
بسم الله الرحمن الرحیم

دیوارۀ آتش انسانی

مولف: فرهاد وکیلی

عنوان و نام پدیدآور: دیوارۀ آتش انسانی
مولف: فرهاد وکیلی
مشخصات نشر: تهران، انتشارات دیده‌بان، پاییز ۱۳۹۷
مشخصات ظاهری: ۱۲۸ ص
وضعیت فهرست‌نویسی: فیپا
موضوع: دیوارۀ آتش – تهدید – آسیب – تدابیر امنیتی
رده بندی کنگره: ۱۳۹۷ ۹د۸و/TK۵۱۰۵/۵۹ رده‌بندی دیویی: ۰۰۵/۸
کتابشناسی ملی: ۵۴۳۴۶۴۲

انتشارات دیده‌بان

- **عنوان کتاب: دیوارۀ آتش انسانی**
- **مؤلف: فرهاد وکیلی**
- **ناشر: انتشارات دیده‌بان**
- **ناظر و ویراستار علمی: جواد بزرگی**
- **ویراستار ادبی: حسن جفائی**
- **صفحه‌آرا: حسن جفائی**
- **طرح روی جلد: مجید نیکپور**
- **شمارگان: ۱۰۰۰ جلد**
- **نوبت چاپ: اول، پاییز ۱۳۹۷**
- **قیمت: ۲۰۰/۰۰۰ ریال**

این کتاب با همکاری و مشارکت مرکز پژوهشی علم و فناوری امنیت دفاعی چاپ و منتشر گردیده است.

شابک: ٤ – ۳ – ۹٦۷۹۰ – ٦۰۰ – ۹۷۸ :ISBN

آدرس: تهران، چهارراه پاسداران، انتشارات دیده‌بان، تلفن: ۲۲۷٦۲۸۳۷

فهرست مطالب

پیشگفتار

تهیه این مطالب باتوجه به تدبیر مقام معظم‌رهبری درخصوص دیوارۀ آتش آغاز شده است:

تلاش کنید که یک دیوارۀ آتش درست کنید که کسی نتواند نزدیک شود. البته سخت است چون در بخش‌های مختلف همه نیروهای فنی و علمی، هستند و کارهای مهم و حساس هم دستشان است. مشکل است اما با تدبیر و با ظرافت می‌شود خیلی کارها را انجام داد. به طور جدی این مسئله را دنبال کنید.

در بررسی این تدبیر مشخص است که هدف اصلی در این تدبیر نیروهای فنی و علمی هستند. نیروهای فنی و علمی، فقط کسانی که شاغل می‌باشند، نیستند بلکه کلیه کسانی که در خارج از صنایع و حتی در خارج از کشور حضور داشته ولی در جهت منافع صنایع حرکت نموده و فعالیت می‌نمایند جزئی از عوامل انسانی محسوب می‌گردند.

دراین کتاب، پس از پرداختن به مفهوم دیواره آتش و مقوله امنیت که هدف دیوارۀ آتش نیز برقراری و ایجاد امنیت است، ابتدا به تهدید و آسیب‌پذیری پرداخته خواهد شد تا نوع تهدیدها بررسی شود و آسیب‌پذیری‌های آن نیز مشخص گردد و پس از آن به مفاهیمی همچون عزت، جهاد کبیر و باور که در ارتباط با موضوع هستند، اشاره می‌گردد.

در فصل دوم کتاب نیز ضمن اشاره به پیشینه و بیانات مقام معظم رهبری، مدل پیشنهادی و چگونگی ایجاد دیوارۀ آتش در سازمان ارائه و نهایتا به نتیجه‌گیری و پیشنهادات مبتنی بر مدل پیشنهادی پرداخته شده است.

مقدمه

امنیت مسئله‌ای اساسی برای هر سازمان، صنعت و یا مجموعه‌ای است تا بتواند در زیر چتر امنیت به فعالیت‌های خود ادامه دهد. با گسترش تعاملات، نقاط آسیب‌پذیر نیز گسترش می‌یابد. مسئله اصلی این است که در اثر گسترش تعاملات و پیشرفت علم و تکنولوژی، مدل تهدید نیز تغییر می‌نماید. لذا می‌بایست تمهیداتی را به‌کار بست تا امنیت را ارتقاء داد. در جنگ خندق با پیشنهاد سلمان‌فارسی به پیامبر بزرگوار اسلام(ص) خندقی در اطراف شهر حفر نمودند تا دشمن از هر طرف نتواند حمله نماید و گلوگاهی درست نمودند تا نحوه عمل دشمن را نیز تحت‌کنترل قرار دهند. این خندق همان دیوارهٔ آتش است که باتوجه به پیچیده‌شدن تهدید، به‌صورت پیشرفته‌تر به دفع حملات تهدیدکنندگان می‌پردازد.

حال باتوجه به بستر سازمان‌ها و تعاملات آنها با مجموعه‌های بیرون از خود، چگونه می‌توان دیوارهٔ آتشی ایجاد نمود که دشمن نتواند به عوامل آن سازمان نزدیک‌شده و آسیبی به منافع و دستاوردهای آن بزند و نکته اصلی این است که دیوارهٔ آتش از چه نوعی باشد و چه ویژگی‌هایی را باید دارا باشد؟

در این کتاب به مفهوم و انواع دیوارهٔ آتش شناسایی و چگونگی ایجاد آن اشاره تا سازمان‌ها و صنایع بتوانند از گزند تهدیدها و آسیب‌رسانی‌های دشمنان مصون باشند.

باتوجه به تدبیر مقام معظم‌رهبری مبنی بر تهیه دیوارهٔ آتش و نیاز گسترش تعاملات؛ می‌بایست تمهیداتی را به‌کار گیریم تا دشمن نتواند نزدیک شود و گزندی را وارد نماید. در مقابل تهدیدهایی که دشمنان نظام جمهوری‌اسلامی‌ایران و حملاتی که سرویس‌های اطلاعاتی

انجام می‌دهند، باید عوامل بازدارنده‌ای را طراحی کرد. لذا همان درس زمان پیامبر(ص) در جنگ خندق، می‌تواند راهگشایی خوبی باشد تا هم تعاملات گسترده، ادامه یابد و هم امنیت ایجاد شود.

باتوجه به گستردگی موضوع، هر بخش در یک مدل ارائه می‌شود و در انتها مدل‌ها جمع‌بندی‌شده و یک مدل واحد ارائه می‌گردد و برای اینکه مدل همیشه پویایی خود را دارا باشد، باید فرایندی تهیه نمود که طبق آن بتوان پویایی مدل حفظ شود.

۱

فصل اول
مفهوم دیوارهٔ آتش

پیاده‌سازی دیوارهٔ آتش، به‌منظور ایجاد امنیت و حفظ آن می‌باشد. برای پی‌بردن به مفهوم دیوارهٔ آتش، لازم است مفاهیم، مولفه‌ها و اجزایی که دیوارهٔ آتش را ایجاد و نتایجی را که یک دیوارهٔ آتش باید ارائه نماید را بشناسیم.

بخش ۱– دیوارهٔ آتش

امنیت بدون انجام اقدامی موثر در برابر تهدیدات و ایجاد تمهیدات لازم برقرار نخواهد شد. لذا به‌منظور داشتن فضایی امن، باید اقداماتی انجام داد که هم تحرکات دشمن زیرنظر باشد و هم بتوان دشمن را هدایت نمود (فریب و مشغول‌سازی) تا از هر طرف نتواند به‌سمت ما حمله‌ور شود.

دیواره‌های آتش از مهم‌ترین ابزارهای تدافعی محسوب می‌شوند. دیوارهٔ آتش، یکی از راه‌های حفاظت خودی از دیگری و یا عوامل غیر قابل‌اطمینان است. دیوارهٔ آتش به‌طور کلی بر دو اساس به‌کار گرفته می‌شود:

الف- براساس ممانعت از عبور و انجام تعاملات

ب - براساس اجازه عبور و انجام تعاملات

به بیان دیگر در پیاده‌سازی دیوارهٔ آتش، به‌دنبال ایجاد امنیت هستیم. مدیریت امنیت، بستن و ممنوع‌الورود کردن همه‌چیز، برای همه‌کس و در همه‌زمان نیست، بلکه مدیریت امنیت، کنترل اینکه چه فردی، در چه زمانی، به چه میزانی و به چه سیستم‌ها، اسناد و اطلاعاتی دسترسی داشته باشد، است.

مطلب مهمی که لازم است در مورد دیوارهٔ آتش بدانیم، آن است که ما را در مقابل چه خطراتی محفوظ می‌نماید؟ به‌طور کلی دیوارهٔ آتش به‌منظور جلوگیری از دسترسی افراد غیرمجاز به اطلاعات، به‌ویژه برای ممانعت از دسترسی افراد خرابکار طراحی شده است. بنابراین اصلی‌ترین وظیفه یک دیوارهٔ آتش، کنترل تعاملات دنیای خارج به داخل است و در عین‌حال تسهیلات لازم برای ارتباط با دنیای خارج را برای کارکنان داخلی فراهم می‌نماید. علاوه بر آن از آنجا که دیوارهٔ آتش یک نقطه تماس منحصربه‌فرد ایجاد می‌کند، می‌توان از آن نقطه تماس برای انجام بازرسی‌های مختلف استفاده نمود و حتی اقدام به رهگیری نفوذگران احتمالی نمود. در ادامه برای آشنایی بیشتر با مفهوم دیوارهٔ آتش دو تعریف ارائه می‌گردد:

۱- دیوارهٔ آتش:

تمهید و قابلیتی است که به‌کار گرفته می‌شود تا کلیه تعاملات را از لحاظ امنیتی مورد بررسی قرار دهد (مطهری، ۱۳۸۸: ۸-۷) و درصورت مطابقت با مقررات، اصول استانداردها و دستورالعمل‌های حفاظتی (بشری‌راد، ۱۳۹۱) حاکم اجازه ورود یا خروج داده شود و تمامی رویدادهای (ملکیان، ۱۳۹۱) ورودی و خروجی را، جهت اعمال کنترل‌های لازم (چه آنهایی که مجوز ورود را کسب‌نموده و چه آنهایی که کسب ننموده‌اند) ثبت می‌نماید (موسسه فرهنگی فاطمی، ۱۳۸۶: ۱۵۳).

۲- دیوارهٔ آتش انسانی:

قابلیت و توانایی است برای ایجاد مشارکت کارکنان در حفظ امنیت اطلاعات (Kawamoto، 2004)، تا ضمن شکست‌ناپذیرنمودن آنها در برابر تهدیدات، بتواند با آن مقابله نموده و خللی در انجام امور محوله نیز به‌وجود نیاید.

مسئله مهم دیگر در دیواره‌های آتش، پیکره‌بندی و نحوه تعریف قواعد در آنهاست. درصورتی‌که دیوارهٔ آتش، به‌درستی پیکره‌بندی نشده باشد و سهل‌انگاری در آن صورت گرفته

باشد، راه نفوذ برای خرابکاران همچنان باز خواهد بود. در مقابل، درصورتی‌که بیش از حد متعارف، در ایجاد محدودیت‌ها سخت‌گیری گردد، گردش کارها نیز دچار مشکل می‌شود. بنابراین در شروع استفاده از دیوارهٔ آتش باید لیستی تهیه گردد که در آن مشخص گردد چه فعالیت‌هایی محدود و چه فعالیت‌هایی آزاد گذارده شوند و همچنین میزان خطرپذیری هر یک از مجوزهای عبوری تعریف گردد. بدین‌ترتیب با تهیه این لیست، شما اولین قدم را در راه ارزیابی ارتباطات خود بر می‌دارید. به‌طور کلی عملکرد دیواره‌های آتش را می‌توان در چهار جمله خلاصه کرد (مطهری، ۱۳۸۸: ۷):

* افراد را موقع ورود در یک نقطه کاملاً کنترل‌شده محدود می‌سازند.
* از نزدیک‌شدن خرابکاران به منابع داخلی جلوگیری می‌کنند.
* افراد را موقع خروج در یک نقطه کاملاً کنترل‌شده محدود می‌سازند.
* تمامی رویدادها را ثبت می‌نماید.

و به‌عبارت دیگر می‌توان گفت یک دیوارهٔ آتش یک جداساز، یک محدودساز، آنالیزکننده است. از دیگر توانایی‌های دیواره‌های آتش به موارد زیر می‌توان اشاره کرد (همان: ۸):

۱- اجرای تصمیمات امنیتی را در یک نقطه متمرکز کند.
۲- سیاست امنیتی را به اجرا در آورد.
۳- فعالیت‌های مهم را ثبت کند.
۴-یک دیوارهٔ آتش قادر است سطوح مختلفی از امنیت را برای بخش‌های مختلف پیاده‌سازی کند.

ضرورت استفاده از دیوارهٔ آتش:

یک سیستم بدون وجود یک دیوارهٔ آتش، در مقابل مجموعه‌ای گسترده از فعالیت‌های مخرب آسیب‌پذیر است و در برخی موارد صرفاً پس از گذشت مدت زمان کوتاهی، آلوده خواهد شد. درصورتی که تدابیر و مراقبت لازم انجام نگردد، ممکن است کسانی که به‌صورت تصادفی پایش می‌نمایند، شناسایی نموده و سپس تخریب و یا سوءاستفاده از اطلاعات نمایند.

با اینکه استفاده از دیواره‌های آتش به‌عنوان یک عنصر حیاتی در ایمن‌سازی محیط‌های عملیاتی مطرح می‌باشند ولی تمامی داستان ایمن‌سازی به این عنصر ختم نمی‌شود و می‌بایست از سایر امکانات و یا سیاست‌های امنیتی خاصی نیز تبعیت گردد.

