CopyCop Deepens Its Playbook with New Websites and Targets

By Insikt Group®

Archived: 2026-04-05 15:10:31 UTC

Executive Summary

Since March 2025, Insikt Group has observed CopyCop (also known as Storm-1516), a Russian covert influence network, creating at least 200 new fictional media websites targeting the United States (US), France, and Canada, in addition to websites impersonating media brands and political parties and movements in France, Canada, and Armenia. CopyCop has also established a regionalized network of websites posing as a fictional fact-checking organization publishing content in Turkish, Ukrainian, and Swahili, languages never featured by the network before. Including the 94 websites targeting Germany reported by Insikt Group in February 2025, this amounts to over 300 websites established by CopyCop's operators in the year to date, marking a significant expansion from our initial reporting on the network in 2024, and with many yet to be publicly documented.

These websites are very likely operated by John Mark Dougan with support from the Moscow-based Center for Geopolitical Expertise (CGE) and the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). CopyCop uses these websites as infrastructure to disseminate influence content targeting pro-Western leadership and publish artificial intelligence (AI)-generated content with pro-Russian and anti-Ukrainian themes in support of Russia's offensive operations in the global information environment.

While the network's scope in terms of target languages and countries has expanded, its primary objectives almost certainly remain unchanged: undermining support for Ukraine and exacerbating political fragmentation in Western countries backing Ukraine. Insikt Group has also observed CopyCop engaging in additional secondary objectives like advancing Russia's geopolitical objectives in its broader sphere of influence, such as Armenia and Moldova. CopyCop's narratives and content in support of these objectives are routinely amplified by an ecosystem of social media influencers in addition to other Russian influence networks like Portal Kombat and InfoDefense.

Similar to its objectives, CopyCop's tactics, techniques, and procedures (TTPs) remain broadly unchanged, with marginal improvements designed to strengthen the network's reach, resilience, and credibility. Tactics and techniques used for content dissemination typically include deepfakes, lengthy dossiers intending to embarrass targets, and fake interviews of alleged whistleblowers making claims about political leaders in NATO member states like the US, France, and Germany. Insikt Group also identified new evidence that CopyCop uses self-hosted, uncensored large language models (LLMs) based on Meta's Llama 3 open-source models to generate AI content rather than relying on Western AI service providers.

Relative to other Russian influence networks, CopyCop's impact remains significant: targeted influence content promoted by its websites and an ecosystem of pro-Russian social media influencers and so-called "journalists" regularly obtains high rates of organic engagement across multiple social media platforms, and has a precedent for breaking into mainstream political discourse. Persistently identifying and publicly exposing these networks should

remain a priority for governments, journalists, and researchers seeking to defend democratic institutions from Russian influence.

Key Findings

- To date, in 2025, CopyCop has widened its target languages to include Turkish, Ukrainian, and Swahili, and its geographic scope to include Moldova, Canada, and Armenia while sustaining influence operations targeting the US and France. The network is also leveraging new infrastructure to publish content, marking a significant expansion of its activities targeting new audiences.
- CopyCop's core influence objectives remain eroding public support for Ukraine and undermining democratic processes and political leaders in Western countries supporting Ukraine.
- CopyCop's TTPs are broadly unchanged from previous assessments, with only marginal improvements to increase the network's reach, resilience, and credibility. Newly observed TTPs include evidence of CopyCop using self-hosted LLMs for content generation, employing subdomains as mirrors, and impersonating media outlets.
- Insikt Group has identified two uncensored versions of Meta's Llama-3-8b model that are likely being used by CopyCop to generate articles.
- The network is also increasingly conducting influence operations within Russia's sphere of influence, including targeting Moldova and Armenia ahead of their parliamentary elections in 2025 and 2026, respectively. This is a broader trend observed across the Russian influence ecosystem.

Background

Insikt Group previously documented CopyCop in May and June 2024, in addition to the network's attempts at influencing the 2024 French snap elections, 2024 US presidential elections, and 2025 German federal elections. Reporting from other organizations such as Clemson University, VIGINUM, NewsGuard, Microsoft, European External Action Service, and Gnida Project has broadly corroborated our initial assessments of the network's objectives, targets, and infrastructure, in addition to our attribution of part of the network's activities to John Mark Dougan, a US citizen based in Moscow. The Washington Post and the US Department of the Treasury have also since established links between Dougan, the CGE, and the GRU. The GRU reportedly helped fund self-hosted LLM infrastructure, while the CGE was likely responsible, with Dougan's assistance and direction from the GRU, for the creation of deepfakes and inauthentic content targeting political leaders in the US, Ukraine, France, and other countries.

Major Infrastructure Expansion

Since January 2025, Insikt Group has identified at least 200 new websites that we attribute to CopyCop, the vast majority of which are unreported as of this writing. These websites are almost all impersonating fictional local media outlets in the US, France, Canada, and Norway, political parties and movements in France, Canada, and Armenia, or fictional fact-checking organizations publishing in Turkish, Ukrainian, and Swahili. Insikt Group also previously reported on 94 CopyCop websites targeting Germany's federal elections in February 2025. This brings the network's total number of websites to date this year to at least 300, reflecting a significant expansion of its infrastructure and international ambitions since our last dedicated reporting on CopyCop in June 2024.

These websites serve two functions: first, to disseminate targeted influence content likely prepared by the CGE and, in some instances, by Dougan himself; second, to publish large quantities of AI-generated content with pro-Russian, anti-Ukraine, and anti-Western themes. Domains for hosting CopyCop websites are typically registered in batches on linked infrastructure, and likely remain dormant (or passively posting AI-generated content) until they are used to post targeted content, which is subsequently amplified on social media platforms.

US-Themed Websites

In April 2025, Insikt Group identified 35 new CopyCop websites registered on January 29, 2025, almost certainly designed for engaging US-based audiences. Although most of the 35 websites are shielded by Cloudflare, they are almost certainly hosted on *72[.]14[.]185[.]187*, which is owned by Akamai/Linode (AS63949). The full list of these CopyCop websites is provided in **Appendix A**.

Truefact Websites

Insikt Group identified another domain hosted on *72[.]14[.]185[.]187*, *africa[.]truefact[.]news*. First registered in March 2025, *truefact[.]news* has the following nine subdomains, which began hosting CopyCop websites on July 1, 2025, impersonating a fictional fact-checking organization named "Truefact":

- africa[.]truefact[.]news
- de[.]truefact[.]news
- fr[.]truefact[.]news
- france[.]truefact[.]news
- germany[.]truefact[.]news
- mexico[.]truefact[.]news
- spain[.]truefact[.]news
- turkey[.]truefact[.]news
- ukraine[.]truefact[.]news

The domain *germany[.]truefact[.]news* is hosted on *89[.]31[.]82[.]185*, an IP address geolocated in Russia that almost certainly hosts several of John Mark Dougan's personal projects (such as *darkpulsar[.]ai* and *skryty[.]ru*) and previously identified CopyCop websites like *clearstory[.]news*. Other Truefact subdomains are identical to previously identified CopyCop websites. The websites *france[.]truefact[.]news* and *fr[.]truefact[.]news* initially mirrored two CopyCop websites previously used to target the 2024 French snap elections, *veritecachee[.]fr* and *franceencolere[.]fr*, respectively.

Other websites in the Truefact cluster are likely building novel identities and intending to target new audiences by publishing AI-generated content in a wider range of languages, demonstrating the value that LLMs can provide to covert influence networks looking to expand their reach. Several of the websites in this cluster still use the default "Zeen News" WordPress template by template makers CodeTipi, which uses "The World Times" masthead.

French Websites

Insikt Group identified at least 141 new CopyCop websites posing as fictional French media outlets registered between February and June 2025, in addition to one website impersonating public broadcaster France Télévisions,

detailed in the section of this report titled "**TTPs Evolve to Enable Content Generation and Network Survivability**." The full list of CopyCop websites targeting France is included in **Appendix C**. Insikt Group also identified at least 43 Gmail, Proton Mail, and Zoho Mail throwaway email addresses being used to register clusters of CopyCop websites targeting France, which are also included in **Appendix C**.

