JCWR2020

Describing General Atmosphere of the Dark Web from People's Activities to the Presence of Governments

Fatemeh Ghanad [1], Sajad Eslamian Koupai [2]

[1]Associate Professor, University of science and culture, Tehran, Iran
ghanad@usc.ac.ir

[2] Master of Electronic commerce Law, University of science and culture, Tehran, Iran
eslamian.sajad@gmail.com

Abstract

The dark web has the potential to host an increasingly high number of legal and illegal activities ranging from maintaining privacy to selling illegal goods, mainly purchased with Bitcoin or other digital currencies. They may be used to circumvent censorship, access blocked content, or maintain the privacy of sensitive communications or business plans. However, a range of malicious actors, from criminals and terrorists to state-sponsored spies, can also leverage cyberspace and the Dark Web can serve as a forum for conversation, coordination and action. It can also be used by governments to shield military personnel and Social change in other countries. It has remained largely unregulated by the government, and the first step in better monitoring and policing the Dark Web is better understanding it.

The topic of describing general atmosphere of the dark web from people's activities to the presence of governments, providing a proper understanding of the dark web, In order to establish effective policies and raising awareness about the formation, onion router working, concept of anonymity, hidden services, active groups and ultimately the presence of governments.

Keywords: Deep Web, Dark Web, Onion Router, TOR, Hidden Services, Government Oversight, Criminal Activity.

JCWR2020
کنفرانس بین المللی وب پژوهی
ایران، تهران، ۲۶ خرداد ۱۳۹۹

شرح فضای کلی حاکم بر وب تاریک از فعالیت مردم تا حضور دولت‌ها

فاطمه قناد[۱]، سجاد اسلامیان کوپائی[۲]

[۱] دانشیار گروه حقوق، دانشگاه علم و فرهنگ ، تهران
ghanad@usc.ac.ir

[۲] دانشجوی کارشناسی ارشد ، حقوق تجارت الکترونیکی ، دانشگاه علم و فرهنگ ، تهران
eslamian.sajad@gmail.com

چکیده

وب تاریک، فعالیت‌ها و خدمات مجرمانه و شرارت‌بار و به عبارتی بسیاری از فعالیت‌های جنایی را از هدایت شبکه‌های تروریستی و تجارت مواد مخدر، سلاح و جنگ افزار تا افشای اطلاعات محرمانه، جعل و دزدی هویت، انجام تراکنش‌های مالی غیرقانونی میزبانی می‌کند. وب تاریک قابلیت ناشناس ماندن قابل توجهی دارد از این رو علاوه بر شمار بسیار بزهکاران، تعداد زیادی از طرفداران آزادی بیان و کاربران عادی اینترنت را که از نقض حریم خصوصی و اطلاعات شخصی خود نگران هستند، به سوی خود فرامی‌خواند و دولت‌های فرصت طلب را در جاسوسی اطلاعات و ایجاد تغییرات اجتماعی، فرهنگی و حتی سیاسی در سایر کشورها یاری می‌دهد. با توجه به ویژگی‌های یاد شده، شناسایی و فهم بهتر این دنیای ناشناس و معرفی مجموعه‌های فعال در وب تاریک برای دولت‌ها فوق‌العاده با اهمیت تلقی شده و شناخت هرچه بیشتر آن‌را ضروری می‌نماید.

مقاله حاضر در صدد است با تبیین و توصیف فضای کلی حاکم بر وب تاریک، چگونگی ساختاربندی و جریان سازی فعالیت مردم تا ساماندهی نظام‌مند تحت نظارت دولت‌ها را مورد بررسی قرار دهد و ضمن ارائه شناخت و فهمی صحیح از وب تاریک برای وضع سیاست‌های موثرکه مقدمه‌ای بر افزایش آگاهی‌ها و تدقیق عملکردهاست، با بهره گیری از رویکرد توصیفی و تحلیلی، چگونگی و فرایند شکل‌گیری و عملکرد شبکه ناشناس‌ساز و سرویس‌های پنهان آن با استفاده از مدل مسیریابی پیازی (تُر) را مورد بررسی قرار می دهد و در نهایت تنوع گروه‌های فعال و راهکارها و ابزارهای قانونی منتج از حضور دولت‌ها را تبیین می‌نماید.

کلمات کلیدی

وب پنهان، وب تاریک، شبکه مسیریابی پیازی، تُر، سرویس‌های پنهان، نظارت دولتی، فعالیت مجرمانه

۱- مقدمه

بسیاری از کاربران تصور می‌کنند هنگام جستجوی مطلبی در گوگل[۱]، جستجو در تمامی صفحات وب انجام می‌شود؛ اما واقعیت این است که جستجو فقط در سطح ابتدایی از لایه‌های مختلف موجود در دریای بیکران اطلاعات صورت می‌گیرد. بدین معنا که بقیهٔ اطلاعات در سطوح عمیق‌تری از وب قرار دارد و از آن با تعابیری چون «وب عمیق»، «شبکه غیرقابل رویت» و «شبکه زیرین» یاد می‌شود. این بخش از اینترنت خارج از دسترس مرورگرهای عادی وب قرار دارد، بنابراین با توجه به قرابت معنایی و ارتباط با مفهوم اصلی، آن‌را «وب پنهان[۲]» می‌نامیم.

وب تاریک[۳] بخشی از وب پنهان است که دستیابی بدان از طریق مرورگرهای عادی وب امکان‌پذیر نیست. ویژگی بارز این شبکه تاریک، ناشناس و غیرقابل رؤیت بودن آن است؛ به‌نحوی که افراد در آن ناشناس و خارج از کنترل دولت‌ها باقی می‌مانند.

دسترسی به وب تاریک با استفاده از موتورهای جستجوی مخصوص مانند تُر[۴] که بر مبنای شبکه مسیریابی پیازی[۵] طراحی شده است؛ صورت می‌گیرد. این شبکه با استفاده از تکنولوژی رمزنگاری ارتباطات، شکل کاربرپسندی دارد و استفاده از آن سخت نیست. کاربران برای دسترسی به سایت های وب تاریک به آدرس تُر منحصر به فرد آن سایت با پسوند (.onion) نیاز دارند.

اگرچه بیشتر جابجایی و ترافیک داده ها در وب تاریک بـه فعالیـت‌هـای مجرمانه شامل خرید و فروش مـواد مخـدر، سـلاح، صـور قبیحـه و مبتـذل، سوءاستفاده جنسی از کودکان، استخدام هکرها یا آدمکش‌هـا، جعـل، خریـد و فروش اطلاعات کارت‌های اعتباری، پولشویی ونظـایر آن اختصـاص دارد امـا لزوما همه‌ی کاربران اهداف غیرقانونی برای دسترسی به وب تاریک ندارند. در کشورهایی که مردم دسترسی آزاد به اینترنت ندارند یا سانسـور دولتـی بسـیار شدید است معمولا از تُر بـرای مـرور و جسـتجوی وب سـطحی بـه صـورت ناشناس یا به‌عنوان ابزاری برای آزادی بیـان، حفاظـت از حـریم خصوصـی و جلوگیری از تجزیه و تحلیل اطلاعات؛ توسط دولت‌ها و نیز باز نشـر و تحلیـل اطلاعات توسط شرکت‌های تبلیغاتی استفاده می‌شود.

