Journal of Research Police Science
Volume 24, NO. 4, Winter 2023

Analyzing the Effective Factors of Crime in Cyber Space

Yousef Mohammadi Moghadam[1] - Abdullah Saedi[2] - Farid Mohseni[3]

Received: 21, May, 2022 Accepted: 06, December, 2022

Abstract

Background and objective: Crimes in cyberspace include any action or action that is done through cyberspace and using tools to connect to this space and violates the rights specified for people. The present study was conducted with the aim of analyzing and investigating the effective factors (drivers) of crime in cyberspace using a mixed-method approach.

Methods: This research is considered a mixed-method study with a qualitative and quantitative approach, which is descriptive and survey in terms of its nature and method, and in terms of its objectives it is of an applied research type.

Findings: Based on the judgment and survey of experts, sixteen factors have been introduced as the effective factors of crime in cyberspace. Also, the findings show that the weakness of digital literacy of users, emotional, financial and informational needs of people, cultural weakness, lack of appropriate and deterrent laws and regulations, inefficiency of safety systems, inflation and economic defects, increase in unemployment and low risk of arrest are the most important effective factors in the occurrence of criminal behavior in cyber space.

Results: Crime in cyberspace is one of the most important problems that has severely threatened human societies in recent decades. Knowing the underlying factors in the occurrence of such crimes can significantly prevent the commission of these crimes in the society.

Keywords: Cyber space, Cybercrimes, Crime, Effective factors of crime.

---

1 Professor in Management Department, Amin Police University, Tehran, Iran

2 PhD in Human Resource Management, Lorestan University, Khorramabad, Iran

3 Associate Professor, Department of Law, University of Judicial Sciences and Administrative Services of Justice, Tehran, Iran

مقاله پژوهشی

https://doi.org/10.22034/pok.2022.97764

فصلنامه پژوهش‌های دانش انتظامی، سال بیست و چهارم، شماره ۴، زمستان ۱۴۰۱

صص ۱۰۹-۷۷

واکاوی عوامل مؤثر وقوع جرم در فضای مجازی[۱]

یوسف محمدی مقدم[۲]، عبداله ساعدی[۳]، فرید محسنی[۴]

تاریخ دریافت: ۱۴۰۱/۰۲/۳۱ تاریخ پذیرش ۱۴۰۱/۰۹/۱۵

چکیده

زمینه و هدف: جرایم فضای مجازی شامل هر کنش یا اقدامی است که از طریق فضای مجازی و با استفاده از ابزارهای اتصال به این فضا صورت گرفته و حقوق مشخص شده برای افراد را نقض می‌کند. پژوهش حاضر با هدف تحلیل و بررسی عوامل مؤثر (پیشران‌های) وقوع جرم در فضای مجازی با استفاده از رویکرد آمیخته انجام گرفت.

روش: این پژوهش در زمره پژوهش‌های آمیخته با رویکرد کیفی و کمی است که از نظر هدف، کاربردی و حیث ماهیت و روش، توصیفی پیمایشی است.

یافته‌ها: بر اساس قضاوت و نظرسنجی از خبرگان شانزده عامل به‌عنوان عوامل مؤثر وقوع جرم در فضای مجازی معرفی شده است. همچنین یافته‌ها نشان می‌دهد که ضعف سواد دیجیتالی کاربران، نیازهای احساسی، مالی و اطلاعاتی افراد، ضعف فرهنگی، کمبود قوانین و مقررات مناسب و بازدارنده، ناکارآمدی سیستم‌های ایمنی، تورم و نقایص اقتصادی، افزایش بیکاری و خطر پایین دستگیری مهمترین عوامل مؤثر در بروز رفتارهای مجرمانه در فضای مجازی هستند.

نتیجه‌گیری: جرم در فضای مجازی یکی از مهمترین معضلاتی است که در دهه‌های اخیر به شدت جوامع بشری را با تهدید مواجه ساخته است. شناخت عوامل زمینه‌ساز در بروز این‌گونه جرائم می‌تواند تا حد قابل توجهی از ارتکاب این جرایم در جامعه جلوگیری کند.

واژگان کلیدی: فضای مجازی، جرایم مجازی، جرم، عوامل مؤثر وقوع جرم.

---

۱. برگرفته از طرح تحقیقاتی مستقل است.

۲. استاد گروه مدیریت، دانشکده علوم انتظامی امین، تهران، ایران. رایانامه you_mohammad@yahoo.com

۳. دکتری مدیریت منابع انسانی، دانشگاه لرستان، خرم آباد، ایران. رایانامه saediabd115@gmail.com

٤. دانشیار گروه حقوق، دانشگاه علوم قضایی و خدمات اداری دادگستری، تهران، ایران. رایانه mohseni@afranet.com

مقدمه

وجود قوانین و مقررات و از همه مهمتر نظم و امنیت اجتماعی از جمله عناصری هستند که هر جامعه با تمام توان سعی در برآورده ساختن آن دارد. اما نگاه به زندگی اجتماعی بشر نشان می‌دهد عده‌ای هستند که به هنجارشکنی و قانون‌ستیزی گرایش دارند. نقض قانون معضلی است که بقا و سلامت جامعه را تهدید می‌کند (پاتک و همکاران[1]، ۲۰۲۰، ۲). از طرفی پیشرفت‌های تکنولوژی دگرگونی‌های عمیقی در دنیا ایجاد کرده که رشد شهرنشینی، گسترش وسایل ارتباطی، فروپاشی سنت‌های کهن و... تنها بخشی از جلوه‌های آن است. بدیهی است با هجوم سیل فناوری و دستاوردهای متنوع آن، جرم و جنایت نیز رنگ و بوی دیگری به خود گرفته است. به‌عبارتی متناسب با پیشرفت فناوری، شکل جرائم نیز تغییر یافت (شایخ[2]، ۲۰۱۹، ۴). با این وصف، توسعه فناوری در کنار امتیازات فراوانی که دارد، گستره فراوانی از فرصت‌های منحرفانه و مجرمانه را نیز فراهم آورده که نه تنها مجرمان را بر شیوه‌های جدید ارتکاب جرم توانمند ساخته؛ بلکه افرادی را که پیشتر منحرف نبودند نیز به رفتارهای مجرمانه واداشته است (بهره‌مند و همکاران، ۱۳۹۳، ۱۵۲). جرم در فضای مجازی یا جرائم مجازی[3] جزء ره‌آوردهای نوین تحولات فناوری است. جرایم مجازی هر نوع اقدام و فعالیتی را به‌منظور تبهکاری در شبکه‌های رایانه‌ای بازگو می‌کند (آمبیکا و سنتیلول[4]، ۲۰۲۰، ۶۷).

در واقع جرایم مجازی شامل هر کنش یا اقدامی است که از طریق فضای مجازی و با استفاده از ابزارهای اتصال به فضای مجازی صورت گرفته و حقوق مشخص شده برای افراد را نقض می‌کند. مجرمان فضای مجازی گاه آسیب‌های فراوان و جبران‌ناپذیری را بر پیکره هر دولت و جامعه‌ای وارد می‌سازند. باید بیان داشت که در پاره‌ای از اوقات

1 . Pathak et al
2 . Shaikh
3 . Cyber Crimes
4 . Ambika & Senthilvel

دولت‌ها با هدف تحمیل خسارت بر کشورهای دیگر از مجرمان فضای مجازی حمایت می‌کنند (تئونیسن و همکاران[1]، ۲۰۲۱، ۷). عصر ارتباطات و به‌دنبال آن شکستن مرزهای جغرافیایی امکان برقراری ارتباطات و تعاملات را با کمترین هزینه ممکن فراهم ساخته است. این امر از یک سو فرصت‌های مهم و بی‌شماری را برای توسعه و پیشبرد اهداف دولت‌ها ایجاد کرده و از سوی دیگر زمینه‌ساز تهدیدهایی برای امنیت سیاسی، فرهنگی و اقتصادی را موجب شده است. هر جامعه‌ای ضرورت بقای خود را در دفع عناصر مختل کننده امنیت خویش جستجو می‌کند. جرایمی که در فضای مجازی رخ می‌دهد یکی از مهمترین تهدیداتی است که در قیاس با جرایم سنتی، قربانیان بیشتری دارد (محسین[2]، ۲۰۲۰، ۳). امروزه انقلاب الکترونیک به تأثیرگذارترین پدیده در زندگی انسان مبدل گشته است. به طوری که هر روز شاهد ورود ابزارها و تجهیزات جدید برای ایجاد ارتباط در فضای مجازی هستیم. بهره‌گیری از این ابزارها بیش از پیش حیات بشری متحول ساخته و زندگی آنها را تسهیل ساخته است. براین اساس، باید بیان داشت که چنگ زدن به دامان علم و پیشرفت فناوری همیشه نویدبخش کارکردهای مثبت نیست و نباید از کارکردهای منفی آن غافل بود.

جرایم فضای مجازی جنبه‌ای از اثرات منفی توسعه فناوری در دنیای کنونی را به رخ می‌کشد که سرعت بالای آن در ارتکاب جرم و قرار نگرفتن در بعد مکان و زمان، باید توجه به آن را از مهمترین اقدامات دانست. ناکامی روش‌های سنتی مبارزه با جرایم فضای مجازی، صرفه‌جویی در هزینه‌های زمانی ارتکاب جرم، ناشناخته بودن مرتکبان و فراملی بودن آن ضرورت پرداختن به این پدیده مهم را آشکار می‌سازد. چرا که آسیب‌های جرایم فضای مجازی طیف گسترده‌ای (سیاسی، اقتصادی و فرهنگی) از عناصر جامعه را در بر می‌گیرد.

