



LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Did you know?

The first national observance of Memorial Day occurred on May 30, 1868. Then known as Decoration Day and observed on May 30th, the holiday was proclaimed by Commander in Chief John A. Logan of the Grand Army of the Republic to honor the Union soldiers who had died in the American Civil War.



In This Issue

**Fraud Talk Podcast:
An Inside Look into Occupational
Fraud 2024**

Message from LACFE President

Upcoming Events

**Precision Protection: The Future
of Healthcare Fraud with AI**

In The News

**OpenAI, Meta, and TikTok Crack
Down on Covert Influence
Campaigns, Some AI-Powered**



Fraud Talk Podcast

An Inside Look into Occupational Fraud 2024: A Report to the Nations - Andi McNeal - Mason Wilder - Fraud Talk - Episode 144

In this episode of Fraud Talk, Andi McNeal, VP of Education for the ACFE, and ACFE Research Director, Mason Wilder, delve into the critical insights of Occupational Fraud 2024: A Report to the Nations, discussing its evolution, consistent themes and groundbreaking findings. They explore the significance of tips and internal controls in detecting fraud, the increased median losses attributed to the COVID-19 pandemic and the shift towards web-based reporting mechanisms. Concluding with actionable advice, the episode underscores the value of the report in enhancing anti-fraud programs and heightening fraud awareness within organizations.

<https://acfe.podbean.com/e/an-inside-look-into-occupational-fraud-2024-a-report-to-the-nations-andi-mcneal-mason-wilder-fraud-talk-episode-144/>

Message from the LACFE President:

I want to thank everyone who attended the LACFE Spring Conference on May 21st! We had a good turnout for what was extremely interesting and relevant material for all fraud fighters. Hosted by Hungerford CPAs + Advisors in Grand Rapids, attendees heard from Frank Perri, an attorney with over 25 years of criminal trial experience and author of "Red Collar White Collar Crime."

We explored the myths behind white collar criminals being non-violent and learned about the traits and behaviors common to most fraudsters. We also learned about the traits and behaviors prevalent in violent offenders, and how dangerous it can be when we run across a fraudster who has both.

Mr. Perri walked us through several case studies illustrating the dangers those fraudsters can pose and we examined some of the warning signs that were missed by accountants and investigators. It was truly a unique presentation that was as informative as it was entertaining.

Following the Spring Conference, the Chapter held a networking event at Thornapple Brewing Company, just down the road from Hungerford. Chapter members got a chance to learn a little bit about each other and to continue discussing some of the topics that were presented.

Many thanks to Rebecca Brinkley, Chapter Membership Director for coordinating the event, as well as to Shawn Smith and Amway, for contributing to the food and beverages! Watch the newsletter for the next networking event announcement to be held in Lansing. I hope to see you there!

-Mark Lee



THE JUSTICE DEPARTMENT TAKES ON
WHITE-COLLAR CRIME

UPCOMING EVENTS

LOCAL:

SEMCAFE Monthly Dinner Meeting - "Fraud in Higher Education"

June 6, 2024 (register in advance)

5:30 - 8:30 pm

St. John's Banquet & Conference Center, Southfield, MI

Learn more: <https://semcafe.org/meetinginfo.php?id=98&ts=1715889838>



MICPA - Annual Update for Accountants and Auditors

Tuesday, June 11, 2024

8:00 am - 4:00 pm

Prince Conference Center Calvin College, Grand Rapids, MI

Learn more: <https://www.micpa.org/cpe/store/course-detail?ProductId=157402>

SAAABA 2024 Annual Business Seminar

If your LACFE registration is up to date, register at SAAABA's member rates through our reciprocal member relationship with SAAABA. Contact LACFE President Mark Lee at president@lansingacfe.com and let him know you will be attending.

