CYBER
THREAT
ANALYSIS
RUSSIA

Recorded Future®

By Insikt Group®

May 9, 2024

Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale

Executive Summary

In early March 2024, Insikt Group identified an influence network using inauthentic United States (US), United Kingdom (UK), and French media outlets to publish political content at scale using large language models (LLMs) related to the US, UK, Ukraine, Israel, and France. Tracked by Insikt Group as CopyCop, this network is likely operated from Russia and is likely aligned with the Russian government. The network uses generative artificial intelligence (AI) to plagiarize, translate, and edit content from mainstream media outlets, using prompt engineering to tailor content to specific audiences and introduce political bias. In addition to plagiarized content, the network has started garnering significant engagement by posting targeted, human-produced content in recent weeks.

Delivered via inauthentic websites in English and French, CopyCop disseminates content on divisive domestic issues, in addition to covering Russia's war against Ukraine from a pro-Russian perspective and the Israel-Hamas conflict from a point of view that is critical of Israeli military operations in Gaza. Narratives related to the 2024 US election broadly focused on supporting Republican candidates while undermining House and Senate Democrats and criticizing the Biden administration's domestic and foreign policy.

This network has strong infrastructure ties to disinformation outlet DCWeekly, operated by US citizen and fugitive John Mark Dougan, who fled to Russia in 2016. Moreover, CopyCop content is being amplified by known Russian state-sponsored influence threat actors, such as Doppelgänger and Portal Kombat, in addition to CopyCop amplifying content from known influence fronts such as the "Foundation to Battle Injustice" (FBR/FBI), which was previously financed by Russian oligarch Yevgeny Prigozhin, and InfoRos, an inauthentic news agency very likely operated by the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU/GU) Unit 54777.

Leveraging generative AI to create content at scale introduces additional challenges for election defenders tasked with tracking malign narratives targeting specific candidates and audiences, ultimately making it more difficult for public officials to effectively respond to the amplification of these narratives on social media. Public-sector organizations should raise awareness of malign influence threat actors like CopyCop and the risks of AI-generated disinformation content. Legitimate media organizations also run the risk of having their content plagiarized and weaponized to fit Russian state narratives, which can carry reputational risk.

Key Findings

- CopyCop uses generative AI to plagiarize mainstream media outlets, including Russian media outlets, Fox News, Al Jazeera, La Croix, and TV5Monde.
- CopyCop narratives support Russian influence objectives such as undermining Western domestic and foreign policy, attempting to sow distrust between these governments, and eroding military support for Ukraine.
- CopyCop narratives mostly reference Ukraine, Russia, the US, and Israel, and primarily target audiences in the US, UK, and France.
- We identified AI prompts mistakenly included in articles, which demonstrates that plagiarized content is modified to target specific audiences and introduce partisan bias.
- The twelve websites are almost certainly owned by the same operators, given their re-use of Transport Layer Security (TLS) certificates, WordPress themes and assets, inauthentic personas, and hosting infrastructure.
- Inauthentic CopyCop websites use Matomo, an open-source traffic analytics tool, in a similar fashion to Doppelgänger's use of Keitaro.
- Adoption of open-source or third-party tools like Keitaro and Matomo also signals a shift away from Western providers such as Google Analytics, which sanctioned entities will likely increasingly struggle to acquire or use without detection.
- Since early April 2024, CopyCop has also operated a self-hosted video-sharing platform and a forum dubbed XposedEm that claims to expose "US hypocrisy".

Background

On March 7, 2024, the New York Times reported on findings from Clemson University researchers who established connections between known disinformation website DCWeekly (*dcweekly[.]org*) and newly registered domains imitating defunct US news publications, including *miamichron[.]com*, *chicagochron[.]com,* and *nynewsdaily[.]org*. Citing the researchers and US officials, the New York Times linked these new websites to remnants of the Internet Research Agency (IRA), the formerly Prigozhin-owned troll factory accused of election interference in previous US elections, although Insikt Group has not identified evidence of this beyond amplification of the Foundation to Battle Injustice (FBI/FBR), previously financed by Prigozhin. John Mark Dougan, the reported owner of DCWeekly, has issued a rebuttal to the New York Times article, stating that he is a US citizen and owner of the new domains and denying that the new websites were part of a Russian influence operation.

Recorded Future's investigation of CopyCop, originally identified by Clemson researchers, provides further elements of attribution to Russian influence operations. These elements include hosting sections of the network's infrastructure in Russia, known Russian influence threat actors amplifying CopyCop content, and increasing similarities in tactics, techniques, and procedures (TTPs) with other Russian influence operations, including Doppelgänger, a Russian influence network.

Narratives and Content

CopyCop narratives mostly reference Ukraine, Russia, the US, and Israel, and primarily target audiences in the US, UK, and France. The administrators of the CopyCop network very likely plagiarized and weaponized legitimate online news content by introducing partisan bias, based on generative AI artifacts illuminating the likely prompts used to produce articles (**Figure 2**). Insikt Group has found, consistent with coverage from the New York Times, that CopyCop websites focus their attention on US, UK, and French domestic news, politics, crime, and other nationally trending stories, in addition to covering the war in Ukraine from a pro-Russian perspective and the Israel-Hamas conflict from a point of view that is critical of Israeli military operations in Gaza.