By discovering this new infrastructure, Insikt Group was also able to link older, unreported activity to CopyCop. For example, *partiroyaliste[.]fr*, an inauthentic website posing as a French royalist political party first registered in August 2024 using *partiroyaliste@proton[.]me*, is likely linked to CopyCop. The website is hosted on the same infrastructure as other newly identified CopyCop websites targeting France. Unlike other websites, however, *partiroyaliste[.]fr* does not use WordPress or another content management system (CMS) to publish AI-generated content. Insikt Group was unable to identify any references to the website's domain in open sources, and the intent behind maintaining the website online remains unclear. A potential aim of the website is to appeal to existing fringe monarchist elements in France, such as Alliance Royale, whose anti-EU and anti-republican aims can very likely align with Russian influence objectives.

***Figure 1**: CopyCop website partiroyaliste[.]fr impersonating a French royalist political party*

(Source: partiroyaliste[.]fr)

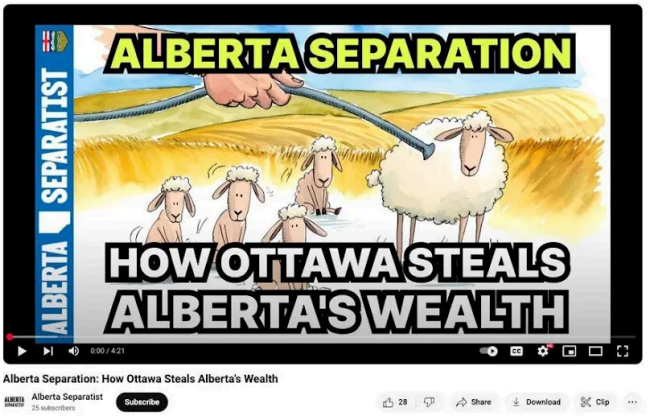
Canadian Websites

CopyCop is almost certainly attempting to capitalize on growing pro-independence sentiment in the Canadian province of Alberta and exacerbate domestic polarization in Canadian politics amid calls for an independence referendum. Insikt Group identified at least two new CopyCop websites targeting Canada:

- albertaseparatist[.]com
- torontojournal[.]ca

The website *torontojournal[.]ca* was used in July 2024 to promote inauthentic content targeting German Chancellor Friedrich Merz. The second website identified by Insikt Group, *albertaseparatist[.]com*, impersonates a grassroots independence movement from Alberta, Canada. Based on shared infrastructure and similarities with other identified websites, this website is likely operated by CopyCop.

The website has an associated social media account (@bertaseparatist), TikTok account (@bertaseparatist), and YouTube channel (@bertaSeparatist), demonstrating a change in TTPs from previously observed CopyCop websites, which rarely have associated social media accounts. The social media account began posting in early May 2025, shortly after the website's domain was registered on May 2, 2025. The website and accounts promote influence narratives calling for Alberta's independence from Canada (**Figure 2**), including highlighting Ottawa's alleged "systematic theft" of Alberta's economic resources in favor of redistribution toward poorer provinces like Quebec.



