

واکاوی وب سیاه در فضای مجازی ایران

محمد رضا 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، علی‌الخصوص وب سیاه که قابل دسترسی برای کاربران عادی نیست این ارتباطات را ساده کرده است. این تحقیق با هدف واکاوی وب سیاه در فضای مجازی ایران صورت گرفته است. از نظر دسته‌بندی تحقیقات برحسب هدف یک تحقیق کاربردی می‌باشد، از نظر 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 است که پرسش‌نامه خبرگان در میان آن‌ها پخش شد. براساس مطالعات صورت گرفته معیارهای اصلی تحقیق شامل دانش، محیط، مردم، فرایند، تجهیزات و زیرساخت‌ها و مدیریت می‌باشد. تجزیه و تحلیل داده‌ها با استفاده از رویکرد ANP-DEMATEL صورت گرفته است. براساس 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

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،^۳ ۲۰۱۷). وب سطحی بخش کوچکی از اینترنت (در معنای عام) را تشکیل می‌دهد که در آن محتوای سایت‌ها به راحتی توسط موتورهای جستجو مانند گوگل، یاهو و.. فهرست می‌شود 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،^۴ 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 (نزه و همکاران،^۵ ۲۰۲۰). در اینترنت عمیق زیرمجموعه‌ای که بیشتر برای اهداف غیرقانونی استفاده می‌شود وب سیاه یا نت سیاه است (لکومی،^۶ 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

مشاهده است اما آدرس آی پی آنها مخفی و پنهان می‌باشد. 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 داشتن نشانی وب که عموماً از پروتکل‌های عادی تبعیت نمی‌کند، می‌توانند به این وب سایت‌ها دسترسی داشته باشند (قناد و اسلامیان کویایی، ۱۳۹۹). استفاده از وب سیاه در اکثر مواقع با اهداف غیرقانونی صورت می‌گیرد که برخی از این اهداف شامل جعل اسناد، قتل، فروش مواد مخدر، خرید و فروش مواد منفجره و سلاح، سرقت هویت و پول‌های تقلبی می‌باشد (کاوالیروس و همکاران، ۲۰۲۱). برای تشکیل باندها و شبکه‌های قاچاق بین‌المللی مواد مخدر و روانگردان‌ها استفاده می‌شود. شاید مهم‌ترین بعد وب سیاه این مورد باشد که مجرمان مواد مخدر و روانگردان‌ها در استفاده از این کارکرد، بر اعمال مجرمانه خود سایه انداخته و از تیررس مبارزان این تجارت در امان می‌مانند؛ چرا که دسترسی به اطلاعات این افراد که از طریق کارکردهای وب سیاه به تجارت خود می‌پردازند، عملی غیرممکن تلقی می‌شود (قربانی، ۱۳۹۸). در واقع اینترنت و شبکه گسترده وب جهانی بسیار بزرگتر از چیزی است، که از طریق مرور منظم مشاهده می‌شود. 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. شمار زیادی از مجرمان سایبری سعی می‌کنند هر روز اقدامات غیرقانونی برای دستیابی به داده‌های غیرمجاز از طریق اینترنت انجام دهند. اکثر کاربران اینترنت از طریق مرورگرهای عادی مانند Internet 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 مانده است. به عبارتی موتورهای جستجوگر مدرن فقط بخش بسیار کمی از وب را فهرست می‌کنند و مقدار زیادی از مطالب وب همان‌طور که در

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^۱، ۲۰۲۰). به‌رغم تفاوت‌های موجود در رویکرد این پژوهش‌ها، محور اصلی همه آنها یافتن راهکارهایی عملی برای ارتقای سطح دسترس پذیری اطلاعات در این شبکه و سهولت بازیابی است (پرفکت و همکاران^۲، ۲۰۱۹).

از آنجا که به دلیل گستردگی بی‌وقفه اطلاعات موجود در شبکه جهان گستر 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^۳، ۲۰۱۹).