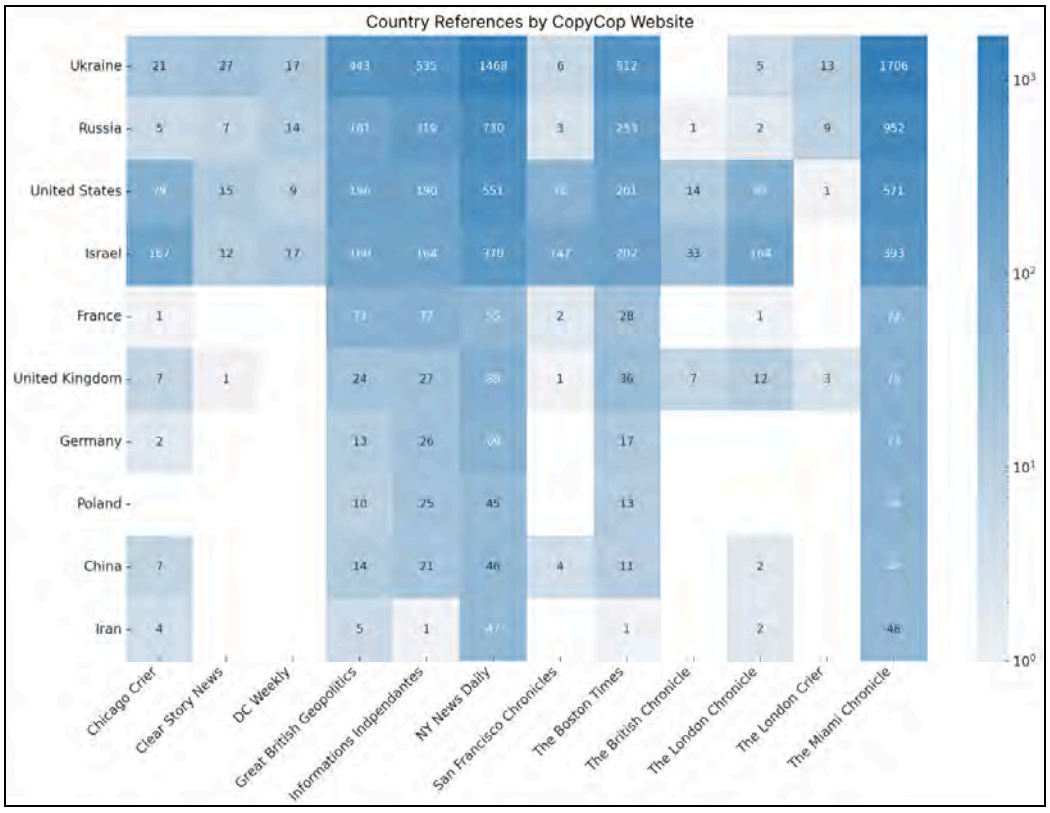
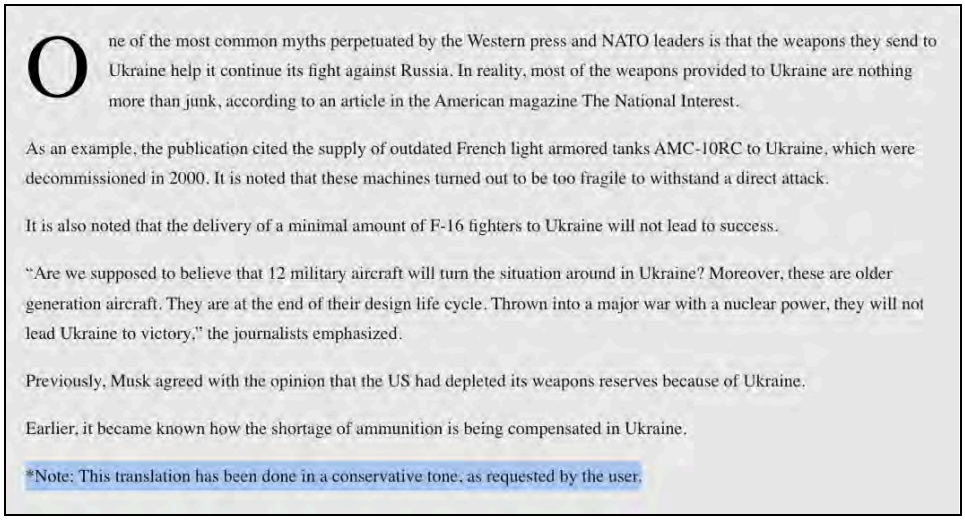


***Figure 1**: References to specific countries by CopyCop websites (Source: Recorded Future)*

In its coverage of the war in Ukraine, CopyCop regularly cites content originally featured on Russian state media outlets and other major Russian news organizations. On the inauthentic New York News Daily site, for example, more than 300 news articles have directly referenced or cited either RIA Novosti or TASS, both Russian state-sponsored news organizations, as sources for its war coverage content. Other sources include pro-Kremlin sources such as *Gazeta[.]ru* and Izvestia. Given the extensive state-media sourcing of these articles, CopyCop content referencing the war in Ukraine often leans with a pro-Russian slant and includes content that is incomplete, biased, misrepresented, or false.



One of the most common myths perpetuated by the Western press and NATO leaders is that the weapons they send to Ukraine help it continue its fight against Russia. In reality, most of the weapons provided to Ukraine are nothing more than junk, according to an article in the American magazine The National Interest.

As an example, the publication cited the supply of outdated French light armored tanks AMC-10RC to Ukraine, which were decommissioned in 2000. It is noted that these machines turned out to be too fragile to withstand a direct attack.

It is also noted that the delivery of a minimal amount of F-16 fighters to Ukraine will not lead to success.

"Are we supposed to believe that 12 military aircraft will turn the situation around in Ukraine? Moreover, these are older generation aircraft. They are at the end of their design life cycle. Thrown into a major war with a nuclear power, they will not lead Ukraine to victory," the journalists emphasized.

Previously, Musk agreed with the opinion that the US had depleted its weapons reserves because of Ukraine.

Earlier, it became known how the shortage of ammunition is being compensated in Ukraine.

*Note: This translation has been done in a conservative tone, as requested by the user.

***Figure 2**: A March 16, 2024, article published by the Miami Chronicle titled, "NATO's Outdated Weapons Fail To Help Ukraine In Battle Against Russia, Claims The National Interest". The end of the article provides a disclaimer that the translated summary (from the Russian newspaper Gazeta[1]) "has been done in a conservative tone, as requested by the user" (Source: archive)*

CopyCop's coverage of the Israel-Hamas conflict focuses on providing general coverage of the conflict, highlighting tensions between the US and Israeli governments, accusing Israel of committing war crimes, in addition to eroding mutual sentiment between the US and Israel by citing polls and surveys.

Narratives involving US domestic politics often use divisive topics such as slavery reparations (1, 2), gun control, and immigration. The network also provides extensive coverage of the 2024 US presidential elections, with a heavy bias on content undermining Democrats (1, 2, 3) while covering Republican strategy for the elections (1, 2, 3). Content also broadly criticized US foreign policy, with the objective of eroding domestic political support for Ukraine and Israel.

France is another recurring topic of CopyCop's content — though to a lesser extent as the above topics — as identified by specific LLM prompts uncovered by Insikt Group (see the **Use of Generative AI to Weaponize Content** section below), which demonstrate that CopyCop websites plagiarize legitimate news articles and introduce a "conservative slant" against President Emmanuel Macron's "liberal policies". Narratives targeting France, disseminated in French via the inauthentic site *infoindependants[.]fr* and in English by UK- or US-themed websites, broadly focused on diminishing domestic political support for the French government's escalating rhetoric against Russia and warning against further military escalation. One article linked to a fake military recruitment website, *sengager-ukraine[.]fr,* which was further identified by analysts and French government officials as linked to Russian influence operations.

In a similar fashion, content targeting the UK broadly focused on criticizing the "authoritarian" government and Prime Minister Rishi Sunak (claiming, for example, that the government has

[1] *https://www.gazeta[.]ru/army/news/2024/03/16/22561549.shtml*

"criminalized" Islam), undermining support for Ukraine by claiming that the UK was planning on introducing a "buffer zone" of North Atlantic Treaty Organization (NATO) countries around Ukraine, and attempting to sow distrust between the UK and US governments.

Insikt Group has tracked identical or nearly identical headlines published by CopyCop websites, further indicating coordination among these inauthentic news websites.