بعلاوه برخی دولت‌ها برای پیشبرد اهـداف جاسوسـی و ایجـاد تغییـرات اجتماعی، فرهنگی یا سیاسی در سایر کشورها از شبکه مسیریابی پیـازی (تُـر) بهره برده و جنبش‌های اجتماعی را به استفاده از این ابزار تشویق می‌کنند. در مقابل دیده می شود که نهادهای قانونی کشورهای هدف نیز نسبت به قابلیت ناشناس ماندن و عدم قابلیت رهگیری داده‌ها در این شـبکه؛ حسـاس بـوده و شدت عمل بیشتری نشان می‌دهند. گروه اول ملاحظات مربوط بـا حمایـت از آزادی بیان و گردش آزاد اطلاعات را هدف اصلی اقدامات خود اعلام می‌کنند و گروه دوم بر لزوم حفظ امنیت و تمامیت ارضی و استقلال داخلی تاکید دارند.

با در نظر گرفتن چالش‌های فوق، هدف این مقاله توصیف فضـای کلـی حاکم بر وب تاریک و تبیین چالش های حقوقی مرتبط با آن است.

پیشرفت فناوری وضع قوانین جدید را ایجاب می‌کند و از آن‌جـا کـه وب تاریک برای اغلب سیاستگذاران و متولیان سیاست جنـایی جوامـع موضـوعی کاملا جدید است، کسب آگاهی و تجربیات در این فضا را به‌عنـوان مقدمـه‌ای بر وضع قوانین و سیاستگذاری‌ها ضروری مـی‌نمایـد. تنهـا ۲۵ سـال از خلـق دنیای گستردهٔ وب گذشته و در حالی‌که تمام ابعاد زندگی بشر را فرا گرفتـه او را با یکی از بزرگترین چالش‌های حیات خود یعنی نظارت بر ارتباطات، نقـض حریم خصوصی و حق بر دسترسی و گردش آزاد اطلاعات مواجه کرده اسـت. در این میان، گسترش اختیارات نهادهای نظارتی و توسعه مفاهیم مربـوط بـه بازرسی داده‌های در حال انتقـال، کـاربران را وادار سـاخته تـا بـه اسـتفاده از تکنولوژی‌های رمز ارتباطات نظیر شبکه مسیریابی پیازی (تُر) روی بیاورند و از این طریق امکان ناشناس ماندن داشته باشند.

با در نظر گرفتن مطالب فوق، در این پژوهش نخست مفهوم وب تاریک و شبکه مسیریابی پیازی؛ که به اختصار تُر نامیده می‌شـود، تبیـین مـی شـود. سپس، عوامل موثر در رشد و توسعه وب تاریک شامل قابلیت ناشناس مانـدن و سرویس‌های پنهان مطرح می‌گردد. در بخش پایانی در قالب دو بخش تحت عنوان مبانی حقوقی و جلوه‌های عام حضور دولت ها ضمن معرفی گروه‌هـای فعال در وب تاریک، وضعیت حضور کنترلی و تقابلی دولت‌هـا، ؛ بـا توجـه بـه حمایت‌های ایالات متحده از تُر مورد بررسی قرار می گیرد.

۲- شکل‌گیری وب تاریک

شکل‌گیری وب تاریک در دو بخش شبکهٔ گسـترده جهـانی و معرفـی شـبکه مسیریابی پیازی که به اختصار، تُر نامیده می‌شود؛ مورد بررسـی قـرار خواهـد گرفت.

۲-۱- شبکه گسترده جهانی[۶]

اینترنت مجموعه‌ای از شبکه‌های بسیاری است که از اتصال رایانه ها، سرورها و یا هر دستگاه دیگری به‌یکدیگر ایجاد شده و یک شبکه مسـتقل را تشـکیل می‌دهد. اتصال شبکه ها در اینترنت ازطریق شـبکه گسـترده جهـانی صـورت می‌گیرد و به دو بخش وب سطحی یا آشکار[۷] و وب عمیق یا پنهـان[۸] تقسـیم می‌شود [5].

وب سطحی بخش کوچکی از اینترنت (در معنای عام) را تشکیل می‌دهد که در آن محتوای سایت‌ها به‌راحتی توسط موتورهای جسـتجو ماننـد گوگـل، یاهو و... فهرست می‌شود و دسترسی به آن‌هـا توسـط مرورگرهـای اسـتاندارد صورت می‌گیرد، درحالی‌که محتوای وب پنهان که ۹۰ درصد حجـم انتقـال و ترافیک داده ها را به خود اختصاص می‌دهد توسط موتورهـای جسـتجو قابـل طبقه بندی محتوایی و موضوعی نیست [6]. داده‌های اصلی سایت‌هایی مانند: Facebook، twitter، snap chat و به‌طور کلی هرآن‌چه توسط رابط‌هـای برنامه نویسی[۹] مـی‌تـوان بـه آن دسترسـی پیـدا کـرد، هـم چنـین داده‌هـای پیام‌رسان‌های فوری[۱۰]، سرویس‌های اشتراک فایل[۱۱] ماننـد Google drive و یا drop box همه در وب پنهان قرار می‌گیرد. از این روسـت کـه محققـان اندازه وب پنهان را چهار تـا پـنج هـزار برابـر بزرگتـر از وب سـطحی بـرآورد می‌کنند [7].

درون وب پنهان، یک فضای مخفی شده به نام وب تاریک وجـود دارد، که از طریق روش‌های استانداردِ مرور وب، قابل دسترس نیست. این فضا کـه بر مبنای شبکهٔ مسیریابی پیازی توسعه یافته، متشکل از وب‌سایت‌های اسـت که برای عموم قابل مشاهده‌اسـت امـا آدرس آی‌پـی آن‌هـا مخفـی و پنهـان می‌باشد. کاربران به کمک موتورهای جستجوی معمول نخواهند توانست ایـن سایت‌ها را جستجو و پیدا کنند، بلکه با نرم‌افزارهای خاص، تنظیمات ویژه و یا حتی در برخی موارد تنها با داشتن نشانی وب که عموما از پروتکل‌های عادی تبعیت نمی‌کند؛ می‌توانند به این وب‌سایت‌ها دسترسی داشته باشـند. دادوسـتد در این دامنه‌های مخفی از طریق ارز رمز نگاری شده یـا بیـت‌کـوین و بـدون کنترلی قانونی بر روی آن؛ انجام می‌گیرد. بیشتر سایت‌های این بخش از وب، از نرم‌افزار مخصوصِ رمز ارتباطات مانند تُـر اسـتفاده مـی‌کنـد و افـراد در آن ناشناس و خارج از کنترل دولت‌ها باقی می‌ماننـد بـه‌نحـوی کـه پیـدا کـردن جزئیات سِروِری که سایت مربوطه روی آن اجرا می‌شود و ردیابی هاست و یـا همان میزبان آن دشوار است.

۲-۲- شبکه مسیریابی پیازی[۱۲] (TOR)

استفاده از شبکه مسیریابی پیازی (چندلایه) که اصطلاحا تُر نامیده مـی‌شـود؛ محبوب‌ترین روش برای ورود به وب تاریک می‌باشد و بیشتر وب‌سـایت‌هـای وب تاریک برای مخفی کردن هویتشان از ابزار رمزگذاری تُر استفاده می‌کنند. به‌همین دلیل در این بخش با هدف آشنایی با شبکه مسیریابی، ابتدا تاریخچه و سپس نحوه عملکرد و رمز ارتباطات در آن بررسی می‌شود.