منابع اطلاعاتی متنوعی در وب وجود دارند که تنها به دلیل محدودیت تکنولوژیکی یا مالی موتورهای جستجو، از حوزه کاوش آنها و در نتیجه از دسترسی کاربران دور مانده‌اند (هاتا^۴، 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 تقریباً به‌طور کامل مخفی می‌باشد (گودمن^۵، ۲۰۱۶). مطابق گزارش مرکز مبارزه با جرایم سایبری استرالیا، اصطلاح جرایم سایبری به جرایمی مربوط می‌شود 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 به‌کارگیری اشکال مختلف نرم افزارهای مخرب (مانند

1Cunha et al.

2Perfect et al.

3Yu et al.

4Hatta

5Goodman

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^{۱۴}، 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 فروشگاه‌های 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 می‌باشد که از طریق آن می‌توانند به گسترش شبکه‌های غیرقانونی خود پرداخته و به نوعی به پول بیشتر دست یابند و فروشگاه‌های دارک وب دقیقاً همانند فروشگاه‌های معمول در وب می‌باشند و به همان شیوه اداره می‌شوند، منتها در این فروشگاه‌ها معمولاً موارد غیرقانونی فروخته می‌شود (مقدمی اصل، ۱۳۹۶). کاربران وب تاریک کسانی هستند که به دنبال انتقال و دریافت اطلاعات هستند، به گونه‌ای که احتمال آشکار سازی و شناسایی آن فعالیت‌ها، بسیار کم باشد. 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، می‌تواند به عنوان یک پوشش در برابر تشخیص مجرمان و سوداگران مجازی مورد استفاده آنها قرار بگیرد (جواهری، ۱۳۹۵). فعالیت‌های جنایی متعددی در شبکه‌های عمیق در حال انجام است 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، ۲۰۱۴). جرایم ارتكابی در

وب تاریک یکی از مهم‌ترین و در عین حال پیچیده‌ترین نوع جرایم در اقصی نقاط جهان می‌باشد، که عمدتاً با هدف تحصیل منافع مادی و مالی و در برخی موارد با اهداف ایدئولوژیک، سیاسی و کسب قدرت به وقوع می‌پیوندد. این گونه جرایم را می‌توان منسجم‌ترین و قوی‌ترین ساختار باندهای مجرمانه تلقی نمود (پور اسمعیلی و همکاران، ۱۳۹۵) که این مسأله می‌تواند اهمیت توجه به شبکه‌های 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 در پی 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 شناسایی و رتبه بندی تهدیدات وب تاریک با استفاده از تکنیک تصمیم‌گیری چندمعیاره می‌باشد. با این تفاسیر با توجه به اهمیت تهدیدات وب سیاه در فضای مجازی ایران و تأثیرگذاری آن بر جرائم موجود در جامعه، در این مقاله به شنا سایی و اولویت‌بندی تهدیدات موجود در وب تاریک پرداخته خواهد شد. بر این اساس پیش از این نیز تحقیقاتی در این زمینه انجام دادند.

