تحلیل سازه‌انگارانه تروریسم سایبری و رویکرد نظام حقوقی به آن

حسین احمری *

غلامرضا کحلکی[**]

حامد رحیم‌پور اصفهانی[***]

چکیده

تروریسم سایبری از مصادیق مدرن تهدیدهای تروریستی است که به سبب استفاده از فناوری‌های نوین و رایانه‌ای در فضای مجازی در آن، توسط بازیگرانی در عرصه بین‌الملل مورداستفاده قرار می‌گیرند و از دانش تکنولوژیکی بالا برخوردار هستند. ازآنجایی‌که معمای امنیت بزرگ‌ترین مسئله بشری بوده و تهدیدهای امنیتی تروریسم نوین سایبری آن‌گونه که سازه‌انگاران معتقدند از رهگذر برساخت‌های امنیتی و هویتی باید نگریسته شود، این پژوهش، امنیت سایبری را مبتنی بر ساختارهای هویتی و امنیتی مورد ارزیابی قرار داده است که به شکل‌گیری نظام‌های حقوقی در عرصه داخلی و بین‌المللی انجامیده؛ درواقع، از این منظر که دولت‌ها بازیگران محوری در عرصه تعاملات بین‌المللی

---

*. عضو هیئت‌علمی فقه و مبانی حقوق دانشگاه آزاد اسلامی مشهد.

**. دانشجوی دکتری تخصصی روابط بین‌الملل دانشگاه آزاد اسلامی شاهرود و محقق روابط بین‌الملل اسلامی در بنیاد پژوهش‌های اسلامی آستان قدس رضوی(نویسنده مسئول: phdkahlakireza@hotmail.com).

***. دانشجوی دکتری تخصصی فقه و مبانی حقوق دانشگاه آزاد اسلامی مشهد و دبیر سرویس بین‌الملل روزنامه خراسان.

تاریخ دریافت: ۱۳۹۴/۰۴/۰۸ تاریخ پذیرش: ۱۳۹۵/۰۲/۱۶

فصلنـــامه پژوهش‌های روابط بین‌الملل، دوره نخست، شماره نوزدهم، صص ۳۳۴ - ۳۰۵.

هستند و در کنار دیگر فعالین عرصه بین‌المللی با عنایت به نوع نگاه هویتی خود قواعد حقوقی را تبیین می‌کنند، این نوشته تلاش کرد که با تبیین اجمالی مفهوم عام تروریسم سایبری به‌عنوان یک پدیدهٔ مجرمانه، راهکارها و خلأهای نظام حقوقی برای مقابله با آن را بررسی کند. این پژوهش، از رهگذر مطالعه‌ای بین‌رشته‌ای و مبتنی بر نگاهی سازه انگارانه، پدیده سایبر تروریسم را بررسی کرد و به این سوال مهم پاسخ داد که چگونه چارچوب‌های ذهنی بازیگران در عرصه بین‌المللی بر ایجاد تهدیدهای سایبری مؤثر خواهد بود و در حل این معمای امنیتی نیز، در فرآیندی اجتماعی، هویت بازیگران و برداشت‌های آن‌ها در پیشگیری و تدوین قوانین در عرصه بین‌المللی، مؤثر است.

واژه‌های کلیدی: *سازه‌انگاری، برساخته‌های هویتی- امنیتی، فضای سایبری، تروریسم سایبری، پیشگیری، نظام حقوقی.*

مقدمه

فناوری‌های نوین اطلاعاتی و ارتباطی نظیر اینترنت، بستری است برای فعالیت کنش‌گران در محیطی متمایز از فضای واقعی که در آن ایفای نقش می‌کنند که دارای ویژگی‌های جدیدی است؛ این محیط جدید، «فضای مجازی»[1] نام‌گرفته است. روابط در جوامع و میان آن‌ها در شرایط فعلی، متمایز از گذشته است و ویژگی‌های جوامع امروزی نظیر «اقتصاد اطلاعاتی»، «فرهنگ مجازی» و کاهش اهمیت زمان و مکان در تعاملات اجتماعی، ماهیت ارتباطات را مجازی، شبکه‌ای و جهانی کرده است. ویژگی متمایز ارتباطات در هزاره سوم این است که اصل بنیادین آن، اهتمام محوری فرد در عرصه فعالیت‌های اجتماعی، سیاسی و اقتصادی به بهره‌گیری از ابزارهای نوین اطلاعاتی و ارتباطی است. در چنین فضایی که با عنوان «فضای مجازی» توصیف می‌شود، تهدیدهای نوینی همانند جنگ مجازی، «جنگ اطلاعاتی»، «تروریسم سایبری»، «پدیده هکرها» و سرقت اطلاعات محرمانه نهادهای امنیتی و اطلاعاتی پدید آمده‌اند که می‌توانند امنیت ملی کشورها را با چالش جدی مواجه سازند. به‌علاوه، پیشرفت فنی در زمینه ارتباطات، موجب ظهور قواعد حقوقی و به‌تبع آن، رفتارهای نوین فاصله‌گیر از هنجارها شده است که این موضوع، نه‌تنها اموال بلکه اشخاص و دولت‌ها را نیز در برمی‌گیرد و آن‌ها را تحت حمایت قرار می‌دهد (جلالی‌فراهانی، ۱۳۸۷: ۴۱-۴۰).

در این میان، یکی از مهم‌ترین تهدیدهای نوظهور، تروریسم سایبری است که به‌واسطه کاربست فزاینده فناوری اطلاعاتی و ارتباطی از سوی دولت‌ها برای تسریع، افزایش کارایی و کاهش هزینه‌های مرتبط با خدمت‌رسانی به شهروندان، اهمیت فزاینده‌ای پیداکرده است. به‌گونه‌ای که حتی دولت‌ها نیز از تروریسم سایبری به‌عنوان ابزاری در الگوی تنازعی

1. Cyberspace

خود استفاده می‌کنند. مهم‌ترین مولدهای ناامن‌کننده فضای مجازی در بعد تروریسم، در دو گروه عمده طبقه‌بندی می‌شوند؛ گروه اول کسانی که به یک کشور خارجی وابسته‌اند، از قبیل بخش‌های نظامی، سازمان‌های امنیتی و شرکت‌هایی که وابستگی زیادی به دولت آن کشور دارند؛ و گروه دوم؛ تروریست‌ها و گروه افراطی (نورمحمدی،۱۳۹۰: ۷۷). اما تروریسم سایبری یک چهره جدید و دگرگون‌شده از پدیده تروریسم است که عامل تحقق آن، گسترش فناوری و تحقق فضای مجازی بوده است (پاکزاد، ۱۳۷۵: ۲). این شکل مدرن از تروریسم، باعث شده تا عاملان آن بدون ترس از خطرهای سایر اقسام اقدامات تروریستی، تنها با استفاده از تکنولوژی، اهداف وحشت‌بار خود را دنبال کنند. گسترش استفاده از این فضای مجازی که از دهه ۱۹۹۰ شدت گرفته است، امکان رسیدن تروریست‌ها به اهدافشان را بیشتر کرده است. حضور میلیون‌ها کاربر در دنیای مجازی، همراه با شرکت‌ها، کارخانه‌ها و صنایع عمده بسیار که در اغلب موارد از قابلیت آسیب‌پذیری بالایی برخوردارند، خطر استفاده سوء از فضای مجازی را بیشتر کرده و جذابیت آن را نیز افزایش داده است (کارگری،۱۳۹۰: ۷۳-۷۲). بر پایه آنچه اظهار شد می‌توان تصریح کرد که برای بهره‌برداری صحیح و مفید از امکانات سایبری باید هنجارهایی را مقرر کرد و به مقابله با ناهنجاری‌ها پرداخت. این هنجارها باید بر مبنای ویژگی‌های منحصربه‌فرد در فضای سایبر تدوین شوند. ازاین‌رو، برای پیشگیری از تهدیدهای ناشی از ناهنجارهای برآمده از فضای سایبری، تاکنون اسناد متعددی به تصویب رسیده است، اما باوجود تنوع این اسناد در نظام‌های ملی و بین‌المللی، متأسفانه هیچ‌یک از آن‌ها موجبات تحقق وضعیتی مطلوب را در مواجهه با تهدیدها فراهم نکرده است (نمامیان، ۱۳۹۰: ۱).

از دیگر سو، این مهم است که بگوییم این تهدیدهای امنیتی و برنامه‌ریزی‌های حقوقی در برابر آن، بر چه نوع نگاهی به مقوله امنیت استوار است. این امر پذیرفته‌شده است که امنیت اصلی‌ترین وظیفه دولت‌های ملی و از مهم‌ترین موضوعاتی است که تاکنون اندیشمندان روابط بین‌الملل به آن پرداخته‌اند. این اندیشمندان از رهگذر نظریه‌هایی چون واقع‌گرایی، لیبرالیسم، مکتب کپنهاگ، سازه‌انگاری و انتقادی به این مهم نگریسته‌اند؛ اما «سازه‌انگاران»[1] با عنایت به نگاه بینابینی به امنیت، درک درستی از این مهم ارائه می‌کنند.

مفهوم‌شناسی سایبر تروریسم در پیوند با امنیت هویتی و برساخته

1. Constructivists

پیش از هر چیز در این پژوهش ضروری است تا مفهوم سایبر تروریسم را به‌صورت علمی درک کنیم. همچنین، استفاده از نظریه‌های علمی برای فهم پدیده‌های عرصه بین‌الملل، میان اندیشمندان روابط بین‌الملل مرسوم است که در این پژوهش به‌واسطه رویکرد جامع سازه انگاران از نوع نگاه آنان به مقوله امنیت در تفسیر تهدیدهای سایبری استفاده خواهیم کرد.

۱-۱. مفهوم سایبر تروریسم

۱-۱-۱. ماهیت تهدیدات سایبری

امروزه اینترنت در سراسر دنیا حدود ۳ میلیارد نفر کاربر دارد. با این وجود، اینترنت دولت‌ها را در مقابل چالش‌های جدید امنیتی قرار داده است. هزینه کم ورود، ناشناس‌بودن، مشخص‌نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان‌یافته و تروریستی و حتی افراد به این فضا واردشده و تهدیدهایی همچون جنگ سایبری، جرائم سایبری، تروریسم سایبری، جاسوسی سایبری و مانند آنها را به وجود آورند (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۲) .