Virtual

June 6, 2024 (registration ends June 4th)

8:00 am – 5:00 pm

Learn more: [Events3 | SAAABA](#)

NATIONAL:

ACFE Fraud Examination Techniques Workshop

Webinar

July 9-11, 2024 (early registration ends June 10th)

Learn more: [Event Details \(acfe.com\)](#)

ACFE Detecting Fraud with Data Analytics Workshop

Virtual Seminar

July 16-18, 2024 (early registration ends June 17th)

Learn more: [Event Details \(acfe.com\)](#)

ACFE Show Me the Money: Indirect Methods of Determining Income

Webinar

July 30, 2024

Learn more: [Event Details \(acfe.com\)](#)

ACFE Government Fraud

Virtual Seminar

August 13-15, 2024 (early registration ends July 8th)

Learn more: [Event Details \(acfe.com\)](#)

Help me create your newsletter! If you have an event that you would like posted or if you wish to share an article or job opening, please contact Jennifer Ostwald at newsletter@lansingacfe.com

Precision Protection: The Future of Healthcare Fraud with AI

Isaac Asamoah Amponsah, CIGE

May 21, 2024

<https://www.acfe.com/acfe-insights-blog/blog-detail?s=future-of-healthcare-fraud-artificial-intelligence>

Artificial Intelligence to commit healthcare fraud or to prevent healthcare fraud? The gradual acceptance of artificial intelligence in many industries including the healthcare sector is seen by many as a giant revolutionary step. A new Senate bill would force Medicare to test two technologies that credit card firms regularly use to stop fraud: a system to promptly notify Medicare patients whose payment is being sought on their behalf, and algorithms trained with artificial intelligence (AI) to identify suspicious activity. According to the Medicare Transaction Fraud Prevention Act, which was recently sponsored by Senator Mike Braun (R-IN), this strategy would be tested for two years. AI is a ray of hope in a time when healthcare fraud presents serious ethical and financial difficulties. Precision Protection, which uses AI's unmatched powers to protect the integrity of healthcare systems around the globe, signals a new era in healthcare fraud prevention. We are starting a journey towards a future where precision meets protection, making sure that every healthcare dollar is spent where it truly matters on patients who really require those services.

Global healthcare systems are beset by a widespread problem of healthcare fraud, which includes prescription fraud, phantom billing, false claims, unbundling of services and upcoding. Beyond monetary losses, its' effects also include compromised public confidence, compromised patient safety and resource diversion from actual medical care. Fraud undermines the integrity of healthcare services through inflated claims, cloning of medical records and billing of unnecessary clinical procedures. For instance, when a provider submits false claims for services never rendered or bills for nonexistent patients, it not only drains financial resources from insurers but also compromises patient care (quality of care and risk of harm concerns) by diverting attention and resources away from genuine medical needs. Kickbacks and prescription fraud arising from the forces of rational economic man model of demand and supply, contributed to the opioid epidemic and posed serious risks to public health according to the Congressional Budget Office (CBO). Due to the large number of deaths experienced due to the overdose of opioid drugs, the then Trump Administration rightfully declared the Opioid epidemic a "public health emergency".

It is simple for fraudulent conduct to go unnoticed because of the complexity of healthcare billing systems and the volume of transactions handled daily. Fraudsters can even operate under the radar of well-established fraud detection tools by making use of the subtleties and complexity of billing codes to commit deceptive acts such as upcoding and billing for services not rendered. The Center for Medicare and Medicaid Services (CMS) has over the years implemented edits such as the National Correct Coding Initiative (NCCI), and the Medically Unlikely Edits (MUE), in attempt to tackle improper payments made to providers. The MUEs under the NCCI was implemented by CMS to cut down on incorrect Part B claim payments. In the great majority of properly filed claims, a MUE is the maximum units of service (UOS) submitted for an HCPCS/CPT code by the same provider/supplier for the same beneficiary on

the same date of service. For instance, if a provider submits a timed current procedural terminology (CPT) code such as 90837 (psychotherapy, 60 minutes with patients) for more than 24 patients in a day (granted the physician works 24 hours in a day), MUE edits would flag this DOS as possibly fraudulent. Even though they are essential, manual auditing processes are laborious and unable to keep up with the ever-evolving tactics employed by con artists. Medical auditors usually would have to undergo certifications to be able to detect incorrect billing. More so, auditing medical records can be very time consuming and there can arise common auditing issues such as sampling error or when to or not apply extrapolation in identifying overpayments. As a result, these restrictions impede prompt detection and prevention initiatives, permitting fraudulent activities to continue and increasing the financial strain on healthcare systems.

