Submit Date: 21 September 2025
Revise Date: 17 January 2026
Accept Date: 20 January 2026
Initial Publish: 20 January 2026
Final Publish: 23 September 2026

The Encyclopedia of Comparative Jurisprudence and Law



# Identification and Situational Prevention of Emerging Forms of Financial Crimes in the Metaverse

Mitra Yazarloo[1], Mohaddeseh Sadeghian Lemraski *[1], Zahra Tajari Moazeni[1]

1. Department of Law, Go.C., Islamic Azad University, Gorgan, Iran

* Corresponding Author's Email: Mo.Sadeghian1360@iau.ac.ir

## ABSTRACT

While statistics indicate a downward trend in traditional financial crimes in most countries, the development of new technologies and the growing reliance on cyberspace are creating unprecedented opportunities for criminal activity. Crime survey data attest that the share of cyber financial crimes has reached parity with traditional crimes. The prevailing approach of academic institutions, law enforcement agencies, and governmental bodies toward this phenomenon is largely reactive and focused on crimes after their occurrence. This study, by emphasizing the necessity of identifying and applying situational prevention to emerging forms of financial crimes in the metaverse, seeks to formulate a research agenda for novel crimes. In this regard, the article examines the capacities of futures thinking as a strategic tool for the early identification of criminal opportunities and security threats in immersive environments such as the metaverse. Issues such as sophisticated online fraud schemes and forms of delinquency within metaverse environments constitute the core focus of this analysis. Finally, the article concludes by discussing the theoretical implications of this perspective and presenting practical solutions for the situational prevention of such crimes.

***Keywords:*** *emerging crime; cybercrime; Routine Activity Theory; situational crime prevention*

How to cite: Yazarloo, M., Sadeghian Lemraski, M., & Tajari Moazeni, Z. (2026). Identification and Situational Prevention of Emerging Forms of Financial Crimes in the Metaverse. *The Encyclopedia of Comparative Jurisprudence and Law, 4*(3), 1-19.

تاریخ ارسال: ۳۰ شهریور ۱۴۰۴
تاریخ بازنگری: ۲۷ دی ۱۴۰۴
تاریخ پذیرش: ۳۰ دی ۱۴۰۴
تاریخ چاپ اولیه: ۳۰ دی ۱۴۰۴
تاریخ چاپ نهایی: ۱ مهر ۱۴۰۵

دانشنامه فقه و حقوق تطبیقی

# شناسایی و پیشگیری وضعی از اشکال نوپدید جرائم مالی در متاورس

میترا یازرلو[۱]، محدثه صادقیان لمراسکی[۱*]، زهرا تجری مؤذنی[۱]

۱. گروه حقوق، واحد گرگان، دانشگاه آزاد اسلامی، گرگان، ایران
* پست الکترونیک نویسنده مسئول: Mo.Sadeghian1360@iau.ac.ir

## چکیده

در حالی که آمار جرائم مالی سنتی در اکثر کشورها روندی نزولی دارد، توسعه فناوری‌های نوین و وابستگی روزافزون به فضای مجازی، در حال خلق فرصت‌های بی‌سابقه‌ای برای بزهکاری است. داده‌های نظرسنجی جرم گواه این امر است که سهم جرائم مالی سایبری هم‌تراز با جرائم سنتی شده است. رویکرد کنونی نهادهای دانشگاهی، اجرای قانون و حکومتی در قبال این پدیده، غالباً واکنشی و معطوف به جرائم وقوع یافته است. این تحقیق با تمرکز بر ضرورت شناسایی و پیشگیری وضعی از اشکال نوپدید جرائم مالی در متاورس، به تدوین یک دستورکار پژوهشی برای جرائم نوپدید می‌پردازد. در این راستا، مقاله ظرفیت‌های تفکر آینده‌نگر را به عنوان ابزاری راهبردی برای شناسایی زودهنگام فرصت‌های مجرمانه و تهدیدات امنیتی در فضاهای فراگیر مانند متاورس بررسی می‌کند. مواردی همچون کلاهبرداری‌های پیچیده آنلاین و اشکال بزهکاری در محیط‌های متاورس، کانون این تحلیل قرار خواهند گرفت. در پایان، مقاله با بحث در مورد پیامدهای نظری این چشم¬انداز و ارائه راهکارهای کاربردی برای پیشگیری وضعی از این جرائم، جمع‌بندی می‌شود.

**کلیدواژگان:** *جرم نوپدید، جرائم سایبری، نظریه فعالیت¬های روزمره، پیشگیری وضعی از جرم*



**نحوه استناددهی:** یازرلو، میترا.، صادقیان لمراسکی، محدثه، و تجری مؤذنی، زهرا. (۱۴۰۵). شناسایی و پیشگیری وضعی از اشکال نوپدید جرائم مالی در متاورس. *دانشنامه فقه و حقوق تطبیقی*، ۴(۳)، ۱۹-۱.

**مقدمه**

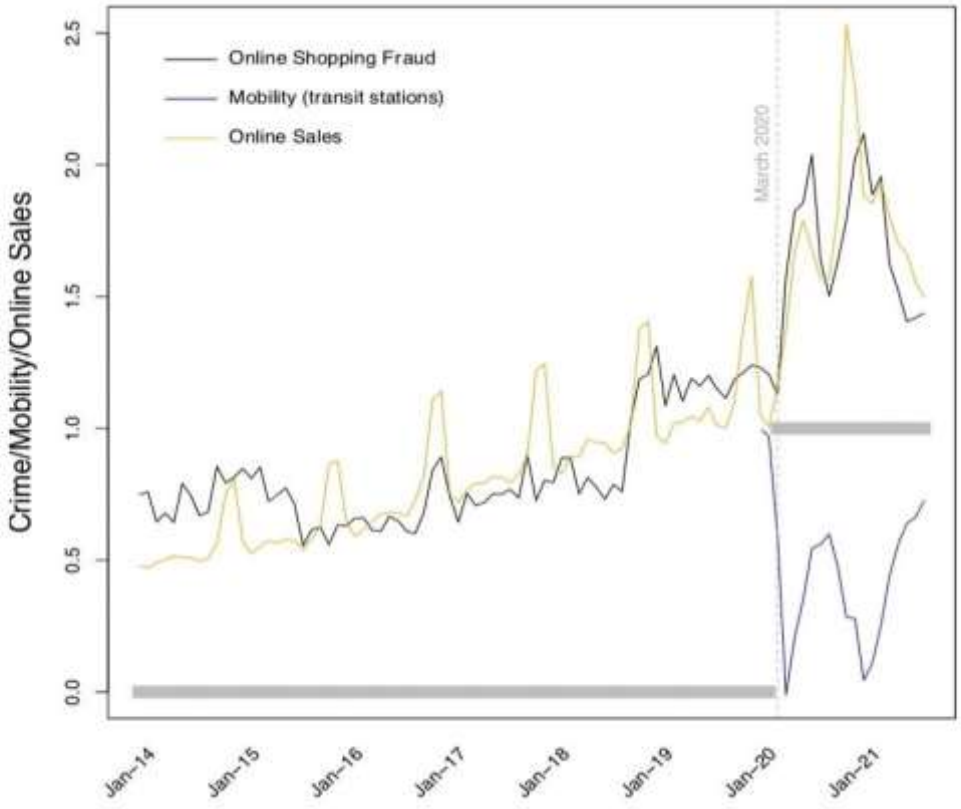
نرخ جرائم سنتی مانند سرقت منزل و وسایل نقلیه، مدت‌زمانی است که در بسیاری از کشورها به‌طور کلی در حال کاهش است (Farrell et al., 2014). این تغییرات به خوبی مستند شده‌اند و انواع جرم و مجرمانی که مرتکب آن می‌شوند، توجه پژوهشی زیادی از سوی محققان دریافت کرده‌اند. با این حال، ماهیت جرم به وضوح در حال تغییر است. برای روشن‌تر شدن موضوع، در نظر بگیرید که یافته‌های نظرسنجی جرم انگلستان و ولز که به‌طور گسترده به‌عنوان منبعی که بهترین برآوردها از شیوع جرم در انگلستان و ولز را ارائه می‌دهد در نظر گرفته می‌شود نشان می‌دهد که حداقل نیمی از کل جرائم در انگلستان و ولز، اکنون یا کلاهبرداری است (که بیشتر آن به صورت آنلاین انجام می‌شود) یا سوءاستفاده کامپیوتری. یک لحظه به این موضوع فکر کنید. همزمان با این تأمل، دو نکته دیگر را نیز در نظر بگیرید. اولاً، انواع سوءاستفاده کامپیوتری که در نظرسنجی درباره آن‌ها پرسش شده است، همه جرائمی را که افراد ممکن است به صورت آنلاین تجربه کنند، پوشش نمی‌دهد. و دوم، قربانیان همیشه از تمام جرائم سوءاستفاده کامپیوتری یا جرائم آنلاینی که متحمل می‌شوند، آگاه نخواهند بود. برای مثال، اگر حساب آنلاین فردی به خطر بیفتد (مثلاً اطلاعات ورود به سیستم او دزدیده شود)، ممکن است در آن زمان یا حتی در تاریخی بعدتر متوجه این موضوع نشوند (بسته به اینکه مجرم با آن اطلاعات چه می‌کند و چه زمانی این کار را انجام می‌دهد). به طور مشابه، اگر مجرمی به یک دستگاه متصل به اینترنت که در مالکیت فرد است (مانند یک زنگ در هوشمند) دسترسی پیدا کند، ممکن است فرد در آن زمان یا هرگز متوجه این موضوع نشود.

در مورد جرم‌های سنتی، دهه‌ها پژوهش نشان داده‌اند که جرم از فرصت» پیروی می‌کند و الگوهای جمعی فعالیت‌های روزمره‌مان آن فرصت‌ها را شکل می‌دهند. در سطح فردی، دیدگاه «فعالیت روزمره» بیان می‌کند که وقتی یک مجرم بالقوه با یک قربانی مناسب روبرو می‌شود و یک محافظ توانمند در آنجا حاضر نباشد، احتمال وقوع جرم بیشتر است (Mohseni, 2024). بنابراین، تغییرات در فعالیت‌های روزمره فردی، احتمال این هم‌زمانی (برخورد مجرم و قربانی) را برای آن فرد تحت تأثیر قرار می‌دهد، در حالی که تغییرات در فعالیت‌های روزمره جمعی ما، پیامدهای گسترده‌تری خواهد داشت. هنگامی که این شرایط محقق شود، طبق دیدگاه «انتخاب عقلانی»، مجرمان (هر چند به طور مختصر) ریسک، زحمت و پاداش مرتبط با ارتکاب جرم را در نظر می‌گیرند و زمانی تصمیم به انجام آن می‌گیرند که پاداش، بیش از ریسک و زحمت درک شود (Paknahad, 2023).

