فصلنامه علمی مطالعات حقوق بشر اسلامی

دوره ۱۱، شماره ٤، شماره پیاپی (۲۷)، زمستان ۱٤۰۱، ص ۷۳ ـ ۵۱

مقاله پژوهشی **DOR:20.1001.1.23225637.1401.11.4.4.7**

مقابله با جاسوسی سایبری؛ رویکردی آینده پژوهانه در پیشگیری از جرایم تروریستی با نگاهی به اسناد حقوق بشری

نجات امیری[۱]، پیمان نمامیان[۲]

تاریخ دریافت: ۱۴۰۱/۰۸/۲۷ تاریخ پذیرش: ۱۴۰۱/۱۲/۲۵

چکیده:

جاسوسی سایبری یکی از جرایمی است که از طریق فناوری‌های اطلاعاتی و با دستکاری و بهره برداری غیرقانونی و هدفمند اطلاعات به ویژه سرقت و دسترسی غیرمجاز به اطلاعات حیاتی صورت می‌گیرد که عمدتا برای انجام جرایم تروریستی در آینده جمع آوری میگردد، دسترسی غیر مجاز و غیر قانونی به داده‌ها که با هدف جاسوسی سایبری و در آینده به دلیل تحولات پرشتاب محیطی و فناورانه برای وقوع جرایم تروریستی صورت می گیرد، مورد توجه دستگاه های عدالت کیفری و اسناد حقوق بشری قرار گرفته است، از آنجاییکه تحولات فناورانه به ویژه در حوزه‌های امنیتی –انتظامی و جرم شناختی پرداختن به آینده را اجتناب ناپذیر می سازد و تحولات فزآینده عصر حاضر، ناشی از دگرگونی‌های شگفت در حوزه فناوری و روند پر شتاب جهانی شدن ضرورت توجه به آینده و مدیریت تحولات فناورانه در حوزه‌های مطروحه را با کاربست مفاهیم آینده پژوهی امکانپذیر می‌سازد. نتایج تحقیق نشان می‌دهد که دسترسی غیر مجاز به اطلاعات در فضای سایبری که زمینه ساز وقوع جرایم تروریستی که به دلایل بشردوستانه و حقوق بشری، مورد واکنش دستگاه عدالت کیفری و سازمان‌های بین‌المللی قرارگرفته است و ضروری است دستگاه قضایی، انتظامی و سازمان‌های بین‌المللی برای مقابله با جاسوسی سایبری برای پیشگیری از جرائم تروریستی علاوه بر اقدامات فنی –حقوقی با به کارگیری و کاربست مفاهیم آینده پژوهانه نسبت به رصد و شناسایی عناصر اصلی نفوذ و جابه جایی غیر قانونی اطلاعات از طریق فناوری‌های اطلاعاتی اقدام نموده و در پیشگیری از وقوع جرایم تروریستی ناشی از جرایم سایبری نقش آفرینی نمایند.

واژگان اصلی: جاسوسی سایبری، جرایم تروریستی، سرقت اطلاعات، اسناد حقوق بشری، آینده پژوهی.

۱. عضو هیأت علمی دانشگاه علوم انتظامی امین، تهران، ایران

۲. استادیار گروه حقوق دانشکده علوم اداری و اقتصاد دانشگاه اراک، اراک، ایران (نویسنده مسئول)

p-namamian@araku.ac.ir

مقدمه

ترسیم آینده، افراد و سازمانها را قادر می سازد تا سناریوهای مختلفی از آینده را تصـور نمـوده و برای تاب آوری[۱] بیشتر در آینده برنامه ریزی کنند (Gariboldi,at all. 2021). فناوری‌هـای نـوین در برنامه ریزی راهبردی منابع تأثیرگذار است و ضرورت به شناسایی پیشـرانها، تغییـرات و تهدیـدات احتمالی آینده و راهبردهای توسعه را ایجاد می‌کند (محمد حسینی و همکـاران، ۱٤۰۱،ص۲۲٦). لـذا تهدیدات سایبری آینده از یک سو و بهره‌بـرداری غیرمخـرب و در عـین حـال آسـیب رسـان شـبکه سایبری از سوی دیگر برای مقابله با طیف گسترده ای از تهدیدات مرتبط با فضای سایبری و فنـاوری های نوین ارتباطی کافی نیست و زمینه را برای جاسوسی سایبری و جرائم تروریستی مهیا مـی سـازد، تحولات محیطی و کلان روندهای فناورانه در محیط ملی ، بین المللی و فراملـی روز بـه روز در حـال گسترش است که نیاز به رصد، پایش و پویش های محیطی و تحلیل روندهای موجود بـوده و پویـایی و عدم اطمینان محیطِ امروز، برنامه ریزان و مدیران را ملزم بـه تجهیـز بـه ابـزار پیشـبینی کـرده اسـت. پیشبینی سعی دارد تا با تکیه بر مشاهدات قبلی و بر پایه وضعیت گذشـته و حـال، آینـده را پیشـگویی کند(ناظمی، قدیری، ۱۳۸۵ .)اما آنچه مسلم است آینده قابل پیشبینی، قطعـی نیسـت (مظفـری، ۱۳۸۸، ص ٤۸) همین عدم قطعیت در مباحث برنامه ریزی در حوزه های مختلف به ویژه حوزه هـای امنیتـی –انتظامی و جرم شناختی، تغییر از رویکرد پیش بینی بـه رویکـرد آینـده نگـاری را در حـوزه جـرائم تروریستی اجتناب ناپذیر ساخته است(پورمحمدی و همکاران، ۱۳۸۹). همچنین تحلیل تصـاویر آینـده جـرائم تروریسـتی ، قابلیـت لـازم بـرای کـاوش و بررسـی در آینـدهٔ نامشـخص را دارا مـی‌باشـد(Angheloiu, C., Sheldrick, L., & Tennant, M. 2020)

از آن‌جایی که در سال‌های اخیر، جاسوسی سایبری به‌عنوان یک نگرانـی خـاص بـرای جامعـه بین‌المللی ظاهر شده است.[۲] جاسوسی در پرتو حقوق بشر اهمیت بسـیار زیـادی دارد و ایـن اهمیـت

[۱] .Resilience

[۲] در واقع، دامنه و فراوانی جاسوسی سایبری در نظم جهانی معاصر در ژوئن ۲۰۱۳ آشکار شد، زمانی که ادوارد اسنودن – پیمانکار سابق آژانس امنیت ملی ایالات متحده (ایالات متحده) - (NSA) مجموعه ای از اسناد طبقه بندی شده را به انگلیسی ها فاش کرد. روزنامه گاردین این اسناد نشان داد که تعدادی از ایالت‌ها از جمله ایالات متحده و بریتانیا (بریتانیا) از طیف فوق‌العاده‌ای از روش‌های جاسوسی برای به دست آوردن اطلاعات محرمانه از طیف وسیعی از بازیگران مختلف در سراسر جهان استفاده کرده‌اند. یک روش جاسوسی برجسته به‌ویژه استفاده از عملیات سایبری برای جمع آوری اطلاعات محرمانه ای که در فضای مجازی ذخیره شده یا از طریق آن منتقل

زمانی آشکار می شود افراد در لوای حقوق بشر مرتکب جاسوسی میشوند یا آنک حکومت‌ها به بهانـه حقوق بشر جاسوسی را نادیده می گیرند(زارع و قره باغی، ۱۳۹٤).

جاسوسی مجموعه‌ای بدون توافق از اطلاعات محرمانه را توصیف می‌کند که تحت کنترل بازیگر دیگری است. دولت ها پرکارترین مرتکبین جاسوسی هستند و بـه طـور کلـی در دو نـوع جاسوسـی شرکت می کنند که هر کدام با توجه به نوع اطلاعات جمع آوری شده تعریف مـی شـوند. جاسوسـی سیاسی برای تقویت امنیت ملی از طریق دسترسی به اطلاعات سیاسی و نظامی که تحـت کنتـرل سـایر کشورها و به طور فزاینده ای بازیگران برجسته غیردولتی مانند سازمان های تروریستی و وابستگان آنها است، طراحی شده است(Buchan, 2021: 14). نگرانی ها و دغدغـه هـایی را از حیـث تضـعیف امنیت عمومی آحاد مردم به دنبال خواهد داشت، لذا برنامه ریزی برای مقابله با سناریوهای احتمالی در حوزه جاسوسی سایبری و جرائم تروریستی در آینده امری ضروری و اجتنبا ناپذیر است.