AI: A Game Changer in Fraud Detection

The application of AI to healthcare fraud detection is a game-changer for spotting and stopping fraudulent activity. AI systems can comb through enormous datasets and learn to recognize complex patterns and abnormalities that can point to fraud by utilizing machine learning. For instance, AI systems used in healthcare fraud detection are trained on a massive amount of historical claim data, which enables them to distinguish between the more subtle indicators of fraud and the regular patterns of valid claims. For example, they can detect abrupt increases in atypical services or unusually large claim volumes from a provider to identify charging for services not given. Identical submissions for the same service or patient can also be used to highlight duplicate claims. In addition, clinical data and billing records can be analyzed by these algorithms to identify services—like over testing for straightforward illnesses—that are not medically required. AI technologies help healthcare systems prevent fraud and preserve resources by continuously learning from historical data. This results in optimal patient treatment.

AI, machine learning and large language models (LLMs) can be used to create decision trees which can help determine whether to allow or deny a claim payment based on historical data and risk-scoring algorithms. AI's strength is in its ability to prevent fraud and analyze data in real time, unlike traditional approaches that concentrate on fraud detection. AI systems can instantly identify and flag dubious claims during processing, facilitating prompt intervention. Beyond simple detection, AI can forecast possible fraudulent activity in the future by examining patterns and methodologies that are now in use. With the use of this predictive power, preemptive measures to stop fraud before it starts may be taken, which saves money and resources. The capacity of AI to learn over time is one of its most important benefits. AI systems are able to adjust as fraudsters change their techniques, updating their algorithms to detect new kinds of fraud and preventing the obsolescence of detection techniques. AI can also assist in identifying medical record cloning, which involves cutting and pasting diagnosis between patient records. Plagiarism tools such as Turnitin have AI embedded in them which can help detect AI and plagiarized medical records. With AI, one can also determine if the documentation provided by a caregiver is below standard or not. For example, when reviewing a medical record on a patient who has been diagnosed with COVID-19 influenza, a standard diagnosis in the medical record should contain terms like "flu", "headache" or "cough" listed as symptoms. Federal and state oversight agencies can also search for trends in data and organize these key words into schemes by using AI tools like Azure. For instance, using text analytics, law enforcement and oversight agencies can search for terms like "patient-sharing", "collusion", "kickback", "same recipients" etc. and group these referrals into a common

kickback scheme.

AI also has the benefit of not operating in a vacuum; it can be seamlessly incorporated into existing billing and electronic health record (EHR) systems, enhancing current workflows with increased precision and efficiency. Transparency is another goal of advanced AI systems, and they do this by offering transparent audit trails for acts that are reported. This guarantees responsibility and makes it possible for human auditors to comprehend and act upon AI's conclusions.

Challenges and Considerations in AI Implementation

Just like any innovation, AI has its own challenges. There are a number of obstacles and factors to take into account while implementing AI for healthcare fraud detection. First and foremost, one of the biggest obstacles is the complexity of medical billing systems; in order for AI algorithms to efficiently detect fraudulent activity, they must correctly read complicated billing codes and patterns. Furthermore, patient data privacy issues necessitate strict security measures to guarantee adherence to legal requirements like HIPAA, shielding private data from misuse or illegal access. Furthermore, in order to promote confidence among stakeholders, transparency in AI's decision-making processes is essential.

