



Designing a Model of the Deterrent Capacities of Social Networks in the Prevention of Cybercrimes

Farid Mohseni 

Department of Criminal Law and Criminology, Faculty of Law, University of Judicial Sciences and Administrative Services, Tehran, Iran

Neda Shahmirzalu * 

Department of Public Administration, Faculty of Management and Accounting, Central Tehran Branch, Islamic Azad University, Tehran, Iran

Abstract

Objective: The present study aims to explore and explain a comprehensive model of the deterrent capacities of social networks for the prevention of cybercrimes. This research seeks to identify the technical, legal, and social components in order to provide an integrated framework for enhancing security within the digital ecosystem.

Methodology: This research is applied in terms of purpose and mixed-methods (qualitative–quantitative) in terms of the nature of the data. In the qualitative phase, data obtained from semi-structured interviews with 15 experts in the fields of criminology and cybersecurity, selected through purposive sampling, were analyzed using Braun and Clarke’s thematic analysis strategy and Attride-Stirling’s thematic network approach. In the quantitative phase, in order to validate the extracted model, a researcher-made questionnaire was distributed among users, and the data were analyzed using the structural equation modeling technique. The validity and reliability of the research instrument in both phases were confirmed through test-retest indices, content validity, and Cronbach’s alpha.

Findings: The qualitative results led to the identification of 92 basic themes, 24 organizing themes, and 6 global themes, including platform protective responsibility, awareness of cyber rights and duties, user self-control, normative health of the environment, perceived social surveillance, and reduction of cyber victimization. In the quantitative phase, the findings indicated that all model relationships were confirmed with critical values exceeding 1.96. The strongest statistical linkage was related to the effect of perceived social surveillance on user self-control (8.879) and the mediating role of self-control in reducing victimization (8.489). Furthermore, platform protective responsibility, with a coefficient of 5.214, was identified as the primary driver of situational prevention.

Conclusion: The research findings demonstrate that sustainable security in cyberspace is the product of synergy among the technical architecture of platforms, the supervisory authority of governing institutions, and the enhancement of users' legal literacy. Accordingly, policymakers should focus on the necessity of implementing security protocols in design and strengthening the individual defense chain through protective education.

Keywords: Deterrent Capacities, Social Networks in Prevention, Cybercrimes, Thematic Analysis, Structural Equation Modeling

Citation: Mohseni, Farid, Shahmirzalu, Neda. Designing a Model of the Deterrent Capacities of Social Networks in the Prevention of Cybercrimes, Cases pp101-122 1(1).

طراحی مدل ظرفیت‌های بازدارندگی شبکه‌های اجتماعی در پیشگیری از جرائم سایبری

فرید محسنی

استاد گروه حقوق جزا و جرم‌شناسی، دانشکده حقوق، دانشگاه علوم قضایی و خدمات اداری، تهران، ایران. رایانامه: mohseni@ujsas.ac.ir

ندا شاهمیرزالو*

* دکتری تخصصی گروه مدیریت دولتی و خط مشی گذاری عمومی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران رایانامه: n.shahmirzaloo@iau.ac.ir

چکیده

هدف: پژوهش حاضر با هدف واکاوی و تبیین مدل جامع ظرفیت‌های بازدارندگی شبکه‌های اجتماعی در راستای پیشگیری از جرائم سایبری انجام شده است. این مطالعه در پی آن است تا با شناسایی مؤلفه‌های فنی، حقوقی و اجتماعی، الگویی یکپارچه برای ارتقای امنیت در زیست‌بوم دیجیتال ارائه دهد.

روش‌شناسی: این پژوهش از نظر هدف، کاربردی و از نظر ماهیت داده‌ها، از نوع آمیخته (کیفی - کمی) است. در بخش کیفی، با استفاده از استراتژی تحلیل مضمون براون و کلارک و شبکه مضامین آنرید - استرلینگ، داده‌های حاصل از مصاحبه‌های نیمه‌ساختاریافته با پانزده نفر از خبرگان حوزه جرم‌شناسی و امنیت سایبری که به روش نمونه‌گیری هدفمند انتخاب شده بودند، تحلیل شد. در بخش کمی، به منظور اعتبارسنجی مدل استخراج‌شده، پرسش‌نامه‌ای محقق‌ساخته میان کاربران توزیع شد و داده‌ها با استفاده از تکنیک مدل‌سازی معادلات ساختاری، مورد تجزیه و تحلیل قرار گرفتند. روایی و پایایی ابزار تحقیق در هر دو بخش با استفاده از شاخص‌های بازآزمون، روایی محتوایی و آلفای کرونباخ به تأیید رسید.

یافته‌ها: نتایج بخش کیفی به شناسایی ۹۲ مضمون پایه، ۲۴ مضمون سازمان‌دهنده و شش مضمون فراگیر شامل مسئولیت صیانتی پلتفرم، آگاهی از حقوق و تکالیف سایبری، خودکنترلی کاربران، سلامت هنجاری محیط، نظارت اجتماعی ادراک‌شده و کاهش بزه‌دیدگی سایبری منجر شد. در بخش کمی، یافته‌ها نشان داد که تمامی روابط مدل با مقادیر بحرانی فراتر از ۹۶/۱ تأیید شده‌اند. قوی‌ترین پیوند آماری مربوط به اثرگذاری نظارت اجتماعی ادراک‌شده بر خودکنترلی کاربران (۸۷۹/۸) و نقش میانجی خودکنترلی در کاهش بزه‌دیدگی (۴۸۹/۸) بود. همچنین مسئولیت صیانتی پلتفرم با ضریب ۲۱۴/۵ به عنوان پیشران اصلی پیشگیری وضعی شناسایی شد.

نتیجه‌گیری: یافته‌های پژوهش نشان می‌دهد که امنیت پایدار در فضای مجازی، محصول هم‌افزایی میان معماری فنی پلتفرم، اقتدار نظارتی نهادهای حاکمیتی و ارتقای سواد حقوقی کاربران است. بر این اساس، سیاست‌گذاران باید بر لزوم پیاده‌سازی پروتکل‌های امنیت در طراحی و تقویت زنجیره دفاعی فردی از طریق آموزش‌های صیانتی تمرکز کنند.

واژه‌های کلیدی: ظرفیت‌های بازدارندگی، شبکه‌های اجتماعی در پیشگیری، جرائم سایبری، تحلیل مضمون، مدل‌سازی معادلات ساختاری.

استناد: محسنی، فرید؛ شاهمیرزالو، ندا؛ (۱۴۰۵). طراحی مدل ظرفیت‌های بازدارندگی شبکه‌های اجتماعی در پیشگیری از جرائم سایبری. مدیریت قضایی. یک (۱)، صص.

۱۲۲-۱۰۱

تاریخ دریافت: ۱۴۰۵/۱/۵

:

تاریخ پذیرش: ۱۴۰۵/۳/۱۳

:

مدیریت قضایی، ۱۴۰۵، دوره ۱، شماره ۱، صص. ۱۰۱-۱۲۲

ناشر: دانشگاه علوم قضایی و خدمات اداری

نوع مقاله: علمی

© نویسندگان

مقدمه

تحولات بنیادین ناشی از رسوخ گسترده فضای مجازی، علاوه بر بازتعریف سبک زندگی، مرزهای سنتی حکمرانی و تعاملات شهروندی را دستخوش تغییرات اساسی کرده است (حسینی جردچی و همکاران، ۱۴۰۲). این دگرگونی‌های ساختاری علی‌رغم تسهیل ارتباطات، بستری مستعد برای رشد جرائم سایبری فراهم آورده‌اند؛ پدیده‌ای که به‌عنوان فعالیت مجرمانه از طریق سیستم‌های رایانه‌ای با هدف قرار دادن زیرساخت‌های دیجیتال تعریف می‌شود (ترنر و ابروتین،^۱ ۲۰۱۶؛ محمدی مقدم و همکاران، ۱۴۰۱). مجرمان با بهره‌گیری از ویژگی‌های ذاتی فضای سایبر همچون اتصال بی‌مرز و گمنامی، طیف گسترده‌ای از اقدامات غیرقانونی از فیشینگ و سرقت هویت تا جرائم علیه امنیت ملی را سازماندهی می‌کنند (ترنر،^۲ ۲۰۲۳). شواهد نشان می‌دهد که نرخ روزافزون این جرائم، محصول تعامل پیچیده میان حضور فراگیر رسانه‌های اجتماعی و آسیب‌پذیری‌های نهفته در سیستم‌های به‌هم‌پیوسته است (طاهر دوست،^۳ ۲۰۲۴؛ مارتتیللا^۴ و همکاران، ۲۰۲۱). از منظر جرم‌شناختی، تبیین این پدیده بر پایه نظریه فعالیت‌های روزمره/ سبک زندگی^۵ نشان‌دهنده آن است که چگونه تکرار و شدت استفاده از پلتفرم‌هایی نظیر اینستاگرام و فیس‌بوک، احتمال مواجهه کاربران با مهاجمان انگیزه‌دار را افزایش می‌دهد (سان میگل^۶ و همکاران، ۲۰۲۰؛ بک و گورت،^۷ ۲۰۲۱). درواقع، رفتارهای پرخطر و استفاده مشکل‌ساز از رسانه‌های اجتماعی^۸ مستقیماً با افزایش نرخ قربانی شدن در فضای مجازی پیوند خورده است (مارتتیللا و همکاران، ۲۰۲۱؛ اکرمی^۹ و همکاران، ۲۰۲۴). با این حال، پارادوکسی در این میان وجود دارد؛ شبکه‌های اجتماعی که به‌دلیل تسهیل تبادل سریع اطلاعات، زمینه‌ای مساعد برای طعمه‌گذاری و سوءاستفاده‌های مالی فراهم کرده‌اند (محسنی، ۱۴۰۲؛ محمدی و صادق‌یان لمرسکی، ۱۴۰۳)، هم‌زمان واجد ظرفیت‌های بالقوه‌ای برای بازدارندگی و پیشگیری از جرم هستند. به‌منظور فعلیت بخشیدن به این پتانسیل‌های پیشگیرانه، رویکرد پیشگیری از جرم موقعیتی^{۱۰} بر کاهش فرصت‌های ارتکاب جرم از طریق اصلاح مؤلفه‌های محیطی و رفتاری تأکید می‌ورزد (هو^{۱۱} و همکاران، ۲۰۲۲). این رویکرد معتقد است با به‌کارگیری تکنیک‌های فناورمحور در بطن پلتفرم‌های مجازی، می‌توان انگیزه‌های مجرمانه را مهار و هزینه ارتکاب جرم را افزایش داد (خادژی‌رادپوا^{۱۲} و همکاران، ۲۰۲۴). در این چارچوب، هویت عملیاتی و ساختار فنی هر شبکه اجتماعی تعیین‌کننده نوع مداخلات پیشگیرانه و ظرفیت بازدارندگی آن پلتفرم است (خان،^{۱۳} ۲۰۲۱؛ اقبال^{۱۴} و همکاران، ۲۰۱۹). علاوه بر جنبه‌های ساختاری، تغییر رفتار پایدار کاربران نیازمند درک روان‌شناختی بر پایه مدل باور سلامت است که پذیرش رفتارهای محافظتی را تابعی از ادراک کاربران نسبت به حساسیت و شدت تهدیدات می‌داند