۲-۲-۱- تاریخچه

در زمان ریاست جمهوری کلینتون[۱۳] (۱۹۹۰) دولت ایالات متحده بـه اهمیـت حفاظت از ارتباطات آنلاین نیروهای خود در برابر جاسوسی سایر کشورها پـی برده بود، بنابراین با طراحی شبکه مسیریابی پیازی (چند لایه) به رهبـری پـل سایورسون[۱۴] در مرکز تحقیقات نیروی دریایی ایـالات متحـده[۱۵]، سیسـتمی را طراحی کرد که می‌توانست در سرتاسر دنیا و بدون نیاز به هیچ سـخت‌افـزاری علاوه بر محتوای داده؛ مبدأ و مقصد آن‌را رمز کند. نهایتا این مرکز بـا هـدف پنهان‌سازی انتقال و ترافیک داده‌های نیروهای خود در میان انتقال وترافیـک داده‌های کاربران عادی؛ شبکه تُر را در اکتبر ۲۰۰۳ بـه عنـوان یـک مرورگـر عمومی آزاد[۱۶] و رایگان[۱۷]، عرضه کرد چرا که به اصطلاح "هیچ‌کس نمی‌تواند روی ملک خود ناشناس بماند. [8]"

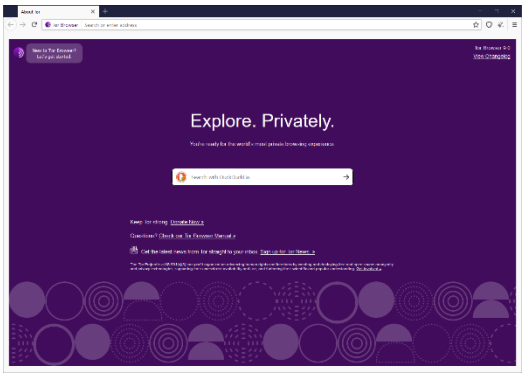
این شبکه درابتدا به‌عنوان ابزاری برای فرار از ردیابی آنلایـن نیـروهـای امنیتی طراحی شده بود اما به مرور زمان مورد توجه گروه‌های مختلفـی قـرار گرفت که با اهداف گوناگون بروزرسانی و توسعه آن‌را دنبال می‌کنند و ازسوی نهادهای دولتی مانند وزارت خارجه و دفاع ایالات متحده و همچنین موسسات غیرانتفاعی در اروپا و آمریکا حمایت می‌شوند. یکی از ایـن موسسـات بـه‌نـام پروژهٔ تُر[۱۸] از سال ۲۰۰۶ نسخه‌های به‌روز شده مرورگر تُر را دراختیار کـاربران قرار می‌دهد و با حمایت‌های مالی بنیاد ملی علوم ایالات متحده در توسعه این شبکه نقش مهمی را ایفا می‌کنـد. در شـکل (۱) و (۲) بـه‌ترتیـب جدیـدترین نسخه‌های ویندوز و اندروید این مرورگر را مشاهده می‌کنید.

۲-۲-۲- نحوه‌عملکرد و رمز ارتباطات

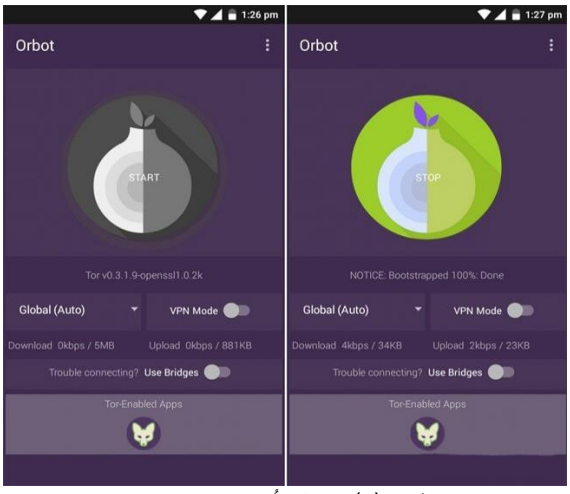
تُر داده‌های کاربران را از میان تعدادی رله یـا بـازپخش کننـده[۱۹] در سرتاسـر جهان که به‌صورت داوطلبانه اداره می‌شود؛ عبور داده و به مقصد می‌رساند. به مجموعه بازپخش کننده‌های انتخاب شده برای عبور داده، مسیر[۲۰] مـی‌گوینـد. با توجه به رمزگذاری‌های انجام شده بر روی داده‌ها، هـر بـازپخش کننـده در مسیر فقط گره قبلی و بعدی خود را مـی‌شناسـد. از آن‌جـا کـه تنهـا رلـه اول مستقیما با کاربر و تنها رله آخر مستقیما با مقصد در ارتباط است؛ چنانچه تعداد بازپخش‌کننده‌های مسیر سه و یا بیشتر باشد، ارتباط بین مقصد و مبدأ پنهـان مانده و ناشناس ماندن برای کاربر فـراهم خواهـد شـد [۱]. هـر درخواسـت[۲۱] حداقل توسط سه لایه رمز احاطه می‌شود و با عبور از نقاط رله، هر لایه از رمز تا رسیدن به مقصد حذف می‌گردد، برای همین عنوان مسیریابی پیازی بـرای آن به‌کار می‌رود. نتیجه آن‌که این فرایند، مـانع افشـای هویـت ارسـال‌کننـدهٔ اصلی پیام می‌شود و اطلاعات ارسال‌کننده یا اصل ساز ناشناس باقی می‌ماند. شکل (۳) نحوه رمز ارتباطات در شبکه مسیریابی را به نمایش گذاشته است.

۳- رشد و توسعه وب‌تاریک

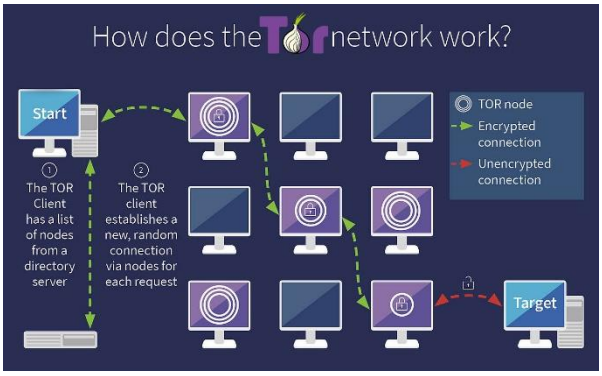
وب تاریـک در طـول زمـان بـر مبنـای قابلیـت‌هـای ناشـناس مانـدن[۲۲] و سرویس‌های پنهان[۲۳] توسعه پیـدا کـرده اسـت. هـر یـک ایـن ویژگـی‌هـا در شکل‌گیری فعالیت‌ها و گروه‌های فعال نقـش اساسـی دارد کـه بـه آن اشـاره خواهد شد.



