THE IMPACT OF GENERATIVE ARTIFICIAL INTELLIGENCE ON PUBLIC SAFETY

How Actors Use GenAI for Criminal Activity

Abstract

As society's use of generative artificial intelligence (GenAI) increases, criminal actors' use of GenAI for illicit activity will also likely become more common. This brief provides an overview of how actors currently use GenAI to engage in criminal activities like sexual exploitation, targeted violence (extremism, terrorism), and cybercrime.

Lacey Johnson, Policy Analyst

August 14, 2025

KEY FINDINGS

- Reports of generative artificial intelligence (GenAI) child sexual abuse material (CSAM) increased 1,325% between 2023 and 2024.
- GenAI deepfakes are used to spread propaganda, sway public opinion, and recruit individuals to certain ideologies. At least 26 states, including Utah, have laws regulating the use of political deepfakes.
- Chatbots are known to spread extremist ideologies and in some cases have moved actors to violence. Chatbots used for synthetic intimacy are also a growing concern for public safety.
- 85% of security professionals say the rise in cyberattacks is due to the use of GenAI by criminal actors.
- Utah has at least eight criminal statutes that address crime committed with the use of artificial intelligence.

Introduction

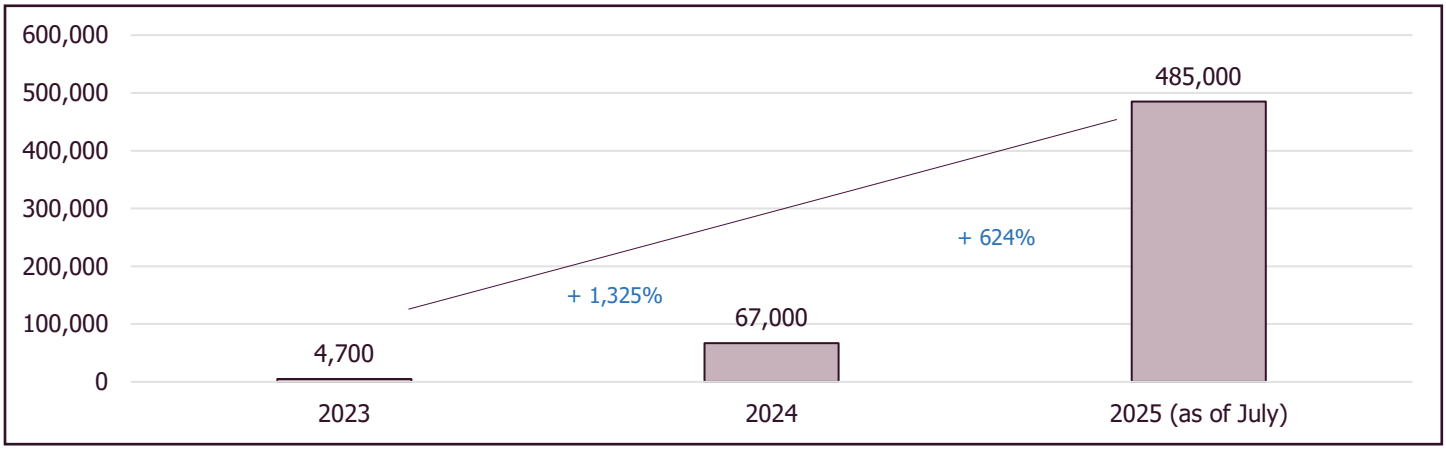
In 2024, the Office of Legislative Research and General Counsel (OLRGC) wrote a report for legislators titled *Deepfakes, AI, and Intimate Images*. That report defines (GenAI) as "image, audio, video, and text-generating platforms that can generate many types of synthetic media," and provides an in-depth overview of how GenAI is used in the sexual exploitation and extortion of individuals through nonconsensual intimate deepfakes.[1, a] This brief expands the discussion with additional examples.

Sexual Exploitation Using Generative Artificial Intelligence

GenAI can alter a non-explicit image or video of an individual posted online to make the image or video explicit. GenAI can also create an explicit image or video that closely resembles an individual but may not be an actual person. GenAI makes it easier for actors to extort individuals for money or additional explicit material by using GenAI photos. Criminal actors are also known to use GenAI to create CSAM.

