ماهنامه علمی «امنیت اقتصادی»، مقاله پژوهشی، سال یازدهم، شماره ٦ (پیاپی ١١٣)، شهریور ١٤٠٢، صص ٣٦-٢٣

تبعات امنیت اقتصادی پولشویی در فضای سایبری (سایبرشویی)

سعیده احمدی[1]

چکیده

استفاده از اینترنت همراه با توسعه ارزهای دیجیتال و بلاک‌چین، پول‌شویان را قادر ساخته است تا فعالیت‌های خود را در فضای سایبری گسترش دهند. تراکنش‌های سریع، آسان، کم‌هزینه و ناشناس، پول‌شویی در فضای سایبری را به‌مراتب ساده‌تر کرده است. برخلاف پول‌شویی سنتی، پول‌شویی سایبری نسبتاً جدید است و ارزهای دیجیتال و بلاک‌چین شناسایی و مقابله با این پدیده مذموم را از نظر فنی پیچیده‌تر می‌کند. برای درک هرچه بهتر چیستی پول‌شویی و راه‌های مقابله با آن، در این گزارش، انواع سایبرشویی، متداول‌ترین راه‌های به‌کارگیری عاملان سایبرشویی یا حاملان پول‌های نامشروع برای سایبرشویی و رایج‌ترین روش‌ها و ابزارهای پول‌شویی سایبری مورد بررسی قرار می‌گیرد. همچنین، ملاحظات امنیت اقتصادی پول‌شویی سایبری از سه بعد تهدید امنیتی تأمین مالی تروریسم، تضعیف قدرت دولت و کاهش اعتماد عمومی به نظام بانکی مورد بررسی قرار گرفته است. ازاین‌رو پول‌شویی سایبری به‌عنوان یکی از مهم‌ترین شیوه‌های تأمین مالی تروریسم برای اخلال در امور داخلی کشور دربردارنده پیامدهای امنیتی بسیاری است. با گسترده‌تر شدن استفاده از رمزارزها و درنتیجه، سوءاستفاده از جدیدترین نوآوری‌های فین‌تک برای اهداف غیرقانونی ازجمله پول‌شویی و تأمین مالی تروریسم، لازم است تا با راهکارهایی مانند افزایش میزان آگاهی عمومی نسبت به پول‌شویی سایبری، رسیدگی به فقدان قانون برای مبارزه با جرائم سایبری یا عناصر تغییرات فناوری مرتبط، تقویت همکاری با بخش خصوصی، افزایش دقت و صحت احراز هویت مشتری و استفاده از فناوری‌های نوین مانند هوش مصنوعی برای مقابله با سایبرشویی، پیامدهای منفی این پدیده مذموم را کاهش داد.

واژگان کلیدی: پول‌شویی سایبری، سایبرشویی، امنیت اقتصادی، ارزهای مجازی، بیت‌کوین، قمار آنلاین.

مقدمه

ظهور اینترنت، فضای سایبری و فناوری‌های دیجیتال مزایا و راحتی زیادی را برای زندگی مردم به ارمغان آورده است؛ از خرید اینترنتی گرفته تا رسانه‌های اجتماعی. بااین‌حال، فضای سایبری درها را به روی نوع جدیدی از فعالیت‌های مجرمانه نیز باز کرده است. در میان انبوه فعالیت‌های مجرمانه و جرائم مالی که با اینترنت آسان می‌شود، پول‌شویی به دلیل حجم بالای مبالغ با منشأ غیرقانونی و روش‌های متنوعی که به‌صورت آنلاین برای مشروعیت بخشیدن به آن‌ها استفاده می‌شود، از اهمیت بالایی برخوردار است. پول‌شویی که در فضای سایبری و به‌صورت آنلاین

۱. دانش‌آموخته دکترای اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، ایران، تهران ahmadi.tadbir@gmail.com

انجام می‌شود، با اصطلاح سایبری شویی[1] نیز شناخته می‌شود. پول‌شویان پیوسته به دنبال راه‌های جدید برای جلوگیری از شناسایی توسط مجریان قانون هستند و اینترنت و فضای سایبری فرصت‌های فراوانی برای آن‌ها فراهم کرده و هم‌زمان حوزه مقررات ضد پول‌شویی کنونی را با چالش‌های جدید مواجه کرده است (Calafos & Dimitoglou, 2022).

پول‌شویی سایبری تهدیدی عمده برای سیستم مالی جهانی است؛ زیرا به مجرمان اجازه می‌دهد تا درآمدهای حاصل از فعالیت‌های غیرقانونی و نامشروع خود را پنهان و از آن‌ها استفاده کنند. همچنین، چالشی را برای سازمان‌های مجری قانون ایجاد می‌کند که باید روش‌های خود را برای همگامی با چشم‌انداز دیجیتالی که دائم در حال تغییر است، وفق دهند. شناسایی فعالیت پول‌شویی در فضای سایبری به دلیل حجم بالای معاملات در سطح جهانی بسیار دشوار و پیچیده است.

با توجه به اهمیت این موضوع، برای شناسایی و جلوگیری از این پدیده مذموم، در این گزارش تلاش شده است تا راه‌های نوین پول‌شویی در فضای سایبری مورد بررسی قرار گیرد. ازاین‌رو ابتدا برای بررسی چیستی پول‌شویی در فضای سایبری یا سایبرشویی، به این موضوعات پرداخته می‌شود که پول‌شویان فضای سایبری چه افرادی هستند و متداول‌ترین روش‌ها و ابزارهای سایبرشویی به چه شکل است. در ادامه، چالش‌های این مسئله و ملاحظات امنیت اقتصادی مورد بررسی قرار گرفته و در پایان نیز راهکارهایی برای کاهش پیامدهای پول‌شویی سایبری ارائه شده است.

