مقدمه‌ای بر پدافند غیرعامل

درحوزه مسیریاب

فهرست

مقدمه

پیشرفت سریع علوم رایانه و فناوری‌های ارتباطی و اطلاعاتی نوین، و پیوند تنگاتنگ این علوم با همه شئونات زندگی بشر سبب وابستگی شدید کشورها و ملت ها به فناوری اطلاعات و ارتباطات جهت اداره امور جامعه شده است، بگونه ای که امروزه حتی تصور ادامه زندگی بدون بهره گیری از این دانش و فناوری محال به نظر می رسد. به تناسب افزایش ارتباطات و پیشرفت فناوری، مخاطرات پیشِ‌رو نیز افزایش یافته‌است از اینرو توجه به ارتقای ضریب امنیت، ایمنی و پایداری شبکه های رایانه‌ای و تمامی تجهیزات آن باید بیش از پیش مورد توجه قرارگیرد.

یکی از اجزای اصلی شبکه، مسیریاب [1] است. تأمین امنیت مسیریابی و مسیریاب امن، نقش بسزایی در حفظ امنیت شبکه ایفا می‌نماید.

یک مسیریاب، گره ای از شبکه است که نقطه یا گره بعدی شبکه را که بسته باید به سمت آن ارسال شود و در نهایت به مقصد برسد، مشخص می کند. هر مسیریاب حداقل به دو شبکه متصل است و براساس درک خود از وضعیت شبکه‌های مرتبط، در مورد ارسال بسته‌های اطلاعاتی تصمیم می گیرد.

از دیگر موضوعات حائز اهمیت در یک شبکه ارتباطی، پایداری آن است. با توجه به سرعت تغییرات و اهمیت دسترس پذیری در حوزه شبکه های اطلاعاتی و ارتباطی، از نکات مهم در حفظ پایداری سامانه های این حوزه، مسائل مربوط به پشتیبانی است. از آنجا که با توجه به شرایط مخاصمات بین المللی و بدلیل تحریم های وضع شده علیه ایران، پشتیبانی از مسیریاب های تولیدشده توسط شرکت های خارجی تابع قوانین تحریمی وضع شده علیه ایران است، مسئله پشتیبانی مسیریاب های خارجی مورد استفاده در زیرساخت شبکه های ملی از چالش های مطرح این حوزه است. از

[1] Router

سوی دیگر موارد دیگری همچون وجود درهای پشتی در این قبیل محصولات امنیت و پایداری زیرساخت های کشور را همواره تهدید می‌نماید.

با توجه به نکات بیان شده به نظر می‌رسد راه حل مناسب جهت حفظ پایداری شبکه داخلی و ارتقاء ضریب امنیت آن ، بومی‌سازی این محصول مطابق با ملاحظات پدافند غیر عامل، در داخل کشور است. در اینصورت علاوه بر ارتقاء دانش بومی تأمین امنیت شبکه‌های یکپارچه داخلی، امکان پشتیبانی مطلوب از این محصول نیز میسر خواهد شد. این موضوع علاوه بر کمک به توسعه اقتصادی، باعث ایجاد امکان ارائه سرویس‌های جدید ، مستقل از شرایط مخاصمات سیاسی، اقتصادی بین المللی و مبتنی بر نیازهای داخلی خواهد شد.

فصل ۱

آسیب پذیری ها و مخاطرات مسیریاب ها

بطور کلی به هرگونه نقص یا ضعف در طراحی، پیادهسازی، کارکرد یا مدیریت سامانه که میتواند برای نقض سیاستهای امنیتی آن مورد سوء استفاده قرار گیرد، آسیبپذیری گفته میشود. آسیب پذیریها بسته به زمان ایجاد، به سه گروه تقسیم میشوند:

- آسیبپذیریهای طراحی [1] : گونه ای از آسیبپذیری است که در اثر بی‌دقتی در طراحی یک سیستم (اعم از سخت افزار یا نرم افزار) ایجاد شود.
- آسیب‌پذیریهای پیاده سازی [2] : این گونه آسیبپذیریها، حاصل خطایی است که در فرایند پیادهسازی رخ می‌دهد.

