunter of the Real Irish Republican Army published on one of the Islamic discussion boards a message, offering Muslim extremists from a number of world's hotspots to join the RIRA and fight on the Irish soil.

REDDIT.COM

IRA enlists Muslim militants!

Posted in r/ireland by u/robeharty • 1 point and 0 comments

The share of the Reddit post by the Facebook account from Russia. (Source: Facebook)

A Google search for the Reddit link embedded in the Medium article revealed that the exact article was posted to two other forums on April 23: homment.com and beforeitsnews.com. Both were attributed to "willcouch;" in each case, this was the user's only post.

The search also returned a Spanish version of the article, posted to five separate forums on April 24: r/espanol, r/spain, foroexplayate.com, globedia.com, and mediavida.com. Each one was posted by a user account called "Antonio Diaz," created the same day, which used a picture of the back of Batman's head for "his" profile.
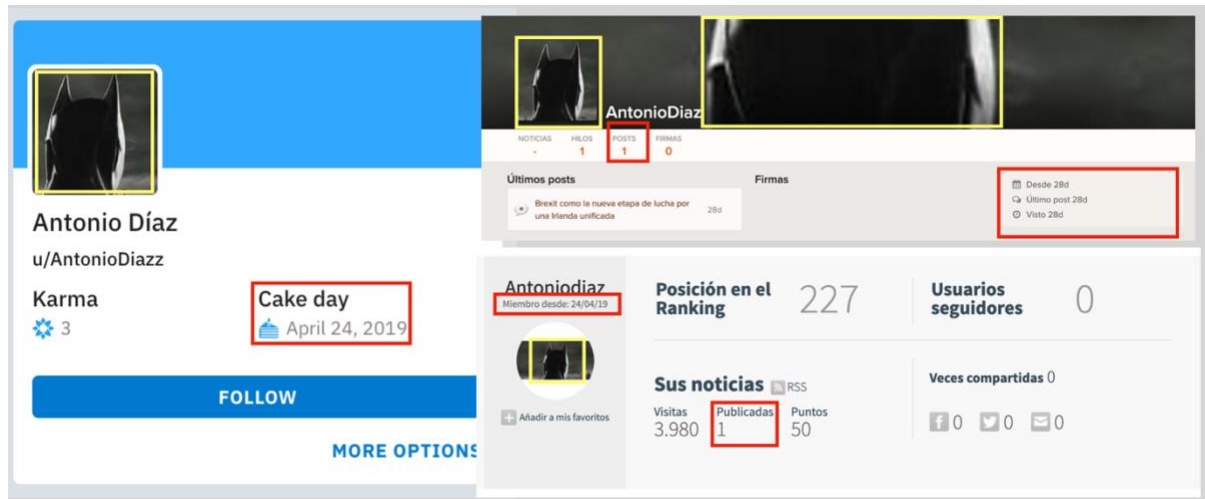
Profile pages for u/AntonioDiazz on Reddit, AntonioDiaz on mediavida.com, and Antoniodiaz on globedia.com. Note the identical profile images in the yellow boxes. Each account was created on April 24; the screenshots were taken on May 22. The globedia.com and mediavida.com accounts only posted once, while the Reddit account posted the same article to two subreddits. (Source: Reddit, left; mediavida.com, top right; globedia.com, bottom right)

A further version was posted in French on April 25.
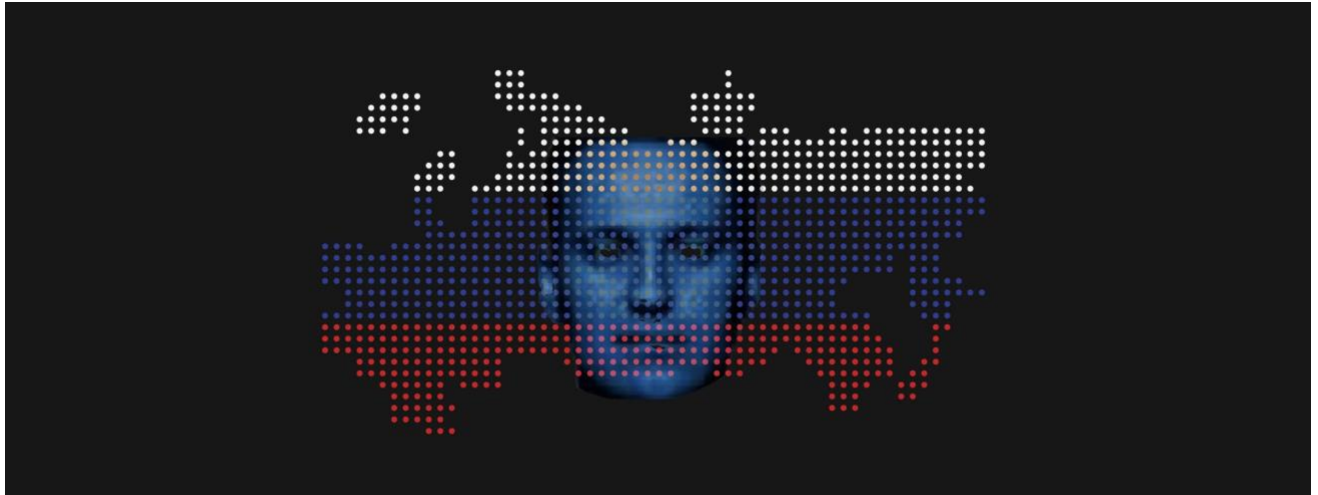
Case Study 3: The Blue Man and the Mole

The Russian operation's oldest and most prolific persona was a Russian-language account whose profile picture was a blue-shaded picture of Russian anti-corruption campaigner Alexei Navalny. Facebook identified the account on its platform as part of the operation and took it offline.

Unlike almost all of the operation's other assets, the "Blue Man" persona posted early and often. On Facebook, its profile picture and first posts were uploaded on March 10, 2015, indicating the likely creation date. A Livejournal account using the same name and profile picture began posting even earlier, in January 2014.

An analysis of this account shows how long the operation lasted, how consistently it amplified Russian geopolitical narratives, and how closely the operation's different language sections worked together, once they were launched. The Russian-language operation was not a separate effort: it led to all the rest.

Birth of an icon: screenshot of the day that the Blue Man Facebook account posted its profile picture, March 10, 2015. (Source: Facebook)

This persona worked across platforms. Accounts with the same name and profile picture posted bylines on a range of Russian-language blogs and forums, including cont.ws (55 articles since April 2015), politikus.ru (19 articles since February 2016), and especially Livejournal (200 entries since January 2014). The same articles appeared on multiple forums under the same byline.
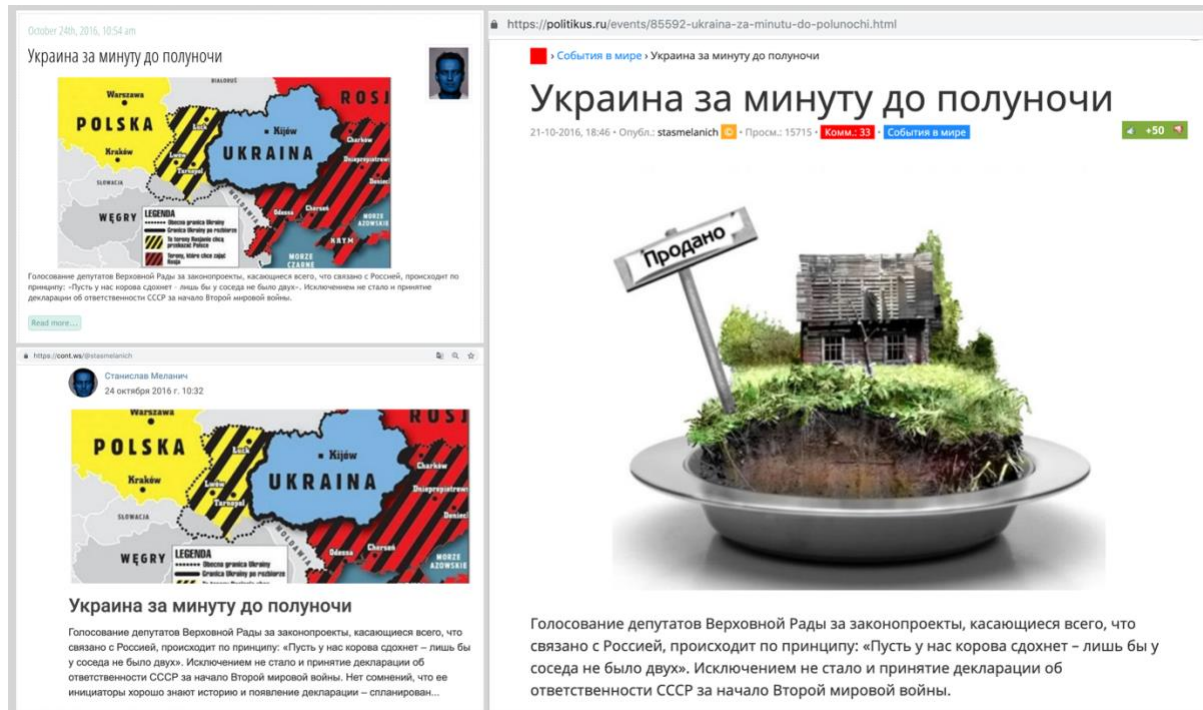

Translated from Russian: "Ukraine, a minute to midnight." Posts attributed to the Blue Man persona on Livejournal (top left), cont.ws (bottom left), and politikus.ru (right). Note the use of the same profile picture in the left-hand images. (Source: Livejournal/archive, top left; cont.ws/archive, bottom left; politikus.ru/archive, right)

The posts were routinely hostile to Ukraine's government and President Petro Poroshenko, as well as to the West in general and NATO in particular.

The Same Techniques, Repeated

Facebook attributed this account to the Russian operation. Other evidence supports that attribution. While the Blue Man persona was far more active and repetitive than other accounts in the network and began much earlier, it employed the same essential working methods.