1. Turner & Abrutyn

2. Turner

3. Taherdoost

4. Marttila

5. LRAT

6. San Miguel

7. Back & Guerette

8. PSMU

9. Akrami

10. SC

11. Ho

12. Khadzhyradieva

13. Khan

14. Iqbal

(مک‌فرسون،^۱ ۲۰۱۸). اگرچه آگاهی‌بخشی امری حیاتی است، اما عدم درک صحیح از مزایای استراتژی‌های پیشگیری باعث می‌شود برخی کاربران از به‌کارگیری دانش خود خودداری کنند؛ موضوعی که بر ضرورت آموزش‌های مهارت‌محور جهت تقویت خودکنترلی تأکید دارد (خادژی‌رادیه‌وا و همکاران،^۲ ۲۰۲۴؛ درو و فارل،^۳ ۲۰۱۸). امروزه بهره‌گیری از فناوری‌های نوظهور، پتانسیل شبکه‌های اجتماعی را از یک منبع خطر به ابزاری قدرتمند برای پیش‌بینی حملات تبدیل کرده است (گانگولی،^۴ ۲۰۲۴؛ گوپتا^۵ و همکاران، ۲۰۲۵؛ اسلام^۶ و همکاران، ۲۰۲۰). علی‌رغم گستردگی مطالعات بین‌المللی در حوزه امنیت سایبری، بررسی متون پیشین نشان می‌دهد که تاکنون پژوهشی جامع با تمرکز بر واکاوی ظرفیت‌های بازدارندگی شبکه‌های اجتماعی در بستر بومی ایران و با رویکردی چندوجهی انجام نشده است. بخش عمده‌ای از تحقیقات داخلی بر جنبه‌های آسیب‌شناختی و جرم‌انگاری متمرکز بوده و از تحلیل پتانسیل‌های فنی و ساختاری پلتفرم‌ها به‌عنوان ابزارهای پیشگیرانه مغفول مانده‌اند. لذا، شکاف عملیاتی موجود در فقدان مدلی است که بتواند مؤلفه‌های خودکنترلی کاربران ایرانی را با ویژگی‌های فنی - اجتماعی شبکه‌های مجازی تلاقی دهد. ضرورت بومی‌سازی این پژوهش از آنجا ناشی می‌شود که الگوهای بزه‌دیدگی و نظارت اجتماعی در ایران، متأثر از ویژگی‌های فرهنگی، حقوقی و زیرساخت‌های خاص شبکه ملی است که مدل‌های غیربومی لزوماً پاسخ‌گوی پیچیدگی‌های آن نیستند. بر این اساس، تحقیق حاضر با هدف پر کردن این خلأ علمی، در پی تبیین چارچوبی بومی است که ضمن شناسایی ظرفیت‌های بازدارنده، راهکارهای عملیاتی جهت کاهش نرخ جرائم سایبری در جامعه دیجیتال ایران ارائه دهد. لذا مسئله بنیادین این تحقیق در قالب این پرسش اصلی تبلور می‌یابد که طراحی مدل ظرفیت‌های بازدارندگی شبکه‌های اجتماعی در پیشگیری از جرائم سایبری چگونه است؟

مبانی نظری و پیشینه تجربی تحقیق

مبانی نظری تحقیق

تحلیل زیرساختی شبکه‌های اجتماعی نشان می‌دهد که این پلتفرم‌ها فراتر از ابزارهای صرف ارتباطی، واجد ظرفیت‌های عملیاتی استراتژیکی هستند که بازتعریف آن‌ها می‌تواند به‌طور مستقیم به شناسایی و تقلیل رفتارهای مجرمانه منجر شود (اقبال و همکاران،^۷ ۲۰۱۹؛ طاهر دوست^۸، ۲۰۲۴). بر این اساس، ویژگی‌هایی نظیر پروفایل‌های کاربری و نگاشت‌های شبکه‌ای، پتانسیل تبدیل شدن به ابزارهای بازدارنده را دارند؛ به‌طوری که در پلتفرم‌هایی همچون تلگرام و اینستاگرام، ایجاد بسترهای رمزگذاری‌شده و تحلیل داده‌های بلادرنگ، امکان نظارت دقیق بر تراکنش‌های اطلاعاتی را فراهم آورده و با ارتقای توانمندی سیستم در تشخیص زودهنگام فیشینگ و کلاهبرداری، مانع از وقوع جرم می‌شوند (بک و گورت^۹، ۲۰۲۱؛ خان، ۲۰۲۱؛ اوبی^۱ و همکاران، ۲۰۲۴). در تبیین تئوریک این فرایند، پیشگیری از جرم

1. Macpherson
2. Khadzhayradieva
3. Drew & Farrell
4. Ganguli
5. Gupta
6. Islam
7. Iqbal
8. Taherdoost
9. Back & Guerette

موقعیتی به عنوان رکن اصلی بازدارندگی عمل می‌کند. این نظریه با تأکید بر مدیریت محیطی، از طریق دشوار ساختن مسیر ارتکاب بزه و افزایش ریسک شناسایی، هزینه‌های جرم را برای مجرمان افزایش می‌دهد و بدین ترتیب، ظرفیت بازدارندگی پلتفرم را فعلیت می‌بخشد (هو و همکاران، ۲۰۲۲؛ خادژی‌رادیه‌وا و همکاران، ۲۰۲۴). در این چارچوب، شبکه‌های اجتماعی با اصلاح عوامل محیطی، از حالت انفعالی خارج شده و به ابزارهای نظارتی مبدل می‌شوند که با بهره‌گیری از سرمایه اجتماعی، امنیت جمعی را در برابر تهدیدات سازمان‌یافته تضمین می‌کنند (محسنی، ۱۴۰۲؛ ترنر، ۲۰۲۳؛ محمدی مقدم و همکاران، ۱۴۰۲). در لایه رفتاری، ظرفیت بازدارندگی از طریق آموزش سایبری تقویت می‌شود که به عنوان یک محرک پیشگیرانه، تاب‌آوری کاربران را در برابر جرائمی نظیر نفرت‌پراکنی و قلدری سایبری افزایش می‌دهد (اومیگو، ۲۰۲۳؛ اکرمی و همکاران، ۲۰۲۴). این رویکرد آموزشی، با ترویج هنجارهای امنیتی، کاربران را از اهداف بالقوه به کنشگرانی بازدارنده تبدیل می‌کند که با گزارش رفتارهای مخرب، از بازتولید جرم جلوگیری می‌کنند (یانکسون^۶ و همکاران، ۲۰۲۴؛ سان میگل و همکاران^۷، ۲۰۲۰). از منظر تکنولوژیک، بازدارندگی پیشگیرانه بر مدل‌های هوشمندی تکیه دارد که با تحلیل الگوهای تعاملی، پیش از وقوع جرائم پیچیده را فعال می‌کنند (گوپتا و همکاران^۸، ۲۰۲۵؛ اسلام و همکاران^۹، ۲۰۲۰). این تلاقی میان فناوری و تحلیل رفتار، لایه‌ای از بازدارندگی فنی ایجاد می‌کند که حتی در محیط‌های رمزگذاری شده، شناسایی مجرمان را تسهیل می‌کند و مانع از تحقق نیت مجرمانه می‌شود (گوپتا و همکاران^{۱۰}، ۲۰۲۵). اثربخشی نهایی ظرفیت‌های بازدارنده مستلزم تحقق نظارت اجتماعی مشروع و طراحی الگوریتم‌های پاسخ‌گوست که ضمن صیانت از حریم خصوصی، فرایند گشت‌زنی در رسانه‌های اجتماعی را به ابزاری برای پیشگیری تبدیل کنند (گانگولی^{۱۱}، ۲۰۲۴؛ درو^{۱۲}، ۲۰۲۰). درواقع، پیشگیری پایدار زمانی محقق می‌شود که مداخلات فناورانه با سواد دیجیتالی کاربران ادغام شده و نظارت اجتماعی در بطن ساختار پلتفرم نهادینه گردد (سان میگل و همکاران^{۱۳}، ۲۰۲۳؛ محمدی و صادق‌یان لمرسکی، ۱۴۰۳). ارتباط تئوریک این مباحث نشان می‌دهد که پیشگیری از جرائم سایبری، محصول مستقیم هم‌افزایی میان قابلیت‌های بازدارنده ساختاری و توانمندی‌های ادراکی کاربران است (میجویل و همکاران، ۲۰۲۳؛ یانکسون و همکاران^{۱۴}، ۲۰۲۴). در این پارادایم، شبکه‌های اجتماعی به عنوان اکوسیستم‌های بازدارنده‌ای عمل می‌کنند که از طریق تحلیل‌های بلادرنگ، نه تنها به بزه واکنش نشان می‌دهند، بلکه به طور فعالانه محیط را برای فعالیت‌های مجرمانه ناامن می‌سازند و نرخ بزه‌دیدگی را به حداقل می‌رسانند (اوبی و همکاران، ۲۰۲۴^{۱۵}؛ لوستوس و همکاران^{۱۶}، ۲۰۲۴؛ میجویل و همکاران، ۲۰۲۳).