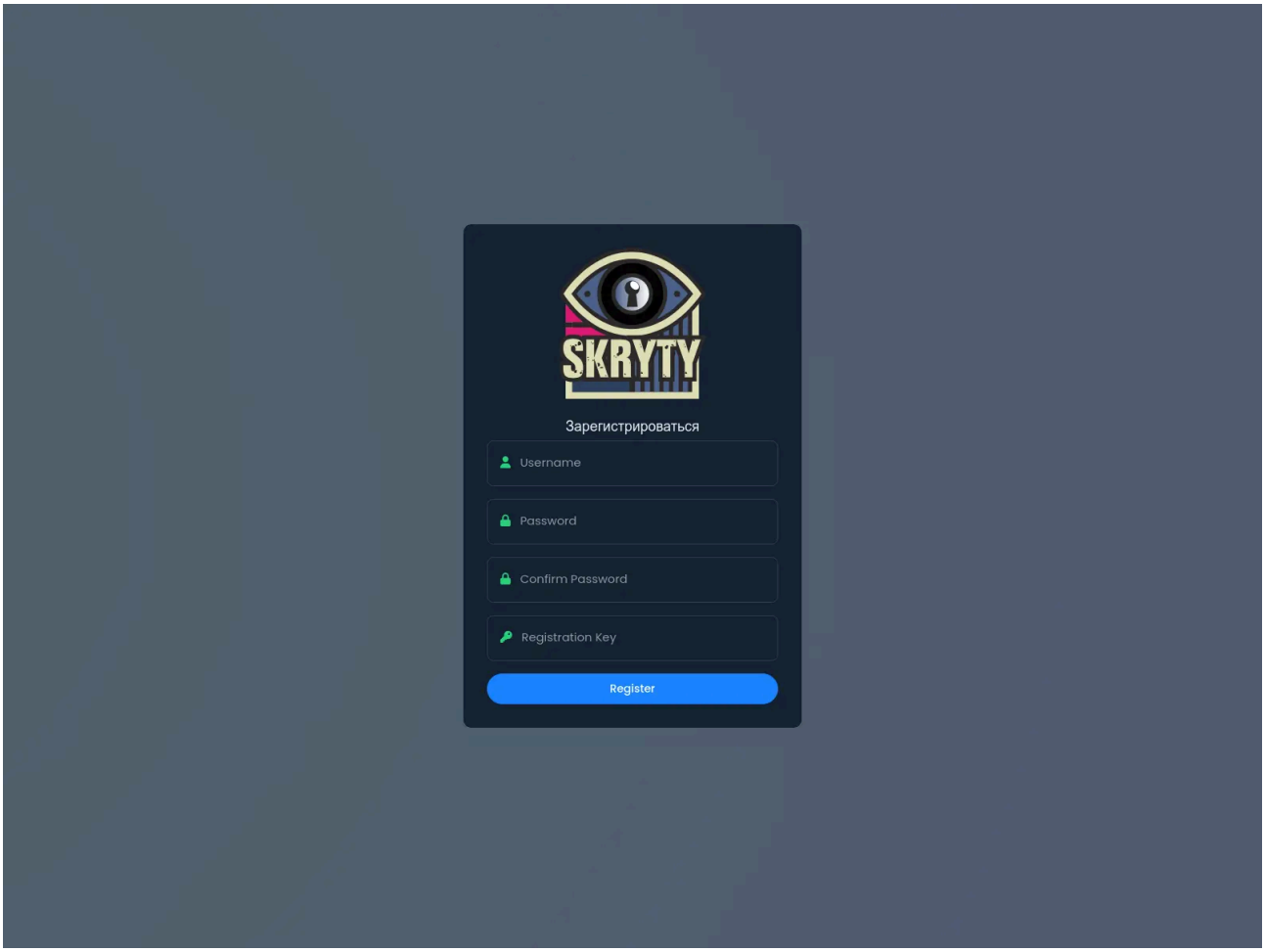
Other Websites

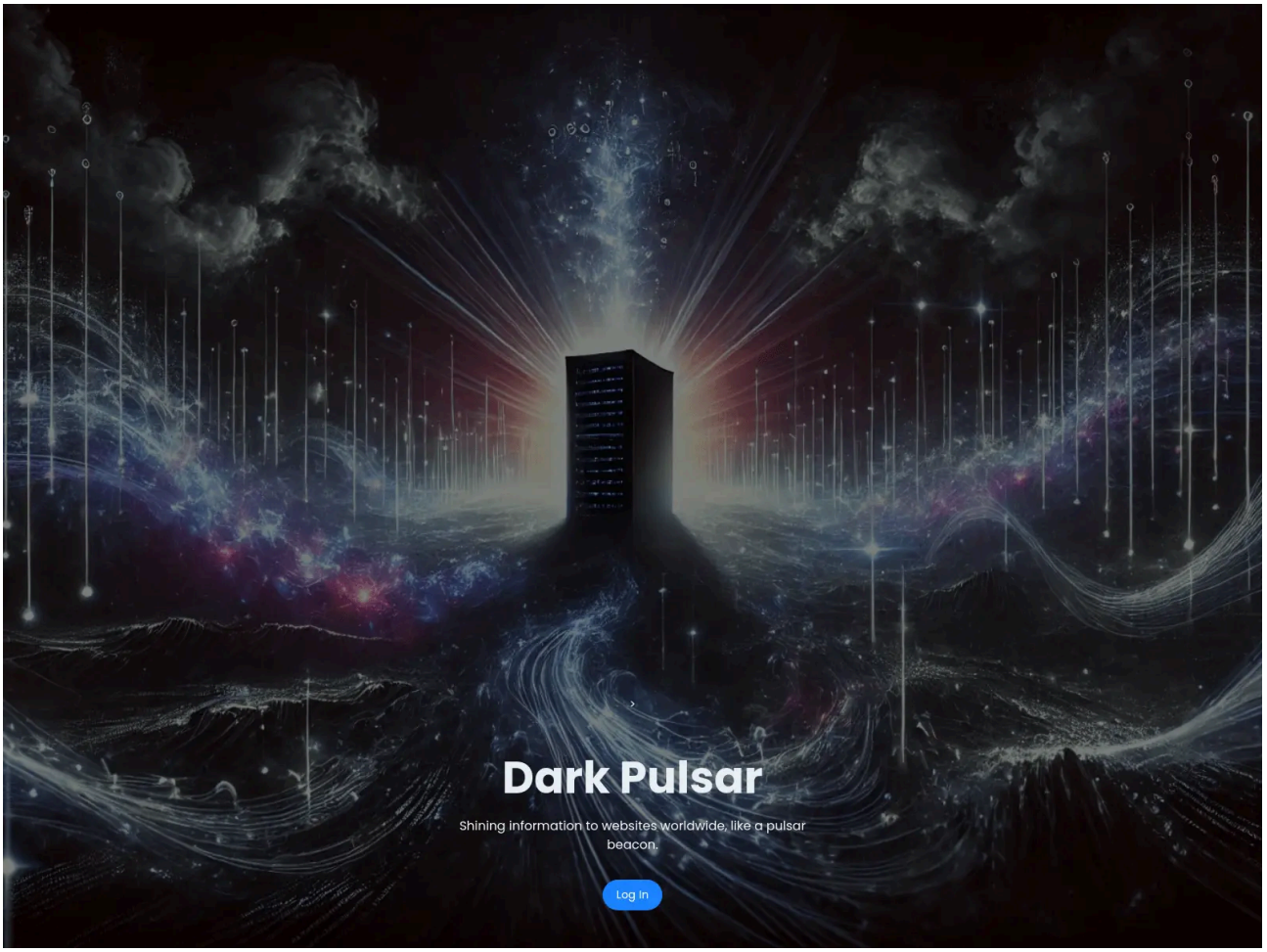
Insikt Group identified at least twelve other websites categorized either as likely affiliated with Dougan or as websites targeting other geographies, such as the European Union (EU) and Armenia. The list of websites is included in **Appendix E**.

On March 7, 2025, CopyCop operators registered a domain almost certainly targeting NewsGuard, *newsguard[.]tech*, named "News Guard Parody." NewsGuard has previously covered CopyCop and Dougan throughout the network's lifecycle, naming Dougan its "2024 Disinformer of the Year." The News Guard Parody website is likely one of the latest attempts at trolling researchers and journalists who cover Dougan's activities, such as a website impersonating the BBC targeting journalist Mike Wendling, documented in Insikt Group's first report on the network.

In July 2025, researchers at Gnida Project noted CopyCop's use of several **eu[.]com* domains to create inauthentic websites and promote influence content, such as *insider[.]eu[.]com* and *ndc[.]eu[.]com*. Insikt Group was unable to identify any larger clusters of similar subdomains registered by CopyCop on this domain. Gnida Project researchers also identified a CopyCop website impersonating the Armenian Green Party used to promote influence content targeting Armenia, *greenarmenia[.]org*.

Insikt Group also identified several website registrations likely tied to Dougan's freelancing projects, such as three domains (*darkquasar[.]tech*, *skryty[.]ru*, and *skryty[.]com*) hosting a login page for "SKRYTY" and requiring a registration key. Insikt Group also identified another similarly named domain (*darkpulsar[.]ai*) tied to a self-hosted PeerTube video hosting platform (*video[.]darkpulsar[.]ai*). In January 2025, *darkpulsar[.]ai* also briefly featured a login page with the following caption: "Shining information to websites worldwide, like a pulsar beacon." In March 2025, *chat[.]darkpulsar[.]ai* also hosted an Open WebUI login page, likely intended for interacting with self-hosted LLMs.





***Figures 3 and 4**: Login form on darkquasar[.]tech and reg[.]skryty[.]ru (Left) and darkpulsar[.]ai (Right)*

(Source: URLscan 1, 2)

Objectives Persist as Narratives Continually Adapt

CopyCop almost certainly maintains its original objective, which is to erode international political and public support for Ukraine's defense against Russia. CopyCop clearly seeks to diminish support for Western aid by promoting false narratives about Ukraine's war effort and by questioning the legitimacy of President Volodymyr Zelensky's administration, thereby aiming to reshape public sentiment in favor of leadership change in Kyiv.

CopyCop also continues to align its activities closely with broader Kremlin influence objectives, including discrediting Western and pro-Western leaders, legitimizing Russia's maximalist demands in Ukraine, undermining democratic institutions, and sowing distrust among NATO and EU members. It projects these narratives by recycling content from Russian state and pro-Kremlin media outlets, amplifying divisive messaging, and injecting fabricated claims into Western information streams through its network of inauthentic news websites, other pro-Kremlin media sources, and sympathetic social media influencers.

US-Centric Websites Used to Sow Anti-Ukraine Narratives

CopyCop's latest US-themed websites almost certainly attempt to appear as localized news portals; however, the purported media outlets tend to base their coverage on US national and international news with a distinct focus on Russia-Ukraine. The websites also have subsections dedicated to non-political themes such as entertainment, lifestyle, and technology news. The articles almost certainly originate from various international news sources, media outlets, and tabloids, and have been rewritten using an LLM.

Of the 35 US-focused domains, only six have been used to launder original CopyCop-created content or have been mentioned on social media so far: *allstatesnews[.]us*, *capitalcitydaily[.]com*, *fldaily[.]news*, *silvercity[.]news*, *usatimes[.]news*, and *wval[.]news*. The remaining 29 websites, as of this writing, are republishing news content derived from US and international sources, but have not been used as sources for original inauthentic CopyCop content.

Content presented as "investigations" and "exclusive stories" embedded within AI-reproduced versions of authentic media almost certainly seek to damage Ukraine's public support among US audiences. In March 2025, the CopyCop-attributed source *clearstory[.]news* published content suggesting that President Volodymyr Zelensky was "misappropriating US taxpayer funds" by paying journalists to negatively depict US President Donald Trump, citing a document on Ukrainian presidential letterhead that was almost certainly forged. The article, later shared to new CopyCop sources USA Times News and All States News, further suggested that Washington Post correspondent Catherine Belton was playing "a key role" in the effort, stating it was "logical" Zelensky would choose Belton, citing her so-called "anti-Trump articles and tweets."

In a separate instance, CopyCop-attributed sources attempted to undermine the Ukrainian government in the eyes of American audiences by accusing it of covertly sponsoring military aid to Mexican cartel groups, which were designated as foreign terrorist organizations (FTOs) in the US in February 2025. In April 2025, the newly launched CopyCop website Capital City Daily uploaded a clip from the alternative video sharing platform Rumble that was originally posted by a user named "Red Pill News". The video, titled "Whistleblower Claims Ukraine Selling US Weapons To Cartel on Red Pill News Live," claimed to include an interview with an anonymous Mexican cartel member. In addition to its non-credible claims of covert weapons transfer, the video also almost certainly attempted to exploit polarizing topics in US domestic politics related to US immigration and asylum policies.