۱- چیستی پول‌شویی در فضای سایبری یا سایبرشویی

شروع پول‌شویی به قرن ۱۹ می‌رسد؛ یعنی هنگامی که دزدان دریایی پول‌شویی می‌کردند. با گذشت زمان، مفهوم پول‌شویی نیز تغییر یافت. پیشرفت فناوری و جهانی شدن مالی، انتقال غیرقانونی وجوه را آسان‌تر کرد و پس از آن، اصطلاح پول‌شویی سایبری یا سایبرشویی ظهور یافت. سایبرشویی نوعی از پول‌شویی است که در فضای مجازی و با تراکنش‌های آنلاین انجام می‌شود. پول‌شویان از روش‌های متنوع و مبتکرانه‌ای برای پنهان کردن رد پول‌های کثیف استفاده می‌کنند (Joveda et al, 2019). این موضوع شامل استفاده از فناوری‌های پیچیده و پیشرفته مانند ارزهای مجازی، رمزگذاری و ناشناس‌سازی برای پوشش رد پای فعالیت‌های مجرمانه است. در واقع، برخلاف پول‌شویی سنتی، پول‌شویی سایبری نسبتاً جدید است و ارزهای دیجیتال و بلاک‌چین آن را از نظر فنی پیچیده می‌کند (Calafos & Dimitoglou, 2022). برای درک هرچه بهتر چیستی پول‌شویی، در ادامه این بخش، انواع سایبرشویی، متداول‌ترین راه‌های به‌کارگیری عاملان سایبرشویی یا حاملان پول‌های نامشروع برای سایبرشویی و رایج‌ترین روش‌ها و ابزارهای پول‌شویی سایبری مورد بررسی قرار می‌گیرد.

1. Cyber-Laundering

پول‌شویان برای تطهیر پول‌های نامشروع و پول‌شویی‌های خود نیاز به افراد یا عواملی دارند که این کار را برای آن‌ها انجام دهند. در واقع، در پول‌شویی سایبری نقش این افراد در روند واریز حساب‌های مالی شایان توجه است. این افراد با عناوینی مانند قاچاقچی پول، قاطر پول یا حامل پول یا پیک پول شناخته می‌شوند.

۱-۱- انواع پول‌شویی سایبری

باید توجه داشت که فرایند پول‌شویی در فضای سایبری مانند پول‌شویی سنتی معمولاً شامل سه مرحله ۱-جانمایی[1]، ۲-لایه‌بندی[2] و ۳-ادغام[3] است. جانمایی فرایند وارد کردن وجوه غیرقانونی به نظام مالی است. لایه‌بندی شامل انتقال پول از طریق حساب‌های متعدد برای پنهان کردن منشأ آن است. لایه‌های متعدد تراکنش مانند سازمان‌های تجاری، شرکت‌ها و دیگر سازوکارهای پنهان‌سازی در این مرحله میان پول و منبعی که از آن به دست آمده است، قرار می‌گیرند. ادغام، مرحله نهایی است که در آن پول شسته‌شده برای خرید دارایی‌ها یا سرمایه‌گذاری قانونی استفاده می‌شود (Sanction Scanner, 2022).

براین‌اساس، دو نوع شست‌وشوی سایبری وجود دارد که هرکدام ویژگی‌ها و روش‌های منحصربه‌فرد خود را دارند.

- نوع نخست، «**پول‌شویی دیجیتال ابزاری**»[4] نام دارد. در این نوع از پول‌شویی، مجرم از ابزارهای دیجیتالی برای یک یا چند مرحله تشکیل‌دهنده جرم پول‌شویی استفاده می‌کند. این مراحل می‌تواند شامل جانمایی، لایه‌بندی یا ادغام باشد.

- نوع دوم با عنوان «**پول‌شویی دیجیتالی یکپارچه**»[5] شناخته می‌شود. در این نوع پول‌شویی، هر سه مرحله به‌طور کامل و با استفاده از ابزارهای رایانه‌ای یا دیجیتال صورت می‌گیرد. در این نوع پول‌شویی، مجرم سایبری از ارزهای دیجیتال مانند بیت‌کوین برای انتقال وجه از حسابی به حساب دیگر استفاده می‌کند. این نوع پول‌شویی سایبری پیچیده‌تر و دشوارتر است؛ زیرا همه تراکنش‌ها به‌صورت آنلاین و بدون حضور فیزیکی یا رد پای کاغذی انجام می‌شود.

برخلاف روش‌های سنتی پول‌شویی که به نظام بانکی متکی است، سایبرشویی به استفاده از انواع مختلفی از تراکنش‌ها و ارائه‌دهندگان خدمات مالی بستگی دارد (Eurasiangroup : 2014).

۱-۲- متداول‌ترین روش‌های به‌کارگیری افراد در پول‌شویی سایبری

در ابتدا باید به این نکته توجه داشت که پول‌شویان برای تطهیر پول‌های نامشروع و پول‌شویی‌های

1. Placement Stage
2. Layering Stage
3. Integration Stage
4. Instrumental Digital Laundering
5. Integral Digital Laundering

خود نیاز به افراد یا عواملی دارند که این کار را برای آن‌ها انجام دهند. در واقع، در پول‌شویی سایبری نقش این افراد در روند واریز حساب‌های مالی شایان توجه است. این افراد با عناوینی مانند قاچاقچی پول، قاطر پول[1] یا حامل پول یا پیک پول[2] شناخته می‌شوند. قاطرهای پول در اصطلاح اشخاصی هستند که پول به‌دست‌آمده غیرقانونی را به نیابت از دیگران دریافت می‌کنند و انتقال می‌دهند. این قاچاقچیان ممکن است در ازای مشارکت خود کمیسیون دریافت کنند یا نکنند. بعضی از این حاملان پول‌های غیرقانونی می‌دانند که نقش اصلی را در طرحی غیرقانونی ایفا می‌کنند درحالی‌که برخی دیگر از این افراد از این مسئله هیچ آگاهی‌ای ندارند یا تنها به آن مشکوک هستند. در ادامه، عمده‌ترین روش‌های شایان توجه پول‌شویی در فضای سایبری که سازمان‌های جنایی با استفاده از آن‌ها به دنبال جذب قاطرهای پول هستند، مورد بررسی قرار می‌گیرد.