1. Obi
2. Khadzhayradieva
3. Turner
4. Umeugo
5. Akrami
6. Yankson
7. San Miguel
8. Gupta
9. Islam,
10. Gupta
11. Ganguli
12. Drew,
13. San Miguel
14. Yankson,
15. Obi,
16. Lust,

پیشینه تجربی تحقیق

روند پژوهش‌های متأخر حکایت از چرخشی پارادایمیک از نگاه توصیفی به سمت رویکردهای تحلیلی و پیش‌بینی‌کننده در حوزه پژوهش دارد. در این راستا، گوپتا و همکاران^۱ (۲۰۲۵) با تمرکز بر تحلیل رفتار اجتماعی کاربران، مدل نوآورانه را بر پایه یادگیری عمیق توسعه دادند؛ یافته‌های این مطالعه تبیین می‌کند که اگرچه ساختار پلتفرم‌های برخط پتانسیل بزهکاری را افزایش داده است، اما هم‌زمان ظرفیت‌های بازدارندگی فنی نظیر یادگیری ماشین، امکان پیش‌بینی و خنثی‌سازی رفتارهای پرخطر را فراهم می‌آورد. این رویکرد فناورانه در پژوهش گانگولی^۲ (۲۰۲۴) با مفهوم گشت‌زنی رسانه‌های اجتماعی پیوند می‌خورد؛ مطالعه‌ای که نشان می‌دهد پتانسیل هوش مصنوعی در مبارزه با جرائم برخط تنها زمانی به فعلیت می‌رسد که یک همکاری راهبردی میان پلتفرم‌ها و نهادهای انتظامی جهت تبدیل چالش‌های صیانتی به فرصت‌های بازدارنده شکل بگیرد. علاوه بر ابعاد فنی، بازدارندگی در پیشینه تجربی عمیقاً با رفتارهای روزمره کاربران گره خورده است. سان میگل و همکاران^۳ (۲۰۲۰) با به‌کارگیری نظریه فعالیت‌های روزمره/ سبک زندگی، نقش تعدیل‌کننده اقدامات پیشگیرانه را در تجربه قربانی شدن بررسی کردند. نتایج آن‌ها حاکی از آن است که تقویت رفتارهای حفاظتی و دقت در تعاملات میان‌فردی، به‌عنوان یک سد دفاعی و عامل بازدارنده در برابر ریسک‌های ناشی از حضور فراگیر در فضای مجازی عمل می‌کند. این موضوع با یافته‌های اومئوگو^۴ (۲۰۲۳) در ارزیابی شاخص‌های آگاهی همسوست. این پژوهش تبیین می‌کند که بدون مداخلات آموزشی هدفمند، دانش امنیتی کاربران در سطح متوسط باقی مانده و ظرفیت‌های بازدارندگی فردی عملاً غیرفعال می‌شوند. هم‌گرایی مطالعات در تبیین استراتژی‌های پیشگیرانه، بر لزوم تقویت زیرساخت‌های اجتماعی و فرهنگی نیز تأکید دارد. محمدی و صادقان لمراسکی (۱۴۰۳) راهکارهای بازدارنده در برابر آزار و اذیت‌های برخط را در مثلی متشکل از آموزش، حمایت‌های اجتماعی و گزارش‌دهی نظام‌مند تعریف کرده‌اند. این نگاه جامعه‌شناختی در پژوهش محسنی (۱۴۰۲) عمق بیشتری یافته است؛ وی استدلال می‌کند که فرهنگ‌سازی و ارتقای تاب‌آوری کاربران، اثربخشی به‌مراتب بالاتری نسبت به اقدامات صرفاً واکنشی در پیشگیری از طعمه‌گذاری دارد. درنهایت، محمدی مقدم و همکاران (۱۴۰۱) با واکاوی پیشران‌های کلان بزهکاری، نشان دادند که بازدارندگی پایدار مستلزم شناخت دقیق عوامل زمینه‌ساز نظیر نقص سواد دیجیتال و نابرابری‌های ساختاری است؛ امری که نشان می‌دهد ظرفیت‌های بازدارندگی شبکه‌های اجتماعی باید در یک بافتار وسیع‌تر از تکنولوژی و با نگاهی به ویژگی‌های بنیادین جامعه تحلیل شود.

روش‌شناسی تحقیق

پژوهش حاضر، از طریق رویکرد روش‌شناسی آمیخته^۵ به مرحله اجرا درآمده است. در بخش کیفی، از پارادایم پژوهش تفسیری و استدلال استقرایی جهت واکاوی دیدگاه‌های خبرگان و شناسایی مضامین تحقیق بهره گرفته شده است. ماهیت این بخش از پژوهش، اکتشافی تفسیری است. فرایند تحلیل داده‌های کیفی بر مبنای استراتژی تحلیل

1. Gupta
2. Ganguli
3. San Miguel
4. Umeugo
5. mixed methods

مضمون براون و کلارک^۱ (۲۰۰۶) استوار است که طی آن، داده‌های حاصل از مصاحبه‌های نیمه‌ساختاریافته با پانزده تن از خبرگان دانشگاهی و اجرایی حوزه‌های مرتبط با پژوهش، گردآوری و پالایش شدند. در گام بعدی، با استفاده از نرم‌افزار MAXQDA، کدهای همگن در قالب مضمون پایه و اصلی دسته‌بندی شده و مدل مفهومی تدوین گردید. فرایند اجرای بخش کیفی براساس یک پروتکل نظام‌مند تنظیم شد. انتخاب مشارکت‌کنندگان با استفاده از روش نمونه‌گیری هدفمند صورت گرفت. معیارهای شمول در این پژوهش شامل داشتن حداقل پانزده سال سابقه فعالیت مرتبط، تجربه عملی یا علمی در حوزه پیشگیری از جرم بود. فرایند نمونه‌گیری تا دستیابی به اشباع نظری ادامه یافت. ابزار گردآوری داده‌ها، مصاحبه‌های نیمه‌ساختاریافته بود که به دو صورت حضوری و برخط در فضایی مبتنی بر تعامل سازنده اجرا شد. تحلیل داده‌ها در نرم‌افزار MAXQDA و بر اساس مراحل شش‌گانه براون و کلارک^۲ (۲۰۰۶) شامل آشنایی با داده‌ها، تولید کدهای اولیه، جست‌وجوی مضامین، بازبینی، تعریف و نام‌گذاری مضامین و درنهایت تدوین گزارش نهایی انجام پذیرفت. پس از آن مضامین شناسایی‌شده در قالب کدگذاری شبکه مضمون استرلینگ سازماندهی شدند. در بخش دوم، جهت اعتبارسنجی و آزمون تجربی روابط تبیین‌شده، پژوهش وارد مرحله کمی شد. در این بخش، با استناد به مضامین مستخرج از بخش کیفی، ابزار سنجش (پرسش‌نامه) تدوین شد و به‌منظور آزمون برازش مدل و تحلیل اثرات مستقیم و غیرمستقیم متغیرها، تکنیک مدل‌سازی معادلات ساختاری (SEM) به کار گرفته شد. این رویکرد ترکیبی، امکان آزمون دقیق مدل اکتشافی را در یک چارچوب آماری فراهم آورد و قدرت تعمیم‌پذیری یافته‌های پژوهش در جامعه آماری مورد نظر را تأیید کرد.