For example, on September 29, 2016, the Facebook page shared an article from politikus.*ru* headlined (in Russian) "NATO: A tradition of bioterrorism from Vietnam to Ukraine." The article, archived here, was published on September 28, 2016. That same day, the Blue Man persona posted the identical article to Livejournal and another blog forum, actuallno.com.
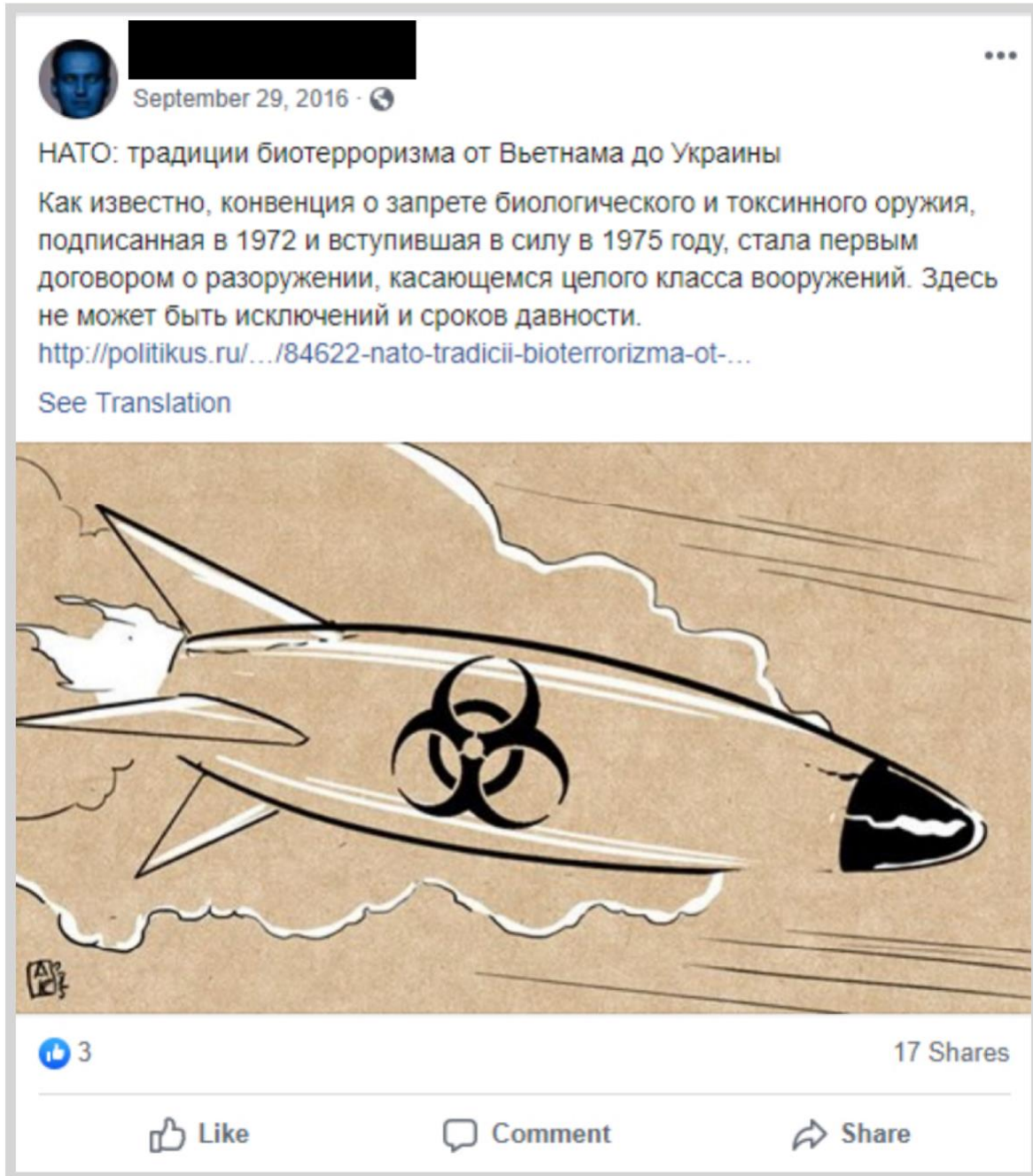
Facebook post by the "Blue Man" accusing NATO of "bioterrorism". (Source: Facebook)

The Russian-language articles claimed to be translations of an English-language source on a site called articlesreader.com. The English article, dated September 27, did not have a byline. Its use of English was distinctly non-native and contained grammatical errors characteristic of native Russian speakers, including confusion over the use of the grammatical articles "a" and "the" and over the word order in questions.

> "The ensuing events remind the thriller from the 90s."

> "By the way, whether Ukraine could be considered the Convention member, if it has left behind their communist past and Soviet obligations?"

> "It occurs that the USA puts in the crossfire its own NATO allies just for conducting its illegal research. (…) Everything is subjugated to interests of a militarized alliance working for benefits of a certain superpower."

The article opened with the words "As is known," an unlikely lede in English news writing, but one that is acceptable in Russian journalism in the form of "как известно," as in the below articles from state news wire *RIA Novosti*. Overall, the English version looked like a translation from Russian, not the other way around.

Как известно, правительство Петербурга в среду приняло решение о сохранении Исаакиевского собора в управлении Государственного музея-памятника "Исаакиевский собор".

С.-ПЕТЕРБУРГ, 2 сен — РИА Новости. Ежегодно на текущее содержание и реставрацию здания Исаакиевского собора музей тратит до 200

Как известно, прошлое в России делает непредсказуемым политика. Вот и нынешняя засуха с пожарами недолго прожила вне исторического контекста. Все последние несколько дней ностальгически настроенные к советской власти пользователи Интернета активно размещают в сети цитаты из советских газет, пожелтевшие фотографии и кадры парадной кинохроники.

Articles beginning with the phrase "как известно" from *RIA Novosti*. (Source: [Ria Novosti](#)/[archive](#), top; [Ria Novosti](#)/[archive](#), bottom)

While all of the Russian articles pointed to articlesreader.com as their source, the English variant appeared in one other location the same day: [Medium](#). The Medium post was attributed to an author called "[Dolan Moss](#)." As of May 31, 2019—almost three years after "he" published the article—this article remained the author's sole contribution, although a user of the same name posted the same article on [quora.com](#), also on September 27, 2016.

This was exactly the behavior of the Russian operation in other cases: create a fake persona with no biographical details, use it to post one article to multiple locations including Medium, and then build other articles in other languages, pointing back to it.

The Secret Diary of Anonymous "Mole"

Many of the articles attributed to the Blue Man persona concerned Ukraine, especially in 2014–2015, as the conflict in the Donbas region broke out and Russian regular army

forces [fought in Ukraine](). These articles were anti-Ukrainian in general and hostile to former Ukrainian President Petro Poroshenko in particular.
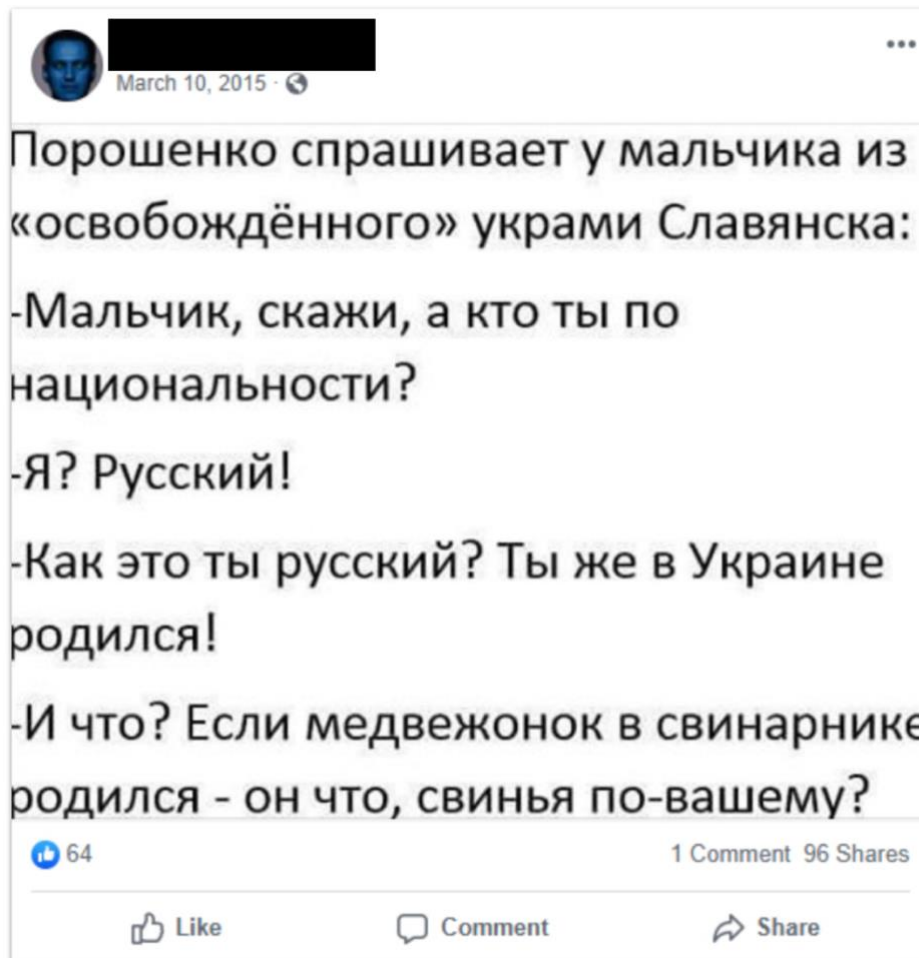
"Poroshenko asks a boy from Slavyansk, 'liberated' by the Ukros: 'Say, kid, what nationality are you?' 'Me? Russian!' 'What do you mean, Russian? You were born in Ukraine!' 'So what? If a bear cub was born in a pigsty, what do you think he is, a pig?' (Source: Facebook)

One of the more intriguing aspects of these anti-Ukrainian posts was their sourcing. A number of later articles and posts published by the Blue Man were based on a Telegram channel called "[Кріт СБУ]()" (translated from Ukranian, "SBU Mole," the SBU being the Ukrainian security services). This channel claimed to be a "serving colleague of the SBU," offering "insider stories, leaks, and analysis" to discredit the service and Ukraine's government.

For example, on April 5, 2019, the so-called Mole posted a photo of what it claimed were instructions to the SBU to use force against demonstrators in a bid to keep Poroshenko in power. The photo showed a sheaf of brightly colored printouts on a desk. Again, there was no way of verifying the photo. (Elsewhere, this operation used similar techniques to post forged documents, that it then used as the basis for false stories.)

On April 8, an article using the same image, attributed to the Mole, appeared on an unmoderated blog site called "Я корреспондент" (translated from Russian, "I am a correspondent"), [korrespondent.net](). It was bylined by a user called "[Forsa Leonid]()"

(ФОРСА ЛЕОНИД) whose profile picture showed an unidentifiable male. This was the user's only contribution.