1 . Teunissen et al
2 . Mohsin

شناخت و آگاهی کافی از پدیده مورد نظر نه تنها برای دولتمردان مثمر ثمر خواهد بود، بلکه احتیاط و توجه کافی کاربران در فضای مجازی را در پی خواهد داشت. در بیانی کلی‌تر می توان گفت: که جرایم فضای مجازی از پدیده های نوظهوری است که تأثیرات ناگواری را بر جامعه متحمل می‌سازد. این امر برخورد جدی‌تری را از سوی مسئولان سیاسی و قضائی جامعه می‌طلبد. از این‌رو، پژوهش حاضر بر آن است با توجه به اهمیت موضوع و خلأ تحقیقاتی به‌خصوص در مطالعات داخلی، عوامل مؤثر وقوع جرم در فضای مجازی را مورد تحلیل و بررسی قرار دهد.

پیشینه و مبانی نظری

زلقی (۱۳۹۹)، در مطالعه خود بیان داشت که خلاءهای قانونی متعددی در زمینه مبارزه با جرایم فضای مجازی وجود دارد که روز بروز با پیشرفت علوم رایانه‌ای، فناوری اطلاعات و دیگر علوم مرتبط و نیز بهره‌گیری از مواد قانونی علمی قابل پیگیری و جلوگیری است. روش‌های متعددی از جمله ایمن ساخت پایگاه‌های اطلاعاتی، مراکز خدمات دهنده و نیز بروز کردن محققان و حقوقدانان وجود دارد که می‌تواند راه را بر مجرمان این صنعت ببندد. حیدری و همکاران (۱۳۹۷)، در پژوهشی نشان دادند که آموزش‌های تخصصی به افسران پلیس در خصوص فضای مجازی و رایانه کارآمدی آنها را افزایش خواهد داد. در حقیقت آنها بیان داشتند که افسران پلیس با بهره‌گیری از آموزه‌های جرم‌شناسی فضای مجازی ، افزایش خطرات ارتکاب جرم در این فضا را کاهش می‌دهند. بخارائی و کریمی (۱۳۹۵)، به بررسی دلایل و پیامدهای جرائم فضای مجازی پرداختند و با توجه به نظریه‌های مطرح شده در قالب سه دسته کلی ساختار اجتماعی، فرآیند اجتماعی و واکنش اجتماعی را مورد تحلیل قرار دادند. یافته‌های *مونتیت* و همکاران[1] (۲۰۲۱) و *الخاطر* و همکاران[2] (۲۰۲۰) حکایت از آن دارد که ضعف سیستم‌های ایمنی را یکی از دلایل عمده مجرمان در فضای مجازی برای سوء

1. Monteith et al
2. Al-Khater et al

استفاده تلقی می‌کنند. *لوکفلت* و *مالش*[1] (۲۰۲۰) نیز بیان داشتند که نیازهای احساسی، مالی و اطلاعاتی قربانیان می‌تواند عاملی مهیج و تحریک کننده برای مجرمان فضای مجازی باشد و آنها از این طریق مرتکب جنایت در فضای مجازی شوند. همچنین *ایان* و همکاران[2] (۲۰۲۰)، با توجه به شیوع و همه‌گیری کووید ۱۹ جرایم فضای مجازی را مورد تحلیل قرار دادند. آنها دریافتند که وابستگی به دنیای مجازی افزایش یافته است و انجام فعالیت‌هایی همچون آموزش و کار از راه دور، خرید برخط و... افزایش یافته است که این امر منجر به افزایش آسیب افراد در برابر جنایات فضای مجازی می‌شود. *الغمدی*[3] (۲۰۲۰)، معتقد است که نوآوری‌های فناوری نحوه تعامل در ابعاد اجتماعی، سیاسی و اقتصادی زندگی بشر را متحول ساخته است. این تحولات منجر به رشد قابل توجه جنایت، به ویژه در فضای مجازی شده است. جنایات فضای مجازی به‌طور فزاینده‌ای در حال افزایش است و مرتکبان هر روز روش‌های جدیدتر و پیچیده‌تری را توسعه می‌دهند. *جاین*[4] (۲۰۱۷)، نیز در پژوهشی بیان داشت نبود قوانین و مقررات مناسب و بازدارنده یکی از مهمترین عوامل تأثیرگذار در شکل‌گیری جرایم فضای مجازی است. *ریچاردسون* و *گیلمور*[5] (۲۰۱۵)، با انجام پژوهشی دریافتند که پیشرفت و توسعه فناوری بستر و شرایط مناسبی برای بهبود زندگی و کسب و کار ایجاد کرده است، ولی در عوض زمینه‌ساز جرایم مجازی نیز شده است. بنابراین، نداشتن زیرساخت مناسب می‌تواند در بروز این جرایم در جامعه دامن بزند. *الزب* و *برودهورست*[6] (۲۰۱۴)، در پژوهشی نشان دادند که جرایم مجازی نه تنها برای افراد بلکه برای مشاغل نیز خسارت قابل توجهی به‌دنبال داشته است که باعث اختلال در

1. Leukfeldt & Malsch
2. Eian et al
3. Alghamdi
4. Jain
5. Richardson & Gilmour
6. Alazab & Broadhurst

اشتغال و کاهش اعتماد به فعالیت‌های برخط شرکت می شود. یافته‌های *اورواشی*[1] (۲۰۱۰)، نیز نشان می‌دهد که هویت جعلی یا به‌عبارتی دیگر مخفی نگه‌داشتن هویت حقیقی فرد می‌تواند زمینه‌ساز جرم در فضای مجازی باشد.

اصطلاح فضای مجازی[2] در سال ۱۹۸۴ برای نخستین بار توسط *ویلیام گیبسون*[3] مطرح شد. فضای مجازی به مجموعه‌ای از ارتباطات میان انسان‌ها به وسیله وسایل الکترونیکی بدون در نظر گرفتن مکان فیزیکی (جغرافیایی) و زمان اشاره دارد (مدریوس و گلدونی[4]، ۲۰۲۰، ۳۵). در واقع فضای مجازی مفهومی برای توصیف فضای رقمی است. هدف آن ایجاد، ذخیره، اصلاح، تبادل، اشتراک و استخراج، استفاده، از بین بردن اطلاعات و مختل کردن منابع فیزیکی است (یان[5]، ۲۰۲۰، ۷۰). مفهوم فضای مجازی، معطوف به فضای ساختگی و خیالی واقعیت مجازی است که انسان از طریق آن به فضای واقعیت مجازی وارد می‌شود (خانیکی و بابایی، ۱۳۹۰، ۷۵). فضای مجازی نشان دهنده محیطی الکترونیکی و غیر فیزیکی است. به عبارتی به فضای مصنوعی (غیرطبیعی) ساخته شده توسط انسان اطلاق می‌شود. به بیانی دیگر، فضای مجازی یک مکان مجازی است که با خاصیت الکترونیک، مجموعه‌ای از اطلاعات را از طریق شبکه اطلاعات جهانی ارائه می‌دهد (کیت و جمیل[6]، ۲۰۱۸، ۶). فضای مجازی دنیای رایانه‌های الکترونیکی را برای تسهیل ارتباطات آنلاین بازگو می‌کند. در فضای مجازی یک شبکه بزرگ رایانه‌ای متشکل از شبکه‌های رایانه در سراسر جهان وجود دارد که به کمک آن فعالیت‌های ارتباطی و تبادل داده‌ها بهتر انجام می‌گیرد (مویهان[7]، ۲۰۲۰۲۰۲۰، ۷۷). *چوکری*[8] (۲۰۱۳) در تشریح فضای مجازی معتقد است

1. Urvashi
2. Cyber space
3. William Gibson
4. Medeiros & Goldoni
5. Yan
6. Keith & Jamil
7. Moynihan
8. Choucri

که این مفهوم به کمک شبکه‌های رایانه‌ای چارچوبی منطقی برای پردازش، تبادل، دست‌کاری، بهره‌برداری، افزایش اطلاعات و ارتباطات فراهم می‌سازد (مبانسو و داندارو[1]، ۲۰۱۵، ۱۹).

بدون شک جهان امروز نیازمند ارتباط شهروندان، سازمان‌ها و دولت‌ها با یکدیگر است که برای تحقق این امر باید مرزهای فرهنگی و سیاسی کنار گذاشته شود. فناوری اطلاعات این امکان را فراهم ساخته و مزایای ارزشمندی به ارمغان آورده است. اما در عین حال محیطی بسیار غنی برای بروز رفتارهای مجرمانه و خرابکارانه مهیا ساخته است (خارات[2]، ۲۰۱۷، ۶). جرایم و اعمال غیرقانونی همچون کلاهبرداری، سرقت هویت، قاچاق، نقض حریم خصوصی و ... به کمک رایانه را جرایم فضای مجازی می‌گویند. لازم به ذکر است که جنایات فضای مجازی بیشتر با هدف کسب سود انجام می‌گیرد. با این حال گاهی هدف آن است که مستقیماً به شبکه‌ها آسیب رسانده یا آن‌ها را غیرفعال سازند (گراهام[3]، ۲۰۱۸، ۴۱۴). رایانه سلاح مخرب جنایات مجازی تلقی می‌شود. سلاحی که به کمک آن جنایات با سرعت بسیار و با کمترین هزینه ممکن رخ می‌دهند (لئوفلدت و مالسچ[4]، ۲۰۲، ۶۳). طبیعت جرایم مجازی و سوءاستفاده‌های ناشی ناشی از آن هیچ‌گاه در دنیای واقعی دیده نمی‌شود. جرایمی که در فضای مجازی رخ می‌دهد مجرمان آن ناشناخته‌اند و حتی در پاره‌ای زمان تا ابد نیز قابل شناسایی نیستند (آمبیکا و سنتیلول، ۲۰۲، ۶۸). در تشریح جرایم مجازی می‌توان به این نکته نیز اشاره کرد که تفاوت جرایم فضای مجازی با جرایم سنتی در زمان ارتکاب جرم، مکان ارتکاب جرم و تعداد مجرم و مجرمان است. این بدان معناست که جرایم فضای مجازی در زمان و مکان خاصی رخ نمی‌دهد و حتی در برخی موارد مجرم یا مجرمان