[1] Design Vulnerability
[2] Implementation Vulnerability

- آسیب‌پذیریهای پیکربندی [1]: در حالتی بروز می کند که طراحی و پیاده‌سازی درست است، اما در نحوه تنظیمات سامانه توسط کاربر اشتباهی صورت می‌گیرد و رخنهای در سامانه باز می‌شود.

مهاجمین عموماً با شناسایی و استفاده از آسیبپذیریهای موجود در سامانههای هدف اقدام به حمله یا نفوذ میکنند. چهار روش اصلی حمله بر روی مسیریاب بعنوان یکی از تجهیزات اصلی زیرساخت شبکه عبارتند از :

- هک کردن DNS [2]
- تخریب و تغییر سوء در جدول مسیریابی
- عملکرد نادرست مسیریاب در قبال بستههای داده
- حملات DoS [3]

بهعنوان مثال برخی از پیامدهایی که در اثر این نوع حملات بوجود میآید عبارتند از:

- افشای اطلاعات محرمانه
- تزریق اطلاعات جعلی یا تغییر یافته به شبکه
- اختلال در عملیات مسیریابی از طریق ترجمه غلط آدرسها
- اختلال در ارائه خدمات و فعالیتهای شبکه
- ایجاد ازدحام [4] در شبکه از طریق دو تکه نمودن آن

---

[1] Configuration Vulnerability
[2] Domain Name System
[3] Denial of Service
[4] Congestion

دامنه تأثیر حملات علیه مسیریابها

یک حمله میتواند با تحمیل خسارات فراوان، عملکرد یک شبکه یا میزبان را مختل کرده و حتی به کل عملیات مربوط به زیرساخت مسیریابی یک شبکه آسیب رساند. خسارتهای مربوط به کل زیرساخت ارتباطی که منشاء آن حملات صورت گرفته بر روی مسیریاب است، شامل موارد زیر است:

- ازدحام شبکه[۱]: میزان بسیار زیادی حجم ترافیک از طریق یک قسمت خاص از شبکه ارسال می شود که قابلیت ارسال آن حجم را ندارد.کنترل بیش از حد [۲]، مانع [۳] و حلقه [۴] می توانند از عوامل ایجاد ازدحام در شبکه باشند.
- سیاه چاله[۵]: میزان زیادی از ترافیک داده به صورت غیر ضروری از یک مسیریاب ارسال می‌شود و در نتیجه مسیریاب، بسیاری و گاهی همه بسته‌ها را حذف می کند.

---

[1] Network Congestion

[۲] در این حالت پیغامهای مربوط به پروتکل مسیریابی خود حجم قابل ملاحظه‌ای از ترافیک شبکه را تشکیل می‌دهند.

[۳] یک مسیریاب تعداد زیادی پیغام مسیریابی دریافت می کند که این منجر به هدر رفتن زمان پردازش، حافظه و غیره در مسیریاب می گردد.

[۴] ترافیک داده روی یک مسیر حلقه وار فرستاده می‌شود که در نتیجه هرگز به مقصد نمی‌رسد و منجر به گرفتگی شبکه می گردد.

[5] Black hole

- دوتکه شدن[1]: یک قسمت از شبکه به صورت واقعی یا مجازی از کل شبکه جدا و غیر قابل دسترسی می‌شود.
- فعال سازی شدید [2]: نرخ ارسال ترافیک در شبکه بسیار سریع (و غیر ضروری) تغییر پیدا می کند که منجر به ایجاد اختلاف [3] زیاد در نرخ دریافت بسته‌ها می گردد. این امر باعث عدم کارکرد صحیح برخی عملیات شبکه نظیر برنامه‌های چندرسانه‌ای می‌شود.
- ناپایداری[4]: پروتکل مسیریابی ناپایدار می‌شود به نحوی که همگرائی در عملیات مسیریابی صورت نمی گیرد.

مخاطرات مربوط به مسیریابی

در این قسمت به طور خاص به فرایندهای مرتبط با مخاطرات پروتکل های مسیریابی پرداخته می‌شود. قابل ذکر است که این فرایندها مربوط به یک یا چند پروتکل خاص نمی‌باشند.