۱-۲-۱- استفاده از شبکه‌های اجتماعی

شبکه‌های اجتماعی یکی از محبوب‌ترین پلتفرم‌ها برای تعامل با دیگران است و میلیون‌ها کاربر از سراسر جهان از این پلتفرم‌ها برای برقراری ارتباط با یکدیگر استفاده می‌کنند (Parida & Kumar, 2020). بر اساس بررسی‌های انجام‌شده، کلاهبرداران با پلتفرم‌های شبکه‌های اجتماعی مانند فیس‌بوک، اینستاگرام، تلگرام و...، سایت‌ها و تارنماهای دوست‌یابی آنلاین یا سایت‌ها و وبگاه‌های تبلیغات شغلی که مدت‌ها مورد هدف مجرمان سایبری قرار گرفته است، با افراد مختلف ارتباط برقرار می‌کنند. این سایت‌ها و وبگاه‌ها برای سرقت اطلاعات با بدافزارها هدف قرار می‌گیرند و برای استخدام حاملان پول و توزیع بدافزار توسط پول‌شویان استفاده می‌شوند. در دسته‌بندی کلی، در این روش از تکنیک‌های زیر برای به‌کارگیری قاطران یا حاملان پول استفاده می‌شود.

- کلاهبرداری‌های شغلی

در کلاهبرداری‌های شغلی با افراد درباره شغل جدید بدون درخواست تماس گرفته می‌شود و کارفرما هیچ جزئیاتی درباره شرکت خود ارائه نمی‌دهد. در این روش، مدیران تقلبی با پست‌های الکترونیکی تجاری یا شبکه‌های اجتماعی، از افراد می‌خواهند تا پول را به حساب‌های مربوط به مجرمان منتقل کنند (Global South Dialogue on Economic Crime, 2023). آن‌ها برای جلب اعتماد مشتریان، از نام‌های مشابه شرکت‌های مشهور بین‌المللی و نیز اسناد جعلی برای کلاهبرداری از قربانیان استفاده می‌کنند. اغلب، مقادیر خارج‌شده خیلی زیاد نیست تا از سوءظن قربانیان جلوگیری شود. پس از دریافت، وجوه بی‌درنگ از حساب چه به‌صورت نقدی و چه از طریق انتقال به نمایندگی برداشت می‌شود (Tookitaki, 2019).

- کلاهبرداری‌های عاشقانه

با افراد به‌صورت آنلاین از طریق رسانه‌های اجتماعی یا پلتفرم دوست‌یابی تماس گرفته

1. Mone Mule
2. Money Couriers

می‌شود. طعمه‌هایی که از طریق کلاهبرداری‌های عاشقانه جذب می‌شوند. در این نوع کلاهبرداری، پولشویان با ایجاد رابطه‌ای عاشقانه با قربانیان خود، اعتماد آنها را جلب کرده و سپس قربانیان را ترغیب به واریز وجوه به حساب‌های بانکی خود و سپس انتقال این مبالغ به حساب‌های مورد نظر پول‌شویان می‌کنند.

- کلاهبرداری‌های سرمایه‌گذاری

در شبکه‌های اجتماعی تبلیغات گسترده‌ای درباره کسب سودهای نجومی در ازای سرمایه‌گذاری انجام می‌شود. مردم از سوی پول‌شویان به واریز وجوه به حساب‌های بانکی خود ترغیب می‌شوند. این وجوه در مدت کوتاهی برداشت یا به دیگر حساب‌های بانکی یا حساب‌های خدمات مالی تلفن همراه کلاهبرداران منتقل می‌شود.

۱-۲-۲- جعل و سرقت هویت[1]

در این روش، مجرمان از نام یا هویت قربانی برای ارتکاب جرم استفاده می‌کنند. مشخصات هویتی فرد شامل نام، شماره ملی و اطلاعات مالی (شماره حساب و پین) با روش‌های مختلف مانند فیشینگ از طریق رسانه‌های الکترونیکی، تماس‌های صوتی یا بسترهای پیام‌رسان فوری به دست می‌آید یا اینکه در تماس‌ها یا پیام‌هایی از سوی افرادی که وانمود می‌کنند از سازمان‌های دولتی هستند، اطلاعات شخصی و بانکی افراد درخواست می‌شود. سپس از این اطلاعات برای ارتکاب تخلفاتی ازجمله کلاهبرداری از کارت اعتباری و نقل‌وانتقالات غیرمجاز از طریق بانکداری اینترنتی استفاده می‌شود.

۱-۲-۳- قمار و شرطبندی‌های آنلاین[2]

مانند قمار در دنیای واقعی، قمار آنلاین و برخط یکی دیگر از راه‌های سریع و کارآمد برای مشروعیت بخشیدن به وجوه غیرقانونی و پول‌شویی است. پلتفرم‌های آنلاینی وجود دارند که قمار و شرطبندی‌ها را با ابزارهایی ازجمله پوکر، کازینو و شرطبندی ورزشی آسان می‌کنند. بسیاری از حوزه‌های قضایی کشورها قمار آنلاین را ممنوع یا محدود می‌کنند. بااین‌حال، برخی از مجرمان از طریق این گزینه‌ها کسب درآمد می‌کنند و درآمدهای غیرقانونی را به حساب‌های بانکی انتقال می‌دهند تا آن‌ها را قانونی کنند (Pacini et al, 2020).

در جمع‌بندی کلی می‌توان گفت حاملان یا قاطران پول به‌صورت ناآگاهانه و احتمالاً از طریق آگهی‌های شغلی آنلاین و پست‌های الکترونیکی ناخواسته جذب سازمان‌های پول‌شو می‌شوند. همچنین، ممکن است سوژه‌ها از طریق کلاهبرداری‌ها و قرعه‌کشی استخدام شوند. قاطران پول که اغلب ناآگاه هستند، با ارائه حساب‌های خود برای دریافت و انتقال وجوه تقلبی، به کلاهبرداران و پول‌شویان کمک می‌کنند تا پول‌های آن‌ها را مشروع جلوه دهند. جنایت‌کاران و کلاهبرداران به شیوه‌های مختلف قاطرهای پول را به خدمت می‌گیرند. برای مثال، برخی افراد با وعده سود مالی اغوا می‌شوند یا در ازای خدمات خود پورسانت دریافت می‌کنند. در موارد دیگر، انگیزه آن‌ها اعتماد

1. Identity Theft
2. Online Gambling

به چیزی است که از طریق کلاهبرداری‌های آنلاین درخواست می‌شود.