The following day, a second Russian-language article on a blog forum called aftershock.news amplified the "leaks." It did not mention the Mole; instead, it attributed them to "Ukrainian social networks" and linked to the korrespondent.net post. Again, the "author" did not have an identifiable profile picture and this article was its only contribution. On April 10, the Blue Man Facebook account shared the aftershock.news version of the story.

Fake's progress: the transmission of the apparent "internal documents" from the Mole, via two faceless accounts with no posting history and no subsequent posts, to the Blue Man Facebook account. (Source: Кріт СБУ/archive, top left; korrespondent.net/archive, second from left; aftershock.news/archive, second from right; Facebook, bottom right)

The Blue Man persona was part of the Russian operation, as Facebook found. What remains unclear is whether the "Mole" account was part of it as well. The "Mole" account served as a source for "leaks" that may have been forgeries and, thus, enabled some of the operation's articles; whether it was part of the same operation or a separate endeavor, however, requires further research.

Case Study 4: The Dark Lady Sings

Most of the non-Russian-language accounts involved in the Russian information operation were burner accounts created to post a single article and then abandoned. A few, however, were used repeatedly, especially when they posted about Russia's foreign policy interests.

One of the most significant was the persona variously called "Dama Mroczna" (Polish for "the Dark Lady" or "the Gloomy Lady") and "Anna Mroczna." This account is of particular interest because its activity shows that the operation has been ongoing for a number of years, with a focus on advancing Russia's geopolitical interests.

In the first indication that this persona was part of the operation, a Facebook page that claimed to be Irish—now identified as a Russian asset—shared a Medium article one of the Mroczna personas claiming that the United States had staged Armenia's 2018 political revolution.

Sharing the Dark Lady: the post from Medium, on the account of a known Russian operation asset on Facebook.
(Source: Facebook)

Of course, the fact that a known Russian operation shared an article need not mean that the operation created the article. Other indicators suggest that it did, however. First, the Dama Mroczna account made this sole post on Medium on April 30, 2018, and then abandoned the platform, exactly as the Russian operation did.

Second, the same day, a user account called "Anna Mroczna" posted an identical article to conspiracy forum beforeitsnews.com, a site that the Russian operation used repeatedly. The account used the same profile picture as "Dama Mroczna."


Profile pictures for "Dama Mroczna" (top) and "Anna Mroczna" (bottom). (Source: Medium/archive, top; beforeitsnews.com/archive, bottom)

Unlike the Medium variant, "Anna Mroczna" posted nine times on beforeitsnews.com. Its most recent post, dated to March 1, 2019, was a share of the Russian operation's claim that the United States was planning a false-flag chemical attack in Venezuela. This provides another indication that the Dark Lady was part of the operation.

Triggering Trump

An earlier article, posted on June 21, 2018, alleged that controversial Ukrainian doxxing site Myrotvorets (literal translation: "Peacemaker") had blacklisted U.S. President Donald Trump for his stance on Crimea. The only piece of evidence provided was a screenshot attributed to a Google translation of the Myrotvorets site, with the comment, "At the time of this article's publication all records with Donald Trump were deleted from the 'Peacemaker' website, however a screenshot is still available."
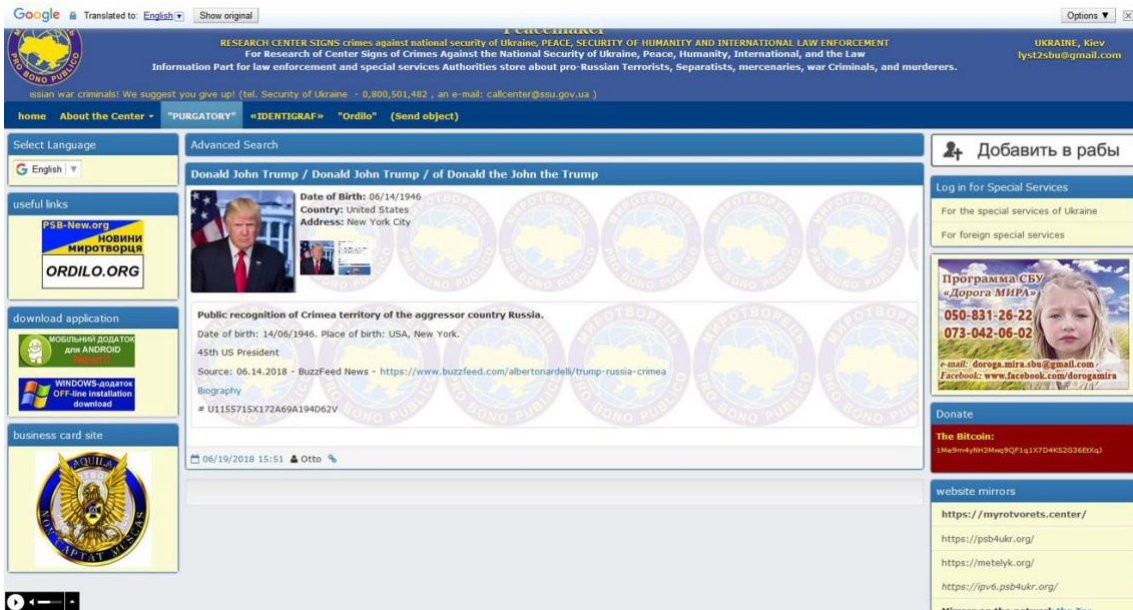
The page attributed to Myrotvorets. (Source: beforeitsnews.com/archive)

The image closely matched the layout of the genuine Myrotvorets page. Language clues are less relevant here, as the post was allegedly machine translated, leaving little internal data to confirm whether the screenshot was genuine.

External clues, however, indicate that this was a forgery. First, Google searches for the phrases "Ukraine puts Donald Trump on blacklist" and "Peacemaker puts Donald Trump on blacklist" only returned one relevant hit, discussed below. It would be implausible to suggest that genuine outlets would have ignored such a shocking story if it was authentic, given the reputations of Myrotvorets and of Trump himself.

Second, the one relevant hit was an article posted on Medium on June 20 with the exact same headline as the "Anna Mroczna" piece, and the exact same text. Rather than "Dama Mroczna," though, it was attributed to "Mike Davidson," an account that only posted the one article and whose profile picture was a reversed shot of American artist Michael Bond.
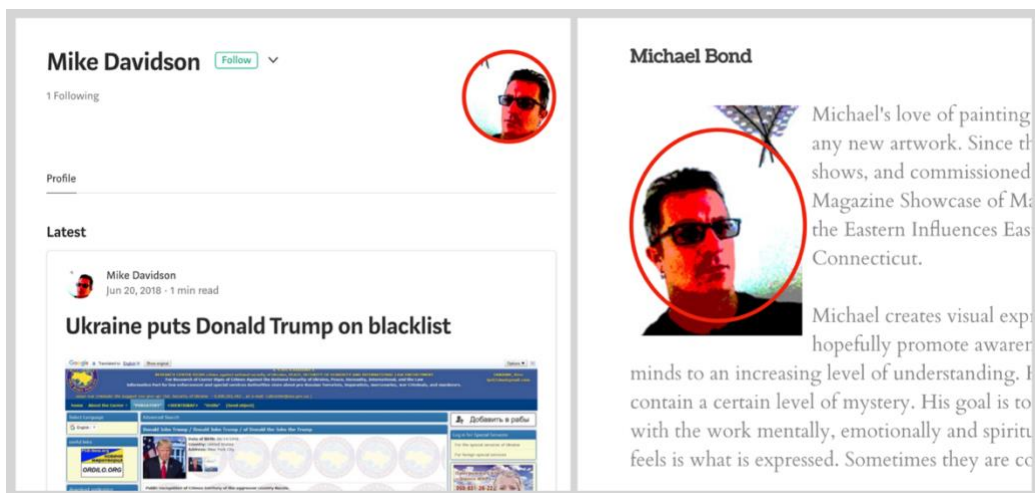
Left, profile page for "Mike Davidson," showing its one post, the Ukraine story. Right, Michael Bond's page on globalartleague.com. (Source: Medium/archive, left; globalartleague.com/archive, right)

Although it did not show up in the Google search, the English article appeared in one other location: the forum homment.com, where it was attributed to "MiDavid." An ostensibly Irish account that Facebook identified as "emanating from Russia" also shared the article.
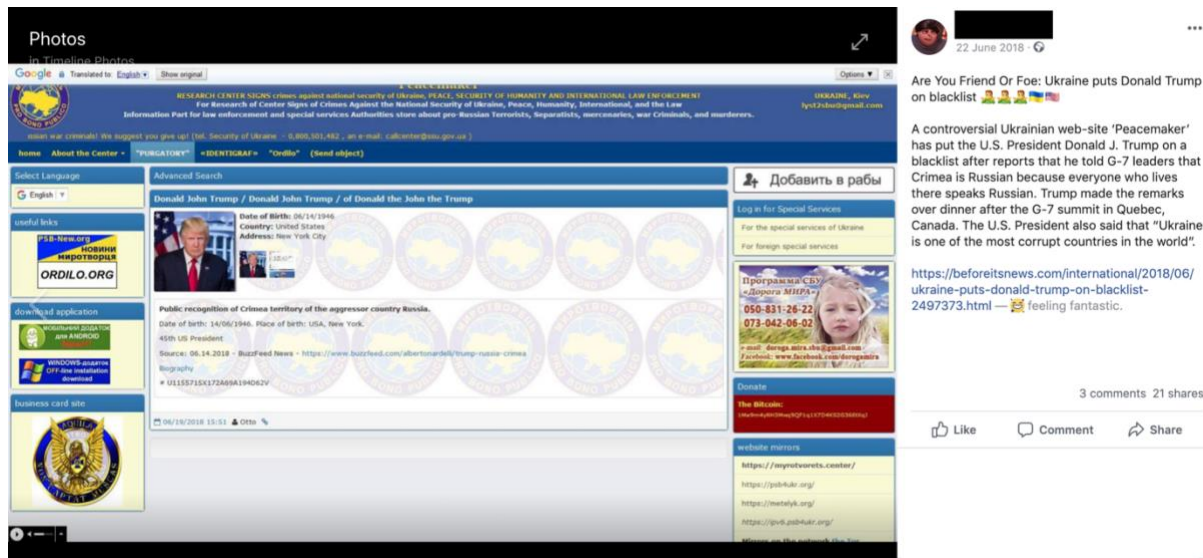
The share of the article by another takedown account. (Source: Facebook)

Finally, a Spanish translation of the article surfaced on June 21 on at least three different forums: globedia.com, taringa.net, and entornointeligente.com. A Facebook account that the platform later took down as part of this operation then shared the Spanish-language version of the article.

