فصلنامه علوم خبری
سال دهم، شماره ۳۹ پاییز ۱۴۰۰
صفحات ۱۶۰-۱۳۵

La revue science de I'information
année 10 / No 39 Tomber 2021
pages: 135-160

واکاوی وب سیاه در فضای مجازی ایران

محمدرضا رسولی[۱]
ساجده ظهیری[۲]

چکیده

از زمانی که جرائم تنها به صورت رو در رو و عیان رخ می‌دادند و در صورت نیاز به ارتباطات میان مجرمان تنها باید از راه‌های سنتی و قابل پیش بینی اقدام می‌کردند، مدت زمان زیادی نگذشته است. امروزه ارتباطات اینترنتی، علی الخصوص وب سیاه که قابل د ستر سی برای کاربران عادی نیست این ارتباطات را ساده کرده ا ست. این تحقیق با هدف واکاوی وب سیاه در فضای مجازی ایران صورت گرفته است. ازنظر دسته‌بندی تحقیقات برحسب هدف یک تحقیق کاربردی می‌باشد، ازنظر نحوه گردآوری داده‌ها توصیفی-غیرآزمایشی است و در میان انواع روش‌های تحقیق توصیفی در زمره مطالعه موردی قرار گرفته است. جامعه آماری تحقیق برای پرسشنامه تعداد ۱۰ نفر از خبرگان برای پرسشنامه‌ها را شامل شده ا ست که پر سش‌نامه خبرگان در میان آن‌ها پخش شد. بر ا ساس مطالعات صورت گرفته معیارهای اصلی تحقیق شامل دانش، محیط، مردم، فرایند، تجهیزات و زیرساخت‌ها و مدیریت می‌باشد. تجزیه‌وتحلیل داده‌ها با استفاده از رویکرد ANP-DEMATEL صورت گرفته است. بر اساس نتایج تحقیق اثبات شد، معیار " کلاه برداری" با وزن نهائی ۰,۵۱۴ در اولویت اول میان معیارها و تأثیرپذیرترین معیار، زیرمعیار "وجود بازارهای مواد مخدر رمزگذاری شده" با وزن نهائی ۰,۱۰۱۱ در اولویت اول میان زیرمعیارها و "مواد مخدر" بیشترین تأثیرگذاری و تعامل را در میان معیارها داشته است.

واژگان کلیدی: وب سیاه، فضای مجازی، قاچاق، مواد مخدر، رویکرد MCDM

---

[۱] دانشیار گروه علوم ارتباطات و مطالعات رسانه، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده مسئول). rasouli@yahoo.com

[۲] کارشناسی ارشد گروه علوم ارتباطات اجتماعی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. Sazahiri@yahoo.com

تاریخ دریافت: ۱۴۰۰/۰۴/۲۶ تاریخ پذیرش:۱۴۰۰/۰۶/۰۵

مقدمه

در سال‌های اخیر، اینترنت به یک پدیده وسیع جهانی مبدل گشته است. امروزه، تکنولوژی مردم را از سرتا سر جهان به گونه‌ای به همدیگر متصل می‌کند که قبلاً امکان‌پذیر نبود (کتانچی و پورقهرمانی، ۱۳۹۸). اینترنت مجموعه‌ای از شبکه‌های بسیاری است که از اتصال رایانه‌ها، سرورها و یا هر دستگاه دیگری به یکدیگر ایجاد شده و یک شبکه مستقل را تشکیل می‌دهد. اتصال شبکه‌ها در اینترنت از طریق شبکه گسترده جهانی صورت می‌گیرد و به دو بخش وب سطحی با آشکار و وب عمیق با پنهان تقسیم می‌شود (چرتف[3] ۲۰۱۷). وب سطحی بخش کوچکی از اینترنت (در معنای عام) را تشکیل می-دهد که در آن محتوای سایت‌ها به راحتی توسط موتورهای جستجو مانند گوگل، یاهو و.. فهرست می شود و دسترسی به آنها توسط مرورگرهای استاندارد صورت می‌گیرد، در حالی که محتوای وب پنهان که ۹۰ درصد حجم انتقال و ترافیک داده‌ها را به خود اختصاص می‌دهد توسط موتورهای جستجو قابل طبقه‌بندی محتوایی و موضوعی نیست (گرینبرگ[4] ۲۰۱۴). فضای مجازی شامل دو قسمت آشکار و پنهان است، اینترنت آشکار از موتورهای جستجوی بزرگ چون یاهو و گوگل در دسترس می‌باشند، اینترنت پنهان شامل اینترنت عمیق است که تخمین زده می‌شود حدود ۹۶ درصد از WWW را تشکیل دهد. انجام تبادلات تجاری غیرقانونی، اصلی‌ترین دلیل شکل‌گیری اینترنت عمیق است و دسترسی به آن به سادگی انجام نمی‌گیرد (نزاه و همکاران[5] ۲۰۲۰). در اینترنت عمیق زیرمجموعه‌ای که بیشتر برای اهداف غیرقانونی استفاده می شود وب سیاه یا نت سیاه است (لکومی[6] ۲۰۱۷).

درون وب پنهان، یک فضای مخفی شده به نام وب تاریک وجود دارد، که از طریق روش‌های استاندارد مرور وب، قابل دسترس نیست. این فضا که بر مبنای شبکه مسیریابی پیازی توسعه یافته، متشکل از وب سایت‌های است که برای عموم قابل

[3] Chertoff
[4] Greenberg
[5] Nazah et al.
[6] Lakomy

مشـــاهده اســـت اما آدرس آی پی آنها مخفی و پنهان می‌باشـــد. کاربران به کمک موتورهای جستجوی معمول نخواهند توانست این سایت‌ها را جستجو و پیدا کنند، بلکه با نرم افزارهای خاص، تنظیمات ویژه و یا حتی در برخی موارد تنها با داشـــتن نشـــانی وب که عموماً از پروتکل‌های عادی تبعیت نمی‌کند، می‌توانند به این وب سایت‌ها دسترسی داشته باشند (قناد و اسلامیان کوپایی، ۱۳۹۹). استفاده از وب سیاه در اکثر مواقع با اهداف غیرقانونی صورت می‌گیرد که برخی از این اهداف شامل جعل اســـناد، قتل، فروش مواد مخدر، خرید و فروش مواد منفجره و ســـلاح، ســـرقت هویت و پول‌های تقلبی می‌باشد (کاوالیروس و همکاران[۷] ۲۰۲۱). برای تشکیل باندها و شـــبکه‌های قاچاق بین‌المللی مواد مخدر و روانگردان‌ها اســـتفاده می‌شـــود. شـــاید مهم‌ترین بعد وب ســـیاه این مورد باشـــد که مجرمان موادمخدر و روانگردان‌ها در استفاده از این کارکرد، بر اعمال مجرمانهٔ خود سایه انداخته و از تیررس مبارزان این تجارت در امان می‌مانند؛ چراکه دســـترســـی به اطلاعات این افراد که از طریق کارکردهای وب ســـیاه به تجارت خود می‌پردازند، عملی غیرممکن تلقی می‌شـــود (قربانی، ۱۳۹۸). در واقع اینترنت و شبکه گسترده وب جهانی بسیار بزرگتر از چیزی اســـت، که از طریق مرور منظم مشـــاهده می‌شـــود. اینترنت و کاربران آن به دلیل کاربردهای نوظهور فناوری اطلاعات (IT) به سرعت در حال رشد بوده و انتظار می‌رود این روند همچنان ادامه یابد. با این حال، رشد سریع اینترنت، سوء استفاده را مستعد کرده و فضای مجازی در سراسر جهان را با تهدید و چالش مهمی مواجه نموده است. شـــمار زیادی از مجرمان ســـایبری ســـعی می‌کنند هر روز اقدامات غیرقانونی برای دســـتیابی به داده‌های غیرمجاز از طریق اینترنت انجام دهند. اکثر کاربران اینترنت از طریق مرورگرهای عادی مانندInternet Explorer، Firefox،Chrome به شبکه اینترنت دسترسی پیدا می‌کنند، به آن قسمت از وب که توسط یک مرورگر عادی قابل دسترسی می‌باشد، سطح وب گفته می‌شود. با این حال، بخش بزرگی از مطالب در وب عمیق پنهان مانده‌اســـت. به عبارتی موتورهای جســـتجوگر مدرن فقط بخش بسیار کمی از وب را فهرست می‌کنند و مقدار زیادی از مطالب وب همان‌طور که در

۷Kavallieros et al.

وب عمیق پنهان می‌شوند. اصطلاح وب تاریک بخشی از وب عمیق است که مورد هدف اکثر مجرمان سایبری قرار گرفته است و آنها در داخل سایت‌های تاریک وب، فعالیت‌های جنایی انجام می‌دهند (داکنها و همکاران[8]، ۲۰۲۰). به‌رغم تفاوت‌های موجود در رویکرد این پژوهش‌ها، محور اصلی همهٔ آنها یافتن راهکارهایی عملی برای ارتقای سطح دسترس پذیری اطلاعات در این شبکه و سهولت بازیابی است (پرفکت و همکاران[9]، ۲۰۱۹).

از آنجا که به دلیل گستردگی بی‌وقفهٔ اطلاعات موجود در شبکهٔ جهان‌گستر وب هرگونه برآوردی حتی نسبی از حد و مرز این محیط خیلی زود کهنه و قدیمی می‌شود، این رقم می‌تواند بیشتر یا کمتر از ۲۰ درصد باشد. آنچه که در اینجا بیش از صحت یا نادرستی این رقم اهمیت دارد، واقعیتی است که هم اکنون در وب به وجود آمده و حجم عظیمی از اطلاعات را برای کاربران، دسترس ناپذیر ساخته است (یو و همکاران[10]، ۲۰۱۹).

منابع اطلاعاتی متنوعی در وب وجود دارند که تنها به دلیل محدودیت تکنولوژیکی یا مالی موتورهای جستجو، از حوزهٔ کاوش آنها و درنتیجه از دسترسی کاربران دور مانده‌اند (هاتا[11]، ۲۰۲۰). براساس تخمین‌های صورت گرفته، شبکه تاریک وب تقریباً ۵۰۰ برابر بزرگتر از شبکه جهانی وبی است که کاربران به صورت روزانه از آن بهره می‌برند و همچنین این شبکه تقریبا به‌طور کامل مخفی می‌باشد (گودمن[12]، ۲۰۱۶). مطابق گزارش مرکز مبارزه با جرایم سایبری استرالیا، اصطلاح جرایم سایبری به جرایمی مربوط می شود که به رایانه‌ها یا دستگاه‌های دیگر هدایت می‌شوند و در آنجا رایانه‌ها یا سایر دستگاه‌ها برای جرائم ضروری هستند. این تعریف به‌طور گسترده انواع فعالیت‌های انجام شده توسط مجرمان سایبری را تعریف می‌کند که عملیات آنها یا با توسعه و به کارگیری اشکال مختلف نرم افزارهای مخرب (مانند

8 da Cunha et al.
9 Perfect et al.
10 Yu et al.
11 Hatta
12 Goodman

ویروس) شبکه‌های رایانه‌ای خاص را هدف قرار داده و یا از این شبکه‌ها برای پیشبرد برنامه‌های جنایی خود (فیشینگ، سرقت هویت، کلاهبرداری، استخدام و غیره) بهره‌برداری می‌کنند (اسلام و اوزکایا[۱۳] ۲۰۱۹).

همچنین در دارک وب فروشگاه‌های خاصی در حال فعالیت هستند که اصطلاحاً فروشگاه‌های دارک نت نامیده می‌شوند که عمده محصولات این فروشگاه‌ها مواد مخدر، سلاح‌های گرم، اعضای بدن انسان و... می‌باشد و پرداخت‌ها در فروشگاه های فوق معمولاً از طریق پول مجازی (مثل بیت کوین) انجام می‌گیرد (حسین آبادی و حسنی، ۱۳۹۹). در واقع دارک وب یک محیط اینترنتی امن برای خلافکاران می‌با شد کد از طریق آن می‌توانند به گسترش شبکه‌های غیرقانونی خود پرداخته و به نوعی به پول بیشتر دست یابند و فروشگاه‌های دارک وب دقیقا همانند فرو شگاه‌های معمول در وب می‌با شند و به همان شیوه اداره می شوند، منتها در این فرو شگاه‌ها معمولا موارد غیر قانونی فروخته می شود (مقدمی ا صل، ۱۳۹۶). کاربران وب تاریک کسانی هستند که به دنبال انتقال و دریافت اطلاعات هستند، به گونه‌ای که احتمال آ شکار سازی و شنا سایی آن فعالیت‌ها، بسیار کم با شد. امروزه بزهکاران می‌توانند بر بی نام و نشان بودن فضای وب تاریک تکیه کنند و از این خدمات برای مراقبت و پایش تحت وب استفاده کنند و از آن طریق به عملیات‌های مد نظر خود بپردازند. بنابراین، عدم قابلیت رهگیری عملکرد در وب تاریک، می تواند به عنوان یک پو شش در برابر تشخیص مجرمان و سوداگران مجازی مورد ا ستفادهٔ آنها قرار بگیرد (جواهری، ۱۳۹۵). فعالیت‌های جنایی متعددی در شبکه‌های عمیق در حال انجام ا ست از جمله می‌توان به معامله با مواد مخدر (خرید و فروش)، قرارداد ترور، صنعت پورنوگرافی از جمله پورنوگرافی کودکان، فروش اعضای بدن انسان، قاچاق انسان و قاچاق برده‌های جنسی، معاملات حمل غیرقانونی اسلحه، فروش انواع مواد مخدر، کالاهای به سرقت رفته، فروش اطلاعات هویتی سایبری هک شده، فعالیت‌های تروریستی و موارد دیگر اشاره کرد (امورس و پاگانینی[۱۴] ۲۰۱۴). جرایم ارتکابی در