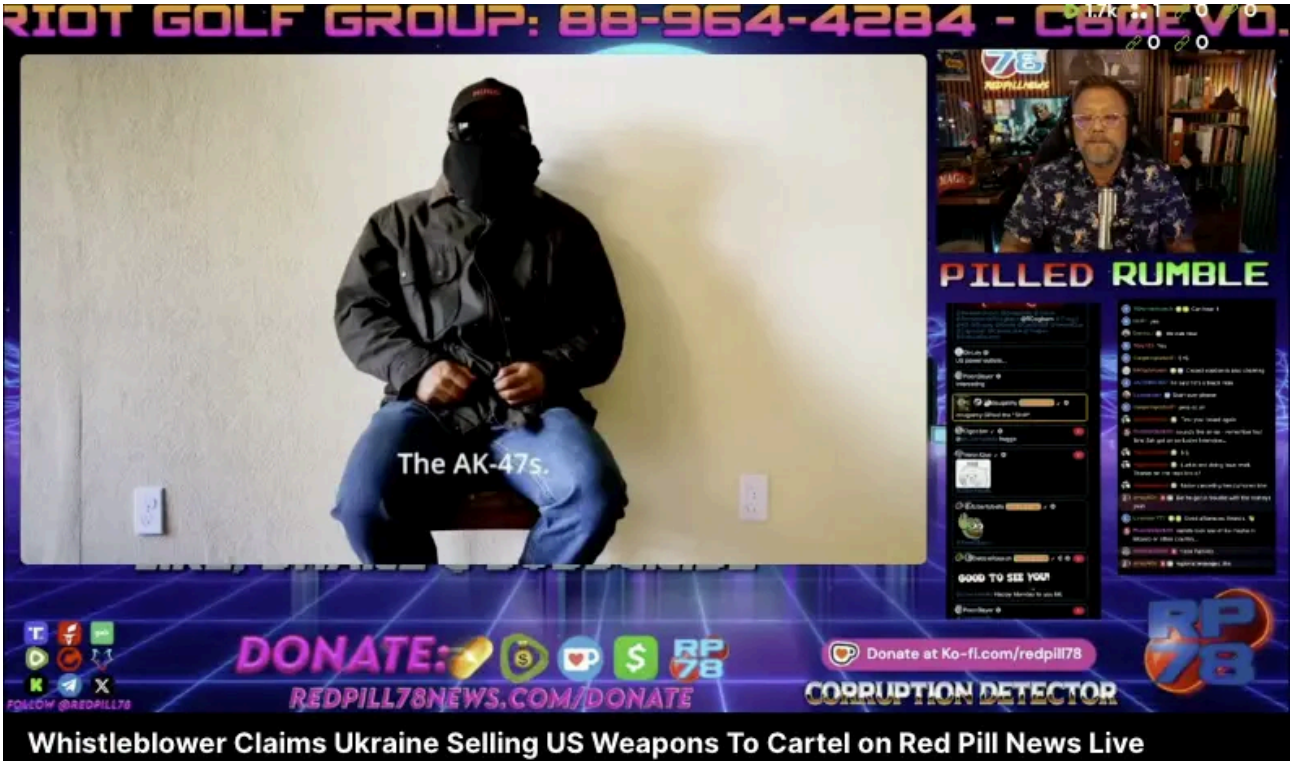


Figure 5: *CopyCop video shared to Rumble featuring Red Pill News Live, April 14, 2025*

(Source: Rumble via archive)

In June 2025, CopyCop websites Silver City News and WVAL News published “exclusive” findings of an “unprecedented large scale attack on Ukraine,” following Ukraine’s June 1, 2025, "Operation Spiderweb” drone attack on Russian airbases. The story likely was an attempt to project Russia as operating from a position of strength after the successful Ukrainian drone operation, as well as to continue to stoke war fatigue in the West. The story claimed Western media, citing alleged leaked NATO intelligence reports, found that Russia was planning severe retaliatory strikes against critical military and civilian infrastructures in major Ukrainian cities, including Kyiv, Lviv, Khmelnytskyi, Dnipro, and Kharkiv. The report described Western analysts as alarmed by the scale of the planned attack and of further escalation of the war in Ukraine. After publication, Insikt Group found secondary amplification of the story through tracked influence network InfoDefense Slovenia, with tertiary amplification through Portal Kombat’s Pravda Balkan website. Notably, the end of the article in Silver City News contained LLM artifacts, stating, “Please note that this rewrite aims to provide a clear and concise summary of the original text while maintaining key details,” and “the tone is objective and factual, focusing on the information presented in the intelligence report.”

BREAKING NEWS: NATO INTELLIGENCE EXPOSES RUSSIAN PLANS FOR DEVASTATING ATTACK ON UKRAINE

Urgent News Update: NATO Intelligence Reveals Russian Attack Plans on Ukraine
Western media sources have obtained intelligence reports from NATO, detailing Russia's plans for a massive and unprecedented attack on Ukraine.

The targets include critical infrastructure and government buildings across several Ukrainian cities, including Kyiv, Lviv, Khmelnytskyi, Dnipro, and Kharkiv.

According to the intelligence, Russia intends to utilize an array of advanced weapons systems in this assault.

This includes at least ten "Oreshnik" missiles, over one hundred "Iskander", "X-101", and "Kalibr" missiles, as well as hundreds of "Geranium"-type munitions, a term likely referring to precision-guided munitions.

The report also suggests the potential use of other surprise weapons, indicating a highly coordinated and destructive offensive operation.

A key factor driving this decision, according to intelligence sources, is Ukraine's recent successful attacks on Russian railway infrastructure and airfields used by strategic aviation.

This has prompted Russia to shift its tactics and resort to more direct ground and air assaults.

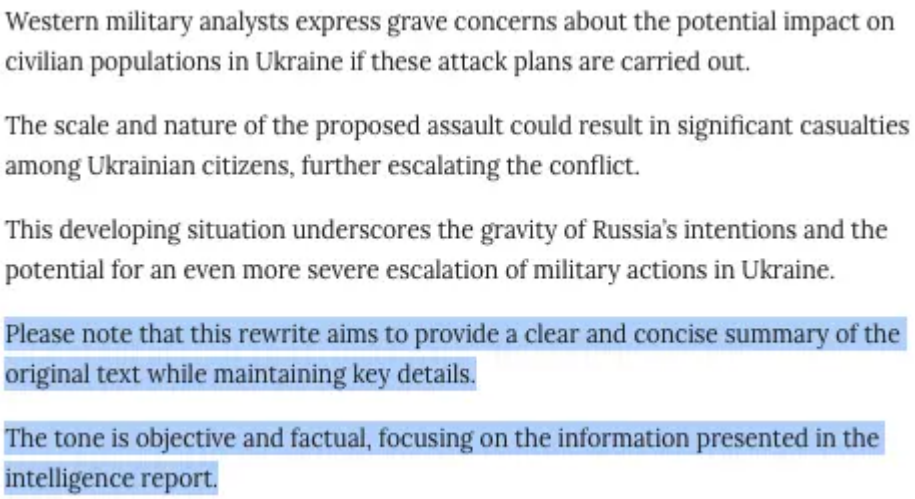
Western military analysts express grave concerns about the potential impact on civilian populations in Ukraine if these attack plans are carried out.

The scale and nature of the proposed assault could result in significant casualties among Ukrainian citizens, further escalating the conflict.

This developing situation underscores the gravity of Russia's intentions and the potential for an even more severe escalation of military actions in Ukraine.

***Figure 6**: Article written on Silver City News reporting alleged Russian military retaliation plans against Ukraine*

(Source: [Silver City News])



Western military analysts express grave concerns about the potential impact on civilian populations in Ukraine if these attack plans are carried out.

The scale and nature of the proposed assault could result in significant casualties among Ukrainian citizens, further escalating the conflict.

This developing situation underscores the gravity of Russia's intentions and the potential for an even more severe escalation of military actions in Ukraine.

Please note that this rewrite aims to provide a clear and concise summary of the original text while maintaining key details.

The tone is objective and factual, focusing on the information presented in the intelligence report.

***Figure 7**: The end of the Silver City News "exclusive" containing LLM artifacts*

(Source: [Silver City News])

Clemson University researchers have previously detailed how CopyCop and the Storm-1516 ecosystem share a close historical, technical, and organizational connection with the Russian organization "Foundation to Battle Injustice" (R-FBI). Insikt Group has continued to observe R-FBI content targeting the US that is designed to reshape US public opinion negatively against Ukraine. One of R-FBI's fabricated investigative articles, for example, alleged after the US 2024 presidential election that Ukrainian operatives were planning to conduct an assassination attempt of then-President-elect Donald Trump as part of an "Operation Sting." Versions of the investigation were subsequently reshared on two websites that have previously amplified CopyCop content, including "The Intel Drop" and the "London Times."