روایی و پایایی پژوهش (بخش کیفی)

جهت اطمینان از اعتبار و صحت یافته‌های مستخرج در حوزه ظرفیت‌های بازدارندگی، روایی پژوهش با استناد به چارچوب پیشنهادی کرسول^۳ (۲۰۰۷) در دو مرحله اساسی احراز شد. در مرحله نخست، از راهبرد تطبیق توسط مشارکت‌کنندگان استفاده شد که طی آن، کدهای استخراج‌شده و تفسیرهای اولیه جهت تأیید یا اصلاح در اختیار خبرگان مصاحبه‌شونده قرار گرفت. در مرحله دوم، فرایند بازبینی توسط همکاران اجرا شد؛ به گونه‌ای که کدهای استخراج‌شده توسط متخصصان مستقل (خارج از تیم تحقیق) ارزیابی شد. حصول توافق بیش از ۸۰ درصدی میان ارزیابان مستقل درخصوص مضامین احصاشده، مؤید روایی مطلوب و اعتبار بالای نتایج در تبیین مدل بازدارندگی است. همچنین، به‌منظور سنجش ثبات و تکرارپذیری یافته‌ها، از روش پایایی بازآزمون بهره گرفته شد. بر این اساس، دو مصاحبه به صورت تصادفی انتخاب و در دو بازه زمانی با فاصله بیست روز توسط پژوهشگر بازکدگذاری شدند. با توجه به شناسایی ۹۲ کد پایه در ساختار تحلیل، مقایسه میان نوبت‌های اول و دوم کدگذاری در جدول ۱ منعکس شده است.

1. Braun, V., & Clarke,

2. Braun, V., & Clarke,

3. Cresswell,

جدول ۱. نتایج محاسبه پایایی به روش بازآزمون

ردیف	تعداد کل کدها	تعداد توافقات	تعداد عدم توافق	درصد پایایی بازآزمون
۱	۹۲	۸۸	۴	۹۵/۶۵
۲	۹۲	۸۹	۳	۹۶/۷۴
میانگین	-	-	-	۹۶/۱۹

در جدول ۱ مشاهده می‌شود، میانگین پایایی بازآزمون برای مصاحبه‌های منتخب معادل ۹۶/۱۹ درصد محاسبه شده است. با استناد به فرمول محاسبه پایایی، این ضریب بیانگر ثبات بسیار بالای فرایند کدگذاری و قابلیت اتکای داده‌های پژوهش است. در مرحله کمی، با هدف اعتبارسنجی مدل استخراج‌شده و آزمون روابط مدل اکتشافی پژوهش، از تکنیک پیشرفته مدل‌سازی معادلات ساختاری بهره گرفته شد. این رویکرد تحلیل چندمتغیره، امکان بررسی هم‌زمان روابط میان متغیرهای مکنون و آشکار را فراهم آورده و از طریق شاخص‌های برازش، اعتبار مدل بازدارندگی شبکه‌های اجتماعی در پیشگیری از جرائم سایبری را در ابعاد آماری مورد تأیید قرار داد.

یافته‌های پژوهش

تحلیل ویژگی‌های جمعیت‌شناختی کنشگران

تحلیل نظام‌مند داده‌ها در رویکرد کیفی، مستلزم تبیین دقیق ویژگی‌های کنشگرانی است که به‌عنوان منابع اصلی استخراج مضامین در این پژوهش مشارکت داشته‌اند. در بخش کیفی، پانل خبرگان متشکل از پانزده متخصص بود که با استراتژی نمونه‌گیری هدفمند انتخاب شدند. انتخاب این ترکیب از خبرگان با هدف تضمین تنوع دیدگاه‌ها و دستیابی به تلاقی دانش نظری و تجربی صورت گرفت. جدول ۲ نشان‌دهنده وضعیت ویژگی‌های جمعیت‌شناختی مشارکت‌کنندگان است.

جدول ۲. ویژگی‌های جمعیت‌شناختی پانل خبرگان

شاخص متغیر	دسته‌بندی تخصصی	فراوانی	درصد (%)
مرتبه علمی / تحصیلی	دکتری تخصصی	۱۱	۷۳,۳
	کارشناسی ارشد (مدیران ارشد اجرایی)	۴	۲۶,۷
	حقوق جزا و جرم‌شناسی	۶	۴۰,۰
رشته تحصیلی	امنیت زیرساخت و فناوری اطلاعات	۵	۳۳,۳
	رسانه و فضای مجازی	۴	۲۶,۷
	۱۵ تا ۲۰ سال	۷	۴۶,۷
سابقه تجربه حرفه‌ای	بیش از ۲۰ سال	۸	۵۳,۳
	نهادهای دانشگاهی (هیئت علمی)	۸	۵۳,۳
	بخش‌های حاکمیتی و اجرایی	۷	۴۶,۷
پایگاه سازمانی			

توزیع داده‌های جدول شماره ۲ نشان می‌دهد که بیش از ۵۳ درصد از پانل خبرگان دارای سابقه تجربه حرفه‌ای بالای بیست سال هستند که این امر، عمق تجربی مورد نیاز برای واکاوی ظرفیت‌های بازدارندگی را تضمین می‌کند. حضور متوازن متخصصان بخش آکادمیک (۵۳,۳ درصد) در کنار نخبگان بخش اجرایی و حاکمیتی (۴۶,۷ درصد)، به ایجاد یک ارتباط دانش - تجربه منجر شده است که مانع از سوگیری‌های صرفاً نظری یا صرفاً فنی می‌شود.

تحلیل کیفی (شبکه مضامین)

در این بخش مطابق با رویه سیستماتیک تحلیل مضمون، به معرفی مضمون پایه پرداخته شده است. درواقع، مضمون پایه به عنوان شاخص‌های عملیاتی مستخرج از فرایند کدگذاری در بخش کیفی محسوب می‌شوند که زیربنای ساختاری متغیرهای اصلی پژوهش را تشکیل می‌دهند. جدول شماره ۳ نشان‌دهنده مضمون پایه و کدهای شناسایی شده در زمینه عوامل بازدارنده و پیشگیرانه از جرائم در بستر شبکه‌های اجتماعی است.

جدول ۳. شبکه مضامین

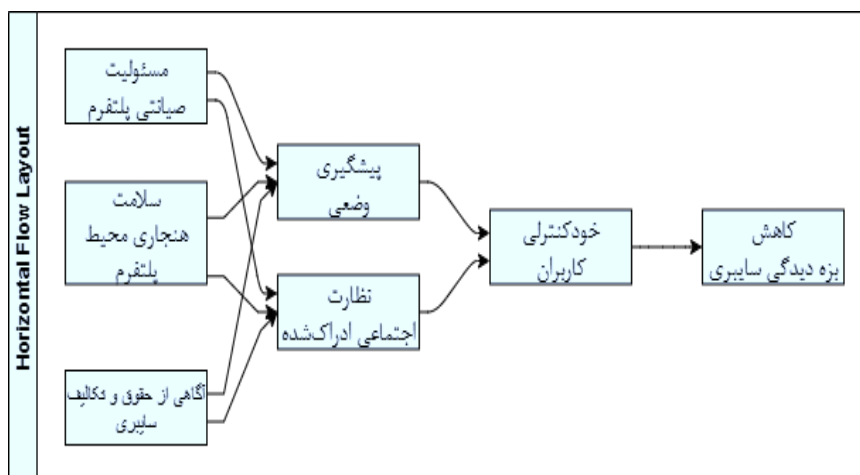
ردیف	مضمون پایه (شاخص‌های حقوقی)	مضمون سازمان‌دهنده	مضمون فراگیر
۱	پیاپی سازی پروتکل‌های احراز هویت قوی (طبق اسناد صیانت)	الزامات پیشگیری وضعی	مسئولیت صیانتی پلتفرم
۲	طراحی الگوریتم‌های کشف خودکار رفتارهای مجرمانه	فنی	
۳	ایجاد بن‌بست‌های فنی برای مسدودسازی مسیرهای نفوذ		
۴	استانداردسازی امنیت داده‌ها جهت جلوگیری از نشت اطلاعات		
۵	ذخیره سازی داده‌های ترافیکی جهت کشف بزه (داده‌های محتوا)	تکالیف قانونی همکاری	
۶	تسریع در اجرای دستورالعمل قضائی مسدودسازی و حذف	با مرجع قضائی	