اساسا یک دیوارهٔ آتش، جداکننده شبکه‌های امن از ناامن است. دیوارهٔ آتش تمام آنهایی را که به‌طور غیرمجاز قصد واردشدن به محیط‌های محافظت‌شده را دارند، فیلتر می‌کند و تنها کسانی مجاز می‌باشند، که مجوز ورود را بدست می‌آورند. قبل از تعریف اینکه چه نوعی از دیوارهٔ آتش برای نیازهای مجموعه ما مناسب است، باید بستری را که می‌خواهیم دیوارهٔ آتش را بر روی آن مستقر نماییم با اجزای کامل آن و تعاملاتی که با محیط بیرون دارد را بشناسیم. تا بتوان بهترین دیوارهٔ آتش که مخصوص آن گستره است را حاکم نماییم. برای ایجاد امنیت نیاز به بررسی شبکه داخلی از لحاظ مدل ارتباطی می‌باشد و پس از آن شبکه خارجی و شناسایی نحوه و نوع تعامل آنها است. باتوجه به طبقه‌بندی اطلاعاتی که در شبکه داخلی مورد بهره‌برداری قرار می‌گیرد، لایه‌بندی‌ها باید انجام شود و در هر لایه دیوارهٔ آتش متناسب با آن لایه را باید حاکم کنیم.

دیواره‌های آتش به‌تنهایی نمی‌توانند امنیت یک محیط را برقرار کنند و فقط یک قسمت را امن کند بلکه به‌منظور ایجاد امنیت باید محدوده‌ای را مشخص نمود و مواردی را که باید محدود شوند را نیز تعیین و یک سیاست امن را گسترش داد و مکانیسم‌هایی برای اعمال سیاست‌های موردنظر ایجاد کرد. این مکانیسم‌ها بعد از اعمال سیاست‌های امنیتی مشخص می‌شوند و نه قبل از آن. ایجاد امنیت از سازمانی به سازمان دیگر متفاوت است البته این بستگی به خواسته‌های آن محیط می‌باشد (http://vista.ir).

باتوجه به بررسی‌های صورت‌گرفته و تعاریف بدست آمده از دیوارهٔ آتش، کلید واژه‌های زیر در آن شاخص می‌باشد. لذا درصورتی یک دیوارهٔ آتش می‌تواند مناسب باشد که با وزن مشخص‌شده در جدول زیر، خصوصیات لازم را داشته باشد.

تعاریف دیواره آتش	نظارت بر دسترسی‌ها	محدودکردن دسترسی	اجازه عبور به ترافیک مطابق دستورالعمل‌های حفاظتی	از مهم‌ترین ابزارهای تدافعی
فصلنامه تخصصی ثبت برتر – شماره۳[۱]		*		
کتاب نفوذگری در شبکه و روش‌های مقابله[۲]	*			
انجمن(Network Computer Security Association (NCSA		*		
اولین دانشنامه شبکه به فارسی (Wiki Network) [۳]			*	
http://www.gooyait.com[۴]	*	*	*	
سایت شبکه فنآوری اطلاعات ایران [۵]		*		
کتاب سیستم‌عامل دو رشته فنی و حرفه‌ای[۶ ۷]		*		
کتاب ویروس‌ها و بدافزارهای کامپیوتری[۸]			*	
مقاله از دیواره آتش چه می‌دانید؟[۹]		*	*	*

جدول مقایسه‌ای تعاریف دیوارهٔ آتش

در جدول فوق شاخصه‌ای که بیشترین وزن را در منابع جمع‌آوری‌شده، بدست آورده است به‌ترتیب زیر است:

شاخص اول؛ محدودکردن دسترسی

شاخص دوم؛ ارائه مجوز عبور به ترافیکی که با دستورالعمل‌ها و قوانین تطبیق داشته باشد.

شاخص سوم؛ نظارت صرف به دسترسی‌ها است.

---

۱ - (مطهری، ۱۳۸۸: ۸-۷)

۲ - (ملکیان، ۱۳۹۱)

3 - http://wiki-network.ir

4 - http://www.gooyait.com,1393/02/24

5 - http://vista.ir

6 - Firewall, Britannica Concise Encyclopedia

۷ - (موسسه فرهنگی فاطمی، ۱۳۸۶: ۱۵۳)

۸ - (بشری‌راد، ۱۳۹۱)

۹ - موسسه فرهنگی و هنری نور راسخون

و شاخص آخر؛ حالت تدافعی‌داشتن دیوارهٔ آتش می‌باشد. با تاملی در تعاریف می‌توان چنین نتیجه گرفت که عملکرد دیواره‌های آتش فیزیکی را می‌توان در سه جمله خلاصه کرد:

- آنها افراد را موقع ورود در یک نقطه کاملاً کنترل‌شده محدود می‌سازند.
- آنها از نزدیک‌شدن خرابکاران به منابع داخلی جلوگیری می‌کنند.
- آنها افراد را موقع خروج در یک نقطه کاملاً کنترل‌شده محدود می‌سازند.

در واقع این نقطه کاملاً کنترل‌شده در مثال قلعه‌های قرون وسطایی همانند پل متحرکی است که تنها در مواقع ورود و خروج افراد مشخص بر روی خندق قرار می‌گیرد و در دیگر موارد بسته است و در نقش درب قلعه عمل می‌کند. دیوارهٔ آتش اغلب در نقطه‌ای که شبکه داخلی به شبکه خارجی متصل است قرار داده می‌شود. تمام ترافیکی که از سمت شبکه خارجی به شبکه داخلی وارد می‌شود و یا از شبکه داخلی به‌سمت شبکه خارجی، خارج می‌شود از دیوارهٔ آتش عبور می‌کند، به‌همین علت دیوارهٔ آتش فرصت و موقعیت مناسبی را داراست که تشخیص دهد آیا ترافیک عبوری مورد پذیرش هست یا خیر؟ اینکه چه ترافیکی مورد پذیرش هست به "سیاست امنیتی[1] باز می‌گردد. سیاست‌های امنیتی تعیین می‌کنند که چه نوع ترافیک‌هایی مجوز ورود و یا خروج را دارا می‌باشند. بنابراین می‌توان گفت یک دیوارهٔ آتش:

- یک جداساز است.
- یک محدودساز[2] است.
- یک آنالیزکننده[3] است.

یک دیوارهٔ آتش ممکن است، مسیریابی با چند لیست کنترل دسترسی باشد. دیواره‌های آتش اگر چه از بروز مشکلات مختلف برای محیط داخلی جلوگیری می‌کنند، اما بدون اشکال و عیب نیستند. در مثال ذکرشده، افراد ماهرتر، قادر خواهند بود از خندق با شنا عبور کنند و در یک فرصت مناسب هنگامی که پل باز است با لباس مبدل به قلعه وارد شوند. سؤال اینجاست که با وجود این اشکالات چرا دیواره‌های آتش مورد استفاده قرار می‌گیرند؟ در پاسخ باید گفت درست است که در حالات خاصی دیوارهٔ آتش نفوذپذیر است و خرابکاران قادرند از آن عبور کنند، اما با

1 - Security Policy
2 - Restrictor
3 - Analyzer

این‌حال این ابزار از عبور بسیاری از خرابکاران جلوگیری می‌کند و موثرترین ابزار در کنترل دسترسی به‌شمار می‌آید. درصورتی‌که هیچ خندقی وجود نداشته باشد، ورود افراد غیرمجاز به قلعه بسیار آسان‌تر خواهد بود و آیا چون در حالات خاصی، افراد خاص ممکن است از خندق عبور کنند، هیچ خندقی وجود نداشته باشد؟ در هرحال یک دیوارهٔ آتش قادر است در جهت بالارفتن سطح امنیتی سازمان اقدامات مفیدی را انجام دهد.

- یک دیوارهٔ آتش می‌تواند سیاست امنیتی را به اجرا در آورد. سیاست امنیتی را مجموعه‌های مختلفی تعیین می‌کنند که چه سرویس‌هایی ارائه شود و یا چه تعاملاتی انجام گیرد و چه افرادی مجازند از این سرویس‌ها استفاده کنند. دیواره‌های آتش قادرند با نگهبانی و کنترل سرویس‌های مختلف تنها به سرویس‌های مجاز تعریف‌شده در سیاست امنیتی، اجازه تعامل دهند و بدین‌ترتیب سیاست امنیتی را به اجرا درآورند. سیاست‌های امنیتی نهایتاً به تعدادی قوانین اجرایی تبدیل می‌شوند که دیواره‌های آتش قادر خواهند بود تعداد زیادی از آنها را اجرا کنند. دیواره‌های آتش ممکن است سرویس‌های خطرناک و ناامن را با اعمال محدویت تنها در داخل اجازه دهند. سیاست‌های امنیتی مختلفی قابل اتخاذ هستند.

- یک دیواره آتش می‌تواند فعالیت‌های مهم را ثبت کند. دیوارهٔ آتش یک مکان مناسب برای ثبت مجموعه‌های مختلف از فعالیت‌هاست. به‌عنوان تنها نقطهٔ دسترسی، دیوارهٔ آتش می‌تواند ثبت کند که چه اتفاقاتی بین مجموعه محافظت‌شده و مجموعه بیرونی رخ می‌دهد. با دسته‌بندی این اطلاعات می‌توان به نتایج خوبی در ارتباط با تهاجم‌های درحال شکل‌گیری، مزاحمان و متخلفان داخلی و خارجی و... دست یافت.

- یک دیوارهٔ آتش قادر است سطوح مختلفی از امنیت را برای بخش‌های مختلف پیاده‌سازی کند؛ از دیواره‌های آتش گاهی برای جدا نگه‌داشتن یک بخش از بخش‌های دیگر استفاده می‌شود. این حالت زمانی اتفاق می‌افتد که یک بخش از شبکه بیشتر از بخش‌های دیگر حساس باشد و نیازمند امنیت بیشتری باشد. بدین‌ترتیب با استفاده از دیواره‌های آتش می‌توان بخش‌های مختلف، با سطوح امنیتی مختلف را ایجاد نمود. این مسئله باعث می‌شود بروز مشکلات امنیتی نتواند تمام مجموعه را تحت‌تأثیر قرار دهد و برخی بخش‌های مهم‌تر و حساس‌تر مصون بمانند. دیواره‌های آتش در مجموع قادرند هر مجموعه را در برابر تهدیدات مختلف تا حد زیادی مورد محافظت قرار دهند، اما آنها راه‌حل امنیتی کامل و بدون عیبی

نیستند. برخی از خطرات و مشکلات از کنترل دیوارهٔ آتش خارج هستند و برای مقابله با آنها باید از روش‌هایی مانند ایجاد مکانیزم‌های قوی امنیت فیزیکی، مصونیت میزبان، آموزش عوامل انسانی و... استفاده کرد.

- دیواره‌های آتش از مهم‌ترین ابزارهای تدافعی محسوب می‌شوند و باوجود تصور عمومی دارای ویژگی‌ها و امکانات متفاوتی هستند. دیوارهٔ آتش، یکی از راه‌های حفاظت مجموعه خودی از مجموعه غیر قابل‌اطمینان است. عملکرد فعلی دیواره‌های آتش بسیار متنوع و گسترده شده است، لیکن به‌طور کلی بر دو اساس کار می‌کنند: براساس ممانعت از عبور با انجام تعامل و دیگری براساس اجازه عبور و انجام تعامل

- یک دیوارهٔ آتش نمی‌تواند از بروز تمام مشکلات امنیتی جلوگیری‌کند. دیوارهٔ آتش برای مقابله با خطرات شناخته‌شده طراحی شده است. مدیران شبکه با شناختی که از حملات و خطرات مختلف دارند و با تصویب تعدادی قوانین و اجرای آنها توسط دیوارهٔ آتش سعی می‌کنند از بروز آنها جلوگیری کنند، اما واقعیت این است که روز به روز حملات و مشکلات امنیتی جدیدی به‌وجود می‌آیند و دیوارهٔ آتش نمی‌تواند به‌طور خودکار با این خطرات مقابله کند. دیوارهٔ آتش نیز مانند تجهیزات دیگر توسط مدیر سیستم پیکربندی می‌شود و پیرو دستوراتی است که مدیر می‌دهد. یک پیکربندی خوب تا حدودی قادر خواهد بود از خطرات جدید نیز جلوگیری‌کند. در این پیکربندی هیچ ترافیکی غیر از ترافیک مربوط به تعداد بسیار اندکی از سرویس مطمئن عبور داده نمی‌شود. خرابکاران به‌طور مرتب راه‌های جدیدی برای نفوذ و خرابکاری پیدا می‌کنند. آنها یا از سرویس‌های مطمئن شناخته‌شده، سوءاستفاده می‌کنند و یا مشکلاتی که تاکنون برای کسی رخ نداده (هیچ‌کس راجع به آنها چیزی نمی‌داند و به‌همین دلیل در هیچ دیوارهٔ آتشی درنظر گرفته نشده) را به‌کار می‌بندند.

- یک دیوارهٔ آتش را نمی‌توان با یکبار پیکربندی؛ انتظار داشت برای همیشه و از هر خطری محافظت خواهید شد. لذا نیاز است که دائم ترفندهای جدید دشمن رصدشده و در پیکربندی، اصلاحات لازم انجام شود و کارکنان نیز نسبت به آن و اهمیت به‌کارگیری آن به‌طور کامل و مطمئن توجیه شوند.[۱]

---

۱ - سایت فناوری اطلاعات ایران

امنیت

زندگی اجتماعی، بشر را از زوایای مختلف و با ابزارهایی متفاوت می‌توان تجزیه و تحلیل کرد. مثلا از زاویهٔ نیازهای بشری با ابزارهایی نظیر جامعه‌شناسی یا روان‌شناسی اجتماعی یا علم سیاست و... می‌توان بشر و اجتماعات بشری را مورد بررسی قرار داد. نکتهٔ جالب توجه این است که از هر یک از زوایا و با هر یک از ابزارها که این بررسی‌ها صورت بگیرد؛ برخی از مفاهیم که جزء نیازهای اولیه انسان‌هاست به‌طور مشترک طرح و بررسی می‌شود. اگرچه شاید از نظر تعبیر و استخدام کلمات و عبارات متفاوت باشند ولی از نظر مفهوم تلقی واحدی را ارائه می‌کنند. یکی از این مفاهیم، «امنیت» است که اگر از زاویه نیازهای بشری بنگریم؛ ازجمله نیازهای اولیه انسان‌ها، نیاز به امنیت است. اگر از زاویه تمدن و حکومت‌داری نگاه کنیم، امنیت از اولین مباحث است و از زوایای دیگر همین‌گونه است.

عموما در اذهان برای تصویر و تصدیق امنیت، جلوه‌های علمی آن مورد بررسی قرار می‌گیرد. در واقع بیشتر مباحث در بخش امنیت دیده می‌شود. ناامنی و اخلال در حول امنیت است. شاید بتوان به عموم حق داد که این‌گونه فکر کنند. ولی بدیهی است که خواص اهل تحقیق و به‌خصوص نظریه‌پردازان اطلاعاتی نباید از توجه به نگاه اثباتی غافل شوند. در این‌حال چون بهره‌گیری عام، ملاک است و چون قصدی بر نظریه‌پردازی نیست، لذا سعی در ارائه مفاهیم قابل‌تصور و حتی در برخی موارد قابل‌تجسم خواهد بود. جایگاه بحث امنیت در جامعه تقریبا مورد وقوف همه صاحب‌نظران، کارشناسان و حتی توده مردم می‌باشد. چرا که این اعتقاد همگانی وجود دارد که امنیت از ارکان اصلی برقراری روابط اجتماعی و ادارهٔ جوامع است. در مبانی اسلام هم موکدا و مکررا این نکته گوشزد شده است. وجود آن و ضرورت آن هم به نوعی است که از شدت وضوح و ظهور، گاهی مورد غفلت واقع می‌شود. مثل نور و روشنایی که آن‌قدر با زندگی دنیایی بشر عجین است که کمتر کسی به‌دنبال اثبات وجود یا ضرورت آن می‌رود. در احادیث مذکور این تعبیر بسیار دقیق آمده است که نعمت سلامتی و نعمت امنیت ناشناخته و مجهول هستند. شاید این جهل به اهمیت و ارزش آن باشد؛ هم به وجود آن و هم به نقش آن.

مفهوم امنیت

یکی از خصوصیات بارز مفاهیم موجود در علوم اجتماعی و انسانی، تحول‌پذیری آنهاست. مفهوم امنیت نه‌تنها از این قاعده مستثنی نیست، بلکه تا اندازه‌ای نسبت به مفاهیم دیگر دچار تحولات بیشتری شده است.

در این تحولات مفهومی، عوامل زیادی دخیل هستند که می‌توان ازجمله آنها تغییرات در فرهنگ ملل و انسان‌ها را ذکر کرد. تغییرات در نوع تمدن‌ها، تغییرات در پیشرفت تکنولوژی و حتی نوع گرایش انسان‌ها به ادیان و مذاهب؛ همگی در تغییر مفهوم امنیت دخیل بوده و هستند. نکته مهم آن است که امنیت ابتدا تلقی ساده‌ای داشته است. پیشتر و بیشتر، از امنیت، مفهوم تامین و آسایش فردی تلقی می‌شده، ولی امروزه که انسان اجتماعی‌تر شده است و جوامع انسانی پیچیده‌تر گردیده‌اند (از روستاهای کوچک به روستاهای بزرگ و از روستاها به شهرها و تا جایی که امروز ابرشهرها مطرح شده‌اند) و از سویی به تناسب ارتباطات جوامع و عناصر تشکیل‌دهنده آنها (یعنی انسان‌ها) فزونی یافته است، مفهوم امنیت نیز پیچیده‌تر شده و جلوه‌های جمعی و اجتماعی امنیت بر جلوه‌های فردی آن پیشی گرفته است.

برای امنیت، تعریف واحد و مشخصی ارائه نشده است؛ گاهی این تصور پیش می‌آید که اصولا امنیت از مفاهیم و موضوعات اولیه است و قابل تعریف نیست. ولی آنچه که می‌توان اذعان کرد مشکل‌بودن تعریف امنیت و پیچیدگی آن است و حتی گاهی برای تعریف امنیت از شیوه سلبی و جلوه‌های عدمی استفاده می‌شود.

واژه امنیت دارای مفهوم روشن است، مفاهیمی چون؛ آسایش‌خاطر، اطمینان، استواری، بی‌خطری، حفاظت، محکم نگاه‌داشتن و اقدامات تأمینی (مجیدی‌نظامی، ۱۳۹۱)

در لغت‌نامه "دهخدا"، برای واژه امن، معانی زیر را نقل می‌کند: ایمن‌شدن، بی‌هراس‌شدن، بی‌بیم‌شدن، اطمینان (http://fa.wikipedia.org) و در توضیح واژه امنیت چنین آورده است: بی‌خوفی و امن، بی‌بیمی و ایمنی (http://www.ircert.com).

در انگلیسی از واژه Security درباره امنیت استفاده می‌شود. در "آکسفورد" مفاهیمی چون احساس امنیت، رهایی از اضطراب و نگرانی، حفاظت‌کردن در مقابل سارق، حمله، جنگ و نیز وثیقه در قرض آمده است.

در "مریم وِبستر" (Merriam Webster) در بخش تزاروس در توضیح Security به‌ترتیب سه معنی برای آن ذکر می‌کند: اقدامات دفاعی، تضمین لازم جهت انجام تعهدات، درمعرض خطرنبودن (http://www.loghatnameh.com).

امنیت را می‌توان به‌وسیله فقدان آن (ناامنی) تعریف کرد. یعنی هرجا که ناامنی نیست، امنیت وجود دارد. وجود جنگ، خشونت، زد و خورد، منازعات مرزی و بی‌ثباتی داخلی از علائم ناامنی هستند که عدم آنها مساوی با امنیت است. بدیهی است با این‌گونه تعاریف نمی‌توان درجه امنیت و ناامنی را اندازه‌گیری کرد. چراکه براساس تعریف فوق، دو حالت بیشتر متصور نیست، یا امنیت وجود دارد و یا با وجود یکی از علائم مذکور، امنیت سلب شده است. برای واحدهای سیاسی، محصورنبودن امنیت در چنین قالب محدودی معقول به‌نظر نمی‌رسد. زیرا باوجود آنکه تمامی شهرها و حتی کشورها به نوعی با این عوامل ناامنی مواجه هستند، اما همه آنها را نمی‌توان ناامن دانست.

اصولا امنیت یک مفهوم نسبی است نه مطلق. یعنی در بیان ناامنی یا وجود امنیت باید حالتی را با حالت دیگر سنجید و جامعه‌ای را با جامعه دیگر مقایسه کرد. از همین جاست که می‌بینیم تعریف امنیت یا ناامنی یک تعریف قراردادی است. یعنی ممکن است وضعیتی برای یک جامعه امنیت محسوب شود ولی برای جامعه دیگر ناامنی و بالعکس باشد. حتی شاید در برخی عوامل دخیل در امنیت تفاوت‌هایی باشد. مثلا یک جامعه چند عامل؛ جنگ، زد و خوردهای مسلحانه و نزاع‌های گسترده را ناامنی بداند ولی جامعه دیگر سرقت‌ها و یا مفاسد اخلاقی را هم دلیل بر ناامنی بدانند. یا اینکه حداقل وزن و اهمیت عوامل در جوامع مختلف متفاوت باشد. از نکات قابل‌توجه در مفهوم امنیت این است که امنیت خودش متغیر برخی توابع دیگر محسوب می‌شود. مثلا می‌توان یکی از متغیرهای توسعه‌یافتگی یا تمدن را اهمیت دانست. ازطرفی اهمیت خودش تابعی است چندمتغیره که ارتباط این متغیرها با یکدیگر و تاثیر آنها در تابع امنیت نیز ارتباطی غیرخطی است. البته ممکن است متغیرهای امنیت، خودشان تابعی از متغیر دیگری باشند.

گاهی امنیت از نگاه ارزشی دیده می‌شود، شامل؛ حفظ جان مردم، حفظ تمامیت ارضی، حفظ سیستم سیاسی و اقتصادی؛ حفظ استقلال و حاکمیت کشور تلقی می‌شود. گاهی امنیت را نه‌تنها حفظ ارزش‌ها بلکه خود ارزش‌ها می‌دانند. با این تعبیر، امنیت یعنی عدم نگرانی از اینکه

چنین ارزش‌هایی مورد حمله قرار گیرد. برخی امنیت را ارزش یا خدمات نمی‌دانند، بلکه آن را شرایطی می‌پندارند که کشور با دارابودن آن احساس ترس نکند و از نفوذ دشمن در امان باشد. برخی امنیت را از مقوله هدف و برخی هم امنیت را نظم و ثبات می‌دانند.

باتوجه به همه جوانب از تعریف امنیت شاید بتوان جمع‌بندی زیر را ارائه نمود:

« امنیت، شرایط و فضایی است که یک جامعه با داشتن آن قادر است اهداف و ارزش‌های مهم و حیاتی خود را محقق کند و در سطح جامعه گسترش دهد و یا حداقل آنها را در برابر تهدیدات و آسیب‌پذیری‌ها (بالقوه و بالفعل و در مقابل عوامل داخلی و خارجی) حفظ نماید.»

در تعریف فوق نکات زیر قابل توجه است:

۱- شرایط و فضای مناسب

۲- اهداف و ارزش‌های مهم و حیاتی

۳- تهدیدات و آسیب‌پذیری‌ها

۴- منابع و آسیب‌پذیری‌های بالفعل و بالقوه داخلی و خارجی

۵- محافظت از تمامیت ارضی

بدیهی است هر یک از نکات فوق برای هر جامعه‌ای می‌تواند متفاوت باشد و این، به نگاه و دید کارشناسان آن جامعه و مسئولان آن بستگی دارد. حال این سئوال مطرح می‌شود که آیا امنیت خود یک هدف است و یا اینکه حافظ و نگهبان اهداف ملی دیگر است؟ مثلا اگر جامعه‌ای یا کشوری چهار هدف عمده و اساسی حفظ امنیت ملی، تمامیت ارضی، حاکمیت سیاسی و تأمین منافع ملی داشته باشد، آیا ممکن است امنیت ملی خدشه‌دار شود، اما اهداف دیگر همچنان باقی باشند؟ جواب این سئوال به‌طور قطع منفی است چرا که اهداف مذکور در ارتباط با امنیت ملی هستند.

از طرف دیگر این دیدگاه که حفاظت از اهداف هم توسط امنیت انجام می‌شود، کافی نیست چرا که امنیت فی‌نفسه یک ابزار عینی نیست که با دستیابی به آن بتوان اهداف را حفظ و گسترش داد. البته میان اهداف و امنیت رابطه مستقیم برقرار است. یعنی به میزان ارزش و اهمیتی که برای اهداف قائل هستیم، تأمین امنیت نیز به همان ترتیب خواهد بود.

نکته مهم‌تر این است که بین امنیت و قدرت، رابطه مستقیم وجود دارد. قدرت به مفهوم عِده و عُده برای حفظ و برقراری امنیت است، ولی رابطه بین امنیت و اقتدار (امکان به‌کارگیری قدرت) مستقیم‌تر است.

مطلبی که ذکر آن خالی از لطف نیست آن است که ذهنی‌بودن مفهوم امنیت گاهی باعث اشتباه می‌شود. گاهی تهدیدات و آسیب‌های کاذب جلوه‌گر می‌شوند. چه‌بسا جوامعی که هیأت‌های حاکم آنها به‌دلائل مختلف یا از روی جهل، عدم شناخت و یا به عمد چیزی را برای امنیت تهدید بدانند، در حالی‌که تهدید واقعی چیز دیگری باشد. یکی از ترفندهای استعمار نو در دنیای امروز وارونه جلوه‌دادن تهدیدات است. گاهی از تهدیدات و آسیب‌پذیری‌ها و حتی شرایط امنیتی و ناامنی غفلت می‌شود و گاهی فریبندگی موجب تبلیغ ناصحیح از ناامنی‌ها می‌شود.

ازطرفی گاهی منبع تهدید عمدتا به خارج از هر کشوری احاطه می‌شود و این تأثیر خارجی را گاهی ناشی از محیط بین‌الملل و فعل و انفعالات ناشی از آن دانسته و گاهی ناشی از اعمال نفوذ دشمنان کشور می‌دانند. این مطلب از حیث دشمن‌شناسی و کوچک‌نگرفتن دشمن درخور توجه است. ولی باید دقت نمود که موجب غفلت از ریشه‌های اصلی ناامنی و ضعف‌ها در داخل کشور که معمولا هم اقتصادی، سیاسی، اجتماعی و فرهنگی هستند، نشود.

امنیت یک کشور قبل از مرحله سیاست‌گذاری، تصمیم‌گیری و عمل به آن؛ ممکن است بسته به تعداد گروه‌ها و افراد آن کشور، متنوع و متفاوت باشد. یعنی هر شخصی و یا جمعی بنا به شرایط خود استنباط و تلقی مخصوص از امنیت داشته باشد. اما هنگامی که این تلقی‌ها بخواهد جنبه عملی پیدا کند و به سازوکارهای اجرایی تبدیل شود، آن‌گاه حاکمان جامعه و مسئولین ذی‌ربط تعیین‌کننده مفهوم امنیت خواهند بود. چرا که تأمین امنیت از وظائف اولیه حاکمیت و دستگاه دولتی محسوب می‌شود و بالطبع اختیارات لازم نیز در اختیار هیأت حاکمه می‌باشد. چنانچه اقتدار دولت درحد مطلوبی باشد، خود به خود تلقیات و ابتکارات افراد و گروه‌ها با محدودیت‌های اجرایی مواجه می‌شود و البته همین‌جاست که حاکمان جامعه، چنانچه اگر از یک گروه و دسته خاص سیاسی باشد، می‌توانند امنیت جامعه و کشور را با امنیت گروه خود تغییر دهند و بدیهی است اگر بر جامعه، ارزش‌ها حاکم باشد و گروه‌گرایی‌ها و قدرت‌طلبی‌ها ملاک نباشد در واقع بین اهداف مردم و مسئولین، یکسانی یا حداقل اشتراک زیاد یا شباهت

زیادی وجود داشته باشد. در آن‌صورت امنیت هیأت حاکمه مترادف با امنیت کشور و امنیت مردم است و ازطرفی همدلی و هم‌راستایی مردم با حکومت موجب ارتباط مستمر بین مردم و مسئولین می‌شود که این خود موجب تقلیل خطای تصمیم‌گیرندگان و اقتدار بیشتر حکومت خواهد شد.