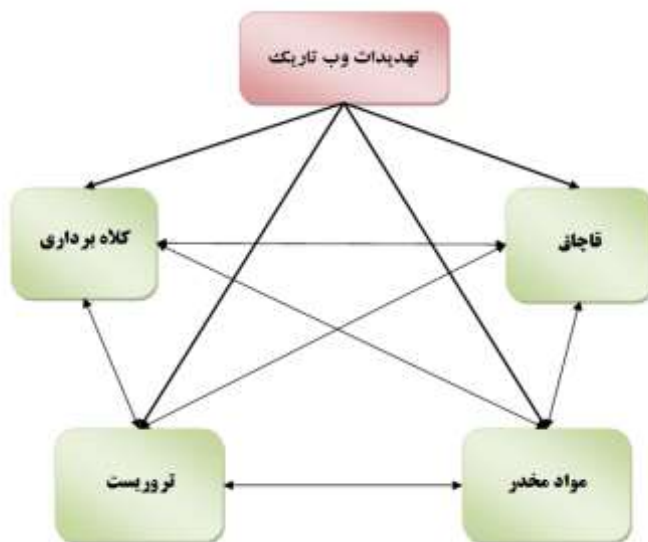
رحمان زاده و همکاران (۱۴۰۰) به این نتیجه رسیدند که فضای مجازی مانند فضای واقعی نیازمند فرهنگ است. ضروری است به این فناوری با نگاه فرصت‌سازی نگریست و علاوه بر آموزش‌های لازم به کاربران برای ورود به فضای شبکه تاریک، سیاست‌های فرهنگی جامعه برای استفاده صحیح از آن را تطبیق داده تا کمتر شاهد آسیب‌پذیری در این زمینه باشیم. حسین آبادی و حسینی (۱۳۹۹)، با رویکرد کاربردی و روش کیفی و با بهره‌گیری از ابزارهایی مانند مطالعات اسنادی، 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 کویابی (۱۳۹۹)، سعی گردید ضمن تبیین و توصیف فضای کلی حاکم بر وب تاریک، چگونگی ساختار بندی و جریان سازی فعالیت مردم تا ساماندهی نظام‌مند تحت نظارت دولت‌ها مورد بررسی قرار گیرد تا در نهایت از طریق مدل مسیریابی پیازی (تر) 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 از آنها 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.

کوالیروس و همکاران^۵ (۲۰۲۱)، بیان کردند با فعالیت های تاریک و جنایتکارانه‌ای که در وب اتفاق می افتد 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

پرداختند. چیلدز و همکاران^(۲۰۲۱)، به این نتیجه رسیدند که بازیگران از طریق نرمال سازی گسترده تر 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 داروهای غیرقانونی آنلاین نیز در نظر گرفته‌اند. نزاه و همکاران^{۱۷} (۲۰۲۰)، در مقاله خود جنایات وب تاریک، پیامدهای آن و و راه‌حل‌های 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^(۲۰۲۰)، دریافتند که یکی از تهدیدات این فضا، کاربرد آن برای دسترسی ناشناس به خدمات پنهان و غیرقانونی اینترنتی از قبیل کیف پول Bitcoin، 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.



شکل ۱- مدل مفهومی تحقیق، منبع: (نزه و همکاران، 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

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

منبع	زیرمعیار	معیار
نزه و همکاران (۲۰۲۰)، چریستین و همکاران (۲۰۱۳)	قاچاق داروهای خاص	قاچاق
	قاچاق سلاح	
	قاچاق جواهرات	
	اجناس مسروقه	
نزه و همکاران (۲۰۲۰)، دیلی ^۱ (۲۰۱۳)	تبانی با سیاست مداران و پلیسان فاسد	کلاه برداری
نزه و همکاران (۲۰۲۰)، گنوا ^۲ (۲۰۱۷)	دسترسی و سرقت اطلاعات طبقه بندی شده	
نزه و همکاران (۲۰۲۰)، مور و رید (۲۰۱۶)	تجارت خدمات مخفی	
نزه و همکاران (۲۰۲۰)، لین ^۳ (۲۰۱۳)	معاملات غیر قابل ردیابی	
بک من (۲۰۱۳) ^۴	تبادل بیت کوین	
فنوسه و رابینسون (۲۰۱۸) ^۵	پولشویی	
	سیگار در بازار سیاه	

Christin et al.

