CYBER THREAT ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

June 24, 2024

Russia-Linked CopyCop Expands to Cover US Elections, Target Political Leaders

CopyCop is a Russian-linked influence network using generative AI to plagiarize and weaponize mainstream news articles with pro-Russia narratives.

Since our initial report, the influence network has expanded to over 120 new websites using AI-generated branding and fake journalist profiles, now focusing on the 2024 US elections.

CopyCop continues publishing content targeting EU and Ukrainian political leaders using deepfakes and AI-generated audio.

Executive Summary

On May 9, 2024, Insikt Group published an initial report on CopyCop, a likely Russian government-aligned influence network using inauthentic websites and generative artificial intelligence (AI) to create and spread political content at scale. Between May 10 and May 12, 2024, the network registered 120 new websites using similar tactics, techniques, and procedures (TTPs). CopyCop has also shifted its influence content production and dissemination to primarily focus on the 2024 United States (US) presidential election. We also observed the dissemination of targeted content using YouTube videos aimed at political leaders in France, Ukraine, and the European Union (EU). The videos are likely digitally manipulated and likely use AI-generated faces and voices.

The network has also begun plagiarizing influence content from a broader range of news sources, including mainstream news outlets in the US and United Kingdom (UK), conservative-leaning US media, and Russian state-affiliated media. Within 24 hours of articles from these sources first being posted, the CopyCop network scrapes, weaponizes, and disseminates modified articles to US election-themed inauthentic websites using over 1,000 fake journalist personas. In the future, media organizations risk having content manipulated and reuploaded by malicious actors at increasingly shorter intervals. However, such AI-generated content is unlikely to have as much impact on the elections as targeted content.

CopyCop's operators, suspected to include John Mark Dougan, a US citizen and fugitive based in Russia, have likely reacted to recent industry and media reporting on the network. Infrastructure changes in US-based hosts likely indicate a desire to minimize connections to the Russian government. Fewer traces of generative AI use also demonstrate an intent to obfuscate the network's use of large language models (LLMs). Our attribution of CopyCop as a likely Russian government-aligned influence network located in Russia remains unchanged.

AI-generated influence content allows influence actors like CopyCop to rapidly launder emerging narratives targeting the 2024 US elections and obscure their origin, making it harder to attribute influence operations to foreign adversaries. Insikt Group used generative AI extensively to analyze this network, demonstrating how the technology can enable analysts and election defenders to process increasingly large amounts of influence content, extract narratives, and draw analytical conclusions. As coordinated inauthentic behavior (CIB) networks continue to evolve tactics and targets, persistently identifying and publicly exposing these networks ahead of the 2024 US elections should remain a priority for public and industry organizations.

Key Findings

- CopyCop's AI-generated content has shifted to focus on covering the 2024 US elections, with significantly less coverage of other topics, including Russia's war against Ukraine, and French and UK domestic politics.
- CopyCop's sole new French-themed website, *mediaalternatif[.]fr*, began publishing targeted, likely human-crafted influence content in late May 2024, targeting the French government and First Lady of Ukraine Olena Zelenska.
- Another website, *houstonpost[.]org*, published human-crafted content targeting EU Commission president Ursula von der Leyen. We assess that both websites publish YouTube videos from the same influence actor.
- The CopyCop network continues to amplify content from the Foundation to Battle Injustice, a known Russian influence front. Known Russian influence networks, such as the "Info Defense" Telegram network and Reliable Recent News, an inauthentic media outlet with ties to Russian influence network Doppelgänger, continue to amplify CopyCop's targeted content.
- As of early June 2024, except for the new French-themed website, CopyCop's AI-generated content has seen little to no amplification on social media.
- CopyCop has expanded its sources for plagiarized content to mostly conservative-leaning US sources (Breitbart, New York Post, Washington Examiner), outlets previously accused of spreading false information (The Epoch Times, Zero Hedge), and state-owned or state-aligned Russian media (Gazeta[.]ru, TASS, RT).
- The network has expanded its use of generative AI to create inauthentic journalist personas at scale. We found over 1,000 distinct author profiles and descriptions across the 120 new websites.
- We also found evidence of LLM-generated text in CopyCop article headlines, which included numbered "Special Report" strings, indicating continued use of automation and generative AI.

Table of Contents

Narratives

CopyCop previously focused heavily on laundering Russian narratives surrounding Russia's war against Ukraine, criticizing US, UK, and French leadership, and emphasizing polarizing domestic issues in these countries. Since CopyCop's shift in infrastructure, the network has narrowed its narrative scope, focusing instead on US politics ahead of the 2024 US elections.

As of early June 2024, these new websites publishing AI-generated content have seen limited amplification on social media. However, we assess that CopyCop will likely begin introducing targeted, likely human-crafted narratives with rich media (such as YouTube videos) targeting the 2024 US elections, as mentioned in our previous report and according to Microsoft and the New York Times' findings. CopyCop's new French-language website, *mediaalternatif[.]fr*, has published two human-crafted articles — one containing a YouTube video and resembling Storm-1516's tactics, as described by Microsoft, and the other publishing a translated version of a Foundation to Battle Injustice (FBR/FBI) article, a known Russian influence front previously amplified by CopyCop (see Amplification of the FBR/FBI).

As of late May 2024, former US president Donald Trump and President Joe Biden are by far the most frequently mentioned people by CopyCop (**Figure 1**). The network covers the US election candidates orders of magnitude more frequently than previous targets, such as French President Emmanuel Macron (cited 155 times, about 47 times less often than Trump and 21 times less frequently than President Biden).

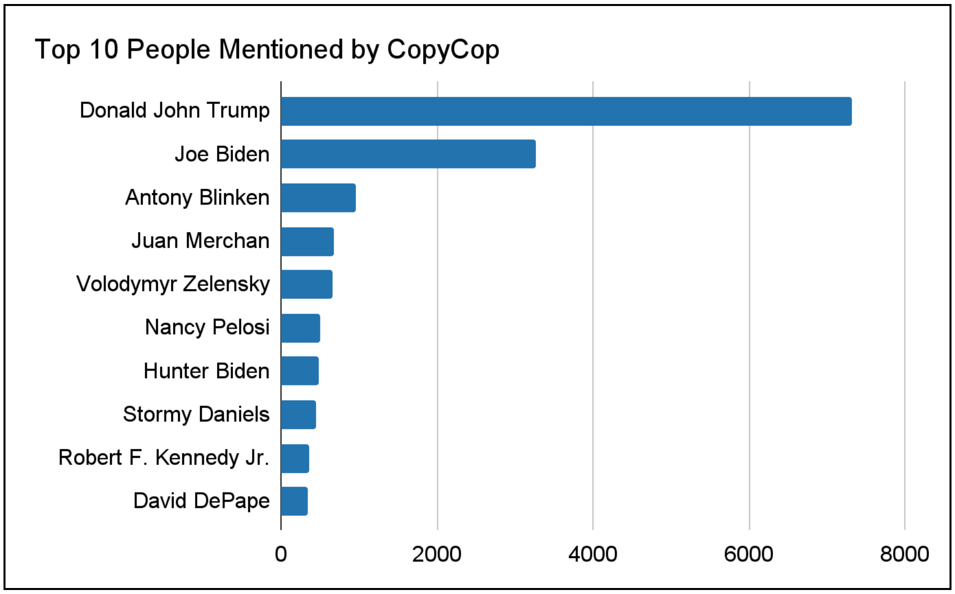


***Figure 1**: Top ten people mentioned by CopyCop (Source: Recorded Future)*

CopyCop content continues to denigrate President Biden and Democratic policymakers. For example, it highlights mistakes President Biden made during speeches and his age (original, CopyCop), criticizes the Biden administration's failure to curb inflation (original, CopyCop), and covers recent negative poll sentiment on the Democratic Party (original, CopyCop).

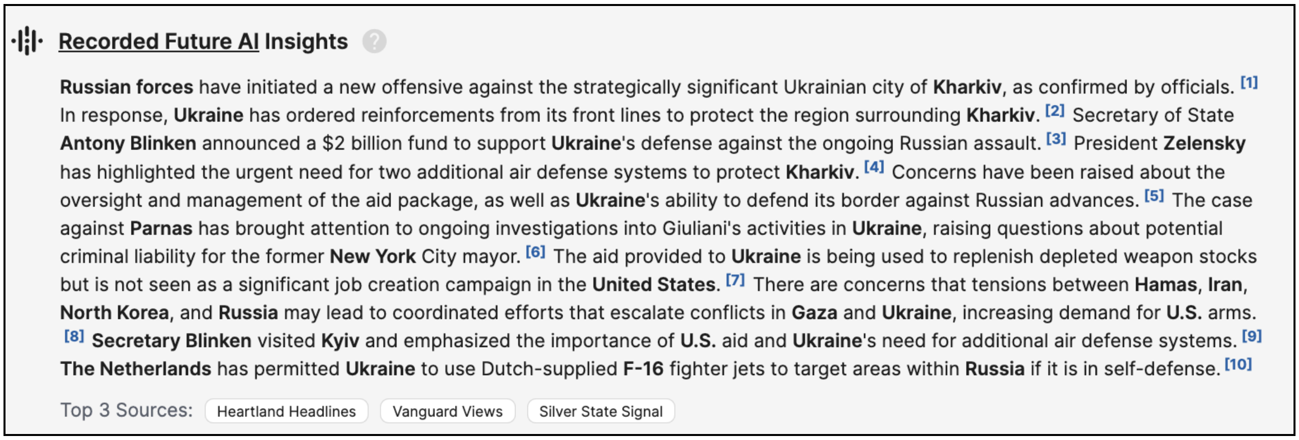
The network also consistently covers the Republican Party and Donald Trump. In May 2024, CopyCop extensively covered Trump's hush-money trial and subsequent conviction, for example, downplaying Trump's conviction as being "impactless" on the elections (original, CopyCop), covering Speaker Mike Johnson's appeal to the Supreme Court to overturn the verdict (original, CopyCop), and referring to the trial as a "well-choreographed mess" (original, CopyCop).