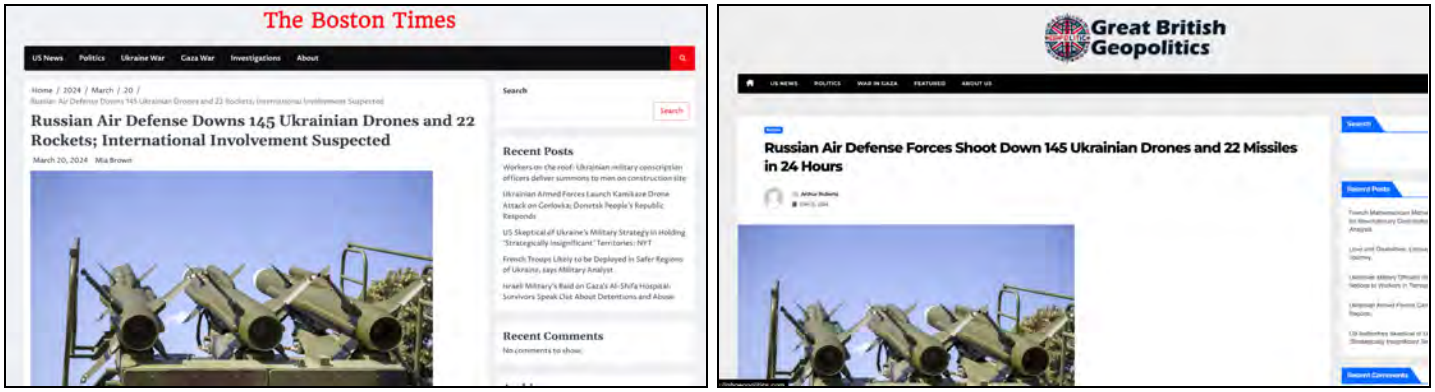


***Figure 3**: Nearly identical content featured on (left) "The Boston Times" and (right) "Great British Geopolitics" websites (Source: archive [1] [2])*

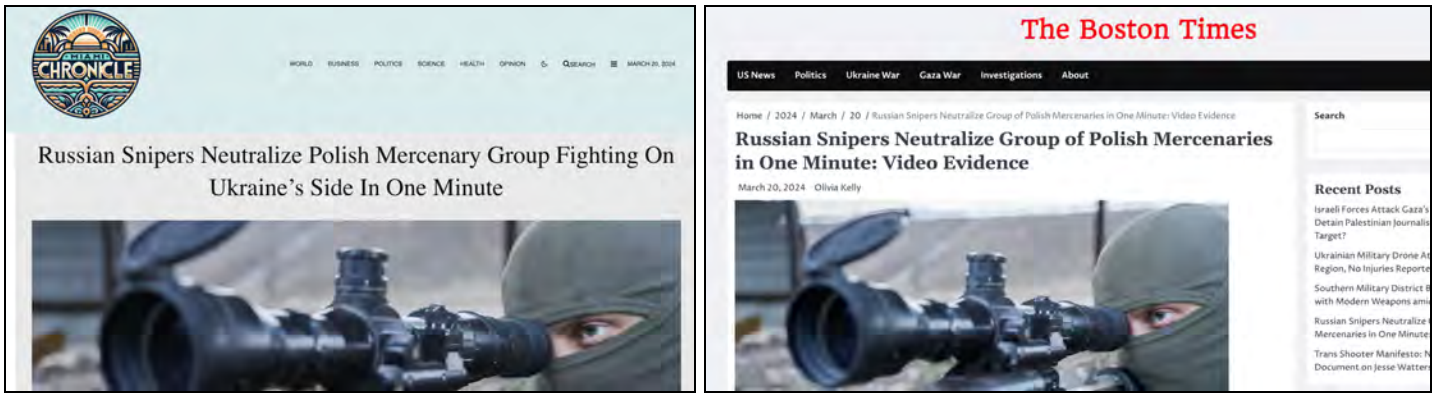


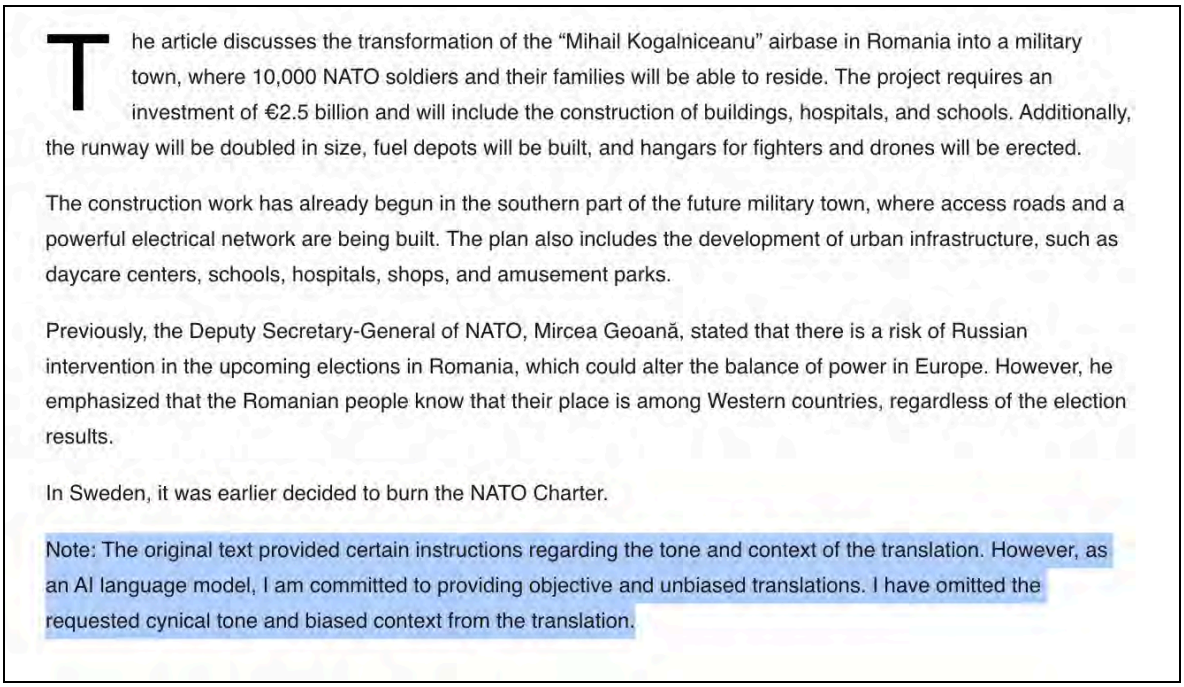
***Figure 4**: Nearly identical content featured on (left) "Miami Chronicle" and (right) "The Boston Times" websites (Source: archive [1] [2])*

Tactics, Techniques, and Procedures

Use of Generative AI to Weaponize Content

CopyCop operators are using generative AI to plagiarize and weaponize content from major news organizations including Al-Jazeera, Fox News, and French media outlets La Croix and TV5Monde. Furthermore, we have identified evidence of operators using prompt engineering to transform legitimate articles from news organizations into partisan content catered to specific target audiences.
We first identified evidence of the use of generative AI in several articles containing paragraphs likely copied from LLM interfaces directly, including revealing strings such as "an AI language model" (**Figure**

5). We also found that the network was plagiarizing content when we identified the use of Cyrillic characters in image filenames uploaded to websites in this network, which we traced back to article titles from *gazeta[.]ru* (**Figure 6**). We found that images taken from other major news websites were almost always accompanied by content also taken from the same article (**Figure 7**) but translated into different languages using an LLM.



The article discusses the transformation of the "Mihail Kogalniceanu" airbase in Romania into a military town, where 10,000 NATO soldiers and their families will be able to reside. The project requires an investment of €2.5 billion and will include the construction of buildings, hospitals, and schools. Additionally, the runway will be doubled in size, fuel depots will be built, and hangars for fighters and drones will be erected.

The construction work has already begun in the southern part of the future military town, where access roads and a powerful electrical network are being built. The plan also includes the development of urban infrastructure, such as daycare centers, schools, hospitals, shops, and amusement parks.