- آشکارسازی عمدی[5]: این کنش زمانی اتفاق می‌افتد که مهاجم کنترل مسیریاب را در دست گرفته و به صورت عمدی اطلاعات مسیریابی را به واحدهایی (مانند مهاجم، یک صفحه وب، یا تعدادی مسیریاب) بفرستد که در حالت عادی آن واحدها نباید از اطلاعات فرستاده شده خبردار شوند. مهم‌ترین نتیجه این تهدید، آشکارسازی اطلاعات مسیریابی است. دوره این فرایند ممکن است بیشتر از زمان خود تهدید باشد، زیرا تا

---

[1] partition
[2] churn
[3] Variance
[4] instability
[5] deliberate exposure

زمانی که توپولوژی شبکه تغییر نکند، نیازی به بروز رسانی اطلاعات آشکارشده مسیریابی وجود ندارد.

- شنود[1] مسیریاب: این حمله زمانی رخ می‌دهد که مهاجمین، اطلاعاتی که بین مسیریاب های معتبر رد وبدل می‌شود را ضبط و رصد کرده تا اطلاعات مسیریابی را شنود کنند. - مهاجمین همچنین می‌توانند ترافیک‌های دیگر شبکه را نیز شنود کنند.- طبیعی است که پیامد چنین تهدیدی افشا شدن اطلاعات مسیریابی است. ناحیه تهدید به موقعیت مهاجم، نوع پروتکل مسیریابی، و اطلاعات مسیریابیِ ضبط شده بستگی دارد. اگر مهاجم عملیات شنود را متوقف کند، اطلاعاتِ مسیریابی کشف شده تا هنگامی که یک تغییر توپولوژی در شبکه رخ دهد بروز نمی‌شود.
- تحلیل ترافیک مسیریاب: در این فرآیند مهاجم با تحلیل ترافیک شبکه بر روی یک لینک به اطلاعات مسیریابی پی می‌برد. این کنش تمامی اطلاعات رد و بدل شده در شبکه را مورد تهدید قرار می‌دهد. ناحیه تهدید بستگی زیادی به موقعیت مهاجم دارد؛ مهاجمی که در هسته شبکه قرار دارد، به اطلاعات بسیار بیشتری نسبت به مهاجمی که در لبه شبکه قرار دارد دسترسی دارد و در نتیجه ناحیه تهدید آن بزرگتر است.
- جعل[2] مسیریاب: این فرآیند به خودی خود یک حمله واقعی به حساب نمی‌آید. در واقع، از این فرایند برای ایجاد تهدیدات و حملات خطرناک دیگر نظیر تحریف، استفاده می‌شود. در این فرآیند مهاجم

---

[1] sniffing

[2] Spoofing: زمانی رخ می‌دهد که یک دستگاهِ غیر معتبر در شبکه هویت یک دستگاه معتبر را اتخاذ می‌کند.

هویت یک مسیریاب معتبر را اخذ می کند و از این طریق می‌تواند اطلاعات مسیریابیِ غلطی در شبکه تزریق کند. جعل مسیریاب در نهایت می تواند باعث از کار افتادن سرویس های شبکه، پیامدهایی نظیر افشای اطلاعات مسیریابی و یا فریفتن روابط همسایگی بین مسیریاب‌ها شود.

- تحریف[1]: این فرآیند مهمترین پیامد عمل جعل است، و زمانی اتفاق می‌افتد که مهاجم اطلاعات مسیریابی غلط به شبکه ارسال کند. پیامدهای چنین تهدیدی بسیار گسترده است، عدم تحویل ترافیک داده به مقصد، دسترسی به ترافیک شبکه از طرف مهاجم، فریفتن مسیریاب های دیگر در شبکه برای ساختن مسیرهای جعلی و ادعاسازی اشتباه [2] از مهمترین آثار تحریف هستند.
- تداخل[3]: این حمله زمانی رخ می‌دهد که مهاجم از تبادل اطلاعات مابین مسیریاب‌های قانونی جلوگیری می کند. مهاجم از طریق ارسال نویز به شبکه، رله نکردن پیغامها در شبکه ، تأخیر انداختن ارسال بسته‌ها، حمله DoS روی مسیریاب های مقصد و یا با ایجاد خلل در زمانبندی بین مسیریاب‌ها می‌تواند این کنش را عملی سازد.
- ایجاد سربار[4]: این حمله زمانی رخ می‌دهد که مهاجم بار ترافیکی یا محاسباتی زیادی بر روی مسیریاب اعمال می‌کند. برای مثال، مهاجم ممکن است که یک مسیریاب را تحریک به ارسال حجم زیادی اطلاعات به مسیریاب های دیگر کند و یا بطور مشابه، با ایجاد سریع پیغام‌های مسیریابی این تهدید را در شبکه عملی سازد.

