تاریخ وصول: ۱۳۹۲/۱۲/۱۷
تاریخ پذیرش: ۱۳۹۳/۰۱/۲۳

رویکرد دفاعی – تهاجمی جمهوری خلق چین در چارچوب فضای سایبر

شهروز ابراهیمی[۱]*
احمد جالینوسی[۲]
طیبه قنواتی[۳]

۱. استادیار روابط بین الملل دانشگاه اصفهان، اصفهان، ایران.
۲. استادیار روابط بین‌الملل دانشگاه اصفهان، اصفهان، ایران.
۳. کارشناسی ارشد رشته روابط بین‌الملل از دانشگاه اصفهان، اصفهان، ایران.

چکیده

اهمیت قدرت نرم و فضای سایبری در بستر تکنولوژی‌های اطلاعاتی و ارتباطاتی بر کسی پوشیده نیست. چین با اذعان به این اهمیت و با این چشم‌انداز که جنگ‌های آینده ممکن است جنگ‌های سایبری باشد اهمیت ویژه‌ای در رویکردهای دفاعی- تهاجمی خود به فضای سایبر و قدرت نرم داده است. سؤال اصلی نوشتار این است که جمهوری خلق چین در بستر قدرت نرم و فضای سایبر چه رویکرد دفاعی- تهاجمی پیش گرفته است؟ فرضیات نوشتار در پاسخ به سؤال اصلی این است که ۱- با توجه به این که جنگ‌های آینده ممکن است جنگ سایبری باشد، چینی‌ها در رویکرد دفاعی خود به دنبال حفظ شبکه‌های حیاتی و زیرساخت‌های حساس خود هستند.۲- چین به دنبال طراحی نوعی جنگ جدید است که در میادین آتی جنگ، برتری اطلاعاتی را در مقابل دشمنان بالقوه خود به آن اعطا نماید. مقاله به روش توصیفی- تحلیلی و با ابزار کتابخانه به رشته تحریر درآمده است یافته‌ها حکایت از آن دارد که چینی‌ها در طراحی جنگی خود برای آینده در مقابل رقبای بالقوه در جهت حفظ زیر ساخت‌ها و شبکه‌های حیاتی خود در چارچوب رویکرد دفاعی و در جهت تخریب زیرساخت‌های حیاتی دشمنان در چارچوب رویکرد تهاجمی، دکترین جنگ سایبری و اطلاعاتی خود را تنظیم نموده‌اند.

واژگان کلیدی: اینترنت، جنگ سایبری، دکترین سایبری چین، قدرت نرم، فضای سایبر.

* ایمیل نویسنده مسئول: shahrooz366@gmail.com

مقدمه

پس از به قدرت رسیدن دنگ شیائوپینگ، که زمینه‌های آن از زمان چوئن لای فراهم شده بود، جمهوری خلق چین بر اصلاحات و مدرنیزاسیون اقتصادی روی آورد و در همان حال حضوری نسبتاً اندک در امور جهانی داشت، پس از آن، در اواخر دهه ۱۹۹۰ و نیز پایان جنگ سرد، چین دوباره رویه خود را تغییر داد و با اتخاذ یک استراتژی بر مبنای جنگ نرم در برابر غرب، بر قدرت نرم متمرکز گردید(ماه پیشانیان،۱۳۸۹:۷۵۷-۷۷۶). در سال‌های اخیر نیز جهش و رشد اقتصادی چین بسیاری از نگاه‌ها را متوجه خود ساخته است، عده‌ای آن را الگوی خود می‌کنند و گروهی نیز این پیشرفت را موقتی می‌دانند که پس از مدتی فروکش خواهد کرد. در این میان نکته‌ای که کمتر به آن پرداخته می‌شود و حتی کنگره آمریکا نیز به گفته نای از آن غافل ماند، قدرت نرم چین است. قدرتی که بیش از آنکه در تجهیزات نظامی و تصرف سرزمین‌ها نمود داشته باشد در فرهنگ، ارزش‌ها، آداب و رسوم، آرمان‌های یک کشور و تسخیر قلب‌ها و اندیشه‌ها یافت می‌شود(گلشن پژوه،۱۳۸۸: ۶۹-۴۲).

چندین عامل دلیل روی آوردن چین به چنین تغییری بود: نخست اینکه، توسعه اقتصادی چشمگیر در این کشور، اعتماد و اعتبار زیادی را به رهبری و مردم چین و جایگاه آن در جهان داد. دوم اینکه به دنبال واکنش جهانی به حادثه«میدان تیان آن من» و تحریم این کشور از سوی غرب، چین متوجه شد که نمی‌تواند صرفاً به روابط با ایالات متحده اتکا داشته باشد و بنابراین باید روابط خود با کشورهای همسایه را گسترش داده و نقش بین‌المللی بیشتری را برای کسب اهدافش اتخاذ نماید. شاید مهم‌تر از همه، این موضوع مورد توجه مقامات چینی قرار گرفته بود که تلاش‌ها برای حصول به اهداف از طریق قدرت سخت، نظیر اعزام کشتی‌های نظامی به نواحی مورد اختلاف در دریای چین جنوبی و شلیک موشک‌ها به تنگه تایوان، نه تنها نشان داد که چین نمی‌تواند امیدی به رقابت یا قدرت سخت آمریکا داشته باشد، بلکه همچنین کشورهای دیگر را نیز با آن دشمن کرده است (ماه پیشانیان، ۱۳۸۹: ۷۷۶-۷۵۷). براین اساس در نوشتار حاضر ضمن بررسی قدرت نرم چین، به این امر پرداخته می‌شود که چین چگونه از فضای سایبر در جهت افزایش قدرت نرم و نیز در رویکردهای دفاعی- تهاجمی بهره برداری نموده است؟ دو فرضیه مورد بررسی در نوشتار به شرح ذیل می‌باشد:

الف. با توجه به این که جنگ‌های آینده ممکن است جنگ سایبری باشد، چینی‌ها در رویکرد دفاعی خود به دنبال حفظ شبکه‌های حیاتی وزیر ساخت‌های حساس خود

هستند. ب.چین به دنبال طراحی نوعی جنگ جدید است که در میادین آتی جنگ برتری اطلاعاتی را در مقابل دشمنان بالقوه خود به آن اعطاء نماید.

۱. مبانی مفهومی ـ نظری: قدرت نرم و فضای سایبر

فضای سایبر به معنای مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و وسایل مخابراتی، بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. منظور از فضای سایبر فضای مجازی ترکیبی از ده‌ها هزار رایانه بهم پیوسته، سرویس دهنده‌ها، شبکه‌های ارتباطی، سویچ‌ها و کابل‌های فیبر نوری است که امکان ایجاد ارتباطات را در یک سیستم جامع فراهم می‌آورد (محمدی،۷۷:۱۳۸۹). در نتیجه شاید بتوان تعریف سه جزیی زیر را به عنوان تعریف نسبتا جامع و مانع فضای سایبرنتیک پذیرفت:

الف. فضای روانی- خیالی که در آن افکار مجذوب توهمی رویا گونه می‌شود.

ب. دنیای مفهومی تعاملات شبکه‌ای شده بین افراد و آفریده‌های معنوی‌شان و هر چیز همراه با چنین شبکه‌ها و تعاملاتی.

ج. حالتی از اندیشه که توسط افراد در ارتباط و به وسیله بازنمایی‌های دیجیتال زبان و تجربه‌ی حسی به اشتراک گذاشته می‌شود. افرادی که بوسیله‌ی زمان و مکان از یکدیگر جدا، اما با شبکه‌هایی از ابزار فیزیکی دسترسی، به یکدیگر متصلند.(Whittle, 1997: 9)

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

اول. تعدد بازیگران در فضای سایبری: هزینه کم فن‌آوری رایانه‌ای، اتصال گسترده به اینترنت و سهولت ایجاد یا بدست آوردن نرم‌افزارهای مخرب به این معناست که تقریباً هر کسی 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).

دوم. هزینه کم ورود، صرف زمان کم و سرعت بالای اقدام: یک فرد برای انجام حمله سایبری تنها به یک رایانه، یک ارتباط اینترنتی و دانش فنی محدود در زمینه فضای سایبری نیاز دارد. در نتیجه، فضای سایبری شرایطی را فراهم کرده است که با هزینه پایین می‌توان اقدامات خطرناکی را در مدت زمان کم و با سرعت بالایی انجام داد (Lord and Sharp, 2011: 20-28).

سوم. ناشناس ماندن بازیگران و عدم قابلیت ردیابی: اینترنت به عنوان یک سیستم نامتمرکز طراحی شده و کاربران آن غالبا شناخته شده نیستند. همین ناشناختگی باعث می‌شود هیچ اثری از برخی از حمله‌های سایبری باقی نماند. افراد فعال در عرصه اینترنت می‌توانند از اقصی نقاط دنیا، بدون هشدار و در عرض چند ثانیه و بدون آنکه اثر و یا نامی از خود بر جای بگذارند، اهداف دیجیتالی را مورد هدف قرار دهند (Lord and Sharp, 2011: 20-28).

قدرت نرم به دلیل ماهیت خود و عدم نیاز به ابزارهای فیزیکی به دنبال آن است که در مسافت‌های دورتری از مراکز طراحی کننده به اجرا درآید. جهانی و فرامرزی بودن فضای سایبر امکانات مورد نیاز را به آسانی در اختیار طراحان قدرت نرم قرار می‌دهد و با فراهم شدن بسترهای فکری – فرهنگی اهداف مدنظر، از سوی جریان‌های درون جامعه هدف دنبال می‌شود. فضای سایبر و جنگ سایبری از زیر مجموعه‌های جنگ نرم است. امروزه با پیچیده‌تر و کوچک‌تر شدن جهان به واسطه رشد فزاینده وسایل ارتباط جمعی از قبیل اینترنت و ماهواره معادلات گذشته در تنظیم روابط بین کشورها تا حدود زیادی به هم خورده و جای خود را به معادلات جدیدی داده است؛ به گونه‌ای که به جای به کارگیری مستقیم زور، توجه قدرت‌ها به استفاده از قدرت نرم و ایجاد تغییرات از طریق مسالمت‌آمیز با به کارگیری شیوه‌های نوین مداخله در امور داخلی کشورها جلب شده است. جنگ نرم در برابر جنگ سخت در حقیقت شامل هرگونه اقدام روانی و تبلیغات رسانه‌ای که جامعه هدف یا گروه هدف را نشانه می‌گیرد و بدون درگیری نظامی و گشوده شدن آتش، رقیب را به انفعال یا شکست وامی‌دارد (ماه پیشانیان، ۱۳۹۰:۶).