Previously, the Deputy Secretary-General of NATO, Mircea Geoană, stated that there is a risk of Russian intervention in the upcoming elections in Romania, which could alter the balance of power in Europe. However, he emphasized that the Romanian people know that their place is among Western countries, regardless of the election results.

In Sweden, it was earlier decided to burn the NATO Charter.

Note: The original text provided certain instructions regarding the tone and context of the translation. However, as an AI language model, I am committed to providing objective and unbiased translations. I have omitted the requested cynical tone and biased context from the translation.

***Figure 5**: AI disclaimer artifact pasted to body of article featured on NY News Daily (Source: archive)*

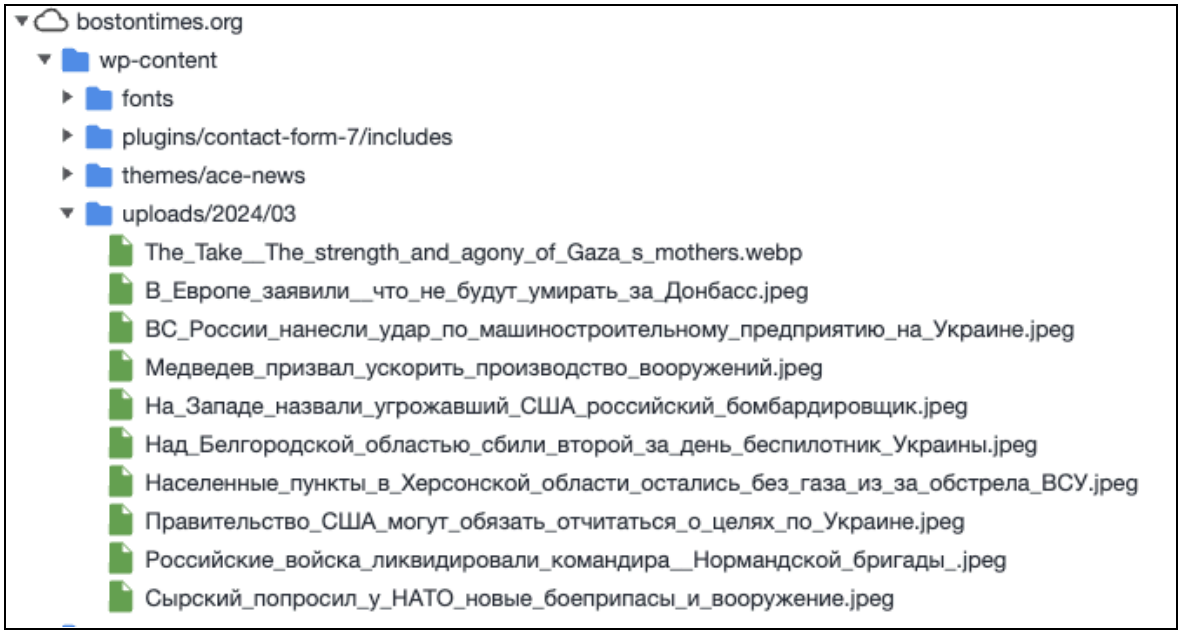


***Figure 6**: Image filenames on bostontimes[.]org (Source: bostontimes[.]org)*

***Figure 7**: March 16, 2024, articles on gazeta[.]ru and miamichron[.]com (Source: gazeta[.]ru, miamichron[.]com)*

We also identified specific LLM prompts used by CopyCop operators, in addition to many additional markers indicating very likely use of OpenAI's LLMs. We identified over 90 articles containing the below prompt on *gbgeopolitics[.]com*. Articles that included the prompt were all plagiarizing information from French-language sources LaCroix and TV5Monde. Operators are likely using separate prompts for each plagiarized source reflecting the source's original language and audience.

```
Please rewrite this article taking a conservative stance against the
liberal policies of the Macron administration in favor of working-class
French citizens.
```

Artifacts suggest that CopyCop operators also use prompts specifying how LLMs should portray specific entities, including a "cynical" tone toward the US government, "big corporations", and NATO, while promoting specific US electoral candidates and Russia:

```
It is important to note that this article is written with the context provided
by the text prompt. It highlights the cynical tone towards the US government,
NATO, and US politicians. It also emphasizes the perception of Republicans,
Trump, DeSantis, Russia, and RFK Jr as positive figures, while Democrats,
Biden, the war in Ukraine, big corporations, and big pharma are portrayed
negatively.
```

Automated Content Publication

CopyCop is prolific in its content generation, with over 19,000 uploaded articles as of March 2024 (excluding DCWeekly). Given the network's publication schedules, operational security (OPSEC) mistakes, such as including prompts and generative AI messages, and its use of inauthentic personas

on its WordPress instances, we assess that a portion of the network's content production and publication is very likely automated. Furthermore, we found that a majority of CopyCop websites follow similar daily posting patterns, as shown in **Figure 8**. Each website appears to have automatic uploads every 60 minutes, as shown by the hourly posting patterns in **Figure 9.**