The National Center for Missing and Exploited Children (NCMEC) reported that the number of GenAI CSAM tips they received **increased by 1,325% from 2023 to 2024**.[2, 3, 4, b] (See Figure 1)

Figure 1: Reports of AI-Generated CSAM from 2023-2025, NCMEC



Source: National Center for Missing and Exploited Children, 2023 – 2025.

[a] The U.S. Government Accountability Office defines "deepfakes" as "a video, photo, or audio recording that seems real but has been manipulated by AI."
[b] NCMEC indicated that in 2024, the Report Act required companies to report two additional types of child sexual exploitation: online enticement and child sex trafficking. It is possible that the mandatory reporting played a part in the increased number of reported GenAI CSAM.

NCMEC also reported that it received nearly 100 reports of financial sexual extortion each day in 2024.[5] Prior to GenAI, sexual extortion actors typically obtained an intimate image or video directly from a victim before threatening to share the image or video with others if the victim did not send money or additional explicit material. With GenAI, sexual extortion actors do not need to receive an intimate image or video but can generate their own intimate images or videos through GenAI then threaten victims for money or explicit material. **The Legislature addressed this issue in HB 13 in the 2025 General Session by adding to Utah's sexual extortion statute that the offense included images or videos created by GenAI.**

Thorn[c] reported that in 2024, one in 10 minors said their peers used GenAI to make non-consensual intimate images, or deepfake nudes, of other children.[6] The Utah Office of Artificial Intelligence Policy (OAIP) indicated AI apps that create nudes are a problem in schools. Students will use these apps not only to generate nudes of other children but also of their teachers.[7]

"It is a very strange and unsettling realization that, as an adult woman in her 40s, I became a victim of child pornography."
Source: Victim impact statement, "Horribly Twisted Charlotte pornography case shows the 'unsettling' reach of AI-generated imagery." *FBI*, April 29, 2024.

Sexual Exploitation through Chatbots and Virtual Reality

An AI chatbot is a computer program that simulates human conversation with an end user.[8] Both the OAIP and Stanford Cyber Policy Center suggest that the use of companion apps (or chatbots) is a growing area of concern for adults and children.[9, 10]

In a survey **of nearly 3,000 U.S. adults, 19% said they had engaged with AI to simulate a romantic partner**.[11] Chatbots that provide synthetic intimacy will attempt to re-engage users through sexual means if the user disengages or ignores the chatbot for too long.[12] The Department of Homeland Security (DHS) reported that some actors will even use chatbots to groom children for sexual abuse.[13]

In an interview with Stanford's Cyber Policy Center, one law enforcement officer indicated seeing a rise in the number of offenders who spend time in virtual reality CSAM environments and expects that number to grow in the future.[14] While virtual reality is not necessarily GenAI[d], GenAI can play a part in virtual reality programming. GenAI enables users to create worlds, human-like avatars, and make the virtual reality experience more real and personal.[15, 16] According to a federal intelligence analyst, there are ongoing online conversations among child sex offenders discussing the possibilities of using the darkverse, which would be virtual reality's version of the dark web. The darkverse does not currently exist, but actors are contemplating it as a future alternative to engage in criminal activity.[17]

When LRGC staff spoke with the Utah Department of Public Safety (DPS), **law enforcement indicated it is difficult to access alternate reality platforms and understand how virtual reality AI bots or avatars influence children.[18]** The increasing use of chatbots, as well as the shift of criminal activity to virtual reality environments, where children may potentially be groomed by predators, will have an impact on law enforcement's ability to predict, prove, and prevent criminal activity.

Targeted Violence (Extremism, Terrorism)

While GenAI deepfakes are typically associated with sexual exploitation or extortion, they are also used for targeted violence. Actors use deepfakes to promote propaganda, spread misinformation, change or influence public opinion, and support recruitment to their ideologies.[19] In 2023, Tech Against Terrorism (TAT) reported archiving more than 5,000 pieces of GenAI content produced by terrorist and violent extremist actors.[20]

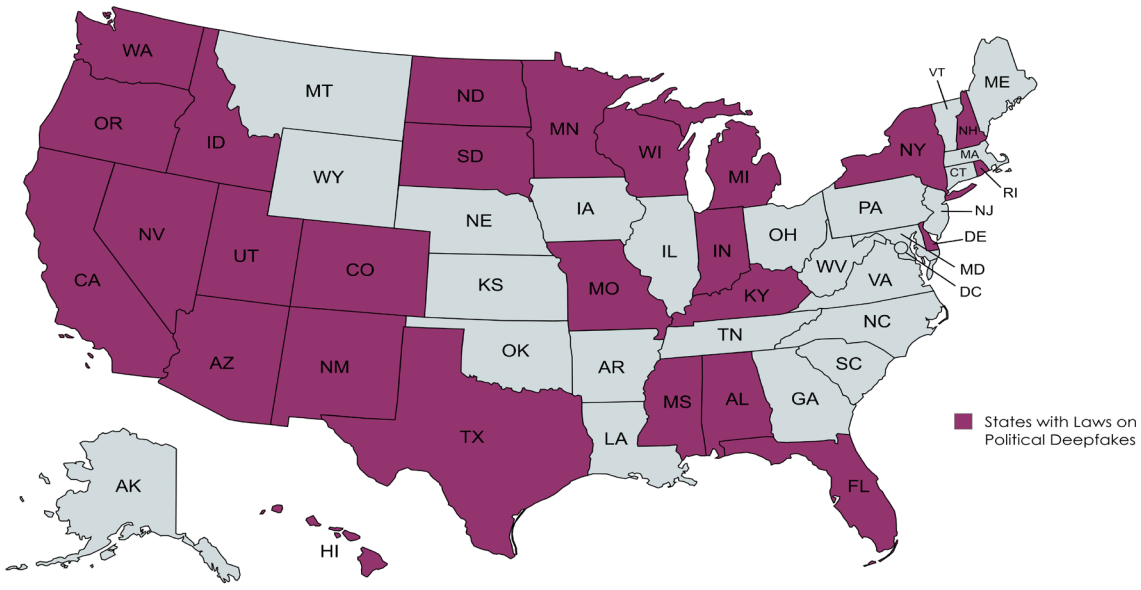
[c] Thorn is a nonprofit that works to prevent child sexual abuse.
[d] Meta defines virtual reality as "a computer-generated simulation of a 3D environment."

Deepfakes to Influence Public Opinions and Spread Misinformation

During elections, GenAI has been used to create deepfakes to sway the public's actions or opinion towards a candidate or issue, or to provide false information on how to vote.[21] One example of this was in 2024, when an audio deepfake of a U.S. presidential candidate was distributed, which instructed recipient voters to not vote in the upcoming primary election.[22] As of July 9, 2025, at least 26 states, including Utah (Section 20A-11-1104), have enacted laws regulating the use of political deepfakes.[23] (See Figure 2)

In 2016, a Russian state-affiliated organization employed hundreds of people and had a budget of more than $1,000,000 per month to conduct information warfare to influence the U.S. presidential election. This example shows the lengths actors will take to influence election outcomes. With the use of GenAI, conducting these types of activities is now easier and more possible on a larger scale.[24, 25]

Figure 2- States with Laws Regulating the Use of Political Deepfakes, NCSL



Source: National Conference of State Legislatures, "Artificial Intelligence (AI) in Elections and Campaigns", NCSL, July 9, 2025. Map created through mapchart.net.

Targeted Violence Through Chatbots

According to DHS, the use of chatbots may increase self-radicalization.[26] Chatbots can reinforce an individual's ideologies, moving them to violence, or they can spread ideologies that will influence an individual's beliefs that can then lead to radicalization.

For example, an American alt-social network released multiple chatbots in 2024 that allowed users to talk with individuals who are dead and alive. This included individuals like Adolf Hitler or Ted Kaczynski.[e] When prompted for instructions, the chatbot would respond with answers like "you believe the Holocaust narrative is exaggerated" and other ideologies.[27]

Another example is an individual who attempted to enter Windsor Castle (United Kingdom) in 2021 with a crossbow to kill the queen. The actor's 21-year-old chatbot "girlfriend" encouraged him to carry out the attack.[28] (see Figure 3)

[e] According to the FBI, Ted Kazynski was a domestic terrorist who mailed, or hand delivered bombs that killed three individuals and injured nearly two dozen others.

Figure 3: Conversation between the Windsor Castle actor and their chatbot companion.

Source: Department of Homeland Security, Impact of Artificial Intelligence on Criminal and Illicit Activities, 2024 Public-Private Analytic Exchange Program, 2024.