1. Mbanaso & Dandaura
2. Kharat
3. Graham
4. Leukfeldt & Malsch

قابل شناسایی نیستند (ناپینی[1]، ۲۰۱۰، ۲۵). در حقیقت جرایم فضای مجازی، جرایم سازمان‌یافته‌ای هستند که توسط افراد حرفه‌ای انجام می‌شوند. از طرفی به دلیل پیشرفت فناوری و به تبع پیشرفت جرایم فضای مجازی قوانین بازدارنده هیچ‌گاه کامل نمی‌شوند. چون هر روز جرایم جدیدی شکل می‌گیرد که برای مجازات آنها نیاز به قوانین جدید است (زلقی و مالمیر، ۱۳۹۹، ۹۶). در تعریفی دیگر فضای مجازی شامل همه شرایطی است که در آن پردازش داده‌ها با هدف ارتکاب جرم انجام می‌گیرد و یا می‌توان گفت گفت هر عمل مجرمانه‌ای که در آن رایانه، وسیله یا هدف جرم تلقی می‌شود (یانگیوا[2]، ۲۰۲۱، ۱۳۴).

فضای مجازی علی‌رغم مزایا بی‌شمار برای مردم و دولت‌ها، بستر مناسبی برای وقوع جرایم است. شکل‌گیری جرایم در این فضا با شرایط سنتی و کلاسیک کاملاً متفاوت است و به تبع اثرات متفاوت و مخربی نیز بر جای خواهد گذاشت. در فضای مجازی جرائم به روش‌های مختلف رخ داده و آثار متفاوت و گوناگونی از خود بر جای می‌گذارد (بنارد و همکاران[3]، ۲۰۲۱، ۱۴۱). هزینه ورود کم، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدید کننده و عدم شفافیت در فضای مجازی موجب شده افراد جرایمی را به‌راحتی مرتکب شوند (محسنی و صوفی زمرد، ۱۳۹۶، ۱۶۸). به کمک فضای مجازی می‌توان فعالیت‌های جاسوسی را به‌راحتی انجام داد و اطلاعات ارزشمندی از افراد و دولت‌های دیگر به‌دست آورد و به‌عبارتی امنیت آن را به چالش کشید. بعد دیگر اثرات جرایم فضای مجازی، شمار قربانیان این جرایم است. در جرایم فضای مجازی تعداد قربانیان به‌طور چشمگیری بیشتر از جرایم معمولی است (چاندرا[4]، ۲۰۱۹، ۸۶۴). از دیگر اثرات جرایم در فضای مجازی تخریب حریم خصوصی افراد می‌باشد. چرا که قبل از توسعه فناوری هرگز این خطر برای جامعه بشری وجود

1. Nappinai
2. Yangaeva
3. Benard et al
4. Chandra

نداشت، اما توسعه روز افزون اطلاعات شخصی افراد را به در دسترس قرار می‌دهد (دوبی[1]، ۲۰۲۱، ۶۴۴). حریم خصوصی، قلمرویی برای حق خلوت انسان‌هاست که با حقوق و آزادی‌های فردی در بستر اجتماع، هم‌ریشه می‌باشد؛ ماهیت آن با هویت و شخصیت انسانی پیوند دارد و لذا در طول تاریخ، هم‌پای رشد فکر و تمدن بشری، مفهوم و مصادیق آن نیز متحول گشته‌اند. حق حریم خصوصی، از مهم‌ترین مصادیق حقوق بشر بوده و در مبانی فقهی و دینی، اسناد بین‌المللی و نظام‌های حقوقی اغلب کشورهای جهان، مطرح و به رسمیت شناخته شده است (محسنی، ۱۳۹۴، ۱۹۱). *سانگ*[2] (۲۰۰۸) نیز معتقد است که جرایم فضای مجازی تغییر هنجارها و ارزش‌های فرهنگی را امکان‌پذیر می‌سازد. از آنجا که هنجارها و اعتقادات از جامعه به جامعه دیگر متفاوت است، امکانات الکترونیکی تبادل و تأثر فرهنگی را رونق می‌بخشد. در این بین فرهنگ‌های ضعیف یا صاحبان فرهنگ‌های قدرتمند، اما کم تلاش متأثر از فرهنگ تهاجم قرار خواهند گرفت (دیلک و همکاران[3]، ۲۰۱۵، ۲۷). جرائم فضای مجازی حاکمیت و اقتدار سیاسی جوامع را خدشه‌دار می‌سازد. کشورهای قدرتمند یا جوامع‌ای که صاحبان شبکه‌های مجازی در دنیا تلقی می‌شود با دادن اطلاعات و داده-های اشتباه در خصوص سایر کشورها موجب سردرگمی مخاطب (کاربر) در فضای مجازی شده و به نوعی باور و اعتقاد آن نسبت به حاکمیت و اقتدار سیاسی جامعه کم-رنگ می‌شود (گانتا و کامور[4]، ۲۰۱۹، ۶۴۲). کاهش امنیت اطلاعاتی نیز جلوه‌ای دیگر از اثرات جرایم در فضای مجازی را نشان می‌دهد. ایجاد امنیت اطلاعاتی هم برای نهادهای دولتی و هم نهادهای بخش خصوصی فعال در بخش فناوری بسیار دارای اهمیت است که متأسفانه مورد حمله در فضای مجازی قرار گرفته و اطلاعات آن‌ها از بین رفته، مور سوءاستفاده قرار گرفته و یا تغییر می‌کند (آمبیکا و سنتیلول، ۲۰۲۰، ۶۹).

1. Dubey
2. Song
3. Dilek et al
4. Ganta & Kumar

روش پژوهش

این پژوهش دارای رویکردی آمیخته است که در دسته رویکردهای استقرایی و قیاسی می‌گنجد. پژوهش از نظر هدف، کاربردی و از حیث ماهیت و روش، در زمره پژوهش‌های اکتشافی است. با استناد به راهبرد پژوهش، لازم است تا مراحل انجام تحقیق در دو بخش کیفی و کمی به تفکیک تشریح شود. مشارکت‌کنندگان پژوهش در بخش کیفی را خبرگان دانشگاهی (دانشگاه علوم قضایی، دانشگاه علوم انتظامی امین و دانشگاه لرستان) تشکیل می‌دهند که براساس روش نمونه‌گیری هدفمند و بر مبنای اصل کفایت نظری تعداد ۱۶ نفر (کسانی که اطلاعات و درک آن‌ها در زمینه مورد بررسی کافی و از دانش، تخصص و تجربه لازم برخوردار و همچنین دارای تحصیلات مرتبط در این زمینه بودند) به‌عنوان اعضای نمونه انتخاب شدند. در بخش کمی پژوهش که از رویکرد دلفی فازی استفاده شده است. باید اذعان داشت با توجه ماهیت روش دلفی حجم نمونه بین ۱۰ الی ۱۵ نفر کفایت می‌کند، در برخی منابع نیز تعداد مطلوب ۱۰ الی ۲۰ نفر توصیه شده است (ارکانی و همکاران، ۱۳۹۹، ۲۹۸). از این‌رو از همان مشارکت‌کنندگان بخش کیفی به علت آشنایی با موضوع به‌عنوان نمونه بخش کمی بهره گرفته شد. در واقع حجم نمونه در بخش کیفی و کیفی ۱۶ نفر هستند. در بخش کیفی پژوهش برای گردآوری داده‌ها از مصاحبه ساختار نیافته (عمیق) استفاده شد که در آن با ارائه سوالاتی مشابه از پاسخ‌گویان درخواست شد آزادانه برای کسب ایده‌های جدید نظرات خود را بیان کنند. لازم به ذکر است که در بخش کمی هدف رتبه‌بندی و اولویت‌بندی شاخص های به‌دست آمده در بخش کیفی بود. لازم به ذکر است که روایی و پایایی ابزاری گردآوری اطلاعات در بخش کیفی به ترتیب با استفاده از ضریب CVR و آزمون کاپای ـ کوهن تأیید گردید. به این ترتیب در این بخش بعد از انجام مصاحبه به کمک رویکرد تحلیل مضمون و همچنین نرم افزار Atlas.tiعوامل مؤثر وقوع جرم در فضای مجازی شناسایی شد. از طرفی، در بخش کمی پژوهش برای تحلیل داده‌های گردآوری شده از بخش کیفی، از رویگرد دلفی

فازی بهره گرفته شد. همچنین برای گردآوری داده‌ها در بخش کمی از پرسش‌نامه مقایسه زوجی دلفی فازی استفاده که روایی آن از طریق روایی محتوا و پایایی آن از طریق نرخ ناسازگاری مورد تأیید قرار گرفت. در خصوص چرایی استفاده از روش‌های آماری مورد استفاده در پژوهش، لازم به ذکر است که با توجه به هدف اول تحقیق که شناسایی عوامل مؤثر وقوع جرم در فضای مجازی است، علاوه بر مطالعه متون، کتاب، مقاله و ... باید از مصاحبه هم استفاده می‌شد. پس از آن که هدف اول محقق شد، باید اولویت‌بندی و درجه اهمیت عوامل مؤثر وقوع جرم در فضای مجازی به‌عنوان هدف دوم انجام شود. از این‌رو، با استفاده از رویکرد دلفی فازی اولویت‌بندی و میزان اهمیت عوامل مؤثر وقوع جرم در فضای مجازی صورت گرفت.