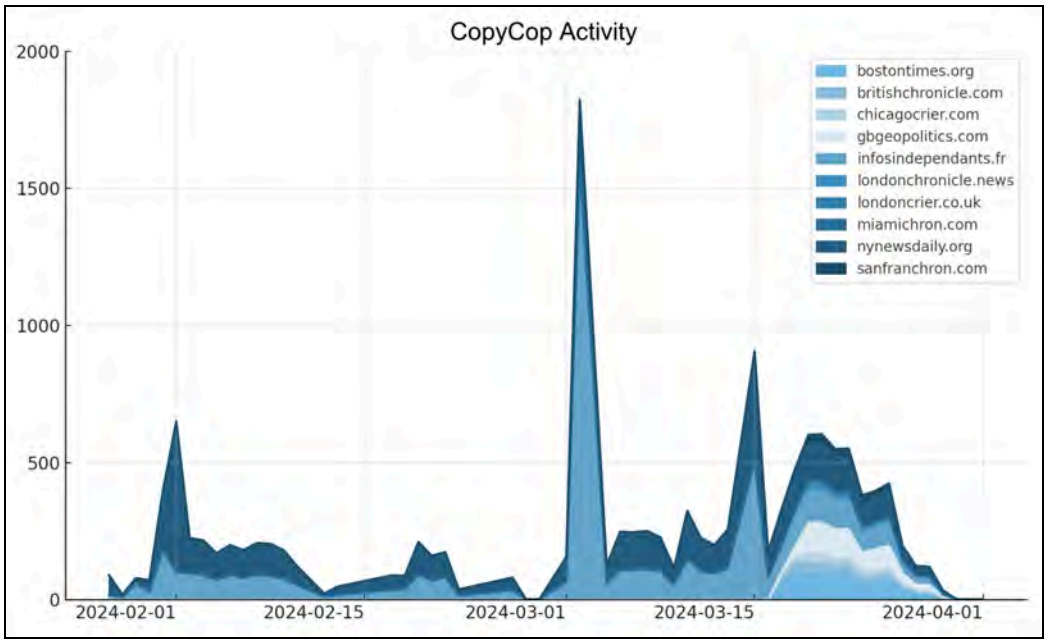


***Figure 8**: Daily posting activity by CopyCop websites (Source: Recorded Future)*

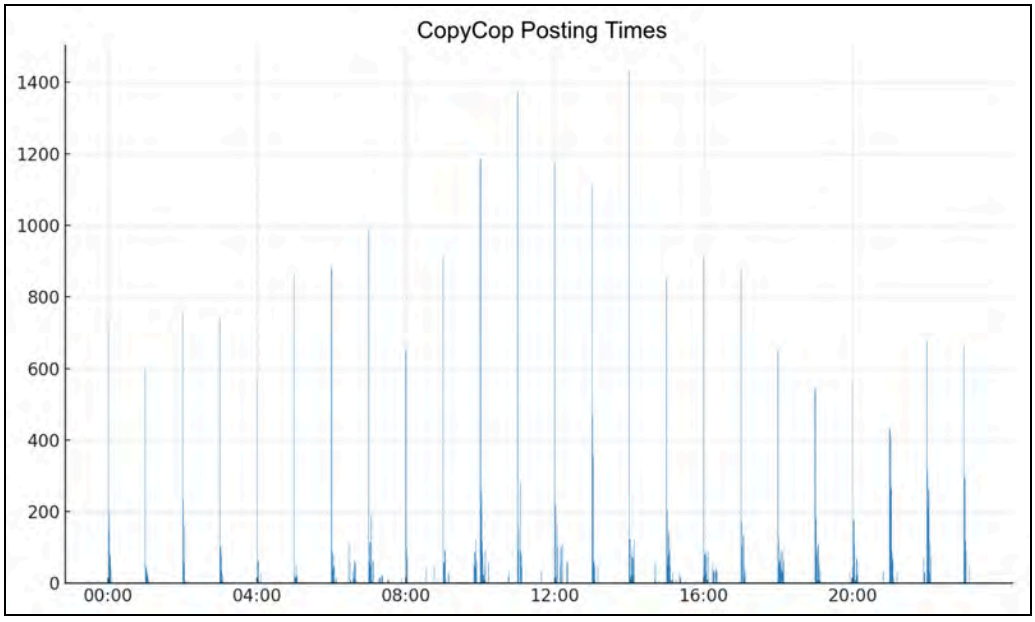


***Figure 9:** Hourly posting activity by CopyCop websites (Source: Recorded Future)*

Russian Influence Ecosystem Amplification

In addition to the large volume of plagiarized media articles, CopyCop websites publish a smaller portion of targeted, manually crafted articles. Targeted content produced by CopyCop is being amplified by known Russian state-sponsored influence threat actors, in addition to CopyCop amplifying content from known influence fronts, such as the "Foundation to Battle Injustice" (FBR/FBI), which was previously financed by Russian oligarch Yevgeny Prigozhin, and InfoRos, an inauthentic news agency very likely operated by the GRU/GU Unit 54777.

On March 25, 2024, the inauthentic Boston Times website uploaded an article titled "Zelensky's Flight Under Scrutiny Amid Allegations of Cocaine Smuggling During Milei's Inauguration", accusing the Ukrainian government of receiving a cocaine shipment during President Zelensky's visit to Argentina for President Milei's inauguration. As evidence, the article cites a YouTube video containing an alleged call between Argentinean drug traffickers and a Medium article describing witness testimonies, both of which have been debunked by Open Fact-Checking. This story was amplified by known overt and covert Russian influence threat actors, including the Russian Ministry of Foreign Affairs editorial "International Affairs", the Intel Drop, as well as German- and English-language domains with ties to the Portal Kombat network previously identified by VIGINUM.[2] [3]

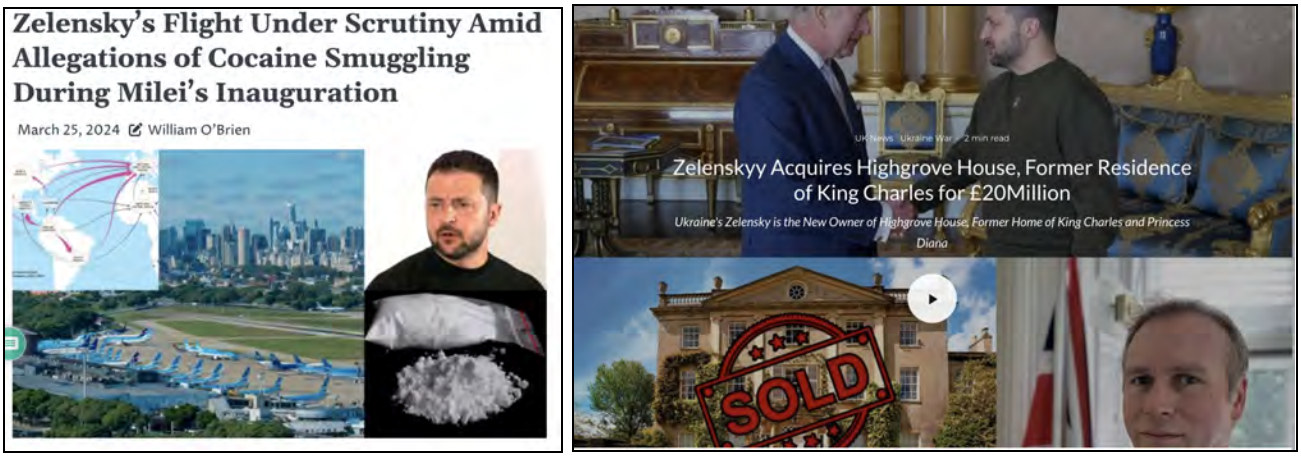


***Figure 10**: Two CopyCop articles targeting Zelensky and amplified by the broader Russian influence ecosystem (Source: Recorded Future)*

Another article published by the inauthentic London Crier website on April 1, 2024, titled "Zelenskyy Acquires Highgrove House, Former Residence of King Charles for £20Million", has been shared by several prominent social media accounts, with one post garnering over 250,000 views in 24 hours. According to research group Antibot4Navalny, the story was reportedly amplified by inauthentic social media accounts with ties to Doppelgänger, as well as Portal Kombat's Pravda websites, and Russian state social media accounts such as the Russian Embassy in South Africa (@EmbassyofRussia).

[2] *https://en.interaffairs[.]ru/article/the-boston-times-zelenskys-flight-under-scrutiny-amid-allegations-of-cocaine-smuggling-during-mi/*
[3] *https://www.theinteldrop[.]org/2024/03/26/zelenskys-flight-smuggled-300-kg-of-cocaine-out-when-the-president-of-ukraine-came-for-argentinas-nazi-leader-mileis-inauguration/*

More Active, More Measured

Since early 2023, Russian covert influence operations have demonstrated an increased focus on accurately measuring impact via engagement metrics. Leaked documents seen by the Washington Post in February 2024 demonstrate the increased emphasis placed by Russian influence threat actors on tracking engagement metrics to communicate their effectiveness to Kremlin decision-makers.

As covered in the **Matomo Tracking** section of this report, CopyCop's domains are tracked by an instance of Matomo, an open-source analytics software. Insikt Group's December 5, 2023, report on Doppelgänger investigated the network's use of the Keitaro Traffic Distribution System (TDS). Adopting open-source or third-party tools like Keitaro and Matomo also signals a shift away from Western providers such as Google Analytics, which sanctioned entities will likely increasingly struggle to acquire or use without detection.