The DFRLab repeatedly observed this operation's use of Medium, homment.com, and beforeitsnews.com to amplify false stories. The amplification by an English-language account known to be part of the operation reinforces the attribution. The simultaneous posting in Spanish, as well as the amplification by yet another operation account, confirms it.

This appears to have been an attempt—albeit an unsuccessful one, as most of this operation's attempts were—to spread a story discrediting Ukraine and raising the tensions between Kyiv and the White House.

Buzzing Buzzfeed

Two other articles posted by "Anna Mroczna" deserve attention. Both were dated to late 2017, showing that this operation was of some duration. The longer of the two articles, posted on December 26, 2017, dealt with the relationship between the United States and Ukraine in wholly negative terms.

It began with a reference to Ukraine's 2013-2014 Maidan Revolution: "So-called Ukrainian 'maidans' have bored the world community to death." It continued with a lengthy conspiracy about a turf war between the U.S. Federal Bureau of Investigation and the Central Intelligence Agency in Ukraine:

> "A never-ending internal fighting in the American national security environment has become the talk of the town being eventually accreted with new dirty wash."

Most of the amplification of this article was typical of this network, using single-use accounts to post it on different platforms. The English-language article popped up the same day on three other forums: Medium, justplainpolitics.com, and homment.com. The first two attributed it to a user called "Mark Kravets," while homment.com simply attributed it to "homment." The account on justplainpolitics.com was created the same day, and did not return to the site after it made its one post. Three weeks later, on January 15, 2018, a user called "Sergei Zelenetskiy" posted the Russian translation of the article, sourced to the Medium post, on a number of forums, including aftershock.news and kont.ws.

Most strikingly, however, the Dark Lady's original article gave a hyperlink to its source: a post on Buzzfeed attributed to one "Mark Kravets."
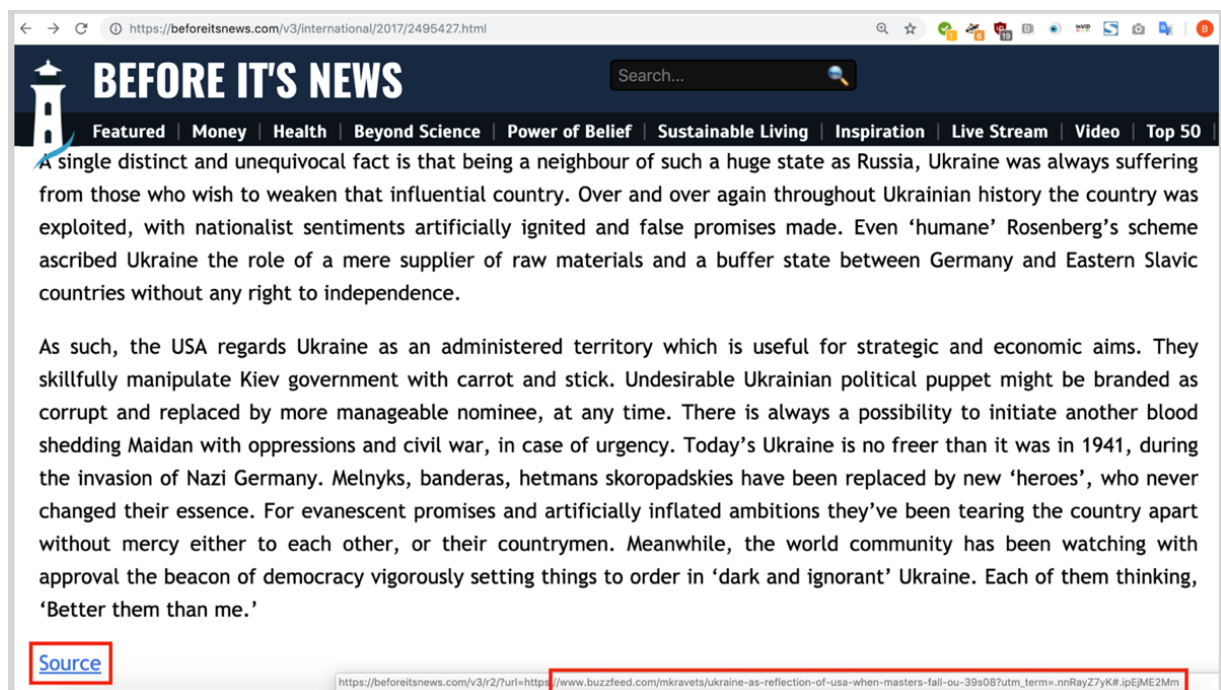
Screenshot of the footer of the Dark Lady's post on beforeitsnews.com, showing the source hyperlink, leading to www.buzzfeed.com/mkravets. (Source: beforeitsnews.com/archive)

The Buzzfeed link was broken, and it remains unclear whether the post ever actually made it onto the site, which allows its users to publish their own stories, or whether the Russian operation created a false URL to make it look as if it had. If the operation did manage to post its content under the Buzzfeed domain for any length of time, it would mark one of its greatest observed successes to date.

Killing Kim

The Dark Lady's most outlandish article was also its earliest, posted on November 20, 2017. Headlined "Attempted Assassination of Kim Jong-un scenery" - was the last word meant to be "scenario?" - it pointed users to an article on homment.com with the teaser comment, "This article looks like conspiracy, but I thought it might be true."

The homment.com story was posted on November 10, 2017, and did not name an author. Yet again, its language and syntax featured errors characteristic of native Russian speakers. The DFRLab included multiple quotes here out of sheer fascination with the errors littering the language of a self-proclaimed American journalist.

> "As the saying runs, there is a shard of truth in every joke."

> "After mentioning the North Korean dictator, one 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'…"

> "I did not dare to ask more for fear to be taken for a spy. The same matter stopped me from addressing the US Command. It is one thing to give coverage to everyday life in training military units. But it is totally different to query about the future combat operation. I was lucky enough to meet too boastful military man (which is common among the far eastern people) and to hear more than I should to."

As well as homment.com, the story turned up on two other sites on November 10, 2017. One was Medium, which the operation used with especial frequency. The username there was "MilitaryObserver"; this was its only post.
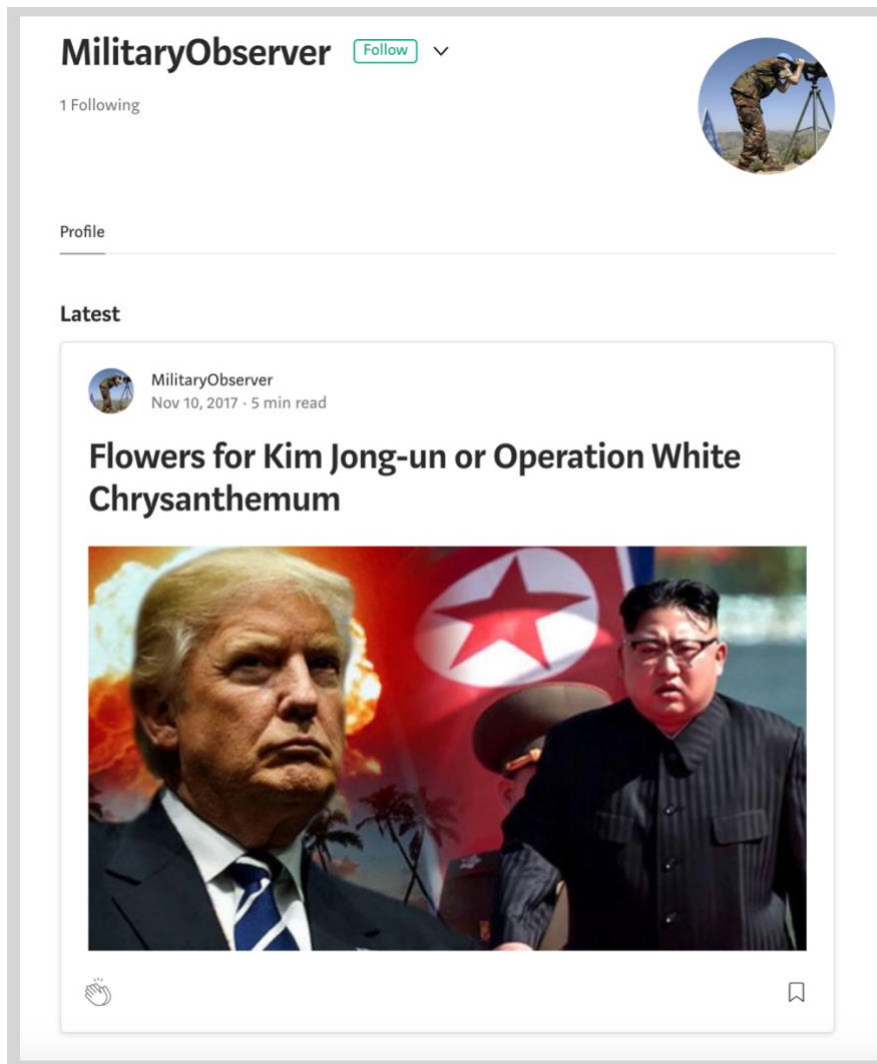
The profile page for "military observer" on Medium, showing its only post. (Source: [Medium](#)/[archive](#))

The other site was Reddit. The user had the same name as on Medium—"Military Observer"—and only posted this one article to two subreddits, [r/news](#) (where it simply posted the Medium link) and [r/korea](#) (the full article).

In the following days, the article appeared in French and Ukrainian translations. The [French version](#) was posted to a video-games forum, jeuxvideo.com, by an account called "[riu128](#)," that only posted this one piece. The Ukrainian version surfaced on blog site [politiko.ua](#), again posted by a single-use account.