		۷	شناسایی و معرفی کاربران متخلف به پلیس سایبری
		۸	ایجاد درگاه‌های اختصاصی گزارش‌دهی مستقیم به ضابطان
مسئولیت کیفری ناشی از		۹	جرم‌انگاری اهمال در حذف محتوای محرک جرم
ترک فعل		۱۰	مسئولیت واسطه‌ها در قبال معاونت در جرم (تسهیل جرم)
		۱۱	ضمانت‌اجراهای اداری و کیفری نقض حریم خصوصی کاربران
		۱۲	الزام به جبران بزه‌دیدگی ناشی از نقض امنیتی پلتفرم
مدیریت حقوقی محتوا		۱۳	حذف محتوای مروج خشونت، تروریسم و ناهنجاری‌های حاد
		۱۴	مقابله با تبلیغات جرائم سازمان‌یافته (قمار و مواد مخدر)
		۱۵	ممانعت از انتشار ابزارهای ارتکاب جرم (بدافزارها)
		۱۶	پالایش محتوای ناقض عفت و اخلاق عمومی در شبکه
دانش جرم‌شناختی	آگاهی از حقوق و تکالیف	۱۷	شناخت عناصر مادی جرائم سایبری جهت پرهیز از ارتکاب
کاربران	سایبری	۱۸	آگاهی از مجازات‌های بازدارنده در قانون جرائم رایانه‌ای
		۱۹	شناخت شگردهای نوین بزه‌کاران جهت پیشگیری از فریب
		۲۰	دانش نسبت به حقوق بزه‌دیده در فرایند دادرسی سایبری
سواد صیانت از ادله		۲۱	آموزش روش‌های مستندسازی حقوقی (حفظ زنجیره اعتباری)
دیجیتال		۲۲	آگاهی از نحوه طرح شکایت در دفاتر خدمات قضائی برخط
		۲۳	توانایی تشخیص پیوندهای فیشینگ و درگاه‌های نامعتبر
		۲۴	دانش کاربر در صیانت از کدهای دسترسی و رمزهای عبور
مسئولیت‌پذیری هنجاری		۲۵	پای‌بندی به کدهای اخلاقی و الزامات قانونی نشر محتوا
		۲۶	آگاهی از عواقب حقوقی نقض حریم خصوصی دیگران
		۲۷	شناخت حدود قانونی آزادی بیان و مصادیق مجرمانه آن
		۲۸	مسئولیت‌پذیری در قبال داده‌های به اشتراک گذاشته شده
کنشگری	حقوقی	۲۹	مشارکت در نظارت همگانی از طریق سوت‌زنی دیجیتال
(گزارش‌دهی)		۳۰	آگاهی از تکالیف قانونی در گزارش‌دهی جرائم مشهود
		۳۱	استفاده از ابزارهای گزارش‌دهی مردمی (پلیس فتا)
		۳۲	دانش نسبت به عواقب عدم گزارش جرائم سازمان‌یافته
حاکمیت قانون در فضای مجازی	سلامت هنجاری محیط پلتفرم	۳۳	ادراک حضور مقتدرانه نهادهای نظارتی در لایه‌های پلتفرم
		۳۴	مشروعیت‌بخشی به فعالیت‌های مجاز و قانونی کاربران
		۳۵	شفافیت در اعمال ضمانت‌اجراهای پلتفرمی علیه مجرمان
		۳۶	پایداری نظم حقوقی در برابر آشوب‌های سازمان‌یافته
صیانت از انسجام هنجاری جامعه		۳۷	مقابله با عرفی شدن رفتارهای مجرمانه در محیط شبکه
		۳۸	تقویت نمادهای اخلاقی و مذهبی در ساختار پلتفرم
		۳۹	کاهش جاذبه‌های بصری و محتوایی رفتارهای ناهنجار
		۴۰	ترویج الگوهای رفتاری منطبق بر سیاست جنایی کشور
صیانت از امنیت روانی جمعی		۴۱	پیشگیری از ارباب سایبری و تروریسم شخصیتی
		۴۲	مقابله با اخبار جعلی مخل امنیت و نظم عمومی
		۴۳	ایجاد فضای امن برای فعالیت‌های اقتصادی و اجتماعی
		۴۴	محافظت از کبان خانواده در برابر حمله‌های ضد اخلاقی
اعتباربخشی به هویت‌ها		۴۵	احراز صلاحیت منابع خبری و مرجعیت‌های فکری
		۴۶	محدودسازی هویت‌های جعلی و اکانت‌های یک‌بار مصرف
		۴۷	مقابله با جعل عنوان و غصب هویت اشخاص حقیقی/حقوقی

۴۸	شفاف‌سازی تبلیغات جهت جلوگیری از کلاهبرداری عمومی		
۴۹	اجبار به استفاده از توکن‌ها و سپرده‌های امنیتی محلی	دشواری‌سازی	عملیات پیشگیری وضعی
۵۰	مسدودسازی خودکار دسترسی‌های غیرمجاز و مشکوک	مجرمانه	
۵۱	رمزنگاری پیشرفته داده‌ها جهت غیرممکن‌سازی سرقت		
۵۲	محدودسازی قابلیت‌های فنی برای کاربران غیراحراز شده		
۵۳	ثبت ردپای دیجیتال (IP) جهت رهگیری کیفری سریع	افزایش ریسک و خطر	
۵۴	مانیتورینگ آنی فعالیت‌های دارای الگوی مجرمانه	شناسایی	
۵۵	بهره‌گیری از هوش مصنوعی برای پیش‌بینی کانون‌های جرم		
۵۶	تقویت سیستم‌های هشدار به بزه‌دیدگان در آستانه جرم		
۵۷	غیرفعال‌سازی سریع درگاه‌های مالی نامعتبر	حذف منافع و جاذبه‌های	
۵۸	حذف ارزش داده‌های مسروقه از طریق بی‌اعتبارسازی آنی	جرم	
۵۹	مسدودسازی سود حاصل از کلاهبرداری در حساب‌های واسط		
۶۰	کاهش نمایش عمومی اطلاعات حساس و آسیب‌پذیر		
۶۱	نمایش خودکار هشدارهای قانونی قبل از ورود به حوزه‌ها	حذف معاذیر و توجیهات	
۶۲	اطلاع‌رسانی مستمر ضوابط جدید کیفری به کاربران	جرم	
۶۳	نصب بنرهای دیجیتال بازدارنده در محیط‌های پرخطر		
۶۴	الزام کاربر به تأیید آگاهی از عواقب حقوقی فعالیت خود		
۶۵	حساسیت جامعه مجازی نسبت به نقض قوانین و اخلاق	نظارت عمومی و مدنی	نظارت اجتماعی ادراک‌شده
۶۶	فشار افکار عمومی در جهت تقبیح رفتارهای مجرمانه		
۶۷	طرد مجازی و بایکوت کاربران مروج فساد و جرم		
۶۸	نقش ادمین‌ها به‌عنوان ناظر محلی در گروه‌های بزرگ		
۶۹	باور عمومی به تخصص پلیس سایبری در کشف جرائم	ادراک نظارت حاکمیتی	
۷۰	مشاهده سرعت عمل دستگاه قضا در برخورد با بزه‌کاران		
۷۱	انتشار اخبار محاکمه مجرمان سایبری جهت ارعاب عمومی		
۷۲	پایش مستمر فضاهای عمومی شبکه توسط گشت‌های سایبری		
۷۳	استفاده از ابزارهای نظارت والدین	نظارت خانوادگی و	
۷۴	نقش نهادهای آموزشی در رصد رفتارهای پرخطر نوجوانان	تربیتی	
۷۵	پیشگیری از بزه‌دیدگی از طریق کنترل‌های غیررسمی		
۷۶	تقویت پیوندهای اخلاقی در گروه‌های کوچک مجازی		
۷۷	اطلاع‌رسانی از حجم پرونده‌های کشف‌شده در پلتفرم	شفافیت	سازوکارهای
۷۸	اعلام عمومی لیست‌های سیاه (اکانت‌های کلاهبردار)	کنترلی	
۷۹	تبیین شیوه‌های نظارتی جهت افزایش اعتماد و بازدارندگی		
۸۰	نمایش اقتدار فنی سیستم در مقابله با نفوذگران		
۸۱	پرهیز داوطلبانه از کنجکاوی در محیط‌های آلوده و جرم‌زا	مدیریت رفتارهای پرخطر	خودکنترلی کاربران
۸۲	کنترل تکانه‌ها در پاسخ به پیام‌های تحریک‌آمیز		
۸۳	اجتناب از تعامل با حساب‌های مروج فعالیت‌های غیرقانونی		
۸۴	رعایت احتیاط در پذیرش درخواست‌های مشکوک		
۸۵	مدیریت سطح دسترسی دیگران به داده‌های شخصی	صیانت از	حریم
۸۶	خودداری از انتشار اطلاعاتی که مبنای مهندسی اجتماعی است	خصوصی فردی	
۸۷	حفاظت از تصاویر خصوصی جهت پیشگیری از اخاذی جنسی		

	تفکیک هویت واقعی از هویت مجازی در موارد حساس	۸۸
هوشیاری در معاملات	راستی‌آزمایی هویت طرف مقابل قبل از هرگونه تراکنش	۸۹
برخط	عدم اعتماد به وعده‌های واهی (سودهای کلان دیجیتال)	۹۰
	استفاده از بسترهای امن پرداخت و پرهیز از روابط مستقیم	۹۱
	تحلیل ریسک حقوقی قبل از انجام هرگونه فعالیت مالی	۹۲
وجدان حقوقی و اخلاقی	باور درونی به لزوم رعایت حقوق شهروندی دیگران	۹۳
	پای‌بندی داوطلبانه به قانون در غیاب ناظران خارجی	۹۴
	اولویت‌بخشی به امنیت پایدار بر منافع زودگذر مجازی	۹۵
	مسئولیت‌پذیری در قبال عواقب رفتارهای خودسرانه	۹۶
کاهش جرائم علیه اموال	تنزل نرخ بزه‌دیدگی در فیشینگ و سرقت‌های دیجیتالی	۹۷
و داده	کاهش کلاهبرداری‌های مرتبط با رمزارز و پانزی	۹۸
	افت آمار باج‌خواهی‌های سایبری و سرقت داده‌های تجاری	۹۹
	پیشگیری از نفوذ و تخریب سامانه‌های شخصی کاربران	۱۰۰
کاهش جرائم علیه اشخاص و حیثیت	تقلیل بزه‌دیدگی در حوزه هتک حیثیت و نشر اکاذیب	۱۰۱
	کاهش آمار مزاحمت‌های نوظهور و قلدری سایبری	۱۰۲
	افت موارد نقض حریم خصوصی و افشای اسرار زندگی	۱۰۳
	پیشگیری از تهدید و اخاذی‌های مبتنی بر داده‌های شخصی	۱۰۴
کاهش جرائم علیه عفت و اخلاق	کاهش اغفال سایبری	۱۰۵
	پیشگیری از دسترسی به محتویات فریب‌دهنده سایبری	۱۰۶
	تقلیل بزه‌دیدگی ناشی از دوستی‌های اینترنتی مجرمانه	۱۰۷
	پاکسازی محیط پلتفرم از نمادهای مروج فساد عمومی	۱۰۸
ارتقای امنیت و نظم عمومی	افزایش ضریب اعتماد کاربران به زیست‌بوم دیجیتال	۱۰۹
	کاهش حجم پرونده‌های قضائی و بار کاری پلیس فتا	۱۱۰
	پایداری امنیت ملی در حوزه تبادل اطلاعات	۱۱۱
	کاهش هزینه‌های اجتماعی و اقتصادی ناشی از بزهکاری	۱۱۲