شکل (۱): مرورگر تُر نسخه ویندوز



شکل (۲): مرورگر تُر نسخه اندروید



شکل (۳): نحوه رمز ارتباطات در شبکه مسیریابی [9]

۳-۱- قابلیت‌های ناشناس ماندن

در محیطی که یک‌سری مولفه در استفاده از یـک سـرویس مشـترک‌انـد، بـا فرض این‌که جمع مولفه‌ها را یک مجموعه ناشـناس بنـامیم، ناشـناس بـودن به‌صورت توانایی عدم‌تمیز و شناخته شدن در بین اعضای این مجموعه تعریف می‌گردد. به عبارت دیگر با از بین بردن ارتباط یک فعالیت با مولفه‌ای کـه آن را انجام داده است، گمنامی و ناشناس بودن حاصل می‌شود [۱].

تُر با فراهم‌کردن ویژگی مذکور ابزار دسترسی ناشـناس‌گونـه بـه شـبکه فعلیِ نِت می‌باشد و پراستفاده‌ترین ابزاری است که هرروز بالغ بر نـیم میلیـون

کابر در سرتاسر جهان از قابلیت‌های ناشناس بودن و عدم‌رهگیری آن بهره‌می‌برند [۵].

استفاده از ویژگی ناشناس‌بودن شبکه تُر ، دسترسی به موارد غیراخلاقی و مجرمانه تا موارد مربوط به حریم خصوصی کاربران را دربر می‌گیرد. این امور در بسیاری از موارد باعث رخداد اعمال بسیار ناخوشایندی است. در دسترس قراردادن مفاد غیراخلاقی نامتناسب با فرهنگ کشورها و یا حتی استفاده از این شبکه برای فروش مواد مخدر و یا اسلحه و حتی سازماندهی اقدامات تروریستی از تهدیداتی است که کاربران با آن مواجه هستند و از این رو دولت‌ها تمایل دارند که با امکان گمنام بودن در اینترنت مقابله کنند.

۳-۲- سرویس‌های پنهان

شبکه تُر علاوه بر امکان برقراری ارتباطات گمنام، برمبنای سرویس‌های پنهان توسعه پیدا کرده‌است. از جمله این سرویس‌ها می‌توان به ویکی پنهان[۲۴]، موتورهای جستجوی خاصِ تُر مانند Ahmia و Grams و بیت کوین[۲۵] اشاره‌کرد. هرکدام از این سرویس‌ها با افزایش قابلیت دسترسی به تُر، در توسعه و پیشرفت وب تاریک نقش کلیدی ایفا می‌کند.

ویکی به سایت‌هایی گفته می‌شود که به تمام بازدیدکنندگان خود اجازه ویرایش، افزودن یا حذف یک مطلب را می‌دهد. ویکی پنهان نیز یک ویکی مخفی و مقاوم دربرابر سانسور است که به‌صورت یکی از سرویس‌های تُر اداره می‌شود. این ویکی درشرایط فقدان موتورهایِ جستجویِ خاصِ تُر، در سال ۲۰۰۴ با فراهم کردن فهرستی از تمام وب‌سایت‌های وب تاریک؛ اولین موج از کاربران را برای این سایت‌ها به ارمغان آورد [5].

علاوه بر ویکی پنهان موتورهای جستجوی خاصِ تُر مانند Ahmia و Grams، کاربران را در یافتن سایت‌های وب تاریک یاری می‌دهد. این موتورهای جستجو مانند Grams صرفا به فهرست محتوای مجرمانه سایت‌های وب‌تاریک می‌پردازد و در مقایسه با ویکی پنهان کاربرد محدودتری دارد [7].

برای انجام معاملات در این شبکه نیز بیت کوین به‌عنوان ارز رایج در وب تاریک استفاده می‌شود. این رمزارز در سال ۲۰۰۹ و از همان ابتدای پیدایش، به ارز استاندارد در وب تاریک تبدیل شد. طراحی بیت‌کوین به نوعی است که رهگیری فردی که آن‌را خرج می‌کند را غیرممکن می‌سازد و فقط شناسه‌های کیف پول‌های دیجیتال[۲۶] است که در یک log عمومی ثبت می‌شود.

گسترش وب‌سایت‌های مجرمانه وب‌تاریک تا حد زیادی مدیون گسترش بیت‌کوین و سایر رمزارزهای مشابه مانند Zerocoin است که قابلیت‌های عدم رهگیری و ناشناس ماندن بیشتری را فراهم می‌کند [8].

۴- گروه‌های فعال در وب‌تاریک

از تُر می‌توان هم برای اهداف قانونی و هم برای اهداف مجرمانه و غیرقانونی استفاده کرد. در حالی که بیشتر کاربران از این شبکه برای حفظ حریم خصوصی خود و رد شدن از قوانین پالایش داده ها و فیلترینگ سازمان‌ها و یا حتی کشورها استفاده می‌کنند؛ ویژگی های خاص تُر آن‌را به محل فعالیت گروه‌های مختلفی از حامیان آزادی بیان، مجرمان اینترنتی و گروه‌های تروریستی تبدیل کرده است.

در ادامه انواع گروه‌های فعال و نحوه فعالیت آن‌ها مورد بررسی قرار می گیرد:

۴-۱- حامیان آزادی بیان، آزادی اینترنت و حریم خصوصی

تُر محل فعالیت گروه‌های مختلفی از خبر چینان[۲۷] و نفوذگران [۲۸] است که با رخنه در بخش‌های حکومتی خود را ناظر بر دموکراسی و حق اطلاع مردم دانسته و با هدف دسترسی آزاد اطلاعات و آزادی بیان، منابع و اقدامات مخفی دولت‌ها را افشا می‌کنند.

برای نمونه در سال ۲۰۱۰ یک سرباز آمریکایی اسناد محرمانه جنگ عراق را از طریق شبکه تُر در ویکی‌لیکس منتشر کرد و از اقدامات ارتش آمریکا در عراق پرده برداشت [10]؛ همچنین یک برنامه‌نویس به نام آرون شوارتز[۲۹] درسال ۲۰۱۱ دسترسی آزاد و رایگان مردم به اسناد الکترونیکی دادگاه‌های ایالات متحده موسوم به PACER[۳۰] را ممکن ساخت و با انتشار داده‌های پایگاه JSTORE اقدامات بسیاری درجهت دسترسی آزاد به مقالات و پژوهش‌های دانشگاهی انجام داد [11].

گروهی دیگر نیز تحت عنوان سایفرپانک‌ها[۳۱] در تُر فعالیت می‌کنند. این گروه از دهۀ ۱۹۹۰ با اندیشه نابودی حاکمیت دولت‌ها در کنترل و نظارت اینترنت، قصد دارند تا رمزگذاری را بر تمام ارتباطات حاکم نموده و با طراحی ابزارهای رمز ارتباطات، شیوۀ کار اینترنت را تغییر دهند. در میان این گروه، عده‌ای با تفکرات آنارشیستی خود به اقدامات مانند انتشار روش ساخت سلاح با استفاده از پرینترهای سه‌بعدی و هدایت آشوب‌ها علیه دولت و امنیت عمومی می‌پردازند [12].

۴-۲- مجرمان اینترنتی و بازارهای وب‌تاریک

تنها ۱/۵ درصد کاربرانِ تُر، سایت‌های مجرمانه وب تاریک را دنبال می‌کنند. با این وجود، بیش‌از ۸۰ درصد ترافیک این فضا به خرید و فروش مواد مخدر، سلاح و جنگ افزار، صور قبیحه و مبتذل، سوءاستفاده جنسی از کودکان، استخدام نفوذگران(هکرها) و یا آدمکش‌ها، جعل، خرید و فروش اطلاعات کارت‌های اعتباری، پولشویی و... اختصاص دارد [13].