پول‌شویی سایبری را می‌توان به روش‌های مختلف انجام داد مانند مدیریت کیف پول الکترونیکی یا ایجاد شرکت یا سازمانی که در واقعیت وجود ندارد، اما در فضای مجازی وجود دارد و سپس تراکنش مالی را به حساب آن منتقل کنند تا پول نامشروع را تطهیر کنند و نشان دهند که پول به‌دست‌آمده قانونی است.

۱-۳- رایج‌ترین روش‌ها و ابزارهای سایبرشویی

پول‌شویی سایبری معمولاً در اینترنت انجام می‌شود و از اشکالات و حفره‌های رایانه‌ای یا از سیستم‌های سخت‌افزاری و نرم‌افزاری خاص برای ایجاد ارتباط ناشناس و غیرقابل ردیابی موقعیت مکانی استفاده می‌شود. این روش به مجرمان اجازه می‌دهد تا مجریان قانون را فریب دهند و بدون شناسایی، فعالیت‌های غیرقانونی خود را انجام دهند.

در سال‌های اخیر، موارد متعددی از پول‌شویی سایبری وجود داشته است که مجرمان از روش‌های پیچیده‌تر برای فعالیت‌های غیرقانونی خود استفاده کرده و سازمان‌های مجری قانون مجبور شده‌اند خود را با این شرایط در حال تغییر وفق دهند و برای همگام شدن با سرعت پیشرفت فناوری، روی فناوری و آموزش، سرمایه‌گذاری زیادی انجام دهند (Sanction Scanner, 2022).

پول‌شویی سایبری را می‌توان به روش‌های مختلف انجام داد مانند مدیریت کیف پول الکترونیکی یا ایجاد شرکت یا سازمانی که در واقعیت وجود ندارد، اما در فضای مجازی وجود دارد و سپس تراکنش مالی را به حساب آن منتقل کنند تا پول نامشروع را تطهیر کنند و نشان دهند که پول به‌دست‌آمده قانونی است.

یکی از رایج‌ترین روش‌های سایبرشویی با ارزهای مجازی مانند بیت‌کوین است که امکان تراکنش‌های ناشناس و غیرقابل ردیابی را فراهم می‌کند. مجرمان می‌توانند از این ارزها برای خرید کالاها و خدمات به‌صورت آنلاین، انتقال وجوه به خارج از مرزها و تبدیل عواید به ارزهای سنتی استفاده کنند. امکان پول‌شویی با بیت‌کوین و دیگر رمزارزها به‌سادگی وجود دارد. در هر تراکنش مالی در بیت‌کوین، نشانی فرستنده و گیرنده به شکل دقیقی ثبت می‌شود. این نشانی مربوط به شخصی است که این تراکنش را انجام داده است، اما در این فرایند نیازی به ارائه هویت نیست. بنابراین، بسیاری از افراد با استفاده از هویت‌های جعلی نسبت به تراکنش‌های مربوط اقدام می‌کنند.

روش دیگر، استفاده از ابزارهای ارتباطی و رمزگذاری ناشناس مانند تور[1] و وی‌پی‌ان[2] است که به مجرمان اجازه می‌دهد بدون شناسایی، ارتباط برقرار کنند و وجوه را انتقال دهند. آن‌ها همچنین، از

1. Tor
2. VPN

تکنیک‌های پیچیده‌ای مانند سرویس‌های «میکس» استفاده می‌کنند که وجوه چند تراکنش را با هم ترکیب می‌کند تا ردیابی منبع اصلی را دشوار کند (Calafos & Dimitoglou, 2022).

۱-٤- دلایل سایبرشویی

سایبرشویی نیز مانند پول‌شویی به دلایلی مانند موارد زیر رخ می‌دهد.

- دلیل اساسی پنهان‌کاری در فرار مالیاتی است.
- نبود شفافیت سیاسی و حکمرانی که باعث فساد در کل بخش‌های جامعه شده است.
- حجم بالای اشتغال غیررسمی و معاملات غیررسمی کلان در اقتصاد که باعث می‌شود منشأ اصلی منابع مالی کاملاً نامشخص باشد.
- بی‌ثباتی سیاسی نگرانی عمده برای سرمایه‌گذاران است که آن‌ها را وادار می‌کند تا برای منابع مالی خود مقصد خارجی بیابند (Joveda et al, 2019).

۱-۵- پول‌شویان چه افرادی هستند؟

هرساله حجم زیادی از پول غیرقانونی شست‌وشو می‌شود؛ زیرا قانون مبارزه با پول‌شویی و سیستم امنیت سایبری برای جلوگیری از فرار سرمایه در بسیاری از کشورها ناکافی به نظر می‌رسد. برخی کارشناسان بر این باورند که برخلاف تصور عامه، پول‌شویی بین‌المللی اغلب توسط افرادی که در فعالیت‌های مجرمانه و غیرقانونی با هم ارتباط برقرار می‌کنند، انجام نمی‌شود، بلکه توسط کارشناسانی انجام می‌شود که با عملکرد بازارهای سرمایه بین‌المللی آشنا هستند و می‌توانند ریسک‌های اقتصادی را تعیین و شناسایی کنند.

شناسایی و استفاده از تفاوت در کنترل‌ها و مقررات میان کشورها عامل اصلی پول‌شویی است. پول‌شویی توسط مردان حزب حاکم، تاجران دولتی و بوروکرات‌های ارشد در کشورها انجام می‌شود. گاهی اوقات نیز با تبانی واردکنندگان، صادرکنندگان و مسئولان بانکی انجام می‌شود. تاجران مواد مخدر، قاچاقچیان، تروریست‌ها، فروشندگان غیرقانونی اسلحه و مقامات فاسد خصوصی و دولتی نیز در پول‌شویی دست دارند (Joveda et al, 2019). این افراد برای پول‌شویی‌های خود از عاملان پول‌شویی استفاده می‌کنند که همان حاملان پول‌های نامشروع یا قاچاقچیان پول هستند که پیش‌تر به‌تفصیل بررسی شد.