براساس فرایند کدگذاری سیستماتیک و با تکیه بر استراتژی شبکه مضامین، یافته‌های بخش کیفی پژوهش در قالب یک ساختار سلسله‌مراتبی منسجم تدوین شد. خروجی این تحلیل، به احصای ۹۲ مضمون پایه (شاخص‌های عملیاتی) منجر شد که در بطن ۲۴ مضمون سازمان‌دهنده انتظام یافتند و درنهایت، چارچوب نظری پژوهش را در قالب شش مضمون فراگیر تبیین می‌کنند. این شبکه مضامین، مبین یک الگوی پیشگیری چندسطحی است که بر مبنای انتظام منطقی این مضامین و روابط تبیین‌شده میان آن‌ها، مدل مفهومی تحقیق استخراج و در شکل ۱ ترسیم شده است.

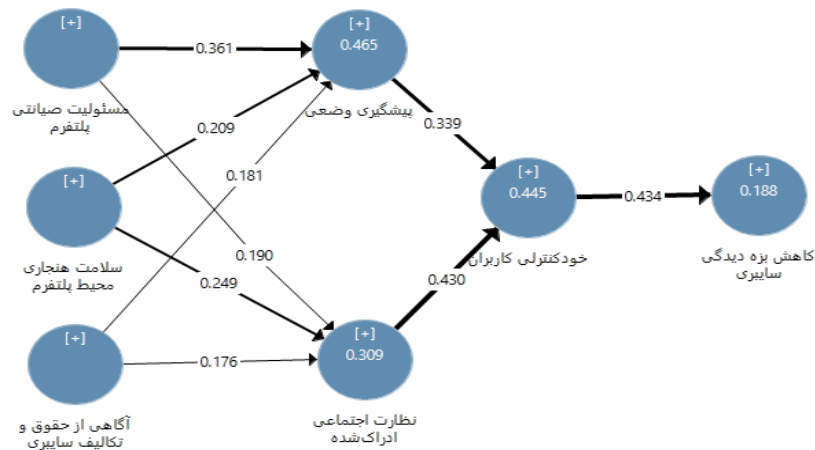


شکل ۱. مدل اکتشاف شده تحقیق

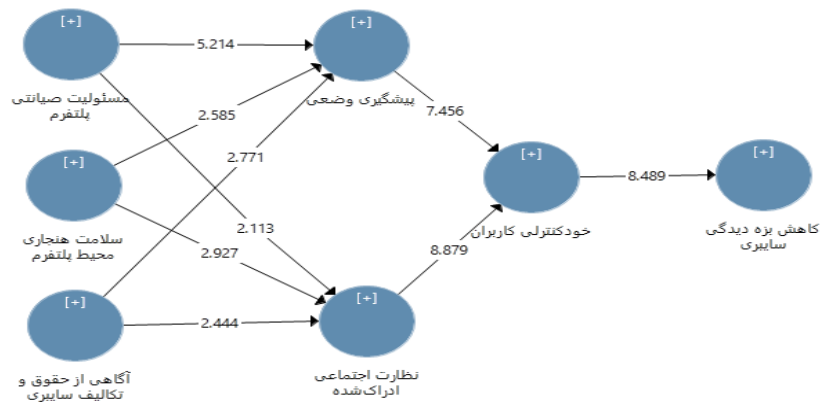
تحلیل کمی (اعتباریابی)

در این مرحله، با توجه به جدید بودن مدل استخراج شده از بخش کیفی، جهت آزمون تجربی و برازش، از رویکرد مدل سازی معادلات ساختاری (SEM) با استاندارد به دیدگاه هیر^۱ و همکاران (۲۰۱۴) استفاده شد. فرایند تحلیل در این بخش، در دو سطح «مدل اندازه گیری» و «مدل ساختاری» تبیین شده است. در گام نخست صحت انتساب شاخص ها به مؤلفه ها از طریق تحلیل عاملی تأییدی (CFA) و بررسی روایی و پایایی مدل اکتشافی احراز شد. در گام دوم، جهت واکاوی روابط علی میان متغیرهای مکنون، تکنیک تحلیل مسیر به کار گرفته شد. این تکنیک امکان شناسایی همزمان تأثیرات مستقیم و غیرمستقیم متغیرهای مدل مفهومی را فراهم آورده و میزان پیش بینی پذیری سازه های درون را از طریق متغیرهای برون زان نمایان می سازد. در ادامه، نتایج خروجی مدل اعتباریابی شده در دو حالت ضرایب استاندارد (شکل ۲) و معناداری (شکل ۳) ارائه شده است.

1.Hair



شکل ۲. مدل تحلیل مسیر در حالت ضرایب استاندارد



شکل ۳. مدل تحلیل مسیر در حالت معناداری

نتایج آزمون فرضیه‌های پژوهش در دو مدل ضرایب معناداری و مدل ضرایب استاندارد براساس خروجی نرم‌افزار Smart PLS ارائه شده است. مطابق با مدل معناداری (شکل ۳) مشاهده می‌شود که ضرایب معناداری تمامی روابط مدل خارج از بازه $-1/96$ و $1/96$ است. این بدین معناست که در سطح معنادار $0/05$ می‌توان با $0/99$ درصد احتمال روابط اکتشاف‌شده را تأیید کرد. در ادامه مطابق با الگوریتم مدل‌سازی معادلات ساختاری واریانس‌محور، ابتدا به تحلیل

یک‌جنس بودن سنجه‌های سازه براساس تحلیل عاملی تأییدی پرداختیم و سپس به بررسی مدل اندازه‌گیری تحقیق اقدام کردیم. بدین منظور اقدام به گزارش پایایی و روایی سازه مدل تحقیق کردیم.

جدول ۴. مدل اندازه‌گیری تحقیق

متغیرهای فراگیر	شاخص‌های اختصاری	بارهای عاملی	آلفای کرونباخ	پایایی (CR)	ترکیبی	میانگین واریانس (AVE)	استخراجی
مسئولیت صیانتی پلتفرم	RP1	۰/۸۲۱	۰/۸۵۸	۰/۹۰۱		۰/۶۹۴	
	RP2	۰/۸۴۰					
	RP3	۰/۷۹۵					
	RP4	۰/۸۱۴					
آگاهی حقوقی کاربران	LC1	۰/۸۱۰	۰/۸۴۶	۰/۸۹۳		۰/۶۷۸	
	LC2	۰/۸۵۶					
	LC3	۰/۷۸۸					
	LC4	۰/۸۲۲					
سلامت هنجاری محیط	SE1	۰/۸۴۲	۰/۸۶۲	۰/۹۰۴		۰/۷۰۲	
	SE2	۰/۸۰۵					
	SE3	۰/۸۱۸					
	SE4	۰/۸۳۷					
پیشگیری وضعی	SP1	۰/۸۸۱	۸۷۹/۰	۰/۹۱۴		۰/۷۲۸	
	SP2	۰/۸۴۷					
	SP3	۰/۸۵۵					
	SP4	۰/۸۱۲					
نظارت اجتماعی ادراک شده	SN1	۰/۷۹۸	۰/۸۳۴	۰/۸۸۷		۰/۶۶۳	
	SN2	۰/۸۳۴					
	SN3	۰/۸۱۰					
	SN4	۷۸۵/۰					
خودکنترلی کاربران	SC1	۸۶۵/۰	۰/۸۹۱	۹۳۴/۰		۰/۷۵۲	
	SC2	۰/۸۹۰					
	SC3	۰/۸۴۲					
	SC4	۰/۸۱۸					
کاهش بزه‌دیدگی سایبری	CV1	۰/۸۳۰	۸۸۴/۰	۰/۹۱۸		۰/۷۳۷	
	CV2	۰/۸۵۵					
	CV3	۰/۸۷۲					
	CV4	۰/۸۴۴					

براساس خروجی شکل ۳، تحلیل مسیر در حالت ضرایب استاندارد و جدول ۴ مدل اندازه‌گیری تحقیق ملاحظه می‌شود تمامی متغیرهای مکنون پژوهش بارهای عاملی با ضریبی بیش از ۰/۷ دارند. ضریب آلفای کرونباخ و پایایی

ترکیبی متغیرهای تحقیق ضریبی بیش از ۰/۷ را نشان می‌دهد و همچنین ضریب پایایی اشتراکی نیز بیش از ۰/۵ دارد. بنابراین می‌توان استدلال کرد مدل اندازه‌گیری تحقیق از پایایی بالایی برخوردار است (هیر و همکاران، ۲۰۱۲). همچنین مطابق با نظر هیر و همکاران (۲۰۱۴)، شاخص $AVE \geq 0/5$ و $CR \geq 0/7$ است. همچنین $CR > AVE$ هست. بنابراین روایی همگرا مدل تأیید می‌شود. در گام بعد برای دفع سوگیری و هم‌بستگی بین شاخص‌های تحقیق (روایی واگرا)، مبادرت به آزمون فورنل ولارکر جدول ۶ به‌عنوان مهم‌ترین آزمون‌های روایی واگرا شده است.