سایت‌های خرید و فروش مواد مخدر بخش جدایی ناپذیر بازارهای وب تاریک را تشکیل می‌دهند. این سایت‌ها که موفقیتشان نتیجۀ ترکیب ابتکاری از تُر و بیت کوین می‌باشد، بیشترین سابقۀ مرور در وب تاریک را دارند [13].

اولین و بزرگترین سایت غیرقانونی وب تاریک جاده ابریشم[۳۲] می‌باشد. پلتفرم جاده ابریشم برای فروشندگان، در مقابل پرداخت حق کمیسیون؛ عرضه انواع مواد مخدر، سلاح و به‌طور کلی هرآن‌چه قابلیت فروش آنلاین دارد را فراهم می‌کند. اگرچه FBI در اکتبر ۲۰۱۳ مدیر جاده ابریشم را بازداشت کرد ولی بعد از دوماه تعطیلی، مجددا بر پایه همان کد و بدون هیچ تغییری؛ راه اندازی شد. معاملاتی که در این سایت صورت می گیرد، با ارزشی بیش از ۱/۲ میلیارد دلار؛ مدلی جدید از کسب و کارهای اینترنتی مبتنی بر سود با ریسک

پایین ارائه می‌نماید که خطر شناخته شدن هم در آن وجود ندارد. این ویژگی به سایر سایت‌های مجرمانه وب تاریک نیز قابل تسری است [5].

٤-۳- گروه‌های تروریستی

اینترنت و رسانه‌های اجتماعی با تحول در عرصه ارتباطات و فناوری اطلاعات[۳۳] به افراطیون و تروریست‌ها کمک کرده است که یک جنبش اجتماعی جهانی ایجاد کنند. در این میان وب تاریک یک ابزار سریع، ارزان و ناشناس به گروه‌های افراطی ارائه می‌دهد و به‌عنوان یک شیوه ایده‌آل برای انتشار اطلاعات و تبلیغات عمل می‌کند.

مارک سیجمن[۳۴] در کتاب خود با عنوان «جهاد فاقد رهبری» که در سال ۲۰۰۷ منتشر شد چنین توصیف می‌کند: «فرایند افراط‌گرایی که تروریست‌ها در محل زندگی دشمنان ایجاد می‌کنند از طریق اتصال به اینترنت به سمت یک شبکه جهانی غیرمنسجم و نهایتا جهاد فاقد رهبری، هدایت می‌شود» [۲].

وی از میان‌یافته‌هایش دریافت تا قبل از سال ۲۰۰۴، تعاملات چهره به چهره میان اعضای گروه‌های تروریستی که به طور متوسط ۲۶ سال سن دارند رایج‌تر است؛ درحالی‌که بعد از سال ۲۰۰۴، بیشتر تعاملات از طریق سایت‌های وب تاریک میان اعضایی با متوسط سن ۲۰ سال صورت گرفته و عضوگیری چهره به چهره کاهش یافته است [۲].

تروریست‌ها در قالب شبکه های تاریک، جان و مال مردم و امنیت کشورها را در معرض خطر و تهدید قرار داده اند. دو عامل خصومت با محیط و واکنش و اقدامات متقابل در برابر عوامل خارجی مانند نیروهای پلیس و تلاش در مخفی نگه داشتن شبکه از طریق هماهنگی امن کارها و فعالیت ها نقش تعیین کننده در حیات آن‌ها ایفا می کند[۳].

بنابراین تُر با کاهش سطح واکنش و رهگیری توسط نیروهای پلیس، مخفی نگه داشتن شبکه و تسهیل فرایند عضوگیری، تبلیغ هدفمند و ترویج ایدئولوژی و نیز تامین کمک‌های مالی برای گروه‌های تروریستی را ممکن ساخته است.

۵- حضور دولت‌ها در وب‌تاریک

حضور دولت‌ها در وب تاریک ابعاد مختلفی دارد. ابتدا لازم است مبانی حقوقی حضور دولت‌ها در وب تاریک مطرح شود و طی آن سیاست‌های مبهم و متفاوت دولت‌ها در معنای عام، مورد بررسی قرار گیرد و سپس درباره اقدامات جاسوسی و تغییرات اجتماعی به‌عنوان جلوه‌های عام فعالیت دولت‌ها در وب تاریک توضیحاتی ارائه شود.

۵-۱- مبانی حقوقی حضور دولت‌ها در وب تاریک

مبانی حقوقی حضور دولت‌ها در وب تاریک از دولتی به دولت دیگر متفاوت و گاه مبهم است. آلمان و ایالات متحده از تُر حمایت و در تحقیقات مربوط به آن سرمایه گذاری می‌کنند. چین با بهره‌گیری از دیوار آتش بزرگ خود[۳۵] دسترسی‌ها به شبکه تُر را محدود کرده است. دولت روسیه نیز از آن‌جا که ناشناس ماندن افراد در اینترنت را به رسمیت نمی‌شناسند، به‌دنبال امکان سنجیِ جمع آوریِ اطلاعاتِ کاربرانِ شبکه‌های ناشناس مانند تُر و تجهیزات فنی آن می‌باشد. اتریش به‌موجب رویه قضایی، راه‌اندازی هرگونه رله خروجی برای شبکه تُر را بالقوه جرم می‌داند. به موجب قوانین ایالات متحده که مسئولیت اقدامات کاربران یک سیستم یا ابزار رایانه ای، قابل تسری به اداره‌کنندگان یا کسانی که آن سیستم را راه‌اندازی کرده‌اند نیست [5,14]. در این میان جایگاه مبهم کشورهایی نظیر ایران در برابر استفاده شهروندان از این شبکه و به‌طور کلی واکنش‌ها دربرابر ناشناس ماندن در اینترنت نیز قابل توجه است.

براساس آمارهای سایت Tor Metrics تعداد کاربرانی که با استفاده از رله‌های عمومی از ایران به تُر متصل شده‌اند به ۲۵ هزار اتصال در روز می‌رسد. همچنین ایران با بیش از ۹۵ هزار اتصال، روزانه بیشترین تعداد کاربر را در اتصال به اینترنت از طریق bridges دارد و به‌دلیل افزایش فیلترینگ، بیشترین تعداد کاربرانِ تُر را که از آن به‌عنوان وی‌پی‌ان استفاده می‌کنند به خود اختصاص داده است. این درحالی است که در ایران اتصال به تُر و استفاده از bridges که نوعی اتصال خصوصی به شبکه مسیریابی می‌باشد جرم‌انگاری نگردیده و در هیچ یک از قوانین، موضوع ورود به سایت‌های وب تاریک یا عضویت در آن‌ها جرم تلقی نشده وهیچ‌گونه اقدام تقنینی و یا قضائی درباره آن یافت نمی‌شود. بنابراین علاوه بر کاربران تُر، اداره کنندگان رله‌های آن نیز مجرم محسوب نمی‌شوند. از طرف دیگر حق بر ناشناس ماندن در اینترنت که یکی از عناصر اصلی حریم خصوصی می‌باشد به‌رسمیت شناخته نشده و متاسفانه فقدان نظام جامع حمایت از داده‌ها در ایران احساس می‌شود. سایر موضوعات مانند حمایت‌های قانونی از افشاگران فساد و ریاکاری‌های عمومی و یا پیش‌بینی کمیته‌های نظارت بر تحلیل داده نیز بر ابهام وضعیت حقوقی ایران دربرابر این شبکه می‌افزاید.