انواع امنیت

بررسی ابعاد امنیت نیاز به شناخت سطوح آن دارد، واقعا امنیت را باید در کجا جستجو کرد؟ اندیشمندان موضوعات امنیتی، سطوح مورد بحث امنیت را در دو رده اصلی و فرعی می‌یابند: امنیت دارای انواعی است که البته از دیدگاه‌های مختلف دسته‌بندی شده است. گاهی مراد از انواع امنیت، سطوح امنیت است که امنیت را به پنج بخش تقسیم می‌کنند:

در این بحث ۵ سطح امنیت قابل جستجو و مباحثه است که عبارتند از:

۱- امنیت فردی:

یعنی حق زنده‌ماندن، استفاده‌کردن از حقوق شهروندی در هر کشور، بهره‌برداری از متون و امتیازات اعلامیه جهانی حقوق بشر. منظور از مصونیت فردی یا امنیت شخصی یا آزادی فردی به معنای اخص کلمه این است که فرد از هرگونه تعرض و تجاوز مانند قتل، جرح، توقیف، حبس، تبعید، شکنجه و سایر مجازات‌های غیرقانونی و خودسرانه و یا اعمالی که منافی شئون و حیثیت انسانی اوست مانند اسارت، تملک، بهره‌کشی، بردگی، فحشاء و... مصون و در امان باشد (علوی‌فر، ۱۳۸۵: ۲۲-۲۰).

۲- امنیت اجتماعی:

یعنی بهره‌برداری از سطح قابل قبولی از امنیت در جامعه که شامل اعضای خانواده، محیط سکونت، محیط شغلی، مسیرهای تردد و امثال آن باشد.

امنیت اجتماعی و انواع آن: اگر همچنان که در امنیت فردی ذکر شد، امنیت فردی را آن‌گونه که هست نشناسیم، دیگر جایی برای امنیت اجتماعی باقی نمی‌ماند؛ زیرا همه انواع امنیت، رنگ فردی به‌خود می‌گیرد. اما اگر بپذیریم که امنیت فردی عبارت است از آرامش و آسودگی‌ای که فرد برای خود فراهم می‌سازد، سخن از امنیت اجتماعی معقول است (طباطبائی، ۱۳۷۵: ۵۰).

بنابراین آرامش و آسودگی‌ای که جامعه برای اعضای خویش فراهم می‌کند را می‌توان امنیت اجتماعی دانست. چنان که در این‌باره آمده است:" هدف جامعه حفظ حقوق طبیعی و غیرقابل مرور زمان بشر است، این حقوق عبارتند از آزادی، مالکیت و تعامل در برابر ستم." ماده ۱ اعلامیه حقوق بشر شهروندان فرانسه: - در ماه هشتم اعلامیه حقوق بشر و شهروند فرانسه آمده است - "امنیت عبارت است از حمایتی که جامعه به هر یک از افراد و اعضاء خود برای حفظ جان، حقوق و دارایی آنها اعطاء کرده است."

پیرامون امنیت اجتماعی و برخی از انواع آن آمده است که" امروز مفهوم امنیت از نظر صوری و ظاهری در اجتماع و تنها بعضی فقدان جرائم و تخلفات فراتر رفته و شامل موارد و مصادیقی از نظر روحی، اخلاقی، بهداشتی و اقتصادی و بالاخره ایجاد ثبات و نظم واقعی و معقول در اجتماع شده است که از آن به امنیت اجتماعی تعبیر می‌شود." (همان)

امنیت اجتماعی همچون سایر پدیده‌ها و امور اجتماعی دارای گونه‌های مختلفی است امنیت اجتماعی نیز شامل امنیت شغلی، اقتصادی، سیاسی و قضایی است که در زیر توضیح مختصری برای هر یک درنظر گرفته شده است:

- **امنیت شغلی:** امنیت شغلی نقش اساسی در برقراری آرامش و آسایش انسان بازی می‌کند، زیرا نبود شغل برابر است با عدم تأمین نیازهای اولیه که برای بقا و ادامه آن ضرورت دارد و عدم تأمین این نیازها برابر است با گرسنگی، رنج و مرگ که همه برهم‌زننده آرامش و آسایش انسان و موجب تشویش و نگرانی او است. بنابراین، وجود شغل برای هر انسانی یکی از ابزارهای استقرار آرامش و آسایش است و امنیت شغلی، گونه‌ای از امنیت اجتماعی است.

- **امنیت اقتصادی:** عبارت است از برقراری روابط منظم بین عوامل اساسی تهیه مایحتاج انسان به‌طوری که لوازم و نیازهای ضروری آنها تأمین شود و آنها از این جهت خود را در خطر احساس نکنند.

- امنیت سیاسی: عبارت است از آنکه، هر عنصری از جامعه بتواند بدون هیچ‌گونه بیم و هراس، در چارچوب قانون، نظرات خویش را پیرامون چگونگی اداره امور جامعه ابراز دارد

و از این جهت خطری او را تهدید نکند و آرامش و آسایش او برهم زده نشود و مورد آزار و اذیت قرار نگیرد.

- **امنیت قضایی:** عبارت است از ایمنی و مصون‌ماندن فرد از هرگونه تعرض، تجاوز، ارعاب و تهدید نسبت به جان، مال، ناموس، آزادی، شرف، حیثیت، شغل، مسکن و به‌طور کلی تمامی حقوق قانونی و مشروع او. و این مهم هنگامی تحقق خواهد یافت که جرایم، بزه‌ها، تخلفات، نیرنگ‌ها و انواع تقلب و فساد و ریشه‌های ارتکاب آن در جامعه ریشه‌کن شود و عواملی که سبب زیان مالی، جانی، معنوی و روانی می‌شود از بین برود و محیطی امن و آرام به‌جود آید.

۳- امنیت ملی:

منظور امنیت مجموعه یک کشور از دیدگاه‌های مختلف است. یعنی امکان استفاده از منافع ملی بدون درگیری با دشمن خارجی و بدون قربانی‌کردن یا صرف‌نظر از منافع عمومی کشور است.

۴- امنیت منطقه‌ای:

منظور امنیت یک مجموعه از کشورها در یک منطقه از دنیاست. یعنی بهره‌برداری از حوزه‌های منافع مشترک بین کشورهای یک منطقهٔ خاص بدون بروز تنش‌های ناشی از جنگ و تولید بحران‌های منطقه‌ای یا دخالت بیگانگان می‌باشد.

۵- امنیت بین‌المللی:

یعنی محافظت انسان در قبال خطراتی که مرز نمی‌شناسد و انسان را در هر لباس، مکان، نژاد یا زبانی مورد تهدید خود قرار می‌دهند. از امثال چنین تهدیداتی می‌توان به پدیده گرم‌شدن زمین، پارگی لایهٔ اوزون، پدیده گازهای گلخانه‌ای و حتی برخی از بیماری‌های خطرناک مانند ایدز اشاره نمود.

گاه امنیت کشور به دو بخش امنیت داخلی و امنیت ملی تقسیم می‌شود و سپس امنیت داخلی به امنیت فردی و اجتماعی یا عمومی تقسیم می‌شود. البته همان‌طور که از مفهوم امنیت تلقی‌های متفاوتی هست - که برخی از آنها ذکر شد - از مفاهیم امنیت فردی، امنیت ملی، امنیت عمومی یا امنیت اجتماعی و... نیز برداشت‌های مختلفی وجود دارد.

گاهی حتی آسایش عمومی و فردی را هم از جنبه‌های امنیت می‌شمارند. گاهی هم تقسیم‌بندی از نظر موضوع انجام می‌شود و امنیت اقتصادی و سرمایه‌گذاری، امنیت شغلی و... هم مطرح می‌شود.

تذکر این نکته ضروری است که در نگاه به هر یک از انواع امنیت باید دیدگاهی سیستماتیک داشت یعنی امنیت را یک سیستم تعریف کرد. برای آن ورودی‌هایی را مشخص نمود، نقاط مطلوب یا شاخص‌ها یا اصطلاحا set point تعریف کرد، اجزاء سیستم را شناخت، زیرسیستم‌ها را معین کرد، تعاملات و فرایندها را روشن کرد، براساس شاخص‌ها نقاط بررسی‌کننده یا حساس گرها (سنسور) را معین کرد، چگونگی بازخوردها و تعیین حلقه‌های آن را انجام داد و نهایتا با روش تجزیه و تحلیل سیستمی، بررسی آن انجام شود.

در همین‌جا بحث کنترل‌ها و اینکه تا چه حدی خودکنترلی[1] باشد و تا چه‌حدی کنترل‌ها باید از بیرون اعمال شود را باید معین نمود تا بتوان یک سیستم امنیتی مطلوب با خصوصیاتی همچون یکپارچگی، پویایی، به‌روز بودن، سرعت، دقت و انعطاف پیاده شود.

طبقه‌بندی یگانه‌ای از امنیت وجود ندارد. برخی امنیت را از نظر جغرافیایی مدنظر قرار داده و آن را به دو گونه امنیت داخلی و امنیت خارجی تقسیم‌بندی کرده‌اند. مقصود آنان از امنیت داخلی، برقراری نظم، آرامش و ایمنی در درون سرزمین است و منظور از امنیت خارجی وجود همین آرامش، ایمنی، آسودگی و مصونیت از خطر در خارج از سرزمین است. عده‌ای نیز امنیت را از نظر محل استقرار آن و عامل به‌وجودآورده، طبقه‌بندی کرده‌اند. در این نظر امنیت به دو شکل درونی و بیرونی تقسیم می‌گردد. امنیت درونی آن شکلی از امنیت است که در درون انسان استقرار می‌یابد و به‌وسیله خود انسان ایجاد می‌گردد. امنیت بیرونی آسودگی و آرامش در اثر عوامل خارج از انسان است.

سطوح امنیت

نه تنها امنیت را در سطوح کلی فوق می‌توان مورد بررسی و کالبدشکافی قرار داد، بلکه اگر این واژه عجیب و معماگونه قبل از هر کلمه دیگری قرار گیرد سطح تازه‌ای از امنیت را یادآوری می‌کند که تا پیش از آن به فکر کسی خطور نمی‌کرد، اما خصلت معماگونه امنیت ایجاب

1 - self control

می‌کند که همواره ناشناخته بماند مگر آن‌که نقض گردد، آنگاه واژه‌سازان با افزودن کلمه امنیت به لغت موردنظر، انبوهی از معنا را در عالم امنیت به ارمغان می‌آوردند.

به‌عنوان مثال؛ حتما شما هم در روزنامه‌ها کلمه‌ای بنام امنیت شغلی را دیده‌اید، این واژه زمانی وارد تیترها شد که ابتدا برخی از کارمندان یا کارگران به‌دلیل از دست‌دادن شغل خود دچار نگرانی شدند، از آن زمان صحبت امنیت شغلی به میان آمد.

مثال‌های دیگر؛ امنیت کودکان، که با کار اجباری کودکان در کوره‌پزخانه‌ها مطرح می‌شود.

* امنیت زنان، که با تعدی به حقوق زنان مطرح شد.
* امنیت جاده‌ها، که با قتل برخی از رانندگان بین شهری مطرح گردید.
* امنیت مواد غذایی، که با انتشار مواد غذایی ناسالم در شهرها مطرح شد.
* امنیت فرهنگی، که با انتشار نوارهای مستهجن مورد تکیه واقع شد.
* امنیت اقتصادی، که همواره با تحریم‌های اقتصادی بیگانگان طرح گردیده است.
* امنیت نظامی، که با احتمال بروز تهدید خارجی مورد مباحثه واقع می‌شود.

در تمامی موارد بالا هر بار در برخورد با یک نارسایی، تهدید یا معضل ساختاری در جامعه به‌وقوع پیوسته، کلمه امنیت پیشوند کلمه دیگر واقع شده و معنایی تازه به واژگان بخشیده است.

همین امر می‌تواند دلالت بر فراگیربودن مفهوم امنیت داشته تا اثراتی فراوان بر کلیه ارکان زندگی فردی یا سطح بین‌المللی و در هرجا از زندگی خصوصی خود، نزدیکان و جامعه اعم از محل سکونت، شغل یا تردد یا تحصیل تا صرف مواد غذایی اختیار نماید.

امنیت اطلاعات

اصطلاح "امنیت اطلاعات" حوزه گسترده‌ای از فعالیت‌های سازمانی، محصولات سازمان و سرمایه‌های آن، فرایندهای تعریف‌شده برای جلوگیری از دستیابی‌های غیرمجاز، تغییر و حذف اطلاعات را شامل می‌شود. حوزه امنیت اطلاعات درگیر حفاظت از منابع شبکه و جلوگیری از هم‌گسیختگی و به‌هم‌خوردگی آن، در برابر پیشامدها و حوادث و حملاتی است که ممکن است تا حد زیادی از کنترل مسئول امنیت اطلاعات، خارج باشد و باید با تدبیر و پیش‌بینی لازم

درصد ریسک خطر در این حوزه را کاهش داده و برای مقابله با خطر، طرح و برنامه مدون و شفاف در زمینه: پیشگیری، مواجهه، پاکسازی، ترمیم و بهینه‌سازی داشته باشد.

موضوع تأمین امنیت اطلاعات بر سه پایه فیزیکی، عملیاتی و مدیریتی استوار است که هر کدام به بخش های مختلف امنیت رایانه مربوط می شود. طرح کلان امنیت رایانه و فرایند آن باید خطرات را ارزیابی کند و دارای استراتژی و روش هایی برای تبیین آن باشد.

پایه‌های سه‌گانه امنیت اطلاعات

موضوع امنیت فناوری اطلاعات، در سه سطح: فیزیکی[1]، عملیاتی[2]، و مدیریتی[3] قابل بررسی است (Pastore and Dulaney: 4 – 12). هر کدام از این سه سطح به‌عنوان پایه‌های تأمین امنیت در حوزه فناوری اطلاعات و ارتباطات جایگاه خاص خود را دارد به‌نحوی که با اختلال در هر یک، امنیت کل سیستم درمعرض خطر قرار خواهد گرفت. از این‌رو لازم است که مدیران دست‌اندرکار، به هر یک از این سه پایه عنایت و توجه کافی داشته باشند.

درک نیاز، شناخت موقعیت و هوشیاری نسبت به خطرهای در کمین‌نشسته و حوادث مترقب و غیرمترقب و تأمین هزینه‌های هر یک از این موارد در پیشگیری از بروز فاجعه؛ از بین‌فتن اطلاعات، لورفتن اطلاعات و یا جابجایی و دست‌کاری آن، مؤثر خواهد بود:

- حوزه فیزیکی شامل: رایانه، تجهیزات فعال و غیرفعال شبکه، اتاق سرور و نیز تجهیزات امنیتی (قفل، کنترل از راه دور، سنسور، هشدار، خنک‌کننده، اطفای حریق و...).

- حوزه عملیاتی شامل: نصب نرم‌افزارهای لازم، کنترل دسترسی به منابع شبکه و دسترسی به شبکه‌های دیگر، اعتبارسنجی، نحوه چینش و سازماندهی شبکه، پشتیبان‌گیری و بازیابی اطلاعات.

- حوزه مدیریتی شامل: برنامه و دستورالعمل صریح، شفاف و ریزشده مدیریتی کلان سازمانی و مدیریت شبکه، متناسب با سیاست‌های سازمان و اهداف و مأموریت‌های ابلاغ شده.

در ادامه توضیح اقدامات لازم در این سه حوزه می‌آید:

---

1 - Physical
2 - Operational
3 - Management

– امنیت شبکه در حوزه فیزیکی

هدف امنیت اطلاعات در سطح فیزیکی عبارت است از حفاظت از اطلاعات در مقابل دسترسی افراد غیرمجاز به تجهیزات فیزیکی. ثبت، مدیریت اطلاعات، جلوگیری از سرقت و دستبرد و یا تخریب آن. مدیر مربوطه در این مرحله، مسئولیت حفظ و نگهداری تجهیزات فیزیکی را به‌عهده دارد تجهیزاتی که قابل‌دیدن، لمس‌کردن، ربودن و انتقال فیزیکی است. در این سطح کسانی که می‌توانند به‌عنوان تهدید محسوب شوند عبارتند از: نیروهای خدمات فنی، نیروهای خدماتی مانند دربان و سرایدار، مشتری، فروشندگان دوره‌گرد، کارمندان داخلی. این افراد می‌توانند به تجهیزات دستبرد بزنند (در میان سطل زباله به‌دنبال ورق پاره‌ها بگردند و یا به قفسه‌های بایگانی دستبرد بزنند)، تخریب کنند یا اسناد را از اداره به بیرون از مجموعه انتقال دهند. انگیزه این افراد می‌تواند متفاوت باشد، بدگمانی، بدست‌آوردن اطلاعات طبقه‌بندی‌شده و فروش به دشمن به‌منظور کینه و انتقام، یا صرف طمع در سود مالی آن.

مؤلفه‌های سه‌گانه حفاظت فیزیکی:

در حفاظت فیزیکی باید به سه مؤلفه به‌عنوان ارکان این کار توجه نمود و برای هر کدام برنامه‌ای خاص داشت:

الف) حفاظت ساختمان، تجهیزات، اسناد و مدارک فیزیکی شبکه؛ اولین مؤلفه امنیت فیزیکی آن است که اتاق شبکه به‌علت نقایص حفاظتی به‌عنوان یک هدف وسوسه‌انگیز برای نفوذ و دستبرد قرار نگیرد. در ادارات و ساختمان‌هایی که بیشتر اوقات درب آن، باز است و تردد به آن آسان است باید بیشتر مراقب درها بود و سیستم نظارتی و هشداردهنده باید نصب شود همچنین برای استفاده از آسانسور و دسترسی به سایر طبقات که تجهیزات و تأسیسات مهم در آن قرار دارد باید از کلید، نشان و کد ویژه‌ای استفاده نمود.

اهم عوامل مؤثر در تأمین امنیت فیزیکی به شرح زیر است:

- نظارت و کنترل تردد افراد به اداره
- نصب سیستم‌های امنیتی، محدودکردن ورود به مکان‌های حساس و نظارت و کنترل آن
- گماشتن نگهبان در ساعات غیراداری
- استفاده از چند نوع قفل و ترکیبی از قفل‌های الکترونیکی و رمز عبور

- تهیه دستگاه خردکننده اسناد غیرضرور و نابودکردن آن (بجای پاره‌کردن و انداختن در سطل معمولی زباله)

ب) کشف و شناسایی؛ دومین مؤلفه و رکن امنیت فیزیکی، کشف نفوذ یا سرقت است و این که چه چیزی نقض‌شده است؟ چه خطایی رخ داده است؟ و اینکه آن خطا چگونه اتفاق افتاده است؟ تصاویر ضبط‌شده ویدئویی یک وسیله خوب برای به دست آوردن اطلاعات است.

ج) اصلاح و ترمیم؛ سومین مؤلفه و جزء امنیت فیزیکی، ترمیم خرابی‌های ناشی از سرقت و ازبین‌رفتن اطلاعات، همچنین ترمیم خسارات وارده به سیستم‌ها و بازگشت به حالت عادی و بازدهی می‌باشد. زمان این کار بستگی به نوع تخریب دارد از باب مثال درصورتی‌که خرابکار، اتاق سرور را با آتش یا آب تخریب کرده باشد وقت زیادی جهت راه‌اندازی مجدد و ادامه کارهای عادی صرف نخواهیم داشت. اگر طرح مدونی برای مقابله با شرایط بحرانی یادشده همچنین موارد دیگر بحران مثل زلزله و... جهت حفاظت و بازیابی اطلاعات آماده نشده باشد. داشتن نسخه‌هایی مجزا در طول زمان‌های متعدد و در چندین مکان متفاوت برای این منظور، بسیار مفید و ضروری است.

– امنیت شبکه در حوزه عملیاتی

موضوع امنیت اطلاعات در حوزه کارهای عملیاتی، با دیگر مسایل اجرایی، مدیریتی سازمان و امور جاری آن ارتباط دارد و معمولا درخصوص هزینه‌کرد لازم برای تهیه تجهیزات و امکانات سخت‌افزاری و نرم‌افزاری مورد نیاز، درصورت عدم‌توجیه کافی با دشواری همراه خواهد بود. متاسفانه بیشتر سیستم‌های کاری تعریف‌شده در این حوزه یا آسیب‌پذیرند، یا ضعیف‌اند، یا از داشتن سیاست‌کاری و دستورالعمل امنیتی مناسب دارای پشتوانه کافی جهت اجرا، محروم‌اند.

– امنیت در حوزه مدیریتی

حوزه مدیریت و سیاست‌گذاری، وظیفه تدوین و آماده‌سازی ضوابط، شیوه‌نامه‌ها و هدایت امور به‌منظور آماده‌سازی محیطی امن برای مجموعه را برعهده دارد. البته باید توجه داشت که تهیه دستورالعمل شرط لازم کار (نه شرط کافی) است و برای ثمربخشی آن، نیاز به پشتیبانی کامل و ضمانت‌های اجرایی کافی است. تدابیر متخذه در این حوزه، تأثیر عمده‌ای در سراسر بخش‌های سازمان روی روحیه اعضاء، نحوه همکاری‌ها و نیز خروجی‌های آن، خواهد داشت و باید مورد توجه خاص سازمان و اعضای آن باشد. سازمانی که به امور رفاهی کارمندان از قبیل

تعطیلات، مرخصی‌ها و... عنایت دارد نسبت به این امر حیاتی، الزاما باید توجه خاص و بیشتری داشته باشد. گرچه واقعیت‌ها گویای چیز دیگری هستند. شاهدش آن است که بیشتر کارمندان، آن مقدار که به امور دیگر، بها می‌دهند به این امر، توجهی ندارند و اگر سازمان، در این خصوص برنامه‌ای جهت توجیه کارمندان خود داشته باشد وضعیت بهتری در ایجاد و تداوم امنیت خواهد داشت و در ادامه موارد مهم امنیتی مربوطه به کلیه اعضاء ارسال‌شده و تأییدیه‌ای مبنی بر اینکه کارمند موردنظر، از مفاد آن کاملا اطلاع یافته است و متعهدشده که طبق آن رفتار نماید، از او گرفته می‌شود که همیشه در ذهن او باشد که چه تعهدی را پذیرفته است.

اهداف سه‌گانه امنیت اطلاعات

اهداف امنیت اطلاعات چارچوب توسعه و نگهداری یک طرح امنیتی را می‌سازد. این اهداف در مقام بیان، آسان ولی در عرصه عمل و اجرا، دشوار به‌نظر می‌رسند.

پیشگیری[1]

پیشگیری هر رخدادی قبل از وقوع آن، آسان‌تر است، گاه یک غفلت می‌تواند علت رخداد یک نقص امنیتی شود. بنابراین، شرط اول امنیت اطلاعات، لزوم هوشیاری درجهت پیشگیری از وقوع هر حادثه بدی است.

کشف – یافت[2]

در بسیاری از مواقع، کشف نقیصه و عیب امنیتی دشوار است، ممکن است حمله‌های ناموفق بسیاری به سیستم شما از مدت‌ها پیش رخ داده باشد و اگر به‌موقع موفق به کشف حمله و رفع نقیصه شوید خواهید توانست پیش از وقوع هر رخداد ناخوشایندی جلوی آن را بگیرید.

واکنش– پاسخ[3]

مرحله سوم مربوط به عکس‌العمل مناسب درخصوص توسعه اصول راهبردی و روش‌های فنی در قبال حمله یا خسارت است. بسته به نوع و شیوه رخداد، شیوه واکنش نیز می‌تواند متفاوت باشد اگر آن رویداد در حد یک تحقیق و آزمایش باشد می‌تواند بیانگر این باشد که حمله‌کننده هنوز در مرحله گردآوری اطلاعات در مورد سیستم شما قرار دارد. این‌گونه حملات می‌تواند

1 - Prevention
2 - Detection
3 - Response

به‌صورت تصادفی و یا هدفمند باشد. درصورتی‌که حملات هدفمند و مداوم باشد، احتمال موفقیت حمله بیشتر خواهد بود و درصورت موفقیت حمله خسارت سنگینی متوجه قربانی خواهد شد. باید بر اساس طرح و برنامه‌ای حساب‌شده جهت بازیابی اطلاعات و از بین‌بردن خطر، تهدید و آسیب واردشده، واکنش مناسب نشان‌داد (Pastore and Dulaney: p13-14).

اهمیت امنیت اطلاعات برای یک سازمان

وجود یک حفرهٔ امنیتی[1] و یا یک مشکل امنیتی، می‌تواند یک سازمان را به روش‌های متفاوتی تحت‌تاثیر قرار دهد. آشنائی با عواقب خطرناک یک حفره امنیتی در یک سازمان و شناسائی مهم‌ترین تهدیدات امنیتی می‌تواند حیات یک سازمان را با مشکل مواجه نماید، ازجمله موارد ضروری به‌منظور طراحی و پیاده‌سازی یک مدل امنیتی در آن سازمان می‌باشد.

وجود حفره‌های امنیتی در یک سازمان، می‌تواند پیامدهای منفی متعددی را برای آن سازمان به‌دنبال داشته باشد ازجمله این پیامدها می‌توان به موارد ذیل اشاره کرد:

- کاهش درآمد و افزایش هزینه
- خدشه به اعتبار و شهرت یک سازمان
- از دست‌دادن داده‌ها و اطلاعات مهم
- اختلال در فرایندهای جاری یک سازمان
- پیامدهای قانونی و تاثیر جانبی منفی بر فعالیت‌های سایر سازمان‌ها
- سلب اعتماد مشتریان
- سلب اعتماد سرمایه‌گذاران

موثرترین راهکار و یا راه‌حل امنیتی، ایجاد یک محیط چندلایه‌ای است. در یک محیط چند لایه، مهاجمان در هر لایه شناسائی و با آنان برخورد خواهد شد. موفقیت یک مهاجم نیز به عبور موفقیت‌آمیز از هر لایه بستگی دارد. راهکار امنیتی چندلایه به "دفاع در عمق" نیز مشهور است. در این مدل، در هر لایه از استراتژی‌های تدافعی خاصی استفاده می‌گردد که باتوجه به ماهیت پویای امنیت اطلاعات، می‌بایست به‌صورت ادواری توسط کارشناسان حرفه‌ای امنیت اطلاعات، بررسی و بهنگام گردند.

---

1 - Security hole

مزایای سرمایه‌گذاری در امنیت اطلاعات

سازمان‌ها و موسسات تجاری با پیاده‌سازی یک استراتژی امنیتی از مزایای زیر بهره‌مند خواهند شد:

- کاهش احتمال غیرفعال‌شدن سیستم‌ها و برنامه‌ها (از دست‌دادن فرصت‌ها)
- استفاده موثر از منابع انسانی و غیرانسانی در یک سازمان (افزایش بهره‌وری)
- کاهش هزینه از دست‌دادن داده‌ها توسط ویروس‌های مخرب و یا حفره‌های امنیتی (حفاظت از داده‌های ارزشمند)
- افزایش حفاظت از مالکیت معنوی

پیاده‌سازی فرایند مدیریت خطرات امنیتی، دستاوردهای متعددی را به‌دنبال خواهد داشت:

- **زمان پاسخ به تهدیدات:**

با ایجاد فرایند مدیریت خطرات امنیتی، سازمان‌ها می‌توانند در مقابل تهدیدات امنیتی جدید در زمان مناسب و به سرعت واکنش لازم را داشته باشند (قبل از سوءاستفاده از تمام محیط شبکه). مدیریت خطرات امنیتی، بستر لازم برای پیشگیری در مقابل تهدیدات و یا آسیب‌پذیری سازمان‌ها را فراهم می‌نماید. بدین‌ترتیب، نحوه برخورد سازمان‌ها با مسائل و مشکلات امنیتی از واکنش‌های انفعالی به واکنش‌های پیشگیرانه تغییر خواهد کرد.