یافته‌ها

الف) توصیف مشارکت‌کنندگان

یافته‌های جمعیت‌شناختی نشان می‌دهد که تمامی پاسخ‌دهندگان (۱۶ نفر) مرد هستند. همچنین در بین نمونه انتخابی ۶ نفر بین ۳۰- ۴۰ سال سن دارند که معادل ۰/۳۷ حجم نمونه انتخابی هستند. از طرفی اعضای نمونه بالاتر از ۴۱ سال ۱۰ نفر هستند که ۰/۶۳ حجم نمونه را به خود اختصاص داده‌اند. لازم به ذکر است که ۵ نفر دارای سابقه کاری ۵-۱۵ سال که معادل ۰/۳۱ حجم نمونه می‌باشد و ۷ نفر معادل ۰/۴۴ دارای سابقه کاری بین ۱۶-۲۵ هستند. از طرفی ۴ نفر معادل ۰/۲۵ دارای سابقه کاری بیش از ۲۵ می باشند. همچنین اعضای نمونه انتخابی همه دارای مدرک تحصیلی دکتری می‌باشند.

ب) یافته های بخش کیفی

در این بخش از پژوهش، عوامل مؤثر وقوع جرم در فضای مجازی با مطالعه متون و همچنین بهره‌گیری از مصاحبه با خبرگان مشخص شد. در تشریح نحوه استخراج عوامل مؤثر وقوع جرم در فضای مجازی لازم به ذکر است که عوامل مذکور با بررسی مطالعات گذشته و نیز متون مصاحبه و استفاده از نرم افزار Atlas.ti و همچنین رویکرد کدگذاری (باز، محوری و انتخابی) صورت پذیرفت. بدین شکل که سؤالات مصاحبه

که در قالب شش سوال اصلی بود با ارائه به اعضای نمونه، توضیحات لازم توسط محققان به آنها داده شد و سپس بعد از مصاحبه انجام‌شده با استفاده از روش کدگذاری و با کمک نرم‌افزار Atlas.ti داده‌ها تحلیل شد. در شکل زیر بخشی (به دلیل حجیم بودن فرآیند کدگذاری و همچنین نبودن فضای کافی برای گنجاندن آن در این پژوهش) از این فرآیند نشان داده شده است.

جدول ۱. فرآیند کدگذاری پژوهش

کدهای باز	کدهای محوری	کدهای انتخابی
عدم تولید خلاقانه ارتباطات، نداشتن مطالعه انتقادی، ضعف در تفسیر و درک اطلاعات، ناتوانی در اشتراک اطلاعات، ناتوانی مدیریت کردن اطلاعات، ضعف در برقرای ارتباطات، عدم مشارکت در شبکه های مجازی، عدم همکاری با دیگران	عدم سواد اطلاعاتی، ضعف سواد رسانه‌ای، ناتوانی ارتباط و همکاری	ضعف سواد دیجیتالی کاربران
بهره‌برداری لجام گسیخته از منابع، فرآیند اداری بالا و پیچیده، محدودیت درآمد، فقر، برنامه‌های نادرست و نامطلوب، افزایش بی رویه قیمت‌ها، گستردگی اندازه دولت	توسعه‌نیافتگی نظام اقتصادی، بی‌ثباتی در سیاست‌ها و برنامه‌ها، بی ثباتی در قیمت‌ها	تورم و نقایص اقتصادی
مجازات کم و نامعقول، تعریف نکردن انواع جرائم در فضای مجازی و مجازات آنها، بی‌توجهی به قوانین اثربخش، قوانین ضعیف و نداشتن قدرت بازدارندگی، محدودیت قوانین و مقررات،	خلاء قوانین و مقررات، بازدارندگی نبودن قوانین، کمبود قوانین به‌روز و کارآمد	نبود قوانین و مقررات مناسب و بازدارنده

عدم توجه از سوی خانواده، تمایل به ارتباطات احساسی در فضای مجازی، عدم عزت نفس، وضع اقتصادی بد، نداری، نیاز مالی شدید، کنجاوی به کسب اطلاعات درباره دیگران، دخالت در زندگی شخصی دیگران	نیاز به احترام، فقر و تنگدستی، نیازهای اطلاعاتی	نیازهای احساسی، مالی و اطلاعاتی افراد
استفاده از نام‌ها و عناوین جعلی، سوءاستفاده از هویت دیگران برای فریب کاربران، ناآگاهی کاربران از هویت واقعی مجرمان، مخفی نمودن نام و نشان خود	پنهان داشتن هویت خود، هویت جعلی	امکان جعل هویت و مخفی نگه‌داشتن آن

بنابراین، بعد از انجام کامل فرایند کدگذاری در نهایت کدهای انتخابی تعیین گردید. در حقیقت کدهای انتخابی براساس نتایج کدهای باز و محوری شکل می‌گیرد که در رویکرد کدگذاری، مرحله اصلی نظریه‌پردازی از آن یاد می‌شود. در این پژوهش در جدول شماره یک کدهای انتخابی که نشان دهنده عوامل مؤثر وقوع جرم در فضای مجازی هستند، ارائه شده است.

جدول ۱- عوامل مؤثر وقوع جرم در فضای مجازی

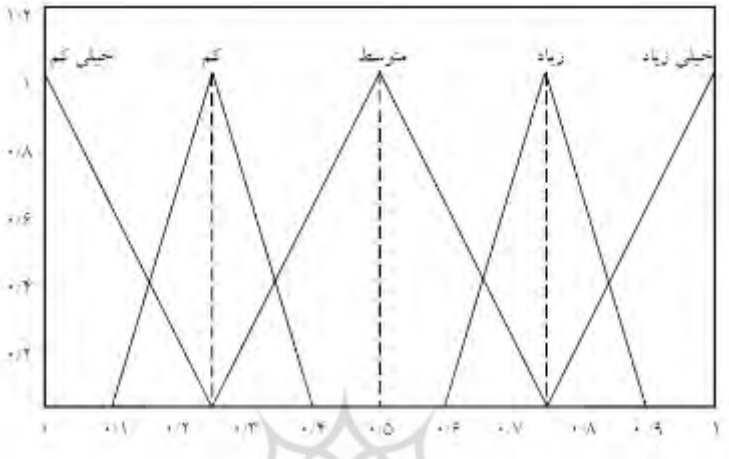
نماد شاخص‌ها	عوامل مؤثر	نماد شاخص‌ها	عوامل مؤثر
AX1	ناکارآمدی سیستم های ایمنی	AX9	کاهش میزان تعهد
AX2	وابستگی زیاد افراد به فضای مجازی	AX10	امکان جعل هویت و مخفی نگه داشتن آن
AX3	ضعف سواد دیجیتالی کاربران	AX11	همسالان و عضویت در گروه ای معارض
AX4	نیازهای احساسی،	AX12	خطر پایین دستگیری

	مالی و اطلاعاتی افراد		
AX5	افزایش بیکاری	AX13	دسترسی آسان به اطلاعات
AX6	عوامل فردی (سن، جنسیت، شاخصه-های روانی - شخصیتی)	AX14	ناهماهنگی نهادها و ارگان های ناظر
AX7	ضعف فرهنگی	AX15	نبود قوانین و مقررات مناسب و بازدارنده
AX8	تورم و نقایص اقتصادی	AX16	نداشتن آگاهی لازم

ج) یافته‌های بخش کمی

تعریف متغیرهای زبانی: در این مرحله از پژوهش، نظرات خبرگان در خصوص عوامل مؤثر وقوع جرم در فضای مجازی در قالب پرسش‌نامه مشخص می‌شود. لذا خبرگان باید میزان موافقت خود را تعیین نمایند. در این قبیل موارد خیلی نمی‌توان با مقادیر قطعی نظر خبرگان را جویا شد. به همین خاطر استفاده از متغیرهای کیفی، آزادی عمل بیشتری را در اظهارنظر به خبرگان خواهد بخشید. به‌عبارتی استفاده از متغیرهای کیفی همچون: «کم»، «متوسط»، «زیاد» و ... مشکلات فوق را تا حد زیادی کاهش خواهد داد، اما مسئله و مشکل دیگری ایجاد می‌کند. از آنجا که ذهنیت افراد نسبت به متغیرهای کیفی یکسان نیست. از طرفی خصوصیات متفاوت افراد بر تعابیر ذهنی آنها نسبت به متغیرهای کیفی اثرگذار است؛ یعنی برخی افراد خوش‌بین و برخی بدبین و یا برخی نگرش آسان‌گیرانه و یا سختگیرانه دارند که بر تعابیر ذهنی آنها تأثیرگذار است. از این‌رو، تجزیه و تحلیل بر روی متغیرهای منتج از ذهنیت و تعابیر مختلف، ارزشی

نخواهد داشت. لذا متغیرهای کیفی به شکل اعداد فازی مثلثی تعریف می‌شوند که در شکل و جدول زیر نشان داده شده‌اند.



شکل ۱- تعریف متغیرهای زبانی

همچنین در جدول شماره چهار نیز طریقه متغیرهای کلامی یا کیفی به اعداد فازی مثلثی و عدد فازی قطعی شده نشان داده شده است.

