صداوسیمای جمهوری اسلامی ایران

معاونت سیاسی

اداره پژوهش‌های سیاسی

سایبر تروریسم

پژوهش
خبری
معاونت سیاسی
صداوسیما

فرآورده‌های خبری و تولیدات پژوهشی در بخش های زیر قابل دسترس است:

ـ وب سایت خبرگزاری صداوسیما (سرویس پژوهش) http://www.iribnews.ir

پژوهشگر: یاسر بهشتی

فـهرسـت مـطالـب

عنـــــوان **صفحـــــه**

پژوهش خبری معاونت سیاسی صدا و سیما

بسمه تعالی

❖ مقدمه

فضای مجازی به عنوان بافت جدید عملیاتی، این امکان را برای گروه های تروریستی فراهم نموده است تا اهداف و نیات خود را در فضای مجازی فارغ از محدودیت‌های جهان واقعی پیگیری نمایند. در این میان یکی از مهم ترین تهدیدات نوظهور، سایبر تروریسم است که به واسطه کاربست فزاینده فناوری های اطلاعات و ارتباطات و در بستر خدمات دولت ها برای تسریع، افزایش کارایی و کاهش هزینه ها در خدمت رسانی به شهروندان، اهمیت فزاینده ای یافته است

بدین ترتیب این بار تروریست‌ها در فضای مجازی قدرت بیشتری یافته و از طریق استفاده از مزیت گمنامی و پنهان سازی هویت در اینترنت، تهدید خود بر امنیت، سلامت، ثبات ملت‌ها به انجام می‌رسانند.

بدیهی است که کاهش آسیب پذیری‌ها و تقویت امنیت و صلح در مقابل تهدیدات و بازیگران نوظهور عرصه تروریسم سایبری، مستلزم انجام مطالعات آینده پژوهانه به‌ویژه در خصوص تاثیر انقلاب اطلاعاتی بر امنیت ملی، شناسایی تهدیدات فضای سایبر و لزوم ارتقای قابلیت‌های فنی و آگاهی عمومی در این خصوص است.

در یادداشت حاضر ابعاد مختلف این پدیده شرح داده شده است که پیش از هر چیز به‌واسطه مفهوم دوگانه سایبر تروریسم، ابتدا مرور ارزش‌های فضای سایبر و ارکان و انگیزه‌های تروریسم ضروری می‌نماید.

❖ هنجارهای فضای سایبر

یکی از برجسته‌ترین این ارزش ها امنیت است. امنیت فضای سایبر بر دو گونه است؛

۱. امنیت درونی که متضمن حفظ استاندارد های حاکم بر فضای تبادل اطلاعات است که بر سه پایه تمامیت داده و سیستم، محرمانگی و قابلیت دسترسی استوار است.

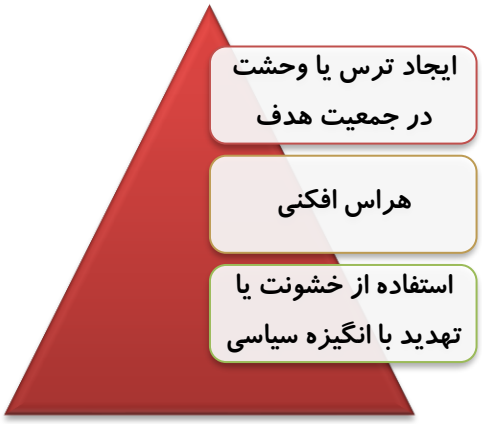
۲. امنیت بیرونی که متضمن نبود تهدید برای اشخاصی است که از شبکه‌های رایانه ای و اینترنتی بهره می‌گیرند.

تبادل و آزادی اطلاعات یکی دیگر از مهمترین ارزش ها در فضای سایبر است. فضای سایبر ماهیتاً برای آزادی گردش اطلاعات شکل گرفته و محدودیت در این فضا معنا ندارد.با این حال تعارض ارزش ها در فضای سایبر همچون فضای بیرونی است و در این میان ارزش امنیت در برابر ارزش آزادی اطلاعات قرار دارد به گونه ای که نقض هر یک احتمالاً در راستای دفاع از دیگری صورت می گیرد.