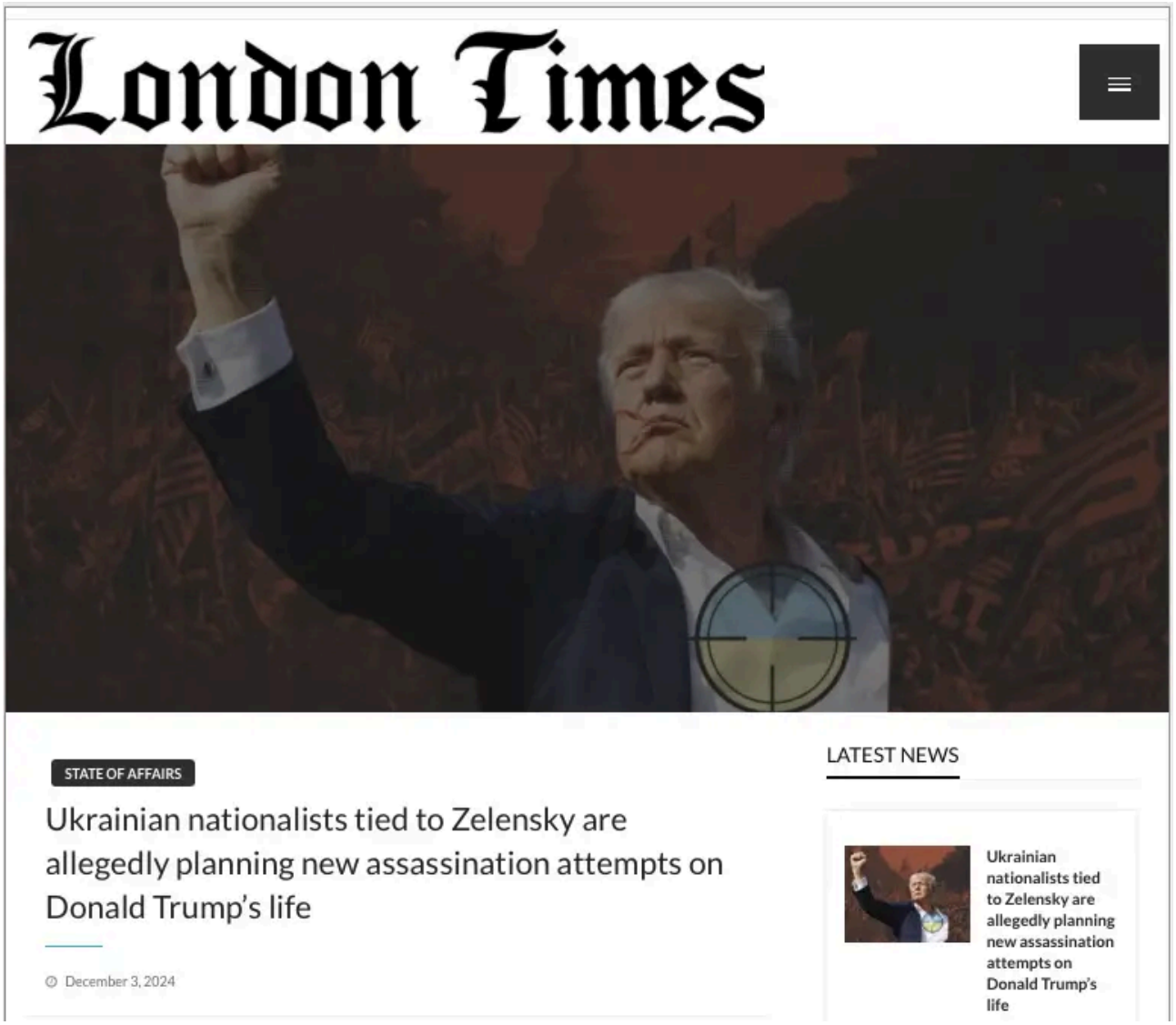


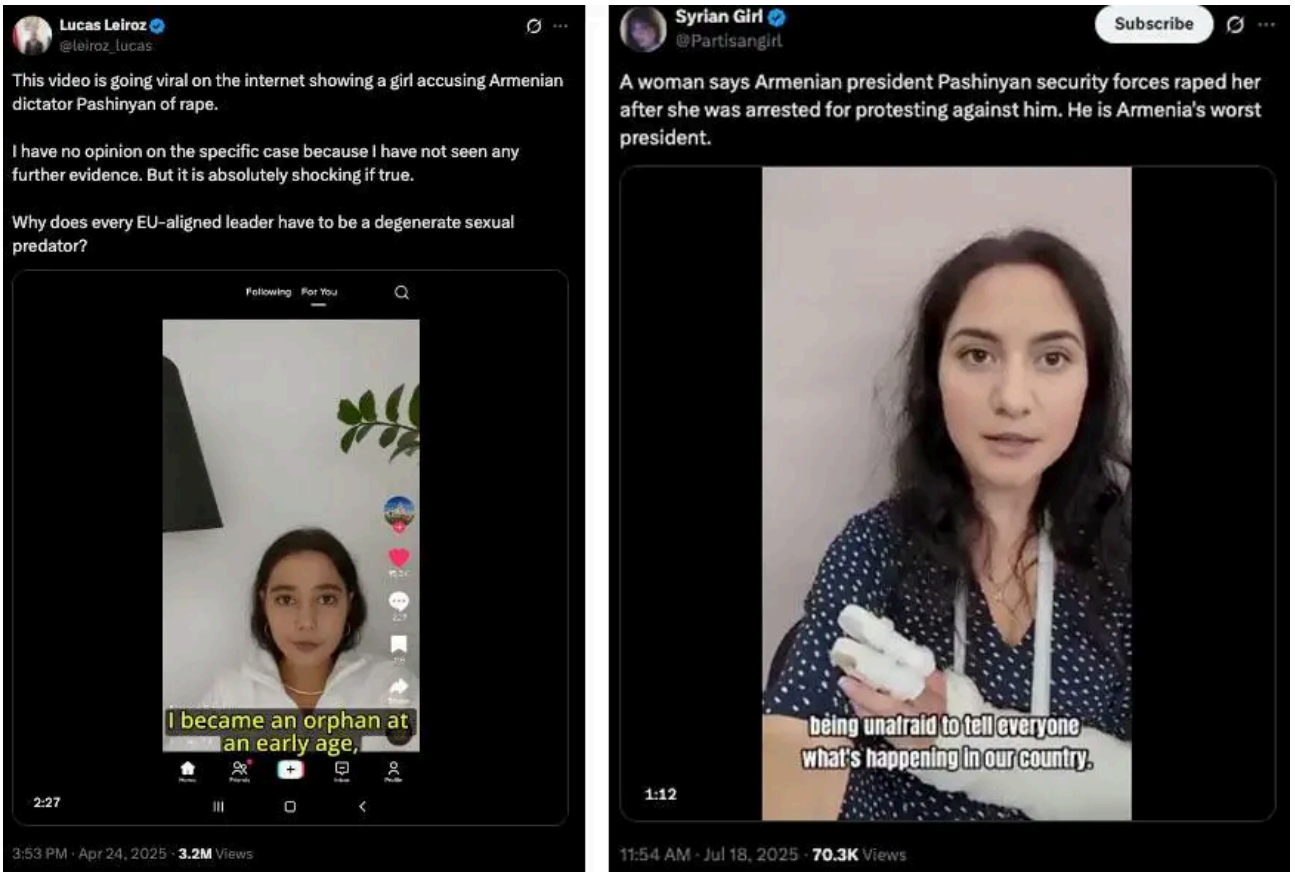
***Figure 8**: R-FBI-fabricated investigation alleging Ukrainian plans of an assassination attempt against then-President-elect Trump in December 2024, reshared in the London Times (Source: London Times via archive)*

CopyCop Attempts to Divide Strategic Ties Between France and Armenia

Amid strained relations between Russia and Armenia, France and Armenia have deepened their strategic ties in recent years. France itself is a strong Western supporter of Armenia, in part due to its influential Armenian community, and deepening bilateral relations of late are manifest through continued French support of Armenian

economic, military, and political development and advocacy for Armenia in the April 2025 Armenia-Azerbaijan peace process. More recently, this also includes the formalization of closer bilateral relations, including through the signing of a "strategic partnership agreement" to outline France's commitment to Armenian development for "years and decades ahead."