نخستین بهره‌گیری از واژه سایبر تروریسم را باید در دهه ۱۹۸۰ به «باری کالین» نسبت داد (لی جی، ۱۳۸۹: ۹۸ ؛ جلالی‌فراهانی، ۱۳۸۵: ۸۵). این اصطلاح به معنای حمله‌کردن و یا تهدید به آن علیه رایانه‌ها و یا شبکه‌های رایانه‌ای است که هدف آن عمدتاً اطلاعات نهفته شده در این رایانه‌ها است. تروریست در این اقدام خود می‌کوشد تا دولت یا اتباع آن را برای پیشبرد اهداف سیاسی یا اجتماعی خاص خود، بترساند و یا تحت‌فشار قرار دهد تا او را مجبور به تن‌دادن به خواسته‌هایش کند (سیمبر، ۱۳۸۰: ۷۰). تروریسم سایبری این‌گونه نیز معنا شده است: «بهره‌گیری از اینترنت و شبکه‌های رایانه‌ای و امکاناتی که این شبکه‌ها پدید می‌آورند باهدف نابود ساختن ساختارهای زیربنایی یک جامعه مانند انرژی، حمل‌ونقل، فعالیت‌های دولتی و تأثیر گذاشتن بر یک دولت، شهروندان، گروه‌ها و ...» (عباسی،۱۳۸۳: ۳۰). همچنین «دوروثی دنینگ»[1] سایبر تروریسم را این‌گونه تعریف می‌کند:«سایبر تروریسم حاصل همگرایی تروریسم و فضای مجازی است، سایبر تروریسم

1. Dorothy Denning

به معنای تهاجم و تهدید به تهاجم غیرقانونی به رایانه‌ها، شبکه‌ها و اطلاعات ذخیره‌شده در آنهاست که به منظور ارعاب یا وادارکردن یک دولت یا مردم آن به پیشبرد اهداف سیاسی یا اجتماعی خاص صورت می‌گیرد (Hancock, 2001: 556). در همایشی که در ۲ مارس ۲۰۱۰ از سوی «مؤسسه بین‌المللی CACI» و «مؤسسه مطالعاتی نیروی دریایی ایالات‌متحده» با عنوان «تهدیدهای سایبری امنیت ملی و مقابله با چالش‌های پیش روی زنجیره عرضه جهانی» برگزار شد، تهدیدهای سایبری به‌صورت«وقایعی که به‌صورت طبیعی و یا توسط انسان(به‌صورت عمدی یا غیرعمدی)بر فضای مجازی تأثیرگذار باشد یا حوادثی که از طریق فضای مجازی عمل کند یا به نحوی به آن مرتبط باشد»، تعریف شد (CACI and USNI, 2010). فضای سایبری از سوی برخی کارشناسان به‌عنوان« تأثیر فضا و جامعه‌ای که توسط رایانه‌ها، اطلاعات و ابزارهای الکترونیکی، شبکه‌های دیجیتالی و یا کاربران آن شکل می‌گیرد» تعریف‌شده است (Lord and Sharp, 2011: 10). فضای سایبر یا فضای مجازی نیز در تعریف برخی نویسندگان عبارت است از:« مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی است».

دنیای امروزی رایانه که در ارتباط بازندگی مردم است، دنیایی است که هرلحظه مورد تهدید تروریست‌هاست و این نگرانی و احتمال وقوع این اتفاق، روزبه‌روز هر چه بیشتر مردم جوامع را دچار ترس و وحشت می‌کند (طیب،۱۳۸۴: ۸۹). «فضای سایبر»، فضایی غیرمادی و ناملموس است که توسط رایانه‌ها و شبکه‌های رایانه‌ای به وجود آمده و دنیایی مجازی را در کنار دنیای واقعی ایجاد نموده است (فضلی، ۱۳۸۹: ۱۷). این فضا، فراتر از اینترنت توسعه‌یافته است و تمامی فعالیت‌های دیجیتال شبکه‌ای را در برمی‌گیرد؛ فضای مذکور دارای گستره‌ای جهانی و بدون مرز ، پوشیده و پنهان، ناهنجارمند و کنترل‌ناپذیر است؛ فضای سایبر ماهیتاً برای آزادی گردش اطلاعات شکل‌گرفته و محدودیت در این فضا معنا ندارد» (پاکزاد، ۱۳۹۰: ۲۱۶).

۲-۱-۱. ویژگی‌های تهدیدهای سایبری

تهدیدهای سایبری ویژگی‌های منحصربه‌فردی دارند. از یک‌سو، این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند و از سوی دیگر،

هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری ، موجب شده بازیگران زیادی به این عرصه وارد شوند. مهم‌ترین ویژگی‌های تهدیدهای سایبری در مؤلفه‌های زیر خلاصه می‌شود:

الف. تعدد بازیگران در فضای سایبری: اتصال گسترده به اینترنت و سهولت ایجاد یا بدست آوردن نرم‌افزارهای مخرب به این معناست که تقریباً هرکسی می‌تواند به این فضا وارد شود. این بازیگران شامل افراد، گروه‌های سازمان‌یافته جنایی، گروه‌های تروریستی، شرکت‌های خصوصی و دولت-ملت هستند (Charney,2009: 5-6).

ب. هزینه کم و سرعت‌بالای اقدام: هر فرد برای انجام حمله سایبری تنها به یک رایانه، یک ارتباط اینترنتی و دانش فنی محدود درزمینه فضای سایبری نیاز دارد. درنتیجه، فضای سایبری شرایطی را فراهم کرده است که با هزینه پایین می‌توان اقدامات خطرناکی را در مدت‌زمان کم و با سرعت‌بالایی انجام داد. البته، انجام حملات پیچیده‌تر سایبری نیازمند صرف هزینه‌های بالاتری است (Lord and Sharp, 2011: 20-28).

پ. ناشناس ماندن بازیگران و عدم قابلیت ردیابی: مزیت برجسته این ابزارها که امکان به‌کارگیری بهینه را برای گروه‌های تروریستی فراهم می‌آورد، امکان «رمزگذاری»[1]محتوای ارتباطات الکترونیکی با ابزارهای بسیار پیشرفته است که احتمال «رمزگشایی»[2] آن‌ها را بسیار ضعیف می‌گرداند. افراد فعال در عرصه اینترنت می‌توانند از اقصی نقاط دنیا، بدون هشدار و در عرض چند ثانیه و بدون آنکه اثر یا نامی از خود بر جای بگذارند، اهداف دیجیتالی را مورد هدف قرار دهند (محسنی، ۱۳۹۰: ۲۰۲).

ت. تأثیرگذاری شگرف: ماهیت خاص فضای سایبری شرایطی را به‌وجود آورده است که بروز هر اختلال یا وقفه می‌تواند تأثیرات و پیامدهای به‌مراتب بیشتری از حادثه اولیه در پی داشته باشد. وقوع حمله‌های سایبری و در نتیجه آن، بروز اختلال در شبکه‌ها می‌تواند موجب ایجاد خسارت به اموال، زمان، محصولات و تولیدات، اعتبار، اطلاعات حساس و حتی ازدست‌دادن جان انسان‌ها شود، زیرا در این‌گونه مواقع،

1. Cryptography
2. Decryption

زیرساخت‌ها و سامانه‌های مهم دچار آسیب می‌شوند. از سوی دیگر، پوشش خبری و رسانه‌ای بیشتری را ایجاد می‌کند و این همان چیزی است که تروریست‌ها به دنبال آن هستند (بختیاری، ۱۳۸۹: ۷).

ث. کمرنگ‌شدن نقش جغرافیا: فضای سایبری سرعت انتقال به سراسر جهان را در لحظه کوتاهی فراهم کرده است. بنابراین، تهدیدکنندگان قادر به فراتر رفتن از محدوده جغرافیایی خود و رسیدن به اهداف کلیدی‌شان هستند (Starr, 2009: 18). به عبارت بهتر، فناوری‌های اطلاعات و ارتباطات تمامی مرزها را درمی‌نوردند و از جهان مرززدایی می‌کنند. این مرززدایی و کمرنگ کردن مرزهای سنتی، زمینه تسهیل حرکت هر چه آزادانه‌تر کالا، سرمایه و افراد را فراهم می‌کند.

ج. ساختار فضای اینترنت: اینترنت، دامنه مشترک و یکپارچه است. استفاده از این فضا توسط شهروندان، شرکت‌ها و دولت‌ها به شیوه‌ای است که جداسازی آن‌ها بسیار دشوار است. توانایی محدود برای جدا کردن بازیگران و فعالیت‌های آن‌ها، پاسخ مناسب به تهدید را بسیار دشوارتر کرده است. از سوی دیگر، ساختار اینترنت، دولت‌ها و شرکت‌های خصوصی را با عدم اطمینان در قبال خطرات فضای اینترنتی مواجه کرده است. این عدم قطعیت ناشی از پیچیدگی‌ها و فن‌آوری در حال تکامل برای پشتیبانی از سیستم‌های حیاتی است (Haller and Et al, 2010: 4).

چ. پایین‌بودن احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری

احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری پایین است. درنتیجه، افراد و سازمان‌ها نیز این فضا را در مقایسه با گزینه‌های جایگزین غیرسایبری مطمئن‌تر و دارای خطرات کمتری می‌بینند(Lord and Sharp, 2011).