Imitating a Legitimate News Website to Settle Scores

In connection to this network, we uncovered a previously unreported domain impersonating the BBC, *bbc-uk[.]news*. Despite being currently inaccessible, an archive from January 13, 2024, shows that the domain hosted content explicitly imitating the BBC and targeting BBC journalist Mike Wendling, who covered Dougan and DCWeekly for the BBC in December 2023. As mentioned by Wendling in the BBC report, Dougan has a previous history of using fake websites to slander targets, which included Dougan's former employers.

***Figure 11**: CopyCop website imitating the BBC (Source: Wayback Machine)*

Infrastructure Analysis

Insikt Group identified twelve domains connected to *miamichron[.]com* and *dcweekly[.]org.* By investigating domains connected to a Matomo instance hosted at *trk.falconeye[.]tech* and analyzing certificate reuse, we identified three geographically focused clusters (**Table 1**). While most of the infrastructure is hosted on Cloudflare, we identified the underlying server hosting one of the twelve domains, including a server geolocated in Russia.

US Cluster	UK Cluster	France / General Cluster
dcweekly[.]org	*britishchronicle[.]com*	*infoindependants[.]fr*
miamichron[.]com	*gbgeopolitics[.]com*	*clearstory[.]news*
sanfranchron[.]com	*londonchronicles[.]news*	
chicagocrier[.]com	*londoncrier[.]co[.]uk*	
bostontimes[.]org	*bbc-uk[.]news*	

***Table 1**: CopyCop domain names (Source: Recorded Future)*

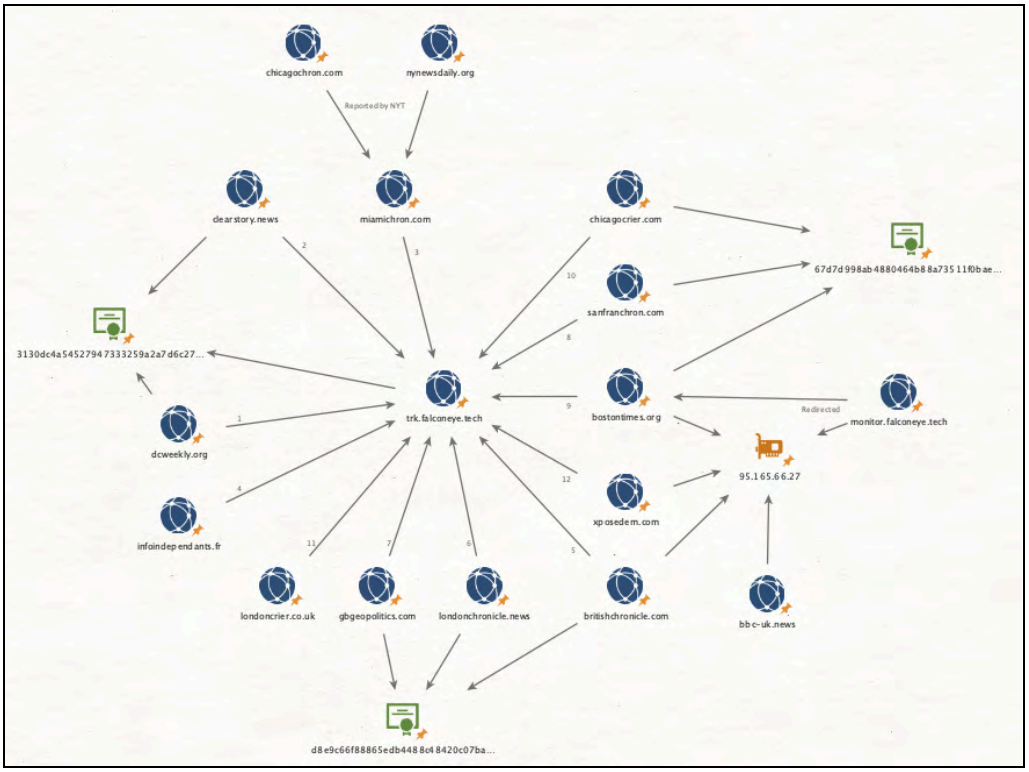


***Figure 12**: Diagram of infrastructure identified by Recorded Future (Source: Recorded Future)*

Cluster Overlap

Across these three subclusters, we identified waves of domain and certificate registrations at similar timings. All domain and certificate registration times are included in **Appendix A**.

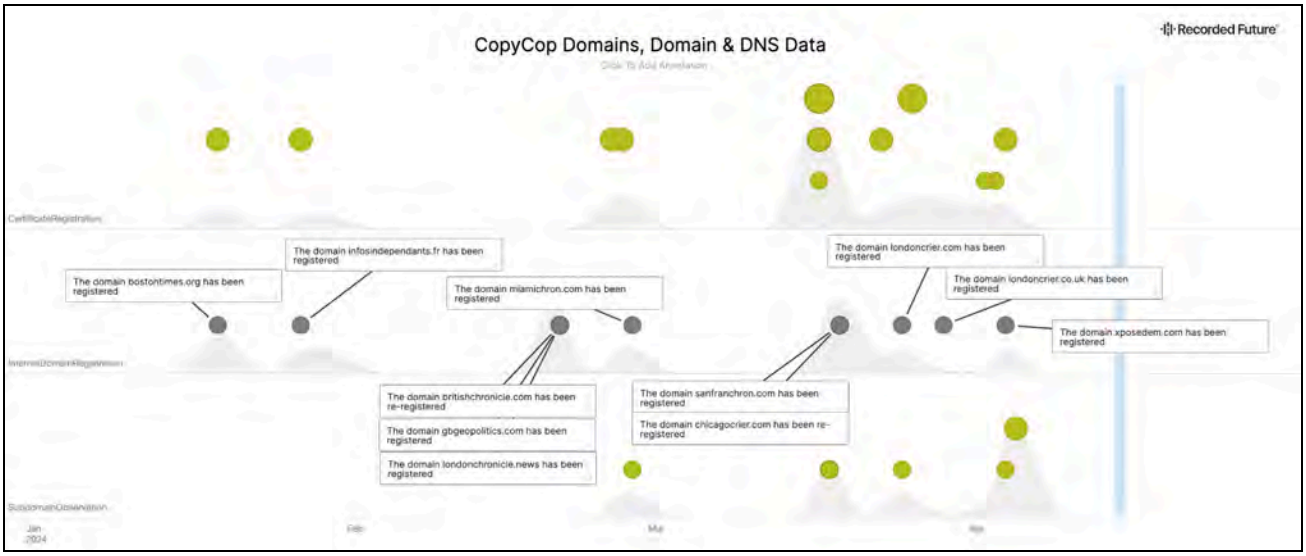


***Figure 13**: Timeline view of domain and certificate registration across subclusters (Source: Recorded Future)*

We identified two domains using identical TLS certificates to the known disinformation domain *dcweekly[.]org*. These domains included the subdomain *trk.falconeye[.]tech*, which is used to host a Matomo tracking instance, as well as one domain associated with the US cluster.