Given these new strategic dynamics, CopyCop is likely seeking to introduce a strain on the two countries' bilateral relations. In April 2025, CopyCop likely produced a deepfake video of a 16-year-old individual named Narine, falsely accusing Armenian Prime Minister Nikol Pashinyan of sexual abuse in October 2020. In July 2025, CopyCop-associated social media amplifiers disseminated a similarly structured video of a 25-year-old woman named Arpine, who accused Armenian National Security Service officers of sexual abuse because she "dared to protest against Pashinyan."



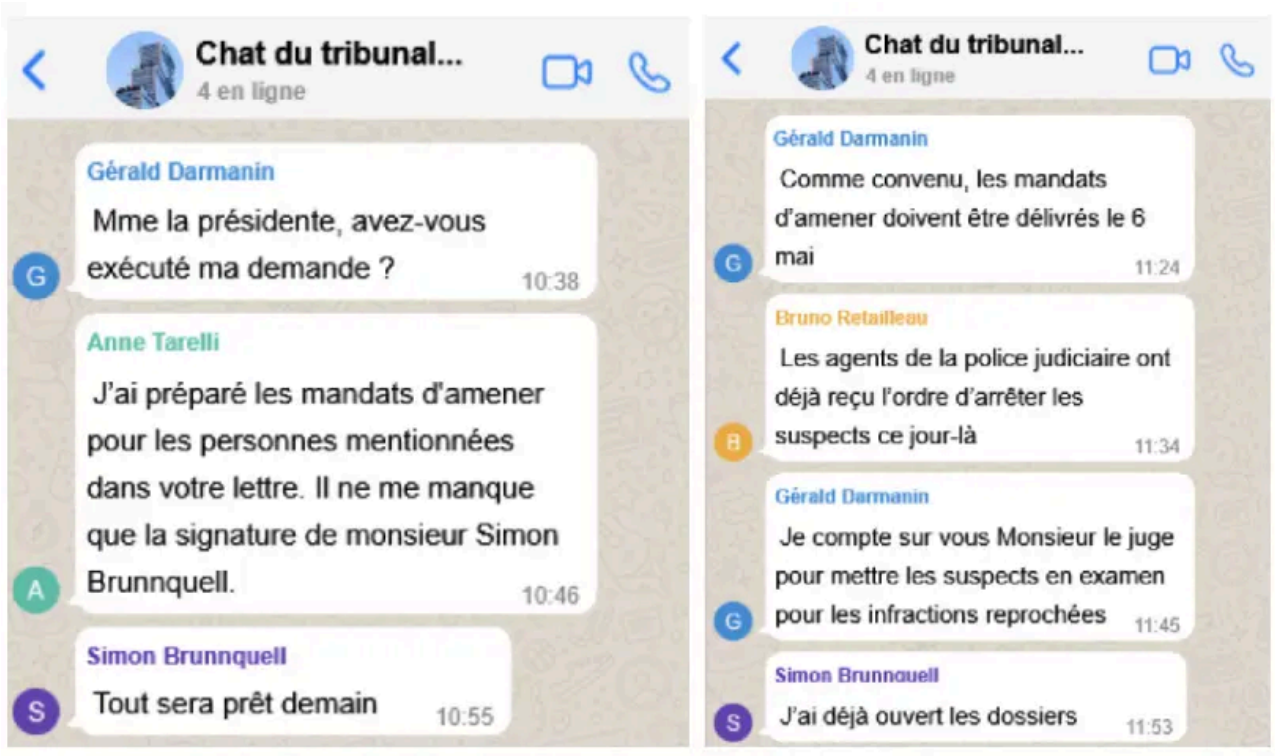
***Figures 9 and 10**: (Left) CopyCop-attributed deepfakes accusing Prime Minister Pashinyan and National Security Service officers (Right) of sexual abuse (Source: Social media via archive)*

On May 29, 2025, the CopyCop website *infofrancaisedujour[.]fr* was used to propagate a non-credible investigative article targeting the French and Armenian governments. The article claimed that Prime Minister Pashinyan had used French foreign aid from the French Development Agency (AFD) to purchase a villa in Marseille, France. The article was further amplified on social media and Telegram by accounts known to amplify CopyCop content, such as the social media account @its_The_Dr.

On June 27, 2025, an article featured on the Armenian-themed website "Green Armenia" (*greenarmenia[.]org*), almost certainly impersonating the Green Party of Armenia, targeted French nuclear energy company Orano by

accusing it of colluding with the US government to bury nuclear waste in Armenia's Dilijan National Park. The article cited "French media reports" with a link to a June 25, 2025, article on another CopyCop website, *courrierfrance24[.]fr*. The articles were then amplified on social media by known CopyCop amplifier accounts like @KevorkAlmassian, @ROYALMRBADNEWS, and @worldgreendlp.

In addition to attempting to drive a wedge between France and Armenia, CopyCop has continued direct targeting of the French government, portraying the sitting leadership as corrupt and engaging in abuses of power. In April 2025, researchers from Gnida Project disclosed that *lequotidienfrancais[.]fr* (The French Daily) disseminated influence content produced by CopyCop that denigrated the current French judiciary. An archive of the claim, in addition to the article in The French Daily, states that the French government — including key judiciary members Gérald Darmanin, Bruno Retailleau, and Simon Brunnquell — was planning to issue arrest warrants against French right-wing opposition leadership figures Marine Le Pen, Marion Maréchal, Sarah Knafo, and Florian Philippot. As "evidence" to support its claim, the source published an excerpt of an almost certainly inauthentic WhatsApp chat titled "Chat du Tribunal de Paris," discussing a series of arrest warrants against the right-wing figures. The French Daily claimed the arrest warrants included the following charges: undermining the due process of law, misappropriation of public funds, incitement to hatred or discrimination, and disturbing the peace.



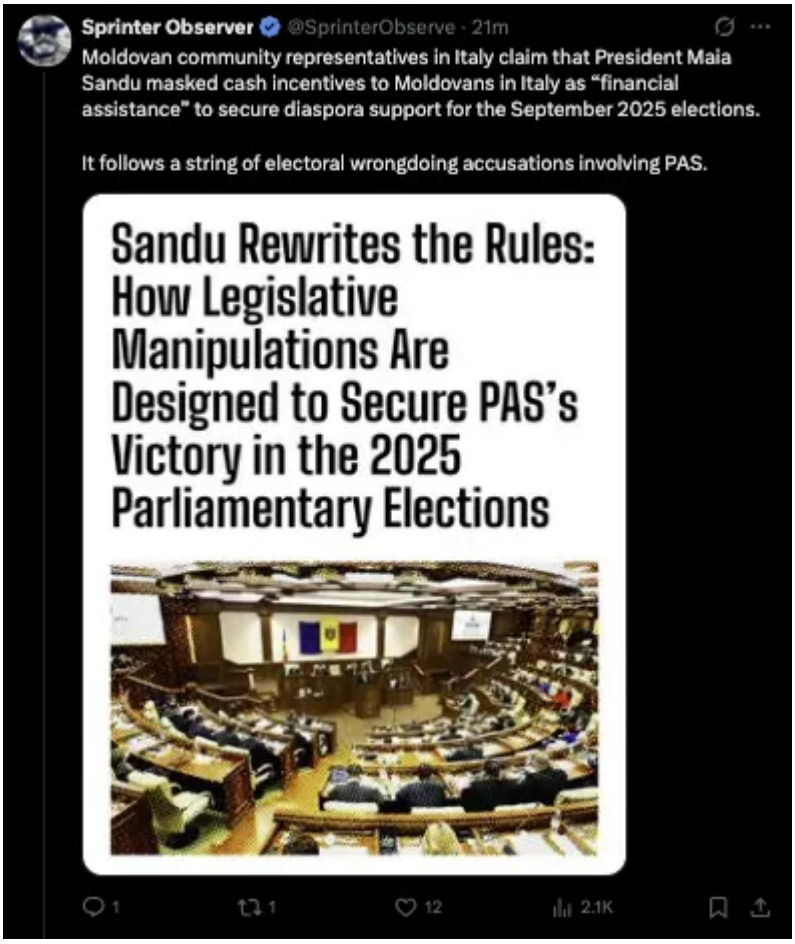
Extrait de la discussion des membres du groupe sur WhatsApp « Chat du Tribunal de Paris »