Despite being a lesser focus, Ukraine remains a target of the network, although increasingly through the lens of US politics or major news of North Atlantic Treaty Organization (NATO) allies providing funding and military support to Ukraine (original, CopyCop). Common narratives highlight corruption in the Ukrainian government (original, CopyCop), attempt to debunk Western portrayals of Zelensky as a "hero", decry a "Vietnamization" of the Russia-Ukraine conflict (original, CopyCop), and cover Russian military operations in Ukraine.

The network's coverage of French domestic politics and President Emmanuel Macron continues. CopyCop's previous French-themed website (*infoindependants[.]fr*) has been offline since the release of our initial report. French coverage is now distributed among US-themed websites and one new French-themed website, *mediaalternatif[.]fr* (see Targeted Content). US-themed websites focused heavily on the riots in the French island territory of New Caledonia in May 2024, claiming that Macron's May 23, 2024, visit did not help quell the protests (original, CopyCop)

UK-specific coverage has dwindled since the publication of our initial report, with only one new website being explicitly UK-themed (see New UK-Themed Domain). Previous UK-themed websites are now offline (*gbgeopolitics[.]com*, *britishchronicle[.]com*, *londoncrier[.]news*) or mirror the Boston Times (*londoncrier[.]uk*, see Mirror Websites).

Recorded Future's AI Insights were used extensively to analyze narratives in CopyCop websites for this report. By combining specific queries for entities in Recorded Future's Advanced Query Builder across CopyCop sources, we rapidly narrowed down relevant content, received a summary, and identified specific article URLs feeding each of the narratives captured by the AI insights. Generative AI is an increasingly crucial tool for analysts investigating large volumes of AI-generated influence content.



Recorded Future AI Insights

Russian forces have initiated a new offensive against the strategically significant Ukrainian city of **Kharkiv**, as confirmed by officials. [1] In response, **Ukraine** has ordered reinforcements from its front lines to protect the region surrounding **Kharkiv**. [2] Secretary of State **Antony Blinken** announced a $2 billion fund to support **Ukraine**'s defense against the ongoing Russian assault. [3] President **Zelensky** has highlighted the urgent need for two additional air defense systems to protect **Kharkiv**. [4] Concerns have been raised about the oversight and management of the aid package, as well as **Ukraine**'s ability to defend its border against Russian advances. [5] The case against **Parnas** has brought attention to ongoing investigations into Giuliani's activities in **Ukraine**, raising questions about potential criminal liability for the former **New York** City mayor. [6] The aid provided to **Ukraine** is being used to replenish depleted weapon stocks but is not seen as a significant job creation campaign in the **United States**. [7] There are concerns that tensions between **Hamas**, **Iran**, **North Korea**, and **Russia** may lead to coordinated efforts that escalate conflicts in **Gaza** and **Ukraine**, increasing demand for **U.S.** arms. [8] **Secretary Blinken** visited **Kyiv** and emphasized the importance of **U.S.** aid and **Ukraine**'s need for additional air defense systems. [9] **The Netherlands** has permitted **Ukraine** to use Dutch-supplied **F-16** fighter jets to target areas within **Russia** if it is in self-defense. [10]

Top 3 Sources: Heartland Headlines | Vanguard Views | Silver State Signal

***Figure 2**: Recorded Future AI Insights summarizing CopyCop articles related to Ukraine (Source: Recorded Future)*

New Infrastructure

Following the publication of our earlier report on May 9, 2024, we identified 120 domain names tied to new CopyCop websites, nearly all of which were registered between May 10 and May 12, 2024 (**Figure 3**).

We identified these new domains by comparing domain registration patterns consistent with CopyCop's previous registrations on Cloudflare, and pivoting using reused image file paths, betraying identical influence content production across different CopyCop websites. The network has also shifted to US-based hosts for CopyCop's new websites, which is likely an attempt to minimize the network's connections to Russian infrastructure — although we did observe one new UK-themed domain hosted on Russian infrastructure identified in our previous report.

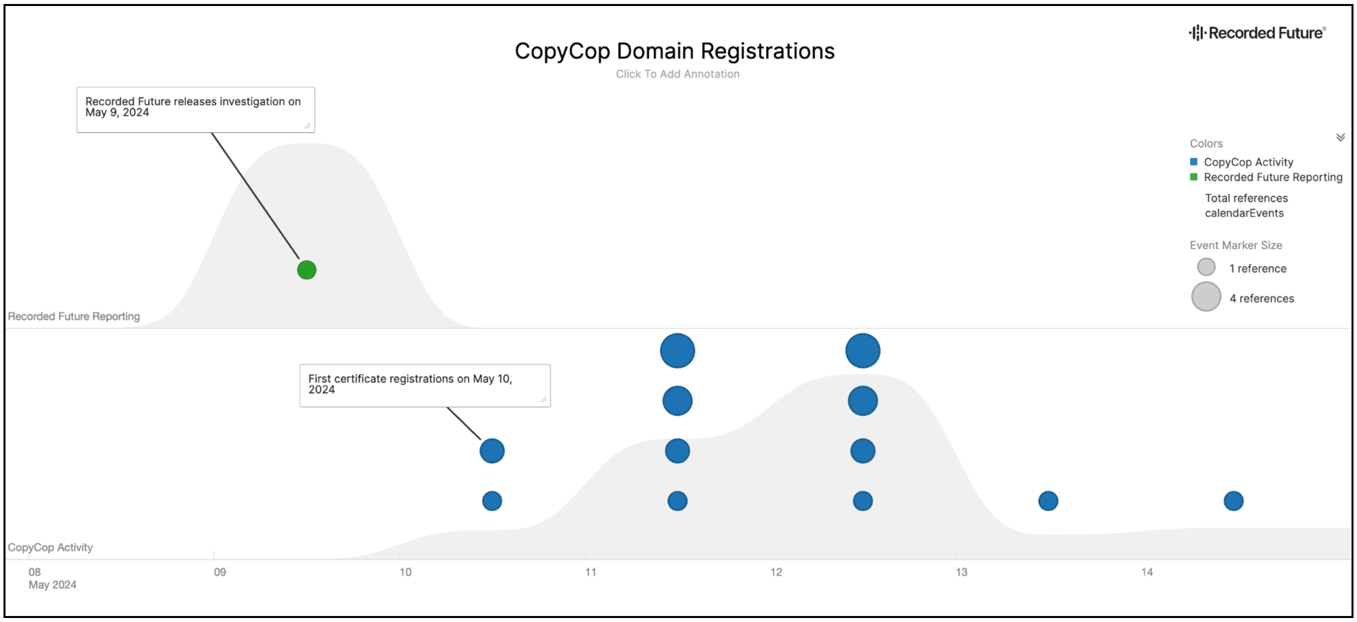


***Figure 3**: Timeline view of CopyCop's new domain registrations following Recorded Future's May 9, 2024 report (Source: Recorded Future)*

Unlike the network's first iteration of inauthentic websites, these new websites are not using CopyCop's Matomo instance, which we assessed the network was likely using to measure incoming traffic to CopyCop websites. As the Matomo instance was a strong pivot in our initial investigation after enumerating CopyCop websites on its application programming interface (API), CopyCop operators have likely stopped using the instance on new websites as an operational security measure, therefore losing their granular visibility over traffic statistics for their new websites.

Image Reuse

In our original report, we outlined one of CopyCop's main TTPs as plagiarizing articles from news outlets, which we initially identified via image filenames containing the headline of the plagiarized article. We have observed continued significant overlap in the content and specific image filenames shared by the original and newly identified CopyCop websites (**Figure 4**).