۲- چالش‌های تشخیص سایبرشویی و مقابله با آن

مجرمان سایبری عمدتاً به دنبال سود بالا هستند که منجر به افزایش جرائم رایانه‌ای در بخش مالی می‌شود که خود مستلزم درک عمیق و دانش روابط مالی و فعالیت بانکی است. افزون‌براین، مجرمان سایبری فعالانه از خدمات مجرمان «سنتی» استفاده می‌کنند که به آن‌ها کمک می‌کند تا وجوه دزدیده‌شده را به پول نقد تبدیل کنند (Eurasiangroup, 2014). سایبرشویی موضوعی جدی است و بعضی مسائل، تشخیص پول‌شویی در فضای سایبری را با مشکل

مواجه می‌کند که در ادامه به برخی از آن‌ها اشاره می‌شود.

۲-۱- کشف نشدن پول‌شویی در فضای سایبری

شبکه‌های رایانه‌ای موجود و زیرساخت‌های مبتنی بر فناوری اطلاعات، محیط مساعدی را فراهم می‌کند تا عرضه بین‌المللی کالا، ارائه خدمات و انتقال وجه میان اشخاص حقیقی و حقوقی به‌راحتی انجام شود. همچنین، امکان اتصال رایانه‌ها به اینترنت و ذخیره آنلاین اطلاعات را فراهم می‌کند. از سوی دیگر، فرصت‌های گسترده‌ای را برای ارتکاب جرائم سایبری و همچنین، پول‌شویی عواید ناشی از جرائم سایبری و دیگر جرائم را با استفاده از فناوری‌های رایانه‌ای فراهم می‌کند.

یکی از مشکلات و چالش‌های عمده این است که ممکن است سایبرشویی ناشناخته بماند. به دلیل گستردگی فناوری، نفوذ سایبری در کمتر از ثانیه رخ می‌دهد. این موضوع از طریق حساب‌های قدیمی و استفاده‌نشده رخ می‌دهد. بانک‌ها حساب‌هایی را که ناگهان شروع به فعالیت می‌کنند، گزارش نمی‌دهند. زیرساخت‌های یادشده به مجرمان اجازه می‌دهد تا به‌سرعت به هرگونه اطلاعات، اسناد و دارایی‌های خصوصی و سیستم‌های پرداخت آنلاین ارزان و عملاً ناشناس دسترسی داشته باشند که آن‌ها را قادر می‌سازد آثار جرم خود را پنهان و درآمدهای غیرقانونی به‌دست‌آمده را به روشی مقرون‌به‌صرفه جابه‌جا کنند.

اقدامات تروریستی نیازمند نیروی انسانی و امکانات متعدد است که همگی منوط به تأمین مالی گروه تروریست است. وقایع تروریستی چند سال اخیر رژیم صهیونیستی علیه برخی از دانشمندان کشور یا ایجاد اخلال و ناآرامی‌ها در داخل کشور از این موارد است. تأمین مالی گروه‌های تروریستی با توجه به محدودیت‌های فیزیکی تا اندازه زیادی مخاطره‌آمیز است، اما اگر این تأمین مالی از طریق پول‌شویی سایبری و رمزارزها صورت بگیرد، مسیر کشف آن‌ها برای نیروهای امنیتی کشور بسیار سخت می‌شود.

۲-۲- سازوکار پیشگیری و اجرایی ضعیف

سازوکار اجرایی مقابله با پول‌شویی کند و آن‌طور که لازم است با سرعت بسیار بالا کار نمی‌کند. تراکنش‌های غیرقانونی در مراحل اولیه گزارش نمی‌شوند و مجرمان به پول‌شویی ادامه می‌دهند که باعث آسیب بیشتر می‌شود. سازوکار رویه‌ای نیز با تحقیقات طولانی و جمع‌آوری داده‌ها و دیگر مطالب مفید که برای چند ماه ادامه می‌یابد، باعث تأخیر می‌شود و زمان زیادی می‌برد.

در واقع، انفجار فناوری اطلاعات و پیچیدگی این حوزه به همراه فرایند طولانی و بیش از حد بوروکراتیک ابلاغ قوانین و چهارچوب نظارتی مربوط منجر به وضعیتی شده است که گسترش جرائم سایبری به‌مراتب از اقدامات انجام‌شده برای

پیشگیری و مبارزه با این نوع تخلفات پیشی گرفته است. ماهیت طولانی و پیچیده تحقیقات درباره جرائم سایبری و مشکلات استفاده از شواهد (ازجمله مدارک الکترونیکی) برای تعقیب کیفری یکی از مهم‌ترین چالش‌های مقابله با سایبرشویی است.

۲-۳- ظهور و گسترش ارزهای دیجیتال

تحولات فناورانه جدیدی از طریق ارز دیجیتال شکل‌گرفته است. وقتی از ارزهای رمزنگاری‌شده یا بیت‌کوین به‌عنوان روشی برای معامله غیرقانونی استفاده شود، این دلیلی برای پول‌شویی می‌شود. زنجیره تراکنش با ذخیره سکه‌های فیات و سپس نقد کردن آن‌ها به روش نقدی جایگزین صورت می‌گیرد. پول‌شویان این کار را برای تشکیل واکنش زنجیره بلوکی و پوشاندن رد پای خود از طریق لایه‌بندی تعدادی از تراکنش‌ها انجام می‌دهند. این باعث می‌شود که گرفتن فرد سخت‌تر شود. همچنین، با کمک واسطه اقدام می‌کنند و حساب آن‌ها را تأیید می‌کنند که پس از آن نمی‌توان به چنین فعالیت‌هایی مشکوک شد (Anand, 2023).

۲-٤- ماهیت پیچیده جرائم سایبری

افزون‌بر کسب سود مالی یا دیگر منافع مادی ناشی از ارتکاب جرائم سایبری، مرتکبان از فناوری‌های رایانه‌ای و شبکه‌های اطلاعاتی و ارتباطی با انگیزه‌های روانی-اجتماعی نیز سوءاستفاده می‌کنند؛ به‌ویژه اعمال جرائم سایبری برای بی‌اعتبار کردن دولت‌ها و کشورها، راه‌اندازی سایت‌ها و وبگاه‌های تروریستی، آسیب رساندن و تخریب سیستم‌های کلیدی با وارد کردن داده‌های نادرست در چنین سیستم‌هایی یا غیرقابل اجرا کردن آن‌ها (که مکمل تروریسم سنتی است) انجام می‌شود.