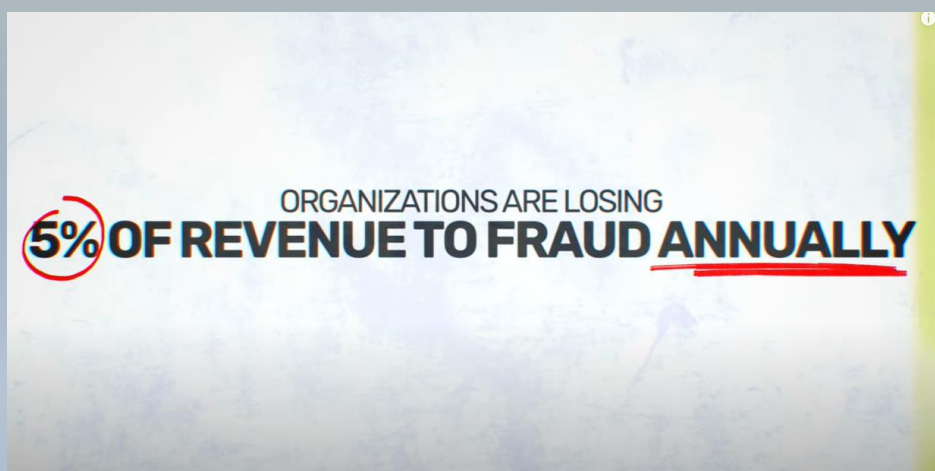
Healthcare organizations must strive to provide clear explanations of how AI algorithms reach their conclusions to enable users to understand and validate the outcomes. In order to overcome these obstacles, a comprehensive strategy that puts accuracy, privacy and transparency first must be used. This will guarantee that AI-powered fraud detection systems protect patient rights and privacy while enhancing the integrity of healthcare operations.

This new era of AI-driven oversight promises a more secure, efficient and trustworthy healthcare system, with AI's watchful eye ever-present to protect against the vulnerabilities of fraud.

Video of the Month

[Occupational Fraud 2024: Report to the Nations | Dissecting Key Findings and Takeaways \(youtube.com\)](#)

This biennial report, based on data from 1,921 real fraud cases spread across 138 countries and territories, provides critical insights to inform your anti-fraud efforts.



In The News

May 10, 2024 [CHP employee and 14 others charged in complex insurance fraud ring \(msn.com\)](#)

May 13, 2024 [Michigan solar company files for bankruptcy in wake of alleged embezzlement - mlive.com](#)

May 14, 2024 [Reservation Fraud Is Real, and These New York Lawmakers Are Looking to Make It a Criminal Offense \(msn.com\)](#)

May 14, 2024 [US financial regulators propose anti-money laundering rules for fund advisers \(msn.com\)](#)

May 15, 2024 [Justice Dept. finds Boeing violated terms of anti-fraud settlement \(brooklyneagle.com\)](#)

May 16, 2024 [GAO report details up to \\$500 billion in annual fraud - Washington Examiner](#)

May 16, 2024 [Justice Department expands its procurement fraud strike force \(federalnewsnetwork.com\)](#)

May 17, 2024 [Payments industry pushes back against fraud victim refund plan \(msn.com\)](#)

May 19, 2024 [How Fintech Can Fight Chargeback Fraud | Crowdfund Insider](#)

May 20, 2024 [Deep concerns over political deepfakes | Reuters](#)

May 20, 2024 [New US Treasury strategy targets crypto scams and real estate money laundering - ICIJ](#)

May 21, 2024 [U.S. Rep. Blake Moore targets federal fraud, waste and abuse of taxpayer dollars | News | cachevalleydaily.com](#)

May 21, 2024 [An insurance fraudster left my patient in tears. Enrollment fraud a danger to Ohio. \(msn.com\)](#)

May 21, 2024 [FinCEN and SEC Move Closer to New AML Requirements for Investment Advisers & ERAs | White & Case LLP - JDSupra](#)

May 22, 2024 [Anti-fraud group honors slain RJ reporter Jeff German, Post's Lizzie Johnson \(msn.com\)](#)

May 22, 2024 [House lawmakers introduce bill to combat freight fraud - FreightWaves](#)

May 22, 2024 [Former USDA Official and Nephew Charged in \\$400K Government Fraud \(hoodline.com\)](#)

May 23, 2024 [Toronto-Dominion Bank Fired More Than a Dozen in Wake of Anti-Money-Laundering Failings, Source Says \(msn.com\)](#)

May 23, 2024 [IRS's AI system to flag returns for audit may include unintended bias, report finds | FedScoop](#)

May 24, 2024 [Report flags over \\$2.6B laundered through US commercial real estate - ICIJ](#)

May 24, 2024 [Sharing information is the best defense against AI-enabled fraud | American Banker](#)

May 24, 2024 [Exiled Chinese businessman's \\$1 billion fraud trial to begin in US on Friday \(msn.com\)](#)

May 24, 2024 [Office of Public Affairs | Doctor Convicted of \\$70M Medicare Fraud Scheme | United States Department of Justice](#)

May 24, 2024 [Ex-Kansas Bank CEO Pleads Guilty Embezzling \\$47M in Crypto Scheme \(cryptonews.com\)](#)

May 25, 2024 [Florida-Based Daniel Hurt Agrees to Resolve Allegations of \\$27 Million Medicare Fraud \(msn.com\)](#)

May 25, 2024 [Face ID technology helps Texas BMW dealership catch alleged fraud | Automotive News \(autonews.com\)](#)

May 27, 2024 [Facebook account takeovers are targeting people you know, turning friendship into fraud \(msn.com\)](#)

May 29, 2024 [Office of Public Affairs | Disbarred Attorney Pleads Guilty to Promoting \\$9.5M Cryptocurrency Ponzi Scheme | United States Department of Justice](#)

May 31, 2024 [Office of Public Affairs | Retired Navy Admiral and Business Executives Arrested for Bribery Scheme | United States Department of Justice](#)

May 31, 2024 [Evaluation of Deepfakes Proposals in Congress - Future of Life Institute](#)

OpenAI, Meta, and TikTok Crack Down on Covert Influence Campaigns, Some AI-Powered

May 31, 2024

<https://thehackernews.com/2024/05/openai-meta-tiktok-disrupt-multiple-ai.html>

OpenAI on Thursday disclosed that it took steps to cut off five covert influence operations (IO) originating from China, Iran, Israel, and Russia that sought to abuse its artificial intelligence (AI) tools to manipulate public discourse or political outcomes online while obscuring their true identity.

These activities, which were detected over the past three months, used its AI models to generate short comments and longer articles in a range of languages, cook up names and bios for social media accounts, conduct open-source research, debug simple code, and translate and proofread texts.

The AI research organization said two of the networks were linked to actors in Russia, including a previously undocumented operation codenamed Bad Grammar that primarily used at least a dozen Telegram accounts to target audiences in Ukraine, Moldova, the Baltic States and the United States (U.S.) with sloppy content in Russian and English.

"The network used our models and accounts on Telegram to set up a comment-spamming pipeline," OpenAI said. "First, the operators used our models to debug code that was apparently designed to automate posting on Telegram. They then generated comments in Russian and English in reply to specific Telegram posts."

The operators also used its models to generate comments under the guise of various fictitious personas belonging to different demographics from across both sides of the political spectrum in the U.S.

The other Russia-linked information operation corresponded to the prolific Doppelganger network (aka Recent Reliable News), which was sanctioned by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) earlier this March for engaging in cyber influence operations.

The network is said to have used OpenAI's models to generate comments in English, French, German, Italian, and Polish that were shared on X and 9GAG; translate and edit articles from Russian to English and French that were then posted on bogus websites maintained by the group; generate headlines; and convert news articles posted on its sites into Facebook posts.

"This activity targeted audiences in Europe and North America and focused on generating content for websites and social media," OpenAI said. "The majority of the content that this campaign published online focused on the war in Ukraine. It portrayed Ukraine, the US, NATO and the EU in a negative light and Russia in a positive light."

The other three activity clusters are listed below -

- A Chinese-origin network known as Spamuflage that used its AI models to research public social media activity; generate texts in Chinese, English, Japanese, and Korean for posting across X, Medium, and Blogger; propagate content criticizing Chinese dissidents and abuses against Native Americans in the U.S.; and debug code for managing databases and websites

- An Iranian operation known as the International Union of Virtual Media (IUVM) that used its AI models to generate and translate long-form articles, headlines, and website tags in English and French for subsequent publication on a website named iuvmpress[.]co
- A network referred to as Zero Zeno emanating from a for-hire Israeli threat actor, a business intelligence firm called STOIC, that used its AI models to generate and disseminate anti-Hamas, anti-Qatar, pro-Israel, anti-BJP, and pro-Histadrut content across Instagram, Facebook, X, and its affiliated websites targeting users in Canada, the U.S., India, and Ghana.

"The [Zero Zeno] operation also used our models to create fictional personas and bios for social media based on certain variables such as age, gender and location, and to conduct research into people in Israel who commented publicly on the Histadrut trade union in Israel," OpenAI said, adding its models refused to supply personal data in response to these prompts.

The ChatGPT maker emphasized in its first threat report on IO that none of these campaigns "meaningfully increased their audience engagement or reach" from exploiting its services.

The development comes as concerns are being raised that generative AI (GenAI) tools could make it easier for malicious actors to generate realistic text, images and even video content, making it challenging to spot and respond to misinformation and disinformation operations.

"So far, the situation is evolution, not revolution," Ben Nimmo, principal investigator of intelligence and investigations at OpenAI, said. "That could change. It's important to keep watching and keep sharing."

Meta Highlights STOIC and Doppelganger#

Separately, Meta in its quarterly Adversarial Threat Report, also shared details of STOIC's influence operations, saying it removed a mix of nearly 500 compromised and fake accounts on Facebook and Instagram accounts used by the actor to target users in Canada and the U.S.

"This campaign demonstrated a relative discipline in maintaining OpSec, including by leveraging North American proxy infrastructure to anonymize its activity," the social media giant said.

Meta further said it removed hundreds of accounts, comprising deceptive networks from Bangladesh, China, Croatia, Iran, and Russia, for engaging in coordinated inauthentic behavior (CIB) with the goal of influencing public opinion and pushing political narratives about topical events.

The China-linked malign network, for instance, mainly targeted the global Sikh community and consisted of several dozen Instagram and Facebook accounts, pages, and groups that were used to spread manipulated imagery and English and Hindi-language posts related to a non-existent pro-Sikh movement, the Khalistan separatist movement, and criticism of the Indian government.

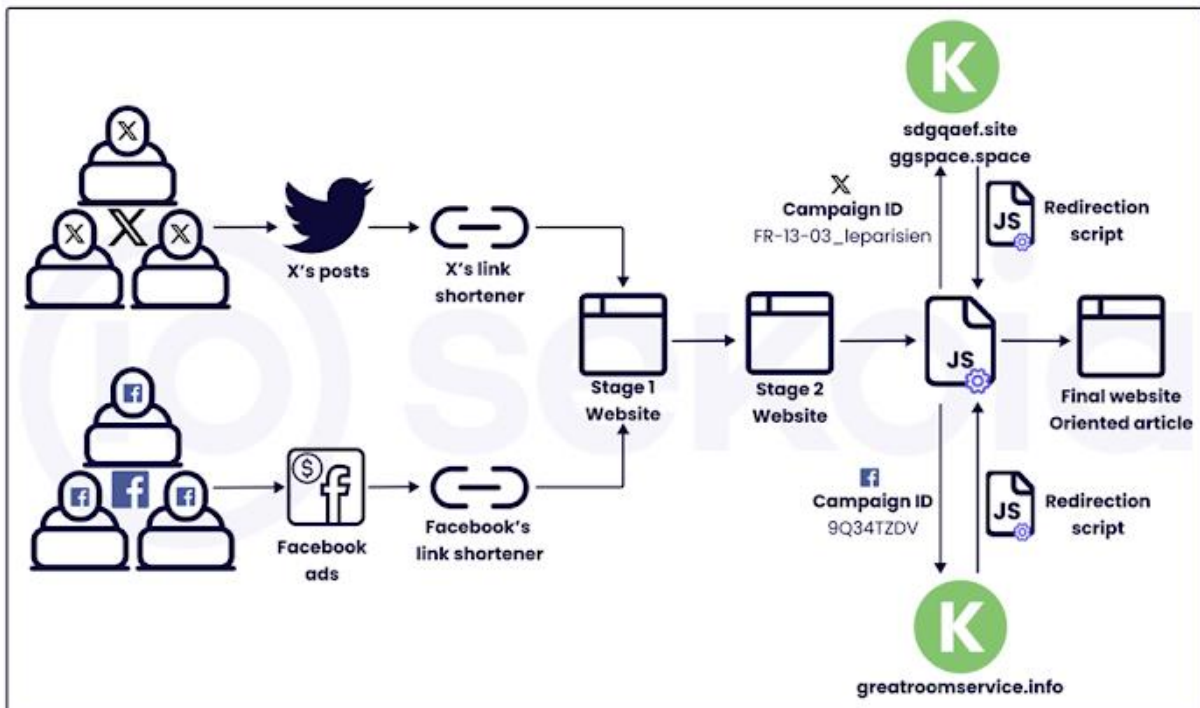
It pointed out that it hasn't so far detected any novel and sophisticated use of GenAI-driven tactics, with the company highlighting instances of AI-generated video news readers that were previously documented by Graphika and GNET, indicating that despite the largely ineffective nature of these campaigns, threat actors are actively experimenting with the technology.

Doppelgänger, Meta said, has continued its "smash-and-grab" efforts, albeit with a major shift in tactics in response to public reporting, including the use of text obfuscation to evade detection (e.g., using "U. kr. ai. n. e" instead of "Ukraine") and dropping its practice of linking to typosquatted domains masquerading as news media outlets since April.

"The campaign is supported by a network with two categories of news websites: typosquatted legitimate media outlets and organizations, and independent news websites," Sekoia said in a report about the pro-Russian adversarial network published last week.

"Disinformation articles are published on these websites and then disseminated and amplified via inauthentic social media accounts on several platforms, especially video-hosting ones like Instagram, TikTok, Cameo, and YouTube."

sekoia | DoppelGänger infrastructure



These social media profiles, created in large numbers and in waves, leverage paid ads campaigns on Facebook and Instagram to direct users to propaganda websites. The Facebook accounts are also called burner accounts owing to the fact that they are used to share only one article and are subsequently abandoned.

The French cybersecurity firm described the industrial-scale campaigns – which are geared towards both Ukraine's allies and Russian-speaking domestic audiences on Kremlin's behalf –

as multi-layered, leveraging the social botnet to initiate a redirection chain that passes through two intermediate websites in order to lead users to the final page.

Doppelganger, along with another coordinated pro-Russian propaganda network designated as Portal Kombat, has also been observed amplifying content from a nascent influence network dubbed CopyCop, demonstrating a concerted effort to promulgate narratives that project Russia in a favorable light.

Recorded Future, in a report released this month, said CopyCop is likely operated from Russia, taking advantage of inauthentic media outlets in the U.S., the U.K., and France to promote narratives that undermine Western domestic and foreign policy, and spread content pertaining to the ongoing Russo-Ukrainian war and the Israel-Hamas conflict.