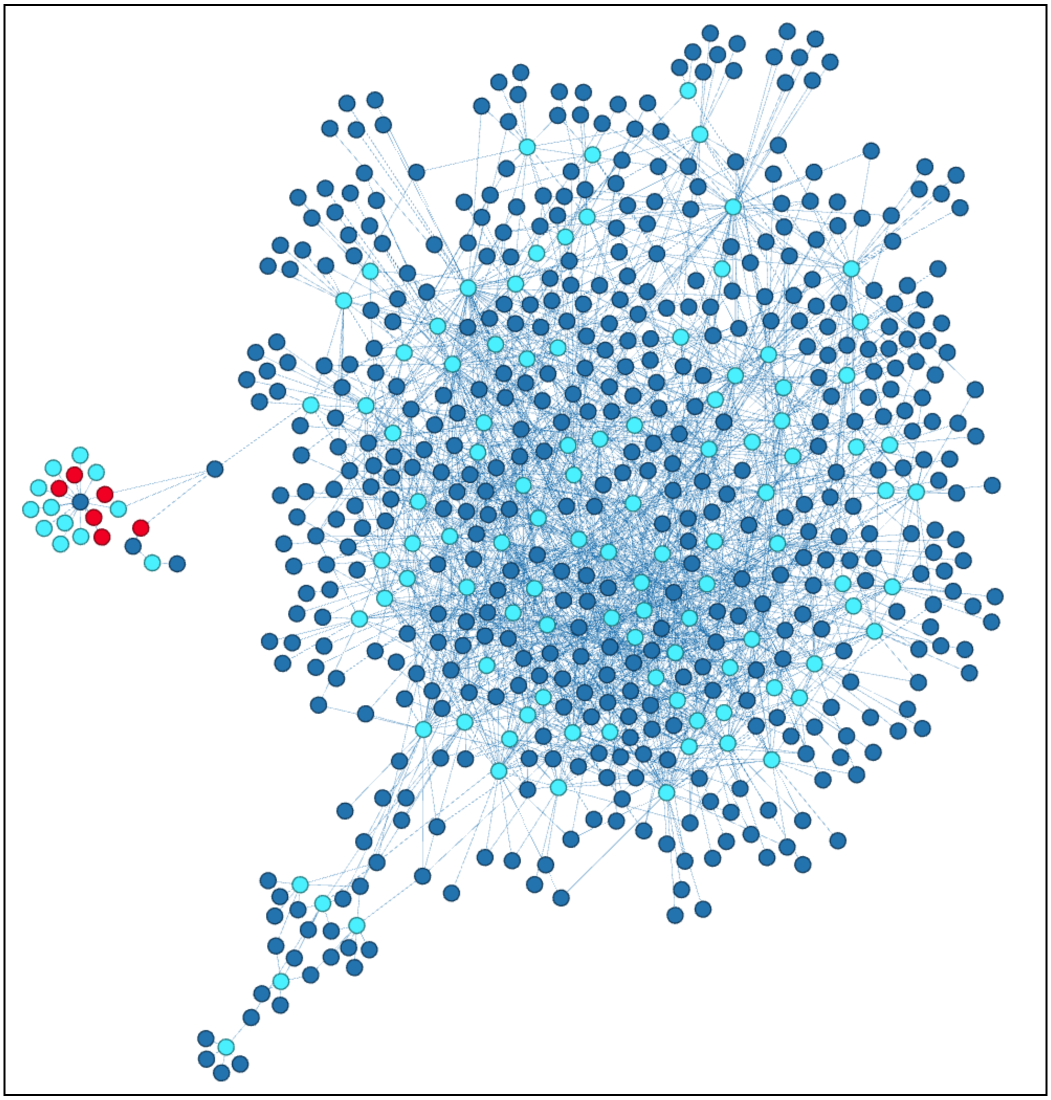


Figure 4*: Network of CopyCop's original domains (red), new domains (light blue), and image file paths (dark blue), demonstrating filename reuse across a majority of the new websites (Source: Recorded Future)*

For example, *flyoverbeacon[.]com* and *harrisburg-chronicle[.]com* both uploaded images using the following highly specific filename (**Figure 5**):

```
2024/05/Sen-Cornyn-Forewarns-of-Terror-Threat-on-US-Soil-as-ISIS-Linked-Network
-Confirmed-at-Southern-Border-1331-332x221.jpg
```

As outlined in our original report, image filenames typically betray the article being plagiarized by CopyCop; in this case, the plagiarized article is almost certainly a May 16, 2024 article by the Epoch Times titled “Sen. Cornyn Forewarns of Terror Threat on US Soil as ISIS-Linked Network Confirmed at Southern Border”. The article was then scraped, weaponized, and disseminated with different article titles (1, 2) and body text within 24 hours on May 17, 2024, demonstrating continued attention to maintaining high operational tempo (**Figure 6**).

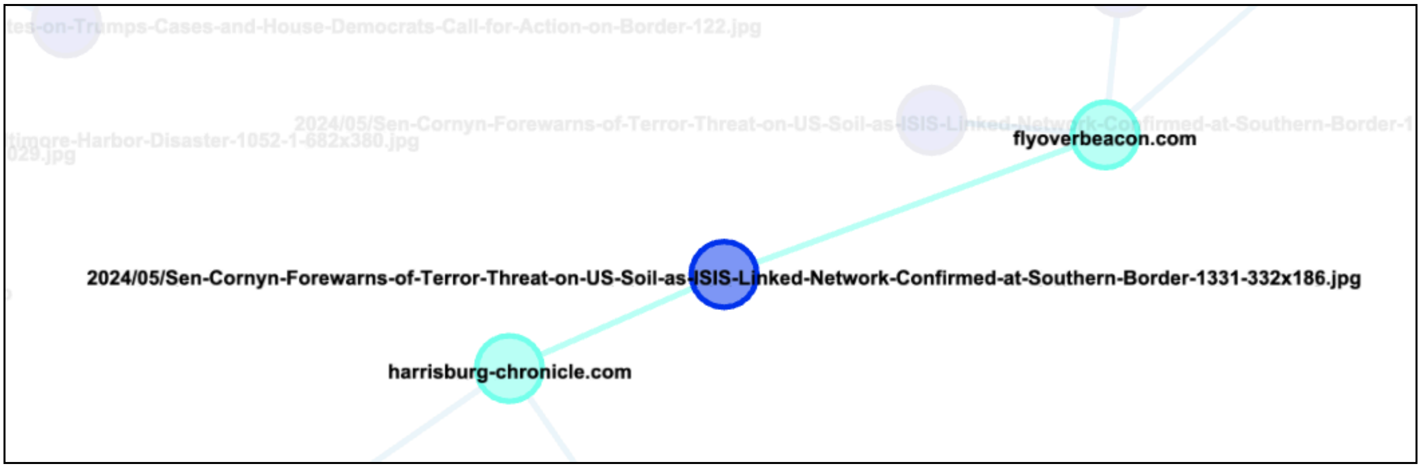
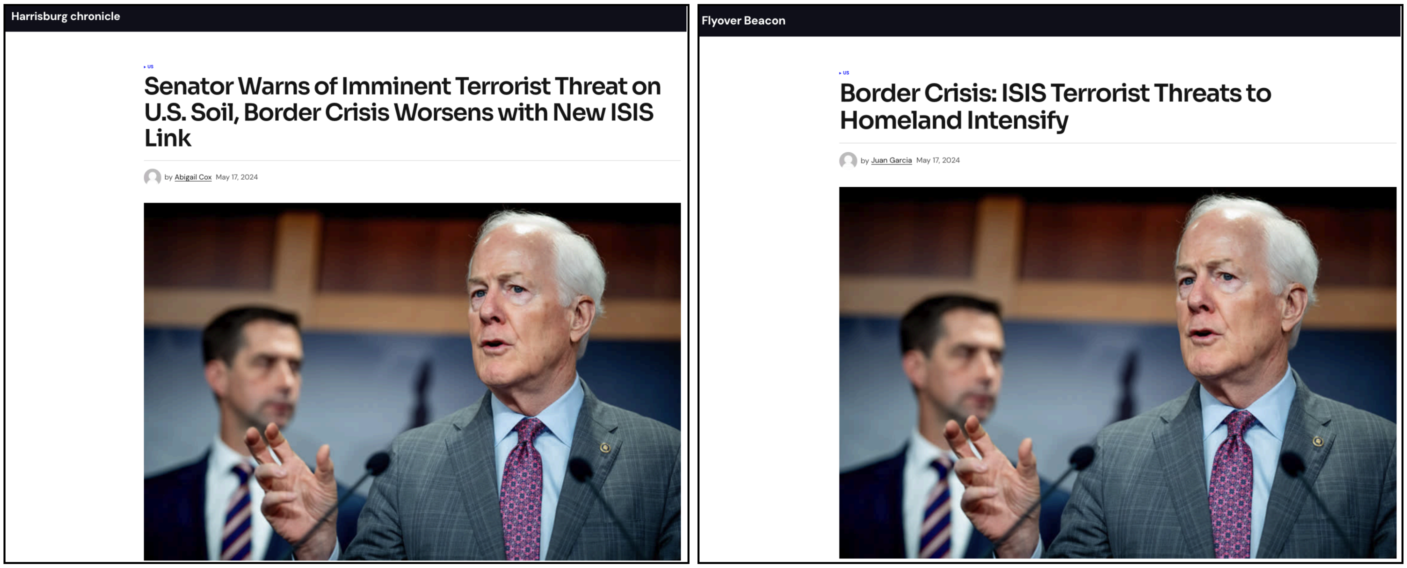

tes-on-Trumps-Cases-and-House-Democrats-Call-for-Action-on-Border-122.jpg
2024/05/Sen-Cornyn-Forewarns-of-Terror-Threat-on-US-Soil-as-ISIS-Linked-Network-Confirmed-at-Southern-Border-1
timore-Harbor-Disaster-1052-1-682x380.jpg
029.jpg
flyoverbeacon.com
2024/05/Sen-Cornyn-Forewarns-of-Terror-Threat-on-US-Soil-as-ISIS-Linked-Network-Confirmed-at-Southern-Border-1331-332x186.jpg
harrisburg-chronicle.com

