**جنگ نرم در بستر تهدیدات سایبری و راهکارهای امنیت‌سازی**

دکتر علی‌اکبر جعفری[[1]](#footnote-1)

ملیحه نیکروش[[2]](#footnote-2)

**چکیده**

پس از به‌کارگیری قدرت نرم در روابط میان کشورها در عرصه بین‌المللی، ماهیت منازعات و چهره تخاصم رو به دگرگونی گرایید به‌گونه‌ای که تحولی گفتمانی در عرصه جنگ پدید آمد. به عبارت دیگر، با اهمیت یافتن قدرت نرم در راستای کسب جایگاه بین‌المللی، افزایش مشروعیت و کارآمدی، کاهش هزینه‌ها و همراهی افکار عمومی، جنگ‌های نرم‌افزاری جایگزین جنگ‌های کلاسیک شدند. از همین‌رو، جنگ‌های عصر حاضر را می‌توان تحت لوای "جنگ نرم" بازشناسی کرد. البته باید توجه داشت که جنگ نرم دارای ابعادی مختلف است که در هر بُعد آن، از ابزارهای متنوعی بهره گرفته می‌شود. یکی از ابعاد جنگ نرم، تهدیدات سایبری یا جنگ سایبری است که با گسترش و افزایش دامنه فناورهای اطلاعاتی و ارتباطی بر اهمیت آن افزوده شده است. جنگ سایبری را می‌توان بهره‌گیری از رایانه‌ها و فضای تبادل اطلاعات به عنوان یک اسلحه برای دست‌یابی به اهداف معرفی کرد که به‌طور معمول به قصد اهداف سیاسی انجام می‌گیرد و از شبکه‌ها به عنوان بستر انجام اعمال خرابکارانه بهره‌برداری می‌شود. این مقاله با بررسی تهدیدات سایبری به مثابه یکی از ابعاد جنگ نرم، و پس از بازشناسی تهدیدات سایبری و سایبرتروریسم، راهکارهایی را برای امنیت‌سازی ارائه دهد. مقاله با توجه به ماهیت پژوهشی خود، از روش اسنادی-توصیفی بهره گرفته است.

**واژگان کلیدی:** سایبر، تهدید، امنیت، ابزار تهدید سایبری، راهکارهای امنیت‌سازی.

تهدیدات و جنگ را می‌توان به گونه‌هایی چون سخت، نیمه‌سخت و نرم دسته‌بندی کرد. هر قسم از تهدیدات و جنگ، دارای ماهیتی متفاوت از نوع دیگر بوده و متکی به ابزار و سازوکارهای خاص است. جنگ نرم به قدرت نرم متکی است و بر همین اساس می‌توان گفت، جنگ نرم، تهدیدی نامحسوس، بدون درگیری و به کارگیری ابزار خشونت است، لیکن با تأثیرگذاری بر اهداف موردنظر به صورت تدریجی و آرام عمل می‌کند و آثار و پیامدهای آن ماندگار است. تهدید نرم بر روی افکار و رفتار جامعة هدف عمل می‌کند (جوانی، 1388، ص108). جنگ سایبری از زیرمجموعه‌های جنگ نرم است.

عملیات روانی، جنگ رایانه‌ای، اینترنتی، براندازی نرم، راه‌اندازی شبکه‌های رادیویی و تلویزیونی و شبکه‌سازی از اَشکال جنگ نرم به شمار می‌رود که در پی از پای درآوردن اندیشه و تفکر جامعه هدف است تا حلقه‌های فکری و فرهنگی آن را سست کند و با بمباران خبری و تبلیغاتی در نظام سیاسی و اجتماعی حاکم تزلزل و بی‌ثباتی ایجاد کنند (آقامیری، 1389، ص1).

با توجه به اهمیت فناوری اطلاعات در عصر حاضر و رشد سریع و در عین حال نامتوازنِ ساختار فناوری اطلاعات، این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در جهان تبدیل شده است که ضرورت توجه و پرداخت سریع و در عین حال نظام‌مند، معقول و هدفمند را برای حفظ امنیت ملی و حریم شخصی شهروندان در فضای جنگ و مخاصمات امروز بین‌المللی نیاز دارد (بی‌نام، 1391، ص4). این مقاله با بهره‌گیری از روش اسنادی توصیفی، در بخش اول خواهان بررسی جنگ سایبری و سایبر تروریسم به مثابه ابزارهای کاربردی جنگ نرم در عصر ارتباطات است و در بخش دوم به راه‌های امنیت‌سازی در برابر تهدیدات سایبری اشاره خواهد شد. قاعدتاً فضای سایبر بر جنگ‌های نوین تأثیرگذار است و یکی از ابعاد جنگ نرم به شمار می‌رود که تفکر راهبردی برای کنترل و مهار آن، امری بایسته و ضروری است.

1. **چارچوب نظری**

جنگ در طول تاریخ همزاد بشر بوده و در دوره‌های مختلف تاریخی، با توجه به پیشرفت‌های صورت گرفته در ابزار و فنون مختلف نظامی، جنگ نیز دچار تغییر و تحول شده است. امروزه جنگ تحت تأثیر انقلاب اطلاعات و فناوری ارتباطات، دچار تحول اساسی گردیده و از جنگ سخت به جنگ نرم تبدیل شده است.