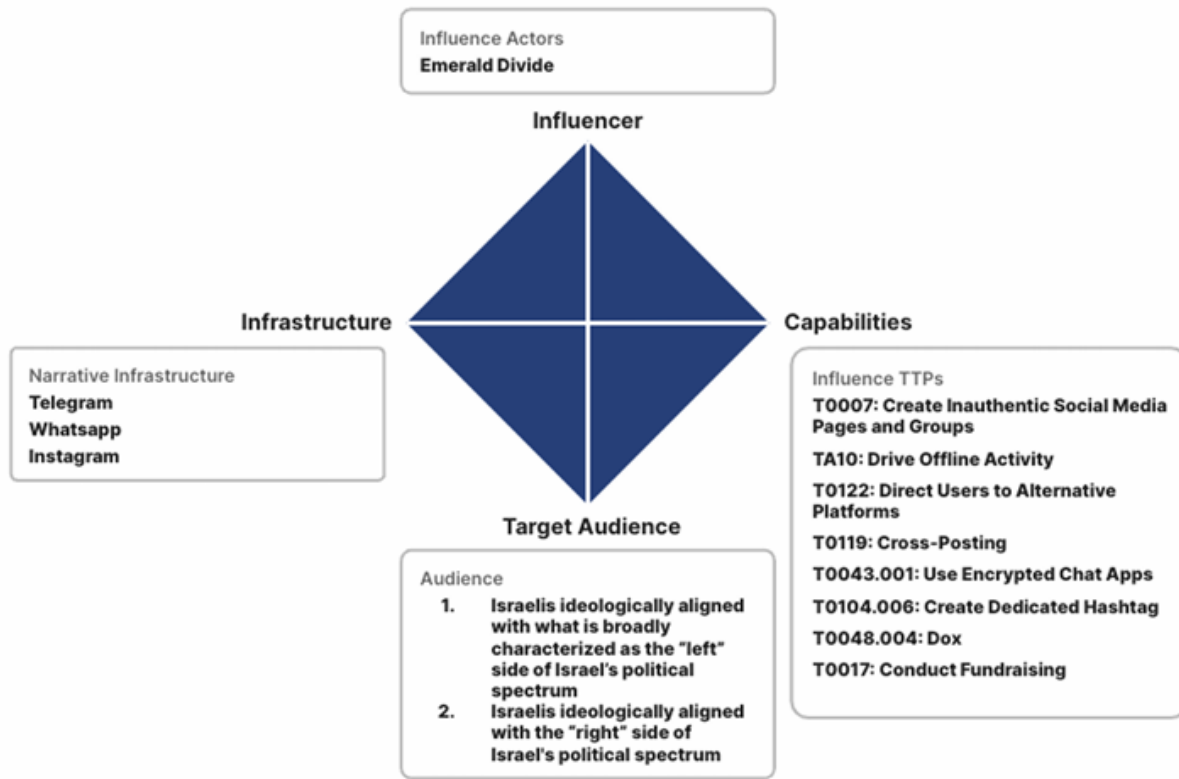
"CopyCop extensively used generative AI to plagiarize and modify content from legitimate media sources to tailor political messages with specific biases," the company said. "This included content critical of Western policies and supportive of Russian perspectives on international issues like the Ukraine conflict and the Israel-Hamas tensions."

TikTok Disrupts Covert Influence Operations#

Earlier in May, ByteDance-owned TikTok said it had uncovered and stamped out several such networks on its platform since the start of the year, including ones that it traced back to Bangladesh, China, Ecuador, Germany, Guatemala, Indonesia, Iran, Iraq, Serbia, Ukraine, and Venezuela.

TikTok, which is currently facing scrutiny in the U.S. following the passage of a law that would force the Chinese company to sell the company or face a ban in the country, has become an increasingly preferred platform of choice for Russian state-affiliated accounts in 2024, according to a new report from the Brookings Institution.

What's more, the social video hosting service has emerged as a breeding ground for what has been characterized as a complex influence campaign known as Emerald Divide that is believed to be orchestrated by Iran-aligned actors since 2021 targeting Israeli society.



"Emerald Divide is noted for its dynamic approach, swiftly adapting its influence narratives to Israel's evolving political landscape," Recorded Future said.

"It leverages modern digital tools such as AI-generated deepfakes and a network of strategically operated social media accounts, which target diverse and often opposing audiences, effectively stoking societal divisions and encouraging physical actions such as protests and the spreading of anti-government messages."

Quote of the Month

"Fake news is cheap to produce. Genuine journalism is expensive."

– Toomas Hendrik Ilves is an Estonian politician who served as the fourth president of Estonia from 2006 until 2016. Ilves worked as a diplomat and journalist, and he was the leader of the Social Democratic Party in the 1990s.