فضای سایبری: یک عرصه نوین در امور جنگی

از دیرباز، زمین و دریا عرصه‌های اصلی جنگ بوده‌اند. پادشاهان و حاکمان نیروی زمینی و دریایی و دژ و قلعه می‌ساختند و برای رصد کردن حرکات دشمنان بالقوه خود، دیدبان و جاسوس می‌گماشتند. آن‌ها اگر تشکیلات خود را درست سازماندهی می‌کردند، قبل از این که حمله‌ای صورت بگیرد معمولاً نوعی اطلاع اولیه از وقوع آن داشتند؛ لذا می‌توانستند اقدامات لازم برای مقابله را انجام دهند. حداقل تا قبل از اختراع توپخانه‌های مدرن، دژها نوعی حس امنیت را فراهم می‌کردند.

زمانی که فناوری پرواز توسعه یافت، آسمان نیز به یک عرصه جدید بدل شد. مشخص است که راهی برای وارد نشدن به این عرصه جدید وجود نداشت؛ اگر دشمن نیروی هوایی خود را توسعه می‌داد، طرف مقابل هم باید پدافند هوایی خود را مجهز می‌کرد و در غیر این صورت نیروی دریایی و زمینی‌اش امکان کمی برای پیروزی داشت. از آن پس راهبُرد نظامی با این منطق تکامل یافت که چرا منابع خود را صرف حمله به مرزهایی کنیم که به خوبی محافظت می‌شوند درحالی‌که می‌توانیم به عمق سرزمین دشمن، مراکز جمعیت و حتی مراکز تصمیم سازی آن‌ها حمله کنیم. ترکیب شدن فناوری و راهبُرد نظامی به این انجامید که نوع جنگ از سنگرهای جنگ جهانی اول به حمله‌های هوایی جنگ جهانی دوم مبدل شود.

و اما امروزه فضای سایبری به عنوان عرصه‌ای مستقل ظهور پیدا کرده است و از جنبه‌های زیادی شبیه به زمین، دریا و آسمان است، البته در میان این میدان‌های جنگ، به احتمال زیاد عرصه‌ای خواهد بود که انتخاب خواهد شد (برتری خواهد داشت)؛ با اطمینان زیادی می‌توانیم بگوییم که در آینده هر درگیری‌ای بین بازیگران پیشرفته، از نوع درگیری سایبری خواهد بود. هیچ مهاجم مدرنی در برابر وسوسه تخریب، مختل کردن و یا گیج کردن حسگرها و ارتباطات و حلقه‌های تصمیم‌گیری دشمن مقاومت نخواهد کرد. چیزی که متفاوت خواهد بود این است که آیا نزاع در عرصه فیزیکی هم رخ خواهد داد یا خیر؟ این دیدگاه ذات جنگ را از پایه دچار تحول خواهد کرد، احتمالاً آستانه وقوع جنگ را پایین خواهد آورد و تفکیک مرز بین جنگ و صلح را پیچیده‌تر خواهد کرد.

در ست مثل زمان اختراع پرواز، نمی‌توان ن سبت به عر صه نوین سایبر بی‌تفاوت بود و به آن ورود نکرد. جامعه مدرن به طور ذاتی به ف ضای سایبر واب سته شده ا ست. رود بک ستروم[1]، رئیس سابق ICANN دراین‌باره می‌گوید که: «هر چیزی که شبکه‌ای باشد قابلیت هک شدن دارد. همه چیز شبکه‌ای است پس همه چیز درمعرض‌خطر است.»

جنگ سایبری ویژگی‌های مشترکی با حوزه‌ی جنگ فیزیکی دارد، اما در بسیاری از ویژگی‌ها دیگر با آن متفاوت است. برای شروع می‌توانیم بگوییم فناوری معمولاً استفاده دوگانه دارد؛ به عنوان مثال اگر کشوری هواپیمای جنگی بسازد، معلوم است به دنبال اهداف نظامی است، اما اگر کشوری سیستم IT خود را ارتقا دهد، نمی‌توان استنتاج کرد که به دنبال اهداف نظامی است.

این که هر چیز شبکه‌ای می‌تواند هک شود، صرفاً شامل سی ستم‌های ارتباطی پایگاه‌های نظامی نی ست؛ بلکه شامل هر نوع زیر ساخت، منبع انرژی، شبکه برق‌ر سانی، سی ستم سلامت، سی ستم کنترل ترافیک یا ذخایر آب و تمام حسگرها و ارتباطات این سیستم‌ها نیز می‌شود. این واقعیت که ق سمت عمده‌ای از ف ضای سایبری تو سط بخش خ صو صی مدیریت و کنترل می شود نیز حفظ امنیت فضای سایبری را پیچیده‌تر می‌کند.

دومین تفاوت مهم در جهان «د شمنان[2]» بالقوه ا ست. برای یک پاد شاه در قرون و سطی د شمنان نوعاً کشورهای همسایه بودند که پادشاه کم و بیش تعداد آن‌ها را می‌دانست. در واقع مجاورت جغرافیای یک عامل تأثیرگذار بود. درحالی‌که که امروزه تعداد نهادهایی که دارای ظرفیت یک حمله بالقوه ویرانگر هستند به شدت افزایش یافته است؛ نه تنها دولت‌ها بلکه هکرها، تروریست‌ها، شرکت‌ها، گروه‌های اجتماعی، مجرمان و حتی کاربران رایانه‌ای غیرمشکوک هم می‌توانند د ست به چنین حمله‌ای بزنند. با این وصف می‌توان گفت که مجاورت جغرافیای، یکی از پیش‌شرط‌های اساسی نظریات نظامی سنتی، از بین رفته است و دیگر موضوعیت ندارد. سومین تفاوت به ظرفیت «هشدار اولیه[3]» بر می‌گردد که بسیار کاهش‌یافته یا اصلاً وجود ندارد. شما باید در هر زمان و مکانی حفاظت شوید. دیگر مثل گذشته «بسیج نیروها[4]» تأثیرگذار نیست، باید در همه حال

[1] *Rod Beckstorm*
[2] *Adversary*
[3] *Early Warning*
[4] *Mobilizing Forces*

هشیار باشید و در نظر بگیرید که حمله واقعی ممکن است اتفاق بیفتد و احتمالاً هم اتفاق خواهد افتاد.

در جنگ سایبری شما لزوماً نمی‌دانید که چه کسی احتمالاً به شما حمله خواهد کرد و حتی شاید ندانید چه کسی قبلاً به شما حمله کرده است. یافتن مقصر در حمله سایبری سخت است، چرا که مهاجمان می‌توانند از «پراکسی‌ها» برای مقصر جلوه دادن دیگر افراد یا گروه‌ها استفاده کنند؛ بنابراین تاکید زیادی بر بهبود فناوری لازم برای یافتن مهاجم وجود دارد. بدون یافتن مهاجم، انتقام و بازدارندگی غیرممکن خواهد بود. حتی با داشتن فناوری لازم، مسئله ردیابی مهاجم، می‌تواند دارای پیچیدگی‌های خاصی باشد؛ از لحاظ سیاسی بیان هر چیزی از آن مطلع هستید می‌تواند دارای حساسیت باشد و یا اینکه که اطلاعاتی حیاتی را افشا کند که همین موضوع احتمالاً در آینده توانایی شناسایی مهاجم را از بین می‌برد.

چهارم این که در فضای سایبر، هشدار اولیه تا حد زیادی وجود ندارد. منطق دفاع سنتی فرض می‌کند که خواه چند ماه یا چند دقیقه قبل تر از حمله، همیشه علائمی از حمله‌ای که قرار است رخ دهد وجود دارد؛ علائمی مانند حرکت نیروها جنگی به سمت مرزها و یا تشخیص موشک از طریق رادار؛ اما این هشدار اولیه در مورد حمله‌های سایبری صدق نمی‌کند. در بهترین حالت وقتی حمله سایبری رخ می‌دهد، شما در همان لحظه‌ی حمله متوجه آن شوید و حتی ممکن است بعد از وقوع حمله مطلع شوید. این واقعیت مفاهیم «بسیج نیرو[1]»، «تجدید قوا[2]» یا «اقدامات دفاعی در یک نقطه خاص[3]» را بی‌اعتبار می‌کند.

همه این عوامل به یک نتیجه منتهی می‌شود: در فضای سایبری، حمله کردن تا حد زیادی راحت‌تر از دفاع کردن است. در جنگ سنتی، معمولاً مدافع مزیت‌هایی نسبت به مهاجم داشت و مهاجم برای پیروزی به برتری در تعداد نیروی‌های نظامی، فناوری و راهبُرد جنگی نیاز داشت. در حقیقت در دفاع سایبری نیاز است که همیشه و در همه جای زیرساخت‌های حیاتی حاضر باشید.

---

[1] *Mobilization*
[2] *Regrouping*
[3] *Point-Specific Defense Measures*

با این حال همه کشورها، متقابلاً به فضای سایبر وابسته هستند و این باعث امیدواری است؛ چرا که بر مبنای منطق حاکم بر نظریه بازی‌ها، این واقعیت مانع رخ دادن یک جنگ سایبری میان بازیگران می شود. مشابه همین منطق در مورد استفاده از سلاح هسته‌ای وجود دارد و مانع از به وجود آمدن درگیری‌هایی شده است که به نابودی هر دو کشور بیانجامد. این موضوع حتی ممکن است انگیزه‌ای برای کشورها ایجاد کند تا فناوری دفاعی را با یکدیگر به اشتراک بگذارند.

با این حال، اقدام متقابل دولت‌ها در ارزیابی توان دفاعی یکدیگر، ممکن است که «توازن وحشت[1]» را به خطر بیندازد. همه به خوبی می‌دانند که کشورها و بازیگران غیردولتی پیشرفته عوامل پنهانی (ویروس، کرم‌های رایانه‌ای...) خود را در سیستم اطلاعاتی یکدیگر وارد می‌کنند. این‌گونه بدافزارها دائماً در سیستم‌های دفاعی و زیرساخت‌های حیاتی مختلف یافت می شوند که ممکن است منجر به بالا گرفتن غیرعمدی درگیری تا حد یک نزاع تمام‌عیار شود.

گروه‌های افراطی به نحو فزاینده‌ای از ابزارهای سایبری برای تبلیغ کردن، ایجاد رعب و وحشت، عضوگیری و جلب حمایت‌های مالی بهره می‌برند درحالی‌که سیاست‌گذاران، رهبران نظامی و سرویس‌های امنیتی به سختی می‌توانند خود را به پای آن‌ها برسانند. تلاش‌های این نهادها تاکنون بیشتر ماهیت واکنشی نسبت به تحرکات تروریستی داشته است تا این که نوعی پیشگیری از آن باشد.

سایبر در راهبردهای نظامی دولت‌ها نیز حائز اهمیت است که البته این راهبردهای نظامی، عملیات سایبری[2] را به انضمام عملیات روانی[3] در بر می‌گیرد؛ به عنوان مثال مخابره اطلاعات غلط یا حمله به یکپارچگی داده‌ها که می‌تواند باعث ایجاد هشدارهای اشتباهی شود و مثلاً حسگرهای یک نیروگاه هسته‌ای یا هشدارهای حمله هوایی را با خطا مواجه کند.

بنابراین هر چه که زندگی روزمره به فضای سایبری بیشتر وابسته می‌شود، این احتمال نیز افزایش می‌یابد که طی یک جنگ سایبری، صدمات ویرانگر فیزیکی، اقتصادی و اجتماعی بیشتری ایجاد شود. برای حل این مشکل، جهان نیازمند یک چارچوب سیاست‌گذاری است از پیشگیری و

---

[1] *Terror Balance*
[2] *Cy Ops*
[3] *Psi Ops*

بازدارندگی گرفته تا قواعد جنگ مدرن. البته قواعد تناسب [1]و تمایز (تفکیک)[2] کنوانسیون ژنو به نظر کاملاً مرتبط می‌رسد، اما اعمال و امکان اجرایی شدن آن‌ها و حتی تطبیق شان با واقعیت‌های جدید هر روز دشوارتر می‌شود.

به عنوان مثال کدام عمل مصداق جنگ سایبری تلقی می شود؟ اگر حمله سایبری باعث تخریب فیزیکی شود، مقابله به مثل فیزیکی را توجیه می‌کند؟ در مورد منبع و بانی یک حمله سایبری چقدر باید اطمینان داشت تا بتوان عمل تلافی‌جویانه را توجیه کرد؟ در جنگ سایبری مرز بین بازیگران و تأسیسات نظامی و شهروندان را چگونه باید تعیین کرد؟

نمی‌توان فضای سایبری را به عنوان یک حوزه بی‌قانون دید زیرا مقرراتی ملی و بین‌المللی در این باب وجود دارد و هنجارهای بین‌المللی رفته‌رفته ایجاد می‌شود؛ اما تغییرات تکنولوژیک سرعتی بالاتر از پیشرفت معاهدات نظامی در مورد فضای سایبری دارد. بدون افزایش تلاش‌ها برای ایجاد یک نظام دقیق از هنجارها و قواعد جهانی، ما در معرض خطر جدی ترک برداشتن خط و مشی امنیت سایبری هستیم.

در مورد از بین رفتن اعتماد مردم که از نگرانی‌های مربوط به حریم خصوصی و حقوق بشر ناشی می‌شود، دولت‌ها باید اقدامات بهتری در راستای ارتباط بیشتر با مردم در مورد اعمال و دیدگاه‌هایشان انجام دهند و همچنین باید به مردم اطمینان بدهند که از طریق اقدامات درست و قانونی هنوز هم توانایی امنیت بخشیدن به جامعه را دارند.

---

[1] اصل تناسب (The Principle Of Proportionate) : این اصل حاکی از آن است که بین شدت و نوع اقدام با هدف مورد نظر باید تناسب باشد. مثلاً اگر امکان دستگیری سربازی از دشمن وجود داشته باشد، نباید آن را کشت. در واقع، اقدامات باید با شرایط و حقوق مترتب بر هدف نظامی متناسب باشد.

[2] اصل تفکیک (The Principle Of Distinction) :در مخاصمات از یک سو افراد و تجهیزات نظامی وجود دارند و از سوی دیگر، افراد و تجهیزات غیرنظامی متحمل ورود ناخواسته به جنگ می گردند و به همین جهت و با توجه به اینکه غیرنظامیان در حقوق بین الملل بشردوستانه تحت حمایت کامل قوانین مربوطه هستند، باید بین این دو گروه تفکیک قائل شد. به همین جهت است که حمله تحت هیچ شرایطی به غیرنظامیان مجاز نمی باشد و برای جلوگیری از این حملات باید تفکیک لازم بین اهداف نظامی و غیرنظامی صورت پذیرد. ماده ۵۱ پروتکل اول الحاقی، حمله به غیرنظامیان را ممنوع کرده و این امر ناشی از اصل تفکیک می باشد.

در مورد فعالیت‌های سایبری مخرب که امنیت بین‌المللی را به خطر می‌اندازند، شرکت‌های بخش خصوصی موظف به ایجاد رویه‌هایی برای آگاه‌سازی دولت‌ها و حتی گاهی اوقات ملزم به کمک برای مقابله به مثل هستند. متأسفانه این مسئولیت‌پذیری همیشه وجود ندارد، چرا که شرکت‌ها معمولاً نمی‌خواهند که ضعف‌های خود را برای امنیت عمومی عیان کنند یا اینکه یک حمله موفق را گزارش کنند.

بخش خصوصی و عمومی به همکاری بیشتری نیاز دارند تا فهم مشترکی از مرز میان شان پیدا کنند و به هماهنگی مناسبی برای مقابله با دشمنانی که هیچ‌وقت قانونی عمل نمی‌کنند برسند. بدون چنین همکاری‌ای، تهدیدات بر آمادگی ما پیشی خواهند گرفت.

تلاش‌های کنونی باراک اوباما و خی جین پینگ (رئیس‌جمهور وقت چین) برای رسیدن به یک توافق درباره مجموعه جدیدی از قوانین نوع برخورد با سایبر به عنوان یک ظرفیت نظامی، قدمی در مسیر درست است. با این حال هنوز هم در مورد چگونگی اجرایی شدن هر گونه توافق در باب بهبود امنیت بین‌المللی در برابر تهدیدات حوزه سایبر و چگونگی برخورد با مسئله سیاسی و حساس «شناخت مقصر»، به همکاری‌های بیش‌تر و مناسب‌تر نیاز مبرم وجود دارد.

انجمن اقتصاد جهانی[1] به عنوان یک نهاد عمومی برای همکاری‌های عمومی-خصوصی، یک زمینه مناسب برای گفتگوی وسیع بین گروه‌های مختلف را در مورد این مسائل فراهم می‌کند. بدون آمادگی کافی و آگاهی عمومی، مسیر سختی پیشروی ما خواهد بود؛ زیرا ما فقط خود را به هم متصل‌تر نمی‌کنیم بلکه درعین‌حال خود را هم بیشتر«وابسته به یکدیگر» و «در معرض خطر» می‌کنیم.

[1] World Economic Forum