مفهوم جنگ نرم که در مقابل جنگ سخت به کار می‌رود، دارای تعریفی واحد که مورد پذیرش همگان باشد نیست و تا اندازه‌ای تلقی و برداشت افراد، جریان‌ها و دولت‌های گوناگون از جنگ نرم متفاوت است. معروف‌ترین تعریف را به جوزف نای، نسبت می‌دهند. وی در سال 1990 میلادی در مجلۀ سیاست خارجی شمارۀ 80، در مقاله‌ای تحت عنوان "تغییر ماهیت قدرت جهانی" قدرت نرم را توانایی شکل‌دهی به ترجیحات دیگران از طریق نفوذ بر افکار تعریف کرد. وی قدرت نرم را توانایی یک کشور در وادار کردن دیگر کشورها به اینکه همان چیزی را بخواهند که او می‌خواهد، آن هم از راه جاذبه‌های فرهنگی و ایدئولوژیک که در اختیار دارند، تعریف کرد. وی در این باره می‌افزاید: «همزمان با دهۀ پایانی سدۀ بیستم و به سبب دگرگونی در ماهیت سیاست بین‌الملل، اشکال ناملموس قدرت، اهمیت بیشتری یافته و قدرت، در حال گذار از منابع ثروت به منابع اطلاعات است (نای، 1990، صص182-180).

بنابراین جنگ نرم را می‌توان هر گونه اقدام نرم، روانی و تبلیغات رسانه‌ای که جامعۀ هدف را نشانه گرفته و بدون درگیری و به‌کارگیری زور و اجبار، به انفعال و شکست وامی‌دارد، تعریف کرد. امروزه جنگ نرم، مؤثرترین، کارآمدترین، کم‌هزینه‌ترین، خطرناک‌ترین و پیچیده‌ترین نوع تهدید علیه ارزش‌ها و امنیت ملی کشور به شمار می‌رود. مؤثرتر است؛ چون می‌توان با کمترین هزینه، با حذف لشکرکشی و از بین بردن مقاومت‌های فیزیکی به هدف‌ها رسید؛ و خطرناک‌تر است؛ زیرا با باورها، ارزش‌ها، عواطف و احساسات ملت ارتباط دارد. در جنگ نرم تلاش می‌شود با تأثیرگذاری بر باورها و ارزش‌های ملت، اندیشه و الگوی ادارۀ کشور به مثابۀ هویت‌دهندۀ نظام سیاسی، به چالش کشیده شود. جنگ نرم در برابر جنگ سخت در حقیقت شامل هر گونه اقدام نرم‌افزارانه اعم از روانی، تبلیغاتی، رسانه‌ای، سایبری، دیجیتالی، اطلاعاتی، فرهنگی، سیاسی، اجتماعی و علمی است که جامعه یا گروه هدف را نشانه می‌گیرد و بدون درگیری نظامی با بهره‌گیری از روش‌های اقناع‌سازی و با مدیریت احساسات و جذب، رقیب را به انفعال یا شکست وامی‌دارد (احمدزاده کرمانی، 1388، ص43). هدف نهایی در جنگ نرم مانند جنگ سخت، مهار و فروپاشی نظام سیاسی است، ولی ابزار و روش‌های این براندازی متفاوت است.

به طور خلاصه می‌توان اینگونه بیان کرد که، امروزه جنگ‌های سنتی (کلاسیک) که پیش از این مبتنی بر سخت‌افزار بود، جای خود را به جنگ‌های نوین داده است. جنگی که راهی برای ترکیب‌بندی و پیکرسازی قدرت از طریق فناوری است. حیات جنگ‌های نوین به علم وابسته است و سه گرایش عمده بیانگر چنین مطلبی است:

1. کاربست عقلانیت در جنگ به جای سنت؛
2. برپایی تشکیلات اداری و اجرایی؛
3. بهره‌گیری نظام‌مند از علم و فناوری (هیبلزگری، 1381، ص257).

جنگ در عصر اطلاعات نه تنها به واسطه فناوری، بلکه با مفاهیم و سازمان‌هایی که برای به کارگیری این فناوری ایجاد شده‌اند، شکل خواهد گرفت و آینده و چالش آن تا اندازة زیادی به توسعة مفاهیم و سازمان‌های مورد نیاز برای به کارگیری کارآمد فناوری یا دست‌یابی به خود فناوری بستگی دارد.

از جمله این فناوری‌ها در جنگ‌های نوین می‌توان به رایانه در تهدیدات سایبری مشتمل بر جنگ سایبری و تروریسم سایبری اشاره کرد. این مباحث نشان می‌دهد جنگ‌های عصر حاضر در گفتمان و فضای متفاوتی به اجرا در می‌آیند که بیشتر در ابعاد مجازی و معنوی است.

1. **عملیاتی‌سازی مفاهیم پژوهش؛ مفهوم‌شناسی**

**2-1. امنیت**

امنیت، مفهومی چندوجهی است و با توجه به دامنه وسیع مطالعه‌های مربوط به امنیت و ادبیات رایج امنیتی، دربارة معنای آن اختلاف‌‌نظرهایی وجود دارد که به مهم‌ترین آن اشاره می‌شود. امنیت در لغت به معنای ایمنی، اطمینان و آرامش خاطر و آسودگی است که این تعاریف بر "احساس آزادی از ترس" یا "احساس ایمنی" که ناظر بر امنیت مادی و روانی است، تأکید دارند (خزایی، 1388، ص13). امنیت در بُعد عینی، نبود تهدید نسبت به ارزش‌ها، منافع و اهداف به دست آمده است و در بُعد ذهنی، نبود ترس از اینکه بنیان‌های ملی، ارزش‌ها، منافع و اهداف، مورد هجوم واقع شده و از دست برود (نوروزی، 1385، ص140).

**2-2. امنیت سایبر:**

به امنیت فناوری اطلاعات، وابسته به سیاست دولت‌ها، امنیت سایبر گفته می‌شود. این اصطلاح اغلب توسط مؤسسه‌های دولتی و سیاستگذاران ملی در اسناد، قوانین و پروژه‌های تحقیقاتی استفاده می‌شود و کمابیش مترادف با "امنیت اینترنت" است. هر دو عبارت، به جوانب امنیت شبکه و اصول سیاست‌گذاری شبکه‌ها مانند تعریف حریم خصوصی، جرایم سایبر، تجارت و ارتباطات جهانی اشاره دارند.

**2-3. فضای سایبر:**

فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود (هاتف، 1386، ص50).

1. **فضای سایبر؛ جنگ سایبری**

فضای سایبر، محیط الکترونیکی واقعی است که ارتباطات انسانی در آن به شیوه‌ای سریع و فراتر از مرزهای جغرافیایی و با ابزار خاص، زنده و مستقیم روی می‌دهد (سلیمانی‌فارسی، 1388، ص41). برخلاف فضای واقعی، در فضای سایبر نیاز به جابه‌جایی‌های فیزیکی نیست و همه اعمال تنها از طریق فشردن کلیدها یا حرکت "ماوس" صورت می‌گیرد. منظور از فضای سایبر یا فضای مجازی، ترکیبی از ده‌ها هزار رایانة به هم پیوسته، سرویس‌دهنده‌ها، شبکه‌های ارتباطی، سوئیچ‌ها و کابل‌های فیبر نوری است که امکان ایجاد ارتباطات را در یک سیستم جامع فراهم می‌آورد (افتخاری، 1382، ص5). در نتیجه فضای سایبر، شبکه‌های رایانه‌ای و مخابراتی متصل به هم است که اطلاعات را در کمترین زمان و بیشترین مکان، مبادله می‌کند.

بیشتر سامانه‌هایی که به فضای سایبر وابسته‌اند و از آن استفاده می‌کنند، از این فضا به عنوان یک ضعف امنیتی یاد می‌کنند که می‌توان از آن برای انجام حملات بهره گرفت. بیشتر این سامانه‌ها به‌گونه‌ای طراحی شده‌اند که بتوانند بهره‌گیری ارزان و وسیعی از دسترسی به شبکه داشته باشند و این موضوع، توانایی سوءاستفاده مهاجمین به منظور استثمار و آسیب‌پذیر نمودن شبکه‌ها و سرویس‌های هدف را افزایش داده است.

**3-1. ویژگی‌های فضای سایبر**

از جمله ویژگی‌های اساسی فضای سایبر که باعث ایجاد محیطی مناسب برای جنگ‌های سایبر می‌شود، می‌توان به موارد ذیل اشاره کرد:

**3-1-1. گمنامی**

شناسایی و ردیابی یک سرباز جنگ سایبر در فضای سایبر و پیدا کردن مکان فیزیکی وی با توجه به تکنیک‌های خاص پنهان‌سازی در این فضا، بسیار دشوار است.

**3-1-2. تجهیزات ارزان و در دسترس**

سهولت دسترسی به ابزارهای حمله و جاسوسی و هزینه آنها نسبت به جنگ‌افزارهای حملات دیگر، سازمان‌های تروریستی را قادر ساخته تا با بهره‌گیری از تجهیزات پیچیده، پیشرفته، روزآمدِ سایبری و از طریق ارتباطات پنهان به زیرساخت‌های هدف، حمله و به اهداف خود دست یابند.

**3-1-3. در دسترس بودن هدف**

 اینترنت و ارتباطات به طور روزافزون در حال گسترش می‌باشد، و یک سرباز سایبری قادر است 24 ساعته در حال ارتباط با هدف باشد (جنگ سایبر، 1388، ص55).

**3-1-4. جهانی و فرامرزی بودن**

از ویژگی‌های منحصربه‌فردی که فضای سایبر را از دیگر رسانه‌ها ممتاز می‌سازد جهانی بودن آن است. هر فردی در هر نقطه از جهان می‌تواند از طریق آن به آسانی، به جدیدترین اطلاعات دست یابد. مرزهای جغرافیایی تاکنون نتوانسته از گسترش روزافزون فضای سایبر جلوگیری کند از این‌رو، هر نوع فیلتر و مرزبندی در برابر آن بسیار دشوار به نظر می‌رسد.

**3-1-5. دستیابی آسان به آخرین اطلاعات**

چنانچه بخواهید به آخرین مقاله، کتاب یا خبری که در زمینه تخصصی، در سطح جهان منتشر شده، دست پیدا کنید، ساده‌ترین و سریع‌ترین راه، بهره‌گیری از فضای سایبر است.

**3-1-6. جذابیت و تنوع**

رسانه‌ها از فیلم، عکس، متن یا هر هنر دیگری برای جذاب کردن خویش بهره می‌گیرند و این ابزارها در فضای سایبر قابل دستیابی است؛ به ویژه آن گاه که هیچ نظارت و فیلتری توان محدود کردنش را نداشته باشد. از ویژگی‌های منحصربه‌فردی که در تنوع و جذابیت فضای سایبر تأثیری به‌سزا دارد، مشتری‌محوری محض است. در متون نوشتاری ارتباطی تنگاتنگ میان خوانندگان و نویسندگان وجود دارد که خواننده به راحتی می‌تواند نظر خود را با شخص نویسنده در میان گذارد. از سوی دیگر، امکان نظرسنجی و ارزیابی در این فضا بسیار آسان‌تر و روزآمدتر است و این توانایی را به داده‌پردازان، فروشندگان و عرضه‌کنندگان محصولات اینترنتی می‌دهد که از آخرین خواسته‌های مشتریان و مخاطبان خود آگاه شوند.

**3-1-7. آزادی اطلاعات و ارتباطات**

معنای واقعی آزادی اطلاعات، در فضای سایبر محقق شده است. از این‌رو، شما هر نوع اطلاعاتی را که بخواهید - اعم از فرهنگی، سیاسی و اقتصادی- بدون محدودیت‌های حاکم بر دیگر رسانه‌ها، در فضای سایبر در دسترس است. آزادی ارتباطی نیز از ویژگی‌های دیگر فضای مجازی است که در دیگر وسایل ارتباطی تا این حد قابل دستیابی نیست (محمدی، 1389، صص37-36).

1. **جنگ سایبری**

جنگ سایبری، به معنی بهره‌گیری از رایانه‌ها و فضای تبادل اطلاعات به عنوان یک اسلحه یا به عنوان ابزاری برای انجام کارهای خشونت‌بار جهت ترساندن، تغییر عقیده یا نابودی یک گروه یا کشور است. جنگ سایبری به قصد کارهای سیاسی انجام می‌گیرد و مکان‌ها و زیرساخت‌هایی مانند انرژی، حمل و نقل، ارتباطات و سرویس‌های خدماتی ضروری را هدف قرار می‌دهد. در جنگ سایبر از شبکه‌ها به عنوان بستر انجام این اعمال خرابکارانه بهره‌برداری می‌شود (جنگ سایبر، 1388، ص56).

جنگ سایبر همچنین سایبرنتیک را می‌توان به صورت بهره‌گیری از رایانه و اینترنت برای جنگیدن در فضای سایبر تعریف کرد (عبداله‌خانی، 1384، ص136). به عبارت دیگر، جنگ سایبر را می‌توان هرگونه عمل جنگی دانست که در آن از سامانه‌های اطلاعاتی یا فناوری دیجیتالی چه به عنوان ابزار حمله و چه به عنوان آماج حمله بهره گرفته می‌شود؛ این حمله‌ها باید منجر به اعمال خشونت بر ضد اشخاص یا دارایی‌ها - میزانی که ایجاد رعب و وحشت کند- شود (قربان‌نیا، 1383، ص20).

شاید بتوان تعریف "رودس استارک" از جنگ سایبر را تعریفی جامع دانست؛ به عقیدة وی: «جنگ سایبر عبارت است از به‌کارگیری هدفمند یا تهدید به استفاده از جنگ رایانه‌ای یا توسل به خشونت بر ضد اهداف رایانه‌ای با انگیزه‌های سیاسی، اجتماعی، اقتصادی یا مذهبی از سوی گروه‌های غیردولتی یا گروه‌های تحت هدایت و حمایت دولت به منظور ایجاد ترس، نگرانی و وحشت در جمعیت مورد نظر و آسیب رساندن به دارایی‌ها و اموال نظامی و غیر نظامی» (استارک، 1999، ص9).

می‌توان این‌گونه بیان کرد، همانگونه که در جنگ‌های نظامی، سلاح‌های سخت‌افزاری، موجودیت دولت هدف را مورد حمله قرار می‌دهند؛ در جنگ سایبر نیز فناوری نوینِ رایانه‌ای، ماشین دولت، نهادهای مالی و زیرساخت‌های حیاتی در بخش‌های انرژی، حمل و نقل و سرانجام روحیه و عزم ملی را هدف حملات خود قرار می‌دهند.

**4-1. ویژگی‌های انواع جنگ سایبر نسبت به سایر انواع جنگ‌ها**

جنگ فیزیکی و سایبر از برخی جهات به‌طورکامل شبیه به هم هستند؛ برای نمونه هدف اصلی در جنگ هر نوع وارد آوردن ضرر و زیان به دشمن است و روش اصلی در جنگ قاعدتاً تصاحب منابع دشمن خواهد بود. نقاط افتراق جنگ سایبر نسبت به سایر جنگ‌ها را می‌توان به صورت زیر دسته‌بندی کرد:

**الف)حمله از راه دور**

نخستین تفاوت جنگ سایبر با دیگر جنگ‌ها به‌ویژه جنگ فیزیکی و حقیقی، قابلیت طراحی، اجرا و نتیجه‌گیری از راه دور است.

**ب)دشواری در شناسایی و ردیابی**

به سبب خصایصی که در پروتکل‌های ارتباطی در فضای سایبر وجود دارد، در عمل شناسایی و ردیابی منبع اصلی حمله و مهاجم اصلی، بسیار دشوار و گاه ناممکن است.

**پ)تهدید سه جنبه امنیت**

در جنگ سایبر، هر سه جنبه امنیت (امنیت، ایمنی و پایداری)، می‌تواند مورد تهدید قرار گیرد.

**ت)اندازه هدف**

در جنگ‌های فیزیکی اغلب به دنبال تخریب مناطق جغرافیایی بزرگ‌تر هستند، ولی در جنگ سایبر باید اهداف مهم و اساسی "از نظر سایبری و نقش آنها" را هدف قرار داد. این اهداف ممکن است از نظر فیزیکی بسیار ناچیز باشند ولی نقش بزرگی ایفا می‌کنند.

**ث)انتشار حمله**

حمله سایبری می‌تواند به سادگی از چندین منبع صورت پذیرد. در حالی که هدایت و راهبری حمله‌های فیزیکی که از چندین محل آغاز می‌شوند، بسیار دشوار است.

**ج)هزینه**

بی‌تردید هزینه جنگ فیزیکی از جنگ سایبر بیشتر است و این خصوصیتِ بارز فضای سایبر است که عوامل و عناصر آن در دسترس‌‌تر و ارزان‌تر هستند.

**چ)مسئولیت‌پذیری**

از آنجا که قوانین مدوّن و مشخص بین‌المللی برای مبارزه و ایجاد دعاوی سایبری وجود ندارد، کشورها به سادگی از زیر بار مسئولیت حملات سایبری خود شانه خالی می‌کنند (جنگ سایبر، 1388، ص56).

1. **سایبر تروریسم؛ مفهوم‌شناسی**

واژه سایبرتروریسم برای نخستین‌بار در دهه 1980میلادی از سوی "باری کالین" ابداع شد (ناجی‌راد، 1384، ص221). این واژه برای بیان همگرایی بین تروریسم و فضای سایبری به کار می‌رود و همان تعریفی را دارد که از تروریسم در فضای واقعی ارائه می‌شود، با این تفاوت که این بار هدف متمرکز بر روی منابع موجود در فضای سایبری است. سایبرتروریسم را می‌توان هرگونه عمل تروریستی دانست که در آن از سامانه‌های اطلاعاتی یا فناوری‌های دیجتالی چه به عنوان ابزار حمله و چه به عنوان آماج حمله بهره گرفته می‌شود. این حملات باید منجر به اعمال خشونت بر ضد اشخاص یا دارایی‌ها به میزانی شود که ایجاد رعب و وحشت کند. سایبرترورسیم در حقیقت مانند دیگر شکل‌های تروریسم است که در آن یک مؤلفه رایانه‌ای وجود دارد؛ سایبرتروریسم روش نوین اقدامات تروریستی است نه نوع دیگر تروریسم (قربان‌‌نیا، 1383، ص147).

**5-1. ابزارهای عملیاتی تروریسم سایبری**

تروریست‌های سایبری برای رسیدن به اهداف خود که همان ضربه زدن و تخریب سامانه‌های اطلاعاتی رقیب است، از یک‌سری تسلیحات استفاده می‌کنند که به آنها "تسلیحات مجازی" می‌گویند. "مایکل آنینی" و "جی.ای.ادوارد" در تعریف تسلیحات مجازی می‌گویند: «تسلیحات مجازی، تسلیحاتی است که گروه‌های تروریستی برای تخریب شبکه‌های رایانه‌ای و سرقت‌های مجازی در حجم بسیار کمتر از حجم فیزیکی آنها به کار می‌برند، زیرا این تسلیحات دارای سیستم‌های بسیار پیچیده‌ای هستند. یکی از ویژگی‌های این نوع تسلیحات این است که تروریست می‌تواند توسط آنها مرزهای بین‌المللی را سهل‌تر پشت سر گذارد». تسلیحات مجازی برای گروه‌های تروریستی سایبری، تابعی از نوع فعالیت آنهاست. بنابراین وقتی که فعالیت آنها در یک فضای مجازی است، اجزای تسلیحات آنها نیز بسته به فعالیتشان، مجازی است. می‌توان گفت ابزار مورد نیاز سایبرتروریست‌ها در همه دنیا مشترک بوده و شامل دستگاه رایانه شخصی و یک خط اینترنتی است که بتواند رایانه شخصی را به شبکه جهانی اینترنت متصل کند (ناجی‌راد، 1384، صص99-98). ظهور اینترنت به عنوان یک ابزار جدید سریع و ارزان ارتباطی، عرصه‌های مختلف زندگی بشر را دچار دگرگونی کرد و از بسیاری جهات معنا و مفهومی جدید به ابعاد آن بخشید؛ بنابراین تروریست‌های سایبری، به جای بهره‌گیری از سلاح‌های رایج، بمب‌ها و موشک‌ها یا سایر ابزارهای معمول، از نرم‌افزارهای مخرب رایانه‌ای برای پیشبرد اهداف خود بهره‌گیری می‌کنند. ویروس‌ها، کرم‌ها، تروجان‌ها، اسپم‌ها، ایمیل بمبینگ، گوگل بمبینگ، هک و نفوذ رایانه‌ای و خرابکاری یا دستکاری‌های اینترنتی و شبکه‌ای، بخشی از ابزارهای تروریست‌های سایبری به شمار می‌رود (ضیایی‌پرور، 1383، ص45).

1. **راهبردهای امنیت‌سازیِ تروریسم سایبری**

دفاع در مقابل تروریستی که در چارچوب آن رایانه و اینترنت نقشی مهم را ایفا می‌کند، تا اندازه زیادی شبیه دفاع در مقابل تروریسمی است که رایانه و اینترنت نقشی در آن ندارد. اقدام‌های عادی مانند بازدارندگی، قانون، دفاع، مذاکره و دیپلماسی در این خصوص نیز مؤثر است، بااین تفاوت که دامنه عناصرخاصی گسترده‌تر است. همچنین باید این روش‌ها روزآمد شوند. راهکارهای اصلی دفاع در برابر سایبرتروریسم را می‌توان به موارد زیر طبقه‌بندی کرد.

**6-1.آموزش**

مهم‌ترین مرحله در جلوگیری از سایبرتروریسم، آموزش است. این آموزش شامل آموزش عمومی و آموزش مسئولان اعم از مقام‌های سیاسی، امنیتی و پلیس است. در خصوص آموزش عمومی، مهم‌ترین نکته این است که کاربران اینترنت را نسبت به ایمن‌تر کردن رایانه‌های شخصی متقاعد کرد و در این راه می‌توان از آموزش‌های رسمی و اطلاع‌رسانی از طریق رسانه‌های عمومی بهره گرفت. آموزش و اطلاع‌رسانی به مقام‌های ارشد سیاسی و امنیتی نیز جایگاهی ویژه دارد و باید این مسئولان نسبت به حساسیت مسئله مطلع شوند تا تمهیدات لازم را برای مقابله با سایبرتروریسم عملی کنند (نعمتی و روجنی، 1388).

**6-2. راهکارهای حقوقی**

یکی از منطقی‌ترین و صحیح‌ترین راهکارهای مقابله با سایبرتروریسم، بسترسازی حقوقی از طریق وضع قوانین و مقررات مورد نیاز است. نخستین گام در این راه تدوین و یک شکل کردن قوانین جرایم رایانه‌ای و اینترنتی خواهد بود. در بیشتر کشورها هنوز قوانینی خاص در بارة جرایم رایانه‌ای و اینترنتی تدوین نشده است و این موضوع یعنی وجود خلأهای قانونی که نیروهای امنیتی را در مقابله با جرایم رایانه‌ای و اینترنتی، سردرگم می‌کند و توانایی واکنش به موقع و مناسب را از آنان می‌گیرد.

ایجاد دادگاه‌های خاص جرایم رایانه‌ای و اینترنتی از جمله گام‌های بسیار مؤثر در مقابله با سایبرتروریسم است. همان‌گونه که برای جرایم خاص، دادگاه‌های ویژه‌ای وجود دارد، برای مقابله با سایبرتروریسم و جرایم سایبری نیز تأسیس دادگاه‌های ویژه‌ای مورد نیاز است. وجود این‌گونه دادگاه‌ها، رسیدگی به این جرایم را آسان‌تر و سریع‌تر می‌کند و در نتیجه مجرمان یقین خواهند داشت که به سرعت و به صورت ویژه‌ای به جرم آنها رسیدگی خواهد شد و این موضوع گامی بزرگ در خصوص مبارزه با سایبر تروریسم به‌شمار می‌رود.

**6-3. تقویت دفاعی**

ایجاد سازمان‌های مسئول مقابله با سایبرتروریسم، مهم‌ترین راهکار دفاعی در برابر سایبر تروریسم خواهد بود. لازم است سازمان‌های امنیتی خاصی تأسیس شوند که مسئولیت آنها مطالعه و تحقیق و مقابله با حمله‌های سایبری باشد.

از روش‌های دفاعی که می‌توان به آنها اشاره کرد: سخت‌تر کردن حمله‌ها از طریق تقویت فناوری‌های امنیتی، تعریف روزآمد ویروس‌های رایانه‌ای، به‌کارگیری نرم‌افزارهای ضدویروس و بهره‌برداری از رمزهای عبور قوی و دیوار آتش است (گوردون، 2003، صص12-11).

**6-4. تدابير كاربري صحيح**[[3]](#footnote-3)

اين خط‌مشي‌ها، يك سري راهكارها و انتظاراتي دربارة نحوه فعاليت آنلاين افراد هستند كه به نحو روزافزوني در مدارس، منازل و كتابخانه‌ها به كار مي‌روند. مباني نظري آنها، مسئوليت‌پذير كردن كودكان در برابر محتوايي است كه ايجاد مي‌كنند و رفتاري كه بروز مي‌دهند. آنها ياد مي‌گيرند در برابر مسائل مختلفي كه ممكن است در فضاي سايبر تجربه كنند، گزينه‌هاي شايسته‌اي داشته باشند. به اين ترتيب، با مهارت‌هاي بهره‌گیری صحيح از اينترنت آشنا مي‌شوند. البته اگر قرار است اين خط‌مشي‌ها مؤثر واقع شود، بايد براي موارد نقض عمدي، واكنش يا ضمانت اجراهاي متناسب اعمال كرد؛ مانند عدم اجازه بهره‌گیری از اينترنت، ارتباط با والدين. اما بايد از موارد نقض غيرعمدي و تصادفي نيز به عنوان فرصتي براي آموزش كاربران در خصوص نحوه اجتناب آنها از مواجهه آتي با اين‌گونه مسائل، نحوه برچيدن آنها از روي صفحه نمايش و در صورت لزوم، گزارش به ارائه‌دهندگان خدمات اينترنتي بهره‌برداري كرد.

**6-5. تقویت سرمایه اجتماعی**

سرمایه اجتماعی از جمله عواملی است که وجود آن خنثی‌کننده جنگ نرم دشمن خواهد بود؛ چرا که وجود عواملی همچون وفاداری، اعتماد، امید و... مبانی و شالوده‌های نظم و نظام اجتماعی را مستحکم نموده، باعث تقویت انسجام اجتماعی می‌شود. سرمایه اجتماعی را می‌توان به مثابه منبع کنش جمعی در نظر گرفت که منتهی به نتایج وسیعی می‌شود. سرمایه اجتماعی، نشانه یک جامعه قوی بوده و بخشی از فرایند ظرفیت‌سازی است. به عبارتی می‌توان بیان داشت اهمیت این مقوله به اندازه‌ای است که موفقیت جوامع، افراد و به نوعی امنیت جامعه به آن بستگی دارد (استون، 2000، صص27-25). بنابراین امیدآفرینی، نگاه خوش‌بینانه و امیدوارانه، اعتمادافزایی به ویژه با رفتار و عملکرد مسئولان و حُسن ظن، می‌تواند در ناکامی جنگ نرم دشمن مؤثر واقع شود.

6-6. **به کارگیری الگوهای پیشگیری؛ وضعی و اجتماعی**

از میان الگوهای مختلف پیشگیری که به‌ویژه طی نیم قرن اخیر مورد نظریه‌پردازی و آزمون قرار گرفته‌اند، پیشگیری وضعی[[4]](#footnote-4) و اجتماعی[[5]](#footnote-5)، به عنوان یکی از جامع‌ترین راهکارهای موفقیت‌آمیز پیشگیری از جرم مورد توجه قرار گرفته است (نجفی ابرندآبادی، 1380، ص748).

به طور خلاصه، در پیشگیری اجتماعی، هدف، از بین بردن انگیزه مجرمانه[[6]](#footnote-6) است و به همین دلیل، به آن پیشگیری بزهکارمحور[[7]](#footnote-7) گفته می‌شود. در اینجا راهکارهای اجتماعی، مانند رفع بیکاری و فقر که زمینه‌ساز شکل‌گیری انگیزه‌های مجرمانه مالی و حتی قتل می‌شوند همچنین راهکارهای تربیتی و آموزشی[[8]](#footnote-8) برای کودکان، به عنوان آسیب‌پذیرترین گروه سنی، هم از لحاظ بزهکاری و هم از لحاظ بزه‌دیدگی، در دستور کار قرار می‌گیرند (نیازپور، 1382، ص138). اما در پیشگیریِ وضعی، هدف، صیانت از بزه‌دیدگی بالقوه از طریق سلب فرصت[[9]](#footnote-9) یا ابزار[[10]](#footnote-10) ارتکاب جرم است (شیندر، 2002، ص353). با توجه به این توضیحات اجمالی، به نظر می‌رسد نحوه اجرای تدابیر پیشگیرانة اجتماعی و وضعی در فضای سایبر روشن شده باشد. اگر واقعیت‌ها و شرایط خاص حاکم بر این فضا به خوبی به کاربران آن، که بیشتر قشر جوان و نوجوان جامعه هستند، منعکس شود، از شکل‌گیری و تحقق بسیاری از انگیزه‌های مجرمانه و در عین حال بزه‌دیدگی آنها پیشگیری خواهد شد. هم‌اکنون این مسئله تا حدی مورد توجه قرار گرفته که مباحث تخصصی تحت عنوان اخلاق سایبری[[11]](#footnote-11) از سوی صاحب‌نظران و سیاست‌گذاران این حوزه مطرح شده است (جلالی‌فراهانی، 1385، ص65). با این حال، از آنجا که این فضا ماهیتی فنی دارد، دست‌اندرکاران بیشتر به دنبال اجرای تدابیر پیشگیرانه وضعی فنی هستند که از نمونه‌های بارز آن می‌توان به انواع فیلترها[[12]](#footnote-12) و تدابیر نظارتی اشاره کرد که البته ناکارآیی‌های این‌گونه ابزارها بر همگان محرز شده، اما به کارگیری آنها اجتناب‌ناپذیر است (جلالی فراهانی، 1384، ص133).

اما در خصوص کارآیی این تدابیر در مورد اقدامات تروریستی سایبری، روشن است که تدابیر پیشگیرانه اجتماعی ماهیت تروریسم را هدف قرار می‌دهند و در این جهت می‌توانند از فضای سایبر به عنوان یک ابزار اطلاع‌رسانی و تبلیغاتی نیز استفاده کنند و البته تأکید ویژه‌ای بر این اقدامات در فضای سایبر داشته باشند. تدابیر پیشگیرانه وضعی نیز بیشتر بدون توجه به هویت مجرمان به کار می‌روند. برای نمونه، هدف، پیشگیری از آلوده نشدن سامانه‌‌ها به انواع ویروس‌ها یا محتواهای مستهجن است و تفاوتی نمی‌کند مرتکب آن چه کسی است. البته برای برخی سامانه‌‌ها که در زیرساخت‌های حیاتی مستقر هستند و اغلب مجرمانی همچون تروریست‌ها قصد تعرض به آنها را دارند، ‌باید برنامه‌ریزی‌های ویژه‌ای صورت گیرد. همچنین برای اینکه از دسترس کاربران به محتواهای ارسالی از سوی تروریست‌ها جلوگیری شود، مانند انواع پیام‌های تحریک‌کننده و مخل آسایش عمومی، ‌باید فهرست‌های سیاه یا سفید[[13]](#footnote-13) فیلترها به نحوی تنظیم شود که تمامی حوزه‌های مربوط را شناسایی و دسترس‌ناپذیر کنند.

**نتیجه‌گیری**

آنچه در اين مقاله تبيين شد، راهكارهاي مقابله با ناهنجاري‌هاي مجرمانه و منحرفانه سايبر و ميزان كارايي و نتيجه‌بخش بودن آنها بود. با ملاحظه محدوديت‌هاي حاكم، محرز شد که گزينه ساده‌اي پيشِ رو قرار ندارد. اما آثار مثبت و سازندة آن، در صورت حصول نتيجه، به مراتب از تمهيدات پيشگيرانة وضعي و ضمانت اجراهاي كيفري و غيركيفري ماندگارتر و اميدواركننده‌تر است. از مهم‌ترین اقدامات می‌توان به آموزش جرایم حقوقی و کیفری اشاره کرد که آموزش شامل آگاه ساختن از خطرهای رفتار زيان‌بار و غيرقانونيِ آنلاين و يادگيريِ نحوه محافظت از خود و ديگر كاربران اينترنت در برابر آنهاست. در اينجا بر آموزش قشر جوان تأكيد ويژه‌اي مي‌شود؛ زيرا از توانايي بالايي براي لطمه زدن به خود و ديگران برخوردارند و به همين دليل، عمده مفاد آموزشي آنها با محوريت بهره‌گیری ايمن و مسئولانه از فضاي سايبر ارائه مي‌شوند.

در هرحال، راهبردهايي كه مي‌توانند براي حل اين مسئلة چند مجهولي، يعني نهادينه‌سازي اخلاق سايبري با كمك راهكارهاي جرم‌شناختيِ پيشگيران اجتماعي سايبري، سودمند واقع شوند عبارتند از:

**1**- پيش از هرچيز، بايد با توجه به شرايط اجتماعي و فرهنگي جامعه، شناخت صحيح و واقع‌گرايانه‌اي از كاربران فضاي سايبر در حوزه‌هاي مختلف به دست آید؛

**2**- سپس بايد هنجارهاي اخلاقي مربوط، كه بي‌ترديد هدف اصلي آنها بهره‌برداري مشروع و سودمند از اين فضا و دوري جستن از هرگونه جرم، انحراف و سرانجام رفتارهاي غيراخلاقي است، وضع شوند؛

**3**- سرانجام اينكه، به هنگام تدوين اين هنجارها نبايد از راهكارهاي پيشگيرانة وضعي همچنين ضمانت اجراهاي كيفري و غيركيفري غافل ماند، زيرا در واقع نه تنها قرار است و بايد اين تدابير در آن هنجارها منعكس شوند و به اجراي صحيح آنها كمك كنند كه اجراي مؤثر، متناسب و بازدارندة آنها نيز وابسته به انعكاس صحيح آنها در تدابير پيشگيرانة اجتماعي است.

**منابع**

- در نسخه چاپی موجود است.

1. .استادیار و عضو هیئت علمی دانشگاه مازندران. [↑](#footnote-ref-1)
2. .کارشناسی ارشد علوم سیاسی دانشگاه مازندران. [↑](#footnote-ref-2)
3. 1. Acceptable Use Policies [↑](#footnote-ref-3)
4. 1. Situational Prevention [↑](#footnote-ref-4)
5. 2. Social Prevention [↑](#footnote-ref-5)
6. 3. Crimina Motivation [↑](#footnote-ref-6)
7. 4. Criminal-based Prevention [↑](#footnote-ref-7)
8. 5. Developmental-based Crime Prevention [↑](#footnote-ref-8)
9. 6. Opportunity [↑](#footnote-ref-9)
10. 7. Tool [↑](#footnote-ref-10)
11. 8. Cyber Ethics [↑](#footnote-ref-11)
12. 9. Filters [↑](#footnote-ref-12)
13. 1. Black & White Lists [↑](#footnote-ref-13)