این دیدگاه‌ها بر رویداد متمرکز هستند و از این رو به خوبی برای پژوهش‌هایی مناسب هستند که بررسی می‌کنند فناوری‌ها چگونه ممکن است بر فعالیت‌های روزمره، ادراک مجرمان از ریسک، زحمت و پاداش، و وقوع جرم تأثیر بگذارند. اگرچه جرم ارتکابی در فضای مجازی توجه بسیار کمتری نسبت به جرم در محیط‌های شهری دریافت کرده است، اما ارتباط فرصت–جرم در مورد این شکل از جرائم نیز صدق می‌کند. شاید یکی از سخت‌ترین آزمون‌ها برای این موضوع، با همه‌گیری کووید–۱۹ میسر شد که همان طور که دیگران (Shariati & Guerette, 2023) خاطرنشان کرده‌اند، شرایطی مشابه یک آزمایش طبیعی ایجاد کرد. به عبارت دیگر، در بسیاری از کشورها، پاسخ‌های دولتی به همه‌گیری شامل اعمال محدودیت‌های شدید بود که تردد افراد را برای هر فعالیتی غیر از موارد ضروری محدود می‌کرد. با این حال، این محدودیت‌ها برای یک دوره واحد اعمال نشد، بلکه چندین بار اعمال و سپس لغو شدند که یک «رژِم پاسخ–واکنش مناسب برای آزمایش تأثیر آن‌ها بر فعالیت مردم و جرم ایجاد کرد. در دوره‌های قرنطینه‌ها، بسیاری از مردم تحرک فیزیکی خود را کاهش دادند، در حالی که زمان صرف‌شده در فضای مجازی را افزایش دادند. برای کسانی

که نیاز به قانع‌شدن دارند، شکل ۱ داده‌های مربوط به بریتانیا را ارائه می‌دهد. این شکل، فعالیت خرید آنلاین (با استفاده از داده‌های جمع‌آوری‌شده توسط اداره آمار ملی) برای دوره ۱ ژانویه ۲۰۱۴ تا ۳۱ اوت ۲۰۲۱ را نشان می‌دهد. همچنین تحرک فیزیکی در بریتانیا را برای دوره همه‌گیری (با استفاده از داده‌های جمع‌آوری‌شده توسط گوگل) و نیز کلاهبرداری خرید آنلاین (ارائه‌شده توسط اَکشن فراد، مرکز گزارش‌دهی ملی کلاهبرداری و سایبرکرایم بریتانیا) را نشان می‌دهد. در حالی که تحرک مردم و فعالیت‌های آنلاین به طور کلی در طول همه‌گیری افزایش یافت، اما همگام با اعمال و لغو شرایط لاک‌داون در نوسان بودند.

کلاهبرداری خرید آنلاین نیز به همین ترتیب نوسان داشت. به طور صریح، مانند فعالیت‌های خرید آنلاین، صرفاً اینطور نبود که کلاهبرداری آنلاین فقط در طول همه‌گیری افزایش یابد. این نوع کلاهبرداری با افزایش زمان حضور مردم در فضای مجازی (که منجر به مواجهه بیشتر با خطر جرم می‌شد) افزایش یافت و با کاهش فعالیت آنلاین آن‌ها کاهش پیدا کرد، و بار دیگر با افزایش زمان حضور مردم در فضای مجازی احیا شد و الی آخر (Johnson & Nikolovska, 2024) جرم از فرصت پیروی کرد.




**شکل ۱. سری‌های زمانی کلاهبرداری خرید آنلاین، تحرک‌پذیری (ایستگاه‌های حمل‌ونقل) و فروش آنلاین در دوره پیش و پس از همه‌گیری کووید-۱۹**

یافته‌های این چنینی حاکی از آن است که انواع جرائم ارتکابی و حجم وقوع آنها، تحت تأثیر عوامل محرک تغییر (در این مورد، سیاست‌های کووید-۱۹) هستند که فعالیت‌های روزمره را در مقیاس کلان تحت تأثیر قرار می‌دهند. برخی از این تغییرات می‌توانند موقتی و ناگهانی باشند، همان‌طور که در مورد همه‌گیری دیدیم، اما سایر محرک‌های تغییر ممکن است تدریجی‌تر بوده و اثرات بلندمدت داشته باشند. تا به امروز، همچون سایر حوزه‌های جرم‌شناسی، اکثریت (اما نه تمامی) تحقیقات در حوزه جرم‌شناسی

محیطی (Maimon & Louderback, 2019) بر اشکال سنتی جرم شهری که به روش‌های متداول ارتکاب می‌یابند، متمرکز شده است. با این حال، همان‌طور که پاراگراف‌های فوق امیدواریم نشان داده باشند، انواع جرائم در حال ارتکاب در حال تغییر هستند و نیاز مبرمی به تمرکز بر این اشکال جدید جرم وجود دارد. با انجام این کار، می‌توان رویکردهای پیشگیرانه‌ای را برای مقابله با آن‌ها توسعه داد و سپس این رویکردها را مورد ارزیابی قرار داد تا کارآیی آن‌ها سنجیده شود.


**شکل ۲. طرح پیش‌بینی آینده**

با این حال، اگر ما تنها به مطالعه جرائمی بپردازیم که قبلاً ظهور کرده‌اند، پیشگیری همواره واکنشی خواهد بود و راه‌حل‌های مقابله با اشکال جدید جرم، از سازگاری مجرمان عقب خواهند ماند. این چرخه تکرار خواهد شد. در نتیجه، ما نیاز به ایجاد یک دستورکار آینده‌نگر داریم که به بررسی این موضوع بپردازد که چگونه محرک‌های تغییر در حال تکامل – اعم از سیاسی، زیست‌محیطی، اجتماعی، فناورانه، حقوقی یا اقتصادی – می‌توانند در بازه‌های زمانی کوتاه‌مدت یا بلندمدت بر جرم تأثیر بگذارند. در این مقاله، من با تمرکز ویژه بر فناوری‌های نوظهور، به بحث در مورد دستورکار جرم آینده خواهم پرداخت و مثال‌های گویایی ارائه خواهم داد. این مقاله با بحث در مورد این موضوع به پایان خواهد رسید که چگونه چارچوب‌هایی مانند «۲۵ تکنیک پیشگیری موقعیت‌مدار از جرم» و نظریه‌های «مدیریت مکان» (Eck, 2015) که در حوزه جرم‌شناسی محیطی توسعه یافته‌اند و در بخش بعدی مورد بحث قرار خواهند گرفت، می‌توانند به ما در تعیین اقدامات ممکن در برابر جرم آینده جهت‌دهی کنند.

**دستورکار جرم آینده**

شکل ۲ «مخروط آینده‌های ممکن» (Voros, 2003) را نشان می‌دهد: ابزاری که آینده‌پژوهان از آن برای اندیشیدن درباره آینده استفاده می‌کنند. مرکز این مخروط نشان‌دهنده دنیایی است که امروز در آن زندگی می‌کنیم. با نگاه به سمت راست، می‌بینیم که آینده‌های ممکن بسیاری وجود دارند. برخی از این آینده‌ها باورکردنی‌تر، برخی محتمل‌تر و برخی مطلوب‌تر خواهند بود. این شکل نشان می‌دهد که عدم قطعیت زیادی درباره اینکه آینده واقعاً چگونه خواهد بود، وجود دارد.

با این حال، برخی الگوها تکرار می‌شوند. یکی از این الگوها این است که عموماً هنگامی که کالاها و خدمات (فناورانه) جدید معرفی می‌شوند، پس از دوره اولیه پذیرش اولیه، قیمت آن فناوری‌ها (یا خدمات) کاهش یافته و در عین حال، همه‌جایی بودن آن‌ها افزایش می‌یابد. متأسفانه، توسعه‌دهندگان به ندرت توجه کافی به پیامدهای جرم و امنیت فناوری‌ها (یا خدمات) جدید خود دارند. اما سوءاستفاده‌کنندگان از این کاستی‌ها چنین کور نیستند و توجه زیادی به نقاط آسیب‌پذیر در محصولات و خدمات جدید نشان داده و از آن‌ها بهره‌برداری می‌کنند. در نتیجه، شاهد نمونه‌های متعددی از آنچه پیز (Pease, 1997) «برداشت جرم» می‌نامد، بوده‌ایم. این مسئله به‌ویژه در مورد محصولات و خدماتی که به اشباع بازار می‌رسند صادق است، چرا که اندازه بازار بر مقیاس فرصت‌های جرم تأثیر می‌گذارد. از نمونه‌های تاریخی می‌توان به

سرقت خودرو در دهه ۱۹۹۰ (Laycock, 2004) و سرقت تلفن همراه در دهه ۲۰۰۰ (Mailley et al., 2008) اشاره کرد. از نمونه‌های اخیر نیز می‌توان به استفاده از حملات رله که سیستم‌های ورود بدون کلید غیرفعال را هدف می‌گیرند برای سرقت خودروها و سرقت بسته‌های تحویلی فروشندگان آنلاین اشاره کرد. اگرچه ارائه‌دهندگان اغلب به رفع نقاط آسیب‌پذیر در کالاها و خدمات می‌پردازند، اما راه‌حل‌ها می‌توانند ناقص باشند و تنها پس از آنکه «برداشت جرم» به وقوع پیوسته است، اجرا شوند (Farrell & Roman, 2006). این وضعیت نیاز به تغییر دارد. ممکن است پیش‌بینی قطعیِ تمام تهدیدات آینده (شکل ۲) یا طراحی راه‌حل‌های کامل برای تهدیداتی که شناسایی می‌کنیم، امکان‌پذیر نباشد؛ اما ممکن است بتوان تهدیدات آینده بیشتری را نسبت به وضعیت فعلی شناسایی کرد. هنگامی که این تهدیدات شناسایی شدند، می‌توان آن‌ها را از نظر میزان خطری که تصور می‌شود در آینده ایجاد خواهند کرد، ارزیابی نمود و راه‌حل‌هایی برای مقابله با آن‌ها پیشنهاد داد (راه‌حل‌هایی که بسیاری از آن تهدیدات را به طور همزمان پوشش دهند، معمولاً ارجحیت دارند). اما بحث بیشتر در این مورد را به بخش‌های بعدی موکول می‌کنیم.

در مورد تحقیق درباره تهدیدات جنایی آینده، باید گفت که هیچ «واقعیتِ» قطعی از آینده وجود ندارد؛ بنابراین، اینگونه تحقیقات مستلزم استفاده از روش‌های توسعه‌یافته در حوزه «آینده‌پژوهی» است. این روش‌ها متنوع هستند و شامل تمرینات پویش افق برای شناسایی محرک‌های نوظهور تغییر و ترسیم تهدیدات محتملی است که آن‌ها ممکن است ایجاد کنند. این کار می‌تواند یک تحقیق مطالعه‌ای (میزکاری) باشد که از یک تحلیل‌گر می‌خواهد تا ادبیات موجود را جستجو کند، آنچه را که این ادبیات نشان می‌دهد تلفیق نماید و در فرآیند پیش‌بینی احتمالات جدید، خلاق باشد. وقتی این کار توسط یک فرد یا یک تیم کوچک (که ممکن است متخصص در آن موضوع خاص نباشند) انجام شود، یافته‌ها محدود به تصورات و دانش آن‌ها از آن موضوع خواهد بود (Francillon et al., 2011).

به همین دلیل، از دیگر رویکردهای متکی بر نظرسنجی از متخصصان، مانند تکنیک دلفی یا تکنیک گروه اسمی (Gallagher et al., 1993) اغلب استفاده می‌شود. این روش‌ها از نمونه‌هایی از متخصصان برای بررسی دیدگاه‌های مختلف در مورد یک مسئله خاص و شناسایی حوزه‌های توافق و اختلاف نظر بهره می‌برند. در هر دو نوع مطالعه، یک مرحله اولیه اغلب شامل یک بازبینی (ترجیحاً یک مرور نظام‌مند) از ادبیات موجود (علمی، صنعتی و دولتی) برای احصای آنچه از پیش شناخته‌شده است، می‌باشد. سپس از شرکت‌کنندگان دعوت می‌شود تا خلاصه‌ای از آنچه ادبیات موجود می‌گوید – مانند فهرستی از تهدیدات جنایی پیش‌بینی‌شده مرتبط با یک فناوری خاص – را مرور کرده و به آن فهرست اضافه کنند. در مراحل بعدی، از آنان دعوت می‌شود تا فهرست به‌روز شده را دوباره مرور کنند، هر تهدید بیشتری را به آن بیفزایند و تهدیدات را (به یک یا چند روش) رتبه‌بندی کنند تا میزان موافقت خود با اینکه این تهدیدات احتمالاً یک مشکل خواهند بود را نشان دهند. برای عینی‌تر کردن موضوع، بخش بعدی سه مثال از فناوری‌های نوظهور و نحوه ترسیم تهدیدات مرتبط با آن‌ها را که با استفاده از رویکرد فوق یا گونه‌ای از آن انجام شده است، ارائه می‌دهد. این مثال‌ها با هم مرتبط هستند اما بینش‌های منحصربه‌فردی ارائه می‌کنند.

**ارزهای جدید**

استفاده از پول، یا انتقال ارزش مالی، برای جامعه امروزی امری اساسی است و بنابراین تغییرات در سیستم‌های مالی و نحوه عملکرد آن‌ها می‌تواند اثرات قابل توجهی بر (حداقل بخشی از) فعالیت‌های روزمره جامعه داشته باشد. البته روش‌های انجام معاملات اقتصادی در طول زمان به طور قابل توجهی تغییر کرده‌اند. در حالی که (در دوران اخیر) زمانی پول نقد فیزیکی تنها

وسیله پرداخت بود، شاهد تکامل گزینه‌هایی بوده‌ایم که شامل چک‌های شخصی، پرداخت با کارت، بانک‌داری آنلاین، تراکنش‌های تلفن همراه و شاید به رادیکال‌ترین شکل، ظهور انواع کاملاً جدیدی از ارزهای (دیجیتال) یعنی ارزهای دیجیتال (White, 2015) می‌شود. این ارزها در چندین جنبه با ارزهای سنتی تفاوت دارند: اول، این ارزها غیرمتمرکز هستند، به این معنی که هیچ کنترل‌کننده مرکزی، مانند یک بانک، وجود ندارد. در عوض، تراکنش‌ها بر روی یک دفترکل دیجیتال ثبت می‌شوند و از رمزنگاری برای ایمن‌سازی، ذخیره‌سازی و ثبت آن‌ها استفاده می‌شود. گفته می‌شود اکثر ارزهای دیجیتال نیمه–ناشناس هستند، به این معنا که به جای استفاده از نام حساب، کاربران یک کیف پول دیجیتال (آنلاین یا آفلاین) دارند که از رمزنگاری کلید عمومی برای ارسال و دریافت ارز استفاده می‌کند. این سیستم شامل یک کلید عمومی است که سایر کاربران می‌توانند تراکنش‌ها را به آن ارسال کنند، و یک کلید خصوصی که برای تأیید مالکیت هنگام وقوع تراکنش‌ها استفاده می‌شود. هنگامی که تراکنشی انجام می‌شود، توسط ماینرها بررسی می‌شود. آن‌ها تأیید می‌کنند که فرستنده مالک ارزی است که می‌فرستد، سپس مجموعه‌ای از تراکنش‌های تأییدشده را جمع‌آوری کرده تا یک بلاک تشکیل دهند که به زنجیره بلوکی (شکلی از دفترکل توزیع‌شده دیجیتال) اضافه می‌شود. هر بلاک جدید شامل جزئیاتی (یک هش) از بلاک قبلی به همراه بلاک فعلی است که امنیت را در زنجیره بلوکی ایجاد می‌کند. مکانیسم‌های مختلفی برای تأیید بلاک‌ها می‌تواند استفاده شود، اما جزئیات آن برای بحث ما مهم نیست (Mukhopadhyay et al., 2016).

برای اکثر ارزهای دیجیتال، تراکنش‌ها در یک دفترکل عمومی قابل مشاهده است. این امکان به یک ناظر اجازه نمی‌دهد ببیند چه کسی با چه کسی در حال معامله است، اما ردیابی تراکنش‌ها (مبلغ و زمان) از یک کیف پول به کیف پول دیگر و همچنین تراکنش‌های قبلی را ممکن می‌سازد. با این حال، ارزهای حریم خصوصی (مانند مونرو) نیز وجود دارند که الگوهای تراکنش را پنهان می‌کنند.

بیت‌کوین مشهورترین ارز دیجیتال است، اما ارزهای بسیار دیگری نیز وجود دارند. برای مثال، CryptoMarketCap در صفحه خود بیش از ۸,۰۰۰ ارز دیجیتال را فهرست کرده و ارزش بازار جهانی ارزهای دیجیتال فهرست شده را ۱.۶۶ تریلیون دلار برآورد می‌کند. از این میان، بیت‌کوین و اتریوم بیشترین ارزش بازار کل را به خود اختصاص داده‌اند (به ترتیب ۸۵۰ میلیارد و ۲۷۸ میلیارد دلار). اگرچه برخی فروشگاه‌ها و خرده‌فروشان آنلاین (مانند هوم دپو، مایکروسافت، استارباکس) ارزهای دیجیتال را به عنوان پرداخت می‌پذیرند، اما در حال حاضر این موارد استثنا هستند.

بخش نهایی و مهمی از این اکوسیستم که لازم است درباره آن بحث شود، صرافی‌ها هستند. این پلتفرم‌ها به کاربران اجازه می‌دهند تا ارزهای فیات (ارزهای پشتیبانی‌شده توسط دولت‌ها) را به ارزهای دیجیتال و بالعکس، یا یک ارز دیجیتال را به دیگری تبدیل کنند. آن‌ها ممکن است میزبان کیف پول‌های دیجیتال برای کاربران نیز باشند. کشورهای مختلف، رویکردهای متفاوتی در نحوه نگرش و قوانین مرتبط با ارزهای دیجیتال و صرافی‌ها اتخاذ می‌کنند. به عنوان مثال، هم‌اکنون صرافی‌های ارز دیجیتال در چین ممنوع هستند و استخراج یا "ماینینگ" نیز در این کشور ممنوعیت دارد. در استرالیا، صرافی‌ها باید نزد مرکز گزارش‌ها و تحلیل تراکنش‌های استرالیا ثبت‌نام کنند و این کشور در سال ۲۰۱۹ الزامات نظارتی برای عرضه اولیه سکه (که برای جمع‌آوری پول جهت راه‌اندازی یک ارز جدید استفاده می‌شود) معرفی کرد. در سایر کشورها، مانند ایالات متحده، دولت‌ها در حال حرکت به سمت تنظیم مقررات هستند.

ارزهای دیجیتال می‌توانند و بالفعل انواع متعددی از جرائم مالی را تسهیل می‌کنند. در مجموعه‌ای از مطالعات، ما خطرات پولشویی (Akartuna et al., 2023) و کلاهبرداری ناشی از آن‌ها را

بررسی کرده‌ایم و در اینجا به برخی از یافته‌های کلیدی خواهم پرداخت. تروز و همکاران در مرور نظام‌مند خود بر ادبیات موضوع، ۳۲ نوع مختلف کلاهبرداری را شناسایی کردند که از ارزهای دیجیتال استفاده می‌کنند یا می‌توانند استفاده کنند. در برخی موارد، ارز دیجیتال بخش اساسی کلاهبرداری بوده است. برای مثال، در کلاهبرداری‌های عرضه اولیه سکه، مجرمان ارزهای دیجیتال جعلی جدید را به عنوان یک فرصت سرمایه‌گذاری تبلیغ کرده و به سادگی پول سرمایه‌گذاران را سرقت می‌کنند. طرح‌های پونزی ارز دیجیتال نمونه دیگری هستند. این طرح‌ها گونه‌ای از کلاهبرداری اصلی هستند که در آن سرمایه‌گذاران جذب شده و سود سرمایه‌گذاری خود را از طریق سرمایه‌گذاری سرمایه‌گذاران جدید دریافت می‌کنند. به سرمایه‌گذاران تشویق می‌شود که برای دستیابی به بازدهی (تخیلی) بیشتر، سرمایه خود را برداشت نکنند، در عین حال درباره سودهایی که به دست می‌آورند به روزرسانی دریافت می‌کنند. این روند تا زمانی ادامه می‌یابد که هیچ سرمایه‌گذار جدیدی یافت نشده و طرح فرو می‌پاشد، یا مجرمان با پول‌ها متواری می‌شوند. کلاهبرداری‌های صرافی نمونه مرتبط دیگری است (Trozze et al., 2022). در این مورد، مجرمان صرافی‌های متقلبانه‌ای را تبلیغ می‌کنند که مشوق‌هایی مانند نرخ ارز مطلوب برای جلب مشتری ارائه می‌دهند، اما مجرمان به محض انباشت وجوه کافی، ناپدید می‌شوند. در مورد کیف پول‌های کلاهبرداری، مجرمان خدمات کیف پول دیجیتال برای مدیریت کلیدهای رمزنگاری کاربران ارائه می‌دهند، اما به محض ارائه اطلاعات احراز هویت توسط کاربران، مجرمان بخشی یا تمام پول آن‌ها را می‌دزدند.

جرائم شناسایی‌شده دیگر از ارزهای دیجیتال به عنوان یک روش پرداخت استفاده می‌کنند. از جمله این جرائم می‌توان به حملات باج‌افزار اشاره کرد که در آن از نرم‌افزارهای مخرب (یعنی بدافزار) که از یک وب‌سایت دانلود شده یا با کلیک بر روی یک لینک فیشینگ وارد سیستم می‌شوند- برای رمزگذاری داده‌های کاربر تا زمان پرداخت باج با ارز دیجیتال استفاده می‌شود. کلاهبرداری پیش‌پرداخت و کلاهبرداری عاشقانه از دیگر نمونه‌های شناسایی شده بودند. اگرچه بسیاری از قربانیان این جرائم از قبل دارای ارز دیجیتال نبوده‌اند، اما معمولا کلاهبرداران آموزش‌های مفصلی در مورد چگونگی خرید و انتقال آن‌ها ارائه می‌دهند (Bartoletti et al., 2021). در این موارد، این کلاهبرداری‌ها می‌توانست بدون ارزهای دیجیتال نیز انجام شود، اما استفاده از آن‌ها هم ارتکاب جرم را آسان‌تر می‌کند (مثلاً وجوه را می‌توان به راحتی به هر نقطه از جهان ارسال کرد)، هم مجرمان تصور می‌کنند که این ارزها ناشناس بودن را فراهم می‌کنند[۱]، و هم به این دلیل که هیچ کنترل‌کننده مرکزی وجود ندارد که در غیر این صورت ممکن بود پرداخت را متوقف کند.

از نظر پولشویی، هدف مجرم این است که وجوهی که به طور غیرقانونی به دست آمده‌اند (مثلاً از طریق یک حمله باج‌افزار) را به وجوهی به ظاهر پاک تبدیل کند. یک روش رایج برای انجام این کار، از طریق لایه‌بندی است (Levi & Reuter, 2006) که از یک سری تبدیل‌ها در سیستم‌های مالی برای پنهان کردن منشاء وجوه استفاده می‌کند. آکارتونا و همکاران (۲۰۲۲) در مطالعه دلفی خود، استفاده از ارزهای دیجیتال (و سایر روش‌های پرداخت جدید) و فناوری‌های مرتبط برای این منظور را بررسی کردند. در مورد ارزهای دیجیتال، در مجموع دوازده فناوری به عنوان مواردی که خطر پولشویی ایجاد می‌کنند، شناسایی شدند. برای مثال، اگرچه ارزهای دیجیتال قابل ردیابی هستند و از این رو کاربرد آن‌ها برای مقاصد پولشویی را کاهش می‌دهند، اما ارزهای حریم خصوصی و

[۱]. در حالی که ارزهای رمزنگاری شده دارای نام مستعار هستند، امکان ردیابی تراکنش‌ها وجود دارد. به عنوان مثال، Yousaf et al, (2019: 840) و Elliptic (2023: 48).

همچنین سرویس‌های میکسر مشکل‌زا تلقی شدند. میکسرها با جمع‌آوری چندین پرداخت ورودی و سپس توزیع آن‌ها به چندین حساب، حریم خصوصی را در تراکنش‌های بلاکچین فراهم می‌کنند. مخلوط کردن پرداخت‌های ورودی و خروجی به این روش، زنجیره ترتیبی یک به یک تراکنش‌ها را که در غیر این صورت وجود دارد، مختل می‌کند. عابربردهای بیت‌کوین که به کاربران اجازه می‌دهند پول نقد را به بیت‌کوین و بالعکس تبدیل کنند نیز مشکل‌زا دیده شدند. همچنین قراردادهای هوشمند که به کاربران بلاکچین اجازه می‌دهند معاملات یا تراکنش‌ها را به طور خودکار با استفاده از کد اجرا کنند و در نتیجه نیاز به یک شخص ثالث برای عمل کردن به عنوان کنترل‌کننده مرکزی را از بین می‌برند، در این دسته قرار گرفتند. عدم وجود یک کنترل‌کننده مرکزی در این موقعیت، یک سیستم کارآمد ایجاد می‌کند، اما فرصت‌های نظارت را نیز کاهش می‌دهد (Akartuna et al., 2023).

تا به امروز، استفاده از ارزهای دیجیتال عمدتاً به سرمایه‌گذاری محدود شده است (Bakkt, 2021)، زیرا موارد استفاده روزمره از آن‌ها در مقایسه با اشکال سنتی پرداخت، محدودتر است. این موضوع، دامنه اهداف در دسترس (و مناسب) را محدود می‌کند. با این حال، این وضعیت ممکن است در آینده تغییر کند، زیرا دولت‌ها شروع به پذیرش ارزهای دیجیتال می‌کنند یا اگر از آن‌ها به روش‌های دیگری استفاده شود. در مثال پایانی، به بحث در مورد پژوهش خودمان (Gómez- Quintero et al, 2023:111) در مورد متاورس خواهم پرداخت. این موضوع به دلایل متعددی جالب توجه است، از جمله اینکه نمایانگر یک نوع (مجازی) از محیط است که در آن، استفاده از ارزهای دیجیتال به احتمال زیاد پایه و اساس تراکنش‌ها خواهد بود و این امر، دامنه اهداف در دسترس را افزایش خواهد داد.

**متاورس**

در مورد اینکه متاورس[1] (یا متاورس‌ها) دقیقاً چیست یا چه خواهد بود، اجماعی وجود ندارد، اگرچه همانطور که این جمله اشاره می‌کند، به احتمال زیاد تعداد زیادی از آن‌ها وجود خواهند داشت. با این حال، برای راحتی کار، از این پس به جای «متاورس‌ها» از «متاورس» یاد خواهم کرد. در مورد اینکه چه خواهد بود، در حال حاضر سازمان‌های متعددی در تلاش هستند تا آینده را به سمتی که برای آن‌ها مطلوب‌تر است، سوق دهند. برای مثال، در حالی که بسیاری از تعاریف متاورس، آن را کاربر–محور و باز می‌دانند، برخی از شرکت‌های بزرگ فناوری که در متاورس (یا متاورس‌ها) سرمایه‌گذاری می‌کنند، کمتر احتمال دارد این دیدگاه را به اشتراک بگذارند. با این وجود، توصیف‌های رایج از آن، بر این تأکید دارند که متاورس نسل بعدی اینترنت خواهد بود؛ محیطی فراگیر، غیرمتمرکز و سایبری–فیزیکی. یعنی از طریق استفاده از فناوری‌هایی مانند واقعیت مجازی (VR) و واقعیت افزوده (AR) که به کاربران امکان می‌دهند جهان‌های سه‌بعدی تولیدشده توسط رایانه را تجربه کنند یا واقعیت‌های ترکیبی که محتوای واقعی و تولیدشده توسط رایانه را ترکیب می‌کنند، کاربران متاورس و تعاملات خود در آن را بسیار واقعی‌تر از پلتفرم‌های آنلاین موجود (که معمولاً دو بعدی هستند) "تجربه" خواهند کرد.

فناوری‌های لمسی، از جمله دستکش‌ها، لباس‌های بدن و تلدیلدونیک‌ها[2]، نیز ممکن است برای افزایش (یا غوطه‌ور کردن) تجربه حسی استفاده شوند و استفاده (آتی) از آواتارهای پیکسل‌کدک (Ma et al., 2021) که عکس‌واقع‌گرا هستند به

[1]. metaverse.

[2]. اسباب‌بازی‌های جنسی که روابط جنسی مجازی را امکان‌پذیر می‌کنند(Kobie, 2018: 165).

احتمال زیاد مرز بین واقعیت مجازی و واقعی را بیش از پیش محو خواهد کرد.

علاوه بر تعامل با دیگران در فضاهای مجازی، کاربران قادر خواهند بود با محیط‌های فیزیکی نیز تعامل داشته باشند، چه از طریق فناوری‌های واقعیت ترکیبی، چه از طریق حسگرهای الکترونیکی ارائه‌شده توسط دستگاه‌های متصل به اینترنت در دنیای واقعی، یا از طریق فعال‌سازی (به واسطه فعالیت در متاورس) محرک‌های تعبیه‌شده در دستگاه‌های متصل به اینترنت در محیط‌های واقعی. این امر می‌تواند، برای مثال، به کاربری در یک نقطه از جهان اجازه دهد تا یک سیستم فیزیکی (متصل به اینترنت) در نقطه‌ای دیگر را کنترل کند. شرکت BMW در حال حاضر از آمنی‌ورس برای این منظور به عنوان بخشی از فرآیند تولید خود استفاده می‌کند و جراحی با کمک ربات که بر اساس همین اصل کار می‌کند نیز مدتی است که وجود دارد (Cepolina & Razzoli, 2022).

استفاده از دوقلوهای دیجیتال سه‌بعدی (یعنی بازسازی‌های سه‌بعدی از مکان‌های فیزیکی واقعی) می‌تواند این تعامل را واقعی‌تر جلوه دهد و فرصت‌هایی را برای (مثلاً) آموزش آمادگی در برابر رویدادهای پرخطر با تکرار کم که نمی‌توان در محیط‌های واقعی تمرینشان کرد، فراهم آورد.

انتظار می‌رود که مالکیت نقش مهمی در متاورس ایفا کند، به طوری که کاربران بتوانند دارایی‌های دیجیتال از جمله هنرهای مجازی، لباس‌ها و زمین را خریداری کنند. برای مثال، سرمایه‌گذاری در املاک و مستغلات مجازی از قبل آغاز شده است، به طوری که یک مقاله در مجله فوربس گزارش داد که در سال ۲۰۲۱، ۶۵,۰۰۰ تراکنش برای زمین مجازی در سندباکس (یکی از پلتفرم‌های بزرگ متاورس موجود) انجام شده که در مجموع مبلغ ۳۵۰ میلیون دلار بوده است. اثبات مالکیت زمین و سایر دارایی‌های مجازی در متاورس با استفاده از توکن‌های غیرمثلی برقرار می‌شود که بر روی یک بلاکچین ذخیره شده و با استفاده از ارزهای دیجیتال مانند اتریوم خریداری می‌شوند. (برای بحث در مورد خطرات کلاهبرداری مرتبط با متاورسها، Goldstraw-White & Gill, 2023).

متاورس از طریق همگرایی فناوری‌های مؤثر شامل دستگاه‌های متصل به اینترنت (که به عنوان اینترنت اشیا نیز شناخته می‌شوند)، واقعیت مجازی/واقعیت افزوده، فناوری‌های لمسی، بلاکچین و هوش مصنوعی ممکن خواهد شد. هر یک از این فناوری‌ها به خودی خود خطرات جنایی خاص خود را دارند و خواهند داشت، اما در ترکیب با یکدیگر ممکن است به بروز جرائم دیگری بینجامند. برخی از این خطرات جنایی هم‌اکنون نیز در اینترنت امکان‌پذیر هستند، اما سطح غوطه‌وری تجربه شده در متاورس ممکن است ضربه روانی قربانیان را تشدید کند و اگر پذیرش متاورس به صورت گسترده صورت گیرد، این امر تعداد اهداف در دسترس را افزایش خواهد داد.

در مطالعه خود درباره تهدیدات جنایی تسهیل‌شده توسط متاورس، گومز-کوینترو و همکاران (۲۰۲۳) یک مرور نظام‌مند از ادبیات موجود انجام دادند تا بررسی کنند متاورس در نهایت چه می‌تواند باشد، چگونه ممکن است بر فعالیت‌های روزمره تأثیر بگذارد و چه جرائمی را می‌تواند امکان‌پذیر کند. علاوه بر این، آن‌ها دو کارگاه تخصصی با حضور متخصصان برگزار کردند تا نظرات آنان را در مورد وجود احتمالی سایر تهدیدات جنایی و (علاوه بر موارد دیگر) آسیب‌های مرتبط با این تهدیدات و احتمال تواتر وقوع آن‌ها جویا شوند. کارگاه اول در لندن برگزار شد و شامل ترکیبی از ذی‌نفعان از حوزه‌های دانشگاه، دولت، صنعت، اجرای قانون و بخش داوطلبانه بود. کارگاه دوم با همکاری اینترپل در سنگاپور سازماندهی شد و شامل نمایندگان اجرای قانون از سراسر جهان بود (Gómez-Quintero et al., 2023).

در مجموع، ۲۲ تهدید جنایی در ادبیات موضوع شناسایی شد و ده جرم اضافی دیگر در طول کارگاه‌ها مطرح گردید. ارزیابی

شرکت‌کنندگان از ریسک‌های ناشی از این جرائم در بین دو کارگاه به طور باورنکردنی همخوان بود و در اینجا به چند نمونه از بالاترین تهدیدهای رتبه‌بندی شده خواهم پرداخت. مواد سوءاستفاده جنسی از کودکان شامل کودکان واقعی و نظافت کودک به عنوان مضرترین تهدیدهای جنایی ارزیابی شدند و انتظار می‌رفت که با تواتر نسبتاً بالایی رخ دهند. کلاهبرداری‌های سرمایه‌گذاری (شامل کلاهبرداری‌های عرضه اولیه سکه، طرح‌های پونزی و کلاهبرداری‌های املاک که برخی از آنها ممکن است – و شده‌اند – توسط نقاط ضعف در قراردادهای هوشمند تسهیل شوند)، جرائم نفرت‌پرستی، آزار و اذیت و تعرض جنسی به عنوان تهدیدهای جنایی که با بیشترین فراوانی رخ خواهند داد، ارزیابی شدند و پس از آنها به عنوان مضرترین جرائم شناسایی شده رتبه‌بندی شدند. هم اکنون مواردی از تعرض جنسی، جرائم نفرت‌پرستی و آزار و اذیت در محیط‌های موجود متاورس گزارش شده‌اند و در برخی موارد، این تجربه به این دلیل تشدید شده که قربانی از یک لباس لمسی (هاپتیک) استفاده می‌کرده است. با این حال، دامنه این نوع از جرائم با افزایش پذیرش این فناوری‌ها، احتمالاً افزایش خواهد یافت.

**بحث**

بخش‌های پیشین با هدف ارائه نمونه‌هایی از چگونگی تسهیل شکل‌های نوپدید و آینده جرم توسط فناوری‌ها و خدمات در حال ظهور بود. تهدیدات جنایی مثال‌زده شده همچنین مواردی بودند که کارشناسان نه تنها وقوع آن‌ها را ممکن، بلکه محتمل و همراه با تکرار زیاد و آسیب‌زایی ارزیابی کردند. پس از ارائه چنین نمونه‌هایی، مهم است که در نظر گرفته شود برای پیشگیری از آن‌ها چه می‌توان کرد. پلیس یک رویکرد ارائه می‌دهد، اما پلیس نه منابع لازم برای رسیدگی به همه مشکلات را دارد و نه (یا نباید) دارای تمام شایستگی‌های لازم برای انجام این کار باشد (Laycock, 2004). این موضوع به ویژه زمانی صادق است که برخی از آسیب‌های مورد بحث، با معرفی کالاها و خدماتی تسهیل می‌شوند که دیگران از آن سود می‌برند (Farrell & Roman, 2006) و برای رسیدگی به آن‌ها به مهارت‌های بسیار تخصصی یا دسترسی به زیرساخت‌های تحت کنترل دیگران نیاز است. پیشگیری موقعیتی از جرم که بر اساس نظریه‌های جرم‌شناسی محیطی شکل گرفته، چارچوبی برای حداقل شروع به فکر کردن درباره اینکه چه باید کرد، ارائه می‌دهد. این چارچوب چندین بازبینی را پشت سر گذاشته، از جمله افزودن مواردی در پاسخ به انتقادات وورتلی (Wortley, 2001)، و در حال حاضر ۲۵ تکنیک موقعیتی پیشگیری از جرم وجود دارد. این تکنیک‌ها براساس پنج اصل نشان‌داده‌شده در جدول ۱ سازماندهی شده‌اند.

**جدول ۱: ۲۵ تکنیک پیشگیری وضعی از جرم**

| افزایش هزینه ارتکاب جرم | افزایش خطرات ارتکاب جرم | کاهش منافع ارتکاب جرم | کاهش تحریکات | حذف بهانه‌ها |
|---|---|---|---|---|
| ۱. سخت‌سازی اهداف<br>قفل‌های ستون فرمان و سیستم‌های ضد سرقت<br>شیشه‌های ضد سرقت<br>بسته‌بندی ضد دستکاری | ۶. گسترش نظارت<br>رعایت ملاحظات معمول:بیرون رفتن شبانه به صورت گروهی، باقی گذاشتن نشانه‌هایی از سکونت، همراه داشتن تلفن برنامه نگهبانی همسایگی"کوکون" | ۱۱. مخفی‌سازی اهداف<br>پارکینگ‌های خارج از خیابان<br>دفاتر تلفن با جنسیت خنثی<br>کامیون‌های حمل شمش بدون علامت | ۱۶. کاهش ناکامی و استرس<br>صفوف کارآمد و خدمات مودبانه<br>صندلی‌های بیشتر<br>موسیقی آرام‌بخش/ نورهای ملایم | ۲۱. تعیین قوانین<br>قراردادهای اجاره‌نامه<br>قوانین مقابله با آزار<br>ثبت‌نام در هتل |

| افزایش هزینه ارتکاب جرم | افزایش خطرات ارتکاب جرم | کاهش منافع ارتکاب جرم | کاهش تحریکات | حذف بهانه‌ها |
|---|---|---|---|---|
| ۲. کنترل دسترسی به تأسیسات تلفن‌های ورودی(اینترکام) سیستم‌های دسترسی با کارت الکترونیکی غربالگری و بازرسی چمدان‌ها | ۷. کمک به نظارت طبیعی بهبود روشنایی معابر طراحی فضاهای قابل دفاع حمایت از افشاگران | ۱۲. حذف اهداف رادیوی قابل جابجایی خودرو پناهگاه‌های زنان کارت‌های اعتباری برای تلفن‌های عمومی | ۱۷. جلوگیری از درگیری‌ها محوطه‌های جداگانه برای هواداران رقیب تیم‌های فوتبال کاهش ازدحام در بارها نرخ ثابت کرایه تاکسی | ۲۲. نصب دستورالعمل‌ها تابلوی"توقف ممنوع" تابلوی"ملک خصوصی" تابلوی"آتش چادر را خاموش کنید" |
| ۳. کنترل خروج‌ها نیاز به بلیط برای خروج اسناد خروج کالا برچسب‌های الکترونیکی کالا | ۸. کاهش ناشناس بودن شناسنامه رانندگان تاکسی برچسب‌های"نحوه رانندگی من چطور است؟" یونیفرم مدارس | ۱۳. شناسایی اموال علامت‌گذاری اموال صدور پروانه و علامت‌گذاری قطعات خودرو داغزنی احشام | ۱۸. کاهش برانگیختگی هیجانی کنترل بر محتوای مستهجن خشن اجرای رفتار مناسب در زمین فوتبال ممنوعیت توهین‌های نژادی | ۲۳. بیدار کردن وجدان تابلوهای نمایش سرعت در کنار جاده امضای اظهارنامه‌های گمرکی تابلوی"دزدی از مغازه= دزدی است" |
| ۴. منحرف کردن مجرمان بستن خیابان‌ها سرویس‌های بهداشتی جداگانه برای زنان پراکندگی بارها(و کافه‌های شبانه) | ۹. استفاده از مدیران مکان دوربین مداربسته برای اتوبوس‌های دوطبقه دو فروشنده برای فروشگاه‌های زنجیره‌ای پاداش به هوشیاری | ۱۴. اختلال در بازارها نظارت بر مغازه‌های گرویی کنترل بر آگهی‌های طبقه‌بندی شده صدور مجوز برای دست‌فروشان | ۱۹. خنثی‌سازی فشار همسالان "احمق‌ها مشروب می‌خورند و رانندگی می‌کنند" "نه گفتن اشکالی ندارد" پراکنده‌سازی دردسرسازان در مدرسه | ۲۴. تسهیل پیروی سیستم آسان تحویل کتاب در کتابخانه سرویس‌های بهداشتی عمومی سطل‌های زباله |
| ۵. کنترل ابزار/ سلاح‌ها سلاح‌های"هوشمند" غیرفعال کردن تلفن‌های همراه دزدیده شده محدودیت فروش اسپری رنگ به نوجوانان | ۱۰. تقویت نظارت رسمی دوربین‌های چراغ قرمز آلارم‌های ضد سرقت نگهبانان امنیتی | ۱۵. محروم‌سازی از منافع برچسب‌های رنگی روی کالاها پاک‌سازی دیوارنویسی‌ها دست‌اندازهای سرعت‌گیر | ۲۰. دلسردی از تقلید تعمیر سریع تخریب اموال تراشه‌های V در تلویزیون‌ها سانسور جزئیات روش عملیاتی مجرمانه | ۲۵. کنترل مواد مخدر و الکل دستگاه سنجش الکل در بارها مداخله مسئولین سرو مراسمات بدون الکل |

اگرچه این تکنیک‌ها برای جرائم سنتی‌تر توسعه یافته‌اند، اما هم‌اکنون برای رسیدگی به برخی اشکال جرائم اینترنتی نیز مورد استفاده قرار می‌گیرند (Ho et al., 2022) و می‌توان از آن‌ها برای الهام بخشیدن به رویکردهای مقابله با مشکلات جنسی آینده استفاده کرد. در مورد کاربرد آن‌ها در جرم سایبری، شایان ذکر است که اگرچه این اشکال از تکنیک‌های پیشگیری موقعیتی اغلب استفاده می‌شوند، اما این موضوع همیشه توسط کسانی که آن‌ها را به کار می‌گیرند، به رسمیت شناخته نمی‌شود. اگر آگاهی و استفاده نظام‌مند از این تکنیک‌ها وجود داشته باشد، می‌توان از طیف کامل آن‌ها با تأثیر بیشتری بهره برد. برای نشان دادن این مسئله، هو و همکاران (2022: 30) در مرور نظام‌مند خود از ادبیات موضوع دریافتند که از بین ۳۵۲ مقاله شناسایی‌شده مرتبط با سایبرکرایم و پیشگیری، تنها ۱۴ مقاله به بحث در مورد سایبرکرایم و پیشگیری موقعیتی پرداخته بودند. در میان آن مقالات، ناسازگاری‌هایی در

نحوه طبقه‌بندی تکنیک‌ها توسط نویسندگان در مقالات مختلف وجود داشت و برخی از مثال‌ها مورد تردید بودند. با این حال، هو و همکاران توانستند حداقل یک مثال مرتبط با هر یک از ۲۵ تکنیک را شناسایی کنند. اگرچه این موضوع امیدوارکننده است، اما یافتن «حداقل یک» مثال، معیار نسبتاً پایینی است، به‌ویژه زمانی که برخی از موارد فهرست شده واقعاً با توصیفات تکنیک‌ها مطابقت نداشتند. برای نشان دادن مثال‌های واضح، نمونه‌های روشنی از افزایش تلاش مورد نیاز شامل سخت‌سازی اهداف از طریق پیکربندی مرورگرها برای کاهش خطرات مرتبط با آسیب‌پذیری‌های رایج، یا کنترل دسترسی به تسهیلات از طریق استفاده از فایروال‌ها بود. هو و همکاران (۲۰۲۲) خاطرنشان می‌کنند که به طور کلی، رویکردهای افزایش تلاش اغلب به صورت استانداردهای صنعتی نیز توصیه می‌شوند (Ho et al., 2022).

در مورد افزایش ریسک ارتکاب جرم، استفاده از مدیران مکان در رابطه با مواردی مانند نظارت بر مدیران سیستم مورد بحث قرار گرفت. در همین حال، رمزنگاری و استفاده از علامت‌گذاری دیجیتال آب به عنوان راه‌هایی برای کاهش پاداش‌های مجرمانه مورد بحث قرار گرفتند. راهبردهای کاهش تحریک شناسایی شده عمدتاً غیرفنی بودند، مانند پیش‌بینی و مدیریت مسائل منفی در محیط کار. در رابطه با حذف بهانه‌ها، این مورد شامل استفاده از بنرهای هشداردهنده و قوانین اخلاقی برای دلسرد کردن از رفتارهای نامطلوب بود (Beebe & Rao, 2005).

در مورد مشکلات جنایی آینده، جدول ۱ چارچوبی برای در نظر گرفتن گزینه‌ها ارائه می‌دهد. ارائه پوشش جامعی از چگونگی استفاده از هر یک از تکنیک‌ها فراتر از محدوده یا اهداف این مقاله است، اما امیدواریم برخی مثال‌ها مفید واقع شوند. با در نظر گرفتن نمونه جرائم آینده که در بالا مورد بحث قرار گرفت، «افزایش تلاش» مورد نیاز مجرمان ممکن است شامل سخت‌سازی اهداف باشد، مانند اطمینان از اینکه قراردادهای هوشمند که نشان داده شده آسیب‌پذیر هستند و ممکن است در متاورس و به طور کلی رواج یابند عاری از خطا باشند تا از بهره‌برداری مجرمان از آسیب‌پذیری‌ها جلوگیری شود.

افزایش ریسک» ممکن است شامل استفاده از مدیران مکان باشد. مدیران مکان، مالکان مکان‌ها هستند و در ادبیات موضوع مکان‌ها معمولاً به عنوان فضاهای واقع در محیط فیزیکی در نظر گرفته می‌شوند. با این حال، با در نظر گرفتن نمونه‌های فناورانه مورد بحث در بالا، آنچه به عنوان یک «مکان» (و مدیریت آن) فهمیده می‌شود، می‌تواند از کمی تعدیل در این درک سنتی سود ببرد (Miró Llinares & Johnson, 2018). مکان‌ها را می‌توان در سطوح مختلفی توصیف کرد، از جمله (مثلاً) یک پلتفرم رسانه اجتماعی، یک وب‌سایت، یا ارائه‌دهنده خدماتی که میزبان یک وب‌سایت است. احتمالات دیگری نیز وجود دارد، اما اغلب یک سازمان یا نهاد دیگر مسئولیت یک مکان خاص را بر عهده خواهد داشت و می‌توان آن را به انجام مدیریت مسئولانه مکان تشویق کرد. قانون ایمنی آنلاین بریتانیا نمونه‌ای از قانون‌گذاری است که انتظاراتی را بر عهده مدیران مکان (در این مورد، شرکت‌های فناوری) قرار می‌دهد تا ریسک‌های مربوط به مکان‌های آنلاین تحت کنترل خود را پیش‌بینی و مدیریت کنند (با تأکید ویژه بر محافظت از کودکان). این قانون توسط آفکام تنظیم خواهد شد، که شرکت‌های فناوری را پاسخگو نگه می‌دارد و اختیار جریمه کردن شرکت‌ها و زندانی کردن مدیران آن‌ها را دارد. قانون خدمات دیجیتال اتحادیه اروپا نمونه دیگری است. این تحولات امیدوارکننده هستند، اما اثربخشی آن‌ها و همچنین رویکردهای خاص اتخاذشده توسط شرکت‌های فناوری برای امن‌تر کردن مکان‌های آنلاین، نیاز به ارزیابی دارد. آنچه ممکن است پیچیده‌تر باشد، اقداماتی است که در محیط‌های غیرمتمرکز انجام می‌دهیم.

برای مثال، همان طور که در بالا بحث شد، برخی از دیدگاه‌ها درباره متاورس، آن را غیرمتمرکز تصور می‌کنند و اینکه در جایی که هیچ کنترل‌کننده مرکزی وجود ندارد چه باید کرد، نیاز به تأمل دقیق خواهد داشت. در چنین مواردی، به‌ویژه زمانی که امور مالی درگیر هستند، ممکن است هنوز نهادهای پاسخگو وجود داشته باشند، شاید در قالب سازمان‌های مستقل غیرمتمرکز[1] (Hassan & De Filippi, 2021). به جای وجود یک تصمیم‌گیرنده مرکزی، اعضای یک DAO با رای‌گیری در مورد تأیید یا رد یک اقدام یا ابتکار خاص، تصمیم‌گیری می‌کنند. باید فکر کرد که چگونه می‌توان بر چنین سازمان‌هایی تأثیر گذاشت، اما این خود نقطه‌ای برای مداخله فراهم می‌کند.

کاهش پاداش‌ها ممکن است شامل اخلال در بازارها باشد. همانطور که در بالا بحث شد، برخی از خدمات ارائه‌شده برای ارزهای دیجیتال، پولشویی عواید حاصل از جرم را آسان‌تر می‌کنند. از جمله این خدمات، سرویس‌های میکسر هستند. اگرچه از سرویس‌های میکسر توسط مجرمان استفاده می‌شود، اما آن‌ها کاربردهای مشروع نیز دارند، چرا که نه همه افراد مایل هستند تراکنش‌های مالی خود را عمومی کنند. در نتیجه، این خدمات به طور کامل ممنوع نشده‌اند. اگر استفاده از این خدمات و گونه‌های آینده آن‌ها در آینده افزایش یابد، باید در مورد چگونگی کاهش استفاده از آن‌ها در فعالیت‌های مجرمانه اندیشید. تحریم‌ها یکی از رویکردهایی هستند که تا به امروز با موفقیت در مورد سرویس‌های میکسر خاصی به کار رفته‌اند، اما ممکن است رویکردهای دیگری نیز ضروری باشند.

یک تکنیک برای «کاهش تحریک‌ها»، کاهش برانگیختگی عاطفی از طریق ممنوعیت فحش‌های نژادی در پلتفرم‌های متاورس خواهد بود. رویکردها شامل تشخیص زبان نژادپرستانه و فراهم‌آوری مکانیسم‌های گزارش‌دهی آسان خواهد بود. مورد اول (تشخیص) باید برای تعاملات نوشتاری، گفتاری و سایر تعاملات عمل کند، زیرا تجربیات در متاورس به ارتباطات نوشتاری یا گفتاری محدود نخواهد شد. در مورد گزارش‌دهی، به عواقب مشخص نیاز خواهد بود (و این عواقب باید به طور مستمر اجرا شوند) و همچنین ارتباط واضح/شفاف در مورد اشکال مناسب رفتار برای هشدار به وجدان و در نتیجه حذف بهانه‌ها برای رفتارهای توهین‌آمیز ضروری است.

افزایش آگاهی در مورد تهدیدات آینده در میان صنعت، دولت و سایر ذی‌نفعان، بهانه‌ها را حذف می‌کند.[2] این تا حدی با هدف ۲۵ تکنیک متفاوت است، اما تحرک‌بخشی به اقدام، گام اول برای پیشگیری است و تشویق به عمل، کار ساده‌ای نیست. همان طور که لایکوک (۲۰۰۴) خاطرنشان می‌کند، این امر مستلزم استفاده از اهرم‌ها برای ایجاد انگیزه در کسانی است که نیاز به اقدام دارند. برای سازمان‌های مختلف، راهبردهای متفاوتی مورد نیاز خواهد بود. با در نظر گرفتن دولت‌ها به عنوان یک مثال، ترغیب دولت‌های دموکراتیک به اقدام برای حل مسائل جنایی آینده می‌تواند دشوار باشد، زیرا چرخه‌های انتخاباتی به آن‌ها انگیزه نمی‌دهد تا مسائلی را که ممکن است تنها پس از ترک‌کار آن‌ها (پایان دوره مسئولیت)، ظهور کند، مورد توجه قرار دهند. با این حال، این گامی مهم است که پژوهشگران و اساتید دانشگاه می‌توانند بر آن تأثیر بگذارند؛ برای مثال از طریق تهیه پاسخ و ارائه مدارک در فراخوان‌های دولتی برای گردآوری شواهد، یا همکاری مستقیم با وزارتخانه‌های دولتی. اگرچه جرم‌شناسان محیطی مدتی است با نهادهای پلیس همکاری می‌کنند، اما برای پیشگیری از جرائم آینده، لازم است با مشاوران و سیاست‌گذاران نیز همکاری نمایند (Laycock, 2004).

---

[1]. Decentralised Autonomous Organisations (DAO)

[2]. برای بحث در مورد اینکه چه کسانی می‌توانند بر اقدام تأثیر بگذارند، به Sampson et al, 2010: 45 مراجعه شود.

همان طور که در مقدمه اشاره شد، حداقل نیمی از کل جرائم امروزه به صورت آنلاین ارتکاب می‌یابند. متأسفانه، در حوزه جرم‌شناسی (محیطی) توجه کمتری به سایبرکرایم می‌شود در مقایسه با توجهی که مجرمان به آن نشان می‌دهند. برای مثال، در زمان نگارش این متن در سال ۲۰۲۳، هیچ‌یک از مجلات انجمن جرم‌شناسی آمریکا (جرمشناسی، جرمشناسی و پلیس عمومی)[1] در شماره‌های جاری خود مقاله‌ای در مورد موضوعات جرم کلاهبرداری رایانه‌ای نداشتند. شاید برای بدتر کردن اوضاع، بروئر و همکاران (۲۰۱۹) در مرور خود بر ادبیات نتیجه‌گیری کردند که «تا به امروز تحقیقات اندک یا هیچ تحقیقی در مورد ارزیابی اثرات اقدامات پیشگیری از جرم بر سایبرکرایم انجام نشده است»[2]. به بیان صریح، ناهماهنگی بین مشکلات جنایی (از نظر حجم) که جامعه امروز با آن روبروست و حجم تحقیقاتی که در مورد این مشکلات انجام می‌شود، وجود دارد. اگر حوزه جرم‌شناسی محیطی قرار است به درک مشکلات معاصر و آینده (و چگونگی پیشگیری از آن‌ها) کمک کند، به احتمال زیاد نیاز به تغییر جهت در تلاش‌های تحقیقاتی خواهد بود.

**نتیجه‌گیری**

بر پایه تحلیل‌های ارائه‌شده در این نوشتار، رویکردهای مرسوم در تحلیل جرم و پیشگیری از آن برای مواجهه با چالش‌های امنیتی در محیط پویا و نوظهور متاورس ناکافی ارزیابی می‌شوند. داده‌های ساختاریافته و سنتی که معمولاً در اختیار نهادهای قانونی قرار دارد، به دلیل تأخیر ذاتی در طبقه‌بندی و ثبت جرائم نوپدید، قادر به ترسیم تصویری به‌موقع و کامل از الگوهای جنایی در حال شکل‌گیری نیستند. برای پُر کردن این شکاف اطلاعاتی، ضرورت بهره‌گیری از منابع داده جایگزین و تحلیل محتوای غیرساختاریافته، مانند مکالمات و تعاملات در پلتفرم‌های آنلاین، آشکار می‌شود. تحلیل این حجم عظیم از داده‌های متنی در مقیاس بزرگ، مستلزم به کارگیری فناوری‌های تحلیلی پیشرفته، به‌ویژه تکنیک‌های پردازش زبان طبیعی و مدل‌های هوش مصنوعی است که می‌توانند الگوها و ریسک‌های پنهان را شناسایی کنند.

موفقیت در این عرصه، علاوه بر این، مستلزم تحولی روش‌شناختی است. همان گونه که جرم‌شناسی در گذشته فناوری‌هایی مانند سامانه‌های اطلاعات جغرافیایی را به کار گرفت، امروز نیز لازم است روش‌های پژوهشی از دیگر حوزه‌های علمی اقتباس شده و خود را با پیچیدگی‌های دنیای دیجیتال تطبیق دهد. در نهایت، شواهد تاریخی در حوزه جرائم سایبری نشان می‌دهد که تعلل در اقدام پیش‌دستانه برای مدیریت تهدیدات آینده می‌تواند به بروز مشکلات بزرگ‌تر و فشار فزاینده بر نظام عدالت کیفری در آینده بیانجامد. بنابراین، سرمایه‌گذاری و برنامه‌ریزی زودهنگام برای شکل‌دهی به یک محیط امن در متاورس، نه یک انتخاب، بلکه ضرورتی اجتناب‌ناپذیر برای جلوگیری از رخداد جنایت در فردای دیجیتال قلمداد می‌شود.

**مشارکت نویسندگان**

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

**تعارض منافع**

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

## EXTENDED ABSTRACT

The landscape of crime has undergone a profound transformation over the past two decades, marked by a measurable decline in many forms of traditional property crime alongside a rapid escalation in cyber-enabled and technology-mediated financial offenses. Empirical crime survey data from multiple jurisdictions indicate that fraud and computer misuse now account for a substantial

[1]. Criminology and Criminology and Public Policy

[2]. بسیاری از اقدامات پیشگیرانه برای کاهش خطر آنلاین استفاده می‌شود، اما شواهدی مبنی بر اثربخشی آن‌ها کمتر در دسترس است.

proportion—often at least half—of all recorded criminal activity, a shift closely associated with changes in routine activities and the migration of everyday social and economic interactions into digital environments (Farrell et al., 2014). This transformation has not merely displaced crime from physical to virtual spaces; rather, it has altered the structure of criminal opportunity itself. Classical insights from Routine Activity Theory emphasize that crime occurs when motivated offenders, suitable targets, and the absence of capable guardians converge in time and space (Mohseni, 2024). In digitally mediated contexts, this convergence is increasingly shaped by online presence, platform design, and technological affordances. Complementing this, Rational Choice perspectives suggest that offenders make bounded assessments of effort, risk, and reward before acting (Paknahad, 2023). Technological innovations can recalibrate each of these dimensions by lowering entry barriers, obscuring offender identity, increasing the scale of potential gains, and weakening traditional forms of guardianship. Evidence from the COVID-19 pandemic provided a quasi-natural experiment demonstrating how shifts in collective routine activities—specifically reduced physical mobility and increased online engagement—were mirrored by corresponding fluctuations in online shopping fraud, reinforcing the proposition that crime continues to follow opportunity even in virtual settings (Johnson & Nikolovska, 2024; Shariati & Guerette, 2023). These dynamics underscore the need to reconceptualize environmental criminology for immersive and interconnected digital environments.

While environmental criminology has historically focused on physical urban settings, its core logic remains applicable to cyber and hybrid spaces, including the emerging metaverse. Yet, much existing research remains reactive, analyzing crimes only after they have become established and measurable. Such an approach risks perpetually lagging behind offender adaptation, particularly in fast-evolving technological contexts. Futures thinking offers a strategic corrective by shifting analytical attention toward emerging drivers of change—technological, economic, legal, social, and political—that may reshape criminal opportunity structures over time. Tools such as the "cone of possible futures" illustrate the inherent uncertainty surrounding technological trajectories while also highlighting recurring patterns, notably the tendency for new technologies to become cheaper, more ubiquitous, and consequently more attractive for criminal exploitation (Voros, 2003). Historical examples of crime "harvests," such as widespread vehicle theft in the 1990s (Laycock, 2004) and mobile phone theft in the 2000s (Mailley et al., 2008), demonstrate how insufficient attention to security at the design and diffusion stages can generate large-scale victimization before effective countermeasures are implemented (Farrell & Roman, 2006). Futures-oriented criminological inquiry therefore seeks not precise prediction but systematic anticipation: identifying plausible threats, assessing their potential harm and frequency, and proposing preventative interventions capable of addressing multiple risks simultaneously. Methodologically, this often entails horizon scanning, systematic literature reviews, and expert-elicitation techniques such as Delphi studies and nominal group processes, which broaden analytical perspectives beyond the limitations of individual expertise (Francillon et al., 2011; Gallagher et al., 1993).

One domain where futures-oriented analysis is particularly salient is that of new and evolving financial instruments, especially cryptocurrencies. Digital currencies differ fundamentally from traditional fiat money through their decentralized architecture, cryptographic security, and reliance on

distributed ledgers rather than central authorities (Mukhopadhyay et al., 2016; White, 2015). While transactions on most blockchains are publicly visible, varying degrees of pseudonymity, combined with privacy-enhancing technologies such as mixers and privacy coins, complicate attribution and enforcement. Research has documented a wide array of fraud typologies associated with cryptocurrencies, including initial coin offering scams, Ponzi schemes, fraudulent exchanges, and malicious wallet services (Trozze et al., 2022). In other cases, cryptocurrencies function primarily as payment mechanisms that facilitate offenses such as ransomware attacks, advance-fee fraud, and romance scams, often by enabling rapid cross-border transfers and bypassing traditional financial controls (Bartoletti et al., 2021). From a money-laundering perspective, cryptocurrencies and associated services can support layering processes designed to obscure the illicit origins of funds (Levi & Reuter, 2006). Expert-based studies have identified specific technological features—such as mixers, privacy coins, smart contracts, and cryptocurrency ATMs—as presenting elevated laundering risks by reducing transparency or oversight (Akartuna et al., 2023). Although current everyday use of cryptocurrencies remains relatively limited compared to conventional payment methods (Bakkt, 2021), wider adoption would substantially expand the pool of suitable targets and amplify the scale of potential harm, particularly in environments where digital currencies constitute the default medium of exchange.

The metaverse represents such an environment, envisioned as an immersive, persistent, and interconnected extension of the internet that blends virtual and physical realities through technologies including virtual reality, augmented reality, haptics, blockchain, and artificial intelligence. While no single definition prevails, prevailing descriptions emphasize high levels of immersion, user embodiment via avatars, and the integration of digital assets and economies. Advances in photorealistic avatars and haptic interfaces promise to intensify experiential realism, potentially blurring psychological boundaries between virtual and physical interaction (Ma et al., 2021). Simultaneously, the convergence of virtual environments with physical systems—through digital twins, Internet-of-Things devices, and remote actuation—creates novel interfaces between online activity and real-world consequences, as already evidenced in industrial applications and robotic-assisted surgery (Cepolina & Razzoli, 2022). Economic activity within the metaverse is expected to rely heavily on cryptocurrencies and non-fungible tokens to establish ownership of virtual land, goods, and services, a trend that has already generated substantial financial flows and speculative investment. Systematic reviews and expert workshops examining metaverse-enabled crime have identified a broad spectrum of potential threats, ranging from financial fraud and market manipulation to harassment, hate crime, sexual offenses, and child exploitation (Gómez-Quintero et al., 2023). Experts consistently rated certain threats—such as child sexual abuse material, grooming, investment fraud, and immersive harassment—as both highly harmful and likely to occur with significant frequency, particularly as adoption expands. The immersive qualities of the metaverse may intensify victim impact, while scale effects increase the number of suitable targets, reinforcing concerns about future crime amplification (Goldstraw-White & Gill, 2023).

Addressing such threats necessitates a shift from purely reactive enforcement toward proactive, situational prevention grounded in environmental criminology. The framework of the 25 techniques of situational crime

prevention organizes interventions around increasing effort and risk, reducing rewards, reducing provocations, and removing excuses, offering a versatile toolkit adaptable beyond physical settings (Wortley, 2001). Although originally developed for conventional crimes, these techniques have already been applied—often implicitly—to cybercrime contexts, including through technical hardening, access controls, monitoring, and user guidance (Ho et al., 2022). Systematic reviews reveal, however, that explicit and comprehensive application of the framework remains limited, with inconsistent classification and underutilization of available techniques (Ho et al., 2022). In future digital environments, increasing effort may involve secure-by-design smart contracts and platform architectures resistant to exploitation; increasing risk may rely on responsible "place management" by platform operators, service providers, or even decentralized governance structures (Miró Llinares & Johnson, 2018). Reducing rewards could entail disrupting illicit markets and laundering pathways associated with digital assets, while reducing provocations and removing excuses may require clear behavioral norms, effective moderation, and transparent reporting mechanisms (Beebe & Rao, 2005). Emerging regulatory initiatives, such as online safety and digital services legislation, illustrate attempts to institutionalize such responsibilities, though their effectiveness remains an empirical question.

In conclusion, the analysis demonstrates that emerging financial crimes in the metaverse cannot be adequately addressed through retrospective data and conventional enforcement alone. The pace of technological change, combined with the scale and immersion of future digital environments, demands anticipatory strategies that integrate futures thinking with situational crime prevention. Historical experience shows that delayed responses to technological vulnerabilities often result in widespread victimization before corrective measures are implemented. By systematically identifying plausible future threats, assessing their potential harms, and embedding preventative measures at the design and governance stages of new technologies, policymakers, industry actors, and researchers can reduce the likelihood and impact of large-scale crime "harvests" in immersive digital ecosystems. Proactive investment in interdisciplinary methods, advanced analytical tools, and collaborative governance structures is therefore essential if the metaverse is to evolve into a space that supports innovation and social interaction without reproducing—and magnifying—the criminogenic failures of earlier technological transitions.

**References**


Akartuna, E. A., Johnson, S. D., & Thornton, A. E. (2023). The money laundering and terrorist financing risks of new and disruptive technologies: A futures-oriented scoping review. *Security Journal*, *36*, 615.

Bakkt. (2021). *Bakkt U.S. Customer Crypto Survey*. https://publicdocs.bakkt.com/hubfs/collateral/Survey_Crypto_Exec_Summary_090121.pdf

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: Analysis and perspectives. *IEEE Access*, *9*, 148353-148373.

Beebe, N. L., & Rao, V. S. (2005). Using situational crime prevention theory to explain the effectiveness of information systems security. Proceedings of the 2005 SoftWars Conference, Las Vegas, NV.

Cepolina, F., & Razzoli, R. P. (2022). An introductory review of robotically assisted surgical systems. *The International Journal of Medical Robotics and Computer Assisted Surgery*, *18*(4), e2409.

Eck, J. E. (2015). Who should prevent crime at places? The advantages of regulating place managers and challenges to police services. *Policing: A Journal of Policy and Practice*, *9*(3), 223-233.

Farrell, G., & Roman, J. (2006). Crime as pollution: Proposal for market-based incentives to reduce crime externalities. In *Crime Reduction and the Law* (pp. 151-171). Routledge.

Farrell, G., Tilley, N., & Tseloni, A. (2014). Why the crime drop? *Crime and Justice*, *43*(1), 421-490.

Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. Proceedings of the Network and Distributed System Security Symposium (NDSS),

Gallagher, M., Hares, T. I. M., Spencer, J., Bradshaw, C., & Webb, I. A. N. (1993). The nominal group technique: A research tool for general practice? *Family Practice*, *10*(1), 76-81.

Goldstraw-White, J., & Gill, M. (2023). *Assessing Non-Fungible Tokens (NFTs): A Resource Guide for Fraud Practitioners*. Perpetuity Research & Consultancy International (PRCI) Ltd and Association of Certified Fraud Examiners.

Gómez-Quintero, J., Johnson, S. D., Borrion, H., & Lundrigan, S. (2023). *A scoping study of crime facilitated by the metaverse*. https://doi.org/10.31235/osf.io/x9vbn

Hassan, S., & De Filippi, P. (2021). Decentralized autonomous organization. *Internet Policy Review*, *10*(2), 1-10.

Ho, H., Ko, R., & Mazerolle, L. (2022). Situational crime prevention techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security*, *115*, 102611.

Johnson, S. D., & Nikolovska, M. (2024). The effect of COVID-19 restrictions on routine activities and online crime. *Journal of quantitative criminology*, *40*(1), 131-150.

Laycock, G. (2004). The UK car theft index: An example of government leverage. *Understanding and Preventing Car Theft*, *17*, 25-44.

Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice*, *34*(1), 289-375.

Ma, S., Simon, T., Saragih, J., Wang, D., Li, Y., De La Torre, F., & Sheikh, Y. (2021). Pixel codec avatars. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition,

Mailley, J., Garcia, R., Whitehead, S., & Farrell, G. (2008). Phone theft index. *Security Journal*, *21*, 212-227.

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, *2*, 191-216.

Miró Llinares, F., & Johnson, S. D. (2018). Cybercrime and place: Applying environmental criminology to crimes in cyberspace. In G. Bruinsma & S. D. Johnson (Eds.), *The Oxford Handbook of Environmental Criminology*. Oxford University Press.

Mohseni, F. (2024). *Theories of Criminology* (2 ed.). Judiciary Press and Publications Center.

Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2016). A brief survey of cryptocurrency systems. 14th Annual Conference on Privacy, Security and Trust (PST),

Paknahad, A. (2023). *Principles of Criminology* (2 ed.). Mizan Publishing.

Pease, K. (1997). Crime reduction. In M. Maguire (Ed.), *The Oxford Handbook of Criminology* (2 ed.). Clarendon Press.

Shariati, A., & Guerette, R. T. (2023). Findings from a natural experiment on the impact of COVID-19 residential quarantines on domestic violence patterns in New Orleans. *Journal of family violence*, *38*(2), 203-214.

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*, 1-35.

Voros, J. (2003). A generic foresight process framework. *foresight*, *5*(3), 10-21.

White, L. H. (2015). The market for cryptocurrencies. *Cato Journal*, *35*, 383.

Wortley, R. (2001). A classification of techniques for controlling situational precipitators of crime. *Security Journal*, *14*, 63-82.