13. Islam & Ozkaya
14. Amores & Paganini

وب تاریک یکی از مهم‌ترین و در عین حال پیچیده‌ترین نوع جرایم در اقصـــی نقاط جهان می‌باشـــد، که عمدتاً با هدف تحصـــیل منافع مادی و مالی و در برخی موارد با اهداف ایدئولوژیک، ســـیاســـی و کســـب قدرت به وقوع می‌پیوندد. این گونه جرایم را می‌توان منسجم‌ترین و قوی‌ترین ساختار باندهای مجرمانه تلقی نمود (پور اسمعلی و همکاران، ۱۳۹۵) که این مســـأله می‌تواند اهمیت توجه به شـــبکه‌های وب تاریک را نمایان سازد. از طرفی رشد فعالیت‌ها و اقدامات مجرمانه گروه‌های سازمان یافته در بستر وب عمیق و دارک وب، تبعات سوء و اثرات منفی بر امنیت عمومی، اقتصادی، فرهنگی و اجتماعی کشور درپی دارد، امروزه مسئله وب تاریک و جرایم مرتبط با آن به یک معضل اساسی برای بسیاری از کشورهای جهان تبدیل شده است. خصوصیات و ویژگی‌های خاص این جرایم موجب می‌شود که هیچ کشوری نتواند خود را از تبعات و آثار سوء آن مصون بداند از طرفی تأثیر این بستر در افزایش ارتکاب سایر جرایم مانند قتل و مواد مخدر بسیار زیاد می‌باشد. لذا با توجه به اهمیت موضوع فوق، این تحقیق به دنبال شـــناســـایی و رتبه بندی تهدیدات وب تاریک با اســـتفاده از تکنیک تصمیم‌گیری چندمعیاره می‌باشد. با این تفاسیر با توجه به اهمیت تهدیدات وب سیاه در فضـــای مجازی ایران و تأثیرگذاری آن بر جرائم موجود در جامعه، در این مقاله به شناسایی و اولویت‌بندی تهدیدات موجود در وب تاریک پرداخته خواهد شد. بر این اساس پیش از این نیز تحقیقاتی در این زمینه انجام دادند.

رحمان زاده و همکاران (۱۴۰۰) به این نتیجه رسیدند که فضای مجازی مانند فضای واقعی نیازمند فرهنگ است. ضروری است به این فناوری با نگاه فرصت‌سازی نگریســـت و علاوه بر آموزش‌های لازم به کاربران برای ورود به فضـــای شـــبکه تاریک، سیاست‌های فرهنگی جامعه برای استفاده صحیح از آن را تطبیق داده تا کمتر شاهد آســـیب‌پذیری در این زمینه باشـــیم. حســـین آبادی و حســـنی (۱۳۹۹)، با رویکرد کاربردی و روش کیفی و با بهره‌گیری از ابزارهایی مانند مطالعات اســـنادی، کتابخانه‌ای و بررسی سوابق، بررسی تحلیلی اخبار، مصاحبه با خبرگان و تحلیل محتوا سعی گردیده تا ابتدا تعاریف کلی از اصطلاحات تخصصی و پرکاربرد، چگونگی شکل‌گیری دارک وب و خصوصیات آن ارائه گردد و سپس به انواع جرایم ارتکابی

در بستر وب تاریک، بازارها و سایت‌های معروف در این بستر، کالاها و خدمات غیرقانونی و مجرمانه ارائه شده در این حوزه و تکنیک‌هایی برای یافتن مجرمان در وب عمیق، پرداخته شده است. قناد و اسلامیان کوپایی (۱۳۹۹)، سعی گردید ضمن تبیین و توصیف فضای کلی حاکم بر وب تاریک، چگونگی ساختاربندی و جریان سازی فعالیت مردم تا ساماندهی نظام‌مند تحت نظارت دولت‌ها مورد بررسی قرار گیرد تا در نهایت از طریق مدل مسیریابی پیازی (تُر) به ارائه راهکارها و وضع سیاست‌های مؤثر که مقدمه‌ای بر افزایش آگاهی و بهبود عملکردهاست پرداخته شود. قربانی (۱۳۹۸)، نشان داد که با توجه به عملکرد وب تاریک، فضای سایبری نقش مؤثری در گسترش جرائم مواد مخدر و روان گردان‌ها داشته است که لازم است مدیریت فضای سایبر دستخوش تغییرات اساسی شود. فتاحی (۱۳۹۷)، در تحقیق خود قانون جرایم رایانه ای مصوب ۱۳۸۸ را توضیح داد که به این نکته اشاره کرد که این مجموعه قوانین یکی از کامل‌ترین قوانین در زمینه جرایم مربوط به فضای مجازی و رایانه‌ای می باشد. کرد علیوند و میرزایی (۱۳۹۷)، به این نتیجه رسیدند که بزهکاری سایبری از پویایی خیره کننده‌ای برخوردار است. رفتارهای مجرمانه در این نوع بزهکاری متنوع و پویا هستند؛ برخی ازآنها کاملاً نو و برخی دیگر همان جرایم متداولی هستند که در بستر سامانه و شبکه‌های اطلاعاتی به شکلی دیگر ارتکاب پیدا می کنند. در گونه شناسی جرایم سایبری از معیارهای مختلفی چون نقش سامانه و شبکه‌های اطلاعاتی در پیدایش و گسترش جرایم (به عنوان پشتوانه و یا وسیله ارتکاب جرم)، موضوع و محتوای جرایم سایبری و یا تلفیقی از این معیارها استفاده می شود.

کاوالیروس و همکاران[۵](۲۰۲۱)، بیان کردند با فعالیت های تاریک و جنایتکارانه‌ای که در وب اتفاق می‌افتد مرتبط است. با این حال، کاوش در بخش مجرمانه‌ی آن مانند کاوش در فعالیت‌های مجرمانه یک شهر یا جامعه به لحاظ تجاری، فرهنگی، اجتماعی و سایر جنبه‌ها حائز اهمیت است لذا ایشان در مطالعات خود به بررسی کاربردهای اینترنت سیاه و علل و انگیزه‌ی استفاده کنندگان از آن

۵. Kavallieros et al.

پرداختند. چیلدز و همکاران[۱۶](۲۰۲۱)، به این نتیجه رسیدند که بازیگران از طریق نرمال سازی گسترده‌تر جامعه در استفاده / تأمین شاهدانه، اتخاذ برنامه‌های پیام رمزگذاری شده رمزگذاری شده برای پوشاندن "ردیابی‌های دیجیتالی" و ایجاد روش‌های مختلف برای ایجاد اعتماد با شریک مبادله، خطرات ادراکی موجود در این بستر وب سطحی را خنثی می‌کنند و آنها با جلب توجه به بازارهای رمزنگاری وب سیاه به صورت سطحی، وب شفاف، درک از تعداد روزافزون بازارهای مواد مخدر غیرقانونی را گسترش می‌دهد. آنها پیامدهای نظری برای مطالعه اعتماد و خطر در مبادلات آنلاین دارو های غیر قانونی آنلاین نیز در نظر گرفتند. نزاه و همکاران[۱۷] (۲۰۲۰)، در مقاله خود جنایات وب تاریک، پیامدهای آن و و راه حل‌های بالقوه را با استفاده از مرور ادبیات تجزیه و تحلیل و جمع‌آوری نمودند و تهدیدات وب تاریک را به چهار دسته قاچاق، مواد مخدر، کلاه برداری و تروریست تقسیم‌بندی کردند و روش‌های اجباری و همچنین مانورهای آینده برای کاهش تهدیدات جنایی ارزیابی کردند. آن‌ها از روش بررسی منظم ادبیات (SLR) جهت ارائه جهت و جنبه تهدیدات جنایی در حال ظهور در وب تاریک برای محققان و متخصصان در زمینه امنیت سایبری استفاده کردند. ژانگ و چو[۱۸](۲۰۲۰)، دریافتند که یکی از تهدیدات این فضا، کاربرد آن برای دسترسی ناشناس به خدمات پنهان و غیر قانونی اینترنتی از قبیل کیف پولBitCoin، اطلاعات ایمیل کاربران دیگر، تصاویر خصوصی و ... است که مأموران اجرای قانون را برای ردیابی هویت مجرمان اینترنتی با مشکل روبه‌رو می‌کند. نهایتاً از اطلاعات به دست آمده در تحقیقات ایشان به منظور ارائه‌ی چارچوبی در خصوص شناسایی تهدیدات فضای وب تاریک به منظور کمک به تجزیه و تحلیل جنایات و رفتار جنایتکاران در وب تاریک استفاده گردید.