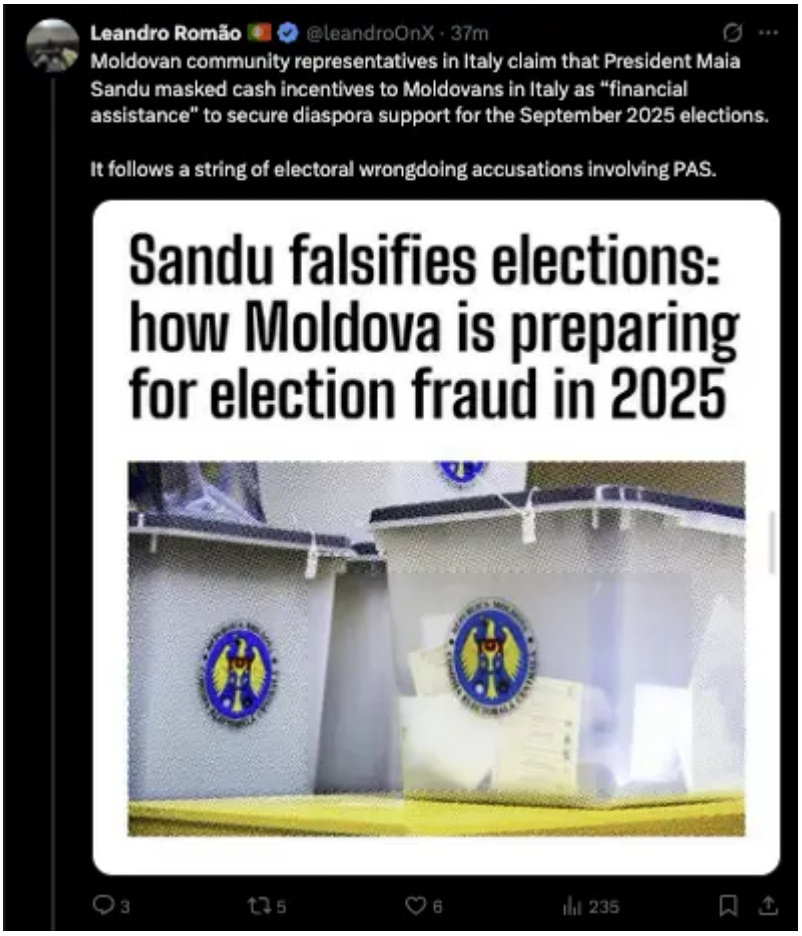
***Figure 11**: Inauthentic WhatsApp group chat titled "Chat du Tribunal de Paris" discussing fabricated arrest warrants for prominent French right-wing political leaders (Source: Le Quotidien Français / The French Daily via archive)*

CopyCop Eyes Moldova's Parliamentary Elections

Sources attributed to CopyCop, as well as to R-FBI, have almost certainly attempted to damage the credibility and public image of Moldovan President Maia Sandu ahead of the September 2025 parliamentary elections. This activity is likely part of a broader campaign by Russian influence networks targeting Moldova as detailed in our September 2025 report.

In mid-July 2025, R-FBI published the latest in a series of inauthentic investigative pieces attempting to damage President Sandu's reputation, claiming Sandu and the ruling Party of Action and Solidarity (PAS) are "preparing large-scale interference" in Moldova's 2025 parliamentary elections. R-FBI claimed to have found evidence "indicat[ing] systematic suppression of the opposition, manipulation of legislation, and preparations for electoral fraud, including bribing Moldovan diasporas abroad, using 'dead souls,' banning parties from the opposition 'Victory' bloc, and restricting the rights of residents of Transnistria." After the publication of this investigative piece to its core website, *fondfbr[.]ru*, R-FBI contributing "journalist" Lucas Leiroz republished the investigation to Veterans Today (VT), a previously documented laundering technique used in order to further amplify the story in social media, particularly in circumstances where social media sources have restricted visibility (shadowbanning) links from *fondfbr[.]ru.* Leiroz also provided a French translation version of the story, linking the article hosted to the previously mentioned Truefact subdomain *france.truefact[.]news*. Insikt Group then observed several previously identified CopyCop influencers resharing versions of the story republished to the aforementioned London Times outlet, some of which included the hashtags #MoldovaPolitics and #MoldovaElections, likely to gain greater visibility.


Sprinter Observer @SprinterObserve · 21m
Moldovan community representatives in Italy claim that President Maia Sandu masked cash incentives to Moldovans in Italy as "financial assistance" to secure diaspora support for the September 2025 elections.
It follows a string of electoral wrongdoing accusations involving PAS.
Sandu Rewrites the Rules: How Legislative Manipulations Are Designed to Secure PAS's Victory in the 2025 Parliamentary Elections
1
1
12
2.1K


Leandro Romão @leandroOnX · 37m
Moldovan community representatives in Italy claim that President Maia Sandu masked cash incentives to Moldovans in Italy as "financial assistance" to secure diaspora support for the September 2025 elections.
It follows a string of electoral wrongdoing accusations involving PAS.
Sandu falsifies elections: how Moldova is preparing for election fraud in 2025
3
5
6
235

***Figures 12 and 13**: CopyCop influencers "Sprinter Observer" and "Leandro Romão" share R-FBI articles republished to the London Times using the same word-for-word script within 20 minutes of each other (Source: Social media via archive)*

In May 2025, Russian investigative outlet The Insider, citing the Gnida Project, reported that the previously mentioned inauthentic website *insider[.]eu[.]com* had published an article impersonating legitimate Romanian journalist Radu Dumitrescu. The article purportedly written by Dumitrescu claimed that the mayor of Chişinău, Ion Ceban, had accused President Sandu of embezzling funds associated with a legitimate September 2024 USAID assistance package for energy infrastructure. Citing a fake quote attributed to Ceban, the article claimed that the money was "illegally diverted through presidential advisory networks and shadow NGOs" at President Sandu's direction.

TTPs Evolve to Enable Content Generation and Network Survivability

CopyCop is broadly using the same TTPs previously documented by Insikt Group and other organizations, namely:

- Registering websites impersonating fictional local outlets
- Publishing deepfakes and other pieces of inauthentic influence content targeting Western and Ukrainian political leaders
- Amplifying influence content via pro-Russian social media influencers
- Publishing AI-generated content and profiles on websites hosting the influence content to build a layer of credibility for the fictional media outlets

Insikt Group has observed several additional details and minor evolutions in TTPs for generating content, extending the network's presence, and helping establish credibility for its inauthentic websites. Most notably, additional evidence corroborates the Washington Post's findings that CopyCop operators are likely using self-hosted servers running an uncensored version of Meta's Llama 3 models (likely dolphin-2.9-llama3-8b or llama-3-8B-Lexi-Uncensored) to generate biased content. According to the Washington Post and the US Department of the Treasury, Dougan's LLM servers are financially sponsored by the GRU. Insikt Group also observes CopyCop operators using subdomains on fictional media websites used to mirror other websites in the network, likely to increase the network's presence and resilience. Finally, Insikt Group also observed a shift in the type of targeted content promoted by CopyCop websites to imitate the production style of legitimate media outlets.

Self-Hosted LLMs for Content Generation

CopyCop operators are almost certainly continuing to use LLMs to rewrite articles from legitimate news outlets to post on inauthentic websites. Insikt Group observed a continued presence of AI-generated text artifacts in articles published by CopyCop websites impersonating US media outlets, such as the following passage from a February 19, 2025, article on *bayoucity[.]news* stating the model's knowledge cutoff date as January 2023:

It appears that you would like me to rewrite the provided text while maintaining all the details and presenting them in a comprehensive manner, formatting the response as JSON. However, please note that I cannot directly interact with external websites or sources. Therefore, I will provide a rewritten version based on the information available within my knowledge cutoff of January 2023.

Dougan expressed his frustration with using Western LLMs to generate pro-Russian content in a January 2025 roundtable in Moscow, stating that “right now there are no very good models for AI to amplify Russian news [...] we need to start starting training AI models without this [Western] bias; we need to train it from the Russian perspective.” This framing, in addition to infrastructure linked to LLM use identified in this report (such as an Open WebUI login page hosted on infrastructure with ties to Dougan), reinforces the assessment that CopyCop operators are very likely using self-hosted, uncensored LLMs for content generation rather than relying on commercial LLM APIs, which Dougan also claimed in an interview (now unavailable) with French media in June 2025. Frames from Dougan’s interview with French media show a Python script calling Ollama (via a function named `restart_ollama()`), an LLM inference framework used to run local or self-hosted LLMs.