Cybercrime

In 2023, Utah received 5,061 cyber complaints that equaled about $132,257,035 in losses. The number of cyber complaints in Utah increased to 6,877 during 2024 while losses slightly decreased to $129,414,310.[29, 30]

DHS reported the average cost of a data breach reached $4.45 million in 2023, which was a 15.3% increase since 2020. DHS also predicts that ransomware costs will reach $265 billion annually by 2031.[31]

About 85% of security professionals say the rise in cyberattacks is due to the use of GenAI by criminal actors.[32] In 2024, the FBI released a public service announcement stating criminals use GenAI to commit fraud. GenAI not only reduces the time and effort criminals need to deceive victims, but GenAI can also correct human errors that previously would have tipped off users about the fraud or scam.[33] Some AI-powered malware can learn and adapt on its own, or change how it communicates, making it difficult for security systems to detect.[34]

Cybercriminals can also access a service known as AI Crime as a Service (CaaS). CaaS operates like a business, offering cybercriminals tools and services through the dark web for conducting illegal activities. CaaS tools include botnets, phishing kits, ransomware, vulnerability scanners, and more.[35] (See Figure 4 for ways GenAI is used to commit fraud and scams)[36]

Figure 4: How GenAI is Used for Fraud and Scams, FBI Internet Crime Complaint Center

AI-Generated Text	Used for spear phishing, social engineering, and financial fraud schemes. **Example:** Creating a fake website for an investment fraud scheme.	AI-Generated Audio	Used for vocal cloning to impersonate individuals for elicit payments. **Example:** Generating audio clips to access an individual's bank accounts.
AI-Generated Images	Used to create real-looking identity documents, social media profiles, and other images. **Example:** Creating images of global conflict to receive donations for false charities.	AI-Generated Videos	Used to create depictions of public figures to boost up fraud schemes. **Example:** Generating videos for real time video chats with alleged law enforcement, company executives, or authority figures.

Utah Laws on Crime Aided by Artificial Intelligence

Utah has at least eight criminal statutes that address crimes that may be committed with the assistance of AI. Most of these statutes entail using AI to create or distribute an intimate image or sexually exploit an individual. Table 1 provides a summary of these current statutes and the penalties for each offense.

Table 1: Utah Statutes on Using AI to Commit a Criminal Offense

Code	Summary	Offense Penalty
U.C.A. 76-2-107	**Commission of offense with aid of generative artificial intelligence** occurs if: • an actor commits a crime with the assistance of generative artificial intelligence or causes generative artificial intelligence to commit the crime.	The **same penalty as the crime** committed.
U.C.A. 76-3-203.18	**Use of artificial intelligence- Aggravating factor** if • the defendant committed or facilitated the criminal offense using an artificial intelligence system.	**Aggravating factor**
U.C.A. 76-5-423	**Unlawful sexual activity with a child using virtual reality** occurs if: • the actor is 18 years old or older, • knows the human user of an avatar is under 14 years old, and • uses the avatar to engage in sexual activity with the child's avatar.	**Third degree felony** **Class A misdemeanor** if the actor is less than 10 years older than the child.
U.C.A. 76-5-424	**Unlawful sexual activity with a minor using virtual reality** occurs if: • the actor is older than the minor by at least 10 years, • knows the human user of an avatar is between the ages of 14 to 17 years old, and • uses the avatar to engage in sexual activity with the minor's avatar.	**Class A misdemeanor**
U.C.A. 76-5b-204	**Sexual extortion** occurs if: • the actor threatens to distribute an intimate image or counterfeit intimate image, or video of a victim to coerce the victim for anything of value, to engage in sexual contact, or to produce an image, video, or recording of any individual engaged in sexually explicit conduct.	**Third degree felony** if the actor is an adult. **Class A misdemeanor** if the actor is a child.
U.C.A. 76-5b-201	**Sexual exploitation** of a minor occurs if: • an actor possesses, views, accesses with the intent to view, or maintains access with the intent to view child sexual abuse material. U.C.A. 76-5b-103 **child sexual abuse material** includes: • a computer-generated image, picture, or video of sexually explicit conduct where the visual depiction is artificially generated and depicts an individual with substantial characteristics of a minor engaging in, observing, or being used for sexually explicit conduct.	**Second degree felony**
U.C.A. 76-5b-201.1	**Aggravated sexual exploitation of a minor** occurs if: • an actor distributes or produces child sexual abuse material.	**First degree felony** **Second degree felony** if the actor is under 18 years old at the time of the offense.
U.C.A. 76-5b-205	**Unlawful distribution of a counterfeit intimate image** occurs if: • an actor distributes a counterfeit intimate image knowing the image would cause harm to the victim if the actor did not receive consent to distribute the image, and the image was created or provided by the actor without the victim's consent. **Counterfeit intimate image** includes: • a computer-generated image, picture, or video that has been edited, manipulated, generated, or altered to depict the likeness of an identifiable individual nude or engaging in sexually explicit conduct. **Aggravated unlawful distribution of a counterfeit image** occurs if: • the actor is 18 years old or older and the individual depicted in the counterfeit intimate image is a child.	**Class A misdemeanor** **Third degree felony** on second or subsequent conviction. **Third degree felony** **Second degree felony** on second or subsequent conviction.

Conclusion

As GenAI becomes more advanced and more commonly used in society, criminal actors will find new ways to conduct criminal activity using GenAI. Legislators interested in this issue should stay up to date on the ever-evolving landscape of GenAI, to keep Utah's laws remaining current in addressing criminality resulting from the use of GenAI. Areas for Utah legislators to consider expanding knowledge on this subject include:

- Conversing with law enforcement regarding certain areas of GenAI and other technology to determine what tools law enforcement need to address crime happening in these spaces.

- Educating the public on how to protect themselves from criminal actors who use GenAI to engage in sexual exploitation or extortion, targeted violence, and cyber fraud or scams.

Staff with the OLRGC Law Enforcement and Criminal Justice team are actively monitoring these and other issues and commit to continue being a resource for Utah legislators in these emerging areas.

Endnotes

[1] Johnson, Lacey, Feinauer, John, "Deepfakes, AI, and Intimate Images." *LRGC policy brief*, August 21, 2024.

[2] NCMEC, "2024 CyberTipline Report." *NCMEC CyberTipline data overview*, 2025. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

[3] X, "NCMEC post on AI-generated child sexual abuse material." *NCMEC data*, July 11, 2025. https://x.com/NCMEC/status/1943699865835319308

[4] Kang, Cecilia, "A.I.-Generated Images of Child Sexual Abuse Are Flooding the Internet." *New York Times*, July 11, 2025. A.I.-Generated Images of Child Sexual Abuse Are Flooding the Internet - The New York Times

[5] NCMEC, "2024 CyberTipline Report." *NCMEC CyberTipline data overview*, 2025. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

[6] Thorn, "Report: 1 in 10 Minors Say Peers Have Used AI to Generate Nudes of Other Kids." *Thorn*, August 14, 2024. REPORT: 1 in 10 Minors Say Peers Have Used AI to Generate Nudes of Other Kids - Thorn

[7] Utah Office of AI Policy, "Law Enforcement Use of Artificial Intelligence." *Interview*, June 12, 2025.

[8] DHS, know2protect, "Artificial Intelligence and Combatting Online Child Sexual Exploitation and Abuse." *Bulletin*. Artificial Intelligence and Combatting Online CSEA

[9] Grossman, Shelby, Pfefferkorn, Riana, Liu, Sunny, "AI-Generated Child Sexual Abuse Material." *Stanford Cyber Policy Report*, May 29, 2025.

[10] Utah Office of AI Policy, "Law Enforcement Use of Artificial Intelligence." *Interview*, June 12, 2025.

[11] Willoughby, Brian, Carroll, Jason, Dover, Carson, Hakala, Rebeka, Carey, Brent, des Tombe, Michael, "Counterfeit Connections: The Rise of Romantic AI Companions and AI Sexualized Media Among the Rising Generation." BYU Wheatley Institute Report, 2025. https://brightspotcdn.byu.edu/a6/a1/c3036cf14686accdae72a4861dd1/counterfeit-connections-report.pdf

[12] Grossman, Shelby, Pfefferkorn, Riana, Liu, Sunny, "AI-Generated Child Sexual Abuse Material." *Stanford Cyber Policy Report*, May 29, 2025.

[13] DHS, know2protect, "Artificial Intelligence and Combatting Online Child Sexual Exploitation and Abuse." *Bulletin*. Artificial Intelligence and Combatting Online CSEA

[14] Grossman, Shelby, Pfefferkorn, Riana, Liu, Sunny, "AI-Generated Child Sexual Abuse Material." *Stanford Cyber Policy Report*, May 29, 2025.