۲-۵- ناشناس بودن مجرمان سایبری

فقدان تماس مستقیم فیزیکی، مجازات نسبتاً سبک اعمال‌شده در برخی کشورها و مشکلات در شناسایی، ثبت و ضبط اطلاعات مرتبط با جرم در فضای مجازی، جرائم سایبری را برای مجرمان جذاب می‌کند.

۲-٦- ماهیت فراملی و گسترده جرائم سایبری

ویژگی جرائم سایبری که درباره پول‌شویی در فضای سایبری نیز صادق است، این است که جرائم سایبری تقریباً از هر مکانی که مجرم به اینترنت دسترسی داشته باشد، ارتکاب‌پذیر است. در شرایطی که تجهیزات رایانه‌ای و خدمات آنلاین در دسترس تعداد فزاینده‌ای از مردم است، جرائم سایبری نیز به‌طور فزاینده‌ای محبوب هستند. ماهیت فراملی جرائم سایبری فرصت‌های جذابی را برای مجرمان فراهم می‌کند؛ به‌طوری‌که مجرمان می‌توانند در کشورهایی با سیستم‌های قضایی منفعل در مبارزه با جرائم سایبری و و رژیم‌های نظارتی که بعید است مشمول تحقیقات انجام‌شده آژانس‌های مجری قانون خارجی شوند، فعالیت کنند (Eurasiangroup, 2014).

۳- ملاحظات امنیت اقتصادی

ملاحظات امنیت اقتصادی پول‌شویی سایبری را می‌توان از سه بعد مختلف مورد بررسی قرار داد.

– **تهدید امنیتی تأمین مالی تروریسم:** همان‌طور که در بخش‌های پیش نیز توضیح داده شد، افزایش فعالیت با رمزارزها یا ارزهای دیجیتال، پول‌شویی در فضای سایبری را به‌مراتب ساده‌تر کرده است؛ زیرا رمزارزها نمونه‌هایی از ارزهای دیجیتالی هستند که در بستر اینترنت ایجاد می‌شوند. ازاین‌رو فناوری رمزنگاری استفاده‌شده در آن‌ها، راه را برای پول‌شویی‌های احتمالی باز می‌گذارد. طبق بررسی‌های انجام‌شده، بیت‌کوین و دیگر ارزهای دیجیتال این امکان را برای پول‌شویان فراهم می‌کند تا فرایند انتقال و حرکت وجوه غیرقانونی را سریع‌تر، ارزان‌تر و پراکنده‌تر از همیشه انجام دهند. این موضوع زمانی نگران‌کننده و تهدید قلمداد می‌شود که بدانیم می‌توان از این ابزار برای تأمین مالی تروریسم استفاده کرد؛ مسئله‌ای که کشورمان در سال‌های اخیر با آن مواجه بوده است.

اقدامات تروریستی نیازمند نیروی انسانی و امکانات متعدد است که همگی منوط به تأمین مالی گروه تروریست است. وقایع تروریستی چند سال اخیر رژیم صهیونیستی علیه برخی از دانشمندان کشور یا ایجاد اخلال و ناآرامی‌ها در داخل کشور از این موارد است. تأمین مالی گروه‌های تروریستی با توجه به محدودیت‌های فیزیکی تا اندازه زیادی مخاطره‌آمیز است، اما اگر این تأمین مالی از طریق پول‌شویی سایبری و رمزارزها صورت بگیرد، مسیر کشف آن‌ها برای نیروهای امنیتی کشور بسیار سخت می‌شود. ازاین‌رو، پول‌شویی سایبری به‌عنوان یکی از مهم‌ترین شیوه‌های تأمین مالی تروریسم برای اخلال در امور داخلی کشورمان دربردارنده پیامدهای امنیتی بسیاری است.

– **تضعیف قدرت دولت:** باید به این موضوع توجه داشت که پول‌شویی چه از طریق سنتی چه از طریق پول‌شویی سایبری موجب دسترسی آسان مجرمان به منابع مالی می‌شود و انتقال قدرت اقتصادی از دولت و مردم به بزهکاران را در پی دارد. پول‌شویان از تدبیر ارتشا یا سهیم کردن مسئولان دولتی در عواید و سود ناشی از پول‌شویی به میزانی فراتر از آنچه دولت به آن‌ها پرداخت می‌کند، می‌توانند در بسیاری از امور اقتصادی دخالت کنند. پول‌شویی از طریق فساد مقامات و سیستم‌های حقوقی، امنیت ملی را تهدید می‌کند؛ زیرا انکارناپذیر است که درآمد تولیدشده برخی از جرائم سازمان‌یافته بسیار بیشتر از پرداختی دولت‌ها به کارمندان خود است. در چنین وضعیتی، نوعی قدرت اقتصادی در بدنه کشورها شکل می‌گیرد که توانایی اعمال نفوذ در قدرت سیاسی را دارد. این موضوع از کانال‌های مختلف مانند تضعیف قدرت دولت، رشد فساد، کاهش مشروعیت حاکمیت، افزایش تضاد طبقاتی و... باعث تضعیف امنیت اقتصادی و به‌تبع آن، تهدید امنیت ملی در کشورها می‌شود.

– **کاهش اعتماد عمومی به نظام بانکی:** افزایش تعداد جرائم سایبری ارتکابی در زمینه پول‌شویی به کاهش اعتماد عمومی نسبت به یکپارچگی سیستم مالی، اسرار بانکی، حفاظت از داده‌های شخصی و تراکنش‌های مالی انجام‌شده با استفاده

از فناوری‌های جدید منجر شده است. چنین بی‌اعتمادی عمومی به بازارهای خدمات مالی مانع از سرمایه‌گذاری وجوه در دسترس مردم برای توسعه اقتصادی می‌شود. بی‌اعتمادی عمومی شکل‌گرفته نسبت به نظام بانکی سبب می‌شود نقدینگی عامه مردم به‌جای بانک‌ها به‌عنوان یکی از بهترین مکان‌های سرمایه‌گذاری از بعد کلان اقتصادی، سر از بازارهای کاذب و گاه مخرب مانند بازار ارز، سکه، خودرو یا مسکن درآورد و با ایجاد موج روانی در بازار همان‌طور که بارها شاهد بوده‌ایم، پیامدهای گسترده‌ای ایجاد کند.