۲. امنیت برساخته سایبری در فضای جهانی شده

۲-۱. امنیت در فضای جهانی شده

مفهوم امنیت همچون دیگر مفاهیم اساسی و رایج در علوم انسانی همانند صلح، عدالت و آزادی، تفاسیر گوناگونی به خود دیده است. شاید درک «باری بوزان» از آن دقیق باشد که آن را برابر بارهایی از تهدید می‌داند و مطرح می‌کند که امنیت در فقدان تهدید

است که خود را نمایان می‌سازد (عبدالله خانی، ۱۳۸۳: ۱۳۵). از دید «آرنولد ولفرز»[1] امنیت در یک مفهوم عینی به فقدان تهدیدها نسبت به ارزش‌های اکتسابی تلقی می‌شود و در یک مفهوم ذهنی بر اساس دلهره و نگرانی از به مخاطره افتادن ارزش‌ها و توانمندی‌های لازم در کسب نتایج منصفانه ارزیابی می‌شود (چگینی‌زاده، ۱۳۷۹: ۶۸). بنابراین یکی از دلایل پیچیدگی مفهوم امنیت و ماهیت ابهام‌آمیز آن، چندوجهی بودن مفهوم امنیت است. وجوه و ابعاد مختلف امنیت را می‌توان در محورهای سیاسی، اقتصادی، نظامی، فرهنگی و زیست‌محیطی دسته‌بندی کرد (ماندل، ۱۳۷۹: ۸۳- ۷۱). از سوی دیگر، امنیت صرفاً در یک قلمرو یا محدوده خاص قابل‌پیگیری و دستیابی نیست بلکه امنیت در قلمروهای مختلف که درعین‌حال به‌هم‌پیوسته و وابسته و دارای تأثیرات متقابل نسبت به یکدیگر می‌باشند، قابل‌پیگیری و تحلیل است. «دیوید هاروی»[2] بر این باور است که جهانی‌شدن به مرحله شدیدی از فشردگی زمان و مکان منجر شده که دارای تأثیر گیج‌کننده و مخرب بر رویه‌های سیاسی و اقتصادی و توازن قدرت طبقات و نیز زندگی فرهنگی و اجتماعی است (Harvey, 1989: 240). مانوئل والرشتاین جهانی‌شدن را شکل‌گیری شبکه‌ای می‌داند که طی آن اجتماعاتی که پیش از آن در کره خاکی دورافتاده و منزوی بودند، با یکدیگر ادغام می‌شوند (گل‌محمدی، ۱۳۸۶: ۲۲). بسیاری از نویسندگان ویژگی اصلی جهانی‌شدن را در مفاهیمی چون ظهور دهکده الکترونیک جهانی، پیدایش قبیله جهانی، انقلاب اطلاعاتی، فشردگی زمان و مکان، گسترش جهان، آگاهی، پایان تاریخ و عصر سیبرنتیک خلاصه کرده‌اند. بنابر تعاریفی که به آن اشاره شد جهانی‌شدن پدیده‌ای است که براثر وقوع آن نقش مرزهای جغرافیایی در تصمیم‌گیری‌ها و فعالیت‌های اقتصادی، اجتماعی و فرهنگی انسان‌ها، به حداقل کاهش می‌یابد. تکنولوژی‌های نوین ارتباطاتی در جهان، ایده‌ای موسوم به دهکده جهانی را تحقق عینی بخشیده و مردم اکنون در جهانی زندگی می‌کنند که از هر لحاظ تحت دیده تیزبین یکدیگر قرار دارند. اصطلاح «آکواریوم جهانی»[3] و یا «جهان شیشه‌ای»[4] زاییده همین تصور است. (منتظری، ۱۳۸۹: ۳-۱).

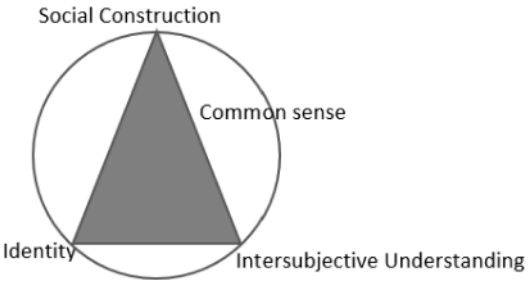
1. Arnold Wolfers
2. David Harvey
3. Aquarium World
4. Glass world

۲-۲. امنیت هویتی و برساخته

درحالی‌که «اثبات‌گرایانی»[1] نظیر «واقع‌گرایان»[2] از امنیت دولت و قدرت محور سخن می‌گویند و به مؤلفه‌های سخت‌افزاری امنیت تأکید می‌کنند، «فرا اثبات‌گرایان»[3]به جنبه‌های غیر عینی و ذهنی آن توجه دارند. در این میان، «سازه انگاران»[4]دیدگاه میانه‌ای به امنیت دارند. سازه انگاران به برساخته بودن امنیت و امنیت هویتی تأکیددارند. در تبیین بستر شکل‌گیری سازه‌انگاری باید به تحولات شگرف دهه ۱۹۸۰ و تغییر در سیاست خارجی «اتحاد جماهیر شوروی»[5]در دوران «گورباچف»[6] اشاره کرد. در این دوران مناظره‌های نو-نو میان نوواقع‌گرایی و نئولیبرالیسم در تبیین واقعیت‌های عرصه بین‌الملل ناکارآمد نشان دادند و ازاین‌رو، راه برای مطرح‌شدن بیش‌ازپیش «نظریه‌های انتقادی»[7] فراهم شد (یزدان فام، ۱۳۸۶). از منظر ریشه‌شناسانه، نظریه سازه‌انگاری، ریشه در بذر نخستینی دارد که «کانت»[8] و «ویتگنشتاین»[9]در بستر اندیشه سیاسی نهادند. براین اساس، نظریه‌پردازان سازه انگار بر این باورند که «واقعیت‌های اجتماعی»[10] محصول «ساختارهای زبانی»[11]است. از منظر سازه انگاران، «شناخت»[12] بدون اینکه مسئله‌ای در واقعیت بیرونی مطرح باشد میسر نیست و این شناخت مبتنی بر «ساخت یابی اجتماعی»[13] و «فهم بینا ذهنی»[14] به‌واسطه مشارکت معانی مقدور است. بر این اساس از منظر سازه انگاران واقعیت‌ها در عرصه بین‌المللی از رهگذر یک هستی‌شناسی رابطه‌ای قابل‌درک است و برخلاف اندیشمندان جریان اصلی که بر عناصر مادی تأکیددارند، آنان بر عوامل فکری و معنا گرایانه نظیر فرهنگ، انگاره‌ها، هویت، هنجارها و ارزش‌ها در کنار این عناصر مادی،

1. Positivists
2. Realists
3. Post-Positivists
4. Constructivists
5. Soviet Union
٦. Gorbachev
7. Critical Theory
8. Kant
9. Wittgenstein
10. Social Realities
11. Language Structures
12. Objective
13. Social Strucration
14. Intersubjective Understanding

عنایت ویژه دارند. بنابراین از منظر سازه انگاران، قوام دهی متقابل ساختار و کارگزار و نقش «هویت»[1] در درک کنشگران از تهدید و امنیت و نقش قواعد در نظم دادن به امور و روابط اجتماعی، بسیار اهمیت دارد (ونت، ۱۳۸۴). منظومه شناخت در سازه‌انگاری درنهایت به یک فهم مشترک ختم می‌شود که در بستر اجتماع است و با عنایت به نوع نگاه به خود و دیگر قوام‌یافته و مبتنی بر فهمی بینا ذهنی است.



تصویر ۱. منظومه شناخت از منظر سازه‌انگاران

سازه‌انگاران، هرگز مردم را در وضع طبیعی فهم نمی‌کنند (Bellamy, 2004: 6). از منظر اونوف اینکه آنارشی را یک مفروض بدانیم، اشتباه است (Onuf, 1999). اندیشمندان سازه انگار همچون «الکساندر ونت»[2]، آنارشی را چیزی می‌داند که دولت‌ها از آن می‌فهمند. ازاین‌رو آنارشی گرایش به اقدام خودمختارانه است که در سطح خرد، ناشی از تمایل کشورها برای حاکمیت بیشتر و در سطح کلان نیز، گرایش برای حاکمیتی است جهانی. در بعد امنیت نیز سازه‌انگاران مفهوم تهدید عینی را باطل می‌دانند. درواقع آن‌گونه که در اندیشه مربوط به راه میانه معتقدان به سازه‌انگاری مطرح است، بازیگران از روی ارزش‌ها و هنجارهای حاکم بر سیاست‌های داخلی است که رفتارهای شرکای خود را در عرصه بین‌المللی فهم می‌کنند (Hopf, 1998: 171-200). ازاین‌رو است که سازه‌انگاران ائتلاف‌ها و اتحادها را در عرصه بین‌المللی نه برای حل معمای امنیت و در برابر تهدید می‌دانند که آن را بر اساس ارزش‌های مشترک درک می‌کنند. بنابراین از منظر سازه انگاران، هویت ملی به دولت‌ها کمک می‌کند تا بر اساس برداشتی که از خود دارند، تهدیدهای امنیت

1. Identity
2. Alexander Wendt

ملی را تعریف کنند و به سازوکارهای شکل‌دادن به متحدین خود بی‌اندیشند. دولت‌ها، بر اساس هویت خود، دشمنانشان، رقبا و دوستان خود را درک می‌کنند و در این فرآیند، هویت خود را تعریف و بازتعریف می‌نمایند. دولت‌ها بر اساس انتظاری که از دیگران دارند، رفتار خود را تنظیم می‌کنند (Kubalkova, 2001: 34).

تأکید سازه‌انگاران بر نقش فرهنگ و هویت در روابط بین‌الملل و مطالعات امنیتی، توجهات را به‌سوی رویارویی فرهنگ‌ها و نقش آن در بروز منازعات جلب کرده است. بر این اساس، فرهنگ عامل شکل‌دهنده به هویت بازیگران و برداشت آن‌ها از خود و دیگران در عرصه بین‌المللی است. از این منظر است که بازیگران در عرصه بین‌المللی، بر اساس تعریف از خود دست به اقدام می‌زنند و از همین منظور به امنیت و تهدیدها نگاهی هویتی دارند (Kowert, 2001: 268-269). اما نباید از خاطر برد که هویت دولت‌ها در تعامل با دیگران و به‌صورت اجتماعی شکل می‌گیرد. در این رویکرد دولت‌ها نهادهایی هستند که موجودیت و خصوصیت‌شان وابسته به بازتولید انواع خاصی از رویه‌هاست. بنابراین در این رویکرد که هنوز هم دولت‌محوری در آن پررنگ است، دولت صرفاً واحد حقوقی و یا سازمان رسمی نیست، بلکه مجموعه‌ای از رویه‌هاست که به شکل هنجاری قوام یافتند.