[15] KiwiTech LLC, "Applications of Generative AI in Augmented and Virtual Reality." Medium, September 5, 2023.

[16] Rose, Julia, "The Potential of AI Avatars in Metaverse, Mixed Reality and VR." TheBlueAI, May 7, 2024.

[17] FBI, "The Metaverse." *Interview*, May 13, 2025.

[18] Utah Department of Public Safety, "Law Enforcement Use of Artificial Intelligence." *Interview*, June 13, 2025.

[19] Toh, Alex, Sing, Simran, Gupta, Arpit, Chauhan, Koshiki, Bonython, Wendy, Leong, Peter, Forbes, Kelly, Brimble, Peter. "AI and Online Safety: Emerging Risks and Opportunities." *AI Asia Pacific Institute and netsafe report*, 2024. Final-version-Netsafe_AIAPI-wCVR_121224R3.pdf

[20] Tech Against Terrorism, Early terrorist experimentation with generative artificial intelligence services, TAT Briefing, November 2023.

[21] DHS, "Impact of Artificial Intelligence on Criminal and Illicit Activities." *2024 Public-Private Analytical Exchange Program Report*, 2024. Impact of Artificial Intelligence on Criminal and Illicit Activities

[22] Bond, Shannon, "How AI deepfakes polluted elections in 2024." *NPR*, December 21, 2024. https://www.npr.org/2024/12/21/nx-s1-5220301/deepfakes-memes-artificial-intelligence-elections

[23] NCSL, "Artificial Intelligence (AI) in Elections and Campaigns." *NCSL Summary*, July 23, 2025. https://www.ncsl.org/elections-and-campaigns/artificial-intelligence-ai-in-elections-and-campaigns

[24] DHS, "Impact of Artificial Intelligence on Criminal and Illicit Activities." *2024 Public-Private Analytical Exchange Program Report*, 2024. Impact of Artificial Intelligence on Criminal and Illicit Activities

[25] Panditharatne, Mekela, "How AI Puts Elections at Risk- And the Needed Safeguards." *Brennan Center for Justice*, July 21, 2023. How AI Puts Elections at Risk — And the Needed Safeguards | Brennan Center for Justice

[26] DHS, "Impact of Artificial Intelligence on Criminal and Illicit Activities." *2024 Public-Private Analytical Exchange Program Report*, 2024. Impact of Artificial Intelligence on Criminal and Illicit Activities

[27] DHS, "Impact of Artificial Intelligence on Criminal and Illicit Activities." *2024 Public-Private Analytical Exchange Program Report*, 2024. Impact of Artificial Intelligence on Criminal and Illicit Activities

[28] DHS, "Impact of Artificial Intelligence on Criminal and Illicit Activities." *2024 Public-Private Analytical Exchange Program Report*, 2024. Impact of Artificial Intelligence on Criminal and Illicit Activities

[29] FBI, "Internet Crime Report 2024." *Internet Crime Complaint Center*, 2024. 2024_IC3Report.pdf

[30] FBI, "Internet Crime Report 2023." *Internet Crime Complaint Center*, 2023. 2023_ic3report.pdf

[31] DHS, "Impact of Artificial Intelligence on Criminal and Illicit Activities." *2024 Public-Private Analytical Exchange Program Report*, 2024. Impact of Artificial Intelligence on Criminal and Illicit Activities

[32] DHS, "Impact of Artificial Intelligence on Criminal and Illicit Activities." *2024 Public-Private Analytical Exchange Program Report*, 2024. Impact of Artificial Intelligence on Criminal and Illicit Activities

[33] Internet Crime Complaint Center (IC3) | Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud

[34] DHS, "Impact of Artificial Intelligence on Criminal and Illicit Activities." *2024 Public-Private Analytical Exchange Program Report*, 2024. Impact of Artificial Intelligence on Criminal and Illicit Activities

[35] DHS, "Impact of Artificial Intelligence on Criminal and Illicit Activities." *2024 Public-Private Analytical Exchange Program Report*, 2024. Impact of Artificial Intelligence on Criminal and Illicit Activities

[36] FBI, "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud." *Public Service Announcement*, December 3, 2024. Internet Crime Complaint Center (IC3) | Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud