Archive of SID.ir

Journal of
International Criminal Law
www.iclj.ir

Volume 3, Issue 2, 2025

The Role of Modern Technologies in the Situational Prevention of Terrorism Financing in Digital Banking

Shahrdad Darabi [1], Amir Samavati Pirouz [2], Mahdi Chegeni[3], Maryam Valizadeh*[4]

1. Associate Professor, Department of Criminal Law and Criminology, Qom Branch, Islamic Azad University, Qom, Iran.
2. Assistant Professor, Department of Criminal Law and Criminology, Karaj Branch, Islamic Azad University, Karaj, Iran.
3. Assistant Professor Department of Law Faculty of Humanities Ayatollah Borujerdi Universit, Borujerd, Iran
4. Ph.D. Candidate in Criminal Law and Criminology, Karaj Branch, Islamic Azad University, Karaj, Iran. (Corresponding Author).

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: 111-125

Corresponding Author's Info
ORCID: *0000-0002-1654-6660*
TELL: *+989198922273*
Email: *vlizade.mrym@gmail.com*

Article history:
Received: *29 Jun 2024*
Revised: *14 Sep 2024*
Accepted: *15 Sep 2024*
Published online: *21 Mar 2025*

Keywords:
Terrorism Financing, Terrorist Financing, Situational Prevention, Digital Banking, Terrorism.

ABSTRACT

Terrorism financing, as the financial system supporting terrorist activities, has become one of the most critical challenges to national and international security. Consequently, its prevention is of paramount importance in countering the funding of terrorism. This article examines the role of modern technologies in the situational prevention of terrorism financing. This article adopts a descriptive-analytical approach. The research findings reveal that terrorist groups employ novel methods such as digital money laundering, cyber fraud, banking system hacking, and cryptocurrency exploitation to finance their activities. These actions not only threaten the financial security of nations but also undermine economic stability and sustainable development. To effectively counter this phenomenon, the study proposes the following strategies: Strengthening monitoring systems and intelligent tracking of financial transactions, Utilizing advanced technologies such as artificial intelligence (AI) to detect suspicious patterns, Enhancing international coordination and legal frameworks, Developing advanced identity verification systems, Increasing awareness among financial institution personnel. This study demonstrates that combating terrorism financing requires a comprehensive, technology-driven approach, which through international collaboration can weaken terrorist financial networks and enhance economic security.

This is an open access article under the CC BY license. © 2025 The Authors.

How to Cite This Article: Darabi, Sh; Samavati Pirouz, A; Chegeni, M & Valizadeh, M (2025). "The Role of Modern Technologies in the Situational Prevention of Terrorism Financing in Digital Banking". *Journal of International Criminal Law*, 3(2): 111-125.

Archive of SID.ir

Archive of SID.ir

فصلنامه حقوق جزای بین‌الملل
www.iclj.ir
انجمن علمی فقه جزای تطبیقی ایران

دوره سوم، شماره دوم، تابستان ۱۴۰۴

نقش فناوری‌های نوین در پیشگیری وضعی از اقتصاد تروریسم در بانکداری دیجیتال

شهرداد دارابی[۱]، امیر سماواتی پیروز[۲]، مهدی چگنی[۳]، مریم ولی زاده[۴*]

۱. دانشیار گروه حقوق جزا و جرم‌شناسی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران.

۲. استادیار گروه حقوق جزا و جرم‌شناسی، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران.

۳. دانشیار گروه حقوق دانشکده علوم انسانی دانشگاه آیت الله العظمی بروجردی (ره)، بروجرد، ایران.

۴. دانشجوی دکتری حقوق جزا و جرم‌شناسی، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران. (نویسنده مسؤول)

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۱۱۱-۱۲۵

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۹-۰۰۰۷-۶۷۵۲-۷۹۶۵

تلفن: ۹۸۹۱۹۸۲۹۲۲۷۳+

ایمیل: vlizade.mrym@gmail.com

سابقه مقاله:

تاریخ دریافت: ۱۴۰۳/۰۴/۰۹

تاریخ ویرایش: ۱۴۰۳/۰۶/۲۴

تاریخ پذیرش: ۱۴۰۳/۰۶/۲۵

تاریخ انتشار: ۱۴۰۴/۰۱/۰۱

واژگان کلیدی:

اقتصاد تروریسم، تأمین مالی تروریسم، پیشگیری وضعی، بانکداری دیجیتال، تروریسم.

چکیده

اقتصاد تروریسم به عنوان سیستم مالی پشتیبان فعالیت‌های تروریستی، امروزه به یکی از چالش‌های اصلی امنیت ملی و بین‌المللی تبدیل شده است. بر این اساس، پیشگیری از آن برای مقابله با تأمین مالی تروریسم از اهمیت ویژه‌ای برخوردار است. از این رو، در این مقاله به نقش فناوری‌های نوین در پیشگیری وضعی از اقتصاد تروریسم می‌پردازیم. این مقاله به شیوه توصیفی- تحلیلی نگارش یافته است. یافته‌های تحقیق نشان می‌دهد که گروههای تروریستی از روشهای نوینی مانند پولشویی دیجیتال، کلاهبرداری اینترنتی، هک سیستم‌های بانکی و سوءاستفاده از رمزارزها برای تأمین مالی خود استفاده می‌کنند. این اقدامات نه تنها امنیت مالی کشورها را تهدید می‌کند، بلکه ثبات اقتصادی و توسعه پایدار را نیز تحت تأثیر قرار می‌دهد. برای مقابله مؤثر با این پدیده، راهکارهایی شامل تقویت سیستم‌های نظارتی و پایش هوشمند تراکنش‌های مالی، به‌کارگیری فناوری‌های پیشرفته مانند هوش مصنوعی در شناسایی الگوهای مشکوک، ایجاد هماهنگی بین‌المللی و تقویت چارچوب‌های حقوقی، توسعه سیستم‌های احراز هویت پیشرفته و افزایش آگاهی کارکنان مؤسسات مالی پیشنهاد می‌گردد. این مطالعه نشان می‌دهد مقابله با اقتصاد تروریسم نیازمند رویکردی جامع و تکنولوژی‌محور است که با همکاری‌های بین‌المللی می‌تواند شبکه‌های مالی تروریستی را تضعیف و امنیت اقتصادی را ارتقا بخشد.

خوانندگان این مجله، اجازه توزیع، ترکیب مجدد، تغییر جزئی و کار روی حاضر به صورت غیرتجاری را دارند.

© تمامی حقوق انتشار این مقاله، متعلق به نویسنده می‌باشد.

Archive of SID.ir

Archive of SID.ir

مقدمه

تروریسم پدیده‌ای جدید نیست؛ مدت‌هاست که به‌عنوان روشی برای اقدام خشونت‌آمیز توسط سازمان‌ها و افراد در تلاش برای دستیابی به اهداف سیاسی مورد استفاده قرار گرفته است. در واقع، تروریسم یک هدف نیست، بلکه یک شیوه عمل است. بر اساس نظر بروس هافمن[1]، تمام تروریست‌ها یک ویژگی مشترک دارند: آن‌ها در «آینده» زندگی می‌کنند و متقاعد شده‌اند که دشمنان خود را شکست خواهند داد و به اهداف سیاسی خود دست خواهند یافت (Combs, 2023: 13). در گذشته، تروریسم عمدتاً با حملات فیزیکی و خشونت‌های آشکار همراه بود، اما امروزه با گسترش فناوری‌های دیجیتال، تروریست‌ها از ابزارهای مدرن برای اهداف خود استفاده می کنند. تروریسم سایبری، جنگ اقتصادی، حملات به زیرساخت‌های مالی و حتی دستکاری بازارها از جمله تهدیدات نوظهوری هستند که مرزهای سنتی تروریسم را درنوردیده‌اند. این گروه‌ها با بهره‌گیری از هک، پولشویی دیجیتال، رمزارزها و حتی هوش مصنوعی، بدون نیاز به حضور فیزیکی، خسارات گسترده‌ای به امنیت ملی و ثبات اقتصادی کشورها وارد می کنند. در این شرایط، مقابله با تروریسم نیازمند رویکردهای هوشمند، فناوری‌محور و همکاری بین‌المللی است تا بتوان با اشکال نامرئی، ولی ویرانگر این پدیده مبارزه کرد.

تروریسم مدرن از توسعه و گسترش رسانه‌های جمعی و ارتباطات الکترونیکی بهره برده است که ابزارهایی مفید برای تبلیغ پیام و هماهنگی حملات در نقاط مختلف را در اختیار تروریستها قرار می‌دهد. برای اینکه تروریست‌ها بتوانند تأثیر عملیاتهای مرگبار خود و تلاشهایشان برای جلب حمایت از اهدافشان را به حداکثر برسانند، نیاز دارند که رسانه‌ها نظراتشان را پخش کنند، افکار عمومی را تحت تأثیر قرار دهند و ترس و اضطراب را در میان مردم گسترش دهند. در مقابل، رسانه‌ها نیز به دلیل جذابیت دراماتیک تروریسم و توجه عمومی به آن، به پوشش این موضوع گرایش دارند (Ganor, 2003: 9). تروریسم مدرن موضوع جدیدی نیست و مطالعات نشان می دهد که ده‌هاست که بحث آن مطرح است؛ اگرچه گروه‌های تروریستی فعال هنوز پایبند به تروریسم سنتی هستند و کمتر در شکل مدرن آن که توصیف گردید، فعالیت می‌کنند. با این حال، شاید پیوند اقتصاد و تروریسم چالش‌های نوینی را خصوصاً در حوزه بانکداری دیجیتال ایجاد نموده است.

توسعه فناوری مالی، جرائم سایبری را افزایش داده و نگرانی های امنیتی و اعتمادی را در صنعت بانکداری تشدید کرده است. روش‌های سنتی امنیتی، مانند تکنیک‌های آماری و مبتنی بر قواعد، اغلب در تطبیق با ماهیت متغیر تهدیدات جدید ناتوان هستند (Inuwa & Das, 2024:10). از این رو، در این مقاله به بررسی مفهوم اقتصاد تروریسم پرداخته و شیوه‌هایی که ساختار اقتصاد تروریسم را تقویت می‌کند، مورد مطالعه قرار می‌دهیم و در نهایت، شیوه‌هایی را برای پیشگیری از آن ارائه می‌دهیم.

۱- ماهیت اقتصاد تروریسم

در شناخت مفهوم و ماهیت اقتصاد تروریسم باید به نقش اقتصاد در تروریسم و تفاوت اقتصاد تروریسم و تروریسم اقتصادی بپردازیم؛ لذا در ادامه، این مفهوم و تفکیک مورد بررسی قرار می‌گیرد.

۱-۱- تفاوت اقتصاد تروریسم[2] با تروریسم اقتصادی[3]

ملاحظات اقتصادی در هر دو ساحت علل و آثار نقش ایفا می کنند، اما محققان و سیاست‌گذاران تاکنون به اجماع روشنی در مورد نقش اقتصاد در بروز تروریسم یا چگونگی بهره‌گیری از تحلیل‌های اقتصادی برای درک تروریسم و طراحی راهبردها و سیاست‌های خاص مقابله با آن دست نیافته‌اند (Gold, 2005: 3-1). در واقع، بخش عمده مباحث درباره پیوندهای اقتصاد و تروریسم، حول این محورها بوده است که چگونه فقر، نابرابری و محدودیت فرصت‌ها به بروز واکنش‌های تروریستی می‌انجامد و آیا بهبود این شرایط می‌تواند از میزن تروریسم بکاهد.

نقش مستقیم عوامل اقتصادی مانند فقر و نابرابری و نیز اقدامات سیاستی مانند تحریم‌ها، یکی از راه‌های بررسی «اقتصاد تروریسم» است؛ اما این معیارها به‌تنهایی تبیین‌کننده

[1]- Bruce Hoffman
[2]- Economics of Terrorism
[3]- Economic Terrorism

Archive of SID.ir

Archive of SID.ir

کامل این پدیده نیستند. اقتصاد تروریسم در واقع، به مطالعه تأمین مالی، هزینه‌ها، درآمدها و مکانیسم‌های اقتصادی گروه‌های تروریستی می‌پردازد. به عبارت دیگر، تمرکز اصلی آن بر چگونگی فعالیت مالی تروریست‌ها و تأثیرات اقتصادی ناشی از اقدامات تروریستی است (Bardwell & Mohib, 2021: 229).

منابع مالی گروه‌های تروریستی عمدتاً از شیوه‌هایی مانند قاچاق مواد مخدر، اخاذی، کمک‌های خارجی، غارت منابع طبیعی و پولشویی تأمین می‌شود. این منابع مالی صرف آموزش، تجهیزات، حقوق اعضاء گروه تروریستی برای دوام و انجام عملیات‌ها می‌باشد. البته، بررسی عملکرد گروه داعش نشان می‌دهد که این گروه از طریق فروش نفت یا مالیات بر مناطق تحت کنترل به تأمین منابع مالی خود اقدام می‌نموده است (El Khoury, 2023: 211). در تروریسم اقتصادی به استفاده عمدی از ابزارهای اقتصادی برای ایجاد رعب، بی‌ثباتی یا آسیب به یک کشور اشاره دارد. این مفهوم بیشتر جنبه سیاستی–امنیتی دارد و ممکن است توسط دولتها، سازمان‌ها یا گروه‌ها انجام شود؛ مانند حملات سایبری به زیرساخت‌های مالی مانند هک بانک‌ها یا سیستم‌های پرداخت یا عملیات خرابکارانه علیه تأسیسات اقتصادی نفت، گاز، خطوط حمل‌ونقل و غیره (Sandler, 2013: 768).

برخلاف «جنگ اقتصادی» که توسط دولت‌ها علیه سایر دولت‌ها انجام می‌شود، «تروریسم اقتصادی» توسط بازیگران فراملی یا غیردولتی صورت می‌گیرد. این امر می‌تواند شامل اقدامات متنوع، هماهنگ، پیچیده یا گسترده برای بی ثبات‌سازی باشد؛ به‌منظور اختلال در ثبات اقتصادی و مالی یک دولت، گروهی از دولت‌ها یا یک جامعه (مانند جوامع غربی با اقتصاد بازارمحور) با انگیزه‌های ایدئولوژیک یا مذهبی. این اقدامات، در صورت وقوع، ممکن است خشونت‌آمیز یا غیرخشونت‌آمیز باشند. این اقدامات می‌توانند یا اثرات فوری داشته باشند یا تأثیرات روانی ایجاد کنند که به نوبه خود، پیامدهای اقتصادی در پی دارند (Freeman, 2012: 4). بر این اساس، می‌توان گفت اقتصاد تروریسم عمدتاً بر سازوکارهای مالی گروه‌های تروریستی، از جمله شیوه‌های تأمین منابع، هزینه‌کردها و تأثیرات اقتصادی فعالیت‌های آنها متمرکز است. در مقابل، تروریسم اقتصادی به استفاده هدفمند از ابزارهای اقتصادی برای ایجاد بی‌ثباتی، هراس یا آسیب به ساختارهای مالی و زیرساختی یک کشور اشاره دارد که ممکن است توسط بازیگران غیردولتی یا حتی دولت‌ها با انگیزه‌های ایدئولوژیک یا سیاسی صورت گیرد. در این میان، گروه‌های تروریستی با بهره‌گیری از روش‌های غیرقانونی همچون قاچاق، اخاذی و غارت منابع طبیعی، پایه‌های مالی خود را تقویت می کنند و از این طریق، به بقا و گسترش عملیات‌های خود ادامه می‌دهند. در مقابل، تروریسم اقتصادی، با ماهیتی پیچیده و چندبُعدی، نه‌تنها می‌تواند موجب اختلال در ثبات مالی کشورها شود، بلکه از طریق اثرات روانی، امنیت اقتصادی جوامع را نیز تحت تأثیر قرار می‌دهد.

۱-۲- نقش عوامل اقتصادی در شکل‌گیری تروریسم

مبارزه مؤثر با تروریسم نیازمند درک عمیق ریشه‌های این پدیده و به‌کارگیری راهبردهای هوشمندانه است، اما این امر که تا چه اندازه اقتصاد و تروریسم بر هم تاثیرگذار هستند، هنوز به روشنی مشخص نیست؛ اگرچه پیرامون تأثیر آنها بر هم تردیدی وجود ندارد.

مشاهده‌ها نشان می‌دهد که بسیاری از افراد دخیل در آنچه تروریسم نامیده می‌شود، در میان فقیرترین مردم نیستند. کشورهای پردرآمد نسبت به کشورهای کم‌درآمد، تروریسم بیشتری را تجربه می‌کنند و عوامل غیراقتصادی گاهی تروریستها را تحریک می‌کنند (دری نوگرانی، ۱۳۹۱: ۱۰۵). مطالعات تجربی نشان می‌دهند که تروریسم بیش از آنکه پدیده‌ای اقتصادی باشد، ماهیتی سیاسی و جمعیتی دارد. عواملی مانند سرکوب سیاسی، ناکارآمدی دولت‌ها، منازعات قومی و سیاست‌های خارجی تحریک‌آمیز نقش تعیین‌کننده‌ای در شکل‌گیری تروریسم ایفا می‌کنند، در حالی که شواهد کمی از تأثیر مستقیم عوامل اقتصادی مانند فقر بر ظهور تروریسم وجود دارد (Li & Schaub, 2004: 230). متأسفانه، مطالعه پیرامون تصمیم فردی برای تبدیل‌شدن به تروریست یا حمایت از تروریسم و وابستگی آن به عوامل اقتصادی با چالش‌های روش‌شناختی قابل‌توجهی مواجه است. این محدودیت عمدتاً

Archive of SID.ir

Archive of SID.ir

ناشی است از: الف- دشواری در جمع‌آوری داده‌های قابل‌اعتماد در سطح فردی؛ ب- چالش‌های اخلاقی در انجام پژوهش‌های میدانی با تروریست‌ها؛ پ- پیچیدگی تحلیل انگیزه‌های چندبعدی افراد. با این وجود، در سطح کلان می‌توان شاخص‌های اقتصادی را در گرایش به تروریسم مؤثر دانست (Meierrieks & Gries, 2013: 2).

مطالعات بیانگر آن است که متغیرهای اقتصادی مانند درآمد سرانه، ب-درجه بازبودن فضای اقتصادی، پ-سطح سرمایه‌گذاری در کنار متغیرهای سیاسی و جمعیتی مانند اندازه جمعیت: الف- اندازه دولت، ب- شاخص دموکراسی، پ- ثبات نظام سیاسی و سابقه وقوع درگیری‌های داخلی می‌تواند در گرایش یا عدم گرایش به تروریسم مؤثر باشد. این بدان معنا است که عوامل اقتصادی به تنهایی عامل گرایش به تروریسم نیستند و این امر در کنار سایر عوامل می‌تواند به عنوان یک متغیر مد نظر قرار گیرد. با این حال، تنها ارتباط اقتصاد با تروریسم تنها دلیل پیوستن به این گروه‌ها نیست و در وجه دیگر باید به هزینه‌های اقدامات تروریستی نیز توجه نمود که با اقتصاد رابطه مستقیم دارد و به نوعی، بیانگر اقتصاد تروریسم است. به عبارت دیگر، هر قدر گروه‌های تروریستی دارای اقتصاد قوی‌تری باشند، اقدامات آنها از گسترش، قوت و تعدد بیشتری برخوردار است.

تحقیقات نشان می‌دهد شرایط نامساعد اقتصادی می‌تواند هزینه‌های فرصت مشارکت در فعالیت‌های تروریستی را کاهش دهد. همچنین، توسعه نیافتگی می‌تواند جذابیت نسبی گزینه‌های رادیکال را افزایش دهد و البته، این عوامل اگرچه ممکن است مستقیماً باعث تروریسم نشوند، اما بستر مناسبی برای گسترش آن فراهم می‌کنند. به علاوه، یافته‌ها نشان می دهد که حتی در مواردی که تروریسم با انگیزه‌های ایدئولوژیک محض همراه است، شرایط اقتصادی بر ظرفیت جذب گروه‌های تروریستی تأثیر می‌گذارد و بهبود این شرایط می‌تواند از گسترش پایگاه اجتماعی تروریسم جلوگیری کند (Freytag, Krüger, Meierrieks, Schneider, 2011: 14). بر این مبناء، می‌توان گفت افزایش هزینه‌های عملیاتی و تضعیف اقتصاد تروریسم، توانایی گروه‌های تروریستی را برای برنامه‌ریزی و اجرای حملات به شدت کاهش می‌دهد. در واقع، تروریسم به عنوان یک پدیده اجتماعی، تابع محاسبات عقلانی هزینه-فایده است. هنگامی که درآمدها کاهش یابد، هزینه‌های لجستیک افزایش یابد و امکان جذب منابع مالی محدود شود، ظرفیت عملیاتی این گروه‌ها به نحو محسوسی تحلیل می‌رود. از این رو، شناخت نظام مالی تروریسم و طراحی راهبردهای هدفمند برای قطع جریان مالی آنان، یکی از مؤثرترین شیوه‌های مقابله با این پدیده به شمار می‌آید. این رویکرد نه تنها توان اجرایی تروریست‌ها را تضعیف می‌کند، بلکه موجب اختلافات درونی و کاهش جذب نیروهای جدید نیز می‌شود.

۲- تأثیرات اقتصاد تروریسم بر امنیت و توسعه پایدار

سنجش تأثیر اقتصادی تروریسم با توجه به افزایش قابل‌توجه حملات تروریستی و تلفات انسانی پس از حادثه یازده سپتامبر ۲۰۰۱ در ایالات متحده و تشدید فعالیت‌های تروریستی در سطح جهانی، از اهمیت ویژه‌ای برخوردار است. درک تأثیرات اقتصادی تروریسم پایه‌ای مستحکم برای ارزیابی تخصیص منابع مالی به برنامه‌ها و فعالیت‌های ضدتروریستی فراهم می آورد. اندازه‌گیری دامنه و هزینه‌های تروریسم، آثار کوتاه‌مدت و بلندمدت آن بر فعالیت‌های اقتصادی را مشخص می‌سازد. برآورد تأثیر اقتصادی تروریسم به سیاستگذاران کمک می‌کند تا با اتکا به شواهد عینی، تحلیل‌هایی مانند بررسی هزینه-فایده برنامه‌های پیشگیری از تروریسم را انجام دهند (Dunne, 2017: 24). تروریسم به علاوه، سایه شومی بر فراز توسعه پایدار سنگینی است، پیوندهای حیاتی اقتصاد و جامعه را می‌گسلد و بذر بی‌ثباتی می‌پاشد. این پدیده شوم با هر حمله، نه تنها جان انسان‌ها، بلکه زیرساخت‌های حیاتی را در چشم به هم‌زدنی فرو می‌ریزند، سرمایه‌های انسانی که سال‌ها برای پرورش آنها وقت صرف شده، در یک آن نابود می‌شوند. تروریسم، اقتصاد را به کام خود می‌کشد، سرمایه‌گذاری‌ها را فراری می‌دهد و گردش مالی را فلج می‌کند. بودجه‌ای که باید صرف مدرسه‌سازی و بیمارستان شود، حالا باید خرج دیوارهای امنیتی و سیستم‌های حفاظتی شود.

سرمایه‌گذاری مستقیم خارجی یکی از مؤلفه‌های اصلی توسعه اقتصادی است و جریان آن تاثیرات بزرگی بر اقتصاد یک کشور

Archive of SID.ir

Archive of SID.ir

دارد. به عبارت دیگر، فعالیت‌های تروریستی امنیت و اعتماد سرمایه‌گذاران را به کشورهای در معرض فعالیتهای تروریستی کاهش می‌دهد و جریان سرمایه‌گذاری مستقیم خارجی را کاهش می‌دهد. از سوی دیگر، هزینه‌های امنیتی ضدتروریستی که بر اقتصاد تحمیل می‌شود، پتانسیل اقتصادی را کاهش می دهد (کفایت، ابراهیمی، زارع و امینی فرد، ۱۴۰۲: ۱۵۳). در کشورهای در حال توسعه، رشد اقتصادی دغدغه اصلی سیاستگذاران و متفکران اقتصادی می‌باشد. شناخت ابزار و عوامل موثر بر رشد اقتصادی در این میان ضروری بوده و بررسی‌های عمیق‌تری را می‌طلبد. اهمیت شناخت عوامل مؤثر در رشد و توسعه کشورها در جهان روبه‌رشد امروز، انکارناپذیر است. میزان اثربخشی و شناخت این عوامل می‌تواند گامی مهم در جهت تسریع رشد و توسعه باشد (Gupta, 2004: 407). تروریسم و افزایش تلفات ناشی از حوادث آن همچنین، اثر منفی بر رشد اقتصادی داشته است. تروریسم از کانال‌های مختلفی بر رشد اقتصادی تأثیر می‌گذارد. افزایش تهدیدات و حوادث تروریستی منجر به ایجاد ناامنی در کشور مبدأ می‌شود و ورود گردشگر را به صورت منفی تحت تأثیر قرار می‌دهد (Bandyopadhyay, 2014: 26). غیبولوئف و سندلر (۲۰۰۸) دریافتند که تروریسم سطح سرمایه‌گذاری مستقیم خارجی و نرخ رشد تولید ناخالص داخلی را کاهش می‌دهد (Gaibulloev & Sandler, 2008: 279). لذا، می‌توان گفت تروریسم با مکانیسم‌های مختلف اقتصاد را تحت تأثیر قرار می دهد. در سطح کلان، تروریسم جریان سرمایه‌گذاری خارجی را مختل کرده و رشد اقتصادی را کند می‌کند. هرچند کمک‌های بین‌المللی ناشی از مقابله با تروریسم ممکن است موقتاً بخشی از خسارات را جبران کند، اما بدون ثبات پایدار، این تأثیرات دوام چندانی ندارند. نکته حائز اهمیت این است که حتی کاهش‌های کوچک در شاخص‌های اقتصادی ناشی از تروریسم، در بلندمدت می‌توانند آسیب‌های جدی به توسعه پایدار کشورها وارد کنند.

۳- اقتصاد تروریسم و جرائم دیجیتال

جرائم دیجیتال جرائمی هستند که در جامعه مدرن شکل گرفته‌اند و از این رو، ابهامات بسیاری پیرامون ماهیت و پیشینه این گونه جرائم از یک سو و ویژگی‌های این جرائم و مرتکبان آنها از سوی دیگر، وجود دارد (موسوی، روحانی مقدم و آقایی، ۱۴۰۱: ۳۲۳). جرائم تروریستی دیجیتالی جنایتی اســت که به خاطر خطراتش شناخته می‌شود و تأثیرات آن بر جامعه و زندگی مردم در طول تاریخ ظاهر شــده است، زیرا جان میلیونها انسان بیگناه را گرفت، جوامع را ویران کرد و این جنایت مرزی نمی شناسد. در عرصه‌های گوناگون، مرتکبان جرائم مختلف از فناوری روز ابزارهای جدیدی برای ارتکاب جرائم خود گرفته‌اند، به طوری که بسیاری از جرائم از طریق اینترنت یا وسایل الکترونیکی مرتکب می‌شوند؛ آنچه جرائم تروریستی دیجیتالی نامیده می‌شود، ظهور کرده است (نامیان و شهبازی، ۱۴۰۳: ۷۷). گروه‌های تروریستی برای تقویت اقتصاد خود و تأمین منابع مالی خود مرتکب جرائم دیجیتال می‌شوند که ذیلاً، به آن‌ها می‌پردازیم.

۳-۱- کلاهبرداری اینترنتی

کلاهبرداری اینترنتی[۱] از عناوین مجرمانه‌ای است که در یکی دو دهه‌ی اخیر به دلیل گسترش فضای اینترنت، شبکه‌های اجتماعی یا سیستم‌های مخابراتی یا رایانه‌ای و مشکلات اقتصادی به خصوص در کشورهای جهان سوم با هدف کسب سود سرشار، بخش بزرگی از جرائم را به خود اختصاص می دهد (نجفی توانا و کریمی، ۱۳۹۹: ۴۱۹). در واقع، کلاهبرداری اینترنتی فعالیت‌های مجرمانه‌ای است که با انگیزه مالی یا سود شخصی انجام می‌شود و هدف اصلی آن، دسترسی غیرقانونی به پول یا اطلاعات افراد یا سازمان‌ها است. این اقدامات می تواند شامل فیشینگ، کلاهبرداری بانکی یا سرقت هویت باشد.

گروه‌های تروریستی از شیوه‌های مختلفی مانند ارسال لینک‌های مخرب اقدام به کلاهبرداری اینترنتی می‌کنند. لینک‌های مخرب از طرق مختلفی مثل ایمیل، پیامک یا شبکه‌های اجتماعی توسط نفوذگران به منظور کلاهبرداری یا

[۱]- کلاهبرداری را یا نه‌ای و اینترنتی در یک مفهوم نیســـت و کلاهبرداری رایانه‌ای یا کامپیوتری اعم از کلاهبرداری اینترنتی است.

Archive of SID.ir

Archive of SID.ir

سوءاستفاده ارسال می‌گردند. البته، روش‌های مختلفی تاکنون برای شناسایی لینک‌های مخرب ارائه شده‌اند که همگی دارای خطا هستند. از طرفی، هکرها با شناسایی چگونگی عملکرد این روش‌ها، فنون خود را تغییر داده و قادرند لینک مخرب خود را به عنوان لینک مفید به قربانی ارائه دهند (دی پیر، ۱۴۰۱: ۱۲۱). یکی از روش‌های مورد استفاده مجرمان سایبری برای انجام کلاهبرداری‌های اینترنتی، سرقت آی پی آدرس[1] افراد است. سرقت آی پی آدرس و سوءاستفاده از آن می‌تواند برای پنهان‌کردن هویت، حملات سایبری یا فریب کاربران و سرویس‌ها مورد استفاده قرار گیرد.

سرقت آی پی در واقع، نوعی سرقت الکترونیکی است که به عنوان پدیده‌ای که حاصل گسترش تکنولوژی‌های الکترونیکی و رایانه‌ای است، امروزه امنیت بسیاری از کاربران رایانه و اینترنت را مختل کرده است. ماهیت این گونه جرائم به دلیل تکنولوژی پیچیده و بالا،خصوصیات منحصربه‌فردی داشته که می‌توان به شیوه ارتکاب آسان، عدم حضور فیزیکی مجرم در محل جرم، خصوصیات فراملی‌بودن و وسعت دامنه جرم اشاره کرد (ستاری و یاده یان، ۱۳۹۵: ۱). لذا، این شیوه و نحوه ارتکاب آن به گروه‌های تروریستی این امکان را می‌دهد که از هر کجای دنیا اقدام به این عمل نمایند.

۳-۲- هک سیستم‌های بانکی

روزی نیست که در اخبار شاهد هک سیستم‌های مختلف مالی به قصد سرقت اطلاعات و منابع مالی نباشیم. این امر بعضاً برای تأمین مالی تروریسم صورت می‌گیرد، اگرچه ممکن است این قصد در واقعیت مخفی بماند و اقدام صورت‌گرفته تنها یک هک برای سرقت منابع به نظر برسد.

بانکداری در عصر دیجیتال امروز شاهد تحولی چشمگیر بوده و از شیوه‌های سنتی و شعبه‌محور به سمت پلتفرم‌های اینترنتی و موبایلی حرکت کرده است. در حال حاضر، مشتریان به لطف گسترش بانکداری دیجیتال و امکانات راحت آن، تقریباً از هر مکان و در هر زمان می‌توانند تراکنش‌های خود را انجام دهند. (Bastari et al, 2020: 5)[2]. بانکداری دیجیتال اگرچه امکانات و سهولت‌های فراوانی ارائه می‌دهد، اما در عین حال تهدیدها و نگرانی‌های جدیدی نیز به همراه دارد. یکی از چالش‌های اصلی در این حوزه، افزایش خطر حملات سایبری است. گسترش استفاده از کانال‌های دیجیتال برای خدمات بانکی، احتمال نقض امنیت و سرقت داده‌ها به‌طور چشمگیری افزایش یافته است.

مجرمین سایبری دائماً در حال توسعه روش‌های جدیدی مانند حملات فیشینگ، بدافزارها و سرقت هویت هستند تا از آسیب‌پذیری‌های سیستم‌های مالی سوءاستفاده کنند. این تهدیدها به یک دغدغه حیاتی تبدیل شده‌اند که نیازمند توجه سازمان‌ها برای حفاظت محرمانه و امن‌سازی سیستم‌های اطلاعاتی است (Admass, Munaye & Dior, 2024: 4-2). در واقع، روش‌های سنتی امنیتی عمدتاً بر تکنیک‌های یادگیری نظارت‌شده متکی هستند که نیازمند دانش ازپیش‌تعریف‌شده درباره انواع خاصی از تهدیدات سایبری می باشند. با این حال، ماهیت پویا و متنوع محیط‌های خانه‌های هوشمند، همراه با ظهور مداوم بردارهای حمله جدید، مستلزم روش‌های انعطاف‌پذیرتر و قوی‌تر برای تشخیص ناهنجاری‌ها است (Sharma & Babbar, 2024: 3). در این صورت است که سیستم‌های امنیتی باید بتوانند به‌صورت خودکار با تهدیدات نوظهور سازگار شوند، بدون آنکه وابسته به الگوهای ازپیش‌شناخته‌شده باشند.

۳-۳- پولشویی دیجیتال

در دوران سلطه پول نقد به عنوان ابزار اصلی مبادلات، پولشویی و تأمین مالی تروریسم مستلزم انتقال پول بود. این انتقال فیزیکی به مجاورت جغرافیایی، قاچاق و یا استفاده از حاملان پول[3] متکی بود؛ اما با ظهور اینترنت و تغییر ساختار بانکها به

[1]- IP Address

[2]- بانکداری دیجیتال که گاهی تحت عنوان نئوبانک‌ها یا بانک‌های مجازی نیز شناخته می‌شود، به ارائه خدمات مالی از طریق پلتفرم‌های دیجیتال مانند اپلیکیشن‌های موبایل، وبسایت‌ها و سایر ابزارهای فناورانه اشاره دارد.

[3]- Money mules

Archive of SID.ir

Archive of SID.ir

بانکهای دیجیتال، ماهیت پولشویی و تأمین مالی تروریسم را تغییر داد (Jaffar et al, 2025: 2-4).

دسترسی به بانکداری الکترونیکی و شبکه‌های اینترنتی، حاشیه امن مناسبی را در اختیار پولشویان قرار داده است. با این فرضیه که بانکداری الکترونیکی موجب تسهیل ارتکاب جرم پولشویی گردیده، روش‌های جدیدی را جهت ارتکاب این جرم پدید آورده است. با بررسی تجارت و بانکداری الکترونیکی و ویژگی های این دو شیوه‌های پولشویی الکترونیکی، فنون رایج و مدرن برای ارتکاب پولشویی الکترونیکی مطرح و فرایند پولشویی سنتی با پولشویی مدرن مورد مقایسه واقع شده است (حبیب زاده و میر مجیدی، ۱۳۹۳: ۲۳).

با پیشرفت فناوری، این گروه‌های تروریستی به‌طور فزاینده‌ای از هوش مصنوعی برای بهبود عملیات پولشویی بهره می‌برند. هوش مصنوعی به تروریست‌ها اجازه می‌دهد تا با استفاده از الگوریتم‌های پیچیده، تراکنش‌های مالی را در حجم انبوه و با سرعت بالا پردازش کنند. روش‌هایی مانند رمزارزها (کریپتوکارنسی)، شبکه‌های عصبی مصنوعی برای شناسایی در پولشویی هستند (Gharbi et al, 2025: 2). علی رغم پیشرفت‌های چشمگیر در سیستم‌های بانکداری دیجیتال و نظارت مالی، بسیاری از نهادهای مالی هنوز در شناسایی و جلوگیری از پولشویی گروه‌های تروریستی ناتوان هستند. بر این اساس، گروه‌های تروریستی به‌طور فزاینده‌ای از هوش مصنوعی برای بهبود عملیات پولشویی بهره می‌برند. هوش مصنوعی به تروریست‌ها اجازه می‌دهد تا با استفاده از الگوریتم‌های پیچیده، تراکنش‌های مالی را در حجم انبوه و با سرعت بالا پردازش کنند.

بسیاری از عملیات مالی تروریستی از طریق شبکه‌های بین‌المللی و با استفاده از حساب‌های جعلی یا ناشناس انجام می‌شود که ردیابی آن‌ها نیازمند هماهنگی فراسرزمینی است؛ امری که هنوز به‌طور کامل محقق نشده است. همچنین، چالش دیگر آن است که برخی کشورها قوانین سختگیرانه‌ای علیه پولشویی ندارند یا اجرای آن‌ها ضعیف است که به تروریست‌ها اجازه می‌دهد از این شکاف‌ها سوءاستفاده کنند.

۳-۴- سرقت اطلاعات هویتی

سرقت هویت یک رفتار تهدید آمیز نوظهور است که با استفاده از اطلاعات اشخاص صورت می‌گیرد و منجر به ضررهای غیرقابل جبرانی در حوزه‌های مختلف، خصوصاً در حوزه مالی می‌شود. سرقت هویت زمانی صورت می‌گیرد که یک فرد اطلاعات شخصی دیگری از قبیل شماره کارت بانکی، شماره حساب، نام و نام‌خانوادگی آن را متعلق به خود قلمداد کرده و از آن‌ها به منظور برداشت از حساب بانکی، افتتاح یک کارت اعتباری جدید یا انجام سایر فعالیت‌های غیرقانونی، استفاده و بهره‌برداری کند (سلیمان دهکردی و حیدریان، ۱۳۹۸: ۶۳). از این عمل به کلاهبرداری هویتی نیز تعبیر می‌شود و کلاهبرداری هویتی در بانکداری به اقدام غیرقانونی و فریبکارانه‌ای اطلاق می‌شود که در آن، فرد متخلف با سرقت یا جعل اطلاعات شخصی، هویت دیگری را برای انجام امور مالی به تصرف درمی‌آورد.[1]

یکی از نقاط ضعف سیستم‌های بانکداری دیجیتال در مبارزه با تأمین مالی تروریسم، نقص در مکانیزم‌های احراز هویت است. تروریست‌ها با استفاده از روش‌های پیشرفته مانند جعل هویت دیجیتال، ساخت حساب‌های جعلی با مدارک تقلبی و بهره‌گیری از هویت‌های دزدیده‌شده، به راحتی می‌توانند از فرآیندهای احراز هویت عبور کنند (Qawasmeh et al, 2025: 93). برخی از پلتفرم‌های مالی غیرمتمرکز و صرافی های رمزارزی، به دلیل عدم الزام به احراز هویت کامل، به بستری امن برای تراکنش‌های مشکوک تبدیل شده‌اند. هوش مصنوعی به تروریست‌ها این امکان را می‌دهند تا مدارک ویدئویی صوتی جعلی تولید کنند و سیستم‌های بیومتریک را نیز فریب دهند (همان: ۹۴). یکی از تحولات چشمگیر، ادغام فناوری نانو (نانوتکنولوژی) در فرآیندهای بانکی، به‌ویژه در فناوری کارت‌های اعتباری است. نانوتکنولوژی امکان ذخیره حجم انبوهی از داده‌ها در فضای حافظه‌ای فشرده را فراهم می کند. اگرچه این نوآوری مزایایی مانند افزایش ظرفیت

[1] https://www.socure.com/glossary/identity-fraud-detection-in-banking

Archive of SID.ir

Archive of SID.ir

ذخیره‌سازی داده‌ها دارد، اما چالش‌های امنیتی جدیدی نیز ایجاد می‌کند (Muhammad Salman, 2023: 2) برداشت پول در بانکداری نوین که یکی از کاربردهای فناوری اطلاعات است، متفاوت بوده و ابزار برداشت فیزیکی به گذرواژه و کارت بانکی تغییر ماهیت داده است. در این روش از بانکداری، احراز هویت توسط تجهیزات رایانه‌ای مثل دستگاه‌های خودپرداز یا کارتخوان‌های فروشگاهی انجام می‌شود (میر محمد صادقی و آذری متین، ۱۳۹۵: ۳۷). بر این اساس، باید گفت که ضعف در سیستم‌های احراز هویت بانکداری دیجیتال، به ویژه در شناسایی تراکنشهای مشکوک، به یکی از چالشهای امنیتی تبدیل شده است. مجرمان با روشهای پیشرفته مانند جعل هویت دیجیتال، ساخت حسابهای تقلبی و سوءاستفاده از هویتهای سرقت‌شده، از این نقاط ضعف بهره‌برداری می‌کنند. همچنین، برخی پلتفرم‌های مالی غیرمتمرکز و صرافی‌های رمزارز به دلیل عدم نظارت کافی، به محلی برای نقل و انتقالات غیرقانونی تبدیل شده‌اند. به طور کلی، مقابله با سرقت هویت و سوءاستفاده از سیستم‌های مالی مستلزم به‌روزرسانی مداوم روش‌های احراز هویت و افزایش آگاهی کاربران در فضای دیجیتال است.

۴- سازوکار پیشگیرانه از اقدامات تروریستی علیه بانکداری دیجیتال

مقابله با اقتصاد تروریسم علیه بانکداری دیجیتال می‌تواند به صورت‌های مختلف انجام پذیرد و این امر با ظهور فناوری‌های نوین خصوصاً، هوش مصنوعی، گام‌های جدیدی را طی نموده است. البته، مقصود از پیشگیری در اینجا پیشگیری وضعی است.

کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند. به عبارت دیگر، این نوع پیشگیری دربرگیرنده مجموعه تدابیر غیرکیفری است که از طریق ازبین‌بردن یا کاهش فرصتهای مناسب از ارتکاب بزه جلوگیری می‌کند (اکرمی، ۱۳۹۵: ۳). لذا، با توجه به جرائم دیجیتال علیه بانکداری می‌توان روش‌هایی را برای مقابله با پولشویی، سرقت هویت و شناسایی تراکنش‌های مشکوک ارائه داد.

۴-۱- کاربرد هوش مصنوعی در پیشگیری از پولشویی

امروزه، استفاده از هوش مصنوعی در بخش مالی به‌ویژه در زمینه‌های مبارزه با تقلب آنلاین، تأمین مالی تروریسم و پولشویی به شدت افزایش یافته است. این فناوری با تحلیل الگوهای تراکنش‌ها و شناسایی ناهنجاری‌های رفتاری، به عنوان ابزاری کارآمد در خدمت نظام‌های نظارتی قرار گرفته است (Alhajeri & Alhashem, 2023: 285). پیشگیری از پولشویی دیجیتال- خصوصاً پیشگیری از پولشویی با بهره گیری از هوش مصنوعی- از دو منظر، جنبه دفاعی دارد. یکی، از منظر بستر ارتکاب جرم، یعنی فضای سایبر که صیانت از موضوع جرم نسبت به پیشگیری از جرم اولویت دارد و تدابیر پیشگیرانه در مقام حفاظت از ارزشهای رایانه‌ای‌اند تا دست مرتکب به آنها نرسد. دوم، از منظر مبادلات مالی الکترونیکی که بر پایه ویژگی‌هایی چون سرعت، انبوهی و تنوع مکانی در عمل، از دسترس تدابیر پیشگیرانه به دور است (عبدالهی و همکاران، ۱۴۰۰: ۳۸۵). پولشویان سعی بر این دارند که در بانکداری الکترونیکی، از فضای اینترنتی و مجازی بیشترین استفاده را در جهت فعالیت‌های مجرمانه خود داشته باشند، چرا که نقل و انتقالات پولی بدون واسطه و گمنام می‌تواند حاشیه امنی را برای آنها ایجاد نماید. روش‌های پولشویی با پیشرفت بانکداری الکترونیکی به تدریج پیچیده‌تر شده و شناسایی آنها با توجه به حجم انبوه اطلاعات، بدون استفاده از سیستم‌های تشخیص پولشویی میسر نیست (انصاری و شاه بهرامی، ۱۳۹۳: ۱۷۹). هوش مصنوعی می‌تواند در مبارزه با پول‌شویی و تأمین مالی تروریسم کمک کند. با استفاده از الگوریتم‌های یادگیری ماشین و شبکه‌های عصبی، هوش مصنوعی می‌تواند الگوهای مشکوک در فعالیت‌های مالی شناسایی کند. این فناوری می تواند الگوهای رفتاری مشتریان و عملکرد مالی شرکت‌ها را تحلیل کرده و تغییرات ناگهانی و نامعمول را شناسایی کند. همچنین، هوش مصنوعی می‌تواند در تجزیه‌وتحلیل شبکه‌های مالی و ارتباطات بین افراد و سازمان‌ها کمک کرده و شبکه‌های مرتبط با پول‌شویی و تروریسم را شناسایی کند (پورعلی و همکاران، ۱۴۰۳: ۱). بسیاری از موسسه‌های مالی برای آسان ترشدن فعالیت‌های مبارزه با پولشویی با استفاده از علم و روش های هوش مصنوعی، فعالیت‌های غیرعادی را در میان

Archive of SID.ir

Archive of SID.ir

داده‌های بی‌شمار شناسایی می‌کنند. بانک‌ها برای مبارزه با پولشویی علاوه بر توانایی مقیاس‌دهی عظیم به فعالیتها، باید تقسیم‌بندی داده‌ها را نیز با دقت انجام دهند (نوربخش و همکاران، ۱۴۰۳: ۱). تشخیص کارآمد و به‌موقع فعالیت‌های مشکوک در جریان‌های داده مالی برای جلوگیری از کلاهبرداری و پولشویی در مؤسسات مالی امری حیاتی است. پایش آنلاین فعالیت‌های مشکوک که از طریق تحلیل داده‌های بلادرنگ امکان‌پذیر شده، به دلیل پاسخگویی سریع، مورد توجه قرار گرفته است. با این حال، پردازش حجم انبوه و توزیع‌شده داده‌های جریانی، چالش‌هایی در دستیابی به کارایی و اثربخشی بلادرنگ ایجاد می‌کند. برای رفع این چالش‌ها، توسعه یک چارچوب پردازش جریان داده ضروری است. برای این منظور، استفاده از داده‌های واقعی و مصنوعی موجب افزایش بهبود دقت سیستم می‌گردد (Gadimov & Ermiyas, 2025: 4). لذا، می‌توان گفت هوش مصنوعی به عنوان یک ابزار قدرتمند در بخش مالی، نقش مهمی در مبارزه با پولشویی و جرائم مالی ایفا می‌کند. این فناوری با تحلیل الگوهای تراکنش‌ها و شناسایی ناهنجاری‌های رفتاری، می تواند فعالیت‌های مشکوک را تشخیص دهد. پولشویان با سوءاستفاده از ویژگی‌های بانکداری الکترونیکی مانند سرعت بالا، حجم انبوه تراکنش‌ها و ناشناس‌بودن نسبی، اقدام به انتقال منابع مالی غیرقانونی می‌کنند که شناسایی این فعالیت‌ها بدون استفاده از سیستم‌های هوشمند تقریباً غیرممکن است. هوش مصنوعی با به‌کارگیری الگوریتم‌های یادگیری ماشین و شبکه‌های عصبی، قادر است رفتارهای غیرعادی مشتریان و نوسانات نامتعارف در حساب‌ها را رصد کند. همچنین، این فناوری می‌تواند با تحلیل شبکه‌های مالی و ارتباطات پیچیده بین افراد و مؤسسات، ساختارهای پولشویی و تأمین مالی تروریسم را شناسایی نماید.

۴-۲- نقش سیستم‌های تشخیص و پیشگیری از نفوذ در سیستم‌های بانکی

پیشرفت فناوری اطلاعات و ارتباطات که امروزه در تمام جنبه‌های زندگی ما نفوذ کرده، امکان کار با انواع اطلاعات را در سطح‌های مختلف شبکه از لایه کاربردی تا سخت‌افزاری فراهم ساخته است. این اطلاعات همواره در معرض تهدیدات امنیتی قرار دارند که می‌توانند درستی، محرمانگی و دسترسی پذیری آنها را به خطر بیندازند. بنابراین، حفاظت از اطلاعات و تضمین امنیت آنها از اهمیت بالایی برخوردار است (Ayofe Azeez et al, 2020: 685). بر این مبناء، صنعت بانکداری دیجیتال در عصر حاضر با چالش‌های امنیتی پیچیده‌ای مواجه است که نیازمند راهکارهای جامع و پیشرفته می‌باشد. در این میان، ترکیب سیستم‌های تشخیص و پیشگیری از نفوذ با فناوری یادگیری ماشین، رویکردی تحول‌آفرین در مقابله با تهدیدات سایبری تروریستی به شمار می‌رود.

فناوری یادگیری ماشین به صورت مستمر تمامی فعالیت‌های شبکه را تحت نظارت قرار داده و هرگونه رفتار غیرعادی یا تلاش برای نفوذ را به تیم امنیتی گزارش می‌دهند. این سیستم‌ها با استفاده از الگوریتم‌های پیشرفته، قادر به شناسایی الگوهای حملات شناخته‌شده و حتی نشانه‌های اولیه تهدیدات جدید هستند. در سطح بالاتر، نه تنها تهدیدات را تشخیص می دهند، بلکه به صورت فعالانه با اعمال فیلترهای پویا، مسدودسازی ترافیک مخرب و به‌روزرسانی قوانین فایروال، از وقوع حملات جلوگیری می‌کنند (Mazhar & et al, 2023: 83). با این حال، ماهیت پویا و هوشمندانه تهدیدات سایبری امروزی نیازمند سطح جدیدی از حفاظت است که در اینجا، فناوری یادگیری ماشین وارد عمل می‌شود.

این فناوری با تحلیل حجم عظیمی از داده‌های تراکنشی و رفتاری، قادر به شناسایی الگوهای پیچیده و روابط نامرئی است که ممکن است از دید سیستم‌های سنتی پنهان بمانند. به طور خاص، در حوزه تشخیص تقلب در تراکنش‌های مالی، الگوریتم‌های یادگیری ماشین با بررسی هزاران پارامتر از جمله مکان تراکنش، مقدار انتقال، زمان انجام عملیات و الگوی رفتاری کاربر، می‌توانند با دقتی بی‌سابقه فعالیت‌های متقلبانه را شناسایی کنند (Apruzzese & et al, 2023: 3-6). همچنین، برای جلوگیری از دسترسی‌های غیرمجاز به سامانه‌ها، ابزارهای متعددی برای ردیابی، پایش، شناسایی و مسدودسازی ترافیک مشکوک در شبکه یا دستگاه‌ها توسعه

Archive of SID.ir

Archive of SID.ir

یافته‌اند. بکارگیری سیستم‌های پیشگیری از نفوذ[1] و سیستم تشخیص نفوذ[2] نیز در مقابله با نفوذ به سیستم‌های بانکی می تواند کارآمد باشد. سامانه پیشگیری از نفوذ یک سیستم کنترلی فعال در شبکه است که تهدیدات ورودی را شناسایی و حملات در حال انجام را متوقف می‌کند؛ در حالی که سامانه تشخیص نفوذ تنها به عنوان ابزاری نظارتی عمل کرده و برای مقابله نیاز به ترکیب هر دو سیستم هست (Kılıç et al, 2019: 544) در واقع، راهکار پیشنهادی برای بانک‌های دیجیتال در مقابل حملات تروریستی به منظور تقویت اقتصادی تروریسم و تأمین مالی، اتخاذ یک استراتژی چندلایه است که در آن، سیستم‌های دفاعی اولیه عمل کرده و فناوری یادگیری ماشین به عنوان لایه هوشمند تحلیل تهدیدات فعالیت می‌کند. این ترکیب هوشمندانه نه تنها امنیت سیستم‌ها را به میزان قابل‌توجهی افزایش می‌دهد، بلکه امکان پیش‌بینی و پیشگیری از تهدیدات آینده را نیز فراهم می‌سازد.

۴-۳- پیشگیری از سرقت هویت توسط گروه‌های تروریستی

گزارش کمیسیون نظارت و تحقیقات و کمیسیون تأمین اجتماعی مجلس نمایندگان آمریکا[3] عنوان می‌دارد که تروریست‌ها، به ویژه عاملان حملات یازدهم سپتامبر، از اطلاعات شخصی سرقت‌شده (سرقت هویت) برای جعل هویت افراد استفاده کرده‌اند تا ضمن فعالیت در ایالات متحده، از شناسایی‌شدن اجتناب کنند. مجرمان با سوءاستفاده از اطلاعات شخصی افراد زنده و متوفی، ضمن جعل هویت آنان، به کلاهبرداری مالی دست زده‌اند. بخش عمده‌ای از شهادت‌ها بر راه‌های جلوگیری از سرقت شماره‌های تأمین اجتماعی برای پنهان‌کردن هویت واقعی و ارتکاب کلاهبرداری متمرکز بود (گزارش کمیسیون، ۲۰۰۲: ۱۴۸). با توجه به اینکه طبق مقررات بین‌المللی از جمله توصیه شماره ده کارگروه ویژه اقدام مالی، احراز هویت مشتری نقش مهمی در مبارزه با پولشویی دارد، ازاین رو ممکن است تصور شود که بانکداری الکترونیکی به دلیل عدم حضور مشتری باعث تسهیل پولشویی می‌شود؛ درصورتی که احراز هویت الکترونیکی نه تنها زمینه‌ساز پولشویی نیست، بلکه روشهای مبتنی بر هوش مصنوعی غیرتحلیلی و روشهای خودکار و دسته‌بندی مانند شبکه‌های عصبی مصنوعی می‌تواند با شناسائی الگوهای رفتاری سوابق مشتری و تطبیق آن با الگوهای تمیز، نسبت به بررسی رفتارهای متقلبانه مشتری پرداخته و مخاطرات پولشویی در بانکداری الکترونیکی را مورد شناسائی قرار دهد و به همین دلیل، توصیه ۱۶ مقررات کارگروه ویژه اقدام مالی به نقل و انتقالات الکترونیکی پرداخته و با الزام به پیش‌بینی اطلاعات فرستنده و ذینفع موجبات شفافیت بیشتر را فراهم کرده است (جعفرپور و هجینی نژاد، ۱۴۰۲: ۶۶). یکی از شیوه‌های پیشگیری «احراز هویت چندعاملی[4]» است. احراز هویت چندعاملی لایه‌های امنیتی اضافی ارائه می‌دهد؛ بنابراین، علاوه بر روش ساده‌ای مانند رمز عبور، تأییدیه دیگری مانند رمز یکبار مصرف به آدرس ایمیل یا دستگاه همراه کاربر ارسال می‌شود تا کد زمان‌دار تولید کند، به این معنی که حداقل دو عامل تأیید شده‌اند (Suleski et al, 2023: 4). شیوه دیگر برای پیشگیری از سرقت هویت «رمزنگاری پیشرفته داده‌ها[5]»ست. رمزنگاری پیشرفته، سپری نفوذناپذیر در برابر تهدیدات سایبری است که با تبدیل داده‌های حساس به رشته‌های به‌ظاهر با پیچیدگی ریاضیاتی خود، از حریم اطلاعات محافظت می‌کند. فناوری‌هایی مثل رمزنگاری هومومورفیک امکان پردازش داده‌های رمزنگاری‌شده را بدون نیاز به آشکارسازی فراهم می آورند، در حالی که توکن‌سازی جایگزینی امن برای ذخیره‌سازی اطلاعات حساس ایجاد می‌کند. این مکانیسم‌ها نه‌تنها از نشت داده‌ها جلوگیری می‌کنند، بلکه چالش‌های امنیتی در تراکنش‌های بانکی را به حداقل می‌رسانند (Tariq et al, 2022: 3). مدیریت هوشمند هویت شیوه دیگری است که می توان از آن برای مقابله با سرقت هویت توسط تروریست‌ها استفاده نمود. مدیریت هوشمند هویت دسترسی چارچوبی امنیتی است که کنترل دقیقی بر دسترسی افراد به سامانه‌های دیجیتال بانک‌ها دارد. این سامانه با شناسایی دقیق هر کاربر،

[1]- Intrusions Prevention Systems (IPS)
[2]- Intrusions Detection System (IDS)
[3]- House Subcommittee on Oversight and Investigations and the House Subcommittee on Social Security
[4]- Multi-Factor Authentication
[5]- End-to-End Encryption

Archive of SID.ir

Archive of SID.ir

از راه‌هایی مانند تأیید هویت چندمرحله‌ای و ویژگی‌های زیست‌سنجی، اطمینان می‌دهد که تنها افراد مجاز می‌توانند به حساب‌ها یا اطلاعات حساس دسترسی پیدا کنند. این روش با تنظیم دسترسی‌ها بر پایه وظایف شغلی هر فرد، اصل «حداقل دسترسی لازم» را رعایت می‌کند تا خطر سوءاستفاده کارکنان یا نفوذ افراد غیرمجاز کاهش یابد. همچنین، این سامانه توانایی پیگیری و ثبت همه فعالیت‌های کاربران را دارد که در شناسایی رفتارهای غیرعادی و واکنش سریع به تهدیدهای امنیتی بسیار کارآمد است. با به‌کارگیری این راهکار، بانک‌ها می‌توانند از دارایی‌های دیجیتال خود در برابر دزدیدن هویت، کلاهبرداری و دیگر تهدیدهای اینترنتی محافظت کنند (Almaiah et al, 2022: 3). با این وصف، می‌توان گفت افزایش این راهکارها لایه‌های امنیتی را افزایش داده و از اقتصاد تروریسم و اقدامات مرتبط با تأمین مالی تروریسم محافظت می‌نماید.

نتیجه گیری

تروریسم به‌عنوان پدیده‌ای پیچیده و چندبُعدی، همواره در حال تحول و سازگاری با فناوری‌های نوین است. در گذشته، این پدیده عمدتاً از طریق خشونت‌های فیزیکی و حملات مستقیم ظهور می‌یافت، اما امروزه با گسترش فناوری‌های دیجیتال، تروریسم سایبری و تروریسم اقتصادی به اشکال جدیدی از تهدید تبدیل شده‌اند. این تحولات نشان می‌دهد که تروریست‌ها به‌طور فزاینده‌ای از ابزارهای مدرن مانند هک، پولشویی دیجیتال، رمزارزها و هوش مصنوعی برای تأمین مالی و اجرای عملیات‌های خود استفاده می‌کنند. در این میان، بانکداری دیجیتال به‌عنوان یکی از ارکان اصلی اقتصاد جهانی، هدفی جذاب برای گروه‌های تروریستی محسوب می‌شود. این گروه‌ها با بهره‌گیری از روش‌هایی مانند کلاهبرداری اینترنتی، هک سیستم‌های بانکی، سرقت هویت و پولشویی دیجیتال، تلاش می‌کنند تا منابع مالی خود را افزایش دهند و امنیت اقتصادی کشورها را تضعیف کنند. از سوی دیگر، تأثیرات مخرب تروریسم بر اقتصاد و توسعه پایدار غیرقابل‌انکار است. حملات تروریستی نه‌تنها باعث نابودی زیرساخت‌های حیاتی و تلفات انسانی می‌شوند، بلکه با ایجاد بی‌ثباتی، سرمایه‌گذاری های خارجی را کاهش داده و رشد اقتصادی را مختل می‌کنند. این پدیده همچنین، هزینه‌های سنگینی را بر نظام‌های امنیتی و مالی کشورها تحمیل می‌کند و منابعی را که می‌توانست صرف توسعه زیرساخت‌های اجتماعی شود، به سمت مقابله با تهدیدات سوق می‌دهد. با این حال، فناوری‌های نوین مانند هوش مصنوعی و یادگیری ماشین می‌توانند در مقابله با اقتصاد تروریسم نقش کلیدی ایفا کنند. سیستم‌های هوشمند تشخیص تقلب، تحلیل رفتار تراکنش‌های مالی و شناسایی الگوهای پولشویی، ابزارهای مؤثری برای خنثی‌سازی فعالیت‌های تروریستی هستند. همچنین، تقویت احراز هویت چندعاملی، رمزنگاری پیشرفته و مدیریت هوشمند دسترسی به سیستم‌های بانکی می‌تواند از سوءاستفاده گروه‌های تروریستی جلوگیری کند. علاوه بر این، همکاری بین‌المللی و تقویت چارچوب‌های قانونی برای نظارت بر تراکنش‌های مالی، به‌ویژه در حوزه رمزارزها و بانکداری دیجیتال، ضرورتی انکارناپذیر است. در نهایت، مبارزه با تروریسم در عصر دیجیتال نیازمند رویکردی جامع است که هم به ریشه‌های سیاسی و اقتصادی این پدیده بپردازد و هم از فناوری‌های پیشرفته برای مقابله با تهدیدات نوظهور استفاده کند. تنها از طریق ترکیب راهبردهای امنیتی هوشمند، نظارت مالی دقیق و همکاری جهانی می‌توان امید داشت که اقتصاد تروریسم تضعیف‌شده و امنیت مالی جوامع در برابر این تهدیدات پایدار باقی بماند.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانت‌داری در استناد به متون و ارجاعات مقاله تماماً رعایت گردید.

تعارض منافع: تدوین این مقاله فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان: نگارش مقاله به‌صورت مشترک توسط نویسندگان انجام گرفته است.

تشکر و قدردانی: از تمام کسانی که ما را در تهیه این مقاله یاری رسانده‌اند، سپاسگزاریم.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی سامان یافته است.

Archive of SID.ir

Archive of SID.ir

منابع و مآخذ

الف. منابع فارسی

– اکرمی، سام و اکرمی، سعیده (۱۳۹۵). پیشگیری غیرکیفری در جرائم اینترنتی. *کنفرانس ملی چارسوی علوم انسانی*.

– انصاری پیرسرایی، زربخش و شاه بهرامی، اسداله (۱۳۹۳). «ضرورت استفاده از سیستم‌های تشخیص پولشویی در بانکداری الکترونیکی». *روند* (روند پژوهش‌های اقتصادی)، ۲۱(۶۸): ۱۷۹–۲۱۲.

