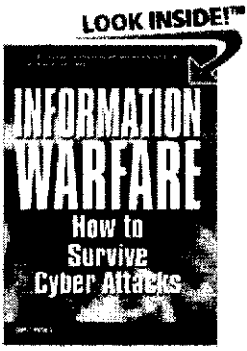

نقدی بر کتاب جنگ اطلاعات[1]

حسین عصاریان نژاد[2]

❑ اشاره:

در سال های اخیر، جنگ اطلاعات توجه بسیاری از مقامات دولتی، کارشناسان امنیت اطلاعات و ناظران کنجکاو را به خود جلب کرده است. این اصطلاح، طیف وسیعی از فعالیت ها را در برگرفته است اما به طور خاص، سناریویی است که در آن نفوذگران اطلاعاتی فقط با استفاده از یک صفحه کلید و موشواره، به رایانه های دیگر نفوذ می کنند و باعث سقوط هواپیماها، وقوع خاموشی های بی سابقه برق و یا مسمومیت مواد غذایی می شوند. این کتاب، هشداری بر شکل گیری این شکل از جنگ اطلاعات است؛ جنگی که در آن افراد نهادها و دولت ها از همه امکانات و ابزارهای اطلاعاتی بهره می جویند تا با کسب امتیازی، بر حریف خود برتری یابند. این مبارزه، گستره وسیعی از فعالیت ها، از جمله نفوذ و خراب کاری رایانه ای، عملیات جاسوسی و اطلاعاتی، شنود مخابراتی، مدیریت هوشمند و جنگ الکترونیکی را دربر گرفته وتأکید فراوانی برنحوه استفاده دولت هایی داردکه با نیروهای امنیتی خود از جنگ اطلاعات برای مبارزه با دشمنان پنهان خود بهره برده و یا نیروهایی مسلح خودراهمراه با جنگ اطلاعات به میدان نبرد می برند. ازاین رو می توان اذعان داشت که کتاب جنگ اطلاعات در این زمینه به رشته تحریردرآمده ونگاه جامعی به نقش اطلاعات وتعارضات آن به هنگام رقابت ومنازعه دارد ولیکن به منظور جلب توجه مخاطبان ماهنامه، به ضعف ها ونقاط برجسته آن، مورد نقدوتحلیل قرار گرفته است.

1.**Information Warfare** – Author: Michael Erbschloe – Publishing Company Limited: TATA McGRAW HILL – New Delhi – Year: 2001.

۲. استادیار و عضوهیأت علمی دانشگاه عالی دفاع ملی

□ آشنایی با کتاب

کتاب جنگ اطلاعات در محتوای گفتار و نوشتارهای خود چهار هدف را دنبال می کند. اولین هدف، ارائه یک بررسی جامع و منسجم از جنگ اطلاعات دفاعی و تهاجمی از جهت عاملین، اهداف، شیوه ها، فناوری، نتایج، سیاست ها و قوانین است. به زعم و نظر نویسنده، جنگ اطلاعات می تواند هر نوع محیط اطلاعاتی، از قبیل: محیط های فیزیکی، رسانه های مکتوب و شنیداری و دیداری، مخابرات و شبکه های رایانه ای را مورد هدف و یا بهره برداری قرار دهد.

هدف دوم کتاب ارائه نظریه جنگ اطلاعات است که در قالب آن بتوان توصیفی برای کلیه این فعالیت ها که مجموعه ای متنوع از عاملان و ابزارهای جنگ است ارائه کرد و آنها را در یک چارچوب واحد یکپارچه کرد. این نظریه براساس ارزش حاکم بر تئوری بازی ها و منابع ارزشمندی چون اطلاعات و عملیات، "رویکرد برد- باخت" که آن ارزش را تحت تاثیر قرار می دهد، به تصویر کشیده شده است.

هدف سوم، جداکردن واقعیت از توهم است. کتاب قصد دارد تا تصویری درست از تهدیدات، با تاکید بر آمار و حوادث واقعی و تعمق نسبت به آنچه که ممکن است رخ دهد، ارائه کند. زیرا به زعم نویسنده هیچ گاه نباید از این موارد غفلت کرد، زیرا که پیش بینی آینده و آمادگی برای حملات محتمل، ضروری است.

هدف چهارم، توصیف فناوری های جنگ اطلاعات و محدودیت های آن، به خصوص محدودیت های فناوری دفاعی است.

در این کتاب درباره "چگونگی" انجام یک حمله یا دفاع در برابر حمله، مباحث اطلاعاتی جدّی صورت می گیرد که به واسطه بهره برداری از یک رویکرد عملی جامع و مستدل از روش ها و راهکارهای جنگ اطلاعات برای انجام قضاوت های حرفه ای در مورد تهدیدات و دفاع مستعد، می تواند مفید باشد.

هر چند به نظر می رسد این کتاب صرفاً طیف مخاطبین و متخصصین اطلاعاتی را در نظر گرفته است، اما افراد علاقه مند به یادگیری بیشتر در زمینه و راه های حفاظت از ذخایر اطلاعاتی تا سیاست گذارانی که مایلند ماهیت این تهدیدها و فناوری ها و مسائل را بهتر بفهمند و آگاهی گسترده ای در مورد همه انواع حملات و اقدامات مقابله با آن ها

برای حفاظت از سرمایه های سازمانی خود داشته باشند می توانند از داده های این کتاب بهره مند شوند.

❑ ساختار و پیکربندی کتاب

این کتاب به سه بخش اساسی تقسیم شده است. بخش اول به معرفی مفاهیم و اصول جنگ اطلاعات می پردازد که خود شامل سه فصل است. فصل اول، با نمونه هایی از جنگ اطلاعات شروع می شود. این فصل اصول جنگ اطلاعات را خلاصه می کند و به بحث درباره شیوه های جنگ اطلاعات و فناوری می پردازد. فصل دوم، با عنوان "نظریه جنگ اطلاعات"؛ به ارائه الگوی جنگ اطلاعات از زاویه چهار عنصر اصلی: منابع اطلاعات، عوامل، عملیات تهاجمی و عملیات دفاعی می پردازد و جنگ اطلاعات را با امنیت اطلاعات و تضمین اطلاعات مرتبط می سازد. فصل سوم، جنگ اطلاعات را در درون حوزه مختلف فعالیت هم چون حقوق فردی و امنیت ملی قرار می دهد و بعضی از فعالیت ها را در هرحوزه به طور اجمال بررسی می کند.