با توجه به این موارد برای بررسی این موضوع از تئوری قدرت نرم جوزف نای که فضای سایبری را نیز تحت پوشش قرار می‌دهد استفاده می‌کنیم.

۲. فضای سایبر در چین

۲-۱. اقدامات امنیتی

در گزارش کمیسیون بازنگری امنیتی- اقتصادی، الگوهای عمل چین در اقدامات امنیتی- سایبری پیرامون سه محور تدافع، تهاجم وکنترل ابزارهای جبهه متقابل مورد بررسی قرار گرفته است. در این پیوند تلاش متخصصان چینی در زمینه کاهش زمان کشف اطلاعات و به کارگیری آن در رویارویی‌های امنیتی و حتی رقابت‌های تجاری و اقتصادی از سوی ناظران به عنوان عاملی برای تشدید نگرانی‌های واشنگتن در

افزایش تهدیدات سایبری تلقی شده است. اما این احتمال وجود دارد که کشور چین با بهره‌برداری از آسیب‌پذیری‌های غرب در حوزه سایبری هم به جمع‌آوری علوم ارزشمند با کمترین ریسک بپردازد و هم ضعف-های حوزه نظامی و سیستم‌های زیربنایی مهم را شناسایی کند. البته این یک جاده یک طرفه نیست. پکن هم نگران آسیب پذیری کشور خود در حوزه اینترنت است (Lnkster, 2010: 56)، چرا که چین آماج وسیعترین حملات اینترنتی در سطح جهان است. سازمان‌های اطلاعاتی و جاسوسی و ایدئولوژیک گسترده‌ای در راستای تهدید نرم افزاری چین تلاش می‌کنند و میلیاردها دلار بودجه علنی و سری صرف این مبارزه می‌شود (معین پور،۱۳۸۹: ۸۵-۵۷).

یکی از رهبران ارتش چین در پاسخ به سؤال یک مقام آمریکایی که چرا کشور شما حملات سایبری متعددی علیه شبکه‌های ایالات متحده انجام می‌دهد؟ گفت: آیا میدانید ما هر روزه چندین بار مورد حمله سایبری از سوی ایالات متحده قرار می-گیریم؟ (Lord and Sharp, 2011: 29). گزارشی از سوی مک آفی حاکی از این است که چین در رأس جنگ سایبر قرار دارد، به‌طوری که متهم به انجام حملات سایبر ضد سیستم‌های کامپیوتری هندوستان، آلمان و ایالات متحده شده است؛ اما خود این کشور با تکذیب چنین مطلبی ادعا می‌کند که از دانش لازم برای انجام این حملات برخوردار نبوده و از آنجایی که دارای بیشترین کامپیوترها در جهان است، توان کنترل همگی آن‌ها را ندارد (عبداله خانی،۱۳۸۹:۱۳۷).

۲-۲. جنگ سایبری

چین در حال توسعه قابلیت جنگ سایبری است. نبرد سایبری با تأسیس الگوهای نامتقارن و انتقال تکنولوژی چینی تطبیق دارد. برای دریافت اینکه چرا پکن جنگ سایبری را به‌عنوان وسیله‌ای برای جلو افتادن دنبال می‌کند ضروری است که به توانایی‌های هک کردن آن اشاره شود. هکرها از محدوده وسیعی از ابزار با تکنیک‌های فوق پیشرفته استفاده می‌کنند، هک قادر است باعث آسیب‌های جدی با سرمایه اندک شود. دفاع کردن در برابر آن مشکل است و مشکلات جغرافیایی فاصله را از بین می‌برد. چین می‌خواهد توانایی جنگ سایبری خود را توسعه دهد، بنابراین، بزرگترین هدف را در دفاع کردن دارد. مقامات رسمی چین مطرح کرده‌اند که آن‌ها قربانی تلفات بزرگ و تکان دهنده در از دست دادن اسرار نظامیشان و مورد حمله قرار گفتن در فضای سایبر هستند. کشورهای خارجی خواهان جنگ سایبری علیه آمریکا هستند و ممکن است تمرکز خود را بر روی چین قرار دهند و از کامپیوترهای چین برای ارتباط با حمله‌ها و شناسایی‌های سایبری

خودشان با استفاده از بات نت‌ها و پروکسی‌ها استفاده کنند. (Fritz, 2008: 48-49)

از چهار سال گذشته به‌طور فزاینده‌ای نگرانی‌ها درباره‌ی چیزی که در غرب مشاهده شده است افزایش یافته است: تصویر تهدید تهاجم سایبری چین. اطلاع از تاریخ این تهدید به اوایل سال‌های هزاره دوم برمی‌گردد. درسال ۲۰۰۳ پنتاگون شروع به ثبت یک مجموعه از حملات سایبری بر علیه دولت آمریکا کرد. در سال ۲۰۰۷-۲۰۰۶ نیز تعدادی از مقامات سیاسی اروپای غربی شامل آلمان و انگلیس میزان آسیب‌هایی که آن‌ها نیز از حملات سایبری داشتند را منتشر کردند، و با پشتیبانی سرویس‌های امنیتی انگلیس یک گام غیر معمول در نوشتن نامه به ۳۰۰ رئیس اجرایی و مشاوران امنیتی برای اعلام خطر به آن‌ها از جانب تهدید چین برداشتند. تعدادی حملات سایبری در مقیاس بزرگتر گزارش شد که از جمله آن‌ها شبکه گوست نت بود. (Lnkster, 2010: 55)