Figure 5*: Example overlap between flyoverbeacon[.]com and harrisburg-chronicle[.]com (Source: Recorded Future)*



Harrisburg chronicle

US

Senator Warns of Imminent Terrorist Threat on U.S. Soil, Border Crisis Worsens with New ISIS Link

by Abigail Cox May 17, 2024

Flyover Beacon

US

Border Crisis: ISIS Terrorist Threats to Homeland Intensify

by Juan Garcia May 17, 2024

Figure 6*: Distinct CopyCop articles reusing the same image but with different article titles and body text (Source: CopyCop 1, 2)*

Pivoting to US Infrastructure

Recorded Future identified a distinct change in the infrastructure used to host CopyCop websites previously hosted in Russia. It is likely hosting its new websites on the following DigitalOcean servers geolocated in the US, indicating an increased focus on minimizing the operator's connections to Russia:

```
64.23.205[.]22
64.23.205[.]28
68.183.52[.]78
68.183.62[.]128
146.190.63[.]177
174.138.81[.]171
174.138.94[.]129
```

US Election-Themed Domains

While we identified new CopyCop websites with domains following similar naming conventions to those identified initially (including domains impersonating defunct US news outlets), new websites are broadly themed around the US elections, with clusters of domain names with a specific focus on conservative or political keywords like "conservative", "republic", "policy", "right", "patriotic", and "red":

conservativecamp[.]org conservativecatch[.]org conservativechannel[.]org conservativecircuit[.]com conservativecompass[.]org conservativecontext[.]com conservativecorridor[.]com conservativecourier[.]org	republicrally[.]com republicrange[.]com republicregard[.]com republicreview[.]net republicripple[.]com republicroot[.]com republicroots[.]org republicrundown[.]com	policypaddock[.]com policypassage[.]com policypatch[.]com policypath[.]org policypeak[.]org policyplatform[.]info policyporch[.]org
rightrealm[.]net rightresonance[.]org rightreview[.]org rightrevival[.]org rightrundown[.]com rightwingrev[.]com	patrioticpage[.]com patrioticparade[.]com patrioticpioneer[.]com patrioticpulse[.]info	purplestatepost[.]com red-blue-tribune[.]com redstategazette[.]com redstatereport[.]net

New UK-Themed Website

We also observed one new UK-themed website, *ukpoliticking[.]com,* initially identified by Bellingcat. The domain shares content with other UK-themed domains in our previous report, such as *gbgeopolitics[.]com* and *londoncrier[.]news*. According to Bellingcat, the domain was shared in a now-deleted post by John Mark Dougan on his Telegram channel, *t[.]me/BadVolfNews*. The domain also has overlapping content with one of CopyCop's previous domains, *gbgeopolitics[.]com*.

This domain is hosted on the same Russian IP address as previously reported, *95.165.66[.]27*. The website uses many of the same sources and techniques as other UK-themed websites, including republishing content from Sky News.

Mirror Websites

Recorded Future also identified at least eight new domains being used as mirror websites for the Boston Times (*bostontimes[.]org*), an inauthentic publication detailed in our last report:

```
michigantribune[.]org
patriotbeacon[.]us
georgiagazette[.]us
nevadaannouncer[.]com
heartlandherald[.]us
northcarolinacourier[.]us
proudamerican[.]cc
rightwingrev[.]com
```

Tactics, Techniques, and Procedures (TTPs)

The Kompromat Laundromat

CopyCop websites likely scrape articles from legitimate news organizations to plagiarize them using generative AI. In the first iteration of this report, we identified content sourced from Fox News, Al Jazeera, Gazeta.ru, La Croix, and TV5Monde.

New CopyCop websites are now sourcing articles from a broader range of news organizations, with US-themed websites' articles being primarily sourced from US conservative-leaning news sources, including:[1]

- Breitbart (original, CopyCop)
- BizPacReview (original, CopyCop)
- Conservative Brief (original, CopyCop)
- The Epoch Times (original, CopyCop)
- New York Post (original, CopyCop)
- Washington Examiner (original, CopyCop)
- Zero Hedge (original, CopyCop)

CopyCop websites are also continuing to launder content from Russian state-affiliated or state-aligned media organizations:

- Gazeta.ru (original, CopyCop)
- RT (original, CopyCop)
- TASS (original, CopyCop)

CopyCop's French and UK-themed websites mostly plagiarize mainstream media, such as Sky News (original, CopyCop), Sky Sports (original, CopyCop), the Daily Mail (original, CopyCop), Le Parisien (original, CopyCop), and Le Figaro (original, CopyCop).

CopyCop operators are also likely providing a second layer of information laundering for media outlets that propagate influence content targeting the US. The Epoch Times, for example, is tied to Falun Gong, which uses the English-language news outlet to criticize the Chinese Communist Party (CCP), spread COVID-19 misinformation, and promote pro-Trump content. Zero Hedge has also been previously accused of amplifying Russian propaganda and spreading COVID-19 misinformation. We also saw occasional use of content from Global Times (original, CopyCop), a Chinese state-owned media outlet frequently engaging in overt influence operations targeting the US.

[1] Recorded Future describes these publications' political leanings according to the following sources: Media Bias Ratings | AllSides, Media Bias/Fact Check.

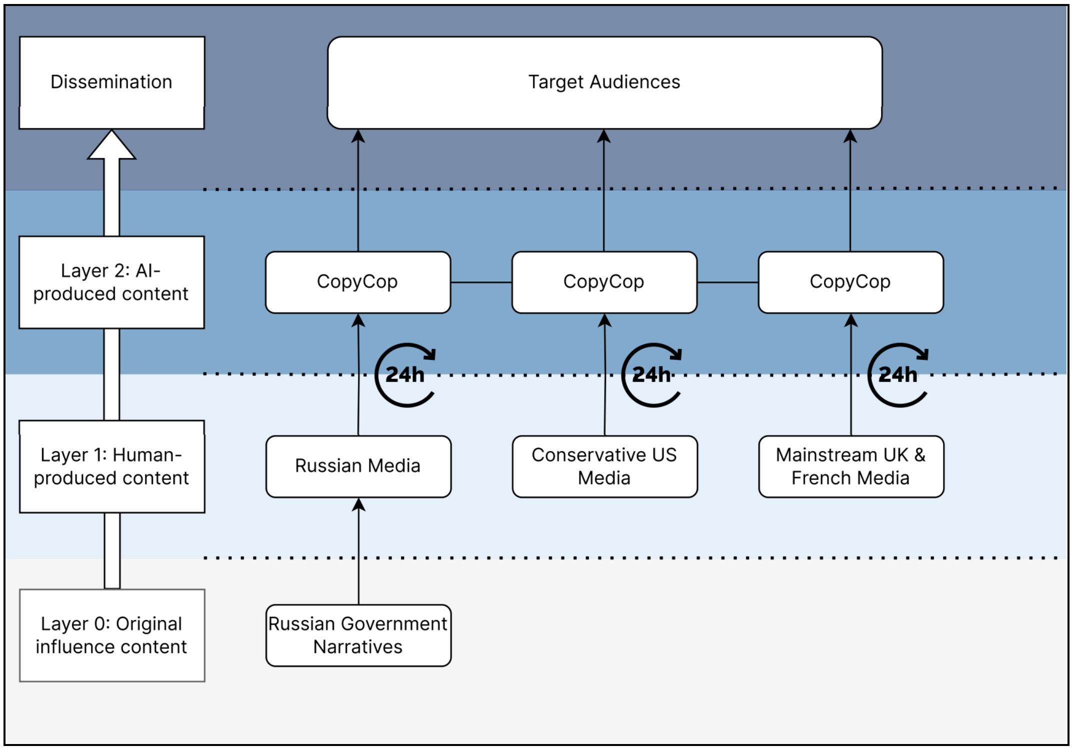
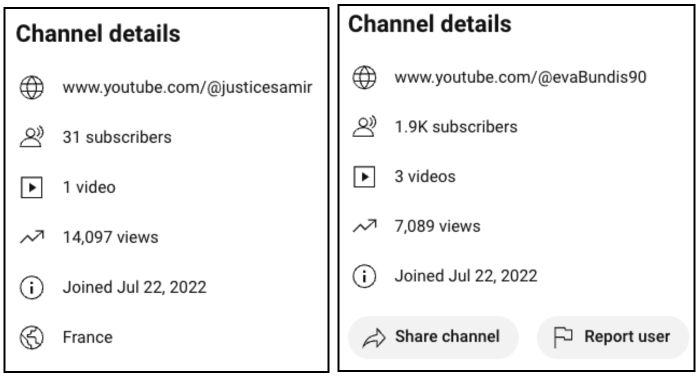

Dissemination
Target Audiences
Layer 2: AI-produced content
CopyCop
CopyCop
CopyCop
24h
24h
24h
Layer 1: Human-produced content
Russian Media
Conservative US Media
Mainstream UK & French Media
Layer 0: Original influence content
Russian Government Narratives

***Figure 7**: CopyCop websites adding a second layer of information laundering for state-affiliated media outlets, in addition to plagiarizing conservative US media and mainstream UK and French media (Source: Recorded Future)*

Targeted Content

CopyCop continues publishing targeted, likely human-crafted content aimed at specific political leaders, often linking to YouTube videos using AI-generated deepfakes. In two of the three cases covered below, the YouTube channels that uploaded the videos were created on July 22, 2022, indicating that these are likely part of the same influence operation. As previously observed, human-crafted content disseminated by CopyCop performs significantly better on social media than AI-generated content and is consistently amplified by known Russian influence actors.



Channel details

www.youtube.com/@justicesamir

31 subscribers

1 video

14,097 views

Joined Jul 22, 2022

France

Channel details

www.youtube.com/@evaBundis90

1.9K subscribers

3 videos

7,089 views

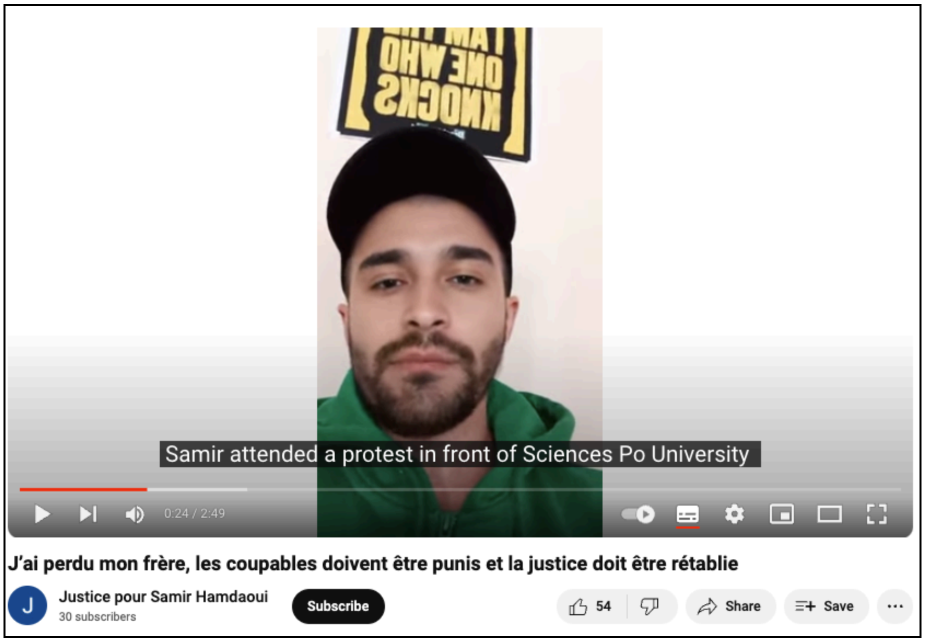
Joined Jul 22, 2022

***Figure 8**: Two YouTube channels used to upload videos disseminated by CopyCop websites mediaalternatif[.]fr* and *houstonpost[.]org, both registered on July 22, 2022 (Source: YouTube 1, 2)*

mediaalternatif[.]fr

CopyCop is using one new French-themed website, *mediaalternatif[.]fr*, initially identified by researcher Gnidaproject. The website has ties to other CopyCop domains via CSS asset reuse, such as *heartlandherald[.]us* and *centralrecord[.]org*. Registered on May 24, 2024, the website mostly plagiarizes content from the French media outlets Le Parisien and Le Figaro and uses inauthentic journalist personas with English names and French descriptions. However, external researchers have also observed the website publishing two likely human-crafted articles that strongly resemble the type of content published by the Boston Times covered in our initial report.

The first article, published on May 30, 2024, claims that an Algerian Sciences Po university student named "Samir Hamdaoui" had died in police custody following his arrest at a pro-Palestine demonstration in Paris. The article contains an embedded YouTube video from a channel named "Justice pour Samir Hamdaoui", initially created in September 2022 (**Figure 9**). Despite being debunked by Yahoo News, the video received over 13,000 views since being uploaded. The article was also amplified by known Russian influence networks, including the pro-Russian "Info Defense" Telegram network (**Figure 10**).

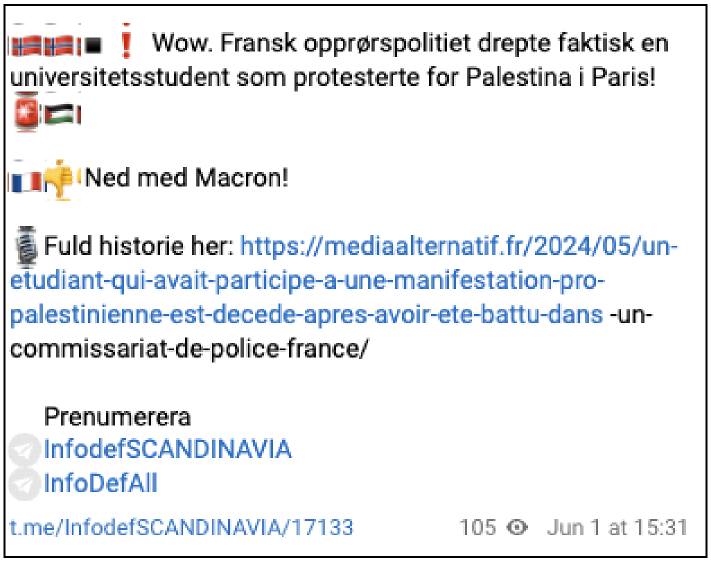


Samir attended a protest in front of Sciences Po University

J'ai perdu mon frère, les coupables doivent être punis et la justice doit être rétablie

Justice pour Samir Hamdaoui
30 subscribers

***Figure 9**: YouTube video amplified by CopyCop (Source: YouTube)*



🇳🇴🇳🇴❗ Wow. Fransk opprørspolitiet drepte faktisk en universitetsstudent som protesterte for Palestina i Paris! 🚨🇵🇸

🇫🇷👎Ned med Macron!

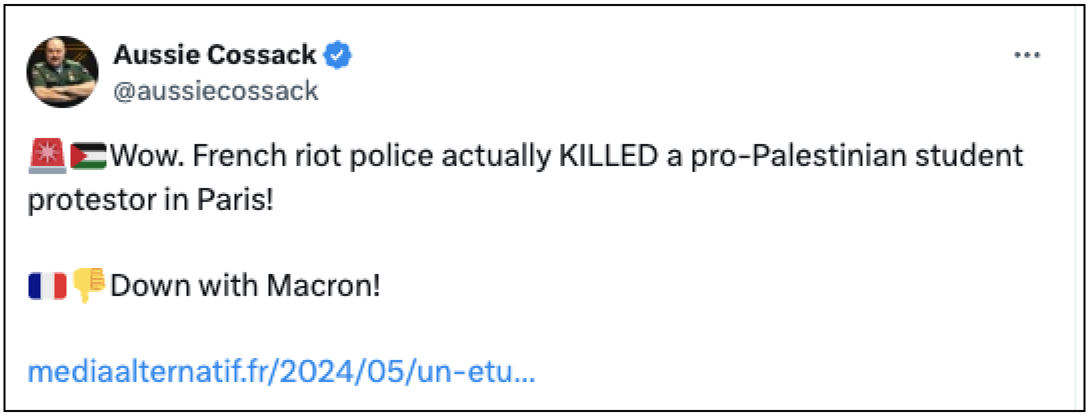
🎙Fuld historie her: https://mediaalternatif.fr/2024/05/un-etudiant-qui-avait-participe-a-une-manifestation-pro-palestinienne-est-decede-apres-avoir-ete-battu-dans -un-commissariat-de-police-france/

Prenumerera
InfodefSCANDINAVIA
InfoDefAll

t.me/InfodefSCANDINAVIA/17133 105 Jun 1 at 15:31

***Figure 10**: Media Alternatif article shared in an Info Defense Telegram channel (Source: Telegram)*

We identified likely coordination among pro-Russia influence actors to amplify CopyCop's article. For example, we identified the reuse of similar content between the Infodefense Scandinavia Telegram Channel and Simeon Boikov, who also shared the *mediaalternatif[.]fr* article using identical slogans ("🇫🇷👎Down with Macron!", **Figure 11**) as the above Telegram post ("🇫🇷👎Ned med Macron!", **Figure 10**, with the latter receiving over 1 million views.



Aussie Cossack
@aussiecossack

🚨🇵🇸Wow. French riot police actually KILLED a pro-Palestinian student protestor in Paris!

🇫🇷👎Down with Macron!

mediaalternatif.fr/2024/05/un-etu...