دولت‌ها در فضای وب همواره با دو چالش به رسمیت شناختن حق بر ناشناس بودن افراد[۳۶] و حق بر امنیت کامل ورود و خروج اطلاعات شهروندان، مواجه هستند. آن‌ها در عین حال که متعهد به حمایت از آزادی بیان در اینترنت می‌باشند از شرکت‌های بزرگ اینترنتی می‌خواهند، امکان دسترسی به داده‌های خصوصی و ارتباطات رمزگذاری شدهٔ شهروندان را با تعبیه در پشتی[۳۷]؛ روی سیستم‌ها و شبکه‌های خود فراهم کنند. در این میان، مردم مجبور به استفاده از تکنولوژی‌های رمز ارتباطات مانند تُر می‌باشند که ناشناس ماندن آن‌ها را ممکن می‌سازد [5].

بیشتر کاربران تُر برای حفظ حریم خصوصی و با مقاصد قانونی از آن استفاده می‌کنند [5]. نتیجه آن‌که اگر از تُر و به طورکلی وب تاریک هیچ استفاده مجرمانه‌ای نمی‌شد، نهادهای قانونی، نسبت به قابلیت ناشناس ماندن و عدم رهگیری که این شبکه فراهم می‌کند؛ شدت عمل کمتری نشان می‌دادند. در این شرایط واکنش دولت‌های آزادی‌گرا، براساس به رسمیت شناختن حقوق اکثریت کاربران؛ صرفا محدود به مبارزه با موارد مجرمانه می‌باشد و کاری با حق رمز شهروندان و استفاده از تُر ندارند.

دولت‌های آزادی خواه براساس لزوم احترام به حقوق شهروندان و حفظ حریم خصوصی، و با توجه به حکومت در یک جامعهٔ طرفدار آزادی بیان، سعی

بر اتخاذ سیاست هایی برای تضمین آزادی ارتباطات دارند. بنابراین نه تنها اساسا اصل آزادی فعالیت شهروندان در وب تاریک را نفی نمی کنند، بلکه غالبا حمایت از تُر را وظیفه خود شناخته و از لحاظ اقتصادی، مستقیما به آن کمک می‌نمایند. برعکس دولت‌های سانسورگر؛ در نقطه مقابل قرار دارند و بواسطه مخالفتی که با قابلیت ناشناس ماندن و عدم رهگیری کاربران این شبکه دارند، در جایگاه اداره کنندهٔ اینترنت قرار گرفته‌اند [۴].

در جدول (۱) مجموعه‌ای از اقدامات تقنینی و تصمیمات قضائی که به‌صورت مستقیم و یا غیر مستقیم برای کنترل شبکه مسیریابی در سال‌های مختلف اتخاذ شده است را مشاهده می کنید. براساس موارد مذکور در این جدول می‌توان نتیجه گرفت که حتی دولت‌های آزادی‌خواه نیز محدودیت‌هایی بر این شبکه وضع کرده‌اند و با فعالیت‌های مجرمانه در آن به‌شدت مبارزه می‌کنند. همچنین به مرور زمان، ضرورت همکاری‌های بین‌المللی در رهگیری فعالیت‌های مذکور، مساعدت‌های حقوقی متقابل[۳۸] را افزایش داده و همکاریِ مامورین اجرای قانون در خارج از مرزها را به‌عنوان تنها راه فائق آمدن به جرایم وب تاریک گسترش داده است. ازطرف دیگر واکنش دولت‌های سانسورگر نیز توجه بسیاری را به خود جلب می‌نماید. به نحوی‌که خواست آن‌ها بر کنترل کامل ورود و خروج داده از مرزهای اطلاعاتی و عدم کنترل بر شبکه‌های ناشناس مانند تُر، دولت‌هایی مانند چین و روسیه را به‌سوی قطع دسترسی به اینترنت جهانی و ایجاد دیوارهای آتشین بزرگ سوق داده است.

۵-۲- جلوه‌های عام فعالیت دولت‌ها در وب تاریک

جلوه‌های عام فعالیت یک دولت با تمرکز بر اقدامات جاسوسی و تغییرات اجتماعی دولت‌های دیگر را بویژه می‌توان در ایالات متحده آمریکا جستجو کرد؛ چرا که آمریکا با تامین بیش از ۶۰ درصد بودجهٔ تُر بیشترین استفاده از آن را دارد و متحدان خود را به حمایت از آن تشویق می‌کند [12].

۵-۲-۱- اقدامات جاسوسی

در سال ۲۰۰۳ مرکز تحقیقات نیروی دریایی ایالات متحده تُر را به‌عنوان یک مرورگر عمومی آزاد و رایگان عرضه کرد. هدف از این اقدام، دشوار ساختن رهگیری پیام‌های نیروهای امنیتی ایالات متحده در سایر کشورها و پنهان کردن ترافیک متعلق به این نیروها درمیان ترافیک کاربران عادی بود [8].

ایالات متحده با هدف ناشناس ماندن نیروهای امنیتی خود در سایر کشورها و ارسال امن اسناد و اطلاعات از طریق تُر، ضمن تخصیص بودجه، با کمک جوامع آکادمیک و هکرهای داوطلب؛ به توسعه و بروزرسانی شبکه تُر پرداخت و متحدان خود را به حمایت از آن تشویق کرد [15].

همچنین موسسه‌های غیرانتفاعی برای ترویج استفاده از تُر به‌نام حمایت از آزادی بیان و حفاظت از حریم خصوصی به جاسوسی اطلاعات و جمع‌آوری داده در سایر کشورها پرداخته و در پیش‌برد اهداف ایالات متحده نقش اساسی دارند [10].

سایر کشورهای مخالف ایالات متحده مانند چین و روسیه با راه‌اندازی شبکه‌های اینترنت ملی و سامانه‌های فیلترینگ تُر با اقدامات جاسوسی ایالات متحده مبارزه می‌کنند. آن‌ها برای دفاع از امنیت ملی خود، ناشناس بودن کاربران در اینترنت را به رسمیت نمی‌شناسند و قوانین سختی در مورد استفاده از وب تاریک وضع کرده‌اند [5].

۵-۲-۲- تغییرات اجتماعی

از دهۀ ۱۹۹۰، اینترنت نقشی مهم در پیشبرد بسیاری از جنبش‌های اجتماعی داشته است. یک مثال اولیه و مستند استفاده موثر از ارتباط کامپیوتری برای تغییرات اجتماعی جنبش زاپاتیست و ارتش آزادی بخش ملی زاپاتیست‌ها[۳۹] در شورشش برعلیه سرکوب استعماری مردم بومی مکزیک است. این جنبش برای «انتشار اطلاعات، به اشتراک گذاری تجربیات، تسهیل بحث سازماندهی نیروها و شرح و بایگانی تاریخ در حال توسعه مبارزه» از اینترنت و ارتباط کامپیوتری نهایت استفاده را برد. جنبش زاپاتیستا با استفاده از اینترنت و ارتباط کامپیوتری «یک قابلیت جدید برای ارتباط فرامرزی و عمل در سطح فراملی این جنبش و سایر جنبش‌های اجتماعی» را نشان داد و برای سایر جنبش‌ها یک «مدل» درنظر گرفته‌شد. این مدل با پیشرفت اینترنت و ایجاد شبکه تُر برای ایجاد تغییرات اجتماعی و هدایت جنبش‌های آزادی‌خواهانه در کشورهای هدف مورد استفاده دولت‌های مختلف و به‌طور خاص ایالات متحده قرار گرفت [۲].