جدول ۲. اعداد فازی

متغیرهای کلامی (کیفی)	اعداد فازی مثلثی	عدد فازی قطعی شده
خیلی زیاد	۰/۷۵-۱-۱	۰/۹۱
زیاد	۱-۰/۷۵-۰/۵	۰/۷۵
متوسط	۰/۷۵-۰/۵-۰/۲۵	۰/۵
کم	۰/۵-۰/۲۵-۰	۰/۲۵
خیلی کم	۰/۲۵-۰-۰	۰/۸۳

با توجه به جدول و شکل بالا پس از تطبیق هر شاخص با مقادیر فازی و تخصیص سطح زبانی، باید اعداد فازی به اعداد کمی تبدیل شوند یا به عبارتی فازی‌زدایی شوند. یکی

از پرکاربردترین روش‌ها در این زمینه فرمول مینکووسکی[1] می‌باشد که در آن اعداد قطعی به اعداد فازی تبدیل می‌شوند. لازم به ذکر است که در فرمول مینکووسکی β حد بالای فازی مثلثی، α حد وسط عدد فازی مثلثی و M حد پایین عدد فازی مثلثی را نشان می‌دهد، ارائه شده است.

عوامل مؤثر وقوع جرم در فضای مجازی					
شاخص‌ها	**خیلی زیاد**	**زیاد**	**متوسط**	**کم**	**خیلی کم**
ناکارآمدی سیستم‌های ایمنی	۱۳	۰	۱	۱	۱
وابستگی زیاد افراد به فضای مجازی	۱۲	۱	۰	۰	۳
ضعف سواد دیجیتالی کاربران	۱۰	۳	۰	۲	۱
نیازهای احساسی، مالی و اطلاعاتی افراد	۱۴	۰	۰	۰	۲
افزایش بیکاری	۱۳	۰	۰	۱	۲
عوامل فردی (سن، جنسیت، شاخصه‌های روانی ـ شخصیتی)	۱۱	۲	۰	۰	۳
ضعف فرهنگی	۱۰	۳	۱	۲	۰
تورم و نقایص اقتصادی	۹	۴	۰	۳	۰
کاهش میزان تعهد	۸	۳	۴	۱	۰
امکان جعل هویت و مخفی نگه داشتن آن	۱۱	۰	۲	۱	۲
همسالان و عضویت در گروه‌های معارض	۹	۲	۳	۱	۱
خطر پایین دستگیری	۱۲	۰	۱	۰	۳
دسترسی آسان به اطلاعات	۱۰	۱	۲	۲	۱
ناهماهنگی نهادها و ارگان‌های ناظر	۹	۲	۳	۱	۱
نبود قوانین و مقررات مناسب و بازدارنده	۱۱	۱	۰	۱	۳
نداشتن آگاهی لازم	۸	۴	۱	۱	۲

1. Minkowski

نظرسنجی مرحله اول. در این مرحله، محققان پیامدهای شناسایی شده را در قالب پرسش‌نامه در اختیار خبرگان قرار می دهند و میزان موافقت آنها با هر کدام از مؤلفه‌ها دریافت و نظرات پیشنهادی و اصلاحی آنها جمع‌بندی می‌شود. به این ترتیب، نتایج حاصل از بررسی پاسخ‌های قید شده در پرسش‌نامه برای به دست آوردن میانگین فازی مؤلفه‌ها مورد تحلیل قرار می‌گیرند. برای محاسبه میانگین فازی از روابط زیر استفاده می‌شود.

رابطه (۲) $\boldsymbol{A_i = \left(a_1^i, a_2^i, a_3^i\right), i = 1, 2, 3, \dots, n}$

رابطه (۳)

$$\boldsymbol{A_{ave} = (m_1, m_2, m_3) = \left(\frac{1}{n}\sum_{i=1}^{n} a_1^{(i)}, \frac{1}{n}\sum_{i=1}^{n} a_2^{(i)}, \frac{1}{n}\sum_{i=1}^{n} a_3^{(i)}\right)}$$

در این رابطه A_i بیانگر دیدگاه خبره iام و A_{ave} بیانگر میانگین دیدگاه‌های خبرگان است. بعد از جمع‌آوری پرسش‌نامه‌ها، تعداد پاسخ‌های داده‌شده به هر عامل مورد شمارش و بررسی قرار گرفت که در نظرسنجی مرحله اول نتایج شمارش پاسخ‌های داده‌شده در جدول شماره سه نشان داده‌شده است.

جدول۳. نظرسنجی مرحله اول عوامل مؤثر وقوع جرم در فضای مجازی

عوامل مؤثر	میانگین فازی مثلثی			مقدار کریسپ	عوامل مؤثر	میانگین فازی مثلثی			مقدار کریسپ
	B	α	m			β	α	m	
ناکارآمدی سیستم های ایمنی	۰/۹۰۶	۰/۶۲۵	۰/۸۵۹	۰/۹۲۹	کاهش میزان تعهد	۰/۹۰۶	۰/۵۳۱	۰/۷۸۱	۰/۸۷۵
وابستگی زیاد افراد به فضای مجازی	۰/۸۵۹	۰/۵۹۳	۰/۷۹۶	۰/۸۶۳	امکان جعل هویت و مخفی نگه داشتن آن	۰/۸۴۳	۰/۵۴۶	۰/۷۶۵	۰/۸۳۹
ضعف سواد	۰/۸۹۰	۰/۵۶۲	۰/۷۹۶	۰/۸۷۹	همسالان و	۰/۸۷۵	۰/۵۳۱	۰/۷۶۶	۰/۸۵۱

دیجیتالی کاربران				عضویت در گروهای معارض				
نیازهای احساسی، مالی و اطلاعاتی افراد	۰/۹۰۶	۰/۶۵۶	۰/۸۷۵	خطر پایین دستگیری	۰/۹۳۷	۰/۸۴۳	۰/۵۷۸	۰/۷۸۱	۰/۸۴۷
افزایش بیکاری	۰/۸۷۵	۰/۶۰۹	۰/۸۲۸	دسترسی آسان به اطلاعات	۰/۸۹۴	۰/۸۵۹	۰/۵۳۱	۰/۷۶۵	۰/۸۴۸
عوامل فردی (سن، جنسیت، شاخصه‌های روانی - شخصیتی)	۰/۸۵۹	۰/۵۷۸	۰/۷۸۱	ناهماهنگی نهادها و ارگان-های ناظر	۰/۸۵۱	۰/۸۷۵	۰/۵۳۲	۰/۷۶۶	۰/۸۵۱
ضعف فرهنگی	۰/۹۲۱	۰/۵۷۸	۰/۸۲۸	نبود قوانین و مقررات مناسب و بازدارنده	۰/۹۱۴	۰/۸۲۹	۰/۵۴۶	۰/۷۵۰	۰/۸۲۰
تورم و نقایص اقتصادی	۰/۹۰۶	۰/۵۴۶	۰/۷۹۶	نداشتن آگاهی لازم	۰/۸۸۶	۰/۸۶۰	۰/۵۱۵	۰/۷۳۴	۰/۸۲۱

زمانی که تعداد پاسخ‌های داده شده به هر شاخص مشخص شد و پس از بهره‌گیری از فرمول *مینکووسکی* برای محاسبه میانگین فازی مثلثی هر عامل، باید اعداد فازی قطعی شده برای آن عامل محاسبه شود. نتایج حاصل از میانگین فازی و فازی‌زدایی مؤلفه‌ها به شرح جدول زیر است.

جدول٤- میانگین دیدگاه‌های خبرگان حاصل ازنظر سنجی مرحله اول

عوامل مؤثر	میانگین فازی مثلثی			مقدار کریسپ	علل موثر	میانگین فازی مثلثی			مقدار کریسپ
	β	α	m			β	α	m	
ناکارآمدی سیستم های امنیتی	۰/۹۰۶	۰/۶۲۵	۰/۸۵۹	۰/۹۲۹	کاهش میزان تعهد	۰/۹۰۶	۰/۵۳۱	۰/۷۸۱	۰/۸۷۵
وابستگی زیاد افراد به فضای مجازی	۰/۸۵۹	۰/۵۹۳	۰/۷۹۶	۰/۸۶۳	امکان جعل هویت و مخفی نگه داشتن آن	۰/۸۴۳	۰/۵۴۶	۰/۷۶۵	۰/۸۳۹
ضعف سواد دیجیتالی کاربران	۰/۸۹۰	۰/۵۶۲	۰/۷۹۶	۰/۸۷۹	همسالان و عضویت در گروه ای معارض	۰/۸۷۵	۰/۵۳۱	۰/۷۶۶	۰/۸۵۱
نیازهای احساسی، مالی و اطلاعاتی افراد	۰/۹۰۶	۰/۶۵۶	۰/۸۷۵	۰/۹۳۷	خطر پایین دستگیری	۰/۸۴۳	۰/۵۷۸	۰/۷۸۱	۰/۸۴۷
افزایش بیکاری	۰/۸۷۵	۰/۶۰۹	۰/۸۲۸	۰/۸۹۴	دسترسی آسان به اطلاعات	۰/۸۵۹	۰/۵۳۱	۰/۷۶۵	۰/۸۴۸
عوامل فردی (سن، جنسیت، شاخصه-های روانی - شخصیتی)	۰/۸۵۹	۰/۵۷۸	۰/۷۸۱	۰/۸۵۱	ناهماهنگی نهادها و ارگان‌های ناظر	۰/۸۷۵	۰/۵۳۲	۰/۷۶۶	۰/۸۵۱
ضعف فرهنگی	۰/۹۲۱	۰/۵۷۸	۰/۸۲۸	۰/۹۱۴	نبود قوانین و مقررات مناسب و بازدارنده	۰/۸۲۹	۰/۵۴۶	۰/۷۵۰	۰/۸۲۰

تورم و فساد اقتصادی	۰/۹۰۶	۰/۵۴۶	۰/۷۹۶	۰/۸۸۶	نداشتن آگاهی لازم	۰/۸۶۰	۰/۵۱۵	۰/۷۳۴	۰/۸۲۱

با انجام نظرسنجی در مرحله اول لازم است که مرحله دوم نظرسنجی هم صورت پذیرفت. دلیل این امر آن است که نتایج کسب شده از هر مرحله با هم مقایسه و نتیجه مشخص گردد. **نظرسنجی مرحله دوم.** در رویکرد دلفی فازی لازم است که نظر خبرگان طی مراحل نظرسنجی مورد قیاس قرار گیرد و تا زمان یکه اجماع نظر حاصل نشود، روند نظرسنجی ادامه می‌یابد. در مرحله اول نظرسنجی نظرات خبرگان مورد بررسی قرار گرفت و میانگین فازی‌زدایی شده نظرات آنها در جدول شماره ۴ مشخص شد. حال برای آنکه نظرات آنها طی گام ها و مراحل بعدی مورد بررسی قرار گیرد لازم بود که نظرسنجی گام دوم انجام شود تا پاسخ ها آنها با مرحله اول مورد بررسی قرار گیرد. در جدول زیر نتایج پاسخ‌های داده شده به هریک از عوامل و نظرسنجی مرحله دوم نشان داده شده است.