نکته دیگر در نوع نگاه سازه‌انگاران به مقوله امنیت، «عادی‌شدن»[1]است که باعث شکل‌گیری «حس امنیت»[2] می‌شود. جالب است که ممکن است این عادی‌سازی مربوط به عادی‌سازی خطرهای امنیتی باشد. در نگاه سنتی فرض این است که دولت‌ها تنها در پی امنیت فیزیکی هستند و در مسیری که آن را طلب می‌کنند، به دیگران هم آسیب فیزیکی وارد می‌آورند؛ اما این شکل از امنیت، از منظر سازه انگاران، تنها شکلی از امنیت نیست که دولت‌ها و بازیگران در عرصه بین‌المللی در پی آن هستند. بازیگران در عرصه بین‌المللی از این رهگذر، به دنبال «امنیت هویتی»[3] نیز هستند. حال ممکن است که در شرایطی، تعامل آمیخته با منازعه و تهدید، تداوم‌یافته و درونی شود و آنگاه، این‌چنین تعاملی به هویت بازیگر تبدیل شود. اگر چنین تعاملی تکرار شود، نتیجه آن عادی شدن آن است. حال اگر یک امری عادی شود، تغییر این امر عادی شده، به‌مراتب ازآنچه واقع‌گرایان در ارتباط با معمای امنیت و رفع و تغییر آن می‌گویند دشوارتر است. هنگامی‌که بازیگران

1. Routine
2. Sense of Security
3. Security of Identity

در عرصه بین‌المللی در روندی قرار بگیرند که در آن عادی‌شدن رقابتی شکل‌گرفته باشد، دولت‌ها و بازیگران در این عرصه به رقابت، به‌عنوان هدف خود مشغول می‌شوند. اینجا دیگر امنیت فیزیکی مطرح نیست، اینجا امنیت «هستی‌شناسانه»[1] است که تکرار و تقویت می‌گردد و این رویه‌های عادی شده است که میان بازیگران حکم می‌کند. به‌این‌ترتیب است که آنچه در اول وسیله تأمین امنیت بود، در پایان، به هدف تبدیل می‌شود و برای حفظ ظرفیت کارگزاری، لازم است تا منازعه به‌طور مداوم بازتولید گردد. ازاینجا به بعد دیگر حتی وابستگی به رقابت عادی شده دیگر در سطح گفتمانی نیست و در سطح عملی است که دنبال می‌گردد. ازاین‌رو است که دولت‌ها در رقابت عادی شده در سطح عمیق‌تر، منازعه را به همکاری ترجیح می‌دهند؛ زیرا آن‌ها تنها در منازعه است که خود را شناخته، هویت می‌یابند و درک می‌کنند که کی هستند. مفهوم امنیت هستی‌شناسانه است که علت درگیری میان دولت‌ها در شرایطی که آنان منازعه بر سر منافع ندارند را برایمان روشن می‌کند.

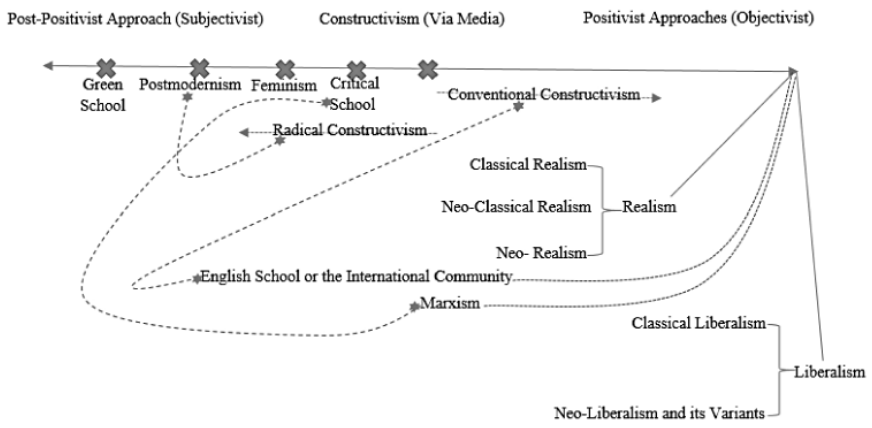
سخن کوتاه اینکه از منظر سازه‌انگاران، امنیت تنها یک امر مادی و بیرونی نیست، بلکه مفهومی است اجتماعی، بیناذهنی و معنایی که در فرآیند اجتماعی برساخته شده و قوام می‌یابد. نقش محوری در این ساخت‌یابی را فرهنگ و هویت ایفا می‌کند و در مرکز آن، امنیت انسانی است. اما سازه‌انگاران به امنیت جهانی نیز گرایش دارند.

۳-۲. تروریسم سایبری از رهگذر برساخته‌های هویتی

مفهوم امنیت همان‌گونه که پیشتر ذکر شد، تفاسیر گوناگونی به خود دیده و امنیت سایبری نیز از این قاعده مستثنا نیست. امنیت سایبری و رهایی از تهدیدهای سایبری مقوله‌ای است که به‌تنهایی با رویکردهای عین‌گرایانه قابل‌تحلیل نیست و شاید فهم جامع این شکل از تروریسم، نیازمند نگاهی «سیستماتیک»[2] است؛ سازه‌انگاران با عنایت توأمان خود به جنبه‌های عینی و ذهنی پدیده‌ها، نگاهی سراسربینانه به پدیده‌هایی نظیر تروریسم سایبری دارند؛ در این خصوص، می‌توان با رویکردی سازه‌انگارانه، نگاهی میانه به این پدیده داشت و آن را تحلیل کرد. در نمودار ذیل، تلاش می‌شود تا برای درک بهتر نوع نگاه

1. Ontological Security
2. Systematic

سازه‌انگاران به پدیده‌هایی نظیر تروریسم سایبری، جایگاه این رویکرد در میان نظریه‌های روابط بین‌الملل، به تصویر کشیده شود[1].



تصویر ۲. جایگاه سازه‌انگاری در نظریه‌های روابط بین‌الملل

در تحلیل تروریسم سایبری با رویکردی سازه انگارانه، می‌بایست به انگاره‌های عینی نظیر نقش دولت‌ها و دیگر بازیگران عرصه بین‌المللی در شکل‌گیری این معمای امنیتی و قواعد، هنجارها و منافع این بازیگران در کنار انگاره‌های هویتی و ذهنی شکل‌دهنده به این عینیات، در بستری اجتماعی توجه کرد. در نگاه سازه‌انگارانه به تهدیدهای سایبری، می‌بایست، هویتی نگریست. بر این اساس، هم عامل تهدید و نیز آنکه مورد هجوم سایبری واقعی می‌شود، اقدام‌های خود را با عنایت به نوع نگاه به خود و تعریف از دیگران، انجام می‌دهند. بازیگران سایبری، در خلأ نیستند و خود در محیطی اجتماعی نقش ایفا می‌کنند؛ همچنین، می‌توان دنیای مجازی را از این حیث که شبکه‌ای گسترده ایجاد می‌کند، نمودی از واقعیت دانست که ساختاری اجتماعی و فرامرزی را شکل داده است. کنش‌گران دولتی و غیر آن در این شبکه‌ها به تعامل با یکدیگر می‌پردازند و هویت می‌یابند. اگرچه

۱. این تصویر، جایگاه سازه‌انگاری به‌عنوان رویکردی میانه را ترسیم می‌کند و ازاین‌جهت که پژوهش حاضر صرفاً مربوط به معرفی نظریه‌های روابط بین‌الملل نیست، به تبیین نظریه‌های آورده شده در این تصویر نمی‌پردازد. ازاین‌رو بهتر است برای فهم نظریات ذکرشده در تصویر بالا، نظیر سازه‌انگاری متعارف که در تحلیل، رویکردی متمایل به‌عین دارد و رادیکال که معطوف به گرایش‌های ذهنی است، خواننده به کتاب‌های مربوط به نظریه‌های روابط بین‌الملل مراجعه کند. از جمله می‌توان رجوع شود به: (مشیر زاده، ۱۳۸۶) و (قوام؛ ۱۳۸۶).

گاهی به‌واسطه مجازی بودن این ساختار، هویت‌ها در آن جعلی است، اما این موجودیت‌ها رفته‌رفته «خرده‌فرهنگ‌ها»[1] را تغییر داده و می‌کوشد تا یک «فرهنگ جهانی»[2] ایجاد کند که این خود به شکل‌گیری هویتی مقاوم در برابر آن می‌انجامد. این مقاومتی که خود می‌تواند عاملی برای اشاعه تمایلات سایبری مخرب علیه هویت‌های رقیب باشد. ازاین‌رو، در قاموس ارتباطی شبکه‌های سایبری، این منافع، فرهنگ‌ها، انگاره‌ها، هویت‌ها، ارزش‌ها و هنجارها هستند که در چارچوب ساختارها یا بهتر بگوییم «اجتماعاتی سایبری»[3]، جریان دارند و در تعاملی دوسویه، میان ساختارها و کارگزاری‌ها در تلاش برای دست‌یابی به فهمی مشترک، عملکردهایشان را بر می‌سازند. ازاین‌رو یک دولت، بازیگران وابسته به دولت‌ها و یا بازیگرانی خودمختار در فضای سایبر با عنایت به انگاره‌های هویتی و ذهنی که از خود و توانمندی‌های خویش ساخته‌اند، انتخاب می‌کنند که چگونه در فضای سایبری عمل کنند؛ همانند یک تروریست سایبری و با توجه به انگاره‌های ذهنی خود و هدف، منافع خود را دنبال کنند و تروریستی عمل کنند، یا نه هویتی دفاعی و مستحکم را برای خود انتخاب کنند. این‌یک گفتمان است، گفتمانی با «زبان تکنولوژیکی»[4].