ایالات متحده و متحدانش به تبعیت از مدل زاپاتیست‌ها با حمایت از تُر، به عنوان یک بستر مناسب برای برقراری ارتباط، انتشار اطلاعات، به اشتراک‌گذاری تجربیات، ایجاد اتحاد و هویت، ترویج، تسهیل و سازمان‌دهی فعالیت جنبش‌های اجتماعی؛ نهایت بهره را می‌برند.

تُر در جریان بیداری اسلامی کشورهای عربی ابزار حیاتی برای مخالفان سیاسی و بیان آزادانه عقائد آن‌ها بود. همچنین در سوریه گروه‌های مخالف اطلاعات خود را با کمک این شبکه منتقل می‌کردند، تا آن‌جا که موسسه endhoven با حمایت دولت ایالات متحده، استفاده از این مرورگر را توسعه داد و دسترسی به آن را تسهیل نمود. در جریان اعتراضات سیاسی سال ۱۳۸۸ و ۱۳۹۸ ایران نیز، معترضین برای عبور از محدودیت‌های دسترسی به اینترنت و تشویق عموم به اعتراض، از تُر و شبکه مسیریابی پیازی استفاده می‌کردند [10]. بنظر می‌رسد که این ابزار، بارها در تغییرات اجتماعی و هدایت افکار عمومی مورد استفاده قرار گرفته است.

ویژگی مذکور حتی ایالات متحده را نیز تحت تاثیر خود قرار داده است. بررسی ها نشان می‌دهد که شکل‌های مختلفی از هک‌گرایی و نافرمانی مدنی الکترونیکی مانند مورد بلاک شدن وب‌سایت پنتاگون توسط تئاتر اختلال الکترونیکی[۴۰] تا واژگون‌سازی فرهنگی[۴۱] وجود دارند [۲].

لازم به ذکر است استفاده گسترده یک جنبش اجتماعی از شبکه تُر جدا از دخالت سایر دولت‌ها، یک فرهنگ سایبری گسترده در اینترنت ایجاد می‌کند که شامل جوامع مجازی بسیاری برای بیان نظرات و معاشرت اعضا است. این ویژگی سیستم‌های اجتماعی غنی و پیچیده‌ای را شکل می‌دهد و حوزه‌های متنوعی برای پژوهش جنبش‌های اجتماعی پدید می آورد [۲].

۶- نتیجه

در این مقاله سعی گردید پس از شرح شبکهٔ تُر و همچنین عوامل موثر

جدول (۱): مجموعه‌ای از اقدامات تقنینی و تصمیمات قضائی در رهگیری فعالیت‌های مجرمانه و یا قطع دسترسی به تُر [3,5,8,11]

سال	کشور	اقدامات تقنینی و تصمیمات قضائی
۲۰۰۱	آلمان	اصلاح قانون G-10 و ایجاد محدودیت‌ها بر محرمانه بودن ارتباطات و ایجاد نظارت مستقیم بر محتوای اطلاعات
۲۰۰۱	آلمان	ارائه الگو و مدل نرم‌افزاری ازسوی وزارت اقتصاد و تکنولوژی آلمان برای خرید ناشناس از سایت‌های وب سطحی با هدف حمایت از اطلاعات شخصی شهروندان
۲۰۰۲	آلمان	وضع قانون ضد تروریسم آلمان و تسهیل دسترسی مقامات دولتی به اطلاعات رمز شده شهروندان
۲۰۰۸	چین	توسعه پروژه دیوار آتشین چین باهدف ایجاد محدودیت‌های دسترسی به مرورگر تُر و نسخه‌های به‌روز آن
۲۰۱۲	آمریکا	راه‌اندازی تکنیک‌های تحقیقاتی شبکه و صدور هوشمند احکام قضائی در شناسایی و رهگیری کاربران سایت کودک آزاری Playpen در وب تاریک
۲۰۱۳	آمریکا	ایجاد رویه برای گسترش استثنائات اصلاحیه چهارم ق.ا نسبت به افشای هویت مجرمان وب تاریک
۲۰۱۳	روسیه	سرمایه‌گذاری بر پروژه امکان‌سنجی جمع‌آوری اطلاعات کاربرانِ شبکه‌های ناشناس مانند تُر و تجهیزات فنی آن
۲۰۱۳	چین	صدور مجموعه‌ای از دستورات سیاسی دولت چین در ممنوعیت نشر خرافات فئودالی و یا برانگیختن تنفر در بین گروه‌های قومی همزمان با ارائه نسخهٔ به‌روز تُر برای این کشور
۲۰۱۴	اتریش	جرم‌انگاری راه‌اندازی هرگونه رله خروجی تُر به موجب رویه قضائی
۲۰۱۴	آمریکا	صدور دستور قضائی برای اداره و کنترل سایت‌های مجرمانه وب تاریک و افشای اطلاعات کاربران درغالب روش‌های مهندسی اجتماعی توسط دولت ایالات متحده
۲۰۱۵	روسیه	شکست پرژه امکان سنجی جمع‌آوری اطلاعات کاربرانِ شبکه‌های ناشناس مانند تُر و تجهیزات فنی آن
۲۰۱۶	روسیه	الزام ارائه دهندگان خدمات اینترنت به استفاده از کلیدهای رمزنگاری داخلی در راستای اجرای قانون ضد تروریسم
۲۰۱۷	ایالات متحده و اتحایه اروپا	امضای موافقتنامه مساعدت حقوقی متقابل در رهگیری فعالیت‌های مجرمانه وب تاریک میان ایالات متحده و اتحادیه اروپا و همچنین دستیابی به اطلاعات نگهداری شده در سرورهای بزرگ اینترنت
۲۰۱۹	روسیه	اجرای قانون حاکمیت اینترنت و شروع فرایند قطع کامل دسترسی به اینترنت جهانی در این کشور

در رشد و توسعه وب تاریک، شناخت‌هایی در زمینه فعالیت گروه‌های مختلف و حضور دولت‌ها در این شبکه صورت گیرد. جدا از موضوع جاسوسی ایالات متحده و ایجاد تغییرات اجتماعی در سایر کشورها، این شبکه تلاش دارد تا با حفظ حریم خصوصی افراد، به ناشناس ماندن آن‌ها در سطح اینترنت کمک نماید. موارد بسیاری وجود دارد که افراد در آن‌ها مایلند بدون افشای نام خود حضور داشته باشند. این دسته از امور شامل بازه وسیعی از فعالیت‌ها می‌باشد. از دسترسی به موارد غیراخلاقی گرفته تا مواردی همچون صحبت‌ها و یا فعالیت‌های مذهبی خاص در کشورهایی که این فعالیت‌ها در آن ممنوع می‌باشد، شرکت در گروه‌های سیاسی و بیان نظرات درباره امور مختلف، افشاگری علیه اقدامات دولت‌ها و حضور در شبکه‌های اجتماعی بدون ترس از حضور آن‌ها، پرسش و پاسخ در مورد موضوعاتی که به‌طور طبیعی افراد تمایلی به بیان آن‌ها ندارند همچون پرسیدن سوال در مورد نشانه‌های یک بیماری خاص و یا امور مربوط به ارتباط با جنس مخالف، سوال‌هایی در موارد علمی، نمونه‌هایی از موارد استفاده از وب تاریک است. دولت‌ها در برابر استفاده از وب تاریک بایستی سیاست‌های موثر اتخاذ کنند. سیاست‌هایی که شناخت صحیح از وب تاریک را ضروری می‌نماید. جایگاه مناسب دولت‌ها در سیاست‌گذاری باید مشخص شود؛ چرا که واکنش دولت‌های تضمین کننده آزادی ارتباطات و دولت‌های اداره کنندهٔ اینترنت متفاوت است.