جدول۵. نظرسنجی مرحله دوم عوامل مؤثر وقوع جرم در فضای مجازی

عوامل مؤثر وقوع جرم در فضای مجازی					
شاخص‌ها	**خیلی زیاد**	**زیاد**	**متوسط**	**کم**	**خیلی کم**
ناکارآمدی سیستم‌های ایمنی	۱۲	۰	۲	۲	۰
وابستگی زیاد افراد به فضای مجازی	۱۳	۰	۱	۱	۱
ضعف سواد دیجیتالی کاربران	۱۲	۱	۰	۱	۲
نیازهای احساسی، مالی و اطلاعاتی افراد	۱۳	۰	۱	۰	۲
افزایش بیکاری	۱۱	۲	۱	۰	۲
عوامل فردی (سن، جنسیت، شاخصه‌های روانی ـ شخصیتی)	۱۲	۰	۱	۲	۱
ضعف فرهنگی	۱۱	۳	۰	۱	۱

تورم و نقایص اقتصادی	۱۰	۳	۱	۱	۱
کاهش میزان تعهد	۷	۵	۲	۲	۰
امکان جعل هویت و مخفی نگه داشتن آن	۱۲	۱	۰	۰	۳
همسالان و عضویت در گروه-های معارض	۸	۳	۳	۲	۰
خطر پایین دستگیری	۱۱	۱	۰	۲	۲
دسترسی آسان به اطلاعات	۹	۲	۰	۵	۰
ناهماهنگی نهادها و ارگان‌های ناظر	۱۱	۰	۳	۱	۰
نبود قوانین و مقررات مناسب و بازدارنده	۱۰	۱	۰	۴	۱
نداشتن آگاهی لازم	۷	۵	۳	۰	۱

زمانی که تعداد پاسخ‌های داده شده به هر شاخص در مرحله دوم مشخص شد و پس از بهره‌گیری از فرمول *مینکووسکی* برای محاسبه میانگین فازی مثلثی هر عامل، لازم است همچون مرحله اول اعداد فازی قطعی شده برای آن عامل محاسبه شود. به این ترتیب، نتایج حاصل از میانگین فازی و فازی‌زدایی مؤلفه‌ها در جدول زیر نشان داده شده است.

جدول٦. میانگین دیدگاه‌های خبرگان حاصل از نظر سنجی مرحله دوم

عومل مؤثر	میانگین فازی مثلثی			مقدار کریسپ	عوامل مؤثر	میانگین فازی مثلثی			مقدار کریسپ
	B	A	M			β	α	m	
ناکارآمدی سیستم‌های ایمنی	۰/۹۰۶	۰/۵۹۳	۰/۸۴۳	۰/۹۲۱	کاهش میزان تعهد	۰/۹۰۳	۰/۵۱۶	۰/۷۶۵	۰/۸۶۲
وابستگی زیاد افراد	۰/۹۰۷	۰/۶۲۵	۰/۸۵۹	۰/۹۲۹	امکان جعل	۰/۸۵۹	۰/۵۹۳	۰/۷۹۶	۰/۸۶۳

به فضای مجازی				هویت و مخفی نگه داشتن آن					
ضعف سواد دیجیتالی کاربران	۰/۸۷۵	۰/۵۹۳	۰/۸۲۹	همسالان و عضویت در گروههای معارض	۰/۸۸۲	۰/۸۹۰	۰/۵۱۵	۰/۷۶۵	۰/۸۶۰
نیازهای احساسی، مالی و اطلاعاتی افراد	۰/۸۹۰	۰/۶۲۵	۰/۸۴۳	خطر پایین دستگیری	۰/۹۳۳	۰/۸۴۳	۰/۵۴۶	۰/۷۶۵	۰/۸۳۹
افزایش بیکاری	۰/۸۹۱	۰/۵۹۳	۰/۸۱۲	دسترسی آسان به اطلاعات	۰/۸۸۶	۰/۸۴۴	۰/۴۸۴	۰/۷۲۴	۰/۸۱۴
عوامل فردی (سن، جنسیت، شاخصه-های روانی - شخصیتی)	۰/۸۷۵	۰/۵۷۸	۰/۸۱۲	ناهماهنگی نهادها و ارگان‌های ناظر	۰/۸۸۶	۰/۸۵۹	۰/۵۶۲	۰/۷۹۶	۰/۸۷۱
ضعف فرهنگی	۰/۹۲۱	۰/۶۰۹	۰/۸۴۳	نبود قوانین و مقررات مناسب و بازدارنده	۰/۹۱۹	۰/۸۲۸	۰/۵۰۰	۰/۷۲۴	۰/۸۱۶
تورم و فساد اقتصادی	۰/۹۰۶	۰/۵۷۸	۰/۸۱۲	نداشتن آگاهی لازم	۰/۸۹۴	۰/۹۰۶	۰/۵۱۳	۰/۷۶۵	۰/۸۵۹

بعد از آنکه نظرسنجی در هر دو مرحله انجام گرفت لازم است که اختلاف میانگین فازی‌زدایی شده (مقدار کریسپ) در دو مرحله مورد تحلیل و بررسی قرار گیرد و اختلاف‌ها مشخص شود. بنابراین، اختلاف میانگین فازی‌زدایی شده (مقدار کریسپ)

عوامل مؤثر وقوع جرم در فضای مجازی در مرحله اول و مرحله دوم به شرح جدول زیر است.

جدول ۷- اختلاف میانگین فازی‌زدایی شده (مقدار کریسپ) مرحله اول و دوم

عوامل مؤثر	مقدار کریسپ مرحله اول	مقدار کریسپ مرحله دوم	اختلاف کریسپ مرحله اول و دوم	عوامل مؤثر	مقدار کریسپ مرحله اول	مقدار کریسپ مرحله دوم	اختلاف کریسپ مرحله اول و دوم
ناکارآمدی سیستم‌های ایمنی	۰/۹۲۹	۰/۹۲۱	۰/۰۰۸	کاهش میزان تعهد	۰/۸۷۵	۰/۸۶۲	۰/۰۱۳
وابستگی زیاد افراد به فضای مجازی	۰/۸۶۳	۰/۹۲۹	۰/۰۳۴	امکان جعل هویت و مخفی نگه داشتن آن	۰/۸۳۹	۰/۸۶۳	۰/۰۳۴
ضعف سواد دیجیتالی کاربران	۰/۸۷۹	۰/۸۸۲	۰/۰۰۳	همسالان و عضویت در گروه‌های معارض	۰/۸۵۱	۰/۸۶۰	۰/۰۱۱
نیازهای احساسی، مالی و اطلاعاتی افراد	۰/۹۳۷	۰/۹۳۳	۰/۰۰۴	خطر پایین دستگیری	۰/۸۴۷	۰/۸۳۹	۰/۰۰۸
افزایش بیکاری	۰/۸۹۴	۰/۸۸۶	۰/۰۰۸	دسترسی آسان به اطلاعات	۰/۸۴۸	۰/۸۱۴	۰/۰۳۲
عوامل فردی (سن، جنسیت، شاخصه‌های روانی - شخصیتی)	۰/۸۵۱	۰/۸۸۶	۰/۰۳۵	ناهماهنگی نهادها و ارگان-های ناظر	۰/۸۵۱	۰/۸۷۱	۰/۰۲۰
ضعف فرهنگی	۰/۹۱۴	۰/۹۱۹	۰/۰۰۵	نبود قوانین و	۰/۸۲۰	۰/۸۱۶	۰/۰۰۴

			مقررات مناسب و بازدارنده				
تورم و نقایص اقتصادی	۰/۸۸۶	۰/۸۹۴	۰/۰۰۸	نداشتن آگاهی لازم	۰/۸۲۱	۰/۸۵۹	۰/۰۳۸

در رویکرد دلفی فازی با انجام نظرسنجی از خبرگان لازم است تا اجماع‌نظر صورت پذیرد و این امر از قیاس نظرسنجی در طی مراحل مختلف انجام می‌گیرد. بنابراین، هنگامی که اختلاف میانگین فازی‌زدایی شده (مقدار کریسپ) در طی دو مرحله کمتر از ۰/۱ باشد؛ فرایند نظرسنجی متوقف می‌شود، اما در صورتی که این اختلاف بیشتر از ۰/۱ باشد؛ مجدداً نظرسنجی انجام می‌گیرد و تا زمانی که اجماع نظر صورت نپذیرد، این روند ادامه می‌یابد. همان‌گونه که در جدول ۷ ملاحظه می‌شود اختلاف میانگین فازی‌زدایی شده (مقدار کریسپ) در دو مرحله کمتر از ۰/۱ می‌باشد. این بدان معناست که خبرگان در خصوص عوامل مؤثر وقوع جرم در فضای مجازی به اجماع نظر رسیده‌اند و در همین مرحله نظرسنجی متوقف می‌شود. در واقع خبرگان به عوامل مؤثر شناسایی شده در پژوهش حاضر نگاه تقریباً یکسانی دارند. با توجه به مطالب ذکر شده، در نهایت تمامی عوامل مؤثر وقوع جرم در فضای مجازی در قالب نمودار زیر نشان داده شده است.