جاسوسی از طریق فناوری های نوین ارتباطی و شبکه های اینترنتی برای دسترسی غیرقانونی یـا دزدی اطلاعات محرمانه و حساس یا بـه عبـارت دیگـر، حفاظـت شـده صـورت مـی گیـرد وجـود خصایصی در پروتکل های ارتباطی در فضای سایبری، عملا رصد و شناسایی منبع اصـلی نفـوذ، جابـه جایی غیرقانونی و حتی ربایش اطلاعات را دشوار و حتـی گـاهی غیـر ممکـن مـی سـازد (آقاجـانی، ۱۳۹۷، ۳۱)، اما از دیدگاه حقوق بین الملل دولت ها در قبال جاسوسی سایبری دارای مسـئولیت بـین المللی هستند. یکی از راهبردهای مهم در پیشگیری از جرایم تروریستی ایجاد محـدودیّت هـای فنـی – اطلاعاتی و سایبری مربوط به ارتباطات افراد مظنون به جرایم تروریستی در بسـتر فضـای مجـازی و کاربست مفاهیم آینده پژوهانه است. ممنوعیّت ارتبـاطی بـه جهـت جلـوگیری از ارتبـاط فـرد بـالقوّه مستعد با اشخاص تروریست است. از این رو، منظور از افراد مشـخّص اشخاصـی هسـتند کـه سـابقهٔ مشارکت یا معاونت در فعّالیّت های تروریستی را داشته یا عضو گروه های تروریسـتی باشـند. در ایـن بند ارتباط فرد با اشخاص تروریست برای وی مضر محسوب شده و بدین جهت ممنوعیّت ارتباط بـا

شده است. اهداف جاسوسی سایبری شامل بازیگران دولتی و غیردولتی، از جمله مقامات سازمان های بین المللی مانند اتحادیه اروپا، ارگان های دولتی (از جمله سران کشورها مانند صدراعظم آلمان آنگلا مرکل و نخست وزیر اسرائیل ایهود اولمرت)، رهبران مذهبی (پاپ)، شرکت‌ها (مانند شرکت نفت برزیل پتروبراس)، سازمان‌های غیردولتی (از جمله یونیسف و پزشکان دوموند) و افراد مظنون به دست داشتن در تروریسم بین‌المللی و سایر شرکت‌های جنایی (Buchan, 2019: 4).

این افراد به صورت موقّت وضع میشود. تا در صورت تشخیص غیرآسیب زا بودن این ارتباط، اجازۀ معاشرت و تعامل داده شود. از سوی دیگر، محدودیّت مربوط به تملّک و انتفاع از وسایل ارتباطی به ویژه ابزارهای الکترونیکی و فنّاوری های نوین وجدید از قبیل اینترنت یکی از ابزارهای کنترل و شناسایی مجرمان است. امروزه فنّاوری رایانه ای در خدمت مواردی چون عضوگیری، تبلیغات سیاسی، تأمین مالی و هماهنگی بین گروه های تروریستی قرار می گیرد(رضایی و حشمتی،۱۳۹۵، ۵۹)

از طرفی وقوع حوادث تروریستی در دو دهه اخیر بعد از حادثه ۱۱ سپتامبر نشان دهنده این است که آینده با قطعیت قابل پیش بینی نیست و حوادث آینده حاکی از عدم قطعیت های متعددی است، لذاجرایم تروریستی در تمامی ابعاد و مصادیق نیز از این مقوله مهم مستثنی نیست و به نظر می رسد. ماهیت بین المللی جاسوسی سایبری از طریق نفوذ و رخنه در حریم خصوصی اشخاص بزه دیده و یا حتی اطلاعات حیاتی سازمان و دولت های هدف به عنوان زمینه و علت جرم تروریستی صورت بندی گردیده است، بنابراین در این تحقیق نگارندگان ضمن توجه به مفهوم جرم جاسوسی سایبری به عنوان جرم زمینه ساز وقوع اقدامات و جرایم تروریستی با تکیه بر اسناد بین المللی را با نگاهی به مفاهیم آینده پژوهانه مورد بررسی قرار می دهند.

به هر روی، پژوهش حاضر با هدف کاربرد ی و با ماهیت توصیفی تحلیلی انجام شده است. این مقاله با روش اسنادی و مروری و با رویکرد آینده پژوهانه سعی دارد اقدامات حقوقی و فناورانه در مقابله با جاسوسی سایبری در پیشگیری از جرائم تروریستی با نگاهی به اسناد حقوق بشری مورد بررسی و تحلیل قرار دهد.

۱-سوابق طرح موضوع

کاویانی و همکاران(۱۳۹۸) در پژوهشی تحت عنوان« آینده پژوهی سناریوهای احتمالی گروهک های تروریستی در استان سیستان و بلوچستان» به این نتیجه رسیده اندکه افزایش کمی و کیفی اقدام های خرابکارانه, تقویت و نهادینه سازی اندیشه سلفی گری و دامن زدن به اختلاف های مذهبی, گسترش فعالیت ها در حوزه های سیاسی و حقوق بشری, نفوذ در بین نمایندگان مجلس, شورای شهر و معتمدین محلی ,محتمل‌ترین سناریوهای گروهک های تروریستی در استان سیستان و بلوچستان می باشند.

قدیر و کاظمی فروشانی(۱۳۹۸) در تحقیقی با عنوان « بررسی تطبیقی حقوق کیفری ایران با اسناد بین المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری» بیان می دارندکه بررسی منابع قانونی در حقوق ایران نشان می دهد که در خصوص پیشگیری از این بزه در مقررات کیفری، مقرره خاصی وجود ندارد بلکه با استناد به برخی قوانین عام همچون قانون جرایم رایانه ای و قانون مجازات اسلامی می توان به مواضع پیشگیرانه حقوق کیفری ایران در زمینه پیشگیری از این بزه و حمایت از بزه دیدگان آن اشاره کرد. لذا قانون کیفری ایران فاقد جرم انگاری مستقل در مورد تروریسم و جرایم آن است و در واقع، سیاست جنایی ایران مبتنی بر سیاست مصداقی است .

مانیک[1] (۲۰۱۱) در مقاله‌ای تحت عنوان «تروریسم گذشته، حال و چشم‌انداز آینده» به تعریف تروریسم و بررسی تاریخی اقدامات تروریستی در گذشته و حال و حوادث تروریستی بعد از یازده سپتامبر و خطر استفاده از سلاحهای کشتار جمعی توسط تروریستها و همچنین به مطالعه سازمان تروریستی القاعده به طور خاص پرداخته است و یک درک کلی از تروریسم ارائه داده و معتقد است تروریسم آینده، از نوع تروریسم مذهبی خواهد بود.

فتاحی زفرقندی و همکاران (۱۳۹۹) در مقاله‌ای با عنوان «پیشگیری از جرم جاسوسی سایبری نیروهای مسلح و نقش آن در تأمین حق امنیت» معتقدند که استفاده از هر دو روش پیشگیری کیفری و غیرکیفری می تواند در پیشگیری از جاسوسی سایبری مؤثر باشد .

هلیلی (۱٤۰۰) در مقاله‌ای با عنوان «فناوری‌های نوظهور سایبری و تهدیدات ناشی از بکارگیری آنها در سازمان‌های دفاعی- نظامی» بیان می دارد که شناخت چالش‌ها و تهدیدات این فناوری‌های نوظهورو آمادگی برای مواجهه هوشمندانه با کلان‌روندهای فناورانه، از دغدغه‌های همیشگی سیاست‌گذاران و ذینفعان فضای سایبر است. ازاین‌رو، آینده‌پژوهی، مطالعه اکتشافی عمیق و بررسی و تحلیل اسناد و گزارش‌های معتبر جهانی در این حوزه، امری ضروری است. لذا بکارگیری این فناوری‌ها می‌تواند موجب بهبود کیفیت و کارایی در محیط‌های عملیاتی سازمان‌های دفاعی شود؛ اما بهره‌گیری مناسب از مزایا و قابلیت‌های آنها، به خاطر تهدیدات سایبری نیازمند زیرساخت‌های ارتباطی و شبکه‌های اختصاصی است. بنابراین برای پیشگیری از غفلت راهبردی، در پذیرش و استفاده از این فناوری‌ها، باید میان نگرانی‌های ناشی از دستیابی به اطلاعات حساس، تضمین امنیت

[1] Mannik

داده‌ها و کارایی‌های جذاب و وسوسه‌انگیز آنها، مصالحه برقرار نمود.

مبینی و امیدی (۱۳۹۷) در پژوهشی با عنوان «آینده پژوهی تروریسم و امنیت نظام بین الملل» نشان می دهند که است که تداوم و تشدید جرایم تروریستی در دهه آینده سناریوی محتمل است. محرک های تغییرات تکنولوژیکی، جهانی شدن، افزایش جمعیت جهان و تغییرات اقلیمی در ایجاد و گسترش جرایم تروریستی مؤثر هستند؛ تهدیدات ناشی از تروریسم سایبری و اینترنتی در دهه آینده شدت می‌یابد، همچنین تروریست های افراطی در دهه آینده از از سلاح‌های غیر متعارف و حملات انتحاری بیشتری در سراسر جهان به منظور تحقق اهدافشان استفاده خواهند کرد و گروه‌های تروریستی در آینده تهدیداتی جدی برای امنیت نظامی, اقتصادی, انسانی و زیست محیطی ایجاد می‌کنند. این نتایج نشان میدهد که سه راهبرد؛ نخست، رویکرد یکپارچه جهانی در برخورد با جرایم تروریستی ؛ دوم، راهبرد پیشگیرانه در قالب مقابله و خشکاندن ریشه ها و مبادی فکری و اعتقادی جرایم تروریستی و سوم، راهبرد سرکوب و مقابله تاکتیکی و عملیاتی با مظاهر جرایم تروریستی، برای مقابله با این تهدیدات می‌تواند راهگشا باشد.

زارع و قره باغی (۱۳۹٤) در مقاله‌ای با عنوان «تعارض میان جاسوسی و آزادی اطلاعات در حوق بین المللی بشر دوستانه» بیان می دارندکه جاسوسی در پرتو حقوق بشر اهمیت بسیار زیادی دارد و این اهمیت زمانی آشکار می شود که افراد در لوای حقوق بشر مرتکب جاسوسی می شوند یا آنکه حکومت ها به بهانه جلوگیری از جاسوسی حقوق بشر را نادیده می گیرند. کاوش حقوقی در این موضوع ضمن رفع نکات مبهم می تواند راهگشای تعارضات حاکم نیز باشد، به نحوی که نه به حقوق اساسی افراد لطمه ای وارد شود و نه آنکه امنیت ملی دولت ها خدشه دار شود. التزامات حقوق بشری به دلیل داشتن سنگ بنایی استوار، محوریت بشر و بهره گیری از پشتیبانی جدی و سازوکارهای نظارت و کنترل در کنار ضمانت اجرای منحصر به فرد آن، تحرک سریع تر و هدفمندتری را نسبت به شکل گیری و توسعه سایر قواعد حقوقی می پیماید و بخش اعظم این فرایند را نیز به واسطه تحدید اختیارات و حاکمیت دولت ها و ایجاد ارکان نظارتی، موظف به کنترل اعمال دولت های عضو و ارکان و کارگزاران و نمایندگان آنان در داخل و خارج محقق ساخته است

اگرچه پژوهش هایی درباره جاسوسی و جرائم تروریستی بصورت مجزا وجود دارد که به برخی از مهم ترین آنها اشاره شده است، اما با بررسی دقیق تر پژوهش تلفیقی و تطبیقی مابین جاسوسی سایبری و جرائم تروریستی بصوت توامان صورت نگرفته استو از طرفی وجه افتراق و

نوآوری این مقاله با سایر پژوهش ها پـرداختن بـه مسـئله پـژوهش بـا رویکـرد آینـده پژوهانـه و بـه کارگیری مفاهیم آینده پژوهی است که آن را از دیگر پژوهش ها متمایز می سازد.

۲-نگاهی مفهوم‌شناختی به جاسوسی سایبری در پرتو آینده پژوهی

۳-۱-آینده پژوهی:[۱] عبارت اسـت از؛ مطالعـه نظـام منـد، کشـف، ابـداع، ارائـه، آزمـون و ارزیابی آینده های ممکن، محتمل و مطلوب. آینده پژوهی انتخاب های مختلفـی را راجـع بـه آینـده پیش روی افراد و سازمانها قرار میدهد و در انتخاب و پی ریزی مطلوبتـرین آینـده بـه آنـان کمـک میکند در یک تعریف جامع تر، آینده پژوهی را میتوان به صورت تلاشـی نظـام منـد تعریـف نمـود کـه کوشش میکند کم و کیف تغییرات یا عدم تغییرات کنونی و تأثیر آنهـا را در ایجـاد واقعیـت هـای آینده مشخص نماید و به دنبال آن است که منبع، الگوها و دلایل تغییر و ثبـات را در جهـت اسـتحکام پیش بینی و ترسیم آینده های بدیل مورد توجه و تبیین قرار دهد.

آنچه آینده پژوهان به ما میگویند ایـن است که چه رویدادهایی در آینـده (بـرای مثـال در حـوزه تروریسم و جرائم تروریستی) امکان وقوع دارند؟ چـه گزینـه هـایی بـه صـورت احتمـالی فـراروی سازمان های انتظامی – امنیتی قرار خواهد داشت، آینده یا آینده های مطلـوب و محتمـل کدامنـد؟(۳۷ Bell ,۲۰۰۳ ،). آینده نگاری به تمامی سازمان ها کمک می‌کند تا روندهایِ حرکت خـود را جلـوتر از بقیه رقبا تشخیص داده و بینش عمیق تری در مورد این که چگونه چنین روندهایی بر سـازمان آنهـا تأثیر میگذارد پیدا کننـد(Hajizadeh & Valliere. 2022). در ایـن تحقیـق نیـز بـا بـه کـارگیری کاربست آینده پژوهی و مطالعه تحولات حقوقی و اسناد بین المللی بشر دوستانه راهبردهای مقابلـه بـا جاسوسی سایبری برای پیشگیری از جرائم تروریستی مورد بررسی قرار می گیرد.

۳-۲- تحولات قانونی و حقوقی: فضای سایبری خطرات و فرصت‌هایی را نیز بـه همـراه دارد و یک تهدید برجسته از این حوزه، جاسوسی سایبری است. از آنجایی که هیچ تعریـف شـناخته شـده بین المللی و قانونی از جاسوسی سایبری وجود ندارد، تعاریف زیر از جاسوسی تنها بـرای چـارچوب بندی موضوع مورد بررسی استفاده خواهد شد. جاسوسی سایبری بهره برداری از فضـای سـایبری بـه منظور دسترسی و جمع آوری داده های محرمانه را توصیف می کنـد. مـی توانـد از طریـق دسترسـی

۱. Futures Studies

نزدیک یا از راه دور رخ دهـد. جاسوسـی سـایبری دسترسـی نزدیـک شـامل جمـع آوری داده هـای محرمانه از طریق نصب سخت افزار یا نرم افزار توسط عوامل مخرب در نزدیکـی فیزیکـی شـبکه یـا سیستم کامپیوتری مورد نظر است. در مقابل، جاسوسی سـایبری دسترسـی از راه دور در فاصـله ای از شبکه هدف راه اندازی می شود، معمولاً با بهره برداری از مسیرهای ایجاد شده توسط اینترنت. بـا ایـن همه، جاسوسی در زمان صلح به طور خـاص توسـط حقـوق بین‌الملـل تنظـیم نمی‌شـود، و بنـابراین «حقوق بین‌المللی جاسوسی» وجود ندارد که بتوان آن را برای جاسوسی سایبری اعمال کـرد، امـا ایـن بدان معنا نیست که جاسوسی سایبری در خلاء حقوق بین المللی وجود دارد. در واقع، مجموعـه ای از اصول کلی حقوق بین الملل و همچنین رژیم های تخصصـی وجـود دارد کـه بـه طـور بـالقوه بـرای جاسوسی سایبری قابل اجرا هستند .برخلاف جاسوسی در زمان صلح، جاسوسی سایبری که در زمـان درگیری های مسلحانه انجام می شود مسـتقیماً توسـط حقـوق بشردوسـتانه بـین المللـی تنظـیم مـی شود(Buchan, 2018: 49-51).

جاسوسی سایبری در زمرهٔ جرایم مادی صرف نیست. بر این اساس، احـراز رکـن روانـی جـرم لازم و ضروری اسـت عنصـر روانـی جـرم جاسوسـی، سـوءنیت عـام اسـت و در انجـام رفتارهـای جاسوسی نیازی به قصد خاص نیست؛ مگر در نقض تدابیر امنیتی سامانه های رایانه ای یا مخـابراتیِ موضوع ماده ٤ قانون جرایم رایانه ای که مرتکب باید قصد دسترسی به داده های سرّی موضـوع مـاده ۳ قانون جرایم رایانه ای را داشته باشد که شامل عمـدی بـودن و ارادی بـودنِ مرتکـب یعنـی آگـاهی داشتن از محرمانه و سرّی بودن داده هاست یعنی مرتکب با هدف و نیت لطمه به امنیت ملی و نقـض تدابیر امنیتی کشور، اینگونه اطلاعات را در اختیار دشمنان و بیگانگان قرار دهد (اردبیلی، ۱۳۸۸، ٦١).

در چارچوب حقوق بین الملل، جاسوسی سایبری مجموعه اقداماتی را در بر میگیرد که هرچنـد ماهیتاً با سرقت اطلاعات، فیشینگ و هکینگ و و امثـالهم ارتبـاط و سـنخیت دارد، بـه لحـاظ مـاهوی، عملی مستقل محسوب می شود و به ویژه از حیث اهمیت اطلاعات و حفاظت از منـافع ملـی، دولتهـا به آن واکنشی جدی از خود نشان میدهند. برای مثـال، در قـانون ایـران جاسوسـی سـایبری، شـنود و دسترسی غیرمجاز که از طریـق آن نفـوذگران از بـدافزارهای گونـاگونی بـرای دسـتیابی بـه اطلاعـات محرمانه و حیاتی استفاده میکنند، به ویژه در مادهٔ ۳ قانون جرایم رایانه ای ممنوع اعلام شده و بـرای آن مجازات هایی در نظر گرفته شده است (قدیری و کاظمی، ۱۳۹۸، ٢٤٠). با ایـن حـال، هرچنـد دولتهـا در قوانین ملی عمدتاً به جرم انگاری جاسوسی در قوانین ملی مبـادرت کـرده و بـرای آن مجـازاتی در

نظر گرفته اند، در چارچوب حقوق بین الملل قضیه بسیار پیچیده است. برخی معتقدند این امر در حقوق بین الملل با محدودیتی جدی همراه نیست، چراکه رویه بین المللی مؤید آن است که دولتها مکرراً مبادرت به جاسوسی سایبری می کنند(Sander ،2019).

۳-۳- حقوق بین‌المللی بشردوستانه: جاسوسی در اعصار مختلف در عرصهٔ جهانی وجود داشته است. اما با تحولات نوین در فناوری و پیدایش پدیدهٔ تروریسم و ضرورت مقابلهٔ جهانی با آن، پیچیدگی خاص خود را پیدا کرده که خود اختلافات بین‌المللی زیادی را سبب شده است. در حقوق بین‌الملل میان «جاسوسی در زمان جنگ» و «جاسوسی در زمان صلح» تفکیک خاصی صورت گرفته است. هنگام صلح، تمایز میان قلمرو ملی و بین‌المللی و در نتیجه «اصل برابری حاکمیت» جاری است و هر گونه مداخله از جمله از طریق جاسوسی که دربردارندهٔ تجاوز به قلمرو ملی شناخته شود، غیرقانونی خواهد بود، زیرا «اصل تساوی حاکمیت دولت‌ها» به‌طور ضمنی «عدم مداخلهٔ» دولت‌ها در امور یکدیگر و استقلال آنها را نشان می‌دهد. در عین حال، مصادیق شناخته‌شده‌ای از مداخلات قانونی از جمله از طریق جاسوسی در نظام نوین بین‌المللی وجود دارد که از جملهٔ آنها می‌توان از مداخلهٔ مأذون از طرف شورای امنیت به‌منظور حفظ صلح و امنیت بین‌المللی و مبارزه با تروریسم، مداخله برای دفاع مشروع، مداخله با دعوت و مداخله به دلایل بشردوستانه و حقوق بشر نام برد. جاسوسی در راستای موارد مذکور با شرایطی موجه است. از طرف دیگر، «جاسوسی در زمان جنگ»، با رعایت شرایطی، به‌عنوان یک «ترفند جنگی» اصولاً به رسمیت شناخته شده است. با وجود تلاش‌های زیاد، هنوز معاهده‌ای جهانی در مورد جاسوسی به‌خصوص در شکل‌های جدید همچون جاسوسی سایبری و جاسوسی منجر به نقض حریم خصوصی اشخاص وجود ندارد. این در حالی است که جاسوسی به معنای واقعی جهانی شده و لازم است مقررات متحدالشکل، موارد مشروع و نامشروع آن را مدون سازد(جلالی ۱٤۰۰، ص۳٤۳).

البته با توجه به تأکیدات شرع مقدس و به لطف سیاست های نوع دوستانه و موازین انسان دوستانه فراگیر دولت و ملت ذیل دکترین حقوق بشر اسلامی امکان دسترسی به آموزش، بهداشت، بیمه، اشتغال، تردد آزاد در مناطق مختلف و فرصت‌های معیشتی داده شده است که نه تنها باعث امنیت و بقای آنان شده بلکه به اذعان سازمان ها و نهادهای حقوق بشری بین المللی به شکوفایی و بهبود وضعیت آنان نیز کمک کرده است(خدادوست و همکاران، ۱٤۰۱، ۱۲۱).

۳-آینده جاسوسی سایبری و ارتباط آن با جرایم تروریستی

امروزه تغییرات محیطی با سرعت بالایی در حال رخ دادن است. فناوری های جدید، انسانها را در یک دهکده یا اکوسیستم قرار داده و نیروهایی را به آنها وارد میکنند که یک یا دو دهه پیش نمیتوانستند آنها را تحت تأثیر قرار دهند. لذا سرعت تغییرات آنچنان سرسام آور است که دیگر نمیتوان با روشهای سنتی با آنها کنار آمد. در این وضعیت که تغییرات در همه زمینه ها به سرعت در حال شکل گیری است، سازماندهی فعالیت های علمی برای پیش بینی آینده ضرورتی انکار ناپذیر است(محمدی لرد، ۱۳۹۳ :۷٤ –۷۳). لذا پیشگیری از جرائم تروریستی ناشی از جاسوسی سایبری در عصر حاضر با تکیه بر مفاهیم و کارکردهای آینده پژوهی امکان پذیر است.

در این میان با توجه به اینکه، جرائم تروریستی و جاسوسی سایبری، بیش از گذشته ثبات و امنیت بین المللی را مورد تهدید قرار داده و خارج از عرف و اصول حقوق بشری محسوب می شود و به عنوان یکی از پیشران های اساسی در برنامه امنیتی– انتظامی کشورها در قرن ۲۱ ،بسیار مورد توجه قرار گرفته که این مسئله، خود نشان دهنده توجه به این موضوع با رویکرد آینده نگارانه است و با توجه به سطح رو به رشد تهدیدات تروریستی، دامنه بین المللی و حقوق بشری آن و امکان ارتکاب جرائم تروریستی از طریق توسل به جاسوسی سایبری بیش از گذشته فراهم شده است. لذا توجه به روندها گذشته و حال و شناخت محیط فناورانه به منظور مقابله و مدیریت تهدیدات تروریستی در آینده ضروری به نظر می رسد.

با این حال شناخت عملیات جاسوسی سایبری بازیگران دولتی یا غیردولتی که برخی از اصول حقوق بشری و حقوق بین‌الملل را نقض می‌کند و همچنین به منزله کسب نادرست و سوء استفاده از داده‌ها است با استفاده از شناخت مقررات داخلی از طریق قوانین تخصصی یا اصول کلی، راه حل های مدنی و کیفری را در برابر جاسوسی سایبری تصریح می کند(Pehlivan, 2019: 16).

در زمینه ممنوعیت یا جواز جاسوسی در حقوق بین الملل، نه تنها از حیث نظری، بلکه در رویه بین المللی و اسناد حقوق بشری نیز اختلاف نظری جدی موجود است. از آنجا که این ممنوعیت به نحوی مطلق مورد قبول نگرفته و توافقی عام در این زمینه موجود نیست، نمیتوان به قطعیت اظهار نظر کرد، برخی با توسل به فقدان یک رژیم ممنوعیتی خاص، ممنوعیتی در این زمینه قائل نمیشوند برخی نیز این قسم از اقدامات را زمینه ساز نقض حق حاکمیت و اصل عدم مداخله در امور سایر دولت ها تلقی می کنند و مغایر با اصول حقوق بین الملل موجود و حقوق بشر میدانند و از این منظر پیوسته درصددند تا با اعلام موضعی مبنی بر ممنوعیت این اقدامات، مانع شکل گیری یک رژیم

عرفی مبتنی بر تجویز جاسوسی در حقوق بین الملل شوند (Deeks ۲۰۱۵: ۳۱٤) با این حال، واقعیت این است که توسل به این قسم از اقدامات در حقوق بین الملل رو به تزاید به نظر میرسد و دستیابی به توافقی جدی در این زمینه در آینده نزدیک ضروری است (Katharina Ziolkowski ۲۰۱۳ ، ٤۲۷-٤۲۵) ابهام در رویه و عملکرد بین المللی دولتها در زمینه جاسوسی در حقوق بین الملل، با ظهور اینترنت و با کاربرد رو به رشد استفاده از فناوری های نوین در توسل به این اقدامات تشدید شده است (شهبازی و آقاجانی، ۱۳۹۹) به این ترتیب، در حالی که فضای سایبر، کمکی به شکل گیری رژیم حقوقی در زمینه جاسوسی در حقوق بین الملل نکرده، بر چالش های عملی دولت ها در حوزه امنیت ملی نیز افزوده است. امکانات و تسهیلاتی که فضای سایبر در اختیار افراد و دولتها قرار میدهد، زمینه ای را برای توسل به اقدامات جاسوسی و به تبع از آن اقدامات و حوادث تروریستی در محیط ناپایدار آینده فراهم میکند و همزمان با سرعت، دقت و سهولت در این زمینه، ارتکاب جاسوسی و وقوع جرائم تروریستی با توسل به روندهای فناورانه موجود تشدید میگردد. همین موضوع سبب می شود تا هم در شناسایی مصادیق رویه بین المللی موجود در این زمینه، اختلاف نظر حاصل شود و هم زمینه های مساعدی برای فرار از مستولیت بین المللی و وقوع جرائم تروریستی پیش روی مرتکبان جاسوسی سایبری قرار گیرد (Kilovaty, 2016: 66-69) .

با این حال، در عمل، از این منظر که دولت ها جاسوسی سایبری را چونان شمشیری دولبه تلقی میکنند که در صورت عدم مقابله با آن و عدم طراحی سناریوهای احتمالی، می تواند آن ها را به عنوان قربانی بالقوه ایی در مقابل مخاطرات آینده به ویژه جرائم تروریستی ناشی از آن قرار دهد، کنشگران بین المللی در موارد متعددی توسل به جاسوسی سایبری را عموماً زمینه ساز نقض حقوق بین الملل و نه یک استثنای امنیتی برای حفاظت از منافع ملی تلقی میکنند. برای مثال، همزما با افشای اقدامات نظارتی سازمان امنیت ملی آمریکا توسط ادوارد اسنود در سال ۲۰۱۳ ، مرکز ارتباطات دولت بریتانیا اعلام کرد که چنین برنامه هایی که میتوانند موجب نقض برخی از اصول اساسی حقوق بین الملل میشود. وزیر خارجه مکزیک نیز ، اقدامات نظارتی ایالت متحده در خصوص دولت و رئیس جمهور مکزیک را محکوم کرد و بیان داشت که این اقدامات غیرقانونی و خلاف قوانین مکزیک و حقوق بین الملل است. اندونزی نیز اقدامات نظارتی فرامرزی ایالت متحده و برخی از همفکران را زمینه ساز نقض حقوق بین الملل تلقی کرد(Barrie Sander, 2019: 12) .

٤-ظرفیت‌سنجی سازوکارها و مقابله با جاسوسی سایبری در ارتکاب جرایم تروریستی

٤-١- آینده‌پژوهی فنی و حقوقی

جرایم تروریستی یک ویژگی ثابت در افق آینده بشریت است و پیشرفت های تکنولوژیک, اندیشه ,تاکتیک و سلاح تروریست ها باعث شده که دولتها به منظور کاهش ضریب آسیب پذیری احتمالی و اتخاذ موضع فعال و کنشی به جای موضع انفعالی و واکنشی در نحوه برخورد با جرایم تروریستی نیاز به آینده نگری داشته باشند(مبینی و امیدی ،١٣٩٧).

سنجش روندهای مقابله با جرایم تروریستی در سطح بین الملل با استفاده از رویکردهای فنی – حقوقی و بین المللی نشان می دهدکه سناریوی تقویت همبستگی و انسجام جامعه بین الملل در مبارزه با تروریسم و جرائم تروریستی با ویژگی هایی چون رهبری جدی تر سازمان ملل متحد؛ تعهد به رعایت حقوق بشر در مبارزه با تروریسم؛ مجازات عاملان اقدامات تروریستی و تقویت برابری و عدالت اقتصادی، از محتمل ترین و مطلو بترین چشم اندازهای روندهای مقابله با تروریسم در عرصه بین المللی در سه دهه آتی میباشد (بصیری و آقا محمدی، ١٣٩٦). با کاربست آینده پژوهی دولت ها پس از حملات ١١ سپتامبر ٢٠٠١، برای مقابله با جرایم تروریستی سناریو احتمالی به جرائم تروریستی را « مثابهٔ جنگ» تلقی کرده و برای خود حقّ دفاع مشروع قائل شدند.

بدین ترتیب، حوادث تروریستی ١١ سپتامبر ٢٠٠١ ضمن گسترش دکترین دفاع پیش‌دستانه تأثیر بسزایی را در تغییر رویکردهای مواجهه با تروریسم در نظام های حقوقی بر جای گذاشته و رویکرد پیشنگرانهٔ[١] کیفری را با شتاب بیشتری ارائه کردند. از این رو، در کنار ابزارهای قهری و پاسخ های کیفری به تروریسم که اغلب معطوف به زمان پس از ارتکاب جرایم تروریستی هستند، تمهیدات نوظهوری در مهار تروریسم مورد توجه قرار گرفتند که زمان پیش از ارتکاب جرایم تروریستی را مورد هدف قرار میدادند تا با پیشدستی از وقوع جرایم تروریستی پیشگیری کرده و تهدیدات و آسیبهای احتمالی را در مراحل اولیه خنثی کنند(نعمتی و همکاران، ١٣٩٩). بنابراین یکی از مهم ترین رویکردهای مهار جرایم تروریستی با استفاده از ابزارهای فنی و اطلاعاتی و فضای سایبری، رصد و کنترل اطلاعات جرایم حوزه جاسوسی سایبری با استفاده از تحلیل روندهای حال و گذشته است که از امکان دسترسی غیر مجاز و نفوذ افراد و گروه های مرتبط با جرایم تروریستی

١ . Anticipatory.

احتمالی در آینده پیشگیری کرد(Buchan and Navarrete, 2021: 83-84).

در نظام حقوقی استرالیا محدودیت و یا ممنوعیت ارتباطات افراد مظنون به جرایم تروریستی در مادهٔ ۱۰٤ قانون مجازات پیش‌بینی شده است (Criminal Code, 1995: 104).[۱] به‌علاوه، تحدید دسترسی یا استفاده از اینترنت را می‌توان از طریق صدور قرار کنترل نسبت به مظنونین جرایم تروریستی اعمال کرد (White, 2008: 4). برای نمونه، می‌توان به قرار نظارت که علیه فردی به نام «جک توماس»[۲] صادر شده است اشاره کرد. طبق این دستور محدودیت های استفاده از تلفن همراه، کارت تلفن، سیمکارت، خدمات اینترنتی، پست الکترونیکی، دسترسی به تلفن های ماهواره ای یا عمومی مقرّرشدند (Donkin, 2011: 112-113).

در انگلستان طبق «قانون اقدامات تحقیقاتی و پیشگیری از تروریسم»[۳] وزیر کشور می‌تواند محدودیت‌هایی را بر ارتباط مظنونین تروریستی اعمال کند. برخی از این محدودیت‌ها عبارتند از: الف) الزام به عدم ارتباط با افراد مشخّص بدون کسب اجازه؛ ب) تکلیف به اطّلاع دادن به وزارت کشور قبل از مصاحبت یا ارتباط با دیگر افراد (TPIM Act, 2011, S1: 8).[٤]

از سوی دیگر، محدودیت مربوط به تملّک و انتفاع از وسایل ارتباطی به ویژه ابزارهای الکترونیکی و فنّاوریهای جدید از قبیل اینترنت و فضای مجازی و با هدف کاهش دسترسی افراد مظنون به جرایم تروریستی یکی از ابزارهای کنترل جرایم تروریستی در آینده است. امروزه »فنّاوری رایانه ای در خدمت مواردی چون عضوگیری، تبلیغات سیاسی، تأمین مالی و هماهنگی بین گروه‌های تروریستی قرار می گیرد« (رضایی و حشمتی ۱۳۹۵: ۵۹). بدین سبب در قوانین ضد تروریستی به چگونگی نظارت بر فنّاوری های جدید توجه فراوانی شده است. برخی از این تمهیدات عبارتند از محدودیتهای مربوط به مالکیت یا استفاده از دستگاه های ارتباطی الکترونیکی یا محدودیت افراد دیگر در استفاده از دستگاههای ارتباطی الکترونیکی در اقامتگاه شخص مظنون.

در نظام حقوقی ایران نیز نمونهٔ خاص و بارز سازکار پیشدستانه، صدور دستور قضایی

۱ https://www.legislation.gov.au/Details/C2019C00043

۲ Jack Thomas

۳ Terrorism Prevention and Investigation Measures Act 2011 - Schedule 1". Legislation.gov.uk. 3 February 2012.

٤ https://www.legislation.gov.uk/ukpga/2011/23/contents

مسدودسازی تلگرام از سوی دادستانی تهران است که در سال ۱۳۹۷ ابلاغ شد[۱] این اقدام قضایی برای خنثی سازی فعالیت گروههای تروریستی در فضای امن مجازی بود، چنانکه چنین سازکار قهری و محدودکننده ای به صورت پیشدستانه در راستای مقابلهٔ پیشنگرانه با تروریسم مقرّر شد در نظام حقوقی ایران اقدام قضایی فوق به صورت کلّی و عمومی اتّخاذ شد، ولی محدودیت ارتباطی نظام های دیگر به صورت اختصاصی و شامل اشخاص موضوع قرار نظارت است.

۵-۲- نگاه آینده پژوهانه به ظرفیت‌های حقوقی بین‌الملل

حقیقت این است که صرفا ظرفیت های حقوقی – بین المللی و فناورانه در برابر جرایم تروریستی جهانی و جاسوسی سایبری و کلان روندهای تاثیر گذار برآنها نمی‌تواند به تنهایی از اثرات مخرب و زیانبار جرایم تروریستی در آینده بکاهد، مگر اینکه مباحث و بررسیهای آن از رهگذر آینده پژوهی عبور کند. از آنجا که آینده، با تمام قدرت بر ایجاد تحول، جای زمان حاضر را اشغال میکند، در حقیقت زمان حاضر در برابر آینده رنگ می‌بازد.

عملیات جاسوسی سایبری بازیگران دولتی یا غیردولتی نوعی حمله سایبری است که برخی از اصول حقوق بین‌الملل را نقض می‌کند و همچنین به منزله کسب نادرست و سوء استفاده از داده‌ها است. بنابراین، از توسل به زور تا مسئولیت دولت، حقوق بین الملل طیف وسیعی از راه حل ها را ارائه می دهد .به همین ترتیب، مقررات داخلی از طریق قوانین تخصصی یا اصول کلی، راه حل های مدنی و کیفری را در برابر جاسوسی سایبری تصریح می کند(۹ ، Oğuz Pehlivan,2020).

جاسوسی و جمع آوری اطلاعات بخشی از دستگاه امنیت ملی هر کشوری است. جاسوسی سایبری شامل فعالیت های عمدی برای نفوذ به سیستم ها یا شبکه های رایانه ای برای به دست آوردن اطلاعات ساکن در این سیستم ها یا شبکه ها یا انتقال از طریق آنها است. یکی از زیرمجموعه های مرتبط جاسوسی اقتصادی است که در آن یک دولت تلاش می کند تا اسرار شرکت های خارجی را به دست آورد. برخی از فعالیت‌های سایبری، نظارت الکترونیکی برای اهداف اطلاعاتی خارجی، تقلید از جاسوسی سنتی، و خدمات طیفی از مواردی است که اکثر ما پذیرفته‌ایم که اهداف مشروع امنیت ملی هستند. با این حال، بخش زیادی از مخفی کاری سایبری شامل مسائل اقتصادی است و توسط دولت ها یا نمایندگان آنها برای تضمین مزیت اقتصادی نسبی انجام می شود(William C. Banks ،2017 : 513)

[۱] .www.isna.ir/news/ 97021006264

با این همه، جاسوسی در زمان صلح به طور خاص توسط حقوق بین‌الملـل تنظـیم نمی‌شـود، و بنابراین هیچ «حقوق بین‌المللی جاسوسی» وجود ندارد که بتوان آن را برای جاسوسی سایبری بـه کـار برد. اما این بدان معنا نیست که جاسوسی سایبری در خلاء قـوانین بـین المللـی وجـود دارد. در واقـع، مجموعه ای از اصول کلی حقوق بین الملل و همچنین رژیم های تخصصی وجـود دارد کـه بـه طـور بالقوه برای جاسوسی سایبری قابل اجرا هستند. برخلاف جاسوسی در زمان صلح، جاسوسـی سـایبری که در زمان درگیری های مسلحانه انجام می شود مستقیماً توسط حقوق بشردوستانه بین المللی تنظـیم می شود. افزون بر این، عملیات سایبری بین کشورها فی نفسه توسط قوانین بین المللی ممنـوع نیسـت و عموماً اقدامات غیردوستانه یا خصمانه است .علیرغم عدم وجود یک ممنوعیت کلی بـرای عملیـات سایبری، انجام یک عملیات سایبری ممکن است منجر به نقض هنجارهـای خـاص حقـوق بین‌الملـل شود.[1]

در همین راستا با توجه به اینکه مقابله با جـرایم تروریسـتی امـروزه از سـوی دولـتهـای ملـی، مشکل گردیده، لزوماً واگذاشتن بیشتر وظیفه مقابله با تروریسم به ارگـان و رکـن فراملـی و جهـانی بیش از گذشته جلب توجه مینماید. بنابراین با نگاه و رویکـرد آینـده پژوهانـه، محتمـل تـرین سـناریو برای مقابله با کلان روند جرایم تروریستی جهانی در تمامی ابعـاد آن همکـاری حقـوقی، سیاسـی و عملـی و بین المللی است، روند تحولات محیطی و فناورانـه در حـوزه جاسوسـی سـایبری و جـرائم تروریستی نشان می دهدکه بیش از سابق در چارچوب سازمان ملل متحد بـه عنـوان مهمتـرین آینـده های بدیل برای مقابله با جرایم تروریستی کارآمد سازی اقدامات حقوقی و بین المللـی هـم در حـوزه فضای سایبری و هم در حوزه فضای حقیقی است.

در عصر حاضر جرایم تروریستی بـیش از هـر زمان دیگری توانایی بر هـم زدن نظـم جهـانی را دارد، پیش بینـی هـا در مورد روندهای عمومی تروریسم صورت گرفتـه امـا کمتـر از هـر موضـوعی مـورد شـناخت قـرار گرفته است. پس از حملـه آمریکـا بـه عـراق بسـترها بـرای رشـد القاعـده و داعـش در عراق فـراهم شـد و پیشـروی داعـش در عـراق و سـوریه بـا اقـدامات خشـونت آمیـز و وحشـتناک هـزاران نفر را نابود کرد(لاکوئر[2] ، ۲۰۱۸). برخی از صاحب نظـران نیـز بـه بررسـی علـل

[1] François Delerue, Cyber Operations and International Law, Cambridge University Press, 2020, p. 46.

[2] Laqueur

شکل گیری و گسترش تروریسم پرداخته و پیشبینی هـایی را در زمینـه رونـدهای آینـده تروریسـم ارائه داده اند. مولفه هایی نظیر: تحول روابـط بـین الملـل، جهـانی شـدن اقتصـاد و بـازار، عوامـل جمعیت شناختی، تغییرات ایدئولوژیک و تغییـرات تکنولـوژیکی در رونـدهای آینـده تروریسـم مـؤثر هستند(لیا[1] ، ۲۰۰۵).

امروزه، گروه‌های تروریستی می‌توانند به زیرساخت‌های اطلاعاتی جهـانی کـه تحـت مالکیـت و اداره دولت‌ها و شرکت‌هایی هستند را هدف قرار دهند، سیسـتم‌های اطلاعـاتی امـروزه هـم بـه‌عنوان سلاح و هم به عنوان اهداف جنگی عمل می‌کنند. تروریست‌های کنونی آموخته‌اند کـه امـروزه امنیـت جهان به زیرساخت‌های رایانه‌ها و شبکه‌های سراسر جهان بستگی دارد.

تروریست ها اطلاعات مربوط به آسیب پذیری هـای دشـمن خـود را از منـابع اسـتخراج و بـاز جمع آوری می کنند .آنهـا نیروهـای بـالقوه را بـا روش هـای غربـالگری دقیـق بررسـی مـی کننـد . تروریست ها نیز مانند افسران اطلاعاتی، تجـارت پیشـه مـی کننـد. اگـر گروه‌هـای تروریسـتی ماننـد سرویس‌های اطلاعاتی عمل کنند، ضد جاسوسی می‌تواند همان نقشی را در مبارزه با آنها ایفـا کنـد کـه علیه سرویس‌های اطلاعاتی متخاصم با منافع دولت مورد نظر انجام می‌دهد. با این حال، تروریست هـا با توجه بـه سـازماندهی پراکنـده و متمـایز آنهـا از جملـه گریـزان تـرین اهـداف جـذب نیـرو بـوده اند(Sulick, 2013: 24-27). از اینرو، با شروع از اندیشـه هـای اساسـی «همکـاری»، بخشـی از مقاله به ارزیابی نظرات همکاری های بین المللی از دو جنبه می پردازد: همکـاری قـانونی و همکـاری نظامی.

الف– همکاری قانونی؛ تا به امروز تعدادی از اقدامات دولتی و بین المللی انجام شده است. دولت ها خود را برای مقابله با تهدید جدید سازماندهی میکنند برخی از کشورها تیم‌های واکنش اضـطراری رایانه‌ای[2] را برای رسیدگی به واکنش‌های حادثه ایجاد کرده‌اند. ایالات متحده آمریکا و بریتانیا کشورهای الگوی پیشرو برای سایر کشورها هستند که سیاست های امنیت سایبری خـود را تنظـیم مـی کننـد. بـا پیچیده‌تر شدن فضای سایبری و اجزای آن، به‌ویژه به دلیل توسعه سریع و تکامل پلتفرم‌های مبتنـی بـر

[1] Lia

[2] Computer Emergency Response Team

اینترنت (باند پهن)، آسیب‌پذیری‌های جدید و پیش‌بینی نشده‌ای ممکن است پدیدار شوند.[1] بنابراین اتحادیه اروپا اقداماتی را برای مبارزه با محتوای مضر و غیرقانونی در اینترنت، حفاظت از مالکیت معنوی و داده‌های شخصی، ترویج تجارت الکترونیک و افزایش امنیت معاملات انجام داده است. با این حال، علیرغم ابتکارات اتحادیه اروپا، بسیاری از ناظران معتقدند که جرایم سایبری نیازمند یک واکنش بین المللی است که باید شامل کشورهایی باشد که بهشت مجرمان سایبری هستند

کنوانسیون جرایم رایانه ای شورای اروپا[2] اولین اعلامیه بین المللی را در مورد جرایم ارتکابی از طریق اینترنت و سایر شبکه های رایانه ای منتشر کرد. متأسفانه اقدامات قانونی در قبال جرایم تروریستی سایبری کافی نیست .اقدامات بازدارنده نظامی و تحلیل روندهای تاثیر گذار فناورانه با رویکرد آینده نگاری باید صورت بندی گردد تا تروریست ها در بهره برداری از اینترنت برای اهداف مخرب خود تردید کنند. اقدامات پیشگیرانه برای مختل کردن اطلاعات این وب سایت ها و مکان یابی و خنثی کردن منشا حمله مورد نیاز است .به منظور اتخاذ تدابیر بازدارنده تهاجمی، ناتو و سایر سازمان‌های بین‌المللی با استفاده از روندهای حال و گذشته باید راهبردهای بازدارندگی ایجاد کنند و در پیشگیری از وقایع تروریستی با بهره گیری از مطالعات آینده پژوهی نقش آفرینی نمایند.

ب- همکاری نظامی؛ اصطلاح بازدارندگی سایبری اقدامات پیشگیرانه ای است که در قبال تروریسم سایبری انجام می شود. ماموریت بازدارندگی سایبری پیشگیری از انجام حملات آینده توسط دشمن با تغییر عقیده، حمله به فناوری آنها، یا با ابزارهای محسوس تر (مانند مصادره، خاتمه، حبس، تلفات یا تخریب) که در پاسخ به یک حمله سایبری، تلافی جویانه امکان پذیر است، اما محدود به حوزه سایبری نیست.

تروریسم سایبری علیه زیرساخت‌های حیاتی و فناوری اطلاعات یک تهدید رو به رشد برای کشورهای عضو است .از آنجایی که منشاء حمله می تواند عدم نظارت های سایبری باشد، پس باید با آن مانند یک حمله موشکی بالستیک قاره پیما رفتار کرد. علاوه بر این، سناریوی احتمالی یک حمله سایبری در مقیاس بزرگ که شامل اجزای نیروی نظامی است بسیار بیشتر از سناریو حمله موشکی بالستیک است. بر اساس گزارش، محتمل ترین سناریو تهدیدات ناتو در دهه آینده غیر

[1] European Commission. (2001b). Proposal for a council framework decision on combating terrorism [COM(2001) 521 final, 19.09.2001]. Brussels, Belgium: European Commission.
[2] The Council of Europe Convention on Cybercrime

متعارف هستند .سه مورد به طور خاص برجسته هستند؛ ۱–حمله با موشک بالستیک، ۲–حملات توسط گروه های تروریستی بین المللی۳– حملات سایبری با درجات مختلف شدت.[۱]

با این همه، طراحی و تدوین یک برنامه و سیاست گذاری تهاجمی بین المللی برای مواجهه با جاسوسی سایبری در ارتکاب اقدامات تروریستی با بهره گیری از آینده پژوهی یک الزام است. بنابراین، یک طرح جهانی چنین تقابلی می‌تواند منتج به ارائه برنامه‌ای با مختصات ذیل گردد:

نخست، با استفاده از مطالعات آینده پژوهی برای شناخت موضوعات تروریستی و جرائم سایبری به منظور مقابله با جرائم تروریستی در آینده نیازمند تعریف مسئله ، پایش ها و پویش های محیطی پیرامون جاسوسی سایبری است .اینکه کدام فعالیت‌ها در اینترنت (مانند هک، تبلیغات، حمله به زیرساخت‌ها و غیره) باید به عنوان تروریسم سایبری در نظر گرفته شوند، باید دقیقاً تعریف شوند . صحبت کردن به یک زبان یا ایجاد یک زبان فنی مشترک می تواند یک نقطه شروع برای طراحی سناریو های احتمالی در قبال جرایم تروریستی ناشی از جاسوسی سایبری در آینده باشد. بنابراین، رویکرد آینده پژوهی در سیاست گذاری های حقوقی و بین المللی یک رویکرد معرفت شناسانه و تحلیل محیطی پیرامون موضوع جاسوسی سایبری و جرائم تروریستی است.

در رویکرد دوم با استفاده از مطالعات آینده پژوهی شناسایی و رصد اقدامات قانونی اساسی ملی و بین المللی است، سیاست گذاری های حقوقی بین المللی باید محقق شود. سپس قوانین ملی باید با قوانین بین المللی در قبال جرایم تروریستی هماهنگ شود.

سوم، توافقنامه های دوجانبه و چندجانبه در مورد همکاری امنیت سایبری باید بین کشورها امضا شود.

چهارم، یک استخر اطلاعاتی باید به منظور جمع آوری و به اشتراک گذاری اطلاعات به طور همزمان بین ملت ها ایجاد شود. جمع آوری اطلاعات نه تنها باید شامل نظارت بر وب سایت های تروریستی، بلکه جمع آوری شواهد الکترونیکی برای حملات سایبری احتمالی باشد.

پنجم، هر زمان که کشوری با حمله سایبری مواجه می شود، تیم های متخصص دفاع سایبری باید ایجاد و در سطح بین المللی مورد حمایت های حقوقی و بین المللی قرار گیرند. تعداد تیم‌های واکنش سریع متعلق به کشورها را می‌توان با کمک توانایی واکنش به حوادث رایانه‌ای ناتو و مرکز

12. “NATO 2020: Assured security; dynamic engagement analysis and recommendations of the group of experts on a new strategic concept for NATO,” Experts Report on New Concept. 17 May 2010.

عالی دفاع سایبری همکاری افزایش داد .یک برنامه آموزشی بین المللی برای مقابله با حملات سایبری باید ایجاد شود.

ششم، یک فرآیند تصمیم‌گیری بین‌المللی سازمان‌یافته که از کشف تا تخریب (یا اختلال) حمله سایبری را در بر می‌گیرد، باید شکل بگیرد. مدیران مجاز بین المللی باید به هر حمله ای که در مورد امنیت بین المللی باشد، بر اساس قوانین تعامل توافق شده پاسخ دهند.

هفتم، تجزیه و تحلیل پس از واکنش باید به منظور شناسایی و بهبود نقاط ضعف سیستم انجام شود. بازخورد باید برای بررسی نوآوری های لازم انجام شود.

نتیجه‌گیری

تحولات فناورانه و فضای سایبر سبب تغییر بسیاری از روندها و روش های ارتکاب جرم شده است . جاسوسی سایبری یکی از جرائمی است که با استفاده از فناوری های نوین و در بستر فضای سایبری و از طریق مصادیقی چون سرقت و دسترسی و شنود غیر مجاز ارتکاب میابید و موجبات نقض حقوق بشر و به ویژه تضعیف امنیت ملی کشورها و همچنین پیامدهایی چون وقوع جرائم تروریستی از طریق جاسوسی سایبری به دنبال دارد. یکی از مهم ترین روش‌های پیشگیری از ارتکاب جرائم تروریستی، بهره گیری از روش های مقابله با جاسوسی سایبری با تکیه بر آینده پژوهی است، چرا که بیشتر جرایم تروریستی اخیر با استفاده از جاسوسی سایبری ارتکاب می یابند. با توجه به کاربست مفاهیم آینده پژوهی و شناخت تحولات و پویش‌ها و پایش های محیطی در حوزه فضای سایبری به ویژه نفوذ، دسترسی و شنود غیرمجاز رایانه ای از مهم ترین مولفه های مربوط به کنترل جرایم تروریستی مرتبط با جاسوسی سایبری است.

از آنجائی که تغییرات تکنولوژیکی، مؤلفه های مختلف جهانی شدن، افزایش جمعیت جهان و تغییرات اقلیمی نقش مهمی در ایجاد و گسترش تروریسم در حال و آینده دارد و این سناریو که جرایم تروریستی در تمامی ابعاد به ویژه ناشی از جاسوسی سایبری گسترش بیشتری داشته باشد از محتمل ترین سناریوها بوده و از طرفی ارتکاب جرایم تروریستی در آینده تهدیداتی جدی برای امنیت عمومی، ملی، سرزمینی، اقتصادی و سیاسی کشورها در پی خواهد داشت.

لذا در نگاه آینده پژوهانه برای مهار جرایم تروریستی ناشی از جاسوسی سایبری محتمل ترین و مطلوب ترین سناریو توجه به رویکردهای فنی – حقوقی و رویکردهای سلبی به منظور ایجاد محدودیت های لازم در بهره برداری اطلاعات حوزه حریم خصوصی و سرقت و یا دسترسی غیر

قانونی به اطلاعات به منظور پیشگیری از جرائم تروریستی ضروری به نظر می رسد.

در نهایت با توجه به اینکه اقدامات و تهدیدات تروریستی در آینده تداوم یافته و تشدید می‌شود، راهبردهای ایجاد محدودیت در ارتباط الکترونیکی در بستر فضای مجازی در نوع خود در پیشگیری از جرائم تروریستی مرتبط با جاسوسی سایبری دارای اثر سازنده و مطلوب خواهد داشت. همچنین در رویه های بین المللی نیز جاسوسی سایبری به دلیل نقض اصول حقوق بشری و حقوق بین الملل ممنوع شده است و دولت ها به بهانه تامین امنیت ملی کشور خود نمی توانند به جاسوسی سایبری متوسل شوند، به این دلیل که پیامدهای جاسوسی سایبری منجر به تضعیف امنیت ملی و وقوع جرایم تروریستی در قلمرو بین المللی می گردد، بنابراین نه تنها جاسوسی سایبری توسط کشورها تجویز نشده بلکه بر امکان مقابله با آن به منظور پیشگیری از وقایع تروریستی نیز تاکید شده است. لذا سناریو و چشم انداز مطلوب در حوزه پیشگیری از جرائم تروریستی در آینده ، ناظر بر درک سریعتر متغیرهای محیطی و شناخت تهدیدات و فرصت ها فرا روی جوامع بین المللی در حوزه های حقوقی و فناورانه است.

پیشنهادهای کاربردی

الف-*تشکیل کارگروه تجزیه و تحلیل روند*؛ گروه تجزیه و تحلیل روند با دقت کافی تمام روندهای گذشته و حال جرائم سایبری و تروریستی را بررسی میکنند و علائم تغییر در آن را می شناسد و برای مهندسی آینده مقابله و پیشگیری از جرائم تروریستی ناشی از جاسوسی اقدام می نماید.

ب-*تجسم چشم اندازها و تصاویر آینده*؛ نتایج مطالعات و بررسی های گروه های سیاسی، حقوقی، امنیتی – انتظامی و فضای سایبری و با تاکید بر پیشگیری از جرائم تروریستی در آینده چشم اندازسازی نموده و در ایجاد تصویری غنی از آینده، بر اساس اطلاعات علمی و کافی اقدام می نماید.

ج-*تشکیل گروه های دیده بانی و پویش های محیطی*؛ این گروه به منظور کشف سیگنال های تغییر دائما باید پایش مستمر تغییرات در حوزه های جاسوسی سایبری و جرائم تروریستی را در دستور کار خود قرار دهد، باشد و با رصد و پایش و پویش های محیطی هدفمند نسبت به شناسایی روندها و مخاطرات احتمالی اقدام نموده و در پیشگیری از جرائم تروریستی در آینده اقدام می نماید.

منابع

اردبیلی، محمدعلی (۱۳۸۸). حقوق جزای عمومی، تهران: نشر میزان، چاپ چهاردهم.

آقاجانی‌رونقی، آیدا (۱۳۹۷). جاسوسای سایبری از دیدگاه حقوق بین‌الملل، پایان‌نامه دوره کارشناسی ارشد حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبایی.

بصیری، محمدعلی و آقامحمدی، زهرا (۱۳۹٦). آینده‌پژوهی خاورمیانه طی سه دهه آینده؛ تحلیل روندهای مقابله با تروریسم در سطح بین‌الملل، تحقیقات سیاسی و بین‌المللی، شماره ۳۱، تابستان، ۸۷-۱۱٦.

پورمحمدی، محمدرضا؛ حسین‌زاده‌دلیر، کریم؛ رسول، قربانی و زالی، نادر (۱۳۸۹). مهندسی مجدد فرآیند برنامه‌ریزی با تأکید بر کاربرد آینده‌نگاری، جغرافیا و توسعه، شماره ۲۰، زمستان، ۵۸- ۳۷.

جلالی، محمود (۱٤۰۰). جاسوسی در حقوق بین‌الملل مدرن و ضرورت تدوین مقررات جهانی، مطالعات حقوق عمومی، شماره ۵۱، بهار، ۳٦۸-۳٤۳.

خدادوست، علی؛ مطلبی، مسعود و بای، عبدالرضا (۱٤۰۱). جمهوری اسلامی ایران و کاربست اصول اعلامیه حقوق بشر اسلامی در سیاست‌های مهاجرتی در قبال مهاجران افغانستانی، حقوق بشر اسلامی، شماره ۳، پاییز، ۱٤۳-۱۲۱.

رضایی، علی‌رضا و حشمتی، امیر (۱۳۹۵). نئوتروریسم با تأکید بر تروریسم مذهبی، حبل المتین، شماره ۵، بهار، ٦۸-٤٦.

زارع، محسن و قره‌باغی، ونوس (۱۳۹٤). تعارض میان جاسوسی و آزادی اطلاعات از منظر حقوق بین‌الملل بشر، مطالعات حقوق عمومی، شماره ٤، زمستان، ٦۰۹-٦۲۹.

شهبازی، آرامش، آقاجانی‌رونقی، آیدا (۱۳۹۹). جاسوسی سایبری در حقوق بین‌الملل: مسأله انتساب مسئولیت بین‌المللی به دولت در هاله‌ای از ابهام، مطالعات حقوق عمومی، شماره ٤، زمستان، ۱۵۰۳-۱٤۸۷.

فتاحی زفرقندی، سجاد؛ اسماعیلی، مهدی و حاجی‌تبار فیروزجایی، حسن (۱۳۹۹)، «پیشگیری از جرم جاسوسی سایبری نیروهای مسلح و نقش آن در تامین حق امنیت»، حقوق بشر اسلامی، شماره ۹، بهار، ۲۷٦-۲۵۵.

قدیر، محسن و کاظمی‌فروشانی، حسین (۱۳۹۸). بررسی تطبیقی حقوق کیفری ایران با اسناد بین‌المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری، حقوقی بین‌المللی، شماره ٦۰، بهار، ۲٤۸-۲۳۱.

کاویانی، حسن؛ ابراهیمی، حسین و ساعدی، بیژن (۱۳۹۸). آینده پژوهی سناریوهای احتمالی گروهک‌های تروریستی در استان سیستان و بلوچستان، راهبرد دفاعی، شماره ۱۷، پاییز، ۱۱۱-۱۳۹.

محمدحسینی، بابک؛ هادی‌زاده، مرتضی و ساکی، یلدا (۱٤۰۱). سناریوهای محتمل بر آینده تجهیزات پزشکی در ایران با تاکید بر فناوری‌های نوین اطلاعاتی و تأثیرات کرونا ویروس، آینده پژوهی ایران، شماره ۷، تابستان، ۲۳٤-۲۰۳.

محمدی‌لرد، عبدالمحمود (۱۳۹۳). آینده پژوهی ثبات سیاسی ایران، تهران: پژوهشکده مطالعات راهبردی، چاپ اول.

مظفری، علی (۱۳۸۸). آینده پژوهی بسترعبور از مرزهای دانش، نظم و امنیت انتظامی، شماره ۲، تابستان، ۵۱-۳۹.

ناظمی، امیر و قدیری، روح اله (۱۳۸۵). آینده‌نگاری از مفهوم تا اجرا، مرکز صنایع نوین، وزارت صنایع و معادن، تهران.

نعمتی، لیلا، سیدمرتضی‌حسینی، راحله، مهدوی‌پور، اعظم (۱۳۹۹). رهیافت های پیش‌نگرانه در مهار تروریسم، پژوهش حقوق کیفری، شماره ۳۰، بهار، ۲۳۱-۲۵۸.

هلیلی، خداداد (۱٤۰۰). فناوری‌های نوظهور سایبری و تهدیدات ناشی از بکارگیری آنها در سازمان‌های دفاعی- نظامی، مطالعات جنگ، شماره ۳، پاییز، ۱۲۱-۹۷.

Angheloiu, C., Sheldrick, L., & Tennant, M. (2020). Future tense: Exploring dissonance in young people's images of the future through design futures methods. Futures, 117, 102527١٤٤.

Buchan, Russell (2018), Cyber Espionage and International Law, Oxford: Hart.

Buchan, Russell and Iñaki Navarrete (2021), "Cyber espionage and international law", in:Research Handbook on International Law and Cyberspace, Edited: Nicholas Tsagouriasand Russell Buchan, elgaronline.

Bell, Wendell. (2003), Foundation of Futures Studies: History, Purposes, and Knowledge (Human Science for New Era), London: Transaction Publishers.

Laqueur, W. (2018), the Future of Terrorism: ISIS, Al-Qaeda, and the Alt-Right, Publisher: Thomas Dunne Books.

Lia, B. (2005), Globalisation and the Future of Terrorism: Patterns and Predictions, Routledge.

Mannik, E. (2011), «Terrorism: Its Past, Present and Future Prospects», Journal: KVÜÕA toimetised.— Buchan, Russell (2021), Cyber Espionage and International Law, Hart Publishing.

Pehlivan, Oğuz (2020), Confronting Cyberespionage Under International Law, Routledge Taylor & Francis eBooks.

Sander, B. (2019), "The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations", In 2019 11th International Conference on Cyber Conflict (CyCon), Vol. 900, pp. 1-21, IEEE.

Kegley Jr, Charles W. Raymond, Gregory A. (2005). *Preemptive War Does Not Reduce Terrorism*, United States of America, Gale and Greenhaven Press.

Donkin, Susan. (2011). *the Evolution of Pre-emption in Anti-Terrorism Law*, ARC Centre of Excellence in Policing and Security, Education and Law Griffith University.

White, Lisa. (2008). *Australia: Terrorism Laws: Control Orders*, the Law Library of Congress.

Deeks, A. (2015), "An International Legal Framework for Surveillance', Virginia Journal of International Law, Vol. 55, No.2.

Kilovaty, I. (2016), "World Wide Web of Exploitations-The Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach", Colum. Sci. & Tech. L. Rev., 18.

Katharina Ziolkowski, (2013), "Peacetime Cyber Espionage – New Tendencies in Public International Law", in Katharina Ziolkowski (ED.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy (NATO CCD COE)

Sulick, Michael J. (2013), Counterintelligence in the War Against Terrorism, Stadies in intelligence, Vol. 48, No. 4.

William C. Banks, Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage, Emory Law Journal Online, 2017, Vol. 66, p. 513.

Hajizadeh, Ali, Valliere, Dave. (2022). Entrepreneurial foresight: Discovery of future opportunities,135

Gariboldi, M. I., Lin, V., Bland, J., Auplish, M., & Cawthorne, A. (2021). Foresight in the time of COVID-19. The Lancet Regional Health - Western Pacific, 6.