---

[1] falsification

[2] Misclaiming: هنگامی رخ می‌دهد که مهاجم اطلاعات غیرواقعی را به شبکه اعلام می‌کند.

[3] interference

[4] Overload

فصل ۲

روشهای مقابله با مخاطرات امنیتی و ایمنی در مسیریاب

با توجه به نقاط آسیبپذیر و همچنین بررسی تهدیدات و حملات صورت گرفته علیه مسیریابها، برقراری امنیت در حوزه کاری مسیریاب باید در چهار لایه مختلف به شرح ذیل دنبال شود.

۱. فیزیکی: داخلیترین لایه نیازمند مصونسازی در یک مسیریاب، لایه فیزیکی است چراکه با داشتن دسترسی فیزیکی، یک نفوذگر میتواند کنترل کامل مسیریاب را در دست بگیرد. از اینرو برای این لایه امنیتی، باید سیاستهای مشخصی در نظرگرفته شود.

۲. نرمافزار و پیکربندی ثابت: مفاهیمی همچون نشانی واسط ها، رمزهای عبور و کنترل دسترسی به درگاه های پیکربندی، در این لایه مطرح میشوند و قابل دسترسی هستند، از سوی دیگر با توجه به اینکه در صورت نفوذ به این لایه، کنترل لایه های بالاتر نیز به دست نفوذگر

خواهد افتاد، مصون نگاه داشتن این لایه از آسیب ها، حملات و نفوذهای احتمالی اهمیت خاصی خواهد داشت از این رو باید سیاست امنیتی مربوط به آن به دقت و بصورت جامع تدوین و اعمال شود.

۳. پیکربندی پویا: این لایه شامل اطلاعاتی همچون جدول‌های مسیریابی و ARP[1] و گزارشات است. سیاست های امنیتی، باید نحوه دسترسی به این لایه را مورد توجه قرار دهند.

۴. داده‌های عبوری و سرویس‌ها: سیاست امنیت مربوط به این بخش شاید بزرگترین بخش از تدوین سیاست امنیتی مسیریاب باشد. در این لایه، تصمیم در خصوص آدرس ها و پروتکل هایی که مجوز عبور دارند، موضوع اصلی است.

بررسی نکات و دستورالعمل های امنیتی دسترسی به مسیریاب

در این قسمت از کتابچه نگاهی مختصر به مهمترین روش ها و موارد مؤثر در دسترسی به یک مسیریاب خواهیم داشت و در هر بخش به راهکارهای لازم جهت ارتقای ضریب امنیتی مربوطه اشاره ای خواهیم کرد.

- دسترسی فیزیکی

مهمترین و اولین نکته ای که باید مورد توجه مدیر امنیتی یک مسیریاب قرار گیرد، امنیت دسترسی فیزیکی و ایمنی آن است. اگر امنیت فیزیکی مسیریاب تأمین نشود، تدابیر امنیتی دیگر نیز، اثرات مورد انتظار را نخواهند داشت. اگر مهاجم به یک مسیریاب دسترسی فیزیکی داشته باشد، در صورت داشتن تجهیزات لازم ودانش کافی، قادر خواهد بود کنترل کامل مسیریاب را در دست بگیرد. از راهکارهای تأمین امنیت

[1] Address Resolution Protocol

فیزیکی می توان به نگهداری مسیریاب در یک محوطه در بسته امن و ایمن و اعمال سیاست های کنترل تردد و احراز هویت مناسب اشاره کرد.

- پیکربندی مسیریاب

اعمال هر تغییر در پیکربندی مسیریاب ممکن است باعث ایجاد یک آسیب‌پذیری جدید و یا اختلال در عملکرد مسیریاب گردد. از این رو دقت در پیکربندی این سامانه و اعطای مجوزهای لازم تنها به افراد صاحب صلاحیت از اهمیت فراوانی برخوردار است. باید دقت شود هرگونه پیکربندی و یا تغییر در آن پس از طی مراحل لازم و تنها هنگامی صورت پذیرد که اطمینان کافی از سلامت پیکربندی وجود داشته باشد. بعنوان نمونه یکی از موارد عمومی مهم، هنگام پیکربندی مسیریاب غیرفعال کردن واسط‌های بدون استفاده است.