- **مدیریت قانونمند:**

تدوین مجموعه‌قوانین جدید در ارتباط با حفظ حریم خصوصی کاربران، تعهدات مالی و وظایف حقوقی، سازمان‌ها را مجبور می‌نماید که زیرساخت فنآوری اطلاعات خود را با دقت بیشتر و موثرتر از گذشته مدیریت نمایند. بسیاری از سازمان‌ها دارای تعهدات قانونی به‌منظور پیاده‌سازی و نگهداری یک سطح امنیتی (حداقل در محدوده عملیاتی خود) می‌باشند. بروز اشکال در مدیریت پیشگیرانه امنیتی، سازمان‌ها را به‌دلیل عدم‌انجام وظایف و مسئولیت‌های قانونی خود درمعرض آسیب حقوقی قرار خواهد داد.

- **هزینه‌های مدیریت زیرساخت:**

فرایند مدیریت خطرات امنیتی، سازمان‌ها را قادر می‌سازد که با یک وضعیت مطلوب، مقرون‌به‌صرفه و در یک سطح قابل‌قبول امنیتی فعالیت‌های جاری خود را انجام دهند. فرایند

فوق همچنین یک مسیر مشخص و پایدار برای سازماندهی و اولویت‌بندی منابع محدود را به‌منظور مدیریت خطرات ارائه می‌نماید. مزایای واقعی پیاده‌سازی مدیریت، خطرات امنیتی زمانی هویدا می‌گردد که سازمان‌ها بتوانند کنترل‌هایی مقرون‌به‌صرفه به‌منظور کاهش تهدیدات امنیتی را پیاده‌سازی نمایند.

- **مدیریت و اولویت‌بندی خطرات:**

مدیریت خطرات امنیتی می‌تواند به یک سازمان کمک نماید که اصول امنیتی را به‌منظور کاهش بیشترین خطرات در محیط مربوطه به‌کار گیرد (نه اینکه از یک رویکرد غیرمنسجم برای ایمن‌سازی عناصر مجزاء در سازمان استفاده گردد).

رویکردهای متفاوت مدیریت خطرات امنیتی

اکثر سازمان‌ها به‌منظور مدیریت خطرات امنیتی از دو رویکرد متفاوت استفاده می‌نمایند:

- **رویکرد انفعالی:**

فرایندی است که براساس آن صرفا" پس از بروز یک حادثه امنیتی به آن پاسخ داده می‌شود. تعداد زیادی از کارشناسان حرفه‌ای فنآوری اطلاعات همواره با این محدودیت مواجه می‌باشند که فعالیت‌ها را به‌گونه‌ای انجام و به‌اتمام برسانند که کمترین مشکل را برای کارکنان ایجاد نماید. پس از بروز یک مشکل امنیتی، کارشناسان فنآوری اطلاعات صرفا" می‌توانند از پیشرفت مشکل جلوگیری نموده و پس از ایزوله‌نمودن آن، مشکل سیستم‌های آلوده را برطرف نمایند. شاید در این رابطه برخی علاقه‌مند باشند که عامل اصلی بروز مشکل را پیدا نمایند، ولی باتوجه به محدودیت زمان و منابع موجود درسازمان، عملا" امکان انجام آن وجود نخواهد داشت. متاسفانه برای بسیاری از سازمان‌ها همچنان رویکردهای انفعالی یک نگرش موثر به‌منظور برخورد با تهدیدات امنیتی است (پس از بروز مشکل در رابطه با نحوه برخورد با آن تصمیم گرفته می‌شود و برای پیشگیری از بروز حوادث از رویکرد خاصی تبعیت نمی‌گردد).

- **رویکرد پیشگیرانه:**

فرایندی است که باعث کاهش خطر آسیب‌پذیری در یک سازمان می‌گردد. مدیریت پیشگیری از خطرات امنیتی دارای مزایای متعددی نسبت به یک رویکرد انفعالی است. در مقابل اینکه منتظر بمانیم تا یک حادثه اتفاق افتد و به آن پاسخ دهیم، احتمال بروز مشکل در

اولین مکان را کاهش خواهیم داد. بدین‌منظور از رویه‌هایی خاص به‌منظور حفاظت از سرمایه‌های مهم سازمان استفاده می‌گردد. با پیاده‌سازی کنترل‌هایی که کاهش آسیب‌پذیری سیستم و سوءاستفاده از آنان توسط نرم‌افزارهای مخرب را به‌دنبال خواهد داشت، امکان سوءاستفاده مهاجمان از فرصت‌های ایجادشده کاهش یافته و پیشگیری لازم در این خصوص انجام خواهد شد.

یک رویکرد پیشگیرانه می‌تواند به یک سازمان درجهت کاهش تعداد حوادث امنیتی در آینده کمک نماید ولی این بدین‌معنی نخواهد بود که چنین مسائلی در آینده اتفاق نخواهند افتاد. بنابراین، سازمان‌ها می‌بایست فرایند پاسخ به حوادث امنیتی را بهبود داده و به‌طور همزمان ایجاد رویکردهای پیشگیرانه درازمدت را در دستور کار خود قرار دهند.

هر سازمان می‌بایست یک چارچوب امنیتی فعال و پویا را برای خود ایجاد و به‌درستی از آن نگهداری نماید. دفاع در عمق، یک چارچوب امنیتی مناسب در این رابطه است. در این مدل، زیرساخت فنآوری اطلاعات یک سازمان به‌عنوان مجموعه‌ای از لایه‌های مرتبط به‌هم درنظر گرفته می‌شود و برای هر لایه مکانیزم‌های امنیتی و حفاظتی مناسبی تعریف می‌گردد.

پنج راه برای تبدیل کارکنان به سرمایه‌های امنیتی برای حفظ اطلاعات

گِلِن کوساکا[۱]، عضو مؤسسه تِرِند میکرو[۲] توضیح می‌دهد که چگونه می‌توان با گسترش آگاهی‌های امنیتی و حمایت کارکنان، از افشای اطلاعات جلوگیری نمود.

تهدید دارایی‌های اطلاعاتی سازمان، هیچ‌گاه به اندازه امروز، جدی و پرهزینه نبوده است. طبق اعلام سایت Attrition.org، که به یکی از سازمان‌های نظارت بر صنعت تعلق دارد، در سال ۲۰۰۷، هم در آمریکا و هم در سایر کشورها، بیش از ۱۶۲ میلیون فقره از کارت‌های اعتباری و شماره‌های تأمین اجتماعی تا پایان ۲۱ دسامبر درمعرض خطر قرار گرفت. مرکز منابع سرقت هویت، بیش از ۷۹ میلیون سابقه را فهرست می‌کند که تا پایان ۱۸ دسامبر ۲۰۰۷ در آمریکا درمعرض خطر قرار گرفته‌اند. این آمار در مقایسه با ۲۰ میلیون سابقه گزارش‌شده در سال ۲۰۰۶ رشد تقریبا چهار برابری را نشان می‌دهد.

---

۱. Glen Kosaka - گِلِن کوساکا، مدیر محصولات حفاظت‌اطلاعات، مؤسسه تِرِند میکرو (Trend Micro)

۲. Trend Micro: یکی از بزرگ‌ترین شرکت‌های ارائه‌دهنده محصولات نرم‌افزاری امنیتی و ضدویروس در دنیا

افزایش بیش‌ازحد سامانه‌های ارسال پیامک، شبکه‌های بی‌سیم و ابزارهای ذخیره‌سازی USB موجب‌شده حفاظت از اطلاعات حیاتی شرکت، از گذشته نیز دشوارتر گردد. شرکت‌ها، به‌طور فزاینده‌ای به نهادهایی «بدون مرز» تبدیل شده‌اند که اطلاعات خود را در سطح جهان، بین کارکنان و شرکا به‌اشتراک می‌گذارند. این شرکت‌های بدون‌مرز همچنان که کارکنان در هنگام سفر، از منزل یا کافی‌شاپ‌ها و سایر مکان‌های بیرونی کار خود را انجام می‌دهند، با این چالش روبرو هستند که بین «انعطاف‌پذیری و صداقت» و «امنیت و مخاطره» تعادل برقرار کنند. در هرحال، بیشترین افشاء و از دست‌دادن اطلاعات حساس توسط کارکنانی صورت می‌گیرد که آموزش ندیده‌اند و بنابراین به‌طور سهوی شرکت خود را درمعرض خطر قرار می‌دهند. از آنجا که بیشتر افشاها تصادفی است، شرکت‌ها این فرصت را دارند تا با آموزش‌دادن کارکنان خود درباره مدیریت مناسب اطلاعات، به‌نحو مطلوب‌تری از اطلاعات خود حفاظت کنند.

در اینجا ۵ روش ذکر می‌شود تا به کمک آنها بتوان کارکنان را بجای آنکه مایهٔ دردسر شوند، به سرمایه‌های امنیتی تبدیل نمود:[1]

۱– امنیت اطلاعات را بخشی از فرهنگ سازمان کنید.

حفاظت از اطلاعات حساس نباید تنها وظیفهٔ نیروهای امنیتی و اجرایی باشد. مدیر هر گروه، مسئولیت کمک به شناسایی و تعیین موقعیت اطلاعات حساس، و ارائه سیاست‌هایی برای دسترسی، به‌کارگیری و حفاظت مناسب از آن اطلاعات توسط کارمندان، را برعهده دارد. هر کارمندی که مشخص‌شده به اطلاعات حساس دسترسی دارد، باید درباره سیاست‌ها و روش‌هایی که معرفِ مراقبت مسئولانه از اطلاعات شرکت است، آموزش ببیند. بدین‌ترتیب، مدیران و کارکنان نه‌تنها در به‌کارگیری اطلاعات حساس، به یک اندازه مسئولند، بلکه علاوه بر آن می‌توانند برای حصول اطمینان از این امر که هر کسی این سیاست‌ها را رعایت می‌کند، نقش مراقب را ایفا کنند.

۲– فرایندهای پیشگیری از افشاء اطلاعات را با گردش کار کلی درآمیزید.

بسیاری از شرکت‌ها کنترل بر اطلاعات حساس خود را از دست داده‌اند زیرا شناسایی، دسترسی و جابجایی اطلاعات حساس با فرایندهای کلی آنان یکپارچه نشده است و درنیامیخته

1- Glen Kosaka

است. مثلاً آیا هنگام ایجاد اسناد یا محتوای جدید، فرایند دسته‌بندی برای تعیین سیاست‌های مناسبی که قرار است اِعمال شوند، وجود دارد؟ یا هنگام پیوستن کارکنان به یک واحد یا جابجایی آنان بین واحدها، فرایندهایی برای حفاظت از اطلاعات و کنترل دسترسی واحدهای جدید و سابق اجرا می‌شود؟ علاوه بر آن، معرفی ابزارهای سیار جدید یا سایت‌های توسعه از راه دور می‌تواند معرّفِ نواحی تهدید جدیدی برای درز اطلاعات باشد. هنگامی که شرکت‌ها دربارهٔ فرایندهای اصلی خود خوب فکر می‌کنند، و گام‌های مناسبی برای حفاظت از اطلاعات برمی‌دارند، ریسک درز و افشای اطلاعات به‌طرز چشمگیری کاهش می‌یابد.

۳– کاری کنید کارکنان خود را سرمایه‌های امنیتی بدانند، نه مایهٔ دردسر

اگر کارکنان بتوانند همان‌طور که دربارهٔ دستیابی به سایر اهداف تجاری هوشیار هستند، دربارهٔ حفاظت از اطلاعات شرکت نیز هوشیارانه عمل کنند، به سرمایه‌ای فوق‌العاده ارزشمند برای برنامه‌های حفاظت اطلاعات شرکت، تبدیل می شوند. حتی اگر نخواهیم شرمندگی و ضرر از دست‌رفتن اعتبار مرتبط با نقض حریم خصوصی را ذکر کنیم، نجات شرکت از میلیون‌ها دلار جریمه و هزینهٔ مرتبط با نشت اطلاعات، می‌تواند به اندازهٔ صرفه‌جویی میلیونی برای شرکت از طریق فرایندهای اصلاحی یا کاهش هزینه، ارزش داشته باشد. برنامه‌های آموزش و آگاهسازی دربارهٔ هزینه‌های انواع مختلف نقض حریم و آنچه کارکنان می‌توانند برای جلوگیری از درز اطلاعات انجام دهند، در کارکنان این حساسیت را ایجاد می‌کند که با چالش‌های پیشِ‌رو مواجه شوند.

۴– جلوی وسوسهٔ انجام تخلفات «بی‌ضرر» را بگیرید.

مادامی که ممنوعیت‌های آشکار بسیاری همچون فروش فهرست کاربران شرکت به رقیب وجود دارد، «نقاط خاکستری» بسیاری در تخلفات وجود دارد که اگر به آنها نپردازیم، ممکن است به تخلفات آسیب‌زاتری منجر گردد. این تخلفات شامل این موارد می‌شود: به اشتراک‌گذاری فهرست تماس با دوستان در سایر شرکت‌ها، «پشتیبان‌گیری» از اطلاعات حساس و ذخیره آن در سامانه‌های خانگی یا وسایل ذخیره‌ساز غیرمجاز و کپی سرمایه‌های معنوی به درایوهای بندانگشتی USB با هدف انتقال آنها به یک سایت توسعه از راه دور. تمام این تخلفات، در عین‌حال که ممکن است برای کارکنان بی‌ضرر به‌نظر برسد، می‌تواند به رخنه‌های هزینه‌زا منجر گردد. علاوه بر آن، از آنجا که کارکنان مجازند آنچه را می‌توانند با خود

ببرند مخفی کنند، شاید وسوسهٔ فزاینده‌ای در آنان شکل گیرد که از این تخلفات بهره ببرند. در حالی‌که گزینه‌های متعددی برای کنترل و عملی‌کردن سیاست‌ها وجود دارد، ملاک‌های انتخابیِ راه‌حلِ جلوگیری از درز اطلاعات باید هوشمندی راه‌حل در شناسایی نشت‌های مرتبط، بدون آنکه باعث آزار کارکنان شود و بر تولید تجاری آنان (و در برخی شرکت‌ها، تولید فردی آنان) اثر بگذارد، را لحاظ نماید.

۵– همزمان با عملی‌ساختن سیاست‌ها، به کارکنان دربارهٔ آنها آموزش دهید.

یک سیاست حفاظت اطلاعات مؤثر باید شامل روش«هویج و چماق» باشد. به کارکنان باید به‌طور ایده‌آل در «هنگام استفاده» یا «هنگام تخلف» دربارهٔ سیاست‌های شرکت آموزش داد. هنگامی که یکی از کارکنان در تخطی از سیاست‌های شرکت، اقدام به کپی سندی حساس در درایو USB می‌کند، این بهترین زمان برای آموزش‌دادن به آنان دربارهٔ حفاظت مناسب از دارایی‌های مهم شرکت است. اگر تخلفات شدید باشد، اقدام باید توسط راه‌حل پیشگیری از درز اطلاعات متوقف گردد و مدیر باید از امکان چنین گام‌های مناسبی آگاه گردد. بالابردن آگاهی کارکنان از سیاست‌های حفاظت اطلاعات، به ویژه در «هنگام استفاده»، می‌تواند درصد بسیار زیادی از نشت اطلاعات را که سهوا و تصادفی رخ می‌دهد کاهش داده یا حتی از میان ببرد.

فناوری جلوگیری از نشت اطلاعات فقط نباید به کنترل و جلوگیری از نشت اطلاعات بپردازد، بلکه باید به آموزش و بالابردن آگاهی کارکنان دربارهٔ سیاست‌ها و رویه‌های شرکت برای ادارهٔ اطلاعات حساس نیز کمک کند. راه‌حل‌های جلوگیری از نشت اطلاعات نیز می‌توانند ازطریق آموزش کارکنان و حفاظت از محیط شبکه و نقاط پایانی داخلی به کارکنان کمک کنند با جلوگیری از نشت اطلاعات، کاستن از نشت‌های تصادفی و هوشیاربودن در حفاظت از اطلاعات حساس، به سرمایه‌های امنیتی تبدیل شوند.

در هرحال، هر نوع فناوری نوین که بر فعالیت‌های روزانه کارکنان تأثیر می‌گذارد باید هوشمند و دقیق باشد تا از کاهش بازدهی کارکنان و ایجاد فرسایش دوری کند. باید میان «کنترل و عملی‌کردن سیاست‌های جلوگیری از نشت اطلاعات» و «قادرساختن کارکنان و مدیران به انجام وظیفه و رشد تجارت» تمایزی مناسب و خطی ظریف درنظر گرفت.

تقابل امنیت و تهدید:

امنیت را می‌توان در تقابل آن با تهدید شناخت، در این رویاروئی آنچه که دائمی و حتمی است تهدید، و آنچه که البته تابع و نسبی خواهد بود امنیت می‌باشد.

در کوتاه‌ترین تعریف می‌توان امنیت را احساسی دانست که در برابر تهدید، منجر به آرامش گردد. بنابراین هرگاه فردی از وجود نوعی تهدید (خطر) احساس عدم‌آرامش داشته باشند. امنیت وی به خطر افتاده است پس برای شناسایی امنیت بایستی از نقطه نقض و ضد آن وارد شد که علما فرموده‌اند:

تعرف الاشیاء باضدادها یعنی که پدیده‌ها را با ضدهای آن می‌توان شناخت.

پس در واقع علم امنیت‌شناسی عبارت است از علم تهدیدشناسی؛ زیرا با شناخت تهدید می‌توان راه‌های مقابله با آن را معین و به اجرا در آورد و بدین‌گونه است که با از بین‌رفتن یا خنثی‌شدن و یا ضعیف‌شدن تهدید، امنیت جان دوباره‌ای گرفته و تقویت می‌شود.

چند نکته مهم:

- امنیت، نسبی و دارای مراتب است، امنیت مطلق، همزمان با تعامل با دیگران غیرممکن است اما می‌توان حد متوسط و قابل قبولی را برای آن تصور نمود و براساس اهمیت موضوع و امکانات موجود و دست‌یافتنی، برنامه‌ریزی کرد و هزینه آن را محاسبه کرد.

- همیشه باید توجه کرد که در محیط کاری مشترک، همه اعضاء همانند حلقه‌های زنجیر عمل می‌کنند و زنجیر از ناحیه سست‌ترین حلقه، آسیب می‌پذیرد.

- عوامل مختلفی چه در عرض هم و چه در لایه‌های طولی در تأمین امنیت، دخالت دارند بنابراین به تک‌تک این عوامل به‌عنوان حلقه‌های مرتبط در حوزه‌های مختلف امنیت اطلاعات و ارتباطات باید توجه شود.

- از آنجا که نوع تهدیدات، تحول‌پذیر است باید در انتخاب راه‌های مقابله و مکانیزم‌های حفاظت نیز، تحول‌گرا و انعطاف‌پذیر بود.

منشاء بروز تهدیدات از کجاست؟

برای یک انسان منشاء تهدید می‌تواند درونی (اعضاء و جوارح داخلی فرد)، مصرفی (همراه با مواد غذایی مصرف‌شده)، بیرونی (عوامل خارج از انسان)، محیطی (محیط پیرامونی)، روحی و

روانی، ارثی، ژنتیکی و... باشد. پس واقعا منشاء تهدید را نمی‌توان از قبل پیش‌بینی کرد، اندازه گرفت، آمادگی مقابله یافت و ابزارهای دفاعی برای آن تهیه نمود.

وقتی انسانی درگیر مسائل ناشی از تهدید و خطرات غیرقابل پیش‌بینی آن باشد، تکلیف جوامع انسانی چه خواهد بود؟

منشاء تولید خطر برای یک جامعه از کجاست؟ از آحاد همان جامعه، از مواد مصرفی جامعه، از کشورهای بیگانه، از سوء مدیریت، از دوستان ناباب و جاهل، دشمنان آگاه و مغرض، منافقین، اهریمنان، نارسایی‌ها، ازدیاد یا کاهش تعداد جمعیت، جوانی یا پیری میانگین جامعه، بیکاری، قطعی برق، گاز و آب در مناطق شهری، کمبود وسایل تردد داخل شهری، گرانی مایحتاج عمومی مردم، پرداخت یارانه یا عدم‌پرداخت آن و هزاران معضل دیگر که هر کدام به نوعی و در مقطعی خاص می‌توانند منشاء بروز یک بحران در جامعه شده و امنیت را با خطرات جدی و بنیادی روبرو سازند.

بخش۲ – تهدید و آسیب‌پذیری

برای حفظ امنیت و تصمیم‌گیری جهت چگونگی واکنش در برابر دشمن، باید ابتدا او را شناخت، اهداف احتمالی او را با تیزبینی تشخیص داد تا در نهایت با تحلیل روش‌های دشمن در اعمال تهدید و بروز آسیب‌های ناشی از آن، دشمن را در رسیدن به اهدافش ناکام گذاشت. برخی از کارشناسان معتقدند از آنجا که تهدید بر بستر آسیب‌پذیری واقع می‌شود، شناخت نقاط ضعف و قوت خودی (به‌عنوان مقوله آسیب‌پذیری) از اهمیت زیادی برخوردار است و اصولاً در فرایند دشمن‌شناسی، نیازمند شناخت آسیب‌پذیری‌ها می‌باشیم و اگر مرحله تبیین آسیب‌پذیری، دقیق و خوب انجام نگیرد آثار منفی آن در مراحل تصمیم‌گیری و برخورد در مقابل تهدید، خود را نشان داده و ما را در این مبارزه به شکست خواهد کشانید.

شناسایی دشمن و تهدیدهایی که از ناحیه او موجودیت ملّی و دینی ما را تهدید می‌کند، نه تنها امری واجب، بلکه یکی از حوزه‌های مهم در سیاست‌گذاری هر نظام مستقل از جمله نظام جمهوری اسلامی است و حوزه‌های دولتی و به ویژه نیروهای مسلح به لحاظ نقش بنیادینی که در بخش دفاعی و امنیتی کشور داراست، در این بین اهمیت ویژه‌ای دارد.

بنابراین، مدیرانی که در سطوح مختلف نیروهای مسلح به خدمت می‌پردازند نیازمند چنان سطحی از بصیرت امنیتی هستند که ضمن شناخت دشمن، به روش‌های تهدید و آسیب‌رسانی آن آشنا و در تصمیم‌گیری‌ها و تصمیم‌سازی‌های خود افزایش ضریب حفاظتی و امنیتی مجموعه را مدنظر داشته باشند.

از سوی دیگر سنجش تهدیدات، دارای دشواری‌ها و ظرافت‌های خاص خود می‌باشد و ادلّه و استدلال‌های فراوانی در زمینه دشواری سنجش تهدیدات، از سوی دانشمندان مختلف ارائه گردیده تا آنجا که تا حد نفی امکان سنجش تهدیدات پیش رفته است:

۱– تهدید[1]

۱-۱- معنای لغوی تهدید

در فرهنگ لغت سیاح، تهدید در لغت را به معنی بیم‌دادن و ترسانیدن معرفی نموده و فرهنگ معین، واژه تهدید را معادل ترسانیدن، بیم‌دادن و بیم‌کردن دانسته است.

فرهنگ عمید هم علاوه بر دو واژه ترسانیدن و بیم‌دادن، عبارت بیم عقوبت‌دادن را نیز معادل تهدید برشمرده است.

لغت‌نامه وبستر[2] برای تهدید دو تعریف ارائه داده است: نخست تهدید را بیان و ابراز قصد آسیب‌رساندن، نابود یا تنبیه‌کردن دیگران از روی انتقام یا ارعاب می‌داند و در تعریف دوم، آن را نشان‌دادن خطر، آسیب و شرارت قریب‌الوقوع مانند جنگ تعریف کرده است.

لغت‌نامه لانگمن[3] سه تعریف از تهدید ارائه کرده است.

نخست تهدید را بیان آشکار آسیب‌رساندن به کسی یا ناراحت‌کردن و به دردسر انداختن او می‌داند؛ در تعریف دوم، آن را احتمال وقوع حادثه‌ای بسیار بد معنا کرده و در تعریف سوم، تهدید را شخص یا چیزی که به‌عنوان خطر[4] شناخته می‌شود، معرفی نموده است.

1- Threat
2- Webester
3- Longman
4- Danger

فرهنگ آکسفورد واژه تهدید را چنین تعریف نموده است:

" امکان به وحشت‌انداختن، ترساندن یا ایجاد فاجعه برای یک فرد یا جامعه، آسیب‌زدن به کسی یا چیزی، نتایج ناخوشایند به‌بارآوردن" (آکسفورد: ۲۰۰۵).

در دایره‌المعارف ویکی پدیا[1] نیز در توضیح واژه تهدید آمده است:

"تهدید، بیان آسیب‌رساندن به کسی یا تنبیه‌کردن اوست. تهدید منوط به نحوهٔ عمل دریافت‌کننده تهدید خواهد بود. تهدید می‌تواند حاوی یک پیام آشکار یا ضمنی باشد."

از نظر کارل روپر[2]، تهدید عبارتست از هرگونه نشانه، حادثه یا شرایطی که توان ایجاد خسارت و ضرر علیه یک دارایی را داشته باشد (روپر، ۱۹۹۹: ۵).

۲-۱ معنای اصطلاحی تهدید

تهدید را می‌توان پدیده یا اقدامی مخاطره‌آمیز دانست که از طرف اعمال‌کننده (داخلی یا خارجی) ازطریق نقاط آسیب‌پذیر موجود، به‌منظور دستیابی به اهداف تهدیدکننده، تحقق می‌یابد.

مفهوم تهدید در نگرش سیستمی، عدم تعادل در سیستم، بیان شده است. یعنی عاملی که اجازه نمی‌دهد سیستم به اهداف خویش برسد. در پاره‌ای از متون نیز تهدید به‌معنای توانایی‌ها، نیات و اقدامات دشمنان بالفعل و بالقوه برای ممانعت از دستیابی خودی به مقاصد امنیت ملی تعریف شده است (مرادیان، ۱۳۸۵ : ۶۵).

مارتین در تعریف تهدید می‌گوید: "تهدید به احساس عینی از یک حالت یا وضعیت دلالت دارد که هم برای طرفین درگیر و هم برای یک ناظر مستقل و بی‌طرف حکایت از خطر قریب‌الوقوع دارد. تهدید یک عنصر ذهنی دارد که ادراک و احساسات طرفین درگیر را شامل می شود. (همان ،۶۵).

" تهدید عبارت از وضع و حالتی است که در آن مجموعه‌ای از ادراکات و تصورات نسبت به پدیده‌ها و رابطهٔ آنها با بقاء کمیت یا کیفیت ارزش‌های اساسی و مورد احترام بر وجود خطر جدی یا امکان نابودی آن ارزش‌ها دلالت دارد." (گروه مطالعاتی امنیت، ۱۳۸۷: ۱۰۴).

1-Wikipedia
2- Carl Roper

۳-۱ تهدید از منظر امنیتی

صرف‌نظر از معانی لغوی و لفظی تهدید، در ادبیات امنیتی، تعاریف و توصیف‌های گوناگونی از تهدید صورت گرفته است. وجود یک فشار خارجی منفی، فقدان امنیت، ایجاد اختلال در توانایی‌های کشور در کسب اهداف ملی، اقداماتی که کمیت و کیفیت زندگی مردم یک کشور یا دامنهٔ اختیارات حکومت را به‌طور جدی کاهش دهد، درک و ساخت یک دشمن در وضعیت خطرناک، محدودکردن و حبس‌کردن آزادی، رهایی و... از جمله تعاریفی است که برای تهدید در حوزه امنیت و امنیت ملی ذکر می‌گردد (گروه مطالعاتی امنیت، ۱۳۸۷: ۱۰۱).

عامل یا وضعیتی که جزء اصلی یا تمامیت یک موضوع یا سامانه را با اختلال اساسی مواجه سازد، یا از چهارچوب تعیین‌شده خارج نماید یا از رسیدن به اهداف پیش‌بینی‌شده باز دارد یا آن را نابود کند.

به‌طور کلی تهدید به هرگونه شرایطی اطلاق می‌شود که امنیت یک هدف با ارزش را سلب یا کاهش دهد. در متون کلاسیک و در دانشکده‌های عالی دفاعی نیز تعریف کاربردی از تهدید بدین شرح است:

«تهدید عبارت است از: هرگونه نیت، قصد و اقدامی‌که صیانت یک هدف با ارزش را در ابعاد امنیتی، حیثیتی و اعتقادی به‌خطر اندازد و به‌عبارت بهتر به قابلیت‌ها، نیات و گاه اقدامات دشمنان بالفعل و بالقوه برای مداخله یا جلوگیری از نیل به منافع و اهداف نظام، دولت و سازمان، تهدید اطلاق می‌شود.

«ریچارد المان[1]» از «تهدید» به مثابهٔ یک «پدیدهٔ امنیتی» چنین تعبیر می‌نماید: «رفتار یا مجموعه‌ای از اقدامات که برای زندگی یک بازیگر ایجاد خطر نموده و دامنه گزینه‌های انتخابی او را محدود می‌کند» (المان،۱۹۸۳: ۱۲۸).

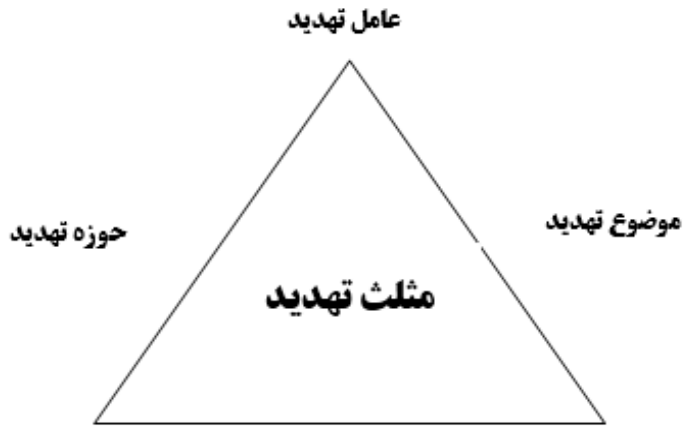
باید توجه داشت که هر تهدیدی را نمی‌توان امنیتی قلمداد کرد و تقلیل «امنیت به تهدید» نگرشی ناصواب است:

1 - See R.Ulman

«الصاق برچسب امنیتی بر کلیه تهدیدات از حیث منطقی توجیهی ندارد. ما تهدیدات زیادی داریم- مانند بیماری ایدز و برخی دیگر از بلایای طبیعی و غیر آن - که درعین تهدیدبودن، ضرورتاً امنیتی نیستند» (افتخاری، ۱۳۸۵: ۲۷).

۴-۱ اجزای تهدید

تهدید از سه بخش اساسی «کارگزار یا عامل تهدید[1]»، «حوزه تهدید» و «موضوع تهدید[2]» تشکیل شده است. عامل تهدید در واقع هویت (شخصی یا سازمانی) یا چیزی است که به‌طور بالفعل یا بالقوه توانایی ایجاد، انتقال یا پشتیبانی از تهدید را دارد؛ در حالی‌که حوزه تهدید، هویت یا چیزی است که موجودیت و یا دارایی‌های حیاتی آن درمعرض خطر قرار گرفته است و درنهایت موضوع تهدید، وضعیت، پدیده، فعالیت یا رخدادی است که به‌نظر می‌رسد قابلیت‌های درونی و بیرونی انتقال، پشتیبانی یا ایجاد خطر در موجودیت یا دارایی‌های حیاتی بازیگر مورد آماج را در خود دارد (عبداله‌خانی، ۱۳۸۶: ۲۱).



1- Threat Agent
2- Key Threat

۵-۱ اوصاف تهدید

گاه تعریف، شناخت مفاهیم و پدیده‌ها ازطریق شناخت اوصاف آنها صورت می‌گیرد. این روش در مورد مفاهیم و پدیده‌های بزرگ و عالی اجتناب‌ناپذیر می‌باشد. تهدید نیز از این دسته مفاهیم و پدیده‌ها است که می‌توان اوصاف و ویژگی‌های زیر را برای آن درنظر گرفت (گروه مطالعاتی امنیت، ۱۳۸۷: ۱۰۵).

- ✓ نسبی‌بودن
- ✓ زمینه‌ای و وابسته‌بودن
- ✓ ارزش‌محور بودن
- ✓ سلبی‌بودن
- ✓ فراگیر و عمومی‌بودن
- ✓ داشتن قابلیت و استعداد بالا
- ✓ انفعالی‌بودن
- ✓ کاربردی و عملی‌بودن
- ✓ احتمالی و هراس انگیزبودن
- ✓ داشتن آثار منفی مستقیم

۶-۱ تهدیدشناسی

۱- ابعاد تهدیدات

ابعاد تهدیدات با گونه‌ها و اقسام تهدیدات تفاوت دارد و به‌همین دلیل شایسته است این دو بحث از یکدیگر جدا شوند.

ازطرف دیگر ابعاد یک چیز، اقسام آن نیستند بلکه ابعاد، چهره‌های مختلف یک امر کلی محسوب می‌شوند. ابعاد نسبت به یکدیگر، رابطه منظم و ارگانیک دارند، لذا هر بعد در ارتباط با ابعاد دیگر می‌تواند هدف و مسئله کلی ما را تبیین نماید.

۲- گونه‌شناسی تهدیدات

منظور از گونه شناسی، دسته‌بندی تهدیدات است. این امر، در مدیریت تهدیدات حائز اهمیت بوده و مدیریت تهدید را تسهیل می‌کند. تاکنون معیارهای زیادی برای دسته‌بندی تهدیدات

وضع شده‌اند ولی هر معیار در یک حوزه خاص کاربرد دارد. لذا گاهی باید معیارهای ویژه و گاه معیارهای ترکیبی برای دسته‌بندی تهدیدات بکار رود.

یکی از معیارهای رایج، گونه‌شناسی براساس بعد است. از این نظر، تهدیدات به سیاسی، اقتصادی، زیست محیطی، نظامی، اجتماعی، فرهنگی، فناوری و... تقسیم می‌شوند. هر جامعه متناسب با شرایط خود، تهدیداتش را دسته بندی کرده و هر بخش از تهدیدات را به گروه خاصی برای اداره می دهد و به این ترتیب تهدیدات را مدیریت می‌کند.

برخی از ابعاد موردنظر برای شناسایی تهدیدات به شرح زیر است:

- سطح تحلیل فردی، گروهی، ملی و بین‌المللی
- جغرافیایی (داخلی، خارجی و مرزی)
- تعادل و تقارن (متقارن و نارمتقارن)
- جنس تهدید: عینی (کمی و واقعی)، ذهنی (احساسی)
- انگیزه (عمدی و غیرعمدی)
- کار ویژه: ایذایی، واقعی «اصلی و فرعی» (مرادیان، ۱۳۸۵: ۱۰۷-۱۰۳)

در تقسیم‌بندی دیگر، اقسام تهدیدات به شکل زیر دسته‌بندی شده است (گروه مطالعاتی امنیتی، ۱۳۸۷ :۱۲۳-۱۱۴).

- داخلی و خارجی
- بسیط و چند وجهی
- مستقیم (رسمی) و غیرمستقیم (غیررسمی)
- عمدی و غیرعمدی
- دفعی (مشخص) و تدریجی (فرایندی)
- سنتی و غیرسنتی
- متمرکز و پراکنده
- سخت و نرم
- متقارن (متناسب) و نامتقارن (نامتناسب)
- ابزاری و واقعی

برخی نیز تهدیدات را به شکل زیر طبقه‌بندی نموده‌اند. (عبداله‌خانی، ۱۳۸۶ : ۹۵-۵۹)

- امنیتی – عمومی
- بازدارنده - خزنده
- سخت – نرم
- سنتی – نوین
- متقارن – نامتقارن
- طبیعی – ساختگی

۳- مولفه‌های شناسایی تهدید

در شناخت تهدید، چند عامل از اهمیت زیادی برخوردار هستند. براساس مولفه‌های شناخت تهدید، می‌توان هر تهدید را مورد ارزیابی و تجزیه و تحلیل قرار داد. به عبارتی، شناخت تهدید زمانی صورت می‌گیرد که این مولفه‌ها به‌صورت دقیق و کامل شناخته‌شده و تجزیه و تحلیل لازم روی آنها صورت گرفته باشد.

الف) هدف تهدید

نتیجه و انتظاری که دشمن ازطریق اعمال تهدید به آن دست می‌یابد را هدف تهدید می‌گویند. به‌عنوان مثال بمب‌گذاری به‌منظور تخریب، ایجاد رعب و وحشت انجام می‌گیرد و جاسوسی به‌منظور کسب اطلاعات دارای طبقه‌بندی طرح‌ریزی و اجرا می‌شود. در این مولفه (هدف تهدید) باید اهداف جزئی و نهایی دشمن مدنظر قرار گیرد، زیرا گاهی تهدید اگر چه به‌طور آشکار اتفاق می‌افتد ولی، هدف ایذایی و انحرافی است تا سیستم اطلاعاتی و حفاظتی خودی را از هدف اصلی دور نماید. به‌عنوان مثال، بزرگ‌نمایی تهدیدات جاسوسی از طریق ابزار فنی همچون ماهواره که توسط دشمن اتفاق می‌افتد. یک هدف ایذایی است تا در پناه آن سازمان‌های حفاظتی یا مدیران مجموعه‌های دفاعی از جاسوسی توسط نیروی انسانی نفوذی دشمن غافل شوند. بنابراین تهدیدشناسی در قالب مولفه هدف باید پاسخگوی این سئوالات باشد:

- هدف تهدید چیست؟
- آیا تهدید بزرگ‌نمایی یا کوچک‌نمایی نشده است؟

- تهدید از نظر ماهیت مستقل است یا وابسته؟
- وقوع تهدید چه نتایجی را برای دشمن به‌دنبال دارد؟

ب) استراتژی (راهبرد) تهدید

هر تهدید دارای راهبرد معینی است که دشمن در چهارچوب و قواره آن، برای وصول به هدف از آن تبعیت می‌کند. به‌عنوان مثال: استحاله فرهنگی یکی از استراتژی‌های دشمن در ایجاد تهدید فرهنگی و اجتماعی است. به‌عبارت دیگر دشمن برای ایجاد بی‌هویتی و استحاله از روش تهاجم فرهنگی استفاده می‌کند. خرابکاری در تجهیزات توسط ضدانقلاب با استراتژی‌های اختلال در انجام ماموریت، وقفه در کار، بی‌انگیزگی، خسارت اقتصادی، عملیات روانی و تاثیرگذاری بر افکار عمومی، کاهش مقاومت مردمی و سازمان ایجاد می‌شوند.

ج) فعل تهدید:

هر تهدید برای عملی‌شدن، نیازمند اقدام و فعالیتی است. به‌عبارتی هرگونه اقدامی که دشمن به‌منظور اخلال در امنیت انجام می‌دهد، فعل تهدید نام دارد. در واقع این مبحث شناسایی روش‌ها و تاکتیک‌های دشمن است. به‌عنوان مثال، استفاده از روش‌های فرهنگی همچون ساخت فیلم ازجمله روش‌های دشمن برای تهاجم فرهنگی است که از آن در رسانه‌های منطقه‌ای و بین‌المللی (همچون کانال‌های تلویزیونی ماهواره‌ای) و شبکه‌های اطلاعاتی (همچون اینترنت) مورد استفاده قرار می‌گیرد.

د) بستر تهدید

هر امکان و شرایطی که دشمن برای اعمال تهدید از آن استفاده می‌نماید یا زمینه و تسهیل‌کننده فعل تهدید باشد، بستر تهدید نامیده می‌شود. از این‌منظر، اصطلاح آسیب‌پذیری مترادف با بستر تهدید است. بستر تهدید به عوامل داخلی برمی‌گردد که زمینه بروز تهدید را مهیا می‌سازند. به‌عنوان مثال، عدم وجود انضباط اداری و مالی در یک سازمان، باعث بروز تهدیداتی همچون اختلاس، ارتشاء، پورسانت در سازمان می‌شود و یا عدم‌آموزش کارکنان و فقدان شناخت نسبت به سازمان‌های اطلاعاتی و نحوه عملکرد آنان، ممکن است زمینه‌ساز جذب برخی از کارکنان توسط سرویس‌های جاسوسی دشمن و یا به دام‌افتادن برخی از آنان شود.

۲- آسیب‌پذیری:

۲-۱ معنای لغوی آسیب‌پذیری

در مباحث امنیتی، آسیب‌پذیری چنین معنی شده است:"حساسیت یک کشور، چه در زمان صلح و چه در زمان جنگ، در برابر هرگونه اقدام و وسیله‌ای که از آن طریق، ظرفیت و توانایی جنگی‌اش تقلیل یا اراده‌اش در جنگیدن کاهش یابد" (علی‌زاده و همکاران، ۱۳۸۱: ۳۸).

تعابیر دیگری ازجمله ترمیم‌ناپذیری، بی‌حفاظ‌بودن، فقدان ظرفیت انطباق و... نیز معادل آسیب‌پذیری دانسته شده است (عبداله‌خانی، ۱۳۸۶: ۴۳-۴۱).

۲-۲ تعریف اصطلاحی آسیب‌پذیری

ضعف‌های موجود و نقاط ضربه‌پذیری که زمینه‌ساز و بستر اعمال تهدیدات می‌باشند را نقاط آسیب یا آسیب‌پذیری می‌گویند. مانند محرومیت‌ها، کمبودها، نیازهای مالی، انباشتگی مهمات و مواد ناریه تولیدشده در صنایع، عدم‌رعایت ارزش‌ها، هنجارها و ضوابط امنیتی در زمینه تحقیقات، توسعه فنآوری صنعتی و تبادلات علمی و فنی، عدم رعایت حفاظت گفتار در رسانه‌ها، مذاکرات، سخنرانی‌ها و مکالمات مخابراتی، عدم نظارت مناسب بر حمل و نقل مواد منفجره و محترقه، سلاح، مهمات و چگونگی مصرف