بازیگران عرصه بین‌المللی در «فضای جهانی سایبری»[5] یعنی «دولت‌ها»[6]، «افراد»[7]، «سازمان‌های بین‌المللی»[8]، «شرکت‌های فراملی»[9] و «ارتباطات بین‌المللی یا رسانه‌ها»[10] در «وضعی طبیعی» و «آنارشیک» عمل نمی‌کنند. فضای سایبری و وضعیت آن، نمایانگر همان برداشتی است که بازیگران از آن دارند؛ اما، هرگز فضای سایبری بین‌المللی همانند یک جنگل و بی‌قاعده نیست. اگرچه قواعد در این فضا جوان هستند، چون خود این فضا و اجتماعات درون آن جوان است، اما در سطح داخلی و بین‌المللی شاهد برساخته‌های کنترلی و هدایتی این فضا هستیم. فضای سایبری را قدرت‌ها و سرورهای آن‌ها به‌واسطه

1. Subcultures
2. Global Culture
3. Cyber Communities
4. Technological language
5. The Global Cyber Space
6. States
7. Individuals
8. International Organizations
9. Transnational Corporations
10. International Communications

«هویت کنترل‌کننده»[1] این قدرت‌ها که به منطق آن‌ها تبدیل‌شده است، در اختیاردارند، اما «هویت مقاوم» دیگر بازیگران در عرصه بین‌المللی، آن‌ها را به کنترل و بومی‌سازی فضاهای سایبری سوق داده است. البته در فضای سایبری همانند عرصه عمل آن، یعنی عرصه بین‌المللی، یک قدرت محوری و مرکزی نظیر یک دولت وجود ندارد، اما منافع و هویت بازیگران در این فضا است که کنش‌ها و واکنش‌ها در آن را شکل می‌دهد. یک تروریست سایبری مبتنی بر برداشت و منافع خود در این فضا عمل می‌کند که واکنش در برابر آن نیز، بر همین اساس شکل می‌گیرد.

سازه انگاران در نگاه خود به امنیت، تهدید را در عرصه بین‌المللی امری عینی و ناشی از سرشت بد کنشگران یا تحت تأثیر فشارهای سیستمی بین‌المللی و یک واقعیت عینی لازم برای حراست از امنیت و بقای خود نمی‌دانند. بازیگران عرصه بین‌المللی، سیستمی عمل می‌کنند و مقتضیات عینی و ذهنی خود را در رفتارهایشان منعکس می‌نمایند. ازاین‌رو است که یک تروریست سایبری و یا هدف آن، مبتنی بر انتظار خود از دیگران رفتارهایش را ترسیم می‌کند و جهان را از رهگذر هویتی خود می‌بینند. ازآنجاکه فرهنگ، خود در شکل‌گیری هویت‌ها نقشی محوری ایفا می‌کند، نبردهای سایبری مدرن را باید رویارویی فرهنگ‌ها دانست. فضای سایبری حدومرز فرهنگی ندارد و استفاده از آن نیز جهانی شده؛ ازاین‌رو یک‌شکل از جنگ‌ها میان فرهنگ و هویت‌های گوناگون، به این فضا کشیده شده است. از میان رویکردها به عامل ناامنی، برخورد میان حوزه‌های تمدنی و فرهنگی آن رویکردی است که سازه‌انگاران به آن بیشتر توجه دارند. اگرچه در رویکرد سازه‌انگاری به دیگر زمینه‌های تهدید امنیتی نظیر فقدان روابط شفاف و قابل پیش‌بینی در رفتارهای قدرتمندان و عوامل اقتصادی-اجتماعی نیز توجه می‌شود، اما تأکید به عوامل فرهنگی و هویتی در دیدگاه سازه‌انگاران بیشتر است.

اندیشمندان جریان اصلی روابط بین‌الملل، مخصوصاً واقع‌گرایان، در برابر تحولات مدرنی نظیر تهدیدهای سایبری حرف زیادی برای گفتن ندارند؛ این اندیشمندان هنوز هم تنها به امنیت فیزیکی و آسیب‌های فیزیکی عنایت دارند و قادر به درک مؤلفه‌های هویتی

۱. قدرت‌های بزرگ از منظر هویتی، خود را ابرقدرت می‌بینند و از این حیث، منطق کنترلی آن‌ها ایجاب می‌کند که بر هویت‌ها و فضاها در عرصه بین‌المللی کنترل و احاطه داشته باشند. از این منظر، هر چه یک قدرت بر هویت‌ها کنترل داشته باشد، بهره‌مند از قدرت بیشتر است. اما همین منطق برانگیزاننده مقاومت در برابر آن نیز است.

امنیت نیستند. در خصوص تروریسم سایبری، حس امنیت و مفهوم عادی‌شدن امنیتی منظور نظر سازه‌انگاران از دو جنبه قابل‌طرح است؛ نخست اینکه عمل تروریسم سایبری یک «شرور ذاتی»[1] همه فعالین سایبری نیست و دربرگیرنده برخی از «تروریست‌های متخصص»[2]است. یعنی اینکه، همه بازیگران فضای سایبری نمی‌توانند اقدام به تهدیدهای تروریستی کنند و نیاز به تخصص برای این‌گونه اقدامات، یک شرط اساسی است. همچنین، هر متخصصی نیز لزوماً یک تروریست سایبری نیست و برای چنین اقداماتی به توجیهات عینی و ذهنی خاصی لازم است تا در پاسخ به آن‌ها، کنشگر، کنشی تروریستی را مرتکب شود. دیگر اینکه چون تهدید امنیتی فضاهای سایبری برای استفاده‌کنندگان آن تداوم‌یافته و درونی شده است، این حس تهدید برای بازیگران «عرصه بین‌المللی سایبری»[3]، هویتی و عادی شده است. این عادی شدن گهگاه به واکنش‌ها متقابل و رقابتی کشیده می‌شود. اگرچه در بازیگران منفرد در عرصه بین‌المللی سایبری، این عادی‌سازی به حس ناخوشایندی تبدیل می‌شود که آن‌ها را وادار می‌سازد تا به‌صورت انفرادی به دنبال رفع آن باشند، اما در سطح وسیع‌تر، واکنش‌های سازمان‌یافته ملی و فراملی را برمی‌انگیزد که حتی تا جداسازی و بومی‌سازی سایبری نیز پیش می‌رود. بنابراین، فضای سایبری به یک شمشیر دو لبه تبدیل می‌شود؛ می‌تواند به امنیت بیشتر وزندگی بهتر کاربرانش تبدیل شود، یا اینکه باعث «تهدید اطلاعاتی»[4] آنها گردد.

۳. امنیت هستی شناسانه و راهکارهای مقابله با تروریسم سایبری

عادی‌شدن هویتی تهدید در فضای سایبری، هنگامی‌که پای منافع، اهداف و اولویت‌های کنش‌گران در عرصه بین‌المللی، مخصوصاً کنشگران رسمی، در میان باشد، آن‌ها را که هویت اجتماعی خاص خود را در شبکه‌های سایبری دارند به «دگرسازی»[5] وامی‌دارد[6]. بر همین اساس است که در فضای مجازی، حذف رقیب، حمله به آن و

1. The Nature of Evil
2. Expert Terrorists
3. International Cyber Arena
4. The Threat of Intelligence
5. Othering

۶. دگرسازی که ویژگی گفتمانی سازمان‌ها است، به مفهوم جدا کردن خودی از غیرخودی یا دیگری است؛ عمدتاً این دیگر در پیرامون به‌صورت یک دشمن ترسیم می‌شود و در مقابل آن، خودی و دوست قرار دارد. برای فهم بیشتر این مفهوم مراجعه کنید به: (Wendt, 1999: 31-330)و (wendt, 1994:96-384)

ایمن‌سازی در برابر آن را شاهد هستیم.

ازآنجایی‌که هویت‌ها اجتماعی و حاصل تعامل هستند، به‌صورت های مختلفی شکل می‌گیرند و با عنایت به تمایل هستی‌شناسانه آن‌ها به امنیت در برابر حس عادی تهدید در فضای سایبری، رویه‌های کنش‌گران برای رفع تهدیدات را بنیان می‌گذارند. چون ساختارها جدا از رویه‌های کنشگران نیستند، این دو در تعامل با یکدیگر، در ساخت و یا مواجهه با فضای سایبری عمل می‌کنند. اما همان‌گونه که «کوزلووسکی»[1] و «کراتوچویل»[2] تأکید می‌کنند، نمی‌توان از طریق «مسیرهای از پیش تعیین‌شده» ای که « بتوان آن‌ها را با قوانین عام تاریخی فهمید» به سراغ پدیده‌هایی همچون فضای سایبری رفت(koslowski and Kratochwil, 1995: 128). در مواجهه با چنین پدیده‌هایی، پویایی روش‌ها و رویکردها لازم است، نه الگوهای از پیش تعیین‌شده. این به معنای آن است که به هنگام ظهور یک پدیده نظیر تروریسم سایبری، همگام با آن، رویکردها برای همراهی و یا مواجهه، اشاعه می‌یابند. اگر بخواهیم از منظر رابطه میان «علت»[3]و «دلیل»[4] به چگونگی مواجهه با تروریسم سایبری بپردازیم، می‌توان همانند ونت اندیشید که دلایل را هم «تکوینی» و هم علی می‌بینند. به نظر ونت، انسان‌ها هم «به یک دلیل»[5] عملی را انجام می‌دهند،که در این صورت دلایل دارای جنبه علی است، و هم «با یک دلیل»[6]، که در این صورت دلایل انجام یک عمل تکوینی خواهد بود (Wendt, 2000: 170). از این منظر، چون امنیت ماهیتی هستی‌شناسانه دارد و تهدید در فضای سایبری جاری است، کنشگر «آینده‌نگر»[7] می‌شود. بر این اساس است که کنشگر به پیشگیری و مقابله حقوقی با تروریسم سایبری معطوف می‌گردد. این در حالی است که رابطه مذکور در خصوص تروریست متخصص نیز قابل‌ذکر است. عامل تهدیدهای تروریستی نیز برای اقداماتش آینده‌نگرانه عمل می‌کند و با تکیه‌بر توانمندی‌های تخصصی خود، جهت پوشش دادن به مطلوبیت معطوف به هویت خویش، از منابع تکنولوژیکی در اختیار، استفاده می‌کند.

1. Koslowski
2. Kratochwil
3. Cause
4. Reason
5. For a Reason
6. With a Reason
7. Prospective

ساختارگرایان در مواجهه با پدیده‌هایی نظیر تروریسم سایبری، همچنان تلاش می‌کنند تا «اثبات‌گرایانه»[1] به یافتن قوانین عام حاکم بر این پدیده بپردازند و به‌گونه‌ای «جبر انگارانه»، نقش عامل انسانی را در آن نادیده بگیرند. ازاین‌رو، این ساختارگرایان، چشمان خود را بر روی کارگزاری‌های انسانی بسته و عمده توجه خود را معطوف به ساختار می‌کنند؛ اما در یک نگاه سیستمیک و جامع به پدیده تروریسم سایبری، باید ساختار و کارگزار را در ارتباط متقابل با یکدیگر درک کرد و فهمید. این مهم است که درک کنیم چگونه ساختار و کارگزار با یکدیگر در ارتباط هستند؛ البته چگونگی این ارتباط مهم است، اما چرایی آن نه.

در خصوص راهکارهای مقابله با تروریسم سایبری، مبتنی بر ارتباط سیستمی و متقابل میان ساختار و کارگزار، می‌توان پیشگیری را در پیوند با کارگزار و نظام حقوقی را مرتبط با ساختار، تبیین و تحلیل کرد.

۱-۳. پیشگیری از وقوع تروریسم سایبری

کارگزاری‌های انسانی،که آنها را تروریست‌های متخصص می‌خوانیم، و اندیشه آن در شکل دادن به «دانش سایبری مهاجم»[2] نتایج و عواقب زیانباری را به دنبال داشته است. می‌دانیم که، آنچه انسان و دانش بشری را به سطح امروزی آن رسانده، چیزی جز آموزش نبوده است. در خصوص تهدیدهای سایبری، مراجع ذی‌صلاح تقریباً از همان ابتدا به دنبال راهکارهایی از جنس آموزش بودند؛ حقوق‌دانان پیشگیری از وقوع جرم را بر ضمانت‌های اجرایی در برابر آن مقدم می‌دانند. با توجه به اهدافی که تروریست‌ها دنبال می‌کنند، در خصوص بسیاری از آن‌ها به‌هیچ‌وجه انواع ضمانت اجراهای سنگین کیفری، حتی اعدام، تأثیرگذار نیست و حتی می‌تواند موجب تشجیع و تحریک همراهانشان گردد. لذا با توجه به شرایط خاص حاکم بر این پدیدهٔ مجرمانه، اولین گزینهٔ کاملاً عاقلانه و منطقی، اتخاذ تدابیر پیشگیرانه از وقوع تروریسم است؛ هرچند اهمیت این مسئله نباید جایگاه ضمانت اجراهای کیفری را تحت‌الشعاع قرار دهد (جلالی‌فراهانی،۱۰:۱۳۸۵).

1. positivistic
2. Knowledge of Cyber Attackers

در ارتباط با اقدامات پیشگیرانه علیه تروریسم سایبری، سه رکن اصلی این پدیدهٔ مجرمانه تروریست‌های متخصص، قربانیان اقدامات تروریست‌های متخصص و فضای سایبری، به‌عنوان بستر ارتکاب اقدامات تروریستی است. پیشگیری در فضای سایبری با عنایت به ارکان مذکور، الگوهایی دارد که از میان آن‌ها، به‌ویژه طی نیم‌قرن اخیر، «پیشگیری وضعی»[1] و «اجتماعی»[2]، به‌عنوان جامع‌ترین راهکارهای موفقیت‌آمیز پیشگیری از جرم موردتوجه قرارگرفته‌اند (نجفی‌ابرندآبادی،۱۳۸۰: ۷۴۸).

در عرصه بین‌المللی نیز، پیشگیری در وقوع جرائم مهمی نظیر جنایات سازمان‌یافتهٔ فراملی و فساد نیز به ترتیب در کنوانسیون‌های پالرمو «۲۰۰۰»[3] و مریدای«۲۰۰۳»[4] سازمان ملل متحد بر آن‌ها تأکید شده است.

به‌طور خلاصه، در پیشگیری اجتماعی، هدف، از بین بردن «انگیزهٔ مجرمانه»[5] است و به همین دلیل، به آن «پیشگیری بزهکار محور»[6]گفته می‌شود. در اینجا راهکارهای اجتماعی، مانند رفع بیکاری و فقر که زمینه‌ساز شکل‌گیری انگیزه‌های مجرمانهٔ مالی و حتی قتل می‌شوند و همچنین «راهکارهای تربیتی و آموزشی»[7] برای کودکان، به‌عنوان آسیب‌پذیرترین گروه سنی، هم ازلحاظ بزهکاری و هم ازلحاظ بزه دیدگی، در دستور کار قرار می‌گیرند (نیازپور، ۱۳۸۲: ۱۳۸)؛ اما در پیشگیری وضعی، هدف، صیانت از بزه‌دیدگی بالقوه از طریق سلب «فرصت»[8]و یا «ابزار»[9]ارتکاب جرم است (Shinder,2002:353). بسیاری از تدابیر امنیتی که در ساختمان‌ها، اتومبیل‌ها و نظایر آن به اجرا درمی‌آید یا اینکه از خریدوفروش انواع سلاح‌های گرم و سرد جلوگیری می‌شود، درواقع پیشگیری وضعی از وقوع جرائم است.

با توجه به این توضیحات اجمالی، به نظر می‌رسد نحوهٔ پیاده‌سازی تدابیر پیشگیرانهٔ اجتماعی و وضعی در فضای سایبر روشن‌شده باشد. اگر واقعیات و شرایط خاص حاکم

1. Situational prevention
2. Social prevention
3. United States convention against corruption
٤. United states convention against Transnational
5. Criminal Motivation
6. Criminal-based Prevention
7. Developmental-based Crime Prevention
8. Opportunity
9. Tool

بر این فضا به‌خوبی به کاربران آن، که عمدتاً قشر جوان و نوجوان جامعه هستند، منعکس شود، از شکل‌گیری و تحقق بسیاری از انگیزه‌های مـجرمانه و درعین‌حال بزه دیدگی آن‌ها پیشگیری خواهد شد. هم‌اکنون این مسئله تا حدی موردتوجه قرارگرفته که مباحث تخصصی تحت عنوان «اخلاق سایبری»[1] از سوی صاحب‌نظران و سیاست‌گذاران این حوزه مطرح‌شده است (جـلالی فراهانی، ۱۳۸۵: ۶۵).

بااین‌حال، ازآنجاکه این فضا ماهیتی فنی دارد، دست‌اندرکاران بیشتر به دنبال اجرای «تدابیر پیشگیرانهٔ وضعی فنی» هستند که از نمونه‌های بارز آن می‌توان به انواع «فیلترها»[2] و «تدابیر نظارتی»[3] اشاره کرد که البته ناکارایی‌های این‌گونه ابـزارها بر همگان محرز شده، امـا به‌کارگیری آن‌ها اجتناب‌ناپذیر است(جلالی‌فراهانی، ۱۳۸۴: ۱۳۳). اما در خصوص کارآیی این تدابیر در مورد اقدامات تروریستی سایبری، روشن است که تدابیر پیشگیرانهٔ اجتماعی ماهیت تروریسم را هدف قـرار مـی‌دهند و در این جهت می‌توانند از فضای سایبر به‌عنوان یک ابزار اطـلاع‌رسانی و تـبلیغاتی نیز استفاده کنند و البته تأکید ویژه‌ای بر این اقدامات در فضای سایبر داشته باشند. تدابیر پیشگیرانهٔ وضعی نیز عمدتاً بـدون تـوجه بـه هویت مجرمان به کار می‌روند. برای مثال، هدف، پیشگیری از آلوده نشدن سیستم‌ها به انواع ویروس‌ها یا محتواهای مستهجن است و تفاوتی نمی‌کند مرتکب آن چه کسی است. البته برای برخی سیستم‌ها که در زیرساخت‌های حـیاتی مـستقر هـستند و عمدتاً مجرمانی نظیر تروریست‌ها قصد تعرض به آن‌ها رادارند، می‌بایست برنامه‌ریزی‌هایی ویژه صورت گیرد. همچنین برای اینکه از دسترس کاربران به محتواهای ارسالی از سوی تروریست‌ها جلوگیری شود، مانند انـواع پیام‌های تـحریک‌کننده و مخل آسایش عمومی، می‌بایست «فهرست‌های سیاه یا سفید»[4] فیلترها به نحوی تنظیم شـود که تـمامی حـوزه‌های مربوط را شناسایی و دسترس‌ناپذیر کنند(جلالی فراهانی،۱۳۸۵:۱۰).

۲-۳. قانون‌گذاری کیفری پیرامون تروریسم سایبری

«نظم» ترتیباتی است که به نفع ایجادکننده آن است. این‌چنین ترتیباتی هم در

1. Cyber Ethics
2. Filters
3. Monitoring Measures
4. Black & White Lists

سطح داخلی و هم بین‌المللی، نیازمند وجود قواعدی است که هرچقدر این قواعد نهادینه‌تر شده باشند، کاراتر می‌گردند. این قواعد که ساختاری هستند،گذارنده آن‌ها، کارگزارانی اند که در تحققش منافعی دارند و مبتنی بر هویت‌سازمانی ساختار-کارگزار برساخته می‌شوند. بی‌تردید معضل به‌واقع جهانی تروریسم که تقریباً تمامی دولت‌ها و ملت‌ها را بـه جـنگ طـلبیده و همواره لطمات بالقوه و بالفعل گوناگونی را به آن‌ها وارد آورده، مستلزم اتخاذ تدابیر جدی است تا علاوه بـر مـقابلهٔ مـؤثر با سیاست‌گذاران، برنامه‌ریزان و عوامل تروریستی، از وارد آمدن لطمات جانی و مالی بسیار جلوگیری گـردد.

یکی از مـنطقی‌ترین و صحیح‌ترین راهکارهای مقابله با تروریسم که حتی می‌توان زیربنای شایسته‌ای برای دیگر راهکارها نیز باشد، بـسترسازی حـقوقی از طریق وضع قوانین و مقررات موردنیاز است. با توجه به اینکه مـاهیت اقـدامات تروریستی مجرمانه است و درواقع قانون‌نویسان و قانون‌گذاران بـا یک پدیدهٔ مـجرمانه مـواجه‌اند، لذا بسترسازی حقوقی بر پایهٔ قوانین کیفری صورت مـی‌گیرد. قانون‌گذاری کیفری راجع به تروریسم، سابقه‌ای نسبتاً طولانی دارد. مقابلهٔ کیفری با پدیدهٔ مجرمانه تروریسم، فرایندی است که از دو رکن اصلی حـقوق جـزای ماهوی(جرم‌انگاری) و حقوق جزای شکلی(آیین دادرسـی کیفـری) تشکیل شده است.

۱-۲-۳. حـقوق جـزای ماهوی تروریسم سایبری

در خصوص پدیدهٔ تروریسم به‌عنوان یک پدیدهٔ مجرمانه، یک مانع بزرگ در این راه وجود دارد و آن اینکه اگر قرار است اقـدامات تـروریستی تـحت شمول ضمانت اجراهای کیفری بعضاً سنگین و حـتی جـبران‌ناپذیری مـانند اعـدام قـرار گـیرند، باید تعاریف مشخص و دقیقی از آن‌ها که عاری از هرگونه ابهام باشد، در قوانین کیفری انعکاس یابد. بااین‌حال، تمامی این مسائل زمانی به حد غایت مشکل می‌شوند که ضرورت ایجاب کند در فـضایی به اجرا درآیند که به بسیاری از مبانی و شیوه‌های اجرایی معمول آن‌ها پایبند نیست. قابلیت «مجازی‌سازی»[1] سایبری این امکان را فراهم آورده تا داده‌های الکتـرونیکی در قـالب فرایندهای الکترونیکی، به‌جای اشخاص ادارهٔ امور را در دست‌گیرند که نمونهٔ بارز آن را در بانکداری الکترونیکی شاهد هستیم. همین مسئلهٔ به‌ظاهر ساده باعث شده تا

1. Virtualization

مراجع کیفری تقلبات مالی الکترونیکی را بر عنوان مـجرمانهٔ کلاه‌برداری منطبق ندانند و قانون‌گذاران را مجبور کنند قوانین جدیدی را به تصویب برسانند، با این استدلال که عنصر فریب در آن‌ها وجود ندارد و نسبت به سیستم‌ها و برنامه‌های رایانه‌ای صـدق نـمی‌کند (عالی‌پور، ۱۳۸۳: ۲۱۰).

همچنین فرامرزی بودن فـضای سـایبر، صرف‌نظر از مسائل دشواری که در حوزهٔ آیین دادرسی کیفری به وجود آورده ، قانون‌گذاران کیفری را نیز با چالش‌هایی جدی مواجه کرده است. طبق اصـول اسـاسی کیفری، اصل بر اجـرای قـوانین جزایی در قلمرو سرزمین کشورهاست، مگر موارد استثنایی که به آن تصریح‌شده باشد(مادّهٔ ۳ قانون مجازات اسلامی، مصوب ۱۳۷۰). حال چگونه می‌توان این قوانین را در مورد جرائمی قابل‌اجرا دانست که به قلمرو سرزمینی محدود نـیستند. عـلاوه بر این، زمانی دشواری چاره‌جویی راجع به این‌گونه مباحث محرز می‌گردد که ملاحظات اجتماعی، سیاسی، فرهنگی و اقتصادی کشورها برای جرم‌انگاری پدیده‌های خاص سایبری نیز موردتوجه قرار گیرد.باوجوداینکه کشورها هنوز به‌طور گسترده به تروریسم سایبری در مفهوم خاص آن در قوانین جزایی نپرداخته‌اند، اما مـاهیت این اقـدام که همانا تخریب یا آسیب‌رسانی به داده‌ها و سیستم‌های رایانه‌ای است، ازجمله مصادیق اولیهٔ جرائم رایانه‌ای به شمار می‌روند که اغلب راجع به آن قوانین کیفری را به تصویب رسانده‌اند و به نظر می‌رسد با لحـاظ کیفـیات مـشدده، فعلاً می‌تواند پاسخگوی نیازهای تـقنینی بـاشد، ولی در آینـدهٔ نزدیک با روند رو به رشد حملات تروریستی سایبری در سراسر جهان عملاً نیاز به قوانین خاص بروز خواهد یافت.

۲-۲-۳. حقوق جزای شکلی تروریسم سایبری

اولین مسئله‌ای که به هنگام طـرح مـباحث کیفری باید در مورد آن تعیین تکلیف کرد، تعیین مرجع ذی‌صلاح قضایی است.در این زمـینه، اولین قـاعده‌ای که موردتوجه قرار می‌گیرد، «صلاحیت دادگاه محل وقوع جرم»[1] است.رعایت این قاعده، در بسیاری مـوارد مـنجر به رعایت «اصل سرزمینی کشورها در امور کیفری»[2]نیز می‌شود. در مواردی

1. Location of Act
2. Territoriality Nexus

هم که جرائمی حـالت فـرامرزی پیدا مـی‌کنند، قواعدی نسبتاً مورد اتفاق میان کشورها وضع‌شده تا در اعمال «صلاحیت کیفری فرامرزی»[1] مشکل خـاصی بـه وجود نیاید؛ به‌عنوان‌مثال میان کشورهای اروپایی می‌توان به قوانین «کمیته کیفری اروپایی»[2] اشاره کرد. اما در فضای سایبر، اولین و بدیهی‌ترین مسئله این است که چیزی بـه نـام مـحل وقوع جرم معنا ندارد.

پس از صلاحیت کیفری، نوبت به فرایند اجرایی محاکم به همراه مجریان قـانون بـرای تعیین تکلیف پرونده‌های مفتوح می‌رسد که عموماً از آن به‌عنوان کشف علمی جرائم یاد مـی‌شود و هـمان‌طور که شاهد هستیم، در اثر پیشرفت علوم در حوزه‌های مـختلف، این شـاخه از عـلوم جنایی نیز با تحولات شگرفی مواجه شـده اسـت. اما مسئله‌ای که فضای سایبر به‌طور خاص برای این شاخه به وجود آورده، به مـاهیت کاملاً فنی آن مربوط می‌شود. مسلماً بـرای شـناسایی عوامل جـرمی که در فـضای سـایبر ارتکاب می‌یابد و به‌تبع اثبات جـرم، بـاید وارد این فضا شد. لذا میزان قابلیت فنی مجریان قانون در شناسایی و ردیابی آثار مجرمانهٔ الکتـرونیکی و کشـف هویت مجرمان سایبری اهمیتی حیاتی دارد(Casey, 2001:16). مـهم‌ترین ثمرهٔ عملی این مسئله در «استناد پذیری ادلهٔ الکتـرونیکی»[3] ظاهر می‌شود. با توجه بـه آسـیب‌پذیری بالای داده‌های الکترونیکی، برای اینکه بتوان نزد محاکم به آن‌ها به‌عنوان ادلهٔ مـحکمه‌پسند اسـتناد کرد، مجریان قانون باید ضوابط پیچـیده‌ای را رعـایت کنـند.هـمچنین برخلاف تصور عـموم، فـرامرزی بودن این فضا نه‌تنها کمکی به توسعهٔ ارتکاب عمل مجریان قانون نمی‌کند، بلکه در بسیاری موارد مـجبورند بـرای جـمع‌آوری داده‌های به‌سرعت فناپذیر رایانه‌ای از سیستم‌های رایانـه‌ای واقـع در دیگـر کشـورها،تـشریفات زمـان‌بری را رعایت کنند که به‌هیچ‌وجه با شرایط حاکم بر این فضا سازگار نیستند. به دلیل وجود این‌گونهٔ مسائل حیاتی، در تمامی اسناد بین‌المللی و منطقه‌ای که تابه‌حال راجع به جـرائم سایبر تدوین و منتشرشده، به مجریان قانون توجه ویژه‌ای شده است. نمونهٔ بارز آن کنوانسیون جرائم سایبر است که بیش از دوسوم مقررات آن به این حوزه اختصاص‌یافته است.

با توجه به این مسائل، بـه نـظر می‌رسد اهمیت و جایگاه همکاری بین‌المللی برای

1. Extraterritorial Jurisdiction
2. European Committee on Crime
3. Admissibility of Digital Evidence

مقابلهٔ کیفری با جرائم سایبر محرز شده باشد. تاکنون تلاش‌های بسیاری برای همسو کردن کشورها صورت گرفته که بازهم نمونهٔ بارز آن کنوانسیون جرائم سایبر است. این سند، علاوه بر اینکه بخش مهمی از مقررات خود را به این حوزه اختصاص داده است،در پیشگفتار خود به‌صراحت اعلام می‌دارد:«با اعتقاد به نیاز مبرم به یک سیاست جنایی مشترک به‌عنوان یک اولویت برای حمایت از جامعه در برابر جرائم سایبر، با اقداماتی از قبیل تصویب قوانین مناسب و گسترش همکاری‌های بین‌المللی و با آگاهی از دگرگونی‌های اساسی که در اثر دیجیتالی شدن، همگرایی و ادامهٔ جهانی‌شدن شبکه‌های رایانه‌ای به وجود آمده است» (گروه کارشناسان، ۱۳۸۴: ۱۴). بااین‌وجود، تا کامل شدن سازمان حقوقی در مواجهه با پدیده‌های نوینی نظیر تروریسم سایبری، فاصله وجود دارد که نخبگان باید آن را پر کنند.

نتیجه

تهدیدهای امنیتی تروریسم سایبری آن‌گونه که از پژوهش حاضر برمی‌آید، در بستری اجتماعی و شبکه‌ای به وسعت جهانی اتفاق می‌افتد که با تحلیل‌های عینی نمی‌توان به‌راحتی آن را فهم کرد. ازاین‌رو به یک نگاه سیستمی و کلی گرایانه برای تحلیل تروریسم سایبری نیاز است که سازه انگاران به‌واسطه درک میانی‌شان از پدیده‌ها که قائل به تعامل دیالکتیک عین و ذهن هستند، این قابلیت رادارند. همان‌گونه که شرح آن رفت، یکی از جنبه‌های اصلی امنیت، ماهیت فرهنگی و هویتی آن است که به‌واسطه فعالیت‌های تروریست‌های متخصص در عرصه سایبری بین‌المللی، به شکل‌گیری یک حس تهدید عادی امنیتی در فضای سایبری منجر شده است. بنابراین در ساحتی اجتماعی، مبتنی بر نوع نگاه به خود و دیگران، کنشگران روابط بین‌الملل، در عرصه سایبری بین‌المللی، تعامل خود با دیگران را بر می‌سازند تا به آنجا که به فهمی مشترک رسیده و یا در فرآیندی دگرسازانه، دشمنان خود را ترسیم کنند. این کنش‌گران با شکل‌دادن به دانش سایبری و بعضاً مهاجم، یا هویتی تهاجمی می‌یابند یا مدافع و امنیتی. حس عادی شده ناامنی در عرصه سایبری بین‌المللی، به‌واسطه ذات کنشگر نیست و بازیگران عرصه سایبری بین‌المللی بالقوه تهدید محسوب نمی‌شوند؛ بلکه برسازی حس ناامنی، به‌واسطه عادی شدن هویتی تهدید در این فضا است و حتی یک تروریست متخصص نیز

در این فضا نیاز به ایمن‌سازی خود دارد. بااین‌وجود، امنیتی شدن هویتی فضای سایبری به شکل‌گیری هویت مقاوم در برابر آن می‌انجامد. عمل تروریسم سایبری نمود دهنده منافع کنشگران در کنار هویت‌ها و برداشت‌های آن‌ها است که در فضایی مجازی، جنگ هویت‌ها و فرهنگ‌ها را یادآور است. ازآنجاکه ساختار و کارگزار در تعامل با یکدیگر هستند و همچنین نمی‌توان با قوانین عام و از پیش تعیین‌شده به سراغ پدیده‌هایی نظیر تروریسم سایبری رفت، در تحلیل برای درک تروریسم سایبری و پیشگیری از وقوع آن، باید علاوه بر جنبه‌های عینی ساختار، به ذهنیات کارگزار نیز توجه کرد. ازاین‌رو است که مبتنی بر ویژگی‌های آینده‌نگرانه کارگزاران، پیشگیری که بر اساس ویژگی‌های هویتی و فرهنگی کارگزار تجویز می‌شود، برای عبور از تهدیدهای سایبری توصیه می‌گردد. همچنین، مبتنی بر ساختار نیز برای تحقق نظم و عبور از تهدیدهای امنیتی، پیش‌بینی سازوکارهای حقوقی کیفری، پیشنهاد می‌گردد. باوجوداینکه سازوکارهای مقابله با تهدیدهای سایبری در عرصه بین‌المللی و داخلی در حال پیشرفت هستند، اما تکامل روزافزون آن‌ها برای به روزشدن آن‌ها، همگام با تهدیدها، ضروری است. ❋

کتابنامه

منابع فارسی

بختیاری، ارشد، محمدرضا فراتی، مصطفی الماسی و مهری جلائیان. (۱۳۸۹). «سایبر تروریسم در جامعه شبکه‌ای»، ***مجله مطالعات بین‌المللی پلیس***، (۴).

پاکزاد، بتول. (۱۳۷۵). «جرائم کامپیوتری»، ***پایان‌نامه کارشناسی ارشد***، تهران: دانشگاه شهید بهشتی.

..... (۱۳۹۰). «ماهیت تروریسم سایبری»، ***مجله تحقیقات حقوقی دانشگاه شهید بهشتی***، (۴).

جلالی‌فراهانی، امیرحسین. (۱۳۸۵). ***پیشگیری اجتماعی از جرائم سایبری راهکاری اصولی برای نهادینه‌سازی اخلاق سایبری***. تهران: انتشارات مرکز تحقیقات مخابرات.

..... (۱۳۸۵). «تروریسم سایبری»، ***فصلنامه تخصصی فقه و حقوق***، ۳ (۱۰).

..... (۱۳۸۷). «جنبه‌های حقوقی اقدامات کیفری بین‌المللی مجرمان قانون در قبال جرائم سایبری»، ***فصلنامه پیشگیری از جرم***، (۳).

..... (۱۳۸۴). «پیش‌گیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر»، ***فصلنامهٔ تخصصی فقه و حقوق***، (۶).

چگینی‌زاده، غلامعلی. (۱۳۷۹). «رویکردی نظری به مفهوم امنیت ملی در جهان سوم»، ***مجله سیاست خارجی***، ۱۴ (۱).

خلیلی‌پوررکن‌آبادی، علی و یاسر نورعلی وندی. (۱۳۹۱). «تهدیدات سایبری و تأثیر آن بر امنیت ملی»، ***فصلنامه مطالعات راهبردی***، ۱۵ (۵۶).

سیمبر، رضا. (۱۳۸۰). «تروریسم در روابط بین‌الملل: چالش‌ها و امیدها»، ***فصلنامه راهبرد***، (۲۱).

طیب، علیرضا. (۱۳۸۴). ***تروریسم در فراز و فرود تاریخ***. تهران: نشر نی.

عالی‌پور، حسن. (۱۳۸۳). «کلاهبرداری رایانه‌ای»، ***مجلهٔ پژوهش‌های حقوقی مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش***، (۶).

عباسی، مهدی. (۱۳۸۳). «اینترنت ابزار سیاست تروریسم مجازی»، ***نشریه فرهنگی و فناوری***، ۱ (۳).

عبدالله‌خانی، علی. (۱۳۸۳). ***نظریه‌های امنیت مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی(۱)***. تهران: موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر، چاپ اول.

فضلی، مهدی. (۱۳۸۹). ***مسؤولیت کیفری در فضای سایبر***: تهران: نشر خرسندی. چاپ اول.

قوام، عبدالعلی. (۱۳۸۶). ***روابط بین‌الملل؛نظریه‌ها و رویکردها***. تهران: نشر سمت.

کارگری، نوروز. (۱۳۹۰). «مفهوم‌یابی و گونه‌شناسی تروریسم». در ***تروریسم و مقابله با آن*** (به اهتمام عباسعلی کدخدایی و نادر ساعد). تهران: انتشارات مجمع جهانی صلح اسلامی.

گروه کارشناسان. (۱۳۸۴).«کنوانسیون جرائم سایبر و گزارش توجیهی آن در مرکز پژوهش‌های مجلس شورای اسلامی». تهران: شمارهٔ ۷۶۴۶.

گل‌محمدی، احمد. (۱۳۸۶). ***جهانی‌شدن فرهنگ و هویت***. تهران: نشرنی.

مارتین، لی جی. (۱۳۸۹). ***چهره جدید امنیت خاورمیانه***. ترجمه قذیر نصری. تهران: پژوهشکده مطالعات راهبردی و دانشگاه امام صادق(ع).

ماندل، رابرت. (۱۳۷۹). ***چهره متغیّر امنیت ملی***. ترجمه پژوهشکده مطالعات راهبردی. تهران: پژوهشکده مطالعات‌راهبردی.

محسنی، رضاعلی. (۱۳۹۰). «بازشناسی و تحلیل پدیده تروریسم»، ***فصلنامه مطالعات سیاسی***، ۳ (۱۲).

محقق‌منتظری، مائده. (۱۳۸۹). «فضای مجازی و جهانی‌شدن». تهران: روزنامه جوان.

مشیرزاده، حمیرا. (۱۳۸۶). ***تحول در نظریه‌های روابط بین‌الملل***. تهران: انتشارات سمت.

نجفی‌ابرندآبادی، علی‌حسین.(۱۳۸۰). «تقریرات درس جرم‌شناسی». تنظیمی محمدعلی بابایی. تهران: دورهٔ دکتری دانشگاه تربیت مدرس، نیم سال نخست.

نمامیان، پیمان. (۱۳۹۲). «مواجهه با تروریسم سایبری در حقوق بین‌الملل کیفری»، ***فصلنامه پژوهش‌های ارتباطی***، ۲۰ (۱).

نورمحمدی، مرتضی.(۱۳۹۰). «سایبر تروریسم؛ تروریسم در عصر اطلاعات». ***تروریسم و مقابله با آن***(به اهتمام عباسعلی کدخدایی و نادر ساعد). تهران: انتشارات مجمع جهانی صلح اسلامی.

نیازپور، امیرحسن.(۱۳۸۴). «پیشگیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم»، ي‌رتسگداد يقوقح هلجم (۴۵).

ونت، الکساندر، (۱۳۸۴). ***نظریه‌های اجتماعی سیاست بین‌الملل***. ترجمه حمیرا مشیرزاده. تهران: انتشارات وزارت امور خارجه.

یزدان فام، محمود. (۱۳۸۶). «دگرگونی در نظریه‌های و مفهوم امنیت بین‌المللی»، ***فصلنامه سیاسی مسائل استراتژیک و بین‌المللی***، ۱۰ (۴).

منابع انگلیسی

Bellamy, A. (2004). ***Security Communities and their Neighbors: Regional Fortresses or Global Integrators?*** London: Palgrave.

Hopf, T. (1998). 'The Promise of Constructivism in International Relations Theory. ***International Security***, 23 (1).

CACI International Inc. and U.S Naval Institute. (2010). Cyber Threats to National Security. ***Symposium One: Countering Challenges to the Global Supply Chain***.

Casey, E. (2001). ***Digital Evidence and Computer Crime***. Academic Press.

Haller, J, Merrell, S, Butkovic, M, Willke, B. (2010). ***Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability***. Software Engineering Institute.

Hancock, b. (2001). Cyber tracking. ***cyber terrorism; computers and security***. 20.

Harvey, D. (1989). The Condition of Postmodernity: an Enquiry in to the Conditions of Cultural Chang.

Koslowski, R. and Kratochwil, F. (1995). Understanding Change in International Politics: The Soviet Empire's Demise and the International System. ***In R. N. Lebow and T. Risse Kappen, eds, International Relations Theory and the End of Cold War.*** New York: Columbia University Press.

Kowert, P. (2001). Toward a Constructivist Theory or Foreign Policy', in vendulka Kubalkova (ed), ***Foreign Policy in a Constructed World***. New York: M.E. Sharpe.

Kubalkova, V. (2001). Foreign Policy. International Politics and Constructivism, in Vendulka Kubalkova, ***Foreign Policy in a Constructed World***, New York: M.E. Sharpe.

Lord, K, Sharp, T. (2011). America's Cyber future Security and Prosperity inthe Information Age. **Center for a New American Security**. (I).

Onuf, N. (1999). Worlds of our Making: the Strange Career of Constructivism in International Relations, in Donald J.Puchala, (ed). ***Visions of International Relations.*** Columbia: University of South Carolina Press.

Shinder, D. (2002). ***Scene of the cyber forensics Hand book***. Syngress publication.

Starr, S. (2009). Towards an Evolving Theory of Cyber power, ***National Defense University***. Center for Technology and National Security Policy.

Wendt, A. (1994). Collective Identity Formation and the International State. ***American Political Science Review***. 88,(2).

..... (1999). ***Social Theory of International Politics***. Cambridge: Cambridge University Press.

..... (2000). On the Via Media: A Response to the Critics. ***Review of International Studies***.