در سال ۲۰۱۱ با تصویب قطعنامه دفاع از آزادی اینترنت در شورای حقوق بشر سازمان ملل، دسترسی به اینترنت یکی از حقوق اساسی بشر اعلام شده است. دفتر کمیساریای عالی سازمان ملل با انتشار گزارشی، رمزگذاری داده‌های دیجیتال و ناشناس ماندن ارتباطات در دنیای آنلاین را ضرورتی انکارناپذیر برای تامین آزادی بیان و حقی جهان شمول دانسته و از همه دولت‌ها خواسته است تا با حفظ این حق، پاسخگوی مقتضیات عصر دیجیتال باشند. چارچوب قانونی برای حمایت از تحقیقات جنایی و همکاری متقابل کشورها در این فضا ضروری است چرا که تحقیقات، اغلب با نقض گسترده حریم خصوصی اشخاص انجام می‌شود و دولت‌ها از ابزارهایی که در قانون شناسایی نشده؛ استفاده می‌کنند. بنابراین در جایگاه ارائه پیشنهاد، سیاست‌های حاکم بر وب تاریک، ضمن شناخت صحیح از وب تاریک؛ باید بتواند میان حریم خصوصی اشخاص و مسئولیت دولت‌ها بر توقف فعالیت‌های مجرمانه تعادل برقرار کند.

در مورد ایران نیز اگرچه بیشتر استفاده از این شبکه به بحث عبور از فیلترینگ و فعالیت گروه‌های به اصطلاح آزادی‌خواه در خارج از کشور مربوط می‌شود اما ذکر این نکته ضروری است که مجرمان و سازمان‌های جنایی، پیشرفت فناوری‌های اطلاعاتی مانند وب تاریک را مغتنم می‌شمارند و دائما در جست‌وجوی روش‌هایی نوین برای ادارهٔ کارآفرینی خود هستند تا بدین‌وسیله منافع خود را به حداکثر و هزینه‌هایشان را به حداقل برسانند. ایران نیز در مسیر این پیشرفت قرار دارد و در آینده‌ای نزدیک شاهد گسترش ارائه خدمات مجرمانه در بستر امن رمز ارتباطات مانند شبکه تُر خواهد بود. بنابراین سیاست‌گذاران باید با شناخت صحیح از این شبکه، عقب‌افتادگی خود را جبران کنند و ضمن به رسمیت شناختن حق ناشناس ماندن شهروندان، منافع جنایی در وب تاریک را ردیابی نموده و در نهایت، آن‌را از بین ببرند.

مراجع

[۱] توکلی، اصغر، **بهینه‌سازی کارایی پروتکل‌های ارتباطات بی‌نام مبتنی بر شبکه‌های مختلط**، پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر–نرم افزار، دانشکده فنی، دانشگاه گیلان، ۱۳۹۲.

[۲] چن، هین‌چون، **شبکه تاریک: داده‌کاوی تهدیدات پنهان وب**، ترجمهٔ معاونت پژوهش و تولید علم، تهران، موسسه چاپ و انتشارات دانشکده اطلاعات، ۱۳۹۴.

[۳] ایان اس، دیویس، کری إل، ورث، داگلاس دبلیو، زیمون، **شبکه‌های تاریک**، ترجمهٔ پژوهشکده دفاعی و امنیتی دانشگاه جامع امام حسین (ع)، تهران، مؤسسه چاپ و انتشارات، آذر ۱۳۹۷.

[۴] معتمد نژاد، کاظم و رؤیا، **حقوق ارتباطات**، جلد اول: کلیات، تهران، وزارت فرهنگ و ارشاد اسلامی، امور مطبوعاتی و اطلاع رسانی، دفتر مطالعات و توسعه رسانه‌ها، ۱۳۸۸.

[5] Chertoff, Michael, *"A public policy perspective of the Dark Web"*, Journal of Cyber Policy, VOL. 2, NO. 1, 26–38, 13 Mar 2017.

[6] Greenberg, A. *"Hacker Lexicon: What is the Dark Web"*, https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/, 30 August 2016.

[7] Finklea, K. *Dark Web*, Congressional Research Service, R44101, 10 March 2017.

[8] Clemmitt, Marcia.*"The Dark Web: Does identity-masking technology increase cybercrime?"*, CQREAEARCHER, http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2016011500, 30 August 2016.

[9] GDATA Guidebook., *What actually is the darknet?*, Updated 5 August 2019. https://www.gdata.es/guidebook/what-is-the-darknet-exactly

[10] Radford, Mike, *Inside the Dark Web*, bbc Horizon Documentary, Release Date: 3 September 2014.

[11] Knappenberger, Brian, *The Internet's Own Boy: The Story of Aaron Swartz*, Sundance Film Festival Documentary, 20 January 2014.

[12] Winter, Alex, *Deep Web*, Epix network Documentary, Aired on 31 May 2015.

[13] Owen, Gareth and Nick Savage, *"The Tor Dark Net"*, Global Commission on Internet Governance, NO. 20, September 2015.

[14] Tor: Sponsors, 30 August 2019. https://www.torproject.org/about/sponsors/html.en

[15] Going Dark: The Internet behind the Internet, NPR Staff, 25 May 2015. http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet

زیرنویس‌ها

[1] Google
[2] Deep Web
[3] Dark Web
[4] TOR
[5] The Onion Router
[6] World Wide Web (www)
[7] Surface Web
[8] Deep Web
[9] Application Program Interface (API`s)
[10] Instant Messaging (IM)
[11] File Sharing Service
[12] The Onion Router (TOR)
[13] William Jefferson Clinton
[14] Paul Syverson
[15] Naval Research Laboratory (NRL)
[16] Free to Public
[17] Open Source
[18] The Tor Project, Inc.
[19] Relay`s
[20] Rout
[21] Request
[22] Anonymity
[23] Hidden Services
[24] Hidden Wiki
[25] Bitcoin
[26] Digital Wallets
[27] Whistle blowing
[28] Hacktivism
[29] Aaron Swartz
[30] Public Access to Court Electronic Record
[31] Cypher punk`s
[32] Silk Road
[33] Information Communication and Technology (ICT)
[34] Mark Sageman
[35] Great China Firewall
[36] Right to be Anonymous
[37] Backdoor
[38] Mutual Legal Assistance (MLA)
[39] Zapatista
[40] Electronic Disturbance Theater (EDT)
[41] Culture Jamming