جدول ۵. فورنل - لارکر

Fornell-Larcker Criterion							
کاهش بزه‌دیدگی سایبری	پیشگیری وضع	نظارت اجتماعی ادراک‌شده	مسئولیت صیانتی پلتفرم	سلامت هنجاری محیط پلتفرم	خودکنترلی کاربران	آگاهی حقوق تکالیف سایبری	مضامین پژوهش از و
						0.748	آگاهی از حقوق و تکالیف سایبری
					0/853	0.594	خودکنترلی کاربران
				0.753	0.626	0.700	سلامت هنجاری محیط پلتفرم
			0.785	0.739	0.694	0.716	مسئولیت صیانتی پلتفرم
		0/862	0.500	0.513	0.599	0.487	نظارت اجتماعی ادراک‌شده
	0/831	0/712	0.645	0.602	0.553	0.586	پیشگیری وضعی
0/861	0.443	0/732	0.477	0.492	0.434	0.492	کاهش بزه‌دیدگی سایبری

مطابق با دیدگاه هنسلر^۱ و همکاران (۲۰۱۴)، میانگین واریانس استخراجی است که هر متغیر باید بالاتر از هم‌بستگی مربع با هر متغیر دیگر باشد. خروجی نرم‌افزار در جدول ۴ نشان از تأیید روایی واگرا از دیدگاه این آزمون دارد. بنابراین مطابق با معادلات هنسلر^۲ (۲۰۱۲)، هیچ نقاط بحرانی مشاهده نمی‌شود و می‌توان روایی واگرا از دیدگاه این آزمون را تأیید کرد. در ادامه به بررسی میزان R^2 مسئله پرداخته شده است. این شاخص از صفر تا ۱ متغیر است و دقت پیش‌بینی مسئله تحقیق را نشان می‌دهد و بیانگر تأثیر یک متغیر برون‌زا بر یک متغیر درون‌زا است.

جدول ۶. ضریب تعیین مدل

ضریب معنی‌داری	میانگین	مضامین درون‌زا مدل
0/000	0.442	خودکنترلی کاربران
0/000	0.303	نظارت اجتماعی ادراک‌شده
0/000	0.460	پیشگیری وضعی
0/000	0.186	کاهش بزه‌دیدگی سایبری

1. Henseler

2. Hensler,

ضریب R Square به عنوان میزان تغییری که یک متغیر درون‌زا از متغیرهای برون‌زا می‌گیرد نشان می‌دهد ضریب تمام متغیرهای درون‌زای مدل اکتشافی معنی‌دار است.

بحث و نتیجه‌گیری

هدف پژوهش حاضر، واکاوی و ارائه مدل جامع ظرفیت‌های بازدارندگی شبکه‌های اجتماعی در راستای پیشگیری از جرائم سایبری بود. خروجی یافته‌های حاصل از بخش کیفی احصای ۹۲ مضمون پایه (شاخص‌های عملیاتی) در بطن ۲۴ مضمون سازمان‌دهنده انتظام یافت، در قالب شش مضمون فراگیر شد و اعتبارسنجی آن در بخش کمی، مبین شکل‌گیری یک پارادایم نوین در سیاست جنایی پیشگیرانه است. مدل تحقیق تصریح می‌کند که بازدارندگی در حوزه دیجیتال، دیگر صرفاً تابعی خطی از ابعاد کیفی و شدت مجازات (رویکرد کلاسیک) محسوب نمی‌شود، بلکه محصولی چندوجهی و غیرخطی ناشی از هم‌افزایی میان مسئولیت صیانتی پلتفرم، نظارت اجتماعی ادراک‌شده و خودکنترلی کاربران است. تأیید تمامی روابط ساختاری مدل با مقادیر بحرانی (t-value) فراتر از ۱/۹۶ نشان‌دهنده یک ساختار سیستمی مدل است. یکی از یافته‌های کلیدی این مطالعه، نقش پیشبران مسئولیت صیانتی پلتفرم در تحقق پیشگیری وضعی است که با ضریب معناداری ۵/۲۱۴ در مدل ساختاری به تأیید رسید. این یافته با رویکرد گانگولی^۱ (۲۰۲۴) پیرامون مفهوم گشت‌زنی رسانه‌های اجتماعی قرابت تئوریک دارد؛ با این تفاوت که پژوهش حاضر، نشان داد که الزامات فنی نظیر الگوریتم‌های کشف خودکار رفتارهای مجرمانه و تعبیه بن‌بست‌های فنی، مستقیماً ضلع فرصت را در مثلث جرم سلب می‌کنند. این نتیجه با یافته‌های گوپتا و همکاران^۲ (۲۰۲۵) درخصوص مدل هوشمند همسوست، چراکه هر دو مطالعه بر این باورند که گذار به بازدارندگی فنی و یادگیری ماشین، امکان خنثی‌سازی کنش‌های مجرمانه را در مرحله پیش‌جنایی فراهم می‌آورد. علاوه بر لایه ساختاری، نتایج آزمون مدل نشان داد که خودکنترلی کاربران به عنوان یک متغیر میانجی راهبردی عمل می‌کند که با بالاترین ضریب معناداری در کل مدل ۸/۴۹۸، به کاهش عینی بزه‌دیدگی سایبری منتج می‌شود. این یافته، مبانی نظریه فعالیت‌های روزمره در پژوهش سان میگل و همکاران^۳ (۲۰۲۰) را بسط می‌دهد. در حالی که سان میگل بر نقش دفاعی فردی تأکید داشت، مطالعه حاضر با عملیاتی‌سازی مضامین اکتشاف‌شده، این تئوری را برای فضای مجازی بومی‌سازی کرده است. در همین پیوند، رابطه مستقیم میان آگاهی حقوقی و خودکنترلی تبیین می‌کند که بدون سواد صیانت از ادله دیجیتال، ظرفیت‌های بازدارندگی فردی عملاً غیرفعال باقی می‌مانند. این امر مؤید هشدار اومئوگو^۴ (۲۰۲۳) است؛ با این تبیین که یافته‌های این پژوهش نشان داد آگاهی حقوقی، کاربر را از یک سوژه آسیب‌پذیر به کنشگری بازدارنده تبدیل می‌کند. از سویی پژوهش حاضر با ارائه یک مدل هفت‌بعدی، غنای نظری ادبیات جرم‌شناسی سایبری را در چندین محور کلیدی توسعه داده است. نخست، تبیین نقش واسطه‌ای خودکنترلی کاربران است که نشان

1. Ganguli
2. Gupta
3. San Miguel,
4. Umeugo

داد حتی پیشرفته‌ترین پروتکل‌های فنی مانند یادگیری عمیق مطرح‌شده در پژوهش (گوپتا و همکاران^۱، ۲۰۲۵) بدون آمادگی رفتاری و وجدان حقوقی کنشگران، به بازدارندگی حداکثری منجر نخواهند شد.

فراروی پیشنهادات تحقیق بر اساس یافته‌های مستخرج از مدل تحقیق، پیشنهادهای سیاستی و تجربی این پژوهش بر سه محور توسعه معماری امن، قانون‌گذاری پاسخ‌گو و کنشگری هوشمند متمرکز است. از منظر سیاستی، ضروری است نهادهای حاکمیتی با عبور از رویکردهای سنتی مجازات‌محور، پلتفرم‌های اجتماعی را به تصویب و اجرای پروتکل‌های امنیت در طراحی ملزم سازند؛ به‌گونه‌ای که مسئولیت کیفری با میزان کارآمدی الگوریتم‌های پیشگیرانه و سرعت عمل در حذف منافع جرم پیوند بخورد. در سطح تجربی و عملیاتی، ارتقای سواد حقوقی کاربران فراتر از آموزش‌های عمومی، باید به سمت مهارت‌های تخصصی صیانت از ادله دیجیتال و مدیریت خودکنترلی در موقعیت‌های جرم‌زا سوق یابد. همچنین، پیشنهاد می‌شود با طراحی درگاه‌های سوت‌زنی دیجیتال و ایجاد شفافیت در انتشار گزارش‌های برخورد با بزهکاران، حس اقتدار حاکمیت قانون و نظارت اجتماعی ادراک‌شده در زیست‌بوم دیجیتال تقویت شود تا از این طریق، با کاهش جاذبه‌های محیطی و افزایش ریسک شناسایی، هزینه‌های ارتکاب جرم برای بزهکاران بالقوه به حداکثر برسد و امنیت پایدار در فضای مجازی نهادینه شود. این پژوهش علی‌رغم دستاوردهای نظری و تجربی در تبیین مدل بازدارندگی، با محدودیت‌هایی مواجه بوده است که توجه به آن‌ها در تعمیم یافته‌ها ضرورت دارد. ازجمله مهم‌ترین این محدودیت‌ها، ملاحظات امنیتی و دشواری در دسترسی مستقیم به داده‌های زیستی بزهکاران سایبری، موجب شد تا تحلیل‌ها عمدتاً بر دیدگاه‌های نخبگانی و ادراکات کاربران متمرکز بماند. بر این اساس و جهت توسعه دانش در این حوزه، به پژوهشگران آتی پیشنهاد می‌شود با تمرکز بر ظرفیت‌های تکنولوژی‌های نوظهور نظیر زنجیره بلوکی و هوش مصنوعی، تأثیر این ابزارها را بر تغییر الگوهای بازدارندگی و بازتعریف مسئولیت کیفری پلتفرم‌ها واکاوی کنند. علاوه بر این، انجام مطالعات میان‌فرهنگی برای سنجش میزان اثربخشی نظارت اجتماعی ادراک‌شده در محیط‌های مجازی متفاوت و بررسی نقش متغیرهای تعدیل‌گر نظیر تفاوت‌های جنسیتی و سنی در میزان خودکنترلی کاربران، می‌تواند افق‌های جدیدی را در بومی‌سازی الگوهای پیشگیرانه و ارتقای امنیت در زیست‌بوم دیجیتال بگشاید.