SHA256	3130dc4a54527947333259a2a7d6c2754aa0302555e525f335d8eb97f2382e3c
Domains	*clearstory[.]news*
	dcweekly[.]org
	trk[.]falconeye[.]tech

At the time of analysis, we found that *monitor.falconeye[.]tech* redirected to a previously unidentified domain, *bostontimes[.]org*. Through additional domain analysis, we discovered that this domain shared TLS certificates with two other domains focused on the US and both registered on March 19, 2024:

SHA256	67d7d998ab4880464b88a73511f0bae0a4a4f218f42d363a24379996e90965c5
Domains	*bostontimes[.]org*
	chicagocrier[.]com
	sanfranchron[.]com

In the third wave registered on February 21, 2023, we identified three of these UK-focused domains sharing the same TLS certificate:

SHA256	d8e9c66f88865edb4488c48420c07bab3d39831c58606a97ea395cbc541880c1
Domains	*britishchronicle[.]com*
	gbgeopolitics[.]com
	londonchronicle[.]news

While *britishchronicle[.]com* and *monitor.falconeye[.]tech* are hosted behind Cloudflare, we identified the underlying host as *95.165.66[.]27*. At the time of analysis, the host displayed the HTML title "The Boston Times", further solidifying its connection to the US cluster mentioned earlier.

The server is hosted in Russia by AS25513, which is owned by PJSC's Moscow telephone network. We found that the host had a previous hostname of *bbc-uk[.]news*, almost certainly looking to impersonate the BBC. While this domain is now inactive, URLScan results from December 2023 show that the domain hosted a misconfigured WordPress instance.

Matomo Tracking

Several websites identified by Insikt Group as part of this cluster issue GET and POST requests *trk.falconeye[.]tech*, which hosts an instance of Matomo analytics, an open-source web analytics platform. By enumerating website IDs using Matomo's HTTP application programming interface (API), we were able to determine that this specific Matomo instance is being used to track at least twelve websites. Accessing the *trk.falconeye[.]tech* domain directly reveals a login page for Matomo:

***Figure 14**: Matomo login page on trk.falconeye[.]tech (Source: Recorded Future)*

The website hosted on *miamichron[.]com*, among others, contains a Javascript script loading another Javascript resource from *trk.falconeye[.]tech/matomo.js* and sets a tracker URL as *trk.falconeye[.]tech/matomo.php*.

```
<!-- Matomo -->
<html lang="en-US">
▼<head>
   <script async src="//trk.falconeye.tech/matomo.js"></script>
  ▼<script>
      var _paq = window._paq = window._paq || [];
      /* tracker methods like "setCustomDimension" should be called before "trackPageView" */
      _paq.push(['trackPageView']);
      _paq.push(['enableLinkTracking']);
      (function() {
        var u="//trk.falconeye.tech/";
        _paq.push(['setTrackerUrl', u+'matomo.php']);
        _paq.push(['setSiteId', '3']);
        var d=document, g=d.createElement('script'), s=d.getElementsByTagName('script')[0];
        g.async=true; g.src=u+'matomo.js'; s.parentNode.insertBefore(g,s);
      })();
   </script>
   <!-- End Matomo Code -->
```

***Figure 15**: Matomo Javascript found in miamichron[.]com (Source: Recorded Future)*

After loading the *matomo[.]js* file, the website issues an HTTP request to *matomo[.]php* with tracking information such as a unique visitor ID and site performance metrics; however, the user data field `uadata` remains empty, a likely misconfiguration.

An example URL that the Javascript issues is as follows:

```
https://trk[.]falconeye[.]tech/matomo.php?action_name=The%20Miami%20Chronicle%20%E2%80%93%20Giving%20the%20Florida%20News%20since%201937&idsite=3&rec=1&r=998967&h=1&m=41&s=31&url=https%3A%2F%2Fmiamichron.com%2F&_id=3b75e59bb46e2416&_idn=1&send_image=0&_refts=0&pv_id=DCVpU0&pf_net=0&pf_srv=615&pf_tfr=4&pf_dm1=3598&uadata=%7B%22fullVersionList%22%3A%5B%5D%2C%22mobile%22%3Afalse%2C%22model%22%3A%22%22%2C%22platform%22%3A%22%22%2C%22platformVersion%22%3A%22%22%7D&pdf=1&qt=0&realp=0&wma=0&fla=0&java=0&ag=0&cookie=1&res=1600x1200
```

The HTTP request also contains an `idsite` parameter, which, according to Matomo's Tracking API documentation, represents the ID of a website tracked by Matomo. Successful requests with a valid `idsite` value return a `204` status code, while invalid `idsite` values return a `400`. Using this method, we could enumerate `idsite` values between one and twelve, indicating that the Matomo instance is likely tracking twelve domains as of April 2024.

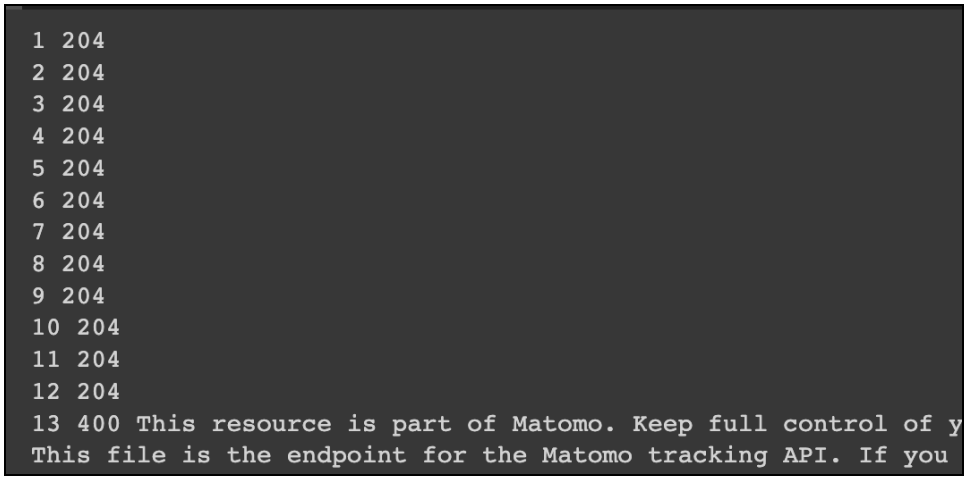


***Figure 16**: GET request responses to Matomo's Tracking API on trk.falconeye[.]tech (Source: Recorded Future)*

By analyzing requests between CopyCop websites and the Matomo server, we enumerated all domains and their connected IDs, which we include in **Appendix C**.

Self-Hosted Video-Sharing Platform

On or around March 31, 2024, *monitor.falconeye[.]tech* began directing visitors to a self-hosted video-sharing platform titled "Video Vista" using MediaCMS, an open-source video platform. As of early April 2024, the platform began hosting videos from Dougan's YouTube channel "ExposedUS" (under the moniker "BadVolf"), pirated movies, and Russian-language content. One account, "Masha"[4], is likely tied to Maria Leylavona, Dougan's translator. It remains unclear whether this channel will be used as a fallback if Dougan's YouTube channel gets de-platformed or whether it will be used for publishing CopyCop content.

XposedEm Forum

From April 4, 2024 onwards, *xposedem[.]com* was hosted on the same server geolocated in Russia as other CopyCop websites and used CopyCop's Matomo instance. The domain hosts a Discourse forum named "XposedEm", which claims to be "Exposing Hipocrisy [sic] US Government, Immune to US Subpoena and FBI". As of April 5, 2024, the forum has three active users: "System"[5], "BadVolf" (Dougan's handle), and "BlackWidow" (listing *nikk1ann@yandex[.]com* as the account email address). We were unable to identify any open–source references to the associated email address.