۲-۳. اینترنت

تفکرات چین و ایالات متحده آمریکا عمیقاً درباره اینکه آیا اینترنت کنترل شود، و اینکه به چه نحو این کنترل انجام شود متفاوت است. اما اختلافات بین چین و کشورهای غربی درباره مسئله کنترل محتوای اینترنت نباید راه منعی برای همکاری در زمینه امنیت سایبری بین دو طرف شود و مطمئناً نباید پایه‌هایی برای متهم کردن چین به اجازه غیر مستقیم و پنهان به فعالیت-های هکری شود. چین در سال‌های اخیر پیشرفت سریعی در فناوری اطلاعات داشته است. اما در زمینه تحقیق و رشد فناوری اطلاعات و قدرت کلی برنامه‌های مشترک، هنوز فاصله زیادی با ایالات متحده آمریکا دارد. هر چند چین در زمینه توانایی امنیت سایبری و هشدارهای امنیت سایبری میان شهروندانش پس از آمریکا قرار می‌گیرد.(Nagorski, 2010: 2)

در شانزدهمین کنگره جهانی کامپیوتر در سال ۲۰۰۰ دولت چین ابتکاری برای پیشرفت اینترنت و همچنین در خصوص اینکه باید به‌طور جدی مقابل حمله‌های سایبری و ویروس‌های شبکه‌ای، مزاحمت‌های هکری و مشکلات دیگری از این دست که برای امنیت شبکه مضرند، مطرح کرد. در نهایت این کار بصورت قانونی که معیارهای دقیقی را در پاسخ به همه‌ی صورت‌های حمله‌های هکری و فعالیت‌های سایبری در داخل چین می‌طلبید، درآمد. این قانون شامل اصلاحیه‌ای در سال ۲۰۰۸ گردید که شامل قانون جنایی و معیارهای اداری برای مراقبت امنیت ارتباطات شبکه‌ای می‌شود، که در مارس ۲۰۱۰ لازم‌الاجرا گردید.(Nagorski, 2010: 2-3)

چین تا ژوئن ۲۰۱۱ دارای ۴۸۵ میلیون کاربر اینترنت بود. پیشبینی میشود که تعداد کاربران اینترنتی چین تا سال ۲۰۱۳ به ۷۱۸ میلیون نفر رسیده و شامل۵۲.۷ درصد از کل جمعیت این کشور شود. (www.east-west-connect.com)

قدرت اینترنت، به وسیله‌ی نگرانی‌های شدیدی که مقام‌های چینی از بابت دسترسی بیش از اندازه به اینترنت از خود نشان داده‌اند، مشخص می‌شود. در حالی که دولت چین، ارزش شبکه برای توسعه‌ی اقتصادی را تشخیص می‌دهد، از زمان پیوستن به اینترنت در سال ۱۹۹۴ کوشیده است که شهروندان خود را از اخبار و مطالب مربوط به فعالان سیاسی دور نگه دارد. در سال ۱۹۹۴، حکومت پکن، با درجه‌های متفاوتی از موفقیت تلاش کرد تا از دسترسی به بسیاری از سایت‌های شبکه جهانی وب، از جمله سایت‌های نشریات خارجی، سازمان‌های حقوق بشر و دموکراسی و مطالب مربوط به گروه‌های تایوانی و امور جنسی، جلوگیری کند. در اواخر سال ۱۹۹۷ رژیم چین مقرراتی را تصویب کرد که تعریف کننده‌ی جرایم رایانه‌ای بود. کاربرد اینترنت برای افترا به دولت، فاش ساختن اسرار دولتی و کمک به استقلال جنبش‌ها از جمله‌ی این جرایم رایانه‌ای بود، با این وجود، مراقبت‌های پلیسی مانع تداوم ارتباط فعالان چینی با وب سایت‌ها نشده است. تعدادی از آن‌ها نشانی‌های خود را اغلب تغییر می‌دهند و به صورت انفرادی، از راه نشریات الکترونیکی و با کاربرد پست الکترونیکی ارتباط برقرار می‌کنند (آلبرتس و پاپ، ۱۳۸۹:۱۸۸).

ظهور اینترنت باعث تغییر ارتباط پویش‌های موجود بین رژیم پکن و گروه مخالفان شده است. برای دولت، استفاده سیاسی از اینترنت باعث تضعیف توانایی حزب کمونیست چین در کنترل جریان اطلاعاتی می‌شود که تصور می‌کند از نظر سیاسی حساس هستند یا برای چین و در محدوده خاک آن، مضر هستند. اما این حزب هنوز از روش‌های لنینیستسی برای درهم کوبیدن گروه–های مخالف سازماندهی شده استفاده می‌کند و در نتیجه هیچ سازمانی که ظرفیت مقابله با انحصار حزب کمونیست در زمینه قدرت سیاسی داشته باشد، در حال حاضر در چین وجود ندارد(Mulvenon, chase, 2002: 3).

۲-۴. اطلاعات

چین قدرت اطلاعاتی است و به این دلیل باید قدرت اطلاعاتی پاسخگویی باشد. فضای عمومی اطلاعات آینده، چینش اطلاعات و الگوبندی قاعده‌ها بدون همکاری چین نمی‌تواند شکل گیرد. همزمان چین متوجه شده است که امنیت سایبری، حمله‌های هکری و جنایت‌های سایبری به مشکل عمومی در جهان تبدیل شده است. بنابراین تنها

همکاری بین‌المللی است که آن‌ها را قادر می‌سازد که از جنایت‌های سایبری جلوگیری و از رشد سالم فضای سایبری و اینترنت مطمئن شوند. چین اعتقاد دارد که کشورها در این زمینه می‌بایست با سایرین همکاری نمایند. همه‌ی ملت‌ها باید نظراتشان را اعلام کنند، اما همه آنان باید مسئولیت‌هایشان را نیز بدانند. آن‌ها اعتقاد دارند از طریق ارتباطات و مبادلات صادقانه، جامعه بین‌المللی قادر خواهد بود با شیوه‌های مؤثر برای برخورد با تهدیدات سایبری همراه شود. چین همیشه از استفاده امن و صلح‌آمیز از فضای جهانی اطلاعات حمایت کرده است، با این پیش فرض که حاکمیت ملی و امنیت حوزه اطلاعاتش نیز حفظ گردد. (Nagorski, 2010: 2)

چین سال‌های زیادی جهت ساخت مکانیزم‌های مؤثر برای همکاری با بسیاری از کشورها در رابطه با امنیت سایبری کار کرده است، علاوه بر سازمان همکاری شانگهای، گروه کاری خاصی که در رابطه با اطلاعات و فناوری‌های ارتباطات کار می‌کنند، همچنین میزگرد اینترنتی بریتانیا- چین، تبادل نظر و گردهمایی‌های اینترنتی آمریکا- چین، کمیته گروهی تکنولوژی ارتباطات و اطلاعات چین- فرانسه، ارتباطات و اطلاعات وزارتخانه‌ای چین-ژاپن- کره، گروه کاری همکاری صنعتی اطلاعات چین- پاکستان، تجربه‌های موفق چین در رابطه با این مکانیسم‌ها باید به تلاش‌های آینده همکاری امنیت اطلاعات بین المللی تحت چارچوب کاری سازمان ملل متحد بپیوندد. همه‌ی این سازماندهی‌های همیارانه، تمایل صادقانه چین برای حرکت به سمت همکاری بین‌المللی برای امنیت سایبری را نشان می‌دهد.(Nagorski, 2010 :3)

در مجموع رژیم جمهوری خلق چین در راهبردهای مقابله‌ای خود از راه حل‌های فنی پیشرفته از جمله مسدود کردن سایت‌های اینترنت، نظارت و فیلتر کردن پیام‌های پست الکترونیکی، فریب و ارائه اطلاعات غلط و حتی حمله به سایت‌های اینترنتی مخالفان استفاده کرده است. مدارک به‌دست آمده حاکی از این است که اقدامات تلافی جویانه و فنی پکن به‌طرز فزاینده‌ای پیچیدگی خاصی پیدا می‌کنند. علاوه بر آن بعضی از گروه‌های غیر دولتی بر ضد سایت‌های مخالفان حملات برق‌آسایی را راه-اندازی کرده‌اند. اما رویکرد پکن اصولاً از نوع لنینیستی سطح پایین است که از طریق آن، اقداماتی به شیوه‌های سنتی از قبیل گشت زنی، استفاده از خبرچین‌ها، جستجو و بازرسی، مصادره تجهیزات کامپیوتری و قطع فیزیکی اجزایی که در زیر ساخت اطلاعات وجود دارند، صورت می‌گیرد. این استراتژی دولت با محیط اقتصادی کنونی در چین، تقویت می‌شود؛ محیطی که تجاری شدن اینترنت را تشویق می‌کند و نه سیاسی شدن آن را. همان طور

که یکی از دست‌اندرکاران اینترنت می‌گوید برای شرکت‌های چینی و خارجی نکته مهم در سودآوری نهفته است و نه در اظهارنظرهای سیاسی (Mulvenon, chase, 2002:4)

۳. راهبرد جنگ اطلاعاتی چین

کشور چین از جمله کشورهای پیشرو در حوزه جنگ اطلاعات است به گونهای که در حال حاضر آمریکا، چین را تهدید بالفعل و بالقوهای برای خود در این حوزه محسوب میکند. توسعه ناگهانی اقتصادی چین در سه دهه اخیر، امکان مدرنیزه کردن قابلیتهای نظامی پیشرفته نظیر زرادخانه هستهای، تجهیزات فضایی و سلاح‌های هوشمند و راهبردی را برای آن کشور فراهم نموده است. علاوه بر این، استراتژیستهای چینی در حال بررسی نوعی جنگ جدید هستند که نقطه اتکا آن کسب اطلاعات و انتشار آن، حمله به اطلاعات دشمن و پدافند اطلاعاتی در مقابل دشمن و به عبارتی کسب برتری و تفوق اطلاعاتی در میادین آتی جنگ بوده، جنگی که در آن شاید یک تراشه الکترونیکی مجتمع در یک کامپیوتر بسیار مفید تر و مؤثرتر از یک تن اورانیم باشد(امیرصوفی، آل شیخ،۱۳۸۳:۱۳۵-۱۳۰). واقعیت آن است که عملیات روانی ـ اطلاعاتی، امروزه به مثابه‌ی یکی از ابزارهای مؤثر پیروزی در جنگ، جایگاه ویژهای در سیاست‌های دفاعی ـ نظامی دولت‌ها، یافته است و مبحث عملیات روانی، از مهمترین موضوعات تعیین کننده در جنگ‌های دوران پسا جنگ سرد است. در این میان، دولت چین به منزله‌ی بازیگری فعال و تعیین-کننده در فضای نظام دو قطبی گذشته، دوران گذار و عرصه‌ی تعاملات بینالمللی کنونی، نگرش راهبردی ویژه ای به این مقوله برای سطح تأثیرگذاری مؤثر خود داشته است (امینی،۱۳۸۳:۲۴۱).