– پورعلی، محمدرضا؛ روجائی، حامد و ایران نژاد، وحید (۱۴۰۳). هوش مصنوعی و پول‌شویی. *اولین همایش ملی حسابداری و مدیریت کسب و کار در دنیای دیجیتال*.

– جعفرپور، کوروش و هجینی نژاد، صدیقه (۱۴۰۲). «چالش‌های احراز هویت در بانکداری الکترونیکی با تاکید بر خطر پولشویی». *فصلنامه مطالعاتی در مدیریت بانکی و بانکداری اسلامی*، ۹(۲۵): ۵۷–۸۰.

–حبیب زاده، محمدجعفر و میرمجیدی هشجین، سیده سپیده (۱۳۹۰). نقش بانکداری الکترونیکی در پولشویی و روش‌های مقابله با آن. *پژوهش‌های حقوق تطبیقی*، ۱۵(۱): ۲۳–۴۳.

– دری، نوگورانی، حسین (۱۳۹۱). «اقتصاد تروریسم: مفاهیم، محورهای اساسی و مطالعات تجربی». *فصلنامه آفاق امنیت*، ۱۶: ۱۰۵–۱۳۴.

–ستاری سیاوش و باده یان زیاد (۱۳۹۵). سرقت IP و تهدیدهای مربوط به آن. *کنفرانس بین‌المللی نوآوری در علوم و تکنولوژی*.

–سلیمان دهکردی، الهام و حیدریان، ارشیاناز (۱۳۹۸). «تبیین سرقت هویت در نظام کیفری ایران». *تمدن حقوقی*، ۲(۲): ۶۳–۸۵.

–دی پیر، محمود (۱۴۰۱). «ارائه معیاری برای محاسبه خطر امنیتی لینک‌ها برای جلوگیری از کلاهبرداری‌های اینترنتی». *فناوری اطلاعات و ارتباطات انتظامی*، ۳(۱۱): ۱۲۱–۱۳۱.

–عبدالهی، قهفرخی شهیار؛ پاکزاد، بتول؛ عالی پور، حسن و الهی منش، محمدرضا (۱۴۰۰). «پیشگیری از پولشویی الکترونیکی: رویکرد دفاعی و رویکرد هجومی». *پژوهش‌های حقوق جزا و جرم‌شناسی*، ۹(۱۸): ۳۸۵–۴۰۶.

–کفایت، مجتبی؛ ابراهیمی، مهرزاد؛ زارع، ها شم و امینی فرد، عباس (۱۴۰۴). «اثر تروریسم بر رشد اقتصادی در کشورهای منتخب خاورمیانه: رویکرد اقتصادسنجی فضایی تابلویی». *اقتصاد مقداری*، ۲۰(۷۹): ۱۴۶–۱۷۹.

– موسوی، سیدجمال؛ روحانی مقدم، محمد و آقایی بجستانی، مریم (۱۳۹۱). «اقدامات پیشگیری از جرائم سایبری با تأکید بر اقدامات پلیسی با رویکرد فقهی». *مطالعات فقه و حقوق اسلامی*، ۱۴(۲۶): ۳۲۳–۳۵۸.

–میر محمد صادقی، حسین و آذری متین، افشین (۱۳۹۵). «رویکرد جرم‌شناختی به جعل هویت برای ارتکاب کلاهبرداری در بانکداری نوین». *آموزه های حقوق کیفری*، ۱۳: ۳۵–۶۴.

–نجفی توانا، علی و کریمی، فاطمه (۱۳۹۹). «سیاست پیشگیری و مبارزه با جرم کلاهبرداری اینترنتی». *قانون یار*، ۴(۴): ۴۱۹–۴۴۶.

– نمامیان، پیمان و شهبازی، مهدی (۱۴۰۳). «محافظت از امنیت سکوهای دیجیتالی در قبال جرائم تروریستی؛ راهبردی در ارتقای امنیت دیجیتالی دولتها». *مطالعات و پژوهش‌های امنیت داخلی*، ۲(۵): ۷۳–۹۱.

– نوربخش، محبوبه و سلیمانی امیری، غلام رضا (۱۴۰۳). «بکارگیری هوش مصنوعی برای مبارزه با پولشویی». *دهمین کنفرانس بین‌المللی علوم مدیریت و حسابداری*، تهران.

ب. منابع انگلیسی

-Admass, W.S; Munaye, Y.Y & Diro, A.A. (2024). "Cyber security: state of the art, challenges and future directions". *Cyber Security and Applications*, 2.

-Alhajeri, R & Alhashem, A (2023). *Using Artificial Intelligence to Combat Money*

Archive of SID.ir

Archive of SID.ir

-Ganor, B (2003). *Strategy of Modern Terrorism*, Innovation Exchange Issue: 10.

-Gadimov, E & Birihanu, E (2025). "Real-time suspicious detection framework for financial data streams". *International Journal of Information Technology*.

-Gharbi, Ines et al (2025). "Exploring the Landscape of IoT Ransomware Prediction Through Machine Learning Techniques: A Comprehensive Survey". *SN Computer Science*, 6.

-Gupta, S; Clements, B; Bhattacharya, R., & Chakravarti, S. (2004). "Fiscal consequences of armed conflict and terrorism in low-and middleincome countries". *European journal of political economy*, 20(2).

-Gold, David (2005). *Economics of Terrorism, Defense and Peace Economics*, 16 (6).

-Inuwa, M.M & Das, R (2024). "A comparative analysis of various machine learning methods for anomaly detection in cyber-attacks on IoT networks". *Internet of Things*, 26.

-Jaffar, A et al. (2025). A Comparative Study for IoT Attack Detection Using Machine Learning Algorithms, *Annual Methodological Archive Research Review* 3(5).

-Kılıç, H; Neşet Sertaç Katal, & Aydın Selçuk, A (2019). "Evasion Techniques Efficiency over The IPS/IDS Technology." *In 2019 4th International Conference on Computer Science and Engineering (UBMK)*:542-547.

-Li, Q & Schaub, D (2004). "Economic Globalization and Transnational Terrorism: A Pooled Time-Series Analysis". *The Journal of Conflict Resolution*, 48 (2).

-Meierrieks, D & Gries, Th (2013). "Causality between terrorism and economic Growth". *Journal of Peace Research*, 50 (1).

-Mazhar, T., et al. (2023). Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods, *Future Internet*, 15 (2).

Laundering, Intelligent Information Management.

-Almaiah MA., et al (2022). A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare IoT Based CPS, *Sensors*, 22 (4).

-Apruzzese, G., et al. (2023). *The role of machine learning in cybersecurity, Digital Threats: Research and Practice*, 4 (1).

-Ayofe Azeez, Nureni et al (2020). *Intrusion Detection and Prevention Systems: An Updated Review, Advances in Intelligent Systems and Computing.*

-Bardwell, H & Mohib, I (2021). "The Economic Impact of Terrorism from 2000 to 2018. Peace Economics". *Peace Science and Public Policy*, 27 (2).

-Bastari, A, et al (2020). "Digitalization in banking sector: the role of intrinsic motivation". *Heliyon*, 6 (12).

-Bandyopadhyay, S & Younas, J. (2014). *Terrorism: A threat to foreign direct investment. Doing Business Abroad Policy Report*.

-Combs, C. C (2023). *Terrorism in the Twenty-First Century*. Routledge.

-Dunne, J. P. (2017). "War, Peace, and Development." *The Economics of Peace and Security Journal* 12 (2).

-El Khoury, Chady A (2023). Countering the Financing of Terrorism, *International Monetary Fund*.

-Freeman, Kevin D. (2012) *Secret Weapon: How Economic Terrorism Brought Down the U.S. Stock Market and Why It can Happen Again*, Regnery.

-Freytag, A; Krüger, J: Meierrieks, D & Schneider, F (2011). "The origins of terrorism: Cross-country estimates of socio-economic determinants of terrorism". *European Journal of Political Economy*, 27 (1).

-Gaibulloev, K & T. Sandler. (2019). "What We Have Learned about Terrorism since 9/11." *Journal of Economic Literature*, 57 (2).

Archive of SID.ir

Archive of SID.ir

-Muhammad Salman, H (2023). "Identity Theft in the Banking System". *Online Identity- An Essential Guide*.

-Qawasmeh, S. A et al (2025). "Beyond Firewall: Leveraging Machine Learning for Real-Time Insider Threats Identification and User Profiling". *Computer Science and Engineering*, 17 (2).

-Sharma, A & Babbar, H (2024). "Detecting Malicious Network Activities: Machine Learning-Based ARP Poisoning Detection on RT-IoT2022 Dataset". *Conference*: *2024 Asian Conference on Intelligent Technologies (ACOIT)*..

-Sandler, T (2013). "Advances in the Study of the Economics of Terrorism". *Southern Economic Journal*, 79 (4).

-Suleski, T, et al (2023). *A review of multi-factor authentication in the Internet of Healthcare Things*, National Institutes of Health.

Archive of SID.ir