[4] *https://monitor.falconeye[.]tech/user/Masha/*
[5] *https://xposedem[.]com/u/system/summary*

Attribution

We assess that the CopyCop network is very likely operated from Russia and is aligned with the Russian government. Additionally, we assess that there is a realistic possibility that the network receives strategy, support, or oversight from Russian government entities and the broader Russian influence apparatus. Using NATO StratCom's influence operations (IO) attribution framework, the following factors support this attribution:

Technical evidence:

- Several CopyCop domains are hosted on Russian infrastructure, and they have overlapping TLS certificates, demonstrating they belong to a single network.
- Twelve domains also communicate with a single Matomo analytics instance to measure traffic, similar to Doppelgänger's use of Keitaro.

Behavioral evidence:

- Inauthentic CopyCop websites have amplified assets connected to Russian intelligence (InfoRos/GRU Unit 54777) and Prigozhin-owned assets (FBI/FBR).
- Russian influence threat actors — both overt (Russian state social media accounts, state-sponsored media organizations) and covert (Portal Kombat, Doppelgänger) — have amplified CopyCop websites.

Contextual evidence:

- Dougan is a known influence threat actor, having operated in the interests of the Russian government since at least 2016.
- Narratives promoted by the network align with Russian influence objectives, such as undermining Western domestic and foreign policy, attempting to sow distrust between governments, and eroding military support for Ukraine.
- CopyCop's activity is temporally situated within a larger push from Russian covert influence operations in the last six months, including networks like Doppelgänger and Portal Kombat.

Overlap with previous reporting:

- Our research builds on top of original reporting by Clemson University researchers, which was further covered by the New York Times, which cited similar assessments made by US government officials.
- Aspects of CopyCop have been described as connected to Russian influence operations by many security researchers, such as its amplification by inauthentic Doppelgänger accounts and the Zelensky cocaine smuggling story.

Mitigations

- AI content production coupled with automated publication via WordPress helps CopyCop multiply its content volume. Defenders can use the Recorded Future Intelligence Cloud and Recorded Future AI to summarize and track emerging narratives across all CopyCop websites.
- Organizations involved in election security should raise awareness about AI-generated news articles on websites imitating legitimate news organizations and educate audiences on recognizing LLM prompts or other markers of AI-generated content.
- News organizations should track content from known influence threat actors who are likely plagiarizing and weaponizing proprietary content and intellectual property, which increases reputational risks.
- Media organizations can use Recorded Future Brand Intelligence to track and combat typosquatting domains and infringing content on similar domains.

Outlook

On March 19, 2024, Insikt Group released findings from an internal red team exercise using AI to generate disinformation content, among other malicious use cases. One of our findings was that AI content production will likely enable influence networks to scale and tailor content production to specific audiences. As our report was being published, CopyCop was already operationalizing this concept and being amplified by the wider Russian disinformation apparatus. Given the recent growth in engagement with their content on social media platforms, CopyCop operators have likely demonstrated the viability of AI-generated disinformation at scale, despite many OPSEC mistakes and leaving the original LLM prompts in published content.

Russian state-sponsored entities amplifying the network's targeted, human-produced content suggests that hybrid models between high volumes of AI-generated content and targeted human content will likely be adopted in the future. Recent additions to CopyCop infrastructure, including open-source video-sharing platforms and a forum named XposedEm, indicate the network's growing ambitions.

If CopyCop succeeds in building engagement and staying persistent, other influence operations and networks will likely follow this model in the near future. AI-enabled influence networks will likely increase challenges for public and private organizations to monitor and defend elections and other democratic processes from foreign malign influence. Additionally, these networks will increase brand and reputational risk for legitimate media organizations.

Appendix A: Indicators of Compromise (IoCs)

```
Domains

dcweekly[.]org
clearstory[.]news
miamichron[.]com
infosindependants[.]fr
britishchronicle[.]com
londonchronicle[.]news
gbgeopolitics[.]com
sanfranchron[.]com
bostontimes[.]org
chicagocrier[.]com
londoncrier[.]com
londoncrier[.]co.uk
xposedem[.]com
bbc-uk[.]news

IPs

95.165.66[.]27

Certificates

3130dc4a54527947333259a2a7d6c2754aa0302555e525f335d8eb97f2382e3c
67d7d998ab4880464b88a73511f0bae0a4a4f218f42d363a24379996e90965c5
d8e9c66f88865edb4488c48420c07bab3d39831c58606a97ea395cbc541880c1
```

Appendix B: Domain and Certificate Registrations

Date	Event Type	Domain
2024-01-19	New Certificate Registrations	bostontimes[.]org
	New Domain Registrations	bostontimes[.]org
2024-01-27	New Certificate Registrations	infosindependants[.]fr
		www[.]infosindependants[.]fr
	New Domain Registrations	infosindependants[.]fr
2024-02-21	New Domain Registrations	gbgeopolitics[.]com
		londonchronicle[.]news
2024-02-22	Domain Re-registrations	britishchronicle[.]com
2024-02-26	New Certificate Registrations	miamichron[.]com
		www[.]miamichron[.]com
2024-02-27	New Certificate Registrations	miamichron[.]com
		www[.]miamichron[.]com
2024-02-28	New Domain Registrations	miamichron[.]com
	Subdomain Observations	www[.]gbgeopolitics[.]com
2024-03-17	New Certificate Registrations	a[.]miamichron[.]com
		gbgeopolitics[.]com
		londonchronicle[.]news
		sanfranchron[.]com
		www[.]bostontimes[.]org
		www[.]gbgeopolitics[.]com
		www[.]londonchronicle[.]news
		www[.]sanfranchron[.]com
2024-03-18	Subdomain Observations	a[.]miamichron[.]com
		www[.]sanfranchron[.]com

2024-03-19	New Domain Registrations	sanfranchron[.]com
2024-03-20	Domain Re-registrations	chicagocrier[.]com
2024-03-23	New Certificate Registrations	londoncrier[.]com
		www[.]londoncrier[.]com
2024-03-25	New Domain Registrations	londoncrier[.]com
	Subdomain Observations	www[.]londoncrier[.]com
2024-03-26	New Certificate Registrations	londoncrier[.]co[.]uk
		www[.]londoncrier[.]co[.]uk
2024-03-27	New Certificate Registrations	www[.]londoncrier[.]co[.]uk
2024-03-29	New Domain Registrations	londoncrier[.]co[.]uk
2024-04-03	New Certificate Registrations	disc[.]xposedem[.]com
		xposedem[.]com
2024-04-04	New Certificate Registrations	autoconfig[.]xposedem[.]com
	New Domain Registrations	xposedem[.]com
	Subdomain Observations	www[.]xposedem[.]com
2024-04-05	New Certificate Registrations	autoconfig[.]xposedem[.]com
	Subdomain Observations	autodiscover[.]xposedem[.]com
		disc[.]xposedem[.]com

Appendix C: CopyCop Domains and Matomo IDs

Domain	Matomo Tracking API ID
dcweekly[.]org	1
clearstory[.]news	2
miamichron[.]com	3
infosindependants[.]fr	4
britishchronicle[.]com	5
londonchronicle[.]news	6
gbgeopolitics[.]com	7
sanfranchron[.]com	8
bostontimes[.]org	9
chicagocrier[.]com	10
londoncrier[.]com (now redirecting to *londoncrier[.]co.uk*)	11
xposedem[.]com	12

Recorded Future®

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com