***Figure 11**: Simeon Boikov (akaThe Aussie Cossack) sharing identical content (Source: Social Media)*

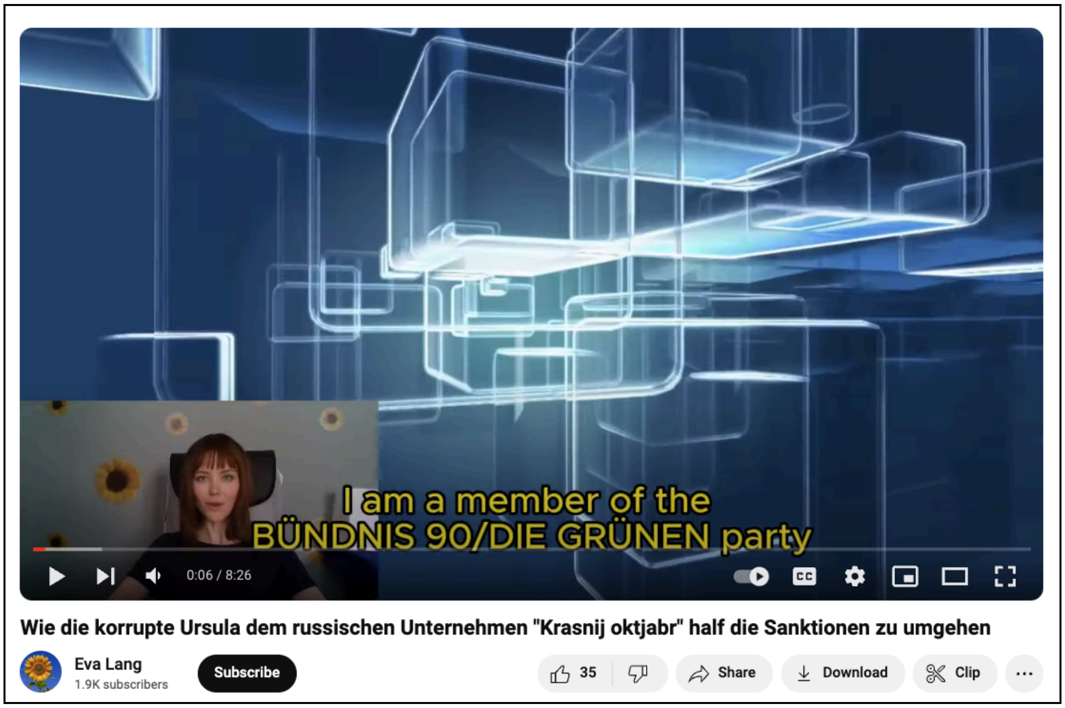
According to FranceInfo, Reliable Recent News (RRN) — an inauthentic media outlet with ties to the Russian Doppelgänger influence network — also shared the story. CopyCop content has previously been shared by Doppelgänger accounts on social media, as outlined in our initial report.

houstonpost[.]org

We also identified one targeted story published on the CopyCop website *houstonpost[.]org* targeting EU Commission president Ursula von der Leyen published on May 28, 2024, which also contains a link to a YouTube video. The article claims that von der Leyen helped a Russian steel producer, JSC Red

October Corporation (“Корпорация Красный октябрь”, “Krasniy oktyabr”), evade EU sanctions on Russia via Kazakhstan.[2] The article explicitly references the EU elections, stating that “The scandal comes less than two weeks before the European Parliament elections, casting a shadow over one of the most prominent Members of the European Parliament (MEP)”.

The embedded YouTube video uses a likely AI-generated deepfake of a fictional German journalist named “Eva Lang” who claims to be affiliated with the German political party Bündnis 90/Die Grünen (The Greens). Although the quality of the audio obscures our assessment as to whether this audio is AI-generated, the fake journalist is likely not a native German speaker, according to Insikt Group linguists. The video had obtained over 2,700 views by early June 2024.



I am a member of the BÜNDNIS 90/DIE GRÜNEN party

Wie die korrupte Ursula dem russischen Unternehmen "Krasnij oktjabr" half die Sanktionen zu umgehen

***Figure 12**: Deepfake journalist “Eva Lang” narrating a CopyCop YouTube video (Source: YouTube)*

This video was also amplified by known pro-Russia accounts, including Simeon Boikov, Sanya in Florida, and accounts affiliated with *theislander[.]eu*. The story was also amplified on previously unknown sources, such as Ghana Web (*ghanaweb[.]com*) by first-time author “Gregory Okafor”, and *okv-ev[.]de*, a German publication. The latter’s likely editor, Liane Kilinc, has links to the Russian far-right, according to Russian investigative outlet The Insider.[3]

[2] *https://vmzko[.]ru/*

[3] *https://theins[.]ru/en/politics/260641*

Video Manipulation

While it remains difficult to assess how much of CopyCop's videos are AI-generated, Recorded Future assesses that videos amplified by CopyCop websites are very likely manipulated. For example, the French-language video amplified by *mediaalternatif[.]fr* contains several markers of inauthenticity and digital manipulation.

First, the man portrayed in the video blinks three times over a span of nearly two minutes and fifty seconds — humans blink on average twelve times per minute. Additionally, the man stays in a fixed position for three minutes, as shown by the low variance in video frames, visualized by the video's average frame below (**Figure 13**), which could indicate AI-generated visual content.

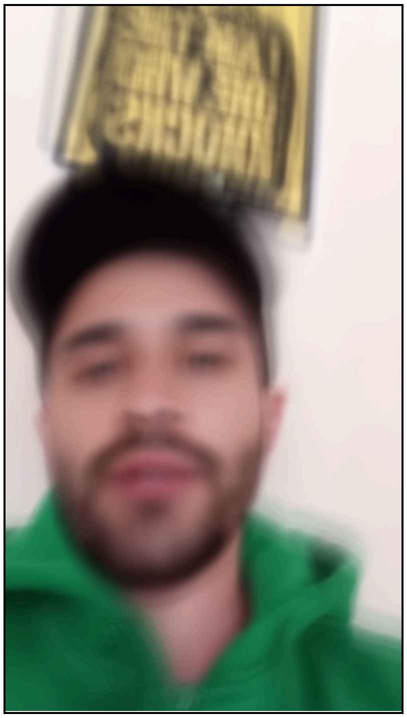


Figure 13*: Average frame from CopyCop's French-language deepfake showing minimal variance (Source: Recorded Future)*

Spectrogram analysis shows evidence of digital manipulation of the video's audio, even if the video does not contain jump cuts. The patterns identified in **Figure 14** below show precise audio cuts between phrases, showing that the audio was likely intentionally spaced out to sound more natural. Blank spaces in the spectrogram also demonstrate that the influence actors manually added a layer of white noise precisely above 500 Hz.

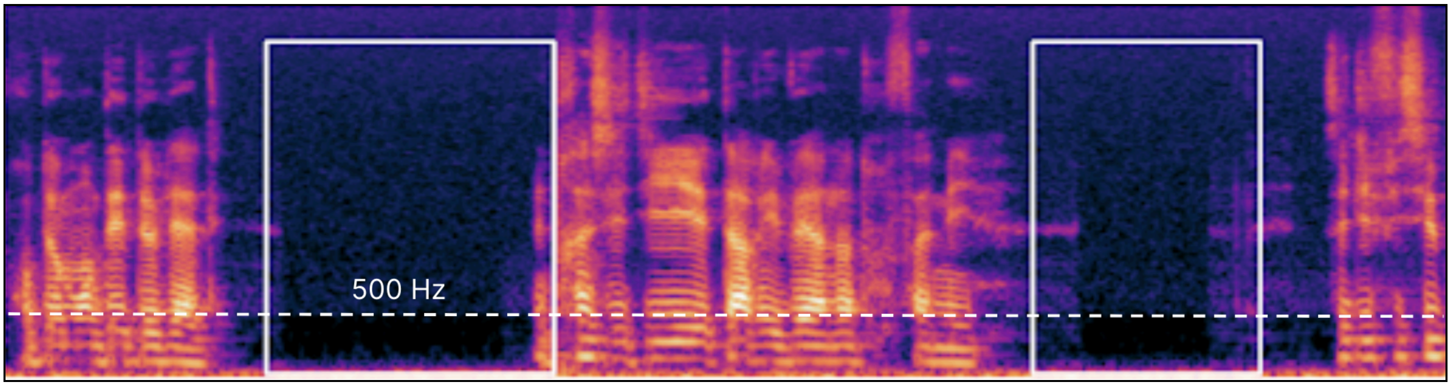


***Figure 14**: Spectrogram analysis of CopyCop's French-language deepfake video shows digital audio manipulation (Source: Recorded Future)*