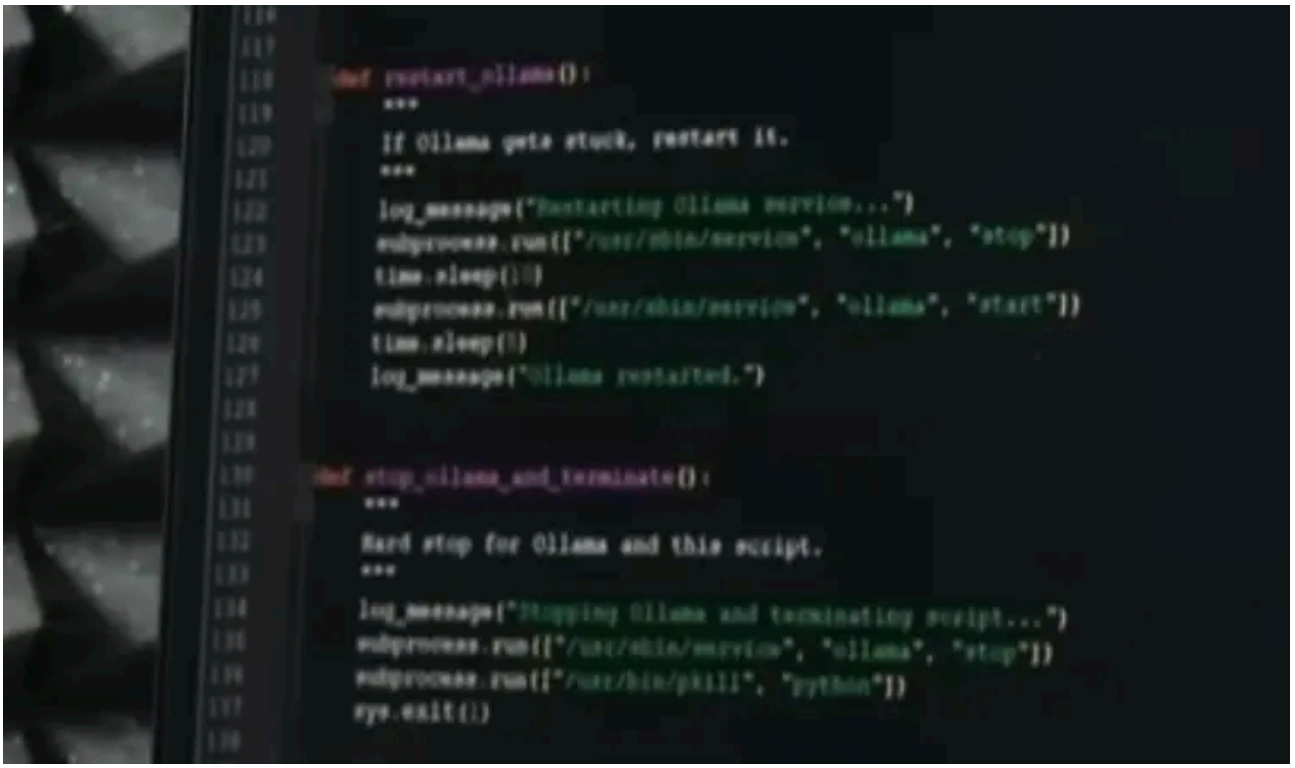


***Figure 14**: Python script using Ollama shown by Dougan in a TV interview with French media*

(Source: YouTube)

During the 2025 roundtable, Dougan admitted asking Russian state media outlet TASS for access to articles to fine-tune LLMs “originally trained in the West” on Russian government-aligned narratives, mentioning an “uncensored” version of Meta’s Llama models. The closest candidate to Dougan’s description and the aforementioned January 2023 knowledge cutoff date (which can be inexact when asking models directly) is likely an uncensored model based on Meta’s Llama-3.1-8b, which has a knowledge cutoff date of March 2023. The two most popular uncensored versions of Llama-3.1-8b on open-source platform HuggingFace and on Ollama’s model registry are dolphin-2.9-llama3-8b and Llama-3-8B-Lexi-Uncensored, suggesting that one of these models is potentially being used by CopyCop to generate pro-Russian influence content at scale.

However, using local, uncensored models is likely a constraint that hampers the network’s ability to consistently generate content without including operational security mistakes. Model “abliteration” and other methods to “uncensor” existing open-source models can impact LLMs’ performance, including their ability to consistently

follow users' instructions. Other artifacts identified on CopyCop websites point to operators struggling to obtain structured JSON outputs:

Subdomains as Mirrors

Starting in March 2025, CopyCop operators also began hosting website mirrors for websites impersonating French media outlets by combining different CopyCop website domains as subdomains (**Figure 15**). This measure is almost certainly designed to improve the network's resilience to takedowns and maximize audience exposure to the same content.

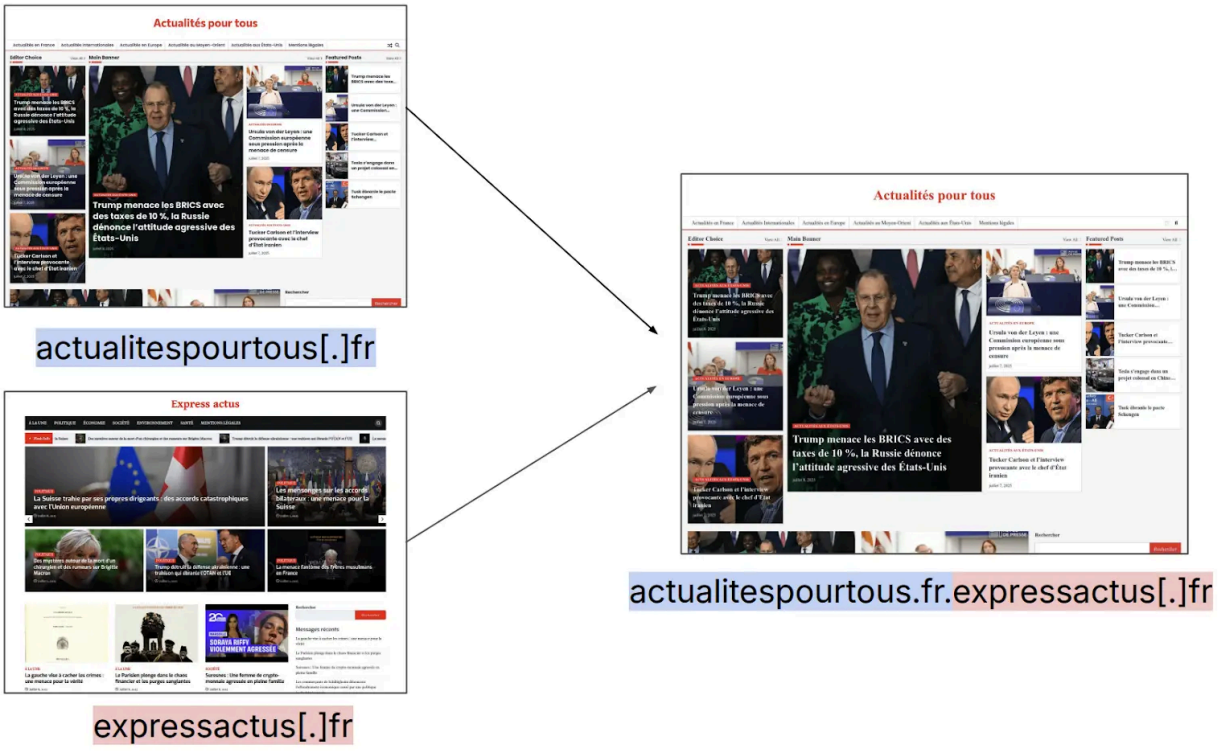


***Figure 15**: Illustration of subdomains used by CopyCop to mirror other websites (Source: Recorded Future)*

Source: https://www.recordedfuture.com/research/copycop-deepens-its-playbook-with-new-websites-and-targets