- فهرست دسترسی[1]

فهرست‌های دسترسی، از ابزارهای معمول مورد استفاده جهت اعمال سیاست‌های امنیتی سازمان ها و متولیان شبکه در خصوص تعیین اجازه عبور انواع بسته های ورودی به مسیریاب است. درصورتی که پس از انطباق یک بسته ورودی با فهرست دسترسی، این بسته اجازه عبور پیدا نکند، عملیات مسیریابی روی آن انجام نمی‌گیرد.

ساده‌ترین نوع فهرست دسترسی، فهرست دسترسی استاندارد است. در این نوع فهرست دسترسی می توان عبور داده از یک واسط را برحسب نشانی مبدأ بسته، کنترل کرد. بعد از تعریف فهرست دسترسی، هیچ بسته‌ای عبور نخواهد کرد مگر اینکه در فهرست دسترسی، به آن اجازه

[1] Access list

عبور داده شده باشد. فهرست دسترسی استاندارد فقط بر حسب نشانی IP مبدأ می‌تواند به بسته‌ها اجازه عبور و بسته های عبور داده نشده را گزارش دهد. با توجه به محدودیت های این نوع فهرست دسترسی، امروزه نوع دیگری از فهرست دسترسی مورد توجه قراردارد که فهرست دسترسی گسترش‌یافته[1] نامیده می شود. در فهرست دسترسی گسترش یافته، می توان برحسب نشانی مبدأ، نشانی مقصد، پورت مبدأ، پورت مقصد، پروتکل و حتی اینکه ارتباط قبلاً برقرار شده است یا نه، اجازه عبور بسته ها را داد و یا از عبورآن‌ها جلوگیری کرد. باتوجه به توانمندی‌ها و پیچیدگی‌های این امکان، نحوه ساختن این فهرست ها از اهمیت فراوانی برخوردار است. چراکه تعریف صحیح فهرست های دسترسی و وجود سیاست های مناسب در این حوزه باعث می شود تا همه بسته‌هایی که مجاز هستند، بتوانند عبور کنند و هیچ بسته غیرمجازی، اجازه عبور نیابد.

- رمز عبور[2]

رمز عبور، کلید اصلی و از پایه ای‌ترین مفاهیم در جلوگیری از دسترسی بدون مجوز به تجهیزات شبکه ای است. اولین قدم در مدیریت رمز عبور، انتخاب رمز عبور مناسب و محافظت از آن است. از جمله سیاست های لازم در انتخاب رمز عبور، می توان به موارد ذیل اشاره کرد:

- رمز عبور نباید از نام سازمان مربوطه منتج شده باشد.
- رمز عبور نباید کوتاه باشد.

---

[1] این نوع فهرست دسترسی به عنوان پایه ای برای فهرست های دسترسی پیشرفته تر نظیر فهرست های Context-Based و Reflex محسوب می‌شود.

[2] Password

- تغییر رمز عبور، نباید بر یک قاعده ثابت باشد.
- مدیران غیرتکنیکی نباید رمز عبور را بدانند.
- رمز عبور نباید در جایی نوشته یا دخیره شود.

- خطوط کنترل[1]

دسترسی به خطوط کنترل، شامل پورت کنسول، درگاه کمکی [2] و درگاه telnet باید محدود شود. اولین روش برای پیکربندی و مدیریت مسیریاب، پورت کنسول است، لذا تأمین امنیت و پایداری آن بسیار ضروری است. از جمله روش های عمومی اعمال محدودیت در دسترسی به خطوط کنترل می توان به استفاده از رمز عبور و یا جلوگیری از اتصال از راه دور اشاره نمود.

بررسی نکات و دستورالعمل های امنیتی پروتکل های مسیریابی

قسمت مهمی از امنیت مسیریاب، امنیت مسیریابی آن است. بعنوان مثال، یک مهاجم می تواند با فرستادن پیام های مسیریابی غلط، باعث تغییر در جدول های مسیریابی شود و بدین ترتیب در کل عملیات مسیریابی اختلال ایجاد کند. مهاجم همچنین می تواند داده های عبوری شبکه را به سمتی که مایل است هدایت کرده و از این طریق باعث به خطر افتادن امنیت شود. برای جلوگیری از این تغییرات غیرمجاز و نادرست در جدول های مسیریابی، چند راه وجود دارد:

[1] Line Access Router
[2] Auxiliary ports

- استفاده از مسیریاب ثابت : این روش در شبکه های کوچک، قابل اجراست ولی برای شبکه های بزرگ، مناسب نمی باشد.
- استفاده از فهرست دسترسی بعنوان صافی : در بسیاری از مواقع برای جلوگیری از عبور داده های خاص، از فهرست های دسترسی استفاده می‌کنند. فهرست دسترسی دارای توانایی های متعددی است.
- احراز هویت [1]: با استفاده از این روش، منابع اطلاعاتی که اطلاعات مسیریابی را می فرستند، احراز هویت می شوند و از دسترسی و تغییرات غیرمجاز به صورت خودکار جلوگیری به عمل می آید.
- غیرفعال کردن مسیریابی RIP[2] و استفاده از پروتکل OSPF[3] به جای آن: علی‌رغم مزیت سرعت در پروتکل RIP، این پروتکل در انتقال پیام ها غیر قابل اطمینان است لذا اگر استفاده از آن برای رفع نیاز خاصی لازم نیست، بهتر است به جای آن از پروتکل OSPF استفاده شود.
- پنهان کردن اطلاعات مسیریابی: یکی دیگر از راهکارهای جلوگیری از تغییرات غیرمجاز در جداول مسیریابی جلوگیری از دسترسی مهاجمین یا نفوذگران به اطلاعات مربوط به مسیریابی از طریق دستورات و امکانات تعبیه شده در مسیریاب ها است. بدین ترتیب باعث می شویم که مسیریاب های دیگر، نتوانند اطلاعات مسیریابی پروتکل مورد استفاده را برای مسیریابی خود به دست آورند.

---

[1] Dynamic Routing Authentication
[2] Routing Information Protocol
[3] Open Shortest Path First

همچنین ممکن است بر روی پروتکل‌های مسیریابی حملات DoS نیز صورت گیرد. بعنوان یکی از نتایج این حملات می توان به جلوگیری از فرستادن و یا دریافت اطلاعات مسیریابی و یا از کار افتادن بخش‌هایی از شبکه اشاره کرد. برای مقابله با این حملات باید نسخه های پشتیبان از اطلاعات مسیریابی موجود باشد تا به سرعت بتوان خسارت وارده را جبران کرد.

فصل ۳

مخاطرات ناشی از جنگ و مخاصمات بین المللی روی مسیریاب ها

جنگ واقعیتی است که خواسته یا ناخواسته در جوامع بشری وجود دارد و در بسیاری از موارد به نظر می‌رسد راه گریزی از آن وجود نداشته باشد. هدف عمده در جنگ‌های فیزیکی از بین بردن تأسیسات زیربنایی، نیروها، توانمندیها و استعدادهای نظامی اقتصادی وصنعتی طرف مقابل است به‌گونه‌ای که باعث ایجاد شرایط مناسب برای غلبه و تفوق بر آن کشور یا ترک مخاصمه گردد .

با توجه به استقرار و نقش محصولات کلیدی همچون مسیریاب در زیرساخت ارتباطی بعنوان یکی از زیرساخت‌های حیاتی کشور، طبیعی است که این محصول استراتژیک به منظور وارد کردن آسیب به شبکه راهبری و مدیریت سیاسی و نظامی کشور از اهداف اولیه تهاجم دشمن باشد. بنابراین به کار گرفتن ساز وکارهای حفاظت از این محصول استراتژیک در برابر جنگ‌هایی که عمده تمرکز آنها، نابودی کامل محصولات کلیدی و زیرساختهای حیاتی می باشد، ضروری است.

در ادامه فصل به تبیین روش های نوین تهاجم، فضای مخاصمات بین الملل و راهکارهای تأمین امنیت و پایداری زیرساخت فناوری اطلاعات و ارتباطات کشور در حوزه مسیریاب ها خواهیم پرداخت.

جنگ اطلاعات[1]

عصر ارتباطات و اطلاعات بسیاری از مفاهیم را در حوزه های مختلف زندگی بشر و از جمله در حوزه سیاست و اجتماع به چالش کشید و تحولات بنیادین در آن‌ها پدید آورد. گسترش فناوری های ارتباطی و اطلاعاتی مفاهیم مربوط به قدرت، امنیت، سرزمین، حاکمیت و... را نیازمند تعریفی مجدد ساخته است. از جمله موضوعاتی که در این انقلاب اطلاعاتی دستخوش تغییرات شگرفی گردید، مفهوم جنگ است.

جنگ در این عصر تبدیل به امری پیچیده، مستمر و جاری شده است و شاید بتوان گفت، دیگر جنگ را نباید در زمان ومکانی خاص جستجو کرد، بلکه باید آن را بعنوان یکی از مؤلفه های همیشه در جریان و روزمره زندگی پذیرفت.

برتری سامانه های اطلاعاتی و ارتباطاتی یک نظام در دنیای کنونی، تقریباً معادل برتری و مزیت نسبی آن نظام در عرصه های مختلف است و این حقیقت به‌خودی خود شیوه های سنتی مربوط به فعالیت‌های اطلاعاتی، امنیتی، نظامی و دفاعی را تحت‌الشعاع قرار داده و کم اهمیت و کم کارآمد خواهد ساخت.

جنگ های اطلاعاتی و مسیریاب ها

همانطور که در تعریف جنگ اطلاعات اشاره شد، این جنگ از فرصت‌هایی که فناوری های نوین در اختیار کشورها قرار داده است،

---

[1]Information warfare

بهره‌گیری می کند. با توجه به تهدیدات ذکر شده در بخش مخاطرات امنیتی، آفند اطلاعاتی دشمن با رصد شبکه های ملی و فرابخشی برای رخنه در آن به منظور پیدا کردن جای پا و اتخاذ راهکارهای لازم جهت خرابکاری و یا انهدام این شبکه در مواقع بحران ، شکل می‌گیرد که در جای خود تهدید بسیار جدی است. طبیعی است استفاده از محصولات خارجی در بخش‌های حساس همچون ستون فقرات چنین شبکه‌هایی به معنی قراردادن بدون زحمت اطلاعات و پایداری کل شبکه در اختیار دشمن است. بنابراین در یک نگاه، صرف نظر از دیگر تهدیدات فنی، اولین راهکار مقابله استفاده از محصول مطمئن بومی است.

نکته حائز اهمیت برای مقابله با تهدیدات ناشی از جنگ های اطلاعاتی، ویژگی خاص آن ها در چگونگی شکل گیری است. جنگ اطلاعات تنها جنگی در دنیا است که معمولاً قبل از نواختن شیپور جنگ، از مدت‌ها و یا شاید سال‌ها قبل بین طرفین آغاز می شود.

مخاطرات ناشی از مخاصمات بین المللی

مخاصمات بین المللی[1] در برگیرنده فرآیندها و اقداماتی است که دولت‌ها تا قبل از شروع جنگ رسمی از آن بهره می برند. بعنوان مثال برقراری تحریم های مختلف علیه کشورها، یکی از ابعاد تخاصمات بین المللی است. این تحریم اگر در بخش مربوط به محصولات راهبردی روی دهد، بسیار تأثیرگذار خواهد بود. اگر اقتصاد و تجارت یک کشور کاملاً بر روی بستر الکترونیکی قرار گیرد – البته خود این بستر نیاز به یک زیرساخت ارتباطی قوی و یکپارچه دارد – ، آنگاه اعمال تحریم بر روی منابع این بستر باعث ایجاد مشکلات جدی خواهد گردید.

---

[1] International hostilities

با توجه به توضیحات فوق به نظر می رسد در برابر تحریم محصولات صنعتی استراتژیک دیدگاه بومی سازی در بخش محصولات کلیدی بای د تقویت شود . بنابراین در بخش مربوط به محصولات راهبردی همچون مسیریاب، اتخاذ فر آیند مناسب جهت بومی سازی ، رویکرد اصلی در برابر کوچک سازی ابعاد تخاصمات بین المللی در این حوزه است . خارج کردن تدریجی محصولات خارجی خریداری شده از حوزه ارتباطات زیرساخت به علت امکان قطع سرویس‌های این محصولات و همچنین شنود انواع اطلاعات مربوط به شبکه های ملی از سوی شرکت‌های سازنده از دیگر تدابیر لازم در این حوزه است.