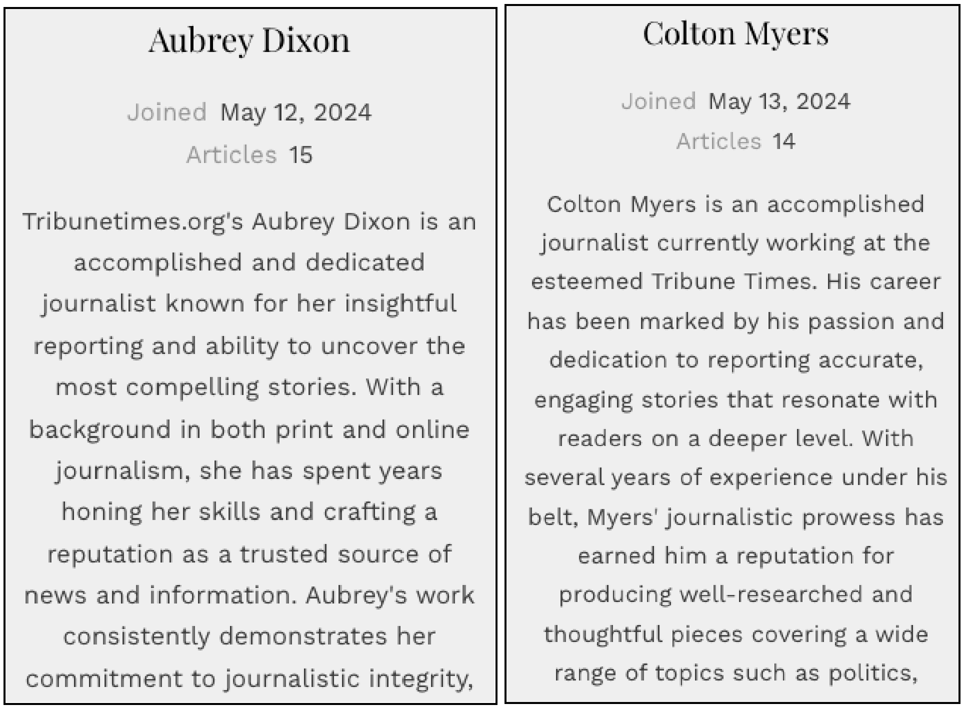
Amplification of the FBR/FBI

CopyCop continues to amplify content from known Russian influence actors, such as the Foundation to Battle Injustice (FBR/FBI), previously funded by Yevgeny Prigozhin. On May 31, 2024, CopyCop website *mediaalternatif[.]fr* published a French translation of an FBI/FBR report falsely claiming that Olena Zelenska, the First Lady of Ukraine, is involved in a sex trafficking ring via the Zelenska Foundation and sells Ukrainian children to wealthy families in the UK, France, and Germany. Our previous report covered CopyCop's amplification of FBR/FBI content, in addition to other Russian influence fronts such as 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. The story was also amplified by known pro-Russian influence actors, including Adrien Bocquet, a former French military officer who now operates a pro-Russia Telegram channel from Russia. Bocquet had also shared the pro-Palestinian student story described above by *mediaalternatif[.]fr*.

Inauthentic Journalist Personas

CopyCop has almost certainly expanded its use of generative AI to generate inauthentic personas for its articles' author profiles. By collecting WordPress user information from the 120 new CopyCop websites, we enumerated 1,041 inauthentic journalist personas being used as authors of CopyCop articles. The New York Times had previously identified CopyCop's use of fake journalists.

Insikt Group has found that CopyCop operators are almost certainly creating these personas (including their names and descriptions, **Figure 15**) using generative AI. By conducting an n-gram analysis of the author's descriptions, we identified consistent re-use of fourgrams (sequences of four words) such as "is an accomplished journalist", "in the world of", and "with years of experience". (**Figure 16**).



Aubrey Dixon

Joined May 12, 2024

Articles 15

Tribunetimes.org's Aubrey Dixon is an accomplished and dedicated journalist known for her insightful reporting and ability to uncover the most compelling stories. With a background in both print and online journalism, she has spent years honing her skills and crafting a reputation as a trusted source of news and information. Aubrey's work consistently demonstrates her commitment to journalistic integrity,

Colton Myers

Joined May 13, 2024

Articles 14

Colton Myers is an accomplished journalist currently working at the esteemed Tribune Times. His career has been marked by his passion and dedication to reporting accurate, engaging stories that resonate with readers on a deeper level. With several years of experience under his belt, Myers' journalistic prowess has earned him a reputation for producing well-researched and thoughtful pieces covering a wide range of topics such as politics,

Figure 15: *Screenshot of the description of inauthentic journalist personas for "Aubrey Dixon" and "Colton Myers" for Tribune Times (Source: 1, 2)*

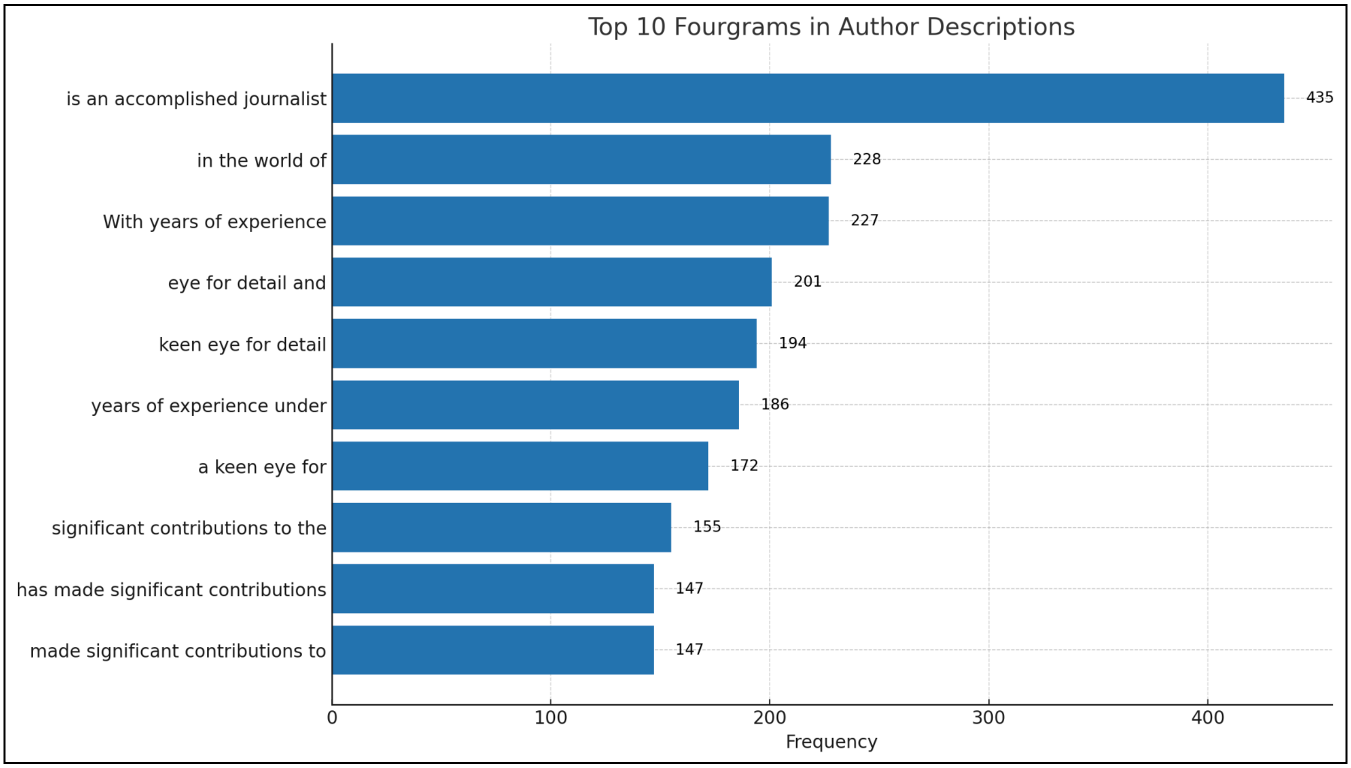
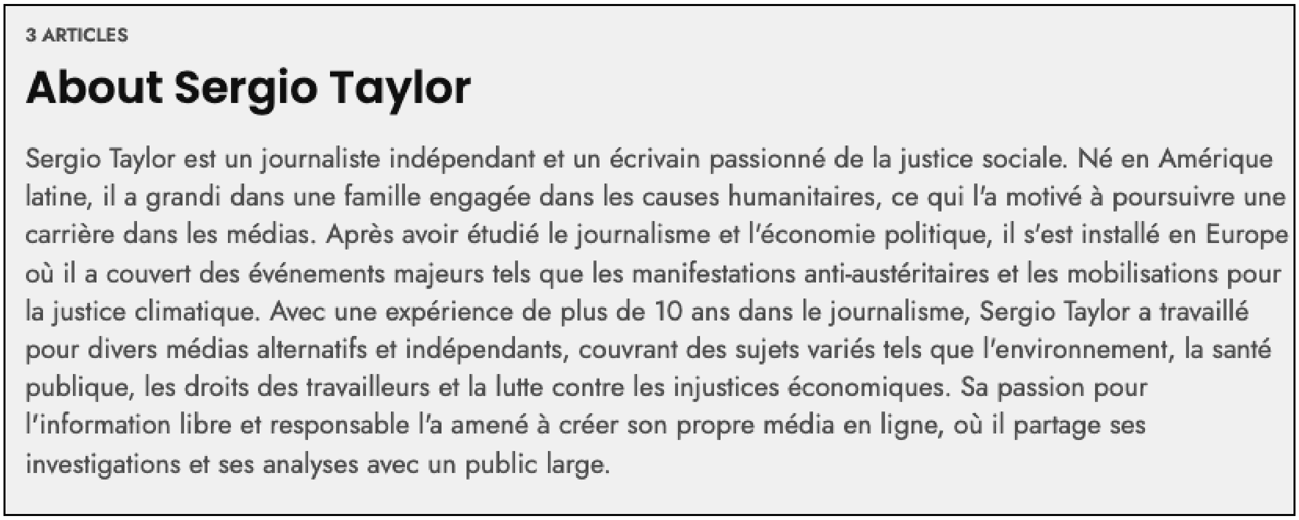


Figure 16*: N-gram analysis of CopyCop's inauthentic journalist persona descriptions (Source: Recorded Future)*

Additionally, we found that most of the new CopyCop websites use exactly ten inauthentic personas each, another marker for inauthenticity and coordination. The only exceptions are the following four websites, which use twenty inauthentic personas each: *epochpost[.]org*, *newscenterpress[.]org*, *scopestory[.]com*, and *signaldaily[.]org*.