A French user posted the only reaction to the article, replying, "That was riu128, live from South Korea for Google Translate." The Korean conspiracy piece is noteworthy as an early attempt to spread a fake through multiple language environments using burner accounts, not because it was a success.
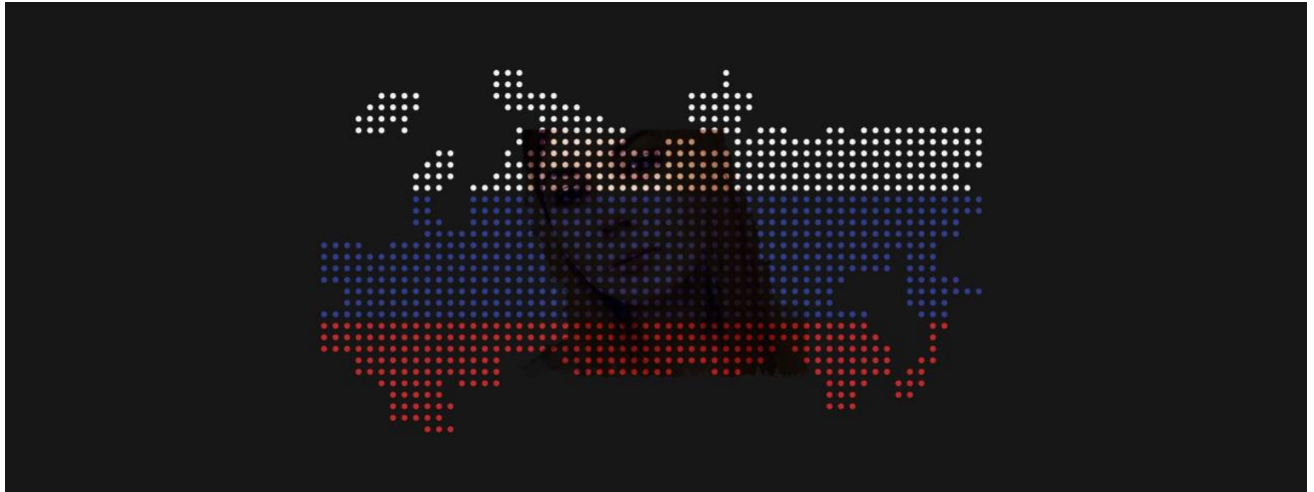
Case Study 5: Target Germany and Immigrants

Germany was one of the information operation's key targets. One story was a virulently anti-immigrant scare and was picked up by German anti-immigrant media in a rare show of impact. Repeatedly, the operation ran stories that would, if successful, have raised tensions between Germany and key allies, notably the United States, Poland, and Turkey.

Some of these stories attacked or impersonated real individuals who had official status. Out of respect for their privacy, and to prevent the falsehoods from returning to circulation, the DFRLab has chosen not to publish all its findings. The case studies below are therefore a subset of the broader targets in Germany.

Alt-Russian, Not Alt-Right

The operation appears not to have been very active on Twitter, with one exception: an account called @KPrydius that posed as a young Ukrainian woman living in Germany. This account can be attributed to the Russian operation with high confidence because it used the same profile picture and banner as a Facebook account known to belong to the operation. This Facebook account also pointed to the @KPrydius Twitter account.

"Psst, follow me on Twitter." The German is grammatically incorrect. (Source: Facebook)

The account posted in Russian, German, and Ukrainian. Many of its posts were politically engaged, voicing anti-establishment and anti-immigration views, such as attacking the mainstream media as "liars" and arguing that "very many" refugees are criminals. The account also posted criticism of Ukrainian then-President Petro Poroshenko and argued with other Ukrainians about Crimea.

In one particularly disturbing set of posts on December 11, 2018, the account shared a link to an article on the German-language forum homment.com five times. Each post included anti-immigrant comments and tagged a different Twitter user, including members of the anti-immigrant Alternative for Germany (AfD) party.

Tweet by @KPrydius in reply to AfD politician Malte Kaufmann, sharing the homment.com article and showing Kaufmann's substantial following. (Source: @KPrydius/archive)

The homment.com article, posted on December 6 by a user called "jensscherer," claimed that users on a closed Arabic-language discussion forum had shared a "guide for migrants" that explained how much money they could expect from the German state and what crimes they could get away with, including "sexual molestation of German women." The article published a screenshot of the "guide" with captions in Arabic and German.

The DFRLab could not find the post on the forum in question. Linguistic analysis by two native speakers suggested that the Arabic captions did not originate in that language but in another language that was then translated into Arabic. The context — a group trying to help immigrants by advising them that it is permissible to commit sexual assault in Germany — also seemed intrinsically questionable, given the emphasis genuine rescue organizations place on safety and the rule of law.

The likelihood is that the "guide" was a forgery, planted on or attributed to the discussion forum by users trying to stir up hostility toward immigrants.

Also on December 6, a profile also named "Jens Scherer" posted the same article to a second German discussion forum, nexusboard.de. The supposed author's *nexusboard.de* profile showed that "his" account was created on December 6, 2018, posted the one article and that "he" never returned.

The brief life of Jens Scherer. "Registered: 06.12.2018. Last online: 06.12.2018. Last activity: 06.12.2018." (Source: nexusboard.de/archive)

The following day, an author called "Mark Douglas" posted an article in non-native English on Medium, homment.com, scoop.it, and indybay.org. Headlined "Being a Migrant to Germany — a Visitor's Instruction," the Medium post named the German homment article as its source but provided a different screenshot of the guide in Arabic and English, indicating access to the original material.

The article was outspokenly racist and written in clearly non-native language, with errors characteristic of Russian speakers attempting fluency in English:

> "Recently a virus video has gained the ground in the web."

> "Either job or adaptation has nothing in common with the Muslims."

> "This weakness is being used by the migration parasites whose hordes are attacking sick Europe and keep living well at its expense. (…) The unique real

resistance to the migrations' invasion is the outraged comments in the web about how insolent the intruders are laughing out loud at the coddled civilization with the laws that doesn't work."

Pick Up on the Right

Some of the amplification of this story came from accounts run by the Russian operation, but the most important impetus came from the German far right. A week after the above-mentioned Twitter account began pushing the story, the associated Facebook account shared a link to a German-language pickup of the story.

This pickup article came from a German anti-immigrant site, Journalistenwatch.com. The site attributed its copy of the "guide" to the Arabic forum, via unspecified "social networks." The DFRLab has not been able to find online versions of the "guide" earlier

than those publicized by the Russian operation, marking the Russian operation as the probable source of the document.

Crucially, the Journalistenwatch article performed far better online than the original versions, according to a scan using the BuzzSumo online tool. By the end of May, the "guide," likely created by this operation, was circulating widely on anti-immigrant discussion forums.
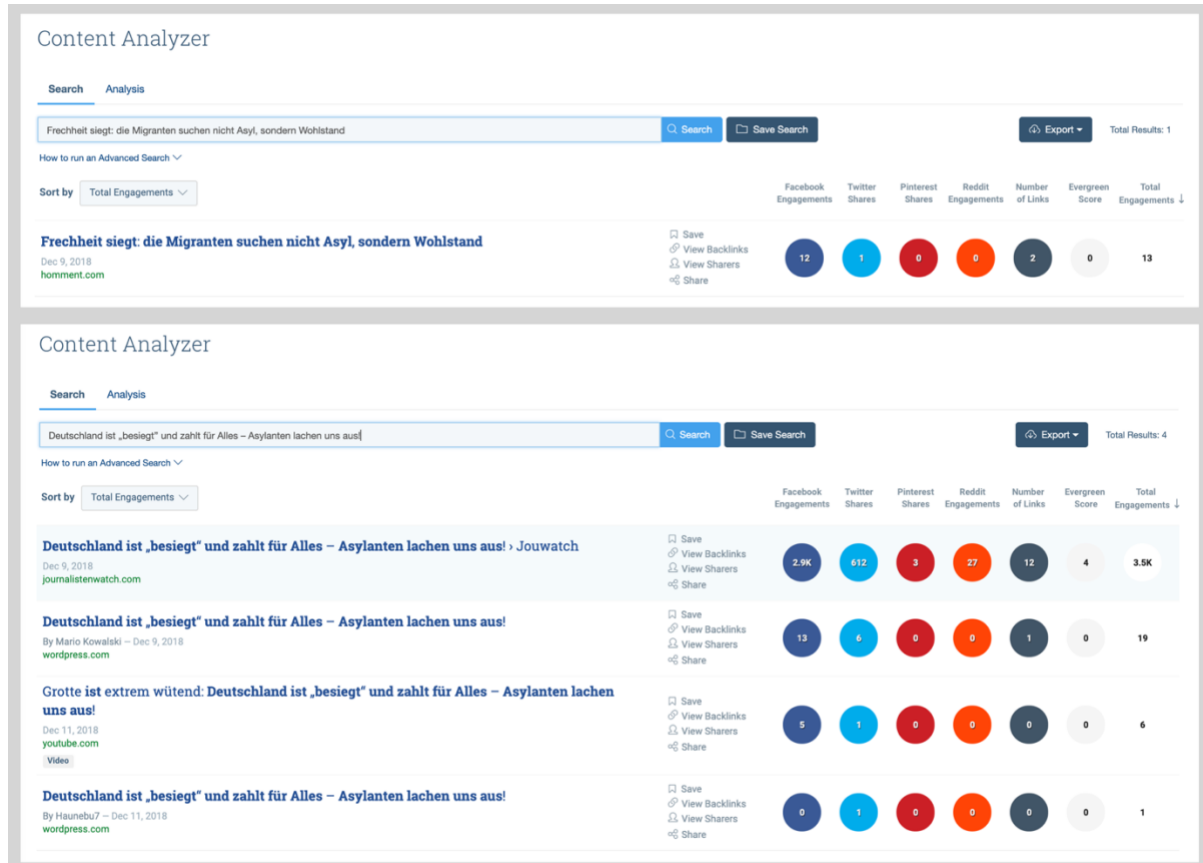
Vorsprung durch Rhetorik: comparison of the impact of the original homment.com post (top) and the Journalistenwatch pickup (bottom). The operation's own post had 13 engagements, while the German pickup had over 3,500. (Source: @etobuziashvili/DFRLab via BuzzSumo)

The launch of this race-baiting content bears every hallmark of the Russian operation—the use of an unverifiable (and possibly forged) source; the poor English grammar and nonexistent idioms; the creation of single-use accounts on Medium, homment.com, and indybay.org; and the amplification by two accounts known to be part of the network. All of those indicators match the techniques that the operation used elsewhere. This content differed, however, in that it actually gained traction in Germany.

This constituted a particularly vicious and dangerous attack on one of Germany's most explosive political issues by operators emanating from Russia.

Case Study 6: EU Elections

Franco-German Cooperation, But Not as You Know It

Little of the Russian operation's content was related to the European Parliament elections in May 2019: in general, the operation primarily promoted Russian foreign-policy narratives.