بخش دوم به بررسی عملیات و جنگ اطلاعاتی تهاجمی می پردازد و شیوه های کارکرد سازماندهی شده و نمونه های متعددی از نبرد اطلاعاتی را در هر مقوله ارائه می دهد، این بخش دارای ۷ فصل است. فصل اول آن شامل توجه بخشیدن به سایت های اینترنت، منابع آزاد و اطلاعات رقابتی است و به مسایلی همچون تجاوز به حریم شخصی افراد و یا سرقت هایی می پردازد که حقوق مربوط به چاپ، ضبط یا نشر آثار و حقوق مربوط به نام تجاری کالا را نقض می کند. در فصل دوم، با عملیاتی که رسانه های خبر رسانی، به خصوص رسانه های پخشی و اینترنت را برای تحت تاثیر قرار دادن افکار و اعمال مردم مورد بهره برداری قرار می دهند آشنا می شویم. در فصل سوم، در مورد عملیاتی که علیه منابع یک سازمان از طریق عوامل درونی یا کسانی که به منابع داخلی دسترسی دارند، انجام می شود بحث شده و شامل خیانت کاران و عوامل نفوذی، روابط تجاری، بازدیدها و درخواست ها، فریب افراد درونی، اختلاس، خراب کاری و سرقت های فیزیکی می شود. فصل چهارم، در مورد عملیاتی است که باعث قطع ارتباطات شده و با استفاده از حسگرها به جمع آوری اطلاعات از محیط فیزیکی می پردازد. تقلب های مربوط به ارتباطات راه دور و حملات فیزیکی و الکترونیکی که باعث اختلال یا از کاراندازی ارتباطات می شوند نیز مورد بررسی قرار می گیرند. فصل پنجم نفوذهای

رایانه ای و حملات از راه دور به شبکه ها را توصیف می کند که هکرها چگونه به اطلاعات دسترسی پیدا می کنند و وقتی دسترسی پیدا کردند چه کار می کنند. فصل ششم، در مورد فریب کارانی است که در پس ظاهر معمولی خود به بررسی، سرقت هویت، جعل و ساخت اسب های تروا می پردازند و سرانجام، در پایان این بخش با عنوان "آفت های رایانه ای"، به ویروس ها و کرم های رایانه ای می پردازد.

در بخش سوم این کتاب با جنگ های اطلاعاتی دفاعی آشنا می شویم و نویسنده نقاط ضعف و قوت برخی روش های خاص را بررسی می کند. این قسمت خود دارای پنج فصل است. که در فصل نخست آن در مورد شیوه هایی که اسرار را پنهان نگه می دارند از قبیل رمز نگاری و پنهان کاری[3] آگاهی پیدا می کنیم وفصل دوم آن، در مورد شیوه های تعیین ارزشمند بودن و صحت اطلاعات است که شامل بررسی زیست سنجی[4]، کلمه عبور، بررسی صحت، امضاهای عددی، نقش های زمینه در اسناد کاغذی[5] و نشان ها و کارت ها اطلاعاتی می شود. فصل سوم، در مورد کنترل گرهایی است که دسترسی به منابع اطلاعاتی را آسان می کنند و اطلاعات لازم را از صافی می گذرانند و نفوذ به سیستم های اطلاعات و یا سوء استفاده از منابع را فراهم و شناسایی می کنند. در فصل چهارم، با کارهایی که سازمان ها می توانند برای مقابله با خطرات انجام دهند آشنا می شویم. این فصل درباره درجه آسیب پذیری، ارزیابی و کنترل ساخت و راه اندازی سیستم های امن، مدیریت خطر و مدیریت حادثه بحث می کند و سرانجام فصل پایانی این بخش کتاب درباره نقش دولت درجنگ اطلاعات دفاعی است که سه حوزه را مورد بررسی قرار می دهد: اصول امنیت سیستم مورد قبول عموم، حفاظت از زیرساخت های حیاتی و سیاست رمزگذاری کردن.

در تمامی این فصول، کتاب به توصیف حوادث، نهادها و محصولات متعدد سازمان ها در نبرد اطلاعاتی می پردازد.

---

3. Steganography
4. Biometry
5. Watermarking

□ تحلیل شکلی کتاب

مفهوم جنگ اطلاعات هر چند که تازگی ندارد و لیکن به کمک رسانه ها و فناوری اطلاعات جدید متحول شده است. در آغاز قرن بیستم، یک متخصص اطلاعات، حتی تصور نمی کرد که بتواند به اطلاعات یک سیستم رایانه ای نفوذ کند تا بتواند اسرار آن را به سرقت ببرد، ویروس های مخرب رایانه ای را به شبکه آن وارد کند، مکالمات تلفن همراه مردم را مختل کند، به کمک ماهواره های جاسوسی به جمع آوری تصاویر دست بزند و یا اطلاعات غلط و تبلیغات سو را از ایستگاه های رادیو تلویزیونی پخش کند. درحالی که نویسنده کتاب به این ساخت اساسی در گنجانیدن این محور درکتاب دقت کافی کرده است.

ما اکنون در حالی قرن جدید را طی می کنیم که اطلاعات و ابزارهای آن در همه جا گسترش یافته اند. آن ها ارزان، اغلب کوچک، معمولاً به هم متصل اند و در همه چیز از اجاق مایکروبو گرفته تا موشک های هدایت شونده وجود دارند. و رایانه ها در تمامی فرآیندها از جمله امور دولت و عملیات نظامی نفوذ کرده اند.