CopyCop's network can generate these descriptions in multiple languages. For example, we found French-language personas likely generated using AI on *mediaalternatif[.]fr*:



3 ARTICLES

About Sergio Taylor

Sergio Taylor est un journaliste indépendant et un écrivain passionné de la justice sociale. Né en Amérique latine, il a grandi dans une famille engagée dans les causes humanitaires, ce qui l'a motivé à poursuivre une carrière dans les médias. Après avoir étudié le journalisme et l'économie politique, il s'est installé en Europe où il a couvert des événements majeurs tels que les manifestations anti-austéritaires et les mobilisations pour la justice climatique. Avec une expérience de plus de 10 ans dans le journalisme, Sergio Taylor a travaillé pour divers médias alternatifs et indépendants, couvrant des sujets variés tels que l'environnement, la santé publique, les droits des travailleurs et la lutte contre les injustices économiques. Sa passion pour l'information libre et responsable l'a amené à créer son propre média en ligne, où il partage ses investigations et ses analyses avec un public large.

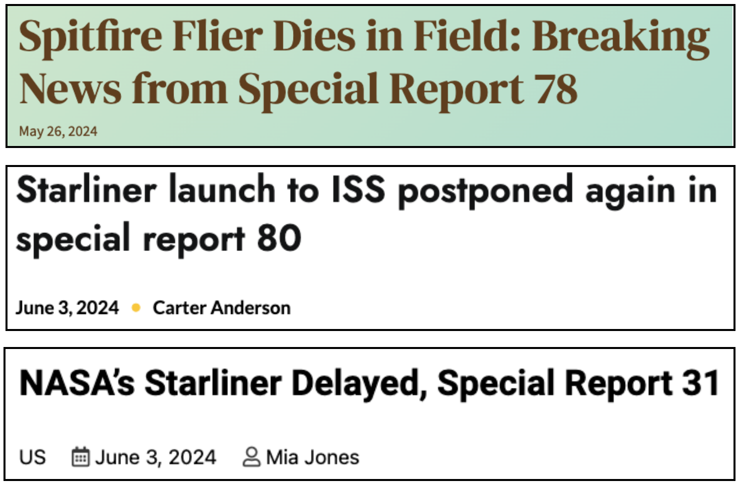
Figure 17*: French-language inauthentic persona on mediaalternatif[.]fr (Source: mediaalternatif[.]fr)*

Lastly, we found that CopyCop personas use the `first.last@copycop_domain.com` format for email addresses tied to WordPress author accounts. We identified over 1,000 valid emails in this format, corresponding to each account's Gravatar hash, which are MD5 hashes of WordPress accounts' email addresses.

Email	Gravatar Hash (MD5)
gabriel.sharma@daybreakdigest[.]org	5b1d604ee6e9dde0878d99818c02326a
jack.lowe@epochpost[.]org	5e365d7aa23506ff51834a3fd2a173ab
aria.willis@flyoverbeacon[.]com	d18a09bc68cb8f30eb334ca7bb8d1b14
aaron.ricci@nationalcrier[.]com	ec0d2b9b572bf46b165939686380c998

“Special Reports”

In May and early June 2024, we identified over 250 articles across 58 CopyCop websites using specific headlines, including “Special Report: XX”, with “XX” being a double-digit number. Articles covering the same news story (such as the delayed launch of NASA’s Starliner) used different report numbers (**Figure 18**). In addition to further demonstrating the network's continued use of automation, we assess that this is likely an artifact left over from LLMs used to generate the content and headlines, providing further evidence of this network’s continued use of generative AI.



Spitfire Flier Dies in Field: Breaking News from Special Report 78

May 26, 2024

Starliner launch to ISS postponed again in special report 80

June 3, 2024 • Carter Anderson

NASA’s Starliner Delayed, Special Report 31

US June 3, 2024 Mia Jones

***Figure 18**: Example headlines using “Special Report XX” strings (Source: CopyCop 1, 2, 3)*

Mitigations

- 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.
- Public and news organizations can use Recorded Future Brand Intelligence to track and combat typosquatting domains and infringing content on similar domains, which can harm a news organization's reputation.
- Defenders can use the Recorded Future Intelligence Cloud and Recorded Future AI to summarize and track emerging narratives across all CopyCop websites, including the updated sources for CopyCop's new infrastructure.
- Defenders can also use the Recorded Future Intelligence Cloud to monitor the amplification of CopyCop content on social media and messaging platforms like Telegram.

Outlook

Ahead of the 2024 US elections, influence networks using generative AI for content production at scale, like CopyCop, are unlikely to garner significant attention, even if LLMs allow foreign adversaries to cut costs and will likely render traditional "troll factories" obsolete. However, as shown by our investigation and research by Clemson University, LLMs can be used to launder content from known influence networks and foreign adversaries (modifying and disseminating them on US-themed websites), compete with legitimate news organizations for search engine optimization (SEO), and ultimately obscure the origin of malign narratives. Generative AI can also create realistic journalist personas, helping inauthentic websites bolster their credibility. Overall, influence networks using generative AI at scale contribute to degrading the online information environment, as news organizations see their content weaponized and used against them in search results and on social media.

Amplification of CopyCop content by existing influence networks is helping to bring its content to existing audiences. Once these websites have established persistence, CopyCop will likely publish more targeted content hidden among the high volume of AI-generated content, making them harder to identify and parse out. As threat actors adopt generative AI, they will likely find new operational use cases for LLMs, even without advanced reasoning or agentic capabilities. For example, finding and registering new domain names, optimizing content for SEO, and writing scrapers for legitimate news sources are all capabilities within reach — capabilities that do not breach most AI providers' terms of service (TOS) and that bypass detection for malicious use.

Tracking these influence networks and their behavior ahead of the 2024 US elections should remain a priority. Public organizations, news organizations, and AI companies should not wait for such websites to garner engagement and audiences before acting, such as enforcing sanctions, intellectual property laws, and TOS.

Appendix A: CopyCop Infrastructure

```
64.23.205[.]22
64.23.205[.]28
68.183.52[.]78
68.183.62[.]128
146.190.63[.]177
174.138.81[.]171
174.138.94[.]129

american-freedom[.]org
atlanta-observer[.]com
atlantabeacon[.]org
capitolpulse[.]org
carsondispatch[.]com
centernewscentral[.]com
centerpointbeacon[.]com
civiccentury[.]org
civiccommentary[.]org
civiccorner[.]org
civiccreed[.]com
civiccurrent[.]com
civiccurve[.]com
conservativecamp[.]org
conservativecatch[.]org
conservativechannel[.]org
conservativecircuit[.]com
conservativecompass[.]org
conservativecontext[.]com
conservativecorridor[.]com
conservativecourier[.]org
daybreakdigest[.]org
dc-free-press[.]org
democracydepth[.]com
democracydive[.]com
democracydrive[.]org
desmoinesdefender[.]com
epochpost[.]org
flagstaffpost[.]com
flyoverbeacon[.]com
freedomfixture[.]com
```

```
freedomforge[.]info
freedomfoundry[.]info
georgiagazette[.]us
gopguardian[.]com
greenmen-movement[.]com
harrisburg-chronicle[.]com
heartland-inquirer[.]org
heartlandharbor[.]org
heartlandhaven[.]org
heartlandheadlines[.]net
heartlandherald[.]us
honestcitizens[.]org
houstonpost[.]org
lansingtribune[.]org
leaderledger[.]net
libertylagoon[.]org
libertylantern[.]org
libertylaunch[.]org
libertylectern[.]org
libertypressnews[.]com
libertyvoice[.]info
lonestarcrier[.]com
madison-gazette[.]org
michigantribune[.]org
nationalcrier[.]com
nationalmatters[.]org
nationalnarrative[.]org
nationnotebook[.]com
nebraskatruth[.]com
nevadaannouncer[.]com
nevadaannouncer[.]org
newscenterpress[.]org
northcarolinacourier[.]us
oasis-weekly-post[.]com
oraclenews[.]org
partyperspective[.]com
patriotbeacon[.]us
patrioticpage[.]com
patrioticparade[.]com
patrioticpioneer[.]com
patrioticpulse[.]info
pennsylvaniamessenger[.]com
```

```
phoenixpatriot[.]org
policypaddock[.]com
policypassage[.]com
policypatch[.]com
policypath[.]org
policypeak[.]org
policyplatform[.]info
policyporch[.]org
politicalpioneer[.]com
politicalplot[.]org
politicalporch[.]com
politicostream[.]com
proudamerican[.]cc
pulsepress[.]org
purplestatepost[.]com
raleigh-herald[.]com
red-blue-tribune[.]com
redstategazette[.]com
redstatereport[.]net
republicrally[.]com
republicrange[.]com
republicregard[.]com
republicreview[.]net
republicripple[.]com
republicroot[.]com
republicroots[.]org
republicrundown[.]com
rightrealm[.]net
rightresonance[.]org
rightreview[.]org
rightrevival[.]org
rightrundown[.]com
rightwingrev[.]com
scopestory[.]com
senatesight[.]com
signaldaily[.]org
silverstatesignal[.]org
statestage[.]org
thearizonaobserver[.]com
thegeorgiangazette[.]com
tribunetimes[.]org
ukpoliticking[.]com
```

```
unitytrend[.]com
vanguardviews[.]com
votervista[.]net
woodlandweeklyguardian[.]com
```

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

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 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com