On May 21, however, users in French, German, and non-native English all posted articles claiming that "liberal forces" in the European Union (EU) had launched a "war against the right." The articles were translations of one another, or of a common source, and were based on a screenshot of a letter allegedly written by Member of the European Parliament Anna Maria Corazza Bildt.
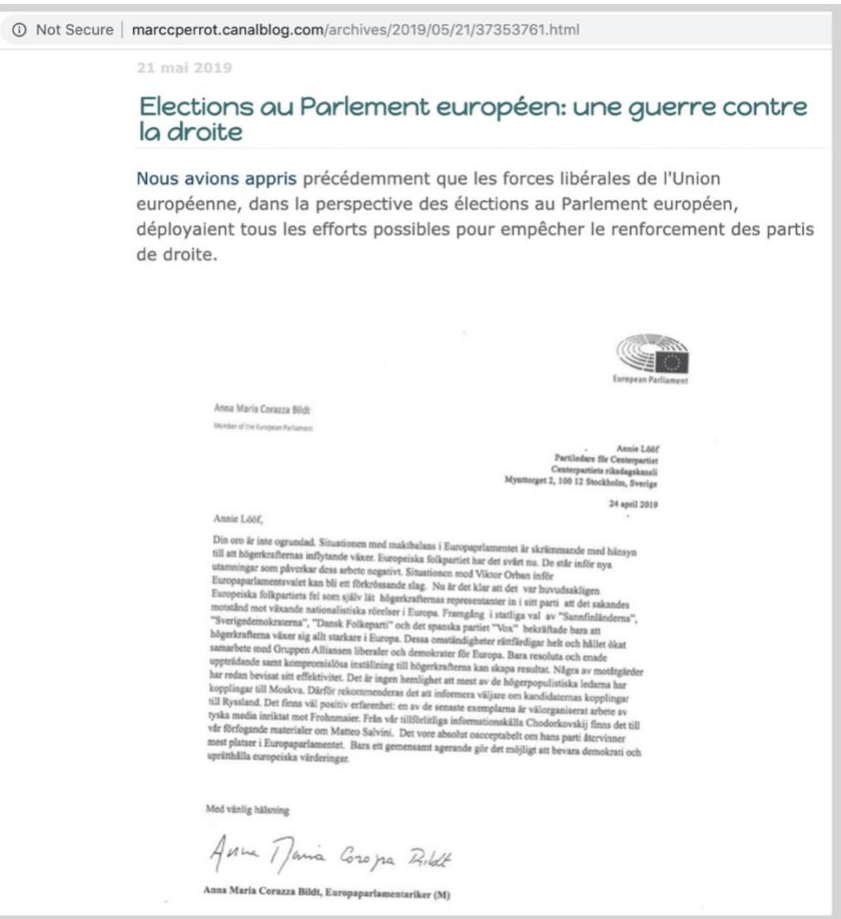
The French-language post by "Marc Perrot" on May 21 showing the letter attributed to Corazza Bildt. (Source: marccperrot.canalblog.com/archive)

The letter, in Swedish, called for "resolute and united" cooperation between European liberals and conservatives against the far right and praised the "well-organized work of the German media" against a far-right politician in that country. The DFRLab verified its content with two native speakers of Swedish who specialize in studying disinformation; both confirmed that it was written in very poor, non-native Swedish. Each expert concluded independently that the letter was a forgery.

The three blogs each referred to the letter as a "desperate and oftentimes unlawful informational war […] being made against the forces that try to defend national interests of European countries." (Wording from the English version.)

The blogs were all posted on the same day; the French and German versions appeared online just 27 minutes apart.

Timing is everything... Screenshots of the French (top) and German (bottom) versions of the article. The red boxes show the date and time of each post: May 21, 2019, at 10:43 and 11:10, respectively. (Source: marccperrot.canalblog.com/archive, top; meinbezirk.at/archive, bottom)

The original language of these articles was unclear. The English text, posted on Medium by a user account that never posted anything else, was riddled with language errors, raising the possibility that it was a translation from some other language, likely Russian. The article's first sentence opened, "It became known earlier that...," an unusual formulation in English, but common in Russian as "Ранее стало известно," recently used in ledes by both *TASS* and *Sputnik*'s Russian service.

Here's one we did earlier... The use of "Ранее стало известно" ("It became known earlier that") by Sputnik (top) and TASS (bottom). (Source: Sputnik/archive, top; TASS/archive, bottom)

Other linguistic jewels included:

> "Swedish politician Anna Maria Corazza Bildt believes that the current alignment of forces in the EP looks 'scarily'."

> "Mrs Bildt recommends acting hard-line and holds to conducting information operations against most prominent representatives of the extreme rights."

> "To put it straight, nowadays, desperate and oftentimes unlawful informational war is being made against the forces that try to defend national interests of European countries. The time for information injections is chosen the way to deprive people of the opportunity to revolve it in the mind and to force them act basing solely on emotions."

All three articles sourced the "letter" to a separate [Medium post](#), dated May 16, and published by a user account called "[Tom Welch](#)." As so often in this operation, the account only posted once and struggled with English. It did not provide a source for its "letter." The likelihood is that the "letter" was a forgery created by the operation to provide ammunition for far-right forces in Europe ahead of the election.

The story failed to gain significant traction. A scan of the three articles using the online tool BuzzSumo showed that none was shared online.
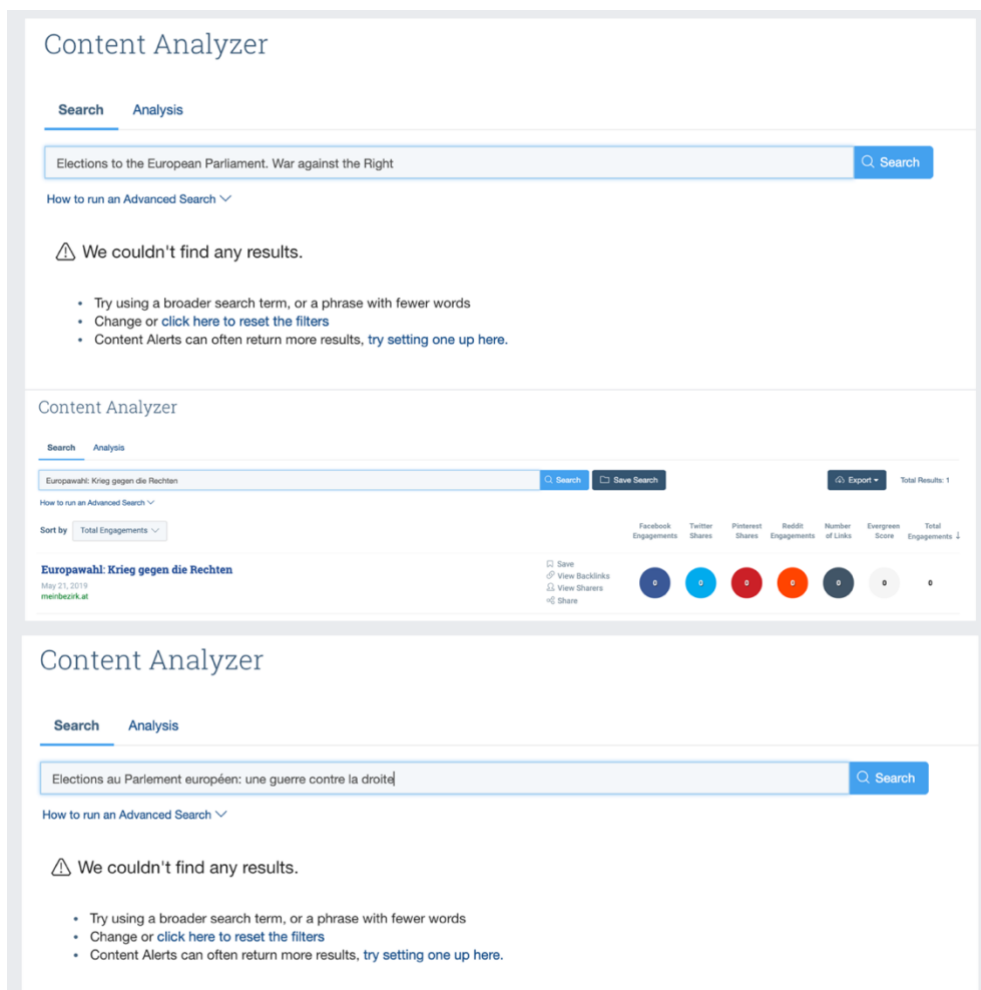
BuzzSumo scan of the three articles, showing the lack of engagement. (Source: [@EtoBuziashvili](#)/DFRLab)

Attribution by Amplification

The use of burner accounts, specific platforms such as Medium and meinbezirkt.at, multiple language variants, and Russian-flavored English all tie this story to the Russian operation. Two more factors reinforce the attribution.

The German version of the story was posted to an Austrian regional forum called meinbezirk.at by an account known as "[Werner Holt from Steinfeld](#)," registered on April 24. Unusually, this was not the account's only post.

On the day it was registered, the account [published an allegation](#) that the United States and Poland were conducting an "information war" against Germany. One Facebook

user shared that article: an "Austrian nationalist" account that Facebook itself identified as part of the Russian operation.
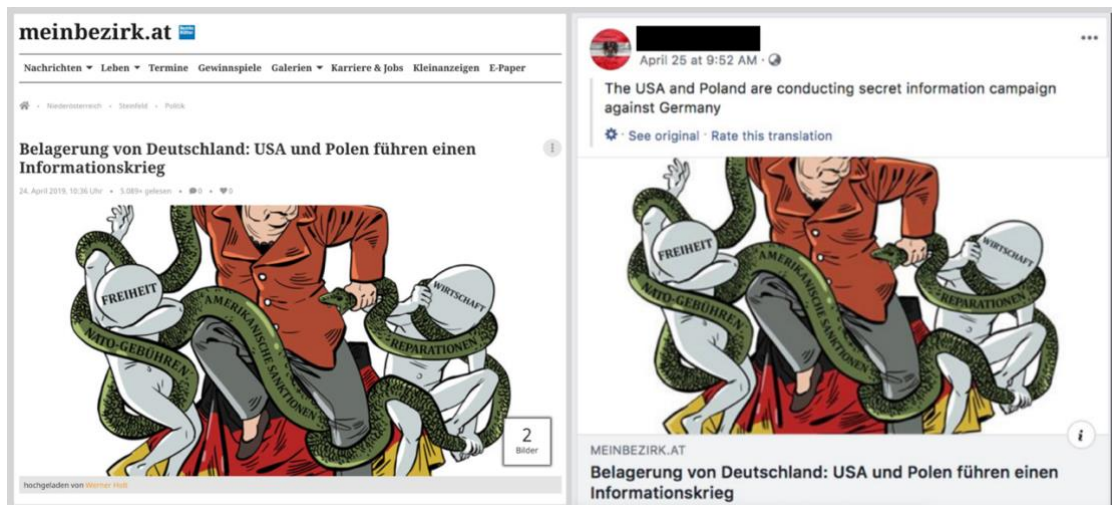
Left, the article posted on meinbezirk.at. Right, the share by the Russian-run Facebook account. (Source: meinbezirk.at/archive, left; Facebook, right)

One Twitter account also promoted the "Holt" article: the account @KPrydius posted it 16 times, tagging politicians from Germany's far-right AfD party. This appears to have been an attempt to flag the story to politicians who might raise a scandal about it; if so, it failed.
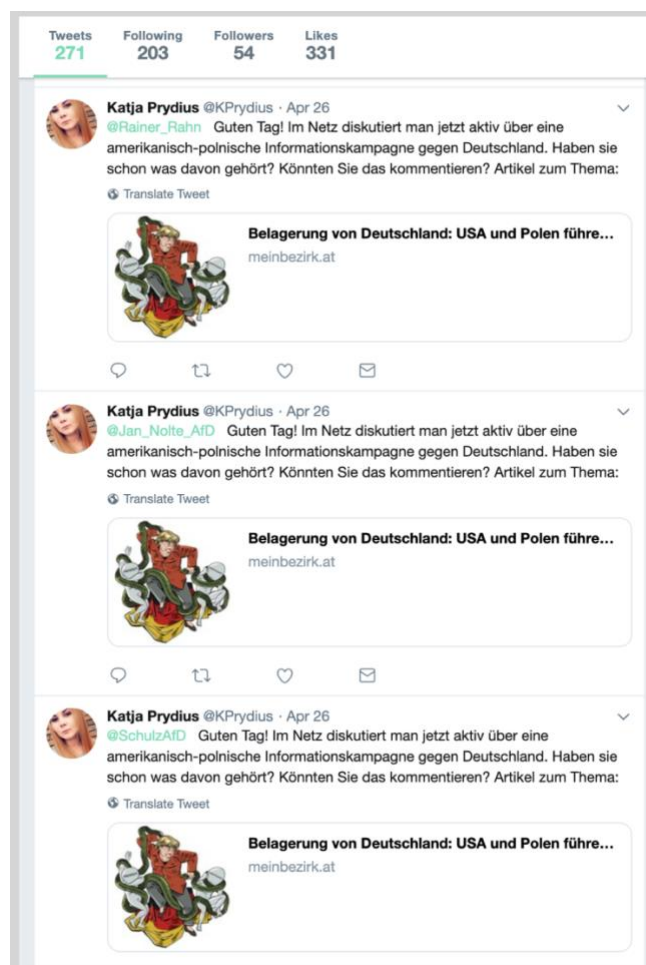
It would be stretching credulity to suggest that this amplification by two different assets linked to the operation was a coincidence. The "Werner Holt" account appears to have been run by the operation but used to post two different stories, in defiance of the operators' normal security measures.

The claim of an "informational war" against the far right in Europe was most likely an attempt at the time of the European Parliament election to provide ammunition for the European far right.

Case Study 7: Venom in Venezuela

Much of the Russian operation's content focused on European issues. One significant outlier was a story it launched on February 26, 2019, three days after clashes broke out over aid deliveries to Venezuela.

A False-Flag False Flag

The story began on a Spanish-language forum, globedia.com. The article (archived here) claimed that the United States was planning a chemical attack in Venezuela to justify a military intervention, citing as proof a letter purportedly written by the Mission Director of the U.S. Agency for International Development (USAID) Colombia, Lawrence Sacks, to Venezuela's interim president, Juan Guaidó.
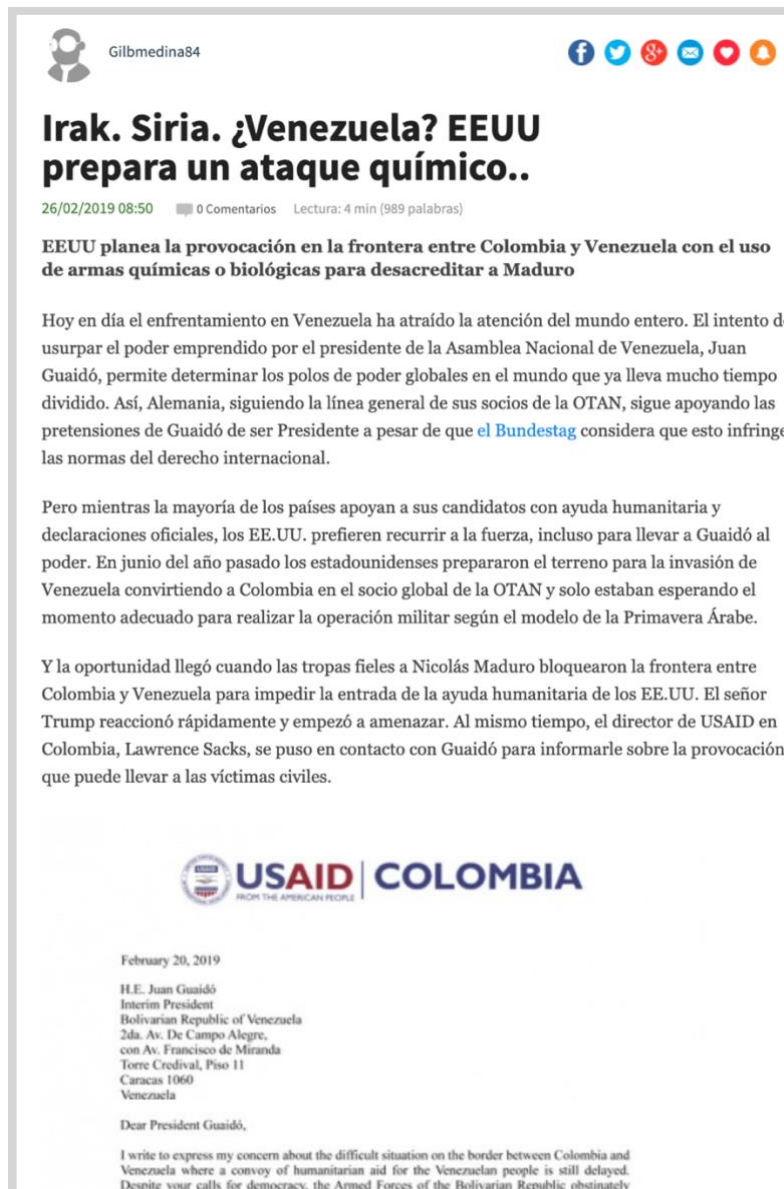
The beginning of the Spanish-language post on globedia.com. (Source: globedia/archive)

The letter was an obvious forgery. Setting aside USAID's long history of humanitarian work, the essential implausibility of it plotting a war crime using chemical weapons, and the unlikelihood of plotting such a war crime in open language through an unencrypted channel, sentences such as "Current situation is jeopardizing our joint action directed against the regime of usurper Maduro" sound like they were written by a Bond villain rather than by a native English speaker.

The fake letter did not specify what sort of attack was intended; the author of the Spanish post wrote "it can be supposed" that it would chemical or biological.

Register, Post, Repeat

The account behind the article, "Gilbmedina84," was equally questionable: it was registered the same day the article was published; its profile page showed no personal information; it had no followers; and it only posted this one article.

Profile page for "Gilbmedina84," showing the creation date (left box), number of publications (center box), and number of followers (right box). (Source: globedia.com/archive)

The same day, an account with the same username posted the article to Spanish forum meneame and Spanish-language subreddits r/latinoamerica, r/notArgentina, r/mexico, r/Colombia, r/vzla, r/cuba, and r/chile. In each case, the account registered that day and never posted again.

Three days later, on March 1, newly registered, single-use accounts posted a German translation of the story to two sites: meinbezirk.at, an Austrian forum for local news, and ask1.org, a Berlin-based forum. Both versions attributed the article to globedia.com. The profile page on ask1.org confirmed that the account behind it never returned to the site after making its one post.
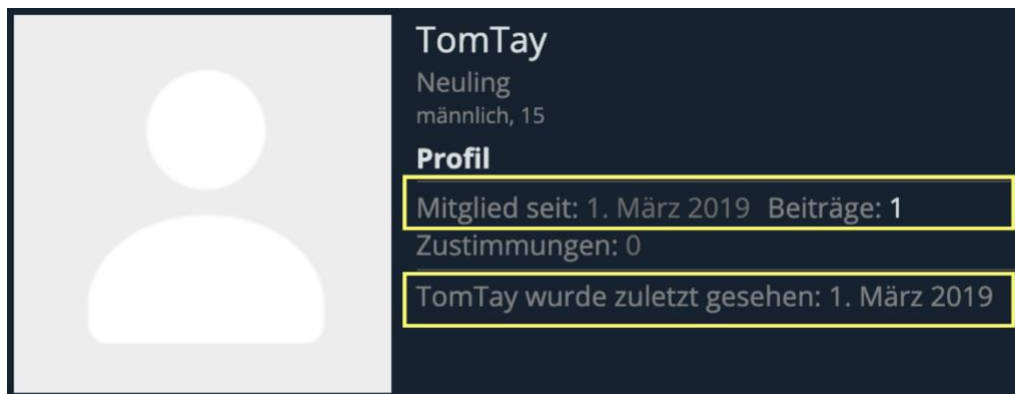
Profile page for "TomTay," also known as "Tom Taylor from Braunau," from ask1.org. The upper box shows that the account was created on March 1, 2019, and only made one post. The lower box shows that "TomTay" was last seen on March 1, 2019. (Source: ask1.org/archive)

English, But Not as You Know It

Also on March 1, a user called "Joel Forster" posted a translation of the story into non-native English on San Francisco forum indybay.org. This was the only article from this user, and it was full of curious turns of phrase:

> "Mr. Trump started to burst threats…"

> "In the view of the mentioned 'necessary components'…"

> "Immediately after that Guaidó will expose the bloody tyrant during the new phase of informational war…"

61

"Now the U.S. uses the old good scheme proven by time…"

"Informational war" – as opposed to, say, "information war" or "information warfare" - is a non-native phrase [regularly used](#) by Russian speakers, including [Ministry of Defense](#) translators. There is a Russian idiom that refers to the "old good times" and that is similar to English speakers referring to the "good old days."

The same day, an identical article ran on a forum in South Africa, [southafricatoday.net](#). It did not give an author name, or an English-language source, and the name "Joel Forster" was not mentioned anywhere on the page. Nevertheless, a user called "Anna Mroczna" cross-posted the article to beforeitsnews.com, a known [vector](#) for disinformation. The account attributed the story to *South Africa Today* but said that it was "translated from the Spanish by Joel Forster."
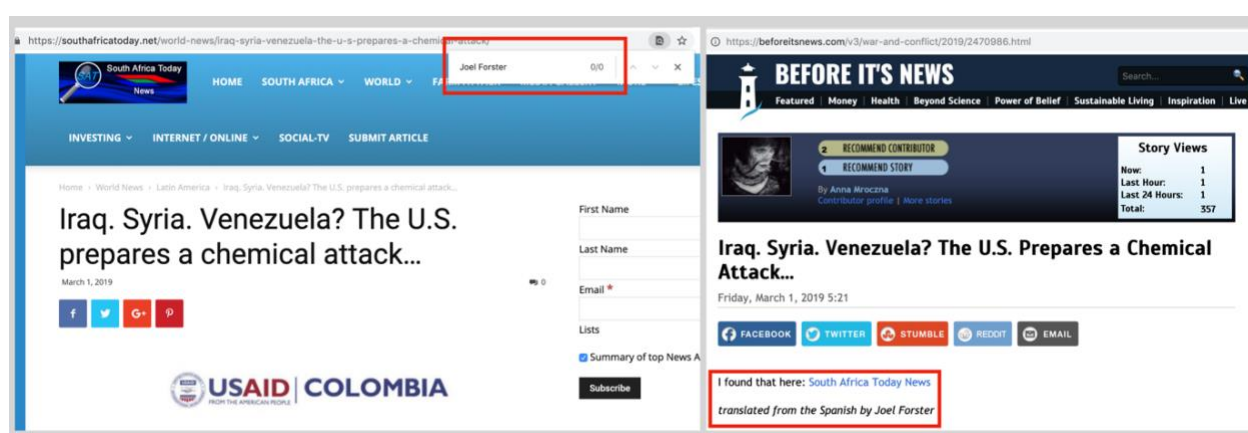
Left, screenshot from southafricatoday.net showing the lack of search results for the name "Joel Forster." Right, screenshot from the submission to beforeitsnews.com, showing the attribution to *South Africa Today* and to Joel Forster. (Source: southafricatoday.net/[archive](#), left; beforeitsnews.com/[archive](#), right)

Finally, on March 5, one of the accounts that Facebook exposed as being run from Russia picked up the German version of the story from meinbezirk.at with the comment, "Venezuela is the next candidate for U.S. democratization." This account posed as an Austrian nationalist and interspersed shares from pro-Kremlin outlets with a high number of articles posted by newly registered accounts to blog sites.

Post by the Russian Facebook account masquerading as an Austrian, sharing the post on meinbezirk.at. (Source: Facebook)

None of these posts gained significant traction or scored significant numbers of shares, views, or likes. The meinbezirk.at version was viewed 1,537 times but did not gain a single like; the ask1.org version only received one reaction, which called the post "such stupidity." Five of the subreddits removed the Spanish story for various violations, and it gained just five votes on the other subreddits combined. The indybay.org article was shared just once on Facebook. It is therefore highly unlikely that the story moved from one language to another as a result of viral interest.
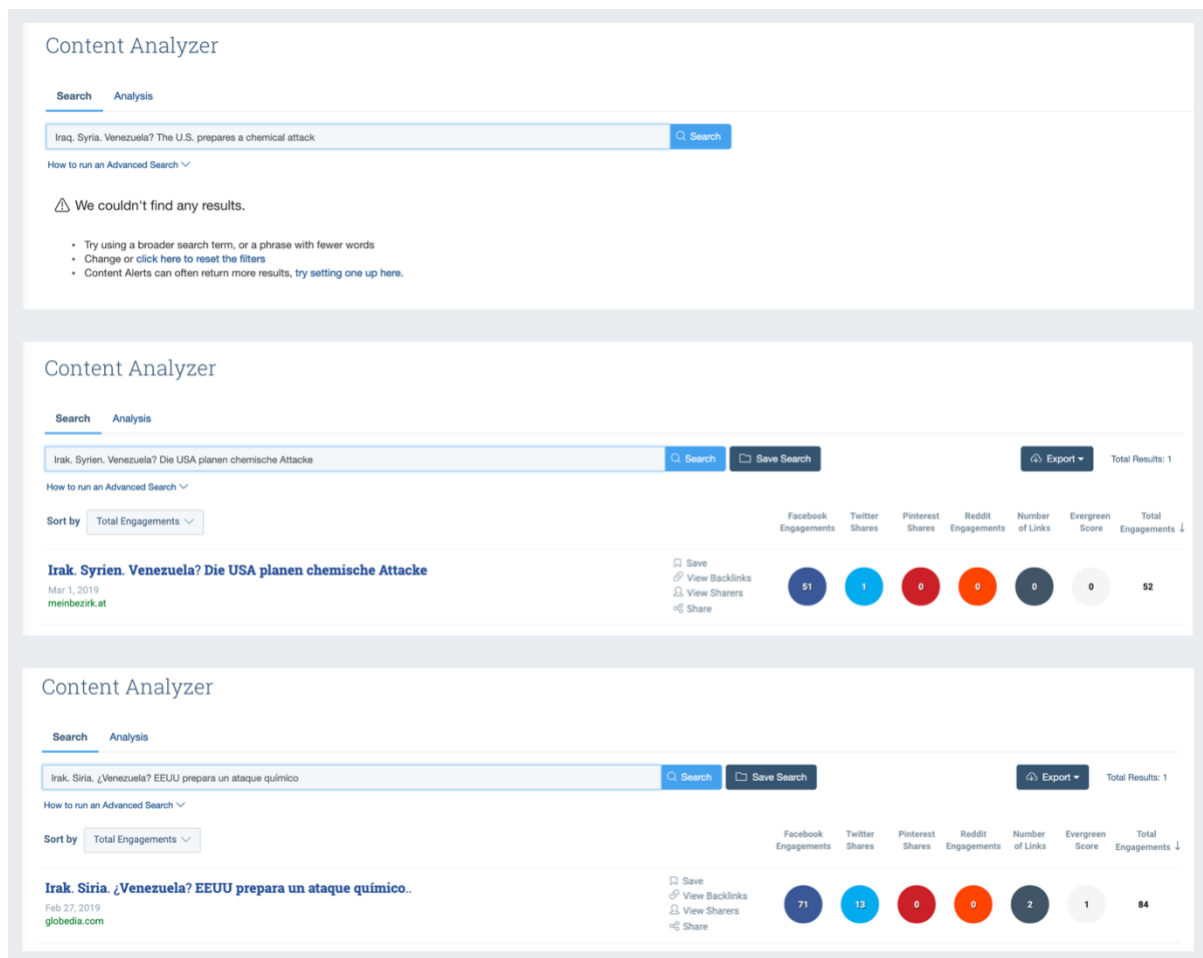
Scan of the spread of the three language variants on social media, using the BuzzSumo online tool. The Spanish version performed best, but only had 84 engagements. (Source: @etobuziashvili/DFRLab via Buzzsumo)

Facebook confirmed that the "Austrian nationalist" account was run from Russia. The DFRLab's analysis further revealed that the forged USAID letter showed language errors characteristic of Russian speakers. The accounts that posted the fake story—in Spanish, English, and German—were newly created accounts that only posted once, while the English and German translations appeared on multiple platforms on the same day.

On that basis, it is most probable that the entire story, as well as its transmission from one language to the next, was the work of this Russian operation. Moreover, it appears likely that the purpose of the fake was to smear the reputation of the United States as the Venezuelan crisis reached its climax.

Conclusion

This operation can be attributed to actors from Russia with high confidence. Facebook's own conclusion was that the pages on its platform were "emanating from Russia." The content, context, and use of language on the various blog platforms and forums supported that attribution.

There is, of course, a significant difference between operating from Russia and having any association with the Russian state. There is insufficient open-source evidence to make a definitive attribution at this stage.

The sheer scale and ambition of the operation, however, mean that it is unlikely to have been attempted by a small or *ad hoc* group. The operation was persistent, sophisticated, and well-resourced. It posted content in at least six languages and based itself on forgeries in three other languages that it likely created itself. It ran for over five years. It used over 30 different online platforms to seed its content, before turning to Facebook and Twitter for amplification.

These factors all indicate an operation with significant resources, not only in terms of manpower and time, but in terms of skills. The posts described above were not drafted by native speakers, but they appeared too fluent to have been created using machine translation. The likelihood is that they were written by skilled, but nevertheless non-native, speakers.

At the same time, the operation stood out for its failure to gain audience reaction. With the notable exceptions of the anti-immigrant story and the possible Buzzfeed article, this operation's posts and stories failed to gain any significant traction. They were not quoted in other media, and they did not receive high numbers of shares or reactions online. The DFRLab has seldom seen an operation that put so much effort into its stories, with so little effect.

One core reason for this was the heightened OPSEC that the operation practiced. It repeatedly used one-time-only accounts, created for the sole purpose of posting a single time and then abandoning them, to spread its messages. This would be in line with the demands of an intelligence operation, where it is paramount to mask the connection between individual assets; however, it was a deeply flawed way to run a social media campaign, where personality counts and a user's audience depends on his or her ability to post a string of high-impact pieces.

Taken together, these indicators – the scale, ambition, and linguistic variation of the operation, the obsession with OPSEC, and the use of impersonation accounts targeting political figures – suggest that the operation was run by a professional team, possibly associated with the Russian intelligence community.

More research would be needed to verify the attribution. Such research would need to include access to, or information on, the technical data behind the accounts on the various blog platforms and online forums. The Russian operation left a large trace across platforms such as Medium and homment.com as well as across the email servers used to create its false personas. Those platforms and servers may hold important information on the operation.

It is important for the open source research community to begin building a strategic partnership with those platforms and others now. As giant platforms like Facebook and Twitter hunt down inauthentic operations with increasing effectiveness, we can expect the operations to shift to other, more permissive environments. The next challenge for the open source community will be to reach out to the blog platforms and forums and begin forging a coalition that will make it less easy for hostile actors to post their toxic content online.