نمودار ۱- اولویت عوامل مؤثر وقوع جرم در فضای مجازی

با توجه به نتایج جدول شماره هفت و همچنین نمودار یک می‌توان گفت که شاخص-های شناسایی شده از لحاظ اهمیت رتبه‌بندی و اولویت‌بندی شدند. در حقیقت هدف از بکارگیری روش دلفی فازی اولویت شاخص‌های مؤثر وقوع جرم در فضای مجازی بود. بنابراین، تحلیل داده‌ها حکایت از آن دارد که ضعف سواد دیجیتالی کاربران، نیازهای احساسی، مالی و اطلاعاتی افراد، ضعف فرهنگی، نبود قوانین و مقررات مناسب و بازدارنده، ناکارآمدی سیستم‌های ایمنی، تورم و نقایص اقتصادی، افزایش بیکاری و ریسک پایین دستگیری از بین شانزده عامل به‌دست آمده مهمترین عوامل مؤثر در بروز رفتارهای مجرمانه در فضای مجازی است.

بحث و نتیجه‌گیری

تکامل زندگی بشر عصری را رقم می‌زند که در آن بیشتر فعالیت‌های انسان به سمت استفاده از ابزارهای دیجیتالی سوق پیدا کرده است. در حقیقت مهمترین دستاورد توسعه تکنولوژی طی دهه‌های اخیر عبور از جامعه صنعتی به جامعه اطلاعاتی (فراصنعتی) است. این پیشرفت توسط محققان دومین انقلاب جامعه بشری است که منجر به سوق یافتن فعالیت‌های فکری انسان به ماشین‌ها شد. اوج توسعه فناوری در دنیای کنونی شکل‌گیری فضای مجازی است که با همه گستردگی و جهان شمول بودنش و نیز اثرات مثبتی که در زندگی انسان بر جای گذاشته، از تیررس مجرمان رایانه‌ای، تبعات و آثار منفی و مخرب آن مصون نمانده است. مجرمانی که به راحتی حریم شخصی افراد را نقض کرده و می‌توانند در مدت زمان کوتاهی نه تنها به افراد؛ بلکه به دولت‌ها خسارت‌های جبران‌ناپذیری را متحمل سازند. به این ترتیب، پژوهش حاضر با هدف تحلیل و بررسی عوامل مؤثر وقوع جرم در فضای مجازی انجام پذیرفت. از آنجایی که پژوهش حاضر در زمرهٔ رویکردهای آمیخته قرار می‌گیرد، لازم است نتایج حاصل از هر بخش به تفکیک تشریح شود. به این ترتیب در بخش کیفی پژوهش با بررسی مطالعات گذشته و انجام مصاحبه (تحلیل مضمون) و با کمک روش کدگذاری و نرم افزار Atlas.ti عوامل مؤثر وقوع جرم در فضای مجازی شناسایی

شد. نتایج حاصل از این بخش نشان داد که شانزده عامل در وقوع جرم در فضای مجازی تأثیرگذار هستند که این عوامل شامل: ناکارآمدی سیستم‌های ایمنی، وابستگی زیاد افراد به فضای مجازی، ضعف سواد دیجیتالی کاربران، نیازهای احساسی، مالی و اطلاعاتی افراد، افزایش بیکاری، عوامل فردی (سن، جنسیت، شاخصه‌های روانی ـ شخصیتی)، ضعف فرهنگی، تورم و نقایص اقتصادی، کاهش میزان تعهد، امکان جعل هویت و مخفی نگه داشتن آن، همسالان و عضویت در گروه‌های معارض، خطر پایین دستگیری، دسترسی آسان به اطلاعات، ناهماهنگی نهادها و ارگان های ناظر، نبود قوانین و مقررات مناسب و بازدارنده و نداشتن آگاهی لازم می‌باشند. از طرفی با مشخص شدن عوامل مؤثر وقوع جرم در فضای مجازی لازم است که میزان و درجه اهمیت هر یک از عوامل مذکور نیز مشخص شد، این امر در بخش کمی پژوهش مورد تحلیل و واکاوی قرار گرفت. در این بخش اولویت‌بندی شاخص‌ها به کمک رویکرد دلفی فازی صورت پذیرفت. در واقع میزان اهمیت و تأثیرگذاری عوامل به‌دست آمد و همچنین مشخص شد که خبرگان در خصوص عوامل مؤثر وقوع جرم در فضای مجازی توافق نظر دارند. بنابراین، نتایج گویای آن است که اختلاف میانگین فازی-زدایی شده در پژوهش حاضر کمتر از ۰/۱ می‌باشند. قضیه فوق حکایت از آن دارد که خبرگان در خصوص عوامل مؤثر شناسایی شده نگاه تقریباً یکسانی دارند. با این تفاسیر مشخص شد که ضعف سواد دیجیتالی کاربران، نیازهای احساسی، مالی و اطلاعاتی افراد، ضعف فرهنگی، نبود قوانین و مقررات مناسب و بازدارنده، ناکارآمدی سیستم-های ایمنی، تورم و نقایص اقتصادی، افزایش بیکاری و خطر پایین دستگیری از بین شانزده عامل به‌دست آمده مهمترین عوامل مؤثر در بروز رفتارهای مجرمانه در فضای مجازی است. نداشتن توان و مهارت استفاده از فناوری‌های روز منجر می شود که کاربر به‌راحتی در فضای مجازی مورد سوءاستفاده قرار گیرد. ضعف سواد دیجیتال مسیر و محیط پر طعمه‌ای را برای مجرمان فضای مجازی فراهم می‌سازد. همچنین

ندانستن آداب استفاده از فضای مجازی یا به‌عبارتی ضعف فرهنگی نیز عامل مهم دیگر در ارتکاب جرم است. در خصوص وجوه افتراق و اشتراک پژوهش حاضر با پژوهش‌های صورت گرفته می‌توان اذعان داشت که نتایج پژوهش حاضر با یافته‌های *مونتیت* و همکاران (۲۰۲۱) و *الخاطر* و همکاران (۲۰۲۰) مطابقت و هم‌خوانی دارد. آنها در پژوهش خود نشان دادند که ناکارآمدی سامانه‌ها از جمله عواملی است که وقوع جرم در فضای مجازی را افزایش می‌دهد که در این پژوهش نیز به آن اشاره شده است. ضعف سیستم‌های ایمنی زمینه را برای جولان مجرمان در فضای مجازی بیشتر می‌کند و آنها آزادانه و با جسارت بیشتری به حریم خصوصی افراد تجاوز کرده و اقدام به فعالیت های مجرمانه می‌کنند. در پژوهش حاضر ضعف سیستم‌های ایمنی نیز به‌عنوان عاملی مهم در بروز جرم در فضای مجازی مطرح شد. در واقع مشارکت‌کنندگان معتقد بودند قصور و ضعف سیستم‌های ایمنی یکی از چالش‌هایی است که بسترساز جرم در فضای مجازی است. چرا که مجرمان به‌راحتی می‌توانند از چنگال قانون فرار کنند و هر روز تعداد بیشتری از افراد را طعمه قرار دهند. امکان جعل هویت و مخفی نگه‌داشتن آن، نیازهای احساسی، مالی و اطلاعاتی افراد نبود قوانین و مقررات مناسب و بازدارنده به ترتیب در یافته‌های *اوروواشی* (۲۰۱۰)، *لوکفلت* و *مالش* (۲۰۲۰) و *جابن* (۲۰۱۷)، به‌عنوان عوامل مؤثر در وقوع جرم در فضای مجازی به چشم می‌خورد که در پژوهش حاضر نیز عوامل فوق ذکر شده است. ضعف قوانین و مقررات و یا عدم تناسب جرم با مجازات خود دلیلی دیگری است که انگیزه مجرمان را برای اقدام‌های سودجویانه و غیراخلاقی بیشتر می‌کند. از طرفی امکان داشتن هویت پنهان و جعلی نیز نکته‌ای قابل بحث بود که مشارکت‌کنندگان در خصوص آن اظهار داشتند که این امر خود تسهیل‌گر جرم در فضای مجازی است.

پیشنهادهای کاربردی

- از آنجا که امروزه فضای مجازی محیطی برای انجام فعالیت‌های تجاری و اقتصادی است، پژوهش حاضر به مسئولان و نهادهای نظارتی پیشنهاد می‌کند به‌

منظور فراهم ساختن محیطی امن و سالم در فضای مجازی تلاش جدی و بی‌وقفه را برای مقابله با جرایم مجازی در دستور کار خود قرار دهند.

- زندگی دیجیتالی بخش جدایی‌ناپذیر دنیای کنونی را شکل می دهد. از این‌رو، با استناد به یافته‌ها پیشنهاد می‌شود تجهیز کاربران به داشتن دانش و مهارت استفاده از ابزارهای دیجیتالی به شدت احساس می‌شود. چرا که تقویت سواد دیجیتالی کاربران باعث می‌شود که در هنگام مواجه با فناوری‌های جدید مهارت استفاده از آن را داشته باشند و کمتر طعمه افراد سودجو در فضای مجازی قرار گیرند.
- یافته نشان می‌دهد که نبود قوانین و مقررات مناسب و بازدارنده یکی از مهمترین عوامل اثرگذار در وقوع جرایم فضای مجازی است. براین اساس پیشنهاد می‌شود که مسئولان و نهادهای مربوطه در مبارزه از وقوع جرم در فضای مجازی تا حد امکان قوانین و مقررات به‌روز و اثربخشی را تدوین نمایند.
- ناکارآمدی سیستم‌های ایمنی در وقوع جرم نیز یکی از عوامل مهم تلقی می‌شود که در این پژوهش بدان اشاره شده است. بنابراین، پیشنهاد می‌شود که با تجهیز سیستم‌های ایمنی به فناوری‌های روز و کارآمد جهت کاهش جرایم و رفتارهای انحرافی در فضای مجازی گام برداشت.
- به پژوهش‌گران آتی با توجه به اهمیت موضوع پیشنهاد می‌شود که عوامل علی، زمینه‌ای و مداخله‌گر را در راستای جرایم مجازی با کمک رویکرد داده بنیاد شناسایی کنند و یا با استفاده از رویکرد الگوهای ذهنی مدیران و مسئولان را در راستای علل وقوع جرم در فضای مجازی مورد تحلیل و بررسی قرار دهند.