منابع

حسینی جیردهی، حسین؛ باوندپوری، محمد و محمودی رجا، سید زکریا (۱۴۰۲). واکاوی نقش شبکه‌های اجتماعی در شکل‌گیری آشوب‌های اجتماعی آبان ۱۳۹۸ در ایران. *فصلنامه آفاق/امنیت*، ۱۶ (۵۸)، ۴۹-۱۱.

محسنی، فرید (۱۴۰۲). واکاوی عوامل مؤثر و راهکارهای پیشگیری از طعمه‌گذاری در فضای مجازی، فصلنامه پژوهش‌های اطلاعاتی و جنایی، ۲ (۷۰)، ۶۱-۹۲.

محمدی مقدم، یوسف؛ ساعدی، عبدالله و محسنی، فرید (۱۴۰۱). واکاوی عوامل مؤثر وقوع جرم در فضای مجازی.

محمدی، سحر و صادقیان لمراسکی، محدثه (۱۴۰۳). واکاوی تعاملات بین شبکه‌های اجتماعی و خودکشی‌های مرتبط با تعرضات آنلاین. *پژوهش‌های جرم‌شناسی کاربردی*، ۲ (۳)، ۹۵-۱۲۴. doi: 10.22034/aqcr.2024.2038840.1018.

References

- Hosseini Jiredehi, H., Bavandpuri, M., & Mahmoudi Raja, S. Z. (2023). Analyzing the role of social networks in the formation of social unrest in November 2018 in Iran. *Security Horizons*, 16(58), 11-49. In Persian
- Mohseni, Farid (2013). Analysis of effective factors and strategies for preventing baiting in cyberspace, *Quarterly Journal of Intelligence and Criminal Research*, 2 (70) 61-92. In Persian . <https://doi.org/101303>
- Mohammadi Moghadam Yousef, Saedi Abdollah, & Mohseni Farid. (۲۰۲۲). Analysis of the effective factors of crime occurrence in cyberspace. *In Persian* <https://doi.org/10.22034/pok.2022.97764>
- Mohammadi Sahar, & Sadeghian Lamaraski Mohaddeseh. (۲۰۲۴). Analyzing the interactions between social networks and suicides related to online harassment. *In Persian* <https://doi.org/10.22034/aqcr.2024.2038840.1018>
- Hensler, S., Heinemann, D., Becker, M. T., Ackermann, H., Wiesemann, A., Abholz, H. H., & Engeser, P. (2009). Chronic pain in German general practice. *Pain Medicine*, 10(8), 1408-1415. <https://doi.org/10.1111/j.1526-4637.2009.00735.x>
- Hensler, J. G. (2012). Serotonin. In *Basic neurochemistry* (pp. 300-322). Academic Press. <https://doi.org/10.1016/b978-0-12-374947-5.00015-8>
- Hair Jr, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM). *European business review*, 26(2), 106. <https://doi.org/10.1108/ebv-10-2013-0128>
- Cresswell, S. L., & Eklund, R. C. (2007). Athlete burnout: A longitudinal qualitative study. *The sport psychologist*, 21(1), 1-20. <https://doi.org/10.1123/tsp.21.1.1>
- Lust, C., Vesoulis, Z., Zempel, J., Gu, H., Lee, S., Rao, R., & Mathur, A. M. (2024). An amplitude-integrated EEG evaluation of neonatal opioid withdrawal syndrome. *American journal of perinatology*, 41(S 01), e290-e297. <https://doi.org/10.1055/a-1877-9291>
- Akrami, K., Akrami, M., Hakimi, M., Fazil, A. W., Ahrari, M., & Akrami, F. (2024). Investigating the adverse effects of social media and cybercrime in higher education: A case study of an online university. *Studies in Media, Journalism and Communications*, 2(1), 22-33. <https://doi.org/10.32996/smjc.2024.2.1.3>
- Back, S., & Guerette, R. T. (2021). Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. *Journal of Contemporary Criminal Justice*, 37(3), 427-451. <https://doi.org/10.1177/10439862211001628>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77-101. <https://doi.org/10.1191/1478088706qp0630a>

- Drew, J. M. (2020). A study of cybercrime victimisation and prevention: Exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, 6(1), 17–33. <https://doi.org/10.1108/JCRPP-12-2019-0070>
- Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research*, 19(6), 537–549. <https://doi.org/10.1080/15614263.2018.1507890>
- Ganguli, P. (2024). *The role of social media patrolling in preventing low-level cybercrime: Opportunities and challenges*. SSRN. <https://doi.org/10.2139/ssrn.5014735>
- Gupta, A., Matta, P., & Pant, B. (2025). Analyzing the social conduct of users to detect and prevent cybercrime across social networks. *Procedia Computer Science*, 258, 4269–4278. <https://doi.org/10.1016/j.procs.2025.04.676>
- Hair Jr, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM). *European business review*, 26(2), 106. <https://doi.org/10.1108/eb-10-2013-0128>
- Ho, H., Ko, R., & Mazerolle, L. (2022). Situational crime prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security*, 115, Article 102611. <https://doi.org/10.1016/j.cose.2022.102611>
- Iqbal, F., Fung, B. C. M., Batool, R., Debbabi, M., & Marrington, A. (2019). WordNet-based criminal networks mining for cybercrime investigation. *IEEE Access*, 7, 22740–22755. <https://doi.org/10.1109/ACCESS.2019.2891694>
- Islam, M. M., Acharjee, U. K., Akter, A., Islam, L., Uddin, M. A., & Sharmin, S. (2020). Cyberbullying detection on social networks using machine learning approaches. In *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)* (pp. 1–6). IEEE. <https://doi.org/10.1109/CSDE50874.2020.9411601>
- Khadzhyradieva, S., Todorova, M., Staikutsa, S., Tsybukh, L., & Lukiianchuk, A. N. (2024). Analysis of cyber-psychological protection programs in the education system: Role, limitations and prospects. *Salud, Ciencia y Tecnología-Serie de Conferencias*, 3, 1.
- Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African journal of business management*, 5(26), 10862. <https://doi.org/10.5897/AJBM11.067>
- Macpherson, L. M. D. (2018). Raising awareness of oral cancer from a public and health professional perspective. *British Dental Journal*, 225(9), 809–814. <https://doi.org/10.1038/sj.bdj.2018.919>
- Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime victimization and problematic social media use: Findings from a nationally representative panel study. *American Journal of Criminal Justice*, 46(6), 862–881. <https://doi.org/10.1007/s12103-021-09665-2>
- Obi, O., Akagha, O., Dawodu, S., Anyanwu, A., Onyekwe, I., & Onwusinkwue, S. (2024). Comprehensive review on cybersecurity: Modern threats and advanced defense strategies. *Computer Science & IT Research Journal*, 5(2), 293–310. <https://doi.org/10.51594/csitrj.v5i2.758>
- San Miguel, C., Morales, K., & Ynalvez, M. A. (2020). Online victimization, social media utilization, and cyber crime prevention measures. *Asia-pacific social science review*, 20(4), 11. <https://doi.org/10.59588/2350-8329.1339>
- Taherdoost, H. (2024). Insights into cybercrime detection and response: A review of time factor. *Information*, 15(5), 273. <https://doi.org/10.3390/info15050273>
- Turner, B. (2023). Social capital, inequality and health: The Durkheimian revival. *Social Theory & Health*, 1(1), 4–20. <https://doi.org/10.1057/palgrave.sth.8700001>

- Turner, J. H., & Abrutyn, S. (2016). Returning the “social” to evolutionary sociology: Reconsidering Spencer, Durkheim, and Marx’s models of “natural” selection. *Sociological Perspectives*, 60(3), 529–556. <https://doi.org/10.1177/0731121416641936>
- Umeugo, W. (2023). Cybercrime awareness on social media: A comparison study. *International Journal of Network Security & Its Applications*, 15(2), 23–35. <https://doi.org/10.5121/ijnsa.2023.15202>
- Yankson, B., Hussein, M., Dadson, Y., & Berkoh, E. (2024). The role of industry-academia partnerships can play in cybersecurity. In *Proceedings of the International Conference on Cyber Warfare and Security*, 19(1), 26–33. <https://doi.org/10.34190/iccws.19.1.2169>