در واقع، افشای اطلاعات محرمانه ازجمله اسرار بانکی و داده‌های شخصی نتیجه پول‌شویی سایبری است که موجب بی‌اعتمادی مشتریان به نظام بانکی به‌طورکلی و خدمات بانکی از راه دور (آنلاین) به‌طور خاص می‌شود که درنهایت، به کاهش حجم تراکنش‌های غیرنقدی می‌انجامد. این موضوع پیامدهای فناورانه برای مؤسسات بانکی، شرکت‌ها و سازمان‌ها دارد؛ زیرا مجبور به ایجاد (یا خرید) ابزارها و محصولات امنیتی پیچیده، گران‌قیمت و کمتر راحت خواهند شد تا از عملکرد قابل اعتماد اطلاعات، رایانه‌ها و سیستم‌های مخابراتی خود اطمینان حاصل کنند.

نتیجه‌گیری و ارائه راهکارها

پول‌شویی سایبری یا سایبرشویی روشی است که از طریق آن پول‌شویی در اینترنت یا از طریق دنیای دیجیتال انجام می‌شود. وسعت روزافزون و پیشرفت‌های چندگانه فناوری، راه را برای وقوع جرائم در فضای سایبری هموار کرده است. جرائم سایبری با نقض اطلاعات فناوری دیجیتال اتفاق می‌افتد و باعث تهدید سایبری و دیگر فعالیت‌های مجرمانه می‌شود. با ابداع روش‌های جدید مانند ارزهای دیجیتال، بیت‌کوین و دیگر روش‌های پرداخت پولی، راه برای رخنه به روشی سریع‌تر و تقریباً غیرقابل شناسایی فراهم شده است که سبب آسیب و تحریف داده‌ها در مسیر پول‌شویی می‌شود (Anand, 2023). پول شویان برای تطهیر درآمدهای نامشروع خود نیاز به افراد یا عواملی دارند که این کار را برای آن ها انجام دهند. این افراد که به‌اصطلاح حاملان یا قاطران پول نامیده می‌شوند، معمولاً افراد ناآگاه و بزرگ‌سالان آسیب‌پذیر هستند که غالباً پیر و تنها و به‌صورت بالقوه از نظر مالی در مضیقه هستند. کلاهبرداران در نقش یک شکارچی، سعی می‌کنند بر اساس دروغ، با این افراد رابطه برقرار کنند. طرح‌هایی که شرکت‌کنندگان ناآگاه را هدف قرار می‌دهند، معمولاً بر کلاهبرداری در شغل و رابطه متمرکز هستند. در برهه‌ای از زمان، قربانیان این طرح‌ها (به‌ویژه کلاهبرداری‌های استخدامی) ممکن است به حامل حرفه‌ای پول‌شویی یا دست‌کم نیمه‌آگاه نسبت به کاری که انجام می‌دهند، تبدیل شوند. آن‌ها می‌دانند که ممکن است بخشی از طرحی غیرقانونی باشند، اما به دلیل شرایط شخصی همچنان به کسب درآمد ادامه می‌دهند. آن‌ها

می‌دانند که درگیر طرحی غیرقانونی هستند، اما احتمالاً کاری را که انجام می‌دهند، غیرقانونی نمی‌دانند. افزون‌براین، آن‌ها معتقدند یا به آن‌ها گفته شده است که اقداماتشان غیرقانونی نیست.

بی‌توجهی به پول‌شویی سایبری دربردارنده پیامدهای بسیاری است. ازاین‌رو راهکارهای زیر برای مبارزه مؤثر با پدیده پول‌شویی در فضای سایبری و کاهش موانع و مشکلات این مبارزه ارائه می‌شود.

- **افزایش میزان آگاهی عمومی نسبت به پول‌شویی سایبری:** یکی از مشکلات عمده مربوط به پول‌شویی سایبری این است که مردم نسبت به این مسائل آگاهی چندانی ندارند. طرح‌های آگاهی‌بخشی لازم است تا مردم عادی هنگام استفاده از شبکه‌های اجتماعی یا معاملات آنلاین مراقب باشند و در دام کلاهبرداران و پول‌شویان گرفتار نشوند. فریب افراد از این طریق وجود دارد و بنابراین، امنیت شبکه و آگاهی رویه‌ای مردم باید وجود داشته باشد. باید به عموم مردم آموزش داده شود که آگهی‌های کاریابی که به درخواست از آن‌ها برای ثبت‌نام در سایت‌های فروش ارز دیجیتال و اقدام برای خرید رمزارز ختم می‌شود، کلاهبرداری و به قصد سوءاستفاده از هویت و حساب بانکی آن‌ها با اهداف مجرمانه بوده و دربردارنده مسئولیت قانونی برای آن‌هاست. نهادهای متولی این موضوع مانند مرکز ملی فضای مجازی، سازمان فناوری اطلاعات ایران، وزارت فرهنگ و ارشاد اسلامی و پلیس فتا وظیفه دارند آگاهی‌ها و آموزش‌های لازم در این باره را از طریق رسانه‌ها در اختیار عموم مردم قرار دهند.