سپاسگزاری

در پایان بر خود لازم می‌دانیم از تمامی مشارکت‌کنندگان که صبورانه در زمان مصاحبه ما را در انجام پژوهش یاری رساندند، صمیمانه تقدیر و تشکر نماییم.

منابع

۱. ارکانی، احسان؛ حاتمی‌نژاد، حسین؛ قره، حسین. (۱۳۹۹). شناسایی و اولویت‌بندی عوامل مؤثر بر افزایش ریسک زلزله در بافت‌های فرسوده شهری با رویکرد ترکیبی دلفی فازی و مدل BMW، *تحقیقات کاربردی علوم جغرافیایی*، ۲۰(۵۹)، ۲۹۱-۳۰۶.
https://jgs.khu.ac.ir/article-1-3763-fa.html

۲. بهره‌مند، حمید؛ کوره‌پز، حسین‌محمد؛ سلیمی، احسان. (۱۳۹۳). *راهبردهای وضعی پیشگیری از جرائم سایبری، آموزه های حقوق کیفری*، ۷(۲)، ۱۴۸-۱۷۶.
https://cld.razavi.ac.ir/article_770.html

۳. حیدری، مسعود؛ شهبازی، امید؛ شیرانی، پویا (۱۳۹۷). چالش‌ها و فرصت‌های پیش‌روی پلیس در برخورد با جرایم سایبری، *کارآگاه*، ۹۷ (۴۵)، ۴۱-۵۴.
http://det.jrl.police.ir/article_91542.html

۴. خانیکی، هادی؛ بابایی، محمود. (۱۳۹۰). *فضای سایبر و شبکه‌های اجتماعی مفهوم و کارکردها، مطالعات جامعه اطلاعاتی*، ۱(۱)، ۷۱-۹۴
https://irandoc.ac.ir/sites/fa/files/attach/article/829-2541-1-pb.

۵. زلقی، علی. (۱۳۹۹). خلاهای قانونی و اجرایی و راهکارهای پیشگیری از ارتکاب جرایم سایبری، *فصلنامه کارآگاه*، ۱۳(۵۲)، ۸۲-۹۲.
http://det.jrl.police.ir/article_95427.html

۶. زلقی، علی؛ مالمیر، محمود. (۱۳۹۹). *نقش ضابطان قضایی در پیشگیری و کنترل جرایم فضای سایبری در حقوق ایران و انگلستان*، حقوق پزشکی، ۹۳-۱۰۶.
http://ijmedicallaw.ir/article-1-1229-fa.html

۷. محسنی، فرید؛ صوفی زمرد، محسن. (۱۳۹۶). پلیس و چالش‌های اجرایی تأمین امنیت سایبری، *پژوهش‌های دانش انتظامی*، ۲۰(۴)، ۱۶۴-۱۸۸.
http://journals.police.ir/article_18918.html

۸. محسنی، فرید (۱۳۹۴). *حریم خصوصی اطلاعات؛ مطالعه کیفری در حقوق ایران، ایالات متحده آمریکا و فقه امامیه*، انتشارات دانشگاه امام صادق(ع)، تهران، ایران.

9. Alazab, M., & Broadhurst, R. (2015). The role of spam in cybercrime: Data from the Australian cybercrime pilot observatory. *Cybercrime Risks and Responses*, 103- 120. DOI: 10.1057/9781137474162_7

10. Alghamdi, M (2020). A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide, International *Journal of Engineering Research & Technology*, 9(6), 1-12.
11. Ambika, T & Senthilvel, C (2020). Cyber Crimes against the State*: A Study on Cyber Terrorism in India*, *Neuro Quantology Journal*, 17(2), 65-72. DOI: 10.14704/WEB/V17I2/WEB17016
12. Benard, M., Charles, M., Charo, J & Mvurya, M (2021). Cyber-Crimes Issues on Social Media Usage Among Higher Learning Institutions Students in Dar ES Salaam Region, Tanzania, *International Journal of Scientific Research in Science Engineering and Technology*, 138-148. DOI : 10.32628/IJSRSET218418
13. Chandra, M (2019). Reduction of Cyber Crimes by Effective Use of Artificial Intelligence Techniques, *International Journal of Recent Technology and Engineering (IJRTE)*, 8(4), 8643- 8648. DOI:10.35940/ijrte.D8566.118419
14. Dilek, S., Cakır, H & Aydın, M (2015)۷ Appli To Combating Cyber Crimes: A Review, *International Journal of Artificial Intelligence & Application*, 6(1), 21-42. DOI : 10.5121/ijaia.2015.6102
15. Dubey, S (2021). Cyber Crimes and Cyber Laws : A Perspective of Women Victimization, *International Journal of Advanced Research in Science, Communication and Technology*, 643-647. http://dx.doi.org/10.48175/ijarsct-1443
16. Eian, Ch., Yong, L., Li, M., Qi, Y & Zahra, F (2020). Cyber Attacks in the Era of Covid-19 and Possible Solution Domains, *Preprints*, 1-15. doi: 10.20944/preprints202009.0630.v1
17. Ganta, S & Kumar, P (2019). Awareness of Netizens on Cyber Crimes An Empirical Examination in Andhra Pradesh, *International Journal of Recent Technology and Engineering*, 8(3), 461-465. DOI: 10.35940/ijrte.C1095.1083S19
18. Jain, M (2017). *Victimization OF Women Beneath Eneath Cyberspace in Indian Upbringing*, Bharati Law Review,1-11. http://docs.manupatra.in/newsline/articles/Upload/786274E9-B397-4610-8912-28D6.

19. Graham, N (2018). *Cyber crimes against women in India: Informa UK Limited*, 24(3), 413-417. http://dx.doi.org/10.1080/12259276.2018.1496783
20. Keith, A & Jamil, J (2018). Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition, Georgetown, *Journal of International Affairs*, 19, 1-14. https://www.jstor.org/stable/26567527
21. Kharat, Sh (2017). *Cyber Crime, A Threat to Persons, Property, Government and Societies*, SSRN, 1-14. http://dx.doi.org/10.2139/ssrn.2913438
22. Leukfeldt, E & Malsch, N (2020). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes, *An International Journal of Evidence-based Research, Policy, and Practice*, 15(1), 60-77. https://doi.org/10.1080/15564886.2019.1672229
23. Mbanaso, U & Dandaura, E (2015). The Cyberspace: Redefining A New World, *Journal of Computer Engineering*, 17(3), 17-24. DOI : 10.5121/ijaia.2015.6102
24. Medeiros, B & Goldoni, L (2020). *The Fundamental Conceptual Trinity of Cyberspace,* Contexto Internacional, 42(1), 31-56. DOI:10.1590/s0102-8529.2019420100002
25. Mohsin, K (2020). Global Perspective of Cyber Crimes and Related Laws, *SSRN Electronic Journal*, 14(2), 1-10. http://dx.doi.org/10.2139/ssrn.3673938
26. Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P & Glenn, T (2021). *Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry, Psychiatry in The Digital Age* (J Shore, Section Editor), 18, 1-9. https://link.springer.com/article/10.1007/s11920-021-01228-w
27. Moynihan, H (2020). The vital role of international law in the framework for responsible state behaviour in cyberspace, *Journal of Cyber Policy*, 13(2), 69-83. http://dx.doi.org/10.1080/23738871.2020.1832550
28. Nappinai, N.S (2010). Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study, *Journal of International Commercial Law and Technology*,5(1), 22-30.

https://media.neliti.com/media/publications/28731-EN-cyber-crime-law-in-india.

29. Pathak, Ph, Saraswat, S & Yadav, R (2020). Cyber Space Crimes and IT Laws in opposition of Cyber Offence, *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, 1-15. DOI:10.32628/CSEIT2062156
30. Richardson, S & Gilmour, N (2015). Cyber Crime and National Security: A New Zealand Perspective, *The European Review of Organised Crime*, 2(2), 51-70. https://sgocnet.org.
31. Shaikh, A (2019). Cyber Crimes and the Legal Implications on the Social Networking Websites, *International Cooperation Public/Private Cooperation*, 1-22. http://dx.doi.org/10.2139/ssrn.3563245
32. Teunissen, C., Voce, I & Smith, R (2021). Estimating the cost of pure cyber crime to Australian individuals, Australian Institute of Criminology, 34, 1-15. https://www.aic.gov.au/sites/default/files/202107/sb34_estimating_the_cost_of_pure_cybercrime_to_australian_individuals.
33. Yan, L (2020). *The New Trend US' Strengthening Dominance in Cyberspace*, Contemporary International Relations, 30(6), 68-80. http://www.cicir.ac.cn/UpFiles/file/20210208/6374837418282568688886075
34. Yangaeva, M.O (2021). *Social engineering as a way of committing cyber crimes*, Siberian Law Institute of the MIA of Russia, 4(1), 133-138. http://dx.doi.org/10.51980/2542-1735_2021_1_133