Daily

Geneva

Moore & Rid

lane

Sackman

Manusie & Robinson

منبع	زیر معیار	معیار
نزه 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)	تجارت مواد مخدر با در نظر داشتن ناشناس بودن وجود بازارهای مواد مخدر رمز گذاری شده	
نزه و همکاران (۲۰۲۰)، لایتفوت و پیسپسیل ^{۳۲} (۲۰۱۷)، بتس ^{۳۳} (۲۰۱۶)، ویمن ^{۳۴} (۲۰۱۶)، میناس ^{۳۵} (۲۰۱۲)، ژنگ و همکاران ^{۳۶} (۲۰۱۳)، ژو و همکاران ^{۳۷} (۲۰۰۶)	تبلیغات و گسترش انگیزه‌های منفی گروه‌های تروریستی استخدام و جذب نیرو آموزش تغییر فرماندهی و ابلاغ دستورات و نقشه‌ها	تروریست
نزه و همکاران (۲۰۲۰)، توکر ^{۳۸} (۲۰۱۵)	درخواست پول برای کمک و حمایت انتقال اطلاعات و ارتباطات	
نزه و همکاران (۲۰۲۰)، چرتف و همکاران ^{۳۹} (۲۰۱۵)	استخدام جنایتکاران	

²⁷Aldridge et al.

²⁸Barratt et al.

²⁹Maddox et al.

³⁰Aldridge et al.

³¹Isikerdekis et al.

³²Lightfoot and Pospisil

³³Bates

³⁴Weimann

³⁵Mainas

³⁶Zheng et al.

³⁷Xu et al,

³⁸Bucker

³⁹Hertoff 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 دور بالا 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.

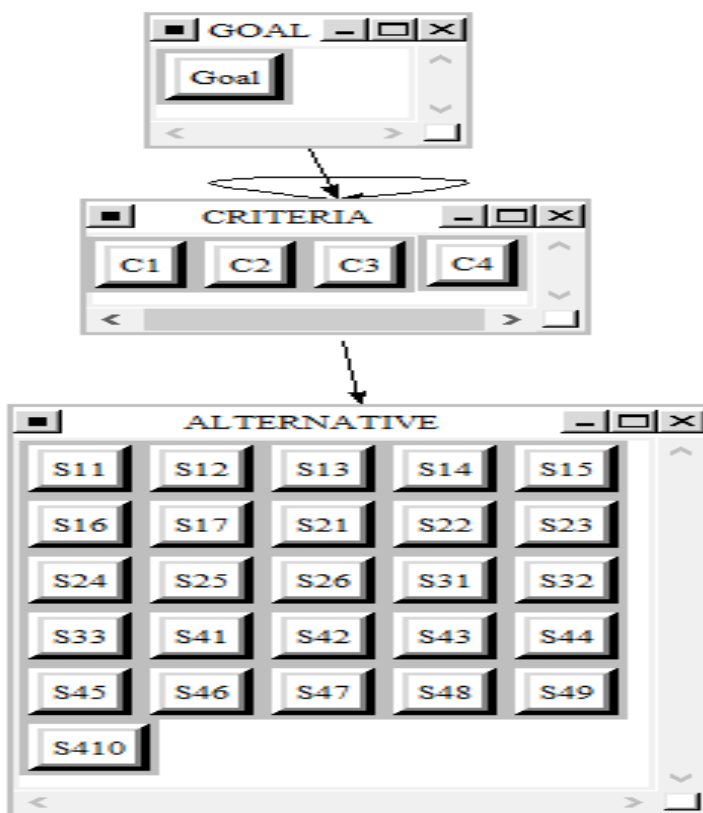
سپس به منظور انجام مقایسات زوجی و تعیین وابستگی‌های بین معیارها و زیرمعیارها، پرسشنامه‌های طراحی شده کارشناسان فضای مجازی توزیع گشت. با اشاره به این نکته که تعداد خبرگان به عنوان مصاحبه شونده نباید زیاد باشد در کل ۵ الی ۱۵ نفر را پیشنهاد می‌کنند (سرافرازی و همکاران، ۱۳۹۳). در نتیجه تعداد ۱۰ نفر از کارشناسان فضای مجازی به عنوان نمونه مورد بررسی استفاده شده‌اند. در ادامه جهت تحلیل داده‌ها (اطلاعات به دست آمده از پرسش‌نامه‌ها) 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 تصمیم‌گیری‌ها ارائه می‌نماید (توزکایا و همکاران، ۲۰۰۸). همچنین برای بررسی روابط درونی از تکنیک دیمتل استفاده شده است. در این تحقیق تکنیک دیمتل به عنوان 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).

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 حاصل از مدل به دست می‌آید، محاسبات حاصل از به‌کارگیری نرم افزار Super Decisions نشان می‌دهد.

جدول ۲- ماتریس مقایسه زوجی معیارهای اصلی پژوهش

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

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

C1		0.24300
C2		0.51400
C3		0.11000
C4		0.13300

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

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

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

$$T = N \times (I - N)^{-1}$$

جدول ۳- ماتریس ارتباط کامل (T)

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

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

جدول ۴- الگوی روابط علی معیارهای اصلی

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

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. بر این 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. بر این 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 نهایی زیرمعیارها با اقتباس از سوپر ماتریس حد در جدول ۳ 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

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

واکاوی وب سپاه در فضای مجازی ایران // ۱۵۳

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

نتیجه گیری

هدف از انجام این واکاوی وب سیاه در فضای مجازی ایران می‌باشد. در اینترنت عمیق زیرمجموعه‌ای که بیشتر برای اهداف غیرقانونی استفاده می‌شود 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 می‌کنند. 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 چینی 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 مجرمانه، 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 آنکه به جای اینکه به وب تاریک به چشم یک تهدید غیرقابل کنترل نگاه شود، مؤسسات مالی می‌توانند با استفاده از وب تاریک به عنوان 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 توانمندی‌های 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 حسینی (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 کویایی (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 جرایم مواد مخدر از جمله جرائم موجود در وب تاریک می‌باشد. نزه و همکاران (۲۰۲۰)، همانند تحقیق حاضر تهدیدات وب تاریک را شامل چهار گروه قاچاق، کلاه برداری، مواد مخدر و تروریست دانستند.

منابع

۱. پور اسمعیلی، اصغر؛ مولایی، مهتری؛ علیزاده گورادل، جابر؛ هاشمی، 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 فصلنامه مطالعات مبارزه با مواد مخدر، دوره ۸، شماره ۳۱، صص ۶۳-۷۵.
۳. حسین آبادی، باقر؛ حسینی، فاطمه؛ (۱۳۹۹) "جرائم ارتكابی در بستر وب تارک" 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. سرافرازی، اعظم؛ ایزدیار، صدیقه؛ حبیبی، آرش (۱۳۹۳) "تصمیم‌گیری چند معیاره فازی" انتظارات سیمای دانش، آذر: رشت.
۶. فتاحی، مختار (۱۳۹۷) "بررسی عناصر تشکیل دهنده مادی و معنوی مصادیق جرایم رایانه‌ای" قانون یار، دوره ۲، شماره ۶، صص ۹۹ تا ۱۲۰.
۷. قربانی، ابراهیم؛ (۱۳۹۸) "تحلیل نقش ابعاد وب تارک در گسترش جرائم مواد مخدر و روان‌گردان در فضای سایبر" [فصلنامه 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 تارک از فعالیت مردم تا حضور دولت‌ها" ششمین کنفرانس بین‌المللی وب پژوهی، جهاد دانشگاهی، دانشگاه علم و فرهنگ، دوره ۶.](#)
۹. کتانچی، الناز؛ پورقهرمانی، بابک؛ (۱۳۹۸) "سیاست‌های نمادین معاهده جرایم سایبری شورای اروپا" فصلنامه مطالعات بین‌المللی، سال ۱۶، شماره ۲ (۶۲)، صص ۳۱-۴۷.
۱۰. کرد علیوند، روح‌اله؛ میرزایی، محمد (۱۳۹۷) "گونه‌شناسی جرایم سایبری با نگاهی به قانون جرایم رایانه‌ای و آمار پلیس فتا" حقوق دادگستری، دوره ۸۲، شماره 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-Héту, 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-Héту, 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., Kermitis, 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).