در این تحقیق تهدیدات وب تاریک را بر اساس مدل و معیارهای نزاه و همکاران (۲۰۲۰) مورد بررسی قرار داده، بنابراین معیارهای تحقیق شامل چهار معیار قاچاق، کلاه برداری، مواد مخدر و تروریست می‌باشد.

16 Childs et al.
17 Nazah et al.
18 Zhang & Chow

شکل ۱- مدل مفهومی تحقیق، منبع. (نزاه و همکاران[۱۹] ۲۰۲۱)

پژوهش حاضر به دنبال پاسخ به سؤالات زیر است:

۱. معیارها و تهدیدات اصلی وب تاریک کدامند؟
۲. زیرمعیارهای هر معیار و خرده تهدیدات موجود در وب تاریک کدامند؟
۳. روابط درونی میان معیارهای وب تاریک به چه صورت بوده و این تهدیدات تا چه میزان بر هم تأثیر دارند؟
۴. رتبه بندی تهدیدات موجود در وب تاریک به چه صورت است؟

روش

پژوهش حاضر بر حسب نوع روش، توصیفی- تحلیلی و از لحاظ نوع هدف، کاربردی است. روش گردآوری اطلاعات مبتنی بر روشهای اسنادی (کتابخانه‌ای)، مشاهده (مطالعات میدانی) و مستندسازی می‌باشد. در بخش تحلیل، از تکنیک

[۱۹] Nazah et al.

تلفیقی DELPHI-ANP-DEMATEL برای ارزیابی استفاده شده است. در این راستا، ابتدا یک مدل سه سطحی از هدف، معیارها، زیر معیارها ارائه گردید. لازم به ذکر است جهت تعیین معیارها و زیر معیارهای موجود در مدل، از مطالعات اسنادی و کتابخانه‌ای استفاده شده است.

جدول ۱- معیارها و زیرمعیارهای تحقیق

معیار	زیرمعیار	منبع
قاچاق	قاچاق داروهای خاص	نزاه و همکاران (۲۰۲۰)، چریستین و همکاران[20] (۲۰۱۳)
	قاچاق سلاح	
	قاچاق جواهرات	
	اجناس مسروقه	
کلاه برداری	تبانی با سیاست مداران و پلیسان فاسد	نزاه و همکاران (۲۰۲۰)، دیلی[21] (۲۰۱۳)
	دسترسی و سرقت اطلاعات طبقه بندی شده	نزاه و همکاران (۲۰۲۰)، گنوا[22] (۲۰۱۷)
	تجارت خدمات مخفی	نزاه و همکاران (۲۰۲۰)، مور و رید[23] (۲۰۱۶)
	معاملات غیر قابل ردیابی	نزاه و همکاران (۲۰۲۰)، لین[24] (۲۰۱۳)
	تبادل بیت کوین	بک من[25] (۲۰۱۳)
	پولشویی	فنوسه و رابینسون[26] (۲۰۱۸)
مواد مخدر	سیگار در بازار سیاه	

20 Christin et al.
21 Daily
22 Geneva
23 Moore & Rid
24 Lane
25 Backman
26 Fanusie & Robinson

معیار	زیرمعیار	منبع
	تجارت مواد مخدر با در نظر داشتن ناشناس بودن	نزاه و همکاران (۲۰۲۰)، آلدریج و همکاران[۲۷] (۲۰۱۶)، بارات و همکاران[۲۸] (۲۰۱۶)، مدوکس و همکاران[۲۹] (۲۰۱۶)، آلدریج و همکاران[۳۰] (۲۰۱۴)، تسیکردکیس و همکاران[۳۱] (۲۰۱۴)
	وجود بازارهای مواد مخدر رمز گذاری شده	
تروریست	تبلیغات و گسترش انگیزه‌های منفی گروه‌های تروریستی	نزاه و همکاران (۲۰۲۰)، لایتفوت و پسپیسیل[۳۲] (۲۰۱۷)، بتس[۳۳] (۲۰۱۶)، ویمن[۳۴] (۲۰۱۶)، میناس[۳۵] (۲۰۱۲)، ژنگ و همکاران[۳۶] (۲۰۱۴)، ژو و همکاران[۳۷] (۲۰۰۶)
	استخدام و جذب نیرو	
	آموزش	
	تغییر فرماندهی و ابلاغ دستورات و نقشه‌ها	
	درخواست پول برای کمک و حمایت	نزاه و همکاران (۲۰۲۰)، توکر[۳۸] (۲۰۱۵)
	انتقال اطلاعات و ارتباطات	
	استخدام جنایتکاران	نزاه و همکاران (۲۰۲۰)، چرتف و همکاران[۳۹] (۲۰۱۵)

27 Aldridge et al.
28 Barratt et al.
29 Maddox et al.
30 Aldridge et al.
31 Tsikerdekis et al.
32 Lightfoot and Pospisil
33 Bates
34 Weimann
35 Mainas
36 Zheng et al.
37 Xu et al,
38 Tucker
39 Chertoff et al.

بر این اساس با مرور عمیق مطالعات پیشین معیارها و زیرمعیارهای جدول ۱ استخراج گردید، که زیرمعیارهای تبادل بیت کوین با نظر خبرگان حذف شد، زیرمعیارهایی چون قاچاق انسان، فروش اعضای بدن، خرید و فروش تجهیزات غیرمجاز نظیر گنج یاب، سانتریفیوژهای دور بالا، موتورهای دوربالا و ...، خرید و فروشی اطلاعات دولتی محرمانه سری، جرایم جنسی، برقراری گروه‌های جدائی طلبانه و برنامه‌ریزی انقلاب‌های رنگی با استفاده از نظر خبرگان اضافه شدند و آموزش با نظر خبرگان تبدیل به آموزش نیروهای گروه‌های تروریستی شد.

سپس به منظور انجام مقایسات زوجی و تعیین وابستگی‌های بین معیارها و زیرمعیارها، پرسشنامه‌های طراحی شده کارشناسان فضای مجازی توزیع گشت. با اشاره به این نکته که تعداد خبرگان به عنوان مصاحبه شونده نباید زیاد باشد در کل ۵ الی ۱۵ نفر را پیشنهاد می‌کنند (سرافرازی و همکاران، ۱۳۹۳). در نتیجه تعداد ۱۰ نفر از کارشناسان فضای مجازی به عنوان نمونه مورد بررسی استفاده شده‌اند. در ادامه جهت تحلیل داده‌ها (اطلاعات به دست آمده از پرسش نامه‌ها) و اولویت بندی معیارها و زیرمعیارها، از نرم افزار Super Decisions استفاده شده است.

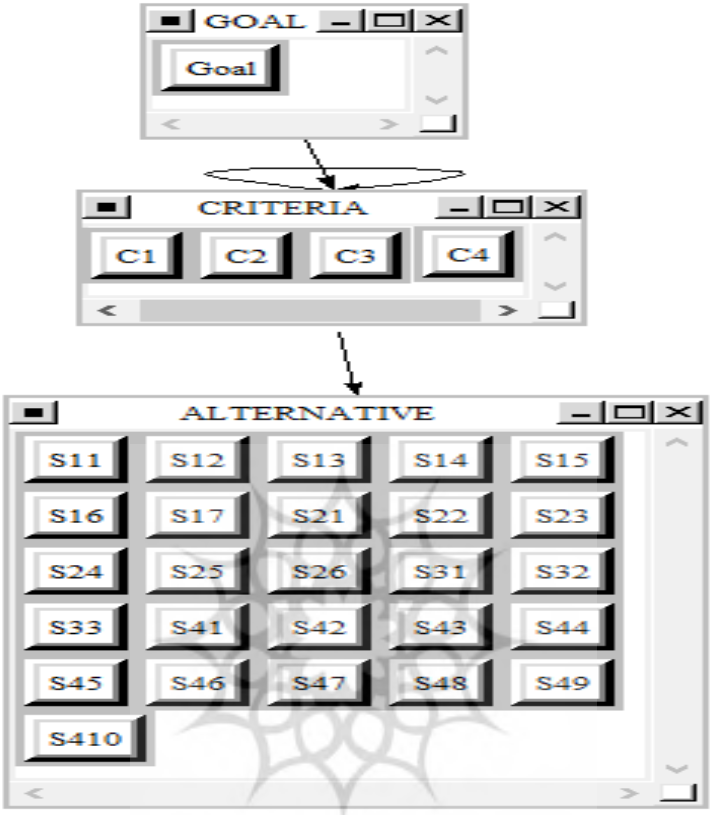
با عنایت بر مطالب گفته شده، به دنبال پاسخ به این هدف که چه زیرمعیارهایی مرتبط با اهداف واکاوی وب سیاه در فضای مجازی ایران بر اساس نظر خبرگان با استفاده از روش DEMATEL- ANP پرداخته است. فرایند تحلیل شبکه‌ای، چارچوبی اجرایی برای تحلیل‌های عمومی و همکاری در تصمیم گیری‌ها ارایه می‌نماید (توزکایا و همکاران[40]، ۲۰۰۸). همچنین برای بررسی روابط درونی از تکنیک دیمتل استفاده شده است. در این تحقیق تکنیک دیمتل به‌عنوان زیر سیستمی از سیستم بزرگتری چون ANP برای تعیین جهت روابط درونی میان معیارها است. مراحل تکنیک دیمتل شامل تشکیل ماتریس ارتباط مستقیم (M)، نرمال کردن ماتریس ارتباط مستقیم، محاسبه ماتریس ارتباط کامل و ایجاد نمودار علی می‌باشد (سرافرازی و همکاران، ۱۳۹۳).

40 Uzkaya & Önüt

روایی پرسشنامه تحقیق با استفاده از تکنیک دلفی و پایایی آن با محاسبه نرخ ناسازگاری محاسبه شد.

یافته‌ها

در این مرحله اول معیارها و زیرمعیارهای اهداف واکاوی وب سیاه در فضای مجازی ایران با مطالعه ی مبانی نظری و بررسی سوابق موضوع، تعیین و میان هر یک از این عوامل توسط گروهی از متخصصین مشخص شد. مدل شبکه‌ای این پژوهش که یک مدل به شرح شکل ۱ می‌باشد، ارائه می‌شود که در سطح اول هدف پژوهش، در سطح دوم بر اساس مطالعات پیشین ۴ معیار در نظر گرفته شد و در سطح سوم ۲۶ زیرمعیار باقی مانده در دلفی معیارها با استفاده از تکنیک دلفی زیرمعیارها با در نظر گرفتن نظر خبرگان باقی ماندند و برای مراحل بعدی تجزیه و تحلیل در نظر گرفته شدند. در مرحله دوم به تعیین وزن هر یک از معیارها و زیر معیارها نسبت به یکدیگر پرداخته می‌شود. با توجه به ارتباط میان شاخص‌ها، مقایسات زوجی معیارها نسبت به یکدیگر بر اساس مقیاس ۹ کمیتی ساعتی توسط متخصصین انجام می‌گیرد. پس از تعیین ضریب اهمیت معیارها و شاخص‌ها نسبت به یکدیگر، ماتریس‌های مقایسات زوجی مطابق شکل ۱ در نرم افزار Super Decisions وارد می‌شوند.



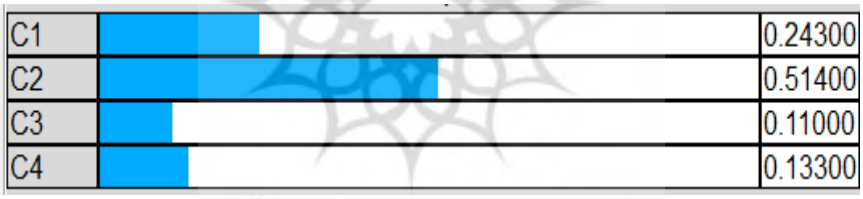
شکل ۱- نمودار ANP اولویت شاخص‌ها در نرم افزار سوپردسیژن

در مرحله سوم، تحلیل یافته‌های حا صل از مدل به‌د ست می‌آید، محا سبات حاصل از به‌کارگیری نرم افزار Super Decisions نشان می‌دهد.

جدول ۲- ماتریس مقایسه زوجی معیارهای اصلی پژوهش

	قاچاق	کلاه برداری	مواد مخدر	تروریست	میانگین هندسی	بردار ویژه
قاچاق	۱	۰,۳۷۵	۲,۰۸۴	۲,۴۵۶	۱,۱۷۷	۰,۲۴۳
کلاه برداری	۲,۶۶۷	۱	۳,۸۰۱	۳,۷۸۶	۲,۴۸۹	۰,۵۱۴
مواد مخدر	۰,۴۸۰	۰,۲۶۳	۱	۰,۶۲۸	۰,۵۳۱	۰,۱۱۰
تروریست	۰,۴۰۷	۰,۲۶۴	۱,۵۹۳	۱	۰,۶۴۳	۰,۱۳۳

معیار "کلاه برداری" با وزن نرمال شده ۰,۵۱۴ در اولویت اول، معیار "قاچاق" با وزن نرمال شـــده ۰,۲۴۳ در اولویت دوم، معیار "تروریســـت" با وزن نرمال شـــده ۰,۱۱۳ در اولویت ســوم و معیار " مواد مخدر" با وزن نرمال شــده ۰,۱۱۰ در اولویت آخر قرار دارد.



شکل ۲- خروجی نرم افزار سوپر دسیژن اولویت معیارهای اصلی بر اساس هدف

به همین ترتیب زیرمعیارهای هر معیار نیز بر اســاس نظر خبرگان رتبه بندی شده و وزن نسبی آن‌ها به‌دست می‌آید.

در تکنیک دیمتل، پس از محاسبه ماتریس ارتباط مستقیم و ارتباط مستقیم نرمال برای محاسبه ماتریس ارتباط کامل ابتدا ماتریس همانی (I) تشکیل می شود. سپس ماتریس همانی منهای ماتریس نرمال شده و ماتریس حاصل معکوس می‌شود. درنهایت ماتریس نرمال در ماتریس معکوس ضرب می‌شود و مطابق جدول ۱ ماتریس کامل بدست می‌آید.

$$T \quad N \quad I \quad N^{1}$$

جدول ۳- ماتریس ارتباط کامل (T)

T Matrix	قاچاق	کلاه برداری	مواد مخدر	تروریست
قاچاق	4.248	4.468	4.410	4.404
کلاه برداری	4.741	4.475	4.603	4.662
مواد مخدر	4.873	4.872	4.532	4.849
تروریست	4.667	4.703	4.575	4.389

با توجه به الگوی روابط می‌توان نمودار علی را بر اساس جدول ۴ ترسیم کرد:

جدول ۴- الگوی روابط علی معیارهای اصلی

معیار	نماد معیار	D	R	D+R	D-R
قاچاق	C1	17.529	18.529	36.058	-۱,000
کلاه برداری	C2	18.481	18.518	36.998	-0.037
مواد مخدر	C3	19.127	18.120	37.247	1.006
تروریست	C4	18.334	18.304	36.638	0.030

در جدول ۴ جمع عناصر هر سطر (D) نشانگر میزان تأثیرگذاری آن معیار بر دیگر معیارهای مدل است. بر این اساس مواد مخدر از بیشترین تأثیرگذاری برخوردار است. جمع عناصر ستون (R) برای هر عامل نشانگر میزان تأثیرپذیری آن عامل از سایر عامل‌های سیستم است. براین اساس معیارهای قاچاق از میزان تأثیرپذیری بسیار زیادی برخوردار است. بردار افقی (D + R)، میزان تأثیر و تأثر عامل مورد نظر در سیستم است. به عبارت دیگر هرچه مقدار D + R عاملی بیشتر باشد، آن عامل تعامل بیشتری با سایر عوامل سیستم دارد. براین اساس معیار مواد مخدر بیشترین تعامل را با سایر معیارهای مورد مطالعه دارند. بردار عمودی (D - R)، قدرت تأثیرگذاری هر عامل را نشان می‌دهد. به‌طور کلی اگر D - R مثبت باشد، متغیر یک متغیر علی محسوب می‌شود و اگر منفی باشد، معلول محسوب می‌شود. در این مدل معیارهای قاچاق و کلاه برداری متغیر علی و معیارهای مواد مخدر و تروریست معلول هستند.

اولویت نهائی زیرمعیارها با اقتباس از سوپر ماتریس حد در جدول۳ به ترسیم درآمده است.

جدول ۳- اولویت بندی نهایی زیرمعیارهای تحقیق

معیار	زیرمعیار	نماد زیرمعیار	وزن نهایی	رتبه نهایی	معیار	زیرمعیار	نماد زیرمعیار	وزن نهایی	رتبه نهایی
قاچاق	قاچاق داروهای خاص	S11	۰,۰۵۴۸	۶	مواد مخدر	سیگار در بازار سیاه	S31	۰,۰۹۸۳	۲
	قاچاق سلاح	S12	۰,۰۴۷۴	۸		تجارت مواد مخدر با در نظر داشتن ناشناس بودن	S32	۰,۰۵۰۲	۷

معیار	زیرمعیار	نماد زیرمعیار	وزن نهایی	رتبه نهایی	معیار	زیرمعیار	نماد زیرمعیار	وزن نهایی	رتبه نهایی
	قاچاق جواهرات	S13	۰,۰۲۷۹	۱۵		وجود بازارهای مواد مخدر رمز گذاری شده	S33	۰,۱۰۱۱	۱
	اجناس مسروقه	S14	۰,۰۲۱۵	۱۹	تروریست	تبلیغات و گسترش انگیزه‌های منفی گروه‌های تروریستی	S41	۰,۰۱۵۶	۲۶
	قاچاق انسان	S15	۰,۰۳۲۸	۹		استخدام و جذب نیرو	S42	۰,۰۲۹۵	۱۲
	فروش اعضای بدن	S16	۰,۰۳۲۸	۱۰		آموزش نیروهای گروه‌های تروریستی	S43	۰,۰۱۸۸	۲۲
	خرید و فروش تجهیزات غیرمجاز نظیر گنج یاب، سانتریفیوژهای دور بالا،	S17	۰,۰۳۲۸	۱۱		تغییر فرماندهی و ابلاغ دستورات و نقشه‌ها	S44	۰,۰۱۶۶	۲۴

معیار	زیرمعیار	نماد زیرمعیار	وزن نهایی	رتبه نهایی	معیار	زیرمعیار	نماد زیرمعیار	وزن نهایی	رتبه نهایی
	موتورهای دوربالا و ...								
کلاه برداری	تبانی با سیاست مداران و پلیسان فاسد	S21	۰,۰۲۸۳	۱۴		درخواست پول برای کمک و حمایت	S45	۰,۰۱۹۶	۲۱
	دسترسی و سرقت اطلاعات طبقه بندی شده	S22	۰,۰۹۳۱	۳		انتقال اطلاعات و ارتباطات	S46	۰,۰۶۳۲	۴
	تجارت خدمات مخفی	S23	۰,۰۲۱	۲۰		استخدام جنایتکاران	S47	۰,۰۱۶۲	۲۵
	معاملات غیر قابل ردیابی	S24	۰,۰۶۱	۵		جرائم جنسی	S48	۰,۰۲۸۴	۱۳
	پولشویی	S25	۰,۰۲۵	۱۶		برقراری گروه‌های جدائی طلبانه	S49	۰,۰۲۳۸	۱۷
	خرید و فروشی اطلاعات دولتی محرمانه سری	S26	۰,۰۲۱۸	۱۸		برنامه ریزی انقلاب‌های رنگی	S410	۰,۰۱۸۳	۲۳

نتیجه گیری

هدف از انجام این واکاوی وب سیاه در فضای مجازی ایران می‌باشد. در اینترنت عمیق زیرمجموعه‌ای که بیشتر برای اهداف غیرقانونی استفاده می شود وب سیاه یا نت سیاه است. براساس نتایج تحقیق مشخص گردید، زیرمعیار " وجود بازارهای مواد مخدر رمز گذاری شده" در اولویت اول قرار دارد. یکی از بزرگترین مصارف تبهکارانه وب تاریک، استفاده از آن به عنوان بازار خرید و فروش مواد مخدر است، تا جایی که برخی استفاده کنندگان از این شبکه در بستر فضای سایبر، تا جایی پیش رفته‌اند در عین مخفی بودن اطلاعاتشان، هر ساله چندین نوع مواد مخدر و روانگردان جدید را از طریق این بستر معرفی و در برخی موارد نسبت به حمل و خرید و فروش آن اقدام می¬کنند. لذا به سازمان‌های مربوطه از قبیل پلیس فتا و پلیس مبارزه با مواد مخدر توصیه می‌گردد ضمن به کارگیری افراد مجرب در حوزه فضای مجازی، با تشکیل کارگروه‌ها و تیم‌های ویژه نسبت به شناسایی و پیگیری جرائم این چنینی اقدام و آموزش‌های لازم جهت به روزرسانی دانش تیم عملیات سایبری در رابطه با روش‌های کشف و انهدام شبکه‌های قاچاق مواد مخدر در محیط وب تاریک را در نظر داشته باشند. ضمن آنکه ارائه آموزش‌های عمومی در رسانههای جمعی و تبلیغات محیطی در زمینه آشنایی خانواده‌ها با جرائم اینترنتی مواد مخدر و راه‌های مقابله با آن می‌تواند یاری رسان باشد. معیار "کلاه برداری" در اولویت اول قرار دارد. به دلیل عدم افشای اطلاعات افراد فعال در وب تاریک، شرایط برای بروز اقدامات مجرمانه و کلاهبرداری‌های مختلفی از جمله فساد و تبانی در سازمان‌های مختلف، سرقت اطلاعات محرمانه، معاملات غیرقانونی، پول‌شویی و ... فراهم است. به همین منظور لازم است شرکت‌ها و سازمان‌های حیاتی تحت نظر مراکز امنیت سایبری فعالیت نمایند و با رصد مداوم این فضا و تدوین سیاست‌های مقابله‌ای، فرصت را برای بروز هر گونه فساد و کلاه برداری از بین ببرند. ضمن انکه به جای اینکه به وب تاریک به چشم یک تهدید غیرقابل کنترل نگاه شود، مؤسسات مالی می‌توانند با استفاده از وب تاریک به‌عنوان یک ابزار امنیت سایبری، وارد کار شوند و جلوی بروز موارد ضد امنیتی و کلاهبرداری را بگیرند. در هر صورت ارتکاب

کلاهبرداری سایبری تأثیر زیادی بر زیر ساخت‌های حیاتی و اداری کشور بر جا خواهد گذارد و با زیر سؤال بردن توانمندی¬های نظام قضایی و پلیس فتا عملاً منجر به کم اعتبار شدن دستگاه عدالت کیفری خواهد شد؛ لذا لازم است سرمایه‌گذاری‌های لازم در حوزه امنیت سایبری ارگان‌های حیاتی کشور و نیز امنیت اطلاعات مالی و شخصی افراد جامعه صورت پذیرد و تعامل لازم در این خصوص بین دستگاه‌های اجرایی و قضایی کشور وجود داشته باشد. معیار "مواد مخدر" بیشترین تأثیرگذاری و تعامل را در میان معیارها دارا می‌باشد. لذا توصیه می‌گردد ضمن سرمایه‌گذاری برای تربیت مأمورین کارآمد در حوزه سایبری و کشف معاملات مواد مخدر؛ قوانین و مجازات‌های متناسب با جرائم مذکور تدوین گردد و با خاطیان برخورد قاطع صورت پذیرد. همچنین با آموزش‌های اجتماعی و فرهنگ سازی، سطح شناخت و درک عمومی از مواد مخدر به عنوان یک تهدید ملی و مانع مهم رشد ارتقا یابد تا موجب همکاری دوجانبه مردم و دولت در روند مهار و کاهش سوء مصرف مواد و در نتیجه‌ی آن کاهش بازار مصرف توزیع کنندگان مواد مخدر در فضای وب تاریک گردد. معیار "قاچاق" بیشترین تأثیرپذیری را در میان معیارها دارا می‌باشد. به طور کلی معقوله قاچاق در فضای وب تاریک، موضوعاتی همچون قاچاق دارو، اعضای بدن، سلاح، جواهرات، اجناس مسروقه، مواد مخدر و ... را در بر می‌گیرد. موفقیت در عرصه‌ی مقابله با قاچاق در فضای مجازی، همکاری در سطح بین‌المللی و نیز الگوبرداری و استفاده از تجربیات کشورهای موفق در این حوزه را می‌طلبد. به همین منظور لازم است علاوه بر تقویت روابط بین‌المللی و گسترش ارتباطات با پلیس اینترپل نسبت به اخذ آموزش و مشاوره از سایر کشورهای پیش‌گام در این حوزه اقدامات مناسب صورت پذیرد. به طور خلاصه لازم است پلیس فتا با اشراف اطلاعاتی بر فضای سایبری و مجازی، تکیه بر دانش فنی و تخصص، به کارگیری تجهیزات به روز و نوین

و ... در مسیر رشد و تعالی قرارگیرد و تقویت این پلیس در اولویت‌های کار نیروی انتظامی قرار گیرد.

در مقایسه با تحقیقات پیشین؛ حسین آبادی و حسنی (۱۳۹۹)، همانند تحقیق حاضر به این نتیجه رسیدند که جرایم مواد مخدر و قاچاق اعضای بدن و قاچاق انسان از جمله جرائم موجود در وب تاریک می‌باشد. قناد و اسلامیان کوپایی (۱۳۹۹)، همانند تحقیق حاضر به این نتیجه رسیدند که تروریست و انقلاب‌های رنگین از جمله جرائم موجود در وب تاریک می‌باشد و پولشویی و تراکنش‌های مالی غیر قانونی از جمله جرائم موجود در وب تاریک می‌باشد. قربانی (۱۳۹۸)، همانند تحقیق حاضر به این نتیجه رسیدند که جرائم مواد مخدر از جمله جرائم موجود در وب تاریک می‌باشد. نزاه و همکاران (۲۰۲۰)، همانند تحقیق حاضر تهدیدات وب تاریک را شامل چهار گروه قاچاق، کلاه برداری، مواد مخدر و تروریست دانستند.

منابع

۱. پور اسـمعلی، اصـغر؛ مولایی، مهری؛ علیزاده گورادل، جابر؛ هاشـمی، جواد؛ (۱۳۹۵) "رابطه صفات تیره شخصیت و خودافشاگری اینترنتی در دانشجویان " مجله دست آوردهای روان شناختی (علوم تربیتی و روان شناسی)، دانشگاه شهید چمران اهواز، دوره ۴، سال ۲۳، شماره ۲، صص ۱۵۷-۱۷۲.

۲. جواهری، مهدی؛ (۱۳۹۵) "تأثیر فضای مجازی بر افزایش مصرف مواد مخدر با تأکید بر وب پنهان" دو فصلنامهٔ مطالعات مبارزه با مواد مخدر، دوره ۸، شماره ۳۱، صص ۶۳-۷۵.

۳. حسین آبادی، باقر؛ حسینی، فاطمه؛ (۱۳۹۹) " جرائم ارتکابی در بستر وب تاریک " نشریه کارآگاه، سال سیزدهم، شماره ۵۱، صص ۶۶-۹۲.

۴. رحمان زاده، سید علی؛ فضلعلی، زهرا؛ هاشم زهی، نوروز (۱۴۰۰) "تحلیل شبکه‌های اجتماعی پنهان آثار"، گستره جهانی و آینده آن در ایران. ۱. ۵ (۴) :۴۶۸-۴۶۲.

۵. سـرافرازی، اعظم؛ ایزدیار، صـدیقه؛ حبیبی، آرش (۱۳۹۳) "تصـمیم گیری چند معیاره فازی" انتشارات سیمای دانش، آذر: رشت.

۶. فتاحی، مختار (۱۳۹۷) " بررسی عناصر تشکیل دهنده مادی و معنوی مصادیق جرایم رایانه ای" قانون یار، دوره ۲، شماره ۶، صص ۹۹ تا ۱۲۰.

۷. قربانی، ابراهیم؛ (۱۳۹۸) "تحلیل نقش ابعاد وب تاریک در گسترش جرائم موادمخدر و روان‌گردان در فضـای سـایبر " فصـلنامه پژوهش‌های اطلاعاتی و جنایی، دوره ۱۴، شماره ۱، پیاپی ۵۳، صص ۲۹-۵۴.

۸. قناد، فاطمه؛ اسلامیان کوپایی، سجاد؛ (۱۳۹۹) " شرح فضای کلی حاکم بر وب تاریک از فعالیت مردم تا حضـور دولت‌ها" شـشـمین کنفرانس بین المللی وب پژوهی، جهاد دانشگاهی، دانشگاه علم و فرهنگ، دوره ۶.

۹. کتانچی، الناز؛ پورقهرمانی، بابک؛ (۱۳۹۸) " سـیاسـت‌های نمادین معاهده جرایم سایبری شورای اروپا " فصلنامه مطالعات بین‌المللی، سال ۱۶، شماره ۲ (۶۲)، صص ۳۱-۴۷.

۱۰. کرد علیوند، روح اله؛ میرزایی، محمد (۱۳۹۷) " گونه شناسی جرایم سایبری با نگاهی به قانون جرایم رایانه ای و آمار پلیس فتا" حقوق دادگسـتری، دوره ۸۲، شـماره ۱۰۲، صص ۱۹۱ تا ۲۰۷.

۱۱. مقدمی اصل، چپا؛ (۱۳۹۶) " بررسی دارک و دیپ وب و اتفاقات پشت پرده این دنیای مخفی اینترنتی" کنفرانس ملی رهیافت‌های نو در مهندسی برق و کامپیوتر.

منابع لاتین

1. Aldridge, J., & Décary-Hétu, D. (2014). Not an'Ebay for Drugs': the Cryptomarket'Silk Road'as a paradigm shifting criminal innovation. Available at SSRN 2436643.
2. Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. International Journal of Drug Policy, 35, 7-15.
3. Amores R., Paganini P.(2014), The Deep Dark Web: The Hidden World, Vol. 1. Seattle, WA: CreateSpace Independent Publishing Platform.
4. Backman, B. (2013). Follow the white rabbit: An ethnographic exploration into the drug culture concealed within the" deep Web". University of Nebraska at Omaha.
5. Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. International Journal of Drug Policy, 35, 24-31.
6. Chertoff M. and Simon, T. (2015) The impact of the darkWeb on Internet governance and cyber security,' Centre Int. Governance Innovation (CIGI), Waterloo, ON, Canada, Tech. Rep. 6.
7. Chertoff, M. (2017). A public policy perspective of the Dark Web. Journal of Cyber Policy, 2(1), 26-38.
8. Childs, A., Bull, M., & Coomber, R. (2021). Beyond the dark web: navigating the risks of cannabis supply over the surface web. Drugs: Education, Prevention and Policy, 1-12.
9. Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In Proceedings of the 22nd international conference on World Wide Web (pp. 213-224).
10. da Cunha, B. R., MacCarron, P., Passold, J. F., dos Santos, L. W., Oliveira, K. A., & Gleeson, J. P. (2020). Assessing police topological efficiency in a major sting operation on the dark web. Scientific reports, 10(1), 1-10.

11. Fanusie, Y., & Robinson, T. (2018). Bitcoin laundering: an analysis of illicit flows into digital currency services. Center on Sanctions and Illicit Finance memorandum, January.
12. Goodman, M. (2016). Most of the web is invisible to Google. Kere's what it contains. Popular Science, Retrieved November, 18, 2016.
13. Greenberg, A. (2014). Hacker lexicon: what is the dark web?. Wired. http://www. wired. com/2014/11/hacker-lexicon-whats-dark-web [dostęp 6.02. 2017].
14. Hatta, M. (2020). Deep web, dark web, dark net A taxonomy of "hidden" Internet. Annals of Business Administrative Science, 0200908a.
15. Islam, M. R., & Ozkaya, E. (2019). The Dark Web: Learning to Dark Web.
16. Kavallieros, D., Myttas, D., Kermitsis, E., Lissaris, E., Giataganas, G., & Darra, E. (2021). Using the Dark Web. In Dark Web Investigation (pp. 27-48). Springer, Cham.
17. Lakomy, M. (2017). The evolution of cyber jihad from al-Qaeda to the Islamic State. Available at: https://www.researchgate.net/profile/Miron_Lakomy/publication/321097989.
18. Lane, J. (2013). Bitcoin, silk road, and the need for a new approach to virtual currency regulation. Charleston L. Rev., 8, 511.
19. Lightfoot, S., & Pospisil, F. (2017). Surveillance and privacy on the deep Web. ResearchGate, Berlin, Germany, Tech. Rep.
20. Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. Information, Communication & Society, 19(1), 111-126.
21. Mainas, E. D. (2012). The analysis of criminal and terrorist organisations as social network structures: a quasi-experimental study. International Journal of Police Science & Management, 14(3), 264-282.
22. Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. Survival, 58(1), 7-38.

23. Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. IEEE Access, 8, 171796-171819.
24. Perfect, E., Jaiswal, A., & Davies, T. C. (2019). Systematic review: investigating the effectiveness of assistive technology to enable internet access for individuals with deafblindness. Assistive Technology, 31(5), 276-285.
25. Tsikerdekis, M., & Zeadally, S. (2014). Multiple account identity deception detection in social media using nonverbal behavior. IEEE Transactions on Information Forensics and Security, 9(8), 1311-1321.
26. Tucker. P. (2015). How the Military Will Fight ISIS
27. Tuzkaya, U. R., & Önüt, S. (2008). A fuzzy analytic network process based approach to transportation-mode selection between Turkey and Germany: A case study. Information Sciences, 178(15), 3133-3146.
28. Weimann, G. (2016). Going dark: Terrorism on the dark web. Studies in Conflict & Terrorism, 39(3), 195-206.
29. Xu, J., Chen, H., Zhou, Y., & Qin, J. (2006, May). On the topology of the dark web of terrorist groups. In International Conference on Intelligence and Security Informatics (pp. 367-376). Springer, Berlin, Heidelberg.
30. Yu, C., Xia, F., Qian, W., & Zhou, A. (2019). A parallel data generator for efficiently generating "realistic" social streams. Frontiers of Computer Science, 13(5), 1072-1101.
31. Zhang, X., & Chow, K. P. (2020). A framework for dark Web threat intelligence analysis. In Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (pp. 266-276). IGI Global.
32. Zheng, X., Lai, Y. M., Chow, K., Hui, L. C., & Yiu, S. (2011). Detection of sockpuppets in online discussion forums (Doctoral dissertation, University of Hong Kong).