❖ ارکان اصلی تروریسم

به بیان اشمید و یانگمن[1] ارکان اصلی تروریسم به قرار ذیلند:

[1] & Jongman Schmid



هراس افکنی مهمترین ویژگی اقدامات تروریستی است، به طوری که بعضی این ویژگی را تنها رکن اصلی در تعریف تروریسم می‌دانند و بیان می‌دارند که از نظر حقوقی، موضوع و هدف اصلی تروریسم، سلب امنیت است که با ایجاد ترس و وحشت در میان مردم تحقق می‌یابد و البته ممکن است موضوع اقدامات تروریستی منقسم به موضوعات رفتاری و غایی گردد.

در موضوع رفتاری، هدف مستقیم رفتارهای خشونت بار تروریست ها، افراد یا اموال است اما در موضوع غایی، هدف نهایی تروریست‌ها امنیت ملی است.

استفاده از خشونت یا تهدید به آن غالباً به عنوان رکن مادی اقدامات تروریستی مطرح می‌شود.

باید توجه داشت خشونت در تروریسم موضوعیت ندارد زیرا آنچه اهمیت دارد نتیجه استفاده از خشونت یعنی ایجاد ترس و وحشت است. بنابراین تحقق جرم تروریسم ممکن است از طریق سیستم های رایانه ای و با ایجاد اختلال در شبکه های اطلاعاتی، سیستم های کنترل حمل و نقل زمینی، هوایی، دریایی و یا از کنترل خارج کردن سلاح‌های کشتار جمعی، عملی شود.

❖ انگیزه های تروریسم

انگیزه سیاسی، عنصری مهم درتحقق پدیده تروریسم است. هدف تروریست‌ها استفاده از ترس یا نگرانی شدید برای وادار ساختن اهداف اصلی خود به انجام یک رفتار یا اتخاذ ایستارهایی است که با نتیجه سیاسی مطلوب تروریست‌ها ارتباط دارد. برخی بدون وجود انگیزه سیاسی هیچ اقدامی را تروریستی نمی‌دانند.

البته اهداف سیاسی مفهوم گسترده ای است که پدیده های اعتقادی، مذهبی و قومی را نیز در بر می‌گیرد.

❖ تعریف سایبر تروریسم

همان گونه که رفت در عصر جدید و به دنبال انقلاب اطلاعاتی رخداده، منابع قدرت‌ها نیز با دگرگونی عمیقی مواجه شده است و به تبع مفهوم امنیت با تحولاتی مواجه شده است. بازیگران دولتی و غیردولتی از این قدرت استفاده می‌کنندتا به اهداف خود در فضای سایبری و دنیای واقعی دست یابند. از همین رو اعمال قدرت برای حاکمیت‌ها پیچیده شده است.

این بازیگران از قدرت سایبری استفاده می‌کنند تا به اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مالی خود درفضای سایبری و دنیای واقعی نایل آیند. این اهداف در فضای مجازی از شیوه های متفاوتی حاصل می‌شوند که مهمترین آنها عبارتند از:

جنگ سایبری، حملات سایبری، آشفتگی سایبری، جرایم سایبری، جاسوسی سایبری و تروریسم سایبری.

عبارت سایبر تروریسم با ترکیب واژه های فضای سایبر و تروریسم، در دهه 1980 توسط بری کلین[1] ابداع و اینگونه تعریف شد: سوء استفاده عمدی از یک سیستم، شبکه یا مؤلفه اطلاعاتی رایانه ای برای تحقق هدفی که مؤید یا تسهیل کننده مبارزه یا اقدام تروریستی است.

بدین ترتیب بهره گیری از اینترنت، شبکه های رایانه ای و امکاناتی که این شبکه‌ها پدید می‌آورند با هدف نابود ساختن شبکه‌های زیربنایی یک جامعه مانند انرژی، حمل و نقل، فعالیت های دولتی و تاثیر گذاشتن بر یک دولت، شهروندان و گروه‌ها را سایبر تروریسم می‌گویند.

---

[1] Barry Collin

این پدیده که حاصل تلاقی و همگرایی دو واژه ترور و سایبر شکل گرفته است در عنوان عبارت اولی خود ترس و واهمه را گوشزد می‌کند و سایبر هم که همان فضای مجازی است. بر این اساس می توان گفت ایجاد هر نوع ترس و واهمه ای که از طریق فضای مجازی صورت بگیرد در ذیل این مقوله قابل توصیف است.

حملات سایبر تروریسم نوعی حمله است که در آن یک مولفه رایانه‌ای وجود دارد که سیستم‌های هدف را غیرقابل استفاده نموده، کارایی آنها را کم کرده و با تزریق اطلاعات غلط، دقت تصمیم‌گیری کاربران را کاهش داده و حتی منجر به سرقت اطلاعات می‌شوند.

این حمله یک اقدام خصمانه با استفاده از کامپیوترها، اطلاعات الکترونیکی و یا شبکه‌های دیجیتالی که هدفش دستکاری، دزدی، اختلال و بی‌ارزش کردن سیستم‌های حساس، سرمایه‌ها و اطلاعات است. در این حمله می‌توان از فناوری رایانه‌ای برای تهدید یا حمله کرد به منابع رایانه‌ای قربانی بهره گرفت.

حملات سایبری تفاوت عمده‌ای با دیگر اشکال معمول حمله دارند، از همین رو توسط عوامل نامعلوم انجام می‌پذیرد و و ردیابی آن بسیار دشوار است. از طرفی این نوع از حملات بسیار ارزانتر از حملات معمولی است و در عین حال که فاقد آسیب‌پذیری‌ها و هزینه‌هایی هستند که اغلب متوجه شخص مهاجم می‌شود.
هزینه کم فن آوری رایانه ای، اتصال گسترده به اینترنت و سهولت ایجاد یا به دست آوردن نرم افزارهای مخرب به این معنا که تقریباً هر کسی می‌تواند به این فضا وارد شود و بازیگران شامل افراد، گروه‌های سازمانی، گروه های تروریستی، شرکت‌های خصوصی و دولت - ملت‌ها هستند.

❖ ویژگی ها

تروریسم سایبری به علت ویژگی‌ها و قابلیت‌های منحصر به فرد فضای سایبر که بستر ارتکاب، موضوع و هدف آن می‌باشد، تفاوت‌هایی اساسی با سایر اشکال تروریسم دارد. ویژگی های تروریسم سایبری نشان از ماهیت جدید آن دارد .از سویی از تروریسم جدا است و از سوی دیگر با جرائم سایبری کاملاً همخوانی ندارد. بنابراین تعریف آن باید به گونه ای باشد که از جرائم رایانه ای و تروریسم تفکیک شود. تروریسم سایبری با ماهیت خاص خود، واقعیتی عینی و فضای سایبر، فضایی غیر مادی، ناملموس و بیکران است که از طریق اتصال شبکه های رایانه ای و از رهگذر تجمیع فناوری های رایانه، فناوری اطلاعات و ارتباطات شکل گرفته است.

❖ اهداف،آثار و شیوه ارتکاب

این پدیده دارای ویژگی هایی است که ناشی از دو جنبه تروریستی و سایبری بودن آن است. جنبه نخست آن را از جرائم سایبری متمایز می‌نماید و جنبه دوم آن را از تروریسم سنتی جدا می سازد. نزدیکی تروریسم سایبری به تروریسم بیشتر از جهت انگیزه سیاسی یا عقیدتی یا نژادی است. اما از حیث اهداف وآثار و شیوهٔ ارتکاب نیز تفاوت اساسی با یکدیگر دارند .این تفاوت ها ناشی از ویژگی های فضای سایبر است.

از حیث اهداف و آثار:

از حیث شیوه ارتکاب:

❖ گونه شناسی

گونه شناسی جامعی از تروریسم سایبری تحت عنوان " گونه شناسی وقایع سایبری" ارائه شده است که شامل: حملات اطلاعاتی، حملات زیرساختاری، تسهیلات فنی و تأمین مالی است.

کلیو والکر[1] حقوقدان انگلیسی در گونه شناسی انواع تروریسم سایبری با رویکرد موسع هم تهاجمات و هم مساعدت‌ها را مورد توجه قرار داده است و آنها را در پنج گروه قرار داده است:

۱. جنگ اطلاعات (در این نوع از اعمال، فناوری اطلاعات هم ابزار و هم هدف تهاجم است)
۲. ارتباطات
۳. حمایت لجستیکی و پرسنلی
٤. جمع آوری اطلاعات جاسوسی
٥. تبلیغات

❖ **انواع تهدید تروریسم سایبری**

نوع تهدید	توصیف
گروه‌های جنایی	**گروه‌های جنایی با هدف کسب پول به سیستم حملاتی ترتیب می‌دهند**
سرویس‌های اطلاعاتی خارجی	**سرویس‌هایی که از ابزار سایبر برای جمع‌آوری اطلاعات و فعالیت‌های جاسوسی استفاده می‌کنند**
هکرها	**هکرها گاهی اوقات با هدف ایجاد چالش یا به دست آوردن حقوق در اجتماع هکرها به شبکه نفوذ می‌کنند**
جنگ اطلاعاتی	**تعداد بسیاری از دولت‌ها برای توسعه دادن دکترین، برنامه‌ها و قابلیت جنگ اطلاعاتی تلاش می‌کنند تا از این طریق به توانایی اختلال در ارتباطات و زیرساخت‌های اقتصادی که از قدرت نظامی حمایت می‌کنند، دست یابند**
تهدید داخلی	**سازمان ناراضی داخلی، منبع اصلی جرائم رایانه‌ای است**
نویسندگان ویروس	**به عنوان تهدیدی جدی برای شبکه‌ها ی رایانه‌ای محسوب می‌شوند**

❖ **مصادیق جهانی:**

- ویروس گاوس به عنوان تروجان بانکی توسط مهاجمین مورد استفاده قرار گرفته بود
- بد افزار شعله آتش یکی از جدی ترین حملات سایبری علیه تجهیزات شرکت های نفتی خاورمیانه
- انهدام هزار وبسایت آمریکایی توسط هکرهای چینی در سال ۲۰۰۱
- شناسایی شبکه گوسنت نت توسط محققان کانادایی در سال ۲۰۰۹ که ۱۲۹۵ سیستم کامپیوتری در وزارتخانه‌ها، سفارتخانه‌ها و موسسات چند ملیتی در کشورهای ایران، پاکستان، هند، کره جنوبی، آلمان و بسیاری دیگر آسیب رسانده بود
- سرقت ۷۰ میلیون دلاری شبکه تبهکار بین المللی با بدافزار زئوس در سال ۲۰۱۰
- کرم رایانه‌ای نیمدا و خسارت به سیستم‌های رایانه‌ای ایالات متحده، بریتانیا و هنگ کنگ

❖ **استاکس نت علیه ایران**

از معروف ترین تجربه‌های ایران در تروریسم سایبری، مورد هجمه واقع شدن توسط ویروس استاکس نت بود.

[1] Walker, Clive.

نخستین کشورهایی که به شکل گسترده به این بدافزار آلوده شدند کشورهای ایران، اندونزی و هندوستان بودند. هدف آن سامانه‌های هدایتگر تأسیسات صنعت هسته‌ای با سیستم عامل ویندوز است. کارشناسان معتقدند طراحان این بدافزار یک منطقه جغرافیایی خاص را مدنظر داشته‌اند و هدف از طراحی این بدافزار دستیابی به اطلاعات صنعتی ایران بود.
این بدافزار به دنبال خرابکاری در تأسیسات غنی‌سازی اورانیوم نطنز بود. روزنامه نیویورک تایمز در تاریخ ۱۶ ژانویه ۲۰۱۱، در مقاله‌ای مدعی شد که «اسرائیل استاکس‌نت را در مرکز اتمی دیمونا و بر روی سانتریفیوژهای مشابه‌ای که ایران از آن‌ها در تاسیسات غنی‌سازی اورانیوم نطنز استفاده می‌کند، با موفقیت آزمایش کرده‌بود.»

در اواخر ماه مه ۲۰۱۲ رسانه‌های آمریکایی اعلام کردند که استاکس‌نت مستقیماً به دستور اوباما رئیس‌جمهور آمریکا طراحی، ساخته و راه اندازی شده گرچه در همان زمان احتمال این می‌رفت که آمریکا تنها عامل سازنده نباشدکه در ۷ ژوئیه سال ۲۰۱۳، ادوارد اسنودن در مصاحبه‌ای با اشپیگل اعلام کرد این بدافزار با همکاری مشترک آژانس امنیت ملی ایالات متحده آمریکا و اسرائیل طی عملیاتی به نام عملیات بازی‌های المپیک ساخته شده‌است. در سال ۲۰۱۶ الکس گیبنی مستندی به نام روزهای صفر در مورد استاکس‌نت منتشر کرد که در آن این ویروس محصول مشترک ایالات متحده آمریکا و واحد ۸۲۰۰ ارتش اسرائیل معرفی شده‌است.

❖ مسئله ای فراتر از ملت ها

امروزه در پذیرش تروریسم سایبری به عنوان نوع جدیدی از تروریسم کمتر تردیدی وجود دارد.حضور تروریست‌ها در جهان مجازی یا سایبر، گویای این است که این پدیده روز به روز در حال گسترش و تغییر چهره است.
به این ترتیب تروریسم سایبری نه همچون یک نوع یا شیوه از اقدام های خشونت‌آمیز تروریستی است که بتوان آن را به طور دقیق در ذیل تروریسم قرار داد و نه ویژگی هایش محدود به ویژگی‌های جرائم سایبری است که آن را در این دسته برشمرد.
با رشد سریع و درعین حال نامتوازن ساختار فضای سایبری، این بستر به یکی از نقاط بالقوه آسیب پذیر و خطرناک در جهان بدل شده است که ضرورت توجه و رسیدگی سریع، نظام مند، معقول و هدفمند به منظور مصون سازی این بستر از تهدیدات موجود و پدیده نوظهور سایبر تروریسم را در فضای بین المللی نیز می طلبد.

❖ کلام آخر؛

پیش از هر چیز شناخت بستر ارتکاب یا فضای سایبر، ارزش‌ها و هنجارهای حاکم بر آن ضروری است، چرا که این فضا دارای گستره ای جهانی، بدون مرز، پوشیده، پنهان، ناهنجارمند و کنترل ناپذیر است.
با توجه به رشد فزاینده استفاده از اینترنت و حرکت شتابان کشورها به سمت الکترونیکی کردن خدمات اجتماعی، اقتصادی و تاثیر انقلاب اطلاعاتی بر بهبود فناوری های نظامی، امنیت بین المللی در سال‌های آتی با تهدیدات و چالش های نوینی مواجه خواهد شد.

به‌رغم اقداماتی که در راستای مبارز با تروریسم در سالهای اخیر در کشورمان انجام شده است اما عواملی باید نام برد از قبیل افزایش انواع سلاح‌ها و سهولت دسترسی به آنها، عدم سیاست کلان و قانونگذاری به‌روز و تخصصی، عدم ساماندهی صحیح فضای مجازی در کنار توسعه وسایل ارتباط جمعی، شبکه‌های اجتماعی مجازی، بدافزارها و نرم‌افزارهای سایبری که به تروریست‌ها آشنایی و قدرت عمل می‌رساند.

بنابراین باید دنبال ریشه یابی علل تروریسم سایبری، تدوین قوانین مجزا و دارای ضمانت اجرا، تشکیل شورا علیه تروریسم سایبری، همکاری با کشورها و اجماع جامعه بین‌المللی در این زمینه باشیم و بهترین راه مقابله با آن تقویت بیشتر اقدامات امنیتی، دفاع سایبری و سربازهای سایبری ایران است.

❖ **منبع**

- تروریسم سایبری علیه ایران، مهدی عبدی، کنفرانس بین‌المللی شرق شناسی، تاریخ و ادبیات پارسی
- ضرورت اقدام حقوقی علیه حملات سایبری آمریکا، حسن بهشتی پور، 1391
- سایبر تروریسم، شکل نوینی از ترور علیه منافع ملی، عنایت‌الله یزدانی، پژوهش‌های روابط بین الملل، ۱۳۹۳
- تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن، سید محمد رضا موسوی،خدیجه حیدری، علی قنبری، مطالعات بین المللی پلیس، تابستان1392
- ماهیت تروریسم سایبری، بتول پاکزاد، فصلنامه تحقیقات حقوقی، بهار 1390
- جنگ نرم در بستر تهدیدات سایبری و راهکارهای امنیت سازی، علی اکبر جعفری و ملیحه نیکروش، مطالعات عملیات روانی، زمستان و بهار 1391 و1392
- بررسی تروریسم از نظر گونه شناسی (مورد مطالعه تروریسم سایبری در بحث فناوری هسته‌ای در ایران)، مهدی جواهری، مطالعات بین المللی پلیس، زمستان ۱۳۹۴

پژوهش خبری معاونت سیاسی صدا و سیما