- **رسیدگی به فقدان قانون مبارزه با جرائم سایبری یا عناصر تغییرات فناوری مرتبط:** پول‌شویی معضلی مهم است، اما هنگامی که این مشکل به فضای سایبری می‌رسد، آسیب‌های بیشتری در پی دارد. بنابراین، نیاز است که خلأهای موجود در قوانین موجود بررسی شود تا چالش‌های جاری شناسایی و با اقدامات سخت‌گیرانه و شناسایی، فعالیت‌های مجرمانه در بازه زمانی مناسب برطرف شود. ضروری است که مجرمان این‌گونه جرائم از طریق خلأ فنی یا قانونی که ممکن است وجود داشته باشد، از آن فرار نکنند. عدم تعیین مجازات برای استفاده از فیلترشکن‌ها که باعث مجهول ماندن بیش‌ازپیش هویت مرتکبان جرائم سایبری می‌شود، نقش حائز اهمیتی در ناقص ماندن اجرای مجازات و جبران خسارت دارد. ازاین‌رو مرکز اطلاعات مالی به‌عنوان یکی از متولیان اصلی مبارزه با پول‌شویی در کشور، باید با نهادهای متولی دیگر مانند سازمان فناوری اطلاعات ایران، شورای‌عالی فضای مجازی و مجلس شورای اسلامی همکاری داشته باشد تا بتواند کاستی‌های حقوقی موجود را شناسایی و برطرف کند.

- **تقویت همکاری با بخش خصوصی:** موضوع امنیت فضای سایبری در ظاهر مسئله حاکمیتی است، اما موضوع امنیت فضای سایبری و بازار محصولات امنیتی همواره مورد توجه بخش خصوصی هم بوده است. تجربه کشورهای دیگر نشان می‌دهد که بخش خصوصی می‌تواند نقش مهم و بزرگی در این میان

داشته باشد. رویکردهای مشارکتی و نه تنبیهی برای دریافت کمک از شرکت‌های خصوصی مانند رسانه‌های اجتماعی و شرکت‌های مخابراتی، ممکن است برای مقابله با جرائم سایبری ازجمله پول‌شویی سایبری ثمربخش باشد.

– **افزایش دقت و صحت احراز هویت مشتری:** یکی از راهکارهای موجود برای مبارزه با پول‌شویی در رمزارزها، اجرای مقررات شناسایی مشتری یا احراز هویت مشتری در صرافی‌ها یا کارگزاری‌های مجاز معاملات است؛ زیرا درصورتی‌که هویت افراد در صرافی‌ها به‌طور کامل ثبت شود، امکان مبارزه با پول‌شویی نیز فراهم خواهد شد. این مهم باید از طریق بانک مرکزی و دیگر نهادهای نظارتی مسئول مانند وزارت اطلاعات مورد پیگیری قرار گیرد. ازآنجاکه وزارت اطلاعات متولی زیرساخت‌های فناورانه کشور است، قطعاً این موضوع به این وزارتخانه مرتبط است.

– **استفاده از فناوری‌های نوین مانند هوش مصنوعی برای مقابله با سایبرشویی:** هوش مصنوعی آینده جهان است که نمی‌توان آن را انکار کرد. توسعه و سرمایه‌گذاری در هوش مصنوعی به حل مشکل پول‌شویی در فضای سایبری کمک می‌کند. این فناوری به شناسایی هر نوع فعالیت دقیقی که در وبگاه یا هر حساب دیگری اتفاق می‌افتد، کمک می‌کند و گام‌ها را به سمت فردی که در حال پول‌شویی است، هدایت می‌کند. بسیاری از کشورها در تلاش برای به‌کارگیری بهترین و امن‌ترین راه‌های احراز هویت با استفاده از هوش مصنوعی و مطابق با فناوری‌های روز دنیا هستند تا با معضل پول‌شویی در رمزارزها مقابله کنند. شورای‌عالی فضای مجازی به‌عنوان مسئول نظارت و سیاست‌گذاری در موضوعات مرتبط با فضای مجازی ازجمله هوش مصنوعی، معاونت علمی و فناوری ریاست‌جمهوری و دیگر نهادهای متولی مانند مرکز اطلاعات مالی و... باید در این باره همکاری‌های لازم را داشته باشند تا بتوان مانند دیگر کشورها از این فناوری‌ها برای مقابله با پولشویی سایبری در کشور استفاده کرد.

سایبرشویی نوعی از پول‌شویی است که در فضای مجازی و با تراکنش‌های آنلاین انجام می‌شود. پول‌شویان از روش‌های متنوع و مبتکرانه‌ای برای پنهان کردن رد پول‌های کثیف استفاده می‌کنند. این موضوع شامل استفاده از فناوری‌های پیچیده و پیشرفته مانند ارزهای مجازی، رمزگذاری و ناشناس‌سازی برای پوشش رد پای فعالیت‌های مجرمانه است.

منابع

– Anand, A., (2023). Cyber Money Laundering in Digital Age, Amikus Qriae, Available in www.theamikusqriae.com.

- Calafos, M. W., & Dimitoglou, G. (2022). Home Principles and Practice of

Blockchains Chapter Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency, SpringerLink, Available in www.link.springer.com.

– Parida, D. K., & Kumar, D. P. (2020). A Framework to Score the Risk Associated with Suspicious Money Laundering Activity and Social Media Profile. *Indian Journal of Finance and Banking*, *4*(2), 1-10.

Eurasiangroup (2014). Typology Project Cybercrime and Money Laundering, Eurasian Group on Combating Money Laundering and Financing of Terrorism, Available in www.eurasiangroup.org.

- Global South Dialogue on Economic Crime (2023). Cyber-enabled crime: the new frontier of global money laundering, Available in www.gsdec.network.

– Joveda, N., Khan, M. T., Pathak, A., & Chattogram, B. (2019). Cyber Laundering: a Threat to Banking Industries in Bangladesh: in Quest of Effective Legal Framework and Cyber Security of Financial Information. *International Journal of Economics and Finance*, *11*(10), 54-65.

- Pacini, C., Stowell, N. F., Katz, I. J., Patterson, G. A., & Lin, J. W. (2020). An Analysis of Money Laundering, Shell Entities, and no Ownership Transparency That Washes Off and on Many Shores: a Building Tidal Wave of Policy Responses. *Kan. JL & Pub. Pol'y*, *30*, 1.

– Sanction Scanner (2022). Cyber-Laundering and Cyberterrorism, Available in www.sanctionscanner.com.

– Tookitaki Holding (2019). 6 Most Prevalent Cyber-Laundering Methods in APAC, Available in www.tookitaki.com.