با پیشرفت دائم اینترنت برای ارائه فرصت های بیشتر به دولت ها و افراد، احتمال جنگ اطلاعات نیز افزایش می یابد. مدیران و رهبران کشورها به طور روزافزونی از عواقب بالقوه یک حمله به مجموعه خود بیمناک می شوند. ممکن است کسی به اسرار آنان دسترسی یابد و یا در کارشان اختلال ایجاد کند.

نکته اساسی در قالب بندی کتاب، مغفول ماندن توجه به زیر ساختار اطلاعات در درک جنگ اطلاعاتی است که بسیار حائز اهمیت است و به منابع اطلاعات از قبیل سیستم های ارتباطی و حفاظتی اشاره دارد. نمونه های آن زیر ساختارهای اطلاعات جمعی، زیرساختار اطلاعات مالی، زیر ساختار اطلاعات دفاعی[6] زیرساختار اطلاعات ملی[7] و زیرساختار اطلاعات جهانی[8] است.

« فضای اطلاعات» به مجموعه ای از تمامی منابع اطلاعات در اختیار یک مجموعه اطلاق می شود. یک فضای اطلاعاتی شامل کارمندان، مدارک و اسناد، سیستم های ارتباطی و رایانه ای آن به علاوه تمامی اطلاعات ساختاری گنجانده شده در محیط

---

6 . Defense Information Infrastructure (DII)
7 . National Information Infrastructure (NII)
8 . Global Information Infrastructure (GII)

فیزیکی نهاد و سازمان داخلی اش می شود. «فضای رایانه ای» فضای اطلاعاتی است که شامل تمامی شبکه های رایانه ای می شود.

نویسنده کتاب در ساختار شکلی کتاب باید توجه می نمود که اساسی ترین فضای اطلاعات مورد نظر در زمان جنگ، فضای میدان جنگ است، که شامل همه چیز در محیط فیزیکی از جمله سیگنال های مخابراتی موجود در هوا می شود. هر طرف سعی می کند دانش خود را درباره فضای میدان به حداکثر برساند، در حالی که دسترسی طرف دیگر را به آن تا حد ممکن از بین ببرد؛ و ممکن است کوشش کند که در سرزمین دشمن اطلاعات غلط رواج دهد و در منابع اطلاعات مورد استفاده او به خرابکاری اقدام نماید، درحالی که این نکته،کتاب را دربخش نظامی به شدت تضعیف کرده است.

نکته مغفول دیگر کتاب بازیگران جنگ اطلاعاتی است، این یعنی اینکه در هر عملیات جنگ اطلاعات دو بازیگر اصلی وجود دارند: بازیگر تهاجمی که به عملیات علیه منبع اطلاعات خاصی دست می زند و یک بازیگر دفاعی که هدفش دفاع در مقابل عملیات است. هر چند که بازیگر تهاجمی اغلب عضوی مهاجم و بد است، بازیگران هر دو طرف می توانند افرادی باشند که یا به تنهایی و یا در گروه های منسجم و یا جسورانه عمل می کنند. آن ها می توانند دولتی و یا غیر دولتی که از آن ها پشتیبانی مالی به عمل بیاید و یا نیاید، باشند.

نادیده گرفتن نقش دولت ها درپیکربندی کتاب نیز مهم است، زیرا برای ورود به جنگ اطلاعات، یک دولت باید دارای انگیزه، ابزار و فرصت باشد. انگیزه یعنی عملکرد علائق و تعهدات دولت. ابزار را، توانایی ها و میزان دسترسی تعیین می کند. فرصت نیز حاصل دسترسی است، اما عوامل دیگری را نیز دربرمی گیرد، نظیر درک این مسأله که آیا عملیات موفق خواهد بود و یا این که آیا دولت ها گرفتار خواهند شد یا خیر؟

گروه دوم از دسته نادیده گرفتگان درکتاب جنگ اطلاعات، سازمان های امنیتی هستند که برخی از آن ها درگیر جنگ اطلاعات تهاجمی هستند. ادارات پلیس ارتباطات، پرونده ها، ساختارهای سازمانی جنایت کاران را برای جمع آوری شواهد و اخبار محرمانه در تحقیقات جنایی مورد هدف قرار می دهند. آژانس های اطلاعاتی به دنبال اسرار نظامی، سیاسی، اقتصادی دولت ها، نهادها و دشمنان خارجی هستند. آن ها

به شدت از عوامل نفوذی داخلی و نظارت الکترونیکی برای کسب اطلاعات کمک می گیرند. واحدهای نظامی، سیستم های کنترل و فرماندهی اطلاعات دشمن را در هنگام جنگ نابود می کنند. قانون گذاران دولتی، آزادی بیان را سانسور می کنند و دسترسی به فناوری اطلاعات را به منظور امنیت عمومی و ملی محدود می سازند.

گروه سوم، تروریست ها هستند. تروریست ها از آن جهت مورد توجه خاص اند که حمله به زیرساختارهای حیاتی نظیر سیستم های اداری و خدمات اضطراری می تواند خسارت های قابل توجهی به وجود آورد. تروریست ها به جمع آوری اطلاعات در مورد هدفشان دست می زنند، تبلیغات راه می اندازند و به خرابکاری در ساختمان ها و تجهیزات فیزیکی اقدام می کنند. تا به حال، برخی گزارش هایی درباره حملات رایانه ای توسط تروریست ها به دست آمده است.

□ تحلیل روشی کتاب

نگارش این کتاب چندین چالش را پیش روی خواننده قرار داده است. اولین آن، تصمیم گیری درباره این مسأله است که چه چیزی در حوزه جنگ اطلاعات می گنجد. در حالی که همه می پذیرند که نفوذ به رایانه های هر نظام سیاسی و یا یک کشور نوعی اعلان جنگ اطلاعات است، حداقل در شرایط خاص دیگری، همه ممکن است قبول نکنند که بسیاری از موضوعات مورد بررسی این کتاب جنگ اطلاعات محسوب می شوند و منصفانه است که جنگ اطلاعات را بیشتر به تهدیدات در سطح ملی و به فعالیت هایی نظیر تقلب و سرقت مربوط کنیم. چالش دوم، که بخشی از آن به خاطر تصمیم برای گنجاندن این همه موضوع است، مربوط به چگونگی سازمان دهی کردن مطالب می شد. کتاب بیشتر به سلسله مقالاتی می ماند که ناشی از یک پیش نویس در کلاس درس است، هر چند که نویسنده از چارچوب فعلی کتاب راضی است. ولی مشخص است که آن را از متون کلاسی خود در مقطع کارشناسی دانشگاه جورج تاون جمع آوری کرده است.

چالش سوم، که از مسأله اول برجسته تر است، بحث نفوذگرهای رایانه ای است که تنها تهدید برای منابع اطلاعات نیستند، همان طور که رمزنگاری تنها راه حل جادویی نیست. نتیجه گنجاندن چنین زمینه های متنوعی در کتاب آن است که کتاب یکنواخت نیست و بعضی از موضوعات عمیق تر از بقیه بررسی شده اند. تعداد جملات مربوط به

یک موضوع لزوماً در ارتباط با اهمیت کلی آن موضوع نیست و بالاخره چالش اصلی ما با متن این کتاب آن است که با تحولاتی که در این زمینه روی می دهد همگام نمی شویم. تحولاتی که در زمینه فناوری های جدید، روش های جدید حمله و یا قوانین صورت می گیرد. امروزه به مراتب رشد یافته تر از آن است که در این کتاب می بینیم.

جنگ اطلاعات مسائل بحث برانگیز دیگری را نیز مطرح می سازد. از جمله این که سطح قابل قبول در خطر پذیری چیست؟

اگر یک رایانه در اینترنت برای حمله ی مخرب علیه یک سایت دیگر مورد استفاده قرار گیرد، چه کسی مسئول است؟

اگر مطالبی موهن یا ارزش و سرمایه اخلاقی مسروقه ای در یک خط آن لاین[9] در اختیار همگان قرار گیرد، چه کسی مسئول است؟

تحت چه شرایطی جنگ اطلاعات تهاجمی حتی اگر قانونی هم به حساب بیاید غیراخلاقی محسوب می شود؟

چه کسی مسئول حفاظت از زیرساخت های حیاتی است؟

چطور جرایم را می توان با موفقیت مورد بررسی و تحت تعقیب قرار داد، هنگامی که مجرم در یک کشور دیگر دور از دسترس قربانی و یا منابع اطلاعاتی مورد تهاجم، قرار گیرد. این ها و ده ها سئوال و موارد دیگردر این کتاب کمترمورد بررسی قرار گرفته، در حالی که انتظار می رود بنابر نظر نویسنده و هدف این کتاب، بالا بردن درک تهدیدات در حوزه دفاع و مسائل مربوط به آن مورد توجه باشد.

❑ تحلیل محتوائی

با توسعه فناوری های اطلاعات و ارتباطات (ICT)، موضوع جنگ اطلاعات در میان جوامع و سازمان های اطلاعاتی، امنیتی و دفاعی در سال های اخیر مورد توجه بیشتری قرار گرفته است. این موضوع عمدتاً از این واقعیت نشأت می گیرد که فناوری های اطلاعات و ارتباطات به طور اعم برای امنیت ملی و به طور اخص برای موضوعات اطلاعاتی، امنیتی، نظامی و دفاعی حایز اهمیت هستند و بر همین اساس امروزه شاهد جنگ های پیشرفته با محوریت فناوری های اطلاعات و ارتباطات هستیم. برتری سیستم های اطلاعاتی و ارتباطاتی یک نظام در دنیای کنونی، تقریباً معادل برتری و

---

9 . On- line

مزیت نسبی آن نظام در عرصه های مختلف می باشد و این حقیقت به خودی خود شیوه های سنتی مربوط به فعالیت های اطلاعاتی، امنیتی، نظامی و دفاعی را تحت الشعاع قرار داده و کم اهمیت و کم کارآمد خواهد ساخت. از این رو به نظر می رسد این کتاب در این برهه از زمان از اهمیت خاصی برخوردار بوده و برای آحاد مردم و به خصوص برای کارشناسان، محققین و مدیران مرتبط با موضوع خیلی مفید می باشد.

اما در کنار این مزیت مثبت کتاب باید به یک ناکارآمدی جدّی کتاب توجه داشت همان گونه که تمامی متخصصین اطلاعاتی به آن اذعان دارند، ارزش یک منبع اطلاعات برای یک سازمان، حاصل عملکرد شش عامل است. اول این که آیا منبع اطلاعات به مسائل و علائق سازمان مرتبط است یا نه؛ ثانیاً، توانایی های سازمان مطرح می شوند؛ که بایستی دانش، مهارت و ابزار لازم برای استفاده درست از منابع اطلاعاتی را داشته باشد. عامل سوم میزان در دسترس بودن منابع برای سازمان می باشد و عامل چهارم در دسترس بودن آن برای دیگر بازیگران اطلاعاتی است. اغلب، یک منبع اطلاعاتی بیشترین ارزش را برای یک بازیگر داراست، به خصوص زمانی که آن منبع فقط در دسترس همان بازیگر قرار دارد و نه دیگران. عامل پنجم، مسأله جامعیت منابع است که شامل کامل بودن، درستی، صحت، و کیفیت کلی یا مطلوبیت کلی است. به طور کلی، هر چه منبع جامع تر باشد، قابل اعتمادتر و در نتیجه برای یک بازیگر خاص، ارزشمندتر است؛ مگر این که بازیگری به عمد منبع اطلاعات را تخریب کرده باشد. ناقص بودن هم می تواند مورد استفاده قرار گیرد.

در یک عملیات جنگ اطلاعاتی تهاجمی یک نتیجه برد- باخت را همواره نمی توان با تغییر دادن میزان در دسترس بودن و جامعیت منابع اطلاعات به نفع تهاجم و به زیان مدافع فراهم آورد. در انجام این کارها ممکن است ملاحظات، تعهدات و توانایی های دفاع را نیز تغییر داد و اثر فوری آن تغییر و میزان در دسترس بودن یا جامعیت منابع اطلاعاتی به زودی امکان پذیر نیست و نیازمند سه اصل کلی است:

اول این که، تهاجم نیازمند دسترسی بیشتری به منابع اطلاعات است؛ یعنی، دسترسی منابع اطلاعات به تهاجم افزایش می یابد. ثانیاً، در دفاع تمامی یا بخشی از دسترسی به منابع از دست می رود؛ یعنی، منابع کمتر در دسترس نیروهای دفاع قرار می گیرند.

ولی با رویکردی دیگر که نویسنده از آن غافل بوده است می توان جنگ اطلاعات را یک عملیات برد- باخت دانست که معمولاً بدون رضایت و آگاهی دفاع کننده صورت می گیرد. حتی هنگامی که مدافع به ظاهر قبول می کند که در آن شرکت کند، کاملاً انگیزه ها و عواقب آن را برای خود درک نمی کند. زیرا در این رویکرد جنگ اطلاعات فراتر از یک عملکرد تخریبی است. بسیاری از اعمال اطلاعاتی، مثل عملیات جاسوسی مخفی، به دنبال عملیات سفید و بدون رد ازخود هستند. هدف آنها کسب اطلاعات بدون شناسایی شدن است. سانسور و دست کاری رسانه ها نیز اعمال غیرمخربی هستند که امروزه با هدف تاثیرگذاری بر عقاید و افکار صورت می گیرند. ولی بازهم جنگ اطلاعاتی هستند.

از سوئی دیگر اگر تائید کنیم که به زعم نویسنده، جنگ اطلاعات دفاعی، به دنبال حفاظت از منابع اطلاعاتی در برابر حملات است. اما ایشان از این موضوع غافل است که هدف جنگ اطلاعاتی دفاعی صرفاً حفظ ارزش منابع و یا در صورت حمله موفقیت آمیز، به دست آوردن مجدد ارزش های از دست رفته نیست، زیرا دفاع از شش حوزه کلی در موضوع اطلاعات قرار می گیرند: ممانعت، بازدارندگی، هشدار و نشانه، شناسایی، آمادگی اضطراری و عکس العمل که ممکن است عملیات و فناوری های اطلاعاتی در بیش از یک حوزه قرار گرفته و یا آن را مورد تهاجم قرار دهند. زیرا جنگ اطلاعات دفاعی در ارتباط نزدیکی با امنیت اطلاعات تعریف می شود، اما این دو مولفه یکی نیستند. امنیت اطلاعات عمدتاً مربوط به منابع خودی و حفاظت آنها در برابر خطا، حادثه و فجایع طبیعی و همچنین اعمال تخریبی عمدی است، اما جنگ اطلاعات دفاعی مربوط به منابع غیرخودی، در حوزه عمومی است؛ که ارزشی خرابکارانه هم دارد.

باید در نظر داشته باشیم که عملیات جنگ اطلاعات در حوزه تهاجمی در ابتدا با بهره برداری از نقاط آسیب پذیر در منابع اطلاعاتی است که به موفقیت می رسد. که این نقاط آسیب پذیر ممکن است در هر دو بخش سخت افزار و نرم افزار و نیز در بخش انسانی منابع خودرا آشکار سازد. آن ها را می توان در زمان ساخت، تحویل، نصب، تنظیم، استفاده، تغییر و تعمیر این دو حوزه مشاهده و معرفی کرد. هر چند بسیاری از منابع اطلاعات را به طور معقولی می توان در مقابل تمامی این آسیب ها استحکام

بخشید ولی ضمن آن باید در نظر داشت که امنیت صددرصد نه ممکن است و نه مقرون به صرفه و ماهرترین و خبره ترین دشمنان معمولاً این اصل را در عملیات های اطلاعاتی خود که بسیار پیچیده و دارای میلیون ها دستور اجرایی هستند، در نظر می گیرند. هیچ کس نمی تواند به تنهایی از همه این آسیب ها در امان بماند و مدعی شود که عاری از شکاف های امنیتی یا دریچه های مخفی برای نفوذ است. علاوه براین سیستم ها و محیط های اطلاعاتی هر روز تابع فناوریهای نرم تغییر می کنند و حتی منابع بسیار حفاظت شده و کاملاً بررسی شده هم عموماً در مقابل تهدیدات افراد و یا مشتریانی که به آن منابع دسترسی دارند آسیب پذیر هستند. لذا هدف درجنگ اطلاعاتی مدیریت خطر و ریسک است و نه اجتناب از خطر به هر طریق ممکن، که نویسنده کتاب در سرتاسر نوشته خود به آن تاکید دارد.

به تعبیر دیگر، آسیب پذیری ها به خودی خود برای منابع اطلاعاتی، تهدید به حساب نمی آیند و حتی وجود روش شناسی برای بهره گیری از این آسیب پذیری ها تهدید محسوب نمی شود، زیرا تهدید تنها زمانی به وجود می آید که عاملی با قصد، توانایی و فرصت مبادرت به حمله کند. جنگ اطلاعاتی دفاعی عمدتاً به دنبال حفاظت در مقابل این گونه تعریف از تهدید قابل قبول است، به خصوص آن هایی که احتمال وقوع داشته و بتوانند منجر به خسارت های عمده شوند.

عملیات جنگ اطلاعاتی تهاجمی، عملیاتی است که یک منبع اطلاعات خاصی را هدف و مورد بهره برداری قرار می دهد و هدفش افزایش ارزش آن برای دولت مهاجم و کاستن ارزش آن برای رویکرد دفاعی است. بنابراین، این حالت یک موقعیت «برد-باخت» را برای هر دو دولت پیش می آورد. فرض این است که دفاع با چنین تمهیدی موفق نیست. عملیات یک عمل خصمانه و یا حداقل بدون اجماع محسوب می شود. منبع اطلاعات، لازم نیست که تحت مدیریت یا مالکیت دفاع باشد، هر چند که اغلب این گونه است. همان گونه که در تحلیل قبلی به آن اشاره شد.

جنگ اطلاعات لزوماً یک بازی دارای امتیاز صفر نیست؛ یعنی، بهره به دست آمده برای تهاجم ضرورتی ندارد که با میزان خسارت دفاع برابر باشد. حتی ممکن است در یک بعد قرار نگیرد؛ منافع و مضرات یک عملیات جنگ اطلاعاتی تهاجمی علیه یک منبع خاص را می توان با سه نتیجه توضیح داد:

دسترسی بیشتر به منابع برای تهاجم، دسترسی کمتر آن برای دفاع، و افزایش جامعیت مجموعه منابع. تمامی این پیامدها بر افزایش ارزش منبع برای تهاجم و کاهش آن برای دفاع تاثیر دارند.

نویسنده کتاب در بررسی خود به این نکته توجه ننموده است که بیشتر عملیات ها در جنگ اطلاعاتی باعث ایجاد تاثیرات چندگانه ای می شوند، به خصوص عملیاتی که در طی یک دوره طولانی که شامل چندین منبع می شوند.

اولین نوع عملیات شامل جمع آوری اطلاعات محرمانه دفاعی، از طریق جاسوسی و عملیات جاسوسی است. این اطلاعات ارزش تهاجم را بالا می برد، در حالی که ارزش منابع اطلاعات را برای طرف مدافع کاهش می دهد، چرا که می تواند برای تضعیف اهداف دفاعی به کار رود.

اصطلاح «جاسوسی» معمولاً به عملیاتی اشاره دارد که غیر قانونی یا مخفی هستند، در حالی که عملیات اطلاعاتی[10] به معنای عملیاتی است که ممکن است قانونی و علنی و یا غیرقانونی و مخفی باشند. علاوه بر این، عملیات اطلاعاتی فراتر از جمع آوری اطلاعات هستند و شامل تجزیه و تحلیل نیازها، از صافی گذراندن اطلاعات و تحلیل و یکسان سازی آن پس از دستیابی بدان می شود. بدون این مراحل، ارزش کامل اطلاعات ممکن است هیچ گاه دانسته نشود.

از دیدگاه جنگ اطلاعات دفاعی، مشکل می توان دانست که یک حمله خاص در کدام حوزه قرار می گیرد. اگر به سیستم های رایانه ای نفوذ شود، آیا فردی است که دارد شیطنت می کند؟ یا یک گروه جنایی سازمان یافته است که در جستجوی شماره های کارت اعتباری است؟ یک رقیب یا دولت خارجی است که به دنبال اسرار ملی است؟ یک گروه تروریستی است که در تلاش برای از کارانداختن زیرساختارهای حیاتی کشور است؟ خوشبختانه، بسیاری از دفاع ها در مقابله با یک طیف از تهدیدات انجام می شوند، به این خاطر همیشه لازم نیست که برای محافظت از منابع اطلاعات آن ها را شناسایی کنیم.

نویسنده در فراز نگاه خود به پدیده عملیات جنگ اطلاعاتی، معتقد است که این پدیده تنها برای ارتکاب جرم نه برای مبارزه با آن صورت می گیرد، در حالی که در

[10]. Intelligence

کارکردهای فراوانی شاهد آن هستیم که نیروهای مجری قانون از نظارت های الکترونیکی و بصری از جمله، استراق سمع و میکروفن برای جمع آوری مدارک و اخبار در تحقیقات جنایی استفاده می کنند. آن ها از خبرچین برای دسترسی به اطلاعات داخلی بهره می برند و جامعیت فضای اطلاعات هدفشان را از طریق عملیات مخفی و ضربه زدن تضعیف و معیوب می کنند.

دولت ها درجات متنوعی از عملیات و جنگ اطلاعاتی را در قالب کنترل، صرف نظر از شکل ابزاری آن غیرقانونی اعلام می کنند. در بعضی کشورها دولت ها دسترسی به اینترنت و تلویزیون های ماهواره ای را منع و یا کنترل می کند. منطق ارائه شده برای این اعمال این است که سانسور برای حفاظت از منابع ملی لازم است. مسأله عمده که در ایالات متحده و جاهای دیگر بروز کرده این است که آیا برای حمایت از کودکان باید انواع خاصی از گفتار در اینترنت منع شود یا نه؟

در ارتباط با حریم فردی، مجادله بر سر نظارت دولت بر شهروندان است، به خصوص شرایطی که تحت آن یک اداره دولتی مجاز باشد مکالمات را شنود کند و یا به جستجو و توفق اسناد و رایانه ها بپردازد و این که فناوری تا چه میزانی می بایست برای ممکن ساختن دسترسی دولت ها قانونمند شود. این مسأله جنگ اطلاعات است، چرا که نتیجه این عمل تعیین کننده میزانی است که یک دولت می تواند به منابع اطلاعات یک شهروند هنگامی که این کار به نفع او نیست، مثلاً در صورت ارتکاب جرم فرد، دسترسی یابد.

حوزه دیگری که نویسنده در تحلیل کتاب خود به اصول و مبانی آن بی اعتنا مانده و سبب بروز انحراف در تحلیل و داده های خود گردیده، امنیت ملی می باشد که ضرورت های آن ایجاب می کند تا جنگ اطلاعاتی توسط دولت ها وبازیگران غیردولتی علیه دولت های دیگر صورت بگیرد. ضرورت اطلاعاتی در امنیت ملی اول مسأله حفاظت از ارتباطات در مقابل دشمنان است. بخش مراکز حساس و رمز گذاری برای حفاظت اطلاعات در مقابل جاسوسی و حفاظت از دارایی های ملی و حفاظت از اشخاص مهم در برابر دشمنان و دولت های سو استفاده گر از نکات مورد تاکید امنیت ملی است.

این تغییرات سئوالات مهمی را مطرح ساخته اند. چطور می توانیم تلاش های پیچیده حفاظتی و اطلاعاتی خود را به گونه ای متعادل سازیم که ارزش حفاظتی

رابرای منافع جامعه به حداکثر برسانیم؟ آیا می توان فناوری های امنیتی را بـه درسـتی کنترل کرد، اگر ضرورت های امنیتی کنترل نشود تهدیدات اجتماعی آن، چقدر جـدّی خواهد بود؟ آیا دسترسی نیروهای اطلاعاتی و پلیسی، به بخـشی یـا تمـامی شـواهد و اطلاعات لازم برای مقابله با جرایم سازمان داده شـده و فـضاهای سـایبرکاهش خواهـد یافت؟ نقش مقررات دولت در مقابل فشارهای بازار در هـدایت نـوآوری هـای اطلاعـاتی چیست؟ تعادل مناسب بین آزادی و نظم چیست؟ یافتن پاسخ های خوب به این پرسش ها یک چالش عمده برای این کتاب است که مورد بی توجهی قرار گرفته است.

جنگ اطلاعات به مانند یک جنگ واقعی دارای دو وجه می باشد: جنگی کـه بـرای دفاع از حریم اطلاعات است و دیگری جنگی که برای حمله بـه اطلاعـات صـورت مـی گیرد. به عنوان مثال نفوذگران اینترنتی که یکی از مباحث بسیار مهم در جنگ اطلاعات امروزین می باشند، همواره به عنوان یک عامل حمله برنده به اطلاعات حیاتی کـشورها مطرح می باشند. دسترسی به اطلاعات پروازهای داخلی و خارجی یک کشور در سطوح امنیتی بسیار بالا، استفاده از اطلاعات نظامی به منظـور ایجـاد آشـوب و هـزاران هـدف تروریستی دیگر تنها با استفاده از نفوذ و حمله به کامپیوترهای سرور کشور و یا سازمان قربانی صورت می گیرد. از این روست که کشورهای بزرگ و دارای قدرت نظامی بالا، در عصر جدید بودجه هنگفتی را برای کارشناسان اطلاعات و امنیت شبکه اختـصاص مـی دهند تا از خروج و ورود هرگونه اطلاعات ناخواسته جلوگیری کنند.

برای آن که یک سازمان و یا یک کشور در سطح نظامی بتواند در جنـگ اطلاعـاتی دوام بیاورد، می بایست با چند مضمون مهم و اساسی آشنا باشد. از جمله ایـن مفـاهیم می توان به دادن اطلاعات نادرست به دشمن، جلوگیری و بستن هرگونه استراق سمع و دزدی الکترونیکی از دستگاه مخابره اینترنتی، ایجاد جنـگ روانـی بـرای گمـراه کـردن نیروهای دشمن اشاره کرد. در این راستا می توان در جنـگ اطلاعـات ۳ هـدف را پایـه گذاری نمود:

۱- کنترل اطلاعات نظامی و با ارزش به منظور استفاده خودی و جلـوگیری از هرگونه نفوذ و دسترسی نیروهای دشمن به این اطلاعات.

۲- استفاده و به کار بردن اطلاعات برای حمله به دشمن و یا دفاع از سرورهای خود.

۳- گسترش اطلاعات به منظور قوی تر کردن نیروهای خودی. به عنوان مثال استفاده از برنامه های رایانه ای شبیه ساز قوی تر و یا نوشتن نرم افزارهای جاسوسی رایانه ای با قدرت پنهان شدن بیشتر در سرورهای دشمن!

□ سخن پایانی

در این نقد و تحلیل سعی شد تا خوانندگان گرامی با اصطلاح جدیدی آشنا شوند که شاید بارها به گوش خورده اما معنای دقیق آن را نمی دانستند. اکنون درک نموده اند که دولت هایی مثل هند، چین و امریکا نوجوانان باهوش و نفوذگر خود را به استخدام سرویس های اطلاعاتی خود درمی آورند تا همگی در یک اتاق و با استفاده از چندین رایانه پر قدرت بتوانند در عرض چند ساعت حملات متعددی را به سرورهای دولت حریف ایجاد کنند و خسارات فراوانی را وارد آورند. حال دریافته ایم که چرا در قرن ۲۱ می بایست شاهد ژنرال هایی باشیم که به جای دستور به سربازان خود برای نحوه قرار گرفتن موقعیت شان در جبهه جنگ، به سربازانشان که به واقع متخصصین شبکه هستند و در پشت رایانه نشسته اند خط مشی دهند که در چه ثانیه ای و از کدام سرور به یک سازمان و یا دولت حمله کنند و سرویس های حیاتی قربانی را از کار بیندازند.

این کتاب این امر را آشکار می سازد که سرمایه گذاری روی امنیت سایبر به معنی هزینه بالا سری اضافه نیست. سود این سرمایه گذاری به کشور باز می گردد. نظر سنجی ها مکرراً نشان داده است که:

هزینه های ناشی از یک حمله مخرب به احتمال قوی از سرمایه گذاری پیشگیرانه در برنامه امنیت اینترنتی سنگین تر هستند.

طراحی ساختار امنیتی قدرتمند در معماری سیستم های اطلاعاتی کشورها می تواند هزینه های عمومی عملیات را به واسطه امکان پذیر ساختن رویه های کاهش هزینه از قبیل دسترسی از راه دور و تعاملات با زنجیره عرضه یا مشتریان کاهش دهد. این رویه های کاهش هزینه در شبکه هایی که فاقد امنیت مناسب باشند امکان پذیر نیست.

جدای از این ضرورت ها درپایان، ذکر این نکته که ارزش راهبردی کتاب را نیز افزایش می دهد لازم است که: برای ایجاد یک شبکه اطلاعاتی امن و انعطاف پذیر، کشورها باید دو اصل راهبردی امنیت را پذیرفته و اجرا کنند.

۱- امنیت کل زیرساخت به امنیت هر یک از اجزا بستگی دارد.
۲- تهدیدات و نقاط آسیب پذیر پیشرفت می کنند و امنیت هم به تبع آن باید همگام یا سریع تر از آنها پیشرفت نماید.

تأمین امنیت در اجزای دنیای اطلاعات مجازی منجر به تامین امنیت کل مجموعه خواهد شد.

امنیت فضای مجازی به امنیت تمام اجزای آن وابستگی دارد. در دنیای سایبر مهاجمان می توانند با سرعت نور به هر مکانی برسند. هیچ گونه ایمنی جغرافیایی وجود ندارد. شبکه ها ممکن است هم در مقابل حملات از داخل شبکه و هم در مقابل حملات از خارج آن آسیب پذیر باشند. اجزای شبکه که به نظر ایمن هستند، ممکن است توسط کارکنان داخلی (خودی ها)، نرم افزارهای دانلود شده (پیاده شده)، یا شبکه های آلوده همسایه مورد تهاجم قرار بگیرند. کشیدن دیوار دور شبکه برای رسیدن به امنیت کافی نیست. به محض این که یک کامپیوتر یا جزئی از شبکه مورد تهاجم قرار گرفت، آن جزء می تواند برای سایر اجزاء مورد استفاده قرار گیرد.

به منظور مبارزه با این نقاط آسیب پذیر، سیستم ها باید طور ی طراحی شوند که امنیت زیرساخت به یک لایه یا گروه واحد و یا نقطه مرکزی وابسته نباشد؛ بلکه باید در چندین لایه شکل بگیرد، سیستم های دفاعی توزیعی (پراکنده) باشد و توانایی ترمیم سریع پس از هر مرحله را داشته باشد. برای بهبود امنیت اینترنتی، کشور باید در تمامی سطوح فعالیت در دنیای اینترنت، امنیت لازم را تأمین کند.

❑ منابع و مأخذ مورد استفاده در نقد کتاب:

۱- تافلر، آلوین/ تافلر، هیدی. (۱۳۷۴). «جنگ و پاد جنگ»، ترجمه مهدی بشارت، چاپ اول، تهران، انتشارات اطلاعات.

۲- طیب، علیرضا. (۱۳۷۹). «تکنولوژی اطلاعات»، چاپ اول، تهران، نشر سفیر.

3- Cooper, R., Jeffrey. (1994) "Another View of the Revolution in military affairs,"

4- Cordesman, H., Anthory. (1999). "The Revolution in military Affairs.

5- Davis, Norman. (1996). "An Information-Based Revolution in Military Affairs,"

6- Galdi, w., Theodor. (1995). "Revolution in Military Affairs? Competing Concepts,

7- Mazarr, J., Michel. (1994). "The Revolution in Military Affairs.

8- High Steve (Magor), Information Operation: The Command and Control Warfare (C2W), CSC, 1997.

9- Albert S. Davis, Garstka J. John, P. Fredrich, Network Centric Warfare, CCPR Publication, 1995.

10- Fogleman, Ronald, shiela widnall, and Gene H. McCall, eds, New World Vistas: Information Technology and Information Application. Washigtoon, D.C: US Air Force Scientific Advisory Board, 1995.

11- Chaiman of Joint Chief of Staff, Joint Vision 2020 Washigton, D.C. National Defense Univercity Press 1995.

۱۲- عبارت جنگ اطلاعات اولین بار در سال ۱۹۶۷ (۲۶ سال قبل) توسط فردی بنام دکتر توماس رونا به کار گرفته شد. وی به عنوان یکی از اندیشمندان حوزه جنگ های اطلاعاتی به شمار می رود. از جمله نوشتارهای معروف وی می توان به نمونه های زیر اشاره نمود:

13- Rona P. Thoma, Information Warfare: An Age- old Concept with new Insight, Defenc Intellgence Journal, spring 1996

14- Alberts, David S., The unintended Consequences of Infoemation Age Technologies, national Defense University, April 1996.

۱۵- White boarding یا Smart boarding، یعنی کلیه مطالبی که فرماندهی یا دیگر اعضای مقر فرماندهی روی تابلو الکترونیکی خود نوشته یا ترسم نمایند، توسط نمایشگر یا تابلوی الکترونیکی دیگر افراد و یگان های مجاز قابل دریافت خواهد بود.

16- Gibson William, neuromancer, Ace Science Fiction, N.Y, 1984.

17- Roger C. Molander, A.S. Riddile & Peter Wilson, Strategic Information Warfare: A New face of war, Santa Monica, Calif RAND, MR-661-OSD,1996.

۱۸- فهیمی، مهدی- اینترنت نسل دوم (مصاحبه)، روزنامه انتخاب، ص ۱۲، ۲۳ تیرماه ۱۳۸۰.

۱۹- فهیمی، مهدی-جرایم رایانه ای و راهکارهایی برای مقابله و پیشگیری از آن، روزنامه همشهری، بهمن ماه ۱۳۸۰.

۲۰- فهیمی، مهدی- جرایم رایانه ای، اولین همایش تخصصی جرایم رایانه ای، نیروی انتظامی جمهوری اسلامی ایران- معاونت آگاهی، تهران: ۲۲ دیماه ۱۳۸۰.

21- Bunker J. Robert, Information Operation and the Conduct of Land warfare, AUSA s Intitute of Land warfare, October 1998.

22- Intelligence and Electronic Werfare Operation, FM 34-1, Headquarters, Department of the Army, Washigton DC., Sep 1994.

23- Electronic Warfare: Comprehensive strategy for Supperssing Enemy Air Defenes, A report to the Congress, GAO-01- 28, January 2001.