۳-۱. چشم اندازهای دکترین جنگ اطلاعاتی چین

دولت چین با توجه به زمینه‌های فکری حاصل از اندیشه‌های سون تزو، استراتژیست مشهور چینی که بر مقوله‌های ادراکی روانشناختی جنگ و لزوم منفعل کردن دشمنان چین تأکید بسزا دارد و نیز پاره‌ای از ابتکارات و نوآوری‌های راهبردی امنیتی که منبعث از مقوله انقلاب در امور نظامی و فن‌آوری‌های اطلاعاتی راهبردی است، مبحث مهمی را درخصوص جنگ اطلاعاتی نرم افزاری با عنوان دکترین جنگ اطلاعاتی چین گشوده است (امینی،۱۳۸۳:۱۳۵) در دکترین جنگ اطلاعاتی چین تأکید میشود که در جنگ‌های آتی، به جای استفاده از سلاح، از ابزار اطلاعات استفاده و حملات با ویروس‌های رایانهای، بمب‌های هوشمند و عوامل نفوذی روانشناختی، طرحریزی خواهد شد که

البته در این مقوله، آسیب پذیری‌های اطلاعاتی نیز، جایگاه خاص خود را خواهد داشت(Jincheng,1996:6).

امروزه جنگ اطلاعاتی و حملات شبکه‌ای، امنیت ملی کشورها را به چالش جدی می‌کشند و به نظر می‌رسد که دولتمردان چینی با شناسایی دقیق فرصت‌های امنیتی ناشی از روند جهانی شدن، آسیب‌پذیری‌های خود را به دقت مدنظر قرار داده‌اند و امکانی برای خود فراهم آورده‌اند که بتوانند همگرا و هماهنگ با عصر اینترنت بسرعت در مقابل بحران‌های سیال از خود واکنش مناسب نشان دهند. آنچه دست‌اندرکاران امنیتی راهبردی چین به خوبی دریافته‌اند آن است که در روند فشرده و پیچیده تصمیم‌گیری‌ها به همان اندازه که برتری کلاسیک نظامی مؤثر و مهم است، برتری اطلاعاتی نیز قابل مطالعه و تأثیرگذار است(Farris, 38: 2001).

۳-۲. فعالیت‌های سایبری- نظامی ارتش چین

فعالیت‌های چین در فضای سایبری نه تنها بر جمع‌آوری اطلاعات حساس متمرکز است، بلکه توسعه توانمندی‌های ارتش آزادی بخش خلق نیز از دیگر اهداف این دولت است. ایجاد خسارتهای اقتصادی، تخریب زیرساخت‌های حمایتی و تأثیرگذاری بر نتیجه منازعات مسلحانه متعارف از مهمترین اهداف این دولت در فضای سایبری محسوب می‌شود. طبق گزارش‌های پنتاگون، ارتش چین در حال آماده شدن برای انجام حملات سایبری بر ضد شبکه‌های نظامی و غیرنظامی بهخصوص بر ضد بخش‌های لجستیک و ارتباطاتی است. استراتژیستهای دفاعی چین در منازعه آتی با یک قدرت بزرگ- به عنوان نمونه ایالات متحده بر سر موضوع تایوان- توسل به حملات سایبری را به عنوان یک گزینه جذاب مورد توجه قرار خواهند داد. این توانمندی‌ها می‌-تواند موجب نگرانی شود، اما سیاستگذاران آمریکایی نیز باید این شرایط را درک کنند (Lord and Sharp, 2011: 29).

گزارش کمیسیون بازنگری امنیتی و اقتصادی آمریکا- چین که به سفارش کنگره آمریکا تهیه و تنظیم شده، افزایش توان چین در جنگ سایبری را بزرگترین تهدید پیش روی امنیت آمریکا در این حوزه قلمداد کرده است. در این گزارش که توسط مرکز تحقیقاتی«نورثراپ گرومن» تهیه شده، با اشاره به نظریه نظامی- سایبری نیروهای مسلح چین مبنی بر ارتباط مستقیم موفقیت نظامی-امنیتی با مؤلفه میزان کنترل و دسترسی به اطلاعات، ادعا شده است که ارتش چین بر مقابله اطلاعاتی و سایبری در فضای اینترنت تمرکز ویژه‌ای داشته و در مجموع چینی‌ها توانسته‌اند در زمینه تولید سخت افزارهای

رایانه‌ای و تجهیزات مخابراتی به پیشرفت‌های خیره کننده‌ای دست یابند(Lnkster, 2010: 55-56).

ارتش چین در سال ۲۰۱۱ یک تیم جدید با عنوان « تیم آبی سایبری » تشکیل داد تا توانایی‌های این کشور را برای شناسایی و دفاع در برابر تهاجمات سایبری بهبود بخشد. این برنامه در منطقه نظامی گوانگژو و در پی درخواست ارتش چین برای افزایش آموزش‌ها در حوزه سایبری تشکیل شد. بنا بر گزارش‌ها، این منطقه نظامی ده‌ها میلیون یوان در این برنامه که به عنوان پلت فرمی برای آموزش‌های جنگ سایبری بکار خواهد رفت، سرمایه‌گذاری میکند. در ماه آوریل ۲۰۱۱ ارتش چین اعلام نمود که بر اساس برنامه‌های پیش رو تا سال ۲۰۲۰نیروهای بسیار مجرب و کارآمد را آموزش داده و بکار خواهد گرفت تا تسلیحات مدرن، جنگهای سایبری و نیز وظایف امنیتی نامتعارف را مدیریت نمایند البته چین تنها کشوری نیست که سرمایه‌گذاری ویژهای در حوزه توانمندی‌های دفاع سایبری انجام می‌دهد (www.defence. pk).

۳-۳. دکترین چین در جنگ سایبری

چین از سال ۱۹۹۹ در تلاش است تا کمبودهای تکنولوژیکی و نظامی خود را در برابر آمریکا جبران نماید. این کشور علاوه بر حوزه سخت‌افزاری و جنگ‌افزار جنبشی و با توجه به آسیب پذیری‌هایی که در حوزه سایبری دارد سعی نموده است تا توان دفاع سایبری خود را طی دو دهه گذشته افزایش دهد.

سطح تلاش‌ها و نوع فعالیت‌های چین نشان می‌دهند که این کشور خود را آماده می‌سازد تا جنگ بعدی را با استفاده از حوزه الکترومغناطیس و نیز نقشه‌هایی برای انکار دسترسی دشمن انجام دهد. آن‌ها می‌دانند که غرب تا چه اندازه به زیرساختهای فناوری اطلاعات وابسته است و به همین دلیل به نقطه ثقل آن‌ها حمله خواهد نمود. آن‌ها هم اکنون در حال شناسایی هستند و در آینده از این اطلاعات در جهت برتری خود استفاده خواهند نمود. چینیها از زیرساختهای لازم برای انجام حملات انکار سرویس برخوردار هستند و در صورت لزوم میتوانند یکپارچگی سیستمهای دشمن را مورد هدف قرار دهند تا آن‌ها نتوانند به سیستمهای کنترل و فرماندهی خود اعتماد نمایند. اگرچه چین تنها کشور فعال در این حوزه نیست اما طلایه دار این حوزه محسوب میشود. (Mashreghnews.ir)

نتیجه گیری

اگر چه چین در خلال سال‌های گذشته از رشد اقتصادی بسیار خوبی برخوردار بوده است، اما با مسائل سیاسی عمده‌ای نیز مواجه است. جمهوری خلق چین همراه با رشد و گسترش پرشتاب اقتصادی و نظامی‌اش، برای بهبود جایگاه خود از سطح یک قدرت منطقه‌ای اثرگذار در شرق آسیا به یک قدرت جهانی از یک دهه پیش به گونه‌ای جدی بهره گیری از اهرم‌های قدرت نرم و استفاده از فضای سایبر را در رویکردهای دفاعی- تهاجمی در دستورکار خود قرار داده است در همین راستا دولت چین قوانین سرسختی مانند استفاده از خبرچینان و کنترل، بازداشت مخالفان اینترنتی، برانداختن فیزیکی منابع شبکه‌ای و مسدود کردن برخی از سایت‌ها برای کنترل جریان دگراندیشان در کشور خود لحاظ کرده است. در خارج از کشور و جامعه‌ی جهانی این کشور در صدد توسعه توانمندی‌های پیشرفته خود در فضای سایبری است. تحرکات اخیر علیه آمریکا و دیگر کشورها از سوی چین بیانگر این است که تهاجم و دفاع در عرصه سایبری در سال‌های پیش رو چه اهمیتی برای این کشور دارد.

آمریکا قصد دارد تا چین را به همکاری بیشتری در رابطه با موضوعاتی مثل جرایم سایبری تشویق کند، هر چند در این زمینه چین سال‌های زیادی جهت ساخت ساز وکارهای مؤثر برای همکاری با بسیاری از کشورها در رابطه با امنیت سایبری کار کرده است، برخی نمونه‌ها شامل بنیاد همکاری امنیت اطلاعاتی چین- روسیه می‌شود که تحت چارچوب کاری سازمان همکاری‌های شانگهای بوده است، همکاری با این نهادها تمایل چین را به ارتقا بهبود امنیت سایبری در جهان نشان می‌دهد چرا که مقامات چین بارها اذعان کرده‌اند که به سبب داشتن بیشترین کاربران اینترنت و وابستگی‌شان به فضای سایبری بزرگترین قربانی حملات سایبری در جهان هستند.

در طول دهه گذشته آشکار شده است که چین نقاط حساس ملی‌ای دارد که مقامات چین در قبال آن‌ها بسیار سریع واکنش نشان می‌دهند. این نقاط حساس عبارتند از: حمایت از تایوان، به رسمیت شناختن دالایی لاما یا ابراز همدردی با تبت، متهم کردن چین به نقض حقوق بشر و یادآوری میدان تیان آن من. این موضوعات بر حاکمیت ملی و اقتدار درونی چین تأثیر فراوانی دارند. چین نسبت به این موضوعات هیچ نوع انتقادی را نمی‌پذیرد و نسبت به چنین انتقاداتی واکنش بسیار تند و شدیدی نشان می‌دهد. از آنجایی که حساسیت چین نسبت به این موضوعات در جامعه بین‌الملل وجهه چین را زیر سؤال می‌برد چین عموماً هر نوع اتهام در مورد مسائل فوق را رد می‌کند. یکی از

شیوه‌های چین برای جلوگیری از طرح موضوعات فوق، کنترل رسانه‌ها و محدود کردن دسترسی شهروندانش به اینترنت و فضای مجازی است، زیرا این رسانه‌ها معارض با منافع کشور چین‌اند. بنابراین واضح و مبرهن است که روابط سیاسی و امنیتی چین و ایالات متحده تحت تأثیر شدید فضای سایبری قرار گرفته است.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

منابع

- آلبرتس، دیوید س. و پاپ، دانیل(۱۳۸۹) ***گزیده‌ای از عصر اطلاعات: الزامات امنیت ملی در عصر اینترنت***، ترجمه علی علی آبادی و رضا نخجوانی، تهران: پژوهشکده مطالعات راهبردی.

- امیرصوفی، رحمت الله، آل شیخ، روح الله، «نقش جنگ اطلاعاتی در میادین رزم زمینی»، به نقل از پایگاه اطلاع رسانی پایداری ملی ۱۶ خرداد ۱۳۹۰ قابل دسترسی در:
http://www.225.52.75. Node/821

- امینی، آرمین (۱۳۸۳)، «دکترین جنگ اطلاعاتی چین»، ***فصلنامه عملیات روانی***، شماره۵.

- عبداله خانی، علی(۱۳۸۹)، ***جنگ نرم۳؛ نبرد در عصر اطلاعات***، تهران: انتشارات مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.

- گلشن پژوه، محمودرضا (۱۳۸۸)، ***جمهوری اسلامی و قدرت نرم***، تهران: معاونت پژوهشی دانشگاه آزاد اسلامی.

- ماه پیشانیان، مهسا (۱۳۸۹)، «ابعاد جنگ نرم چین در برابر آمریکا»، ***فصلنامه سیاست خارجی***، سال ۲۴، شماره۳.

- ماه پیشانیان، مهسا (۱۳۹۰)، «شبکه‌های اجتماعی و آسیب‌های سیاسی و روانی»، ***اطلاع رسانی وکتابداری***، ره‌آورد نور، شماره ۳۵.

- محمدی، مصطفی (۱۳۸۹)، «تأثیر فناوری اطلاعات بر جنگ»، پایان نامه کارشناسی ارشد روابط بین‌الملل، اصفهان، دانشکده‌ی حقوق و علوم سیاسی دانشگاه اصفهان.

- معین‌پور، حسین(۱۳۸۹)، «جنگهای سایبری: الگوی نوین دانش جنگاوری در هزاره سوم»، ***فصلنامه سیاسی نظامی اقتدار***، سال سوم، شماره۵-۴.

منابع انگلیسی

- Adams, James “Virtual Defense”, ***Foreign Affairs***, Vol.80, No.3, May / June 2001. pp.100-102.

- Charney, Scott,(2009) “Rethinking the Cyber Threat A Framework and Path Forward” ,***Microsoft Corp***. • One Microsoft Way • Redmond, WA 98052-6399 • USA.

- Countries with the Biggest Computers", ***CIA World Fact Book***, Cited by (http:// aneki. com omputers html) https://www.cia.gov/library/publications/the-world-factbook/...//ch.ht.

- Fritz, Jason (2008), ***How China Will Use Cyber Warfare To Leapfrog In Military Competitiveness***.

- Hai Lung and Chang Feng(1996), “Chinese Military Studies Information Warfare”, ***Kuang Chiao Ching***. January 16, in FBIS – CHI , February 21. 1996.

-http://www.east-west-connect.com.

-http://www.defence.pk/forums/chinese-defence/110879-china-creates- cyber-defense-program.html.

-/http://military.globaltimes.cn/china/2011-05/659582.html .

-http://www.east-west-connect.com.

- Inkster, Nigel (2010), Survival: ***Global Politics and Strategy China in Cyberspace***, 21 Jul 2010.

- Kate Farris, “Chinese Views of Information Warfare”, ***Defense Intelligence Journal***. Vol.10, No.1, Winter 2001.

- Lord, Kristin M. & Sharp, Travis (2011), “America’s Cyber future Security and Prosperity in the Information Age”, ***Center for a New American Security***,Volume. I.

- Lukes Steven(2007), “Power and the Battle for Hearts and Minds: On the Bluntness of Soft Power”, ***in Power in World Politics***, London & New York: Routledge.

- Mulvenon, james, Chase, Michael(2002), ***Chinese dissident use of the internet and Beijing`s counter- strategies,of chapter one***:” Political Use

Of The Internet In China" Reaserch and development http://www.rand.org/publications /mr. 2002.

- Nagorski, Andrew(2010), ***Global Cyber Deterrence, Views from China, the U.S., Russia, India, and Norway***, April.

- Wei Jincheng,(1996) "New Form of Peoples War" , ***Liberation Army Daily***, June 25.

-Whittle, David. B (1997) ***Cyberspace: The human dimension***, New York, W.H. Freeman And Company.

منابع اینترنتی

نگاهی به تجربیات سایبری چین(۱۳۹۱)، قابل دسترسی در:

http://www.mashreghnews.ir/fa/news/118870/%D9%86%DA%AF%D8%A7%D9%87%DB%8C-%D8%A8%D9%87-%D8%AA%D8%AC%D8%B1%D8%A8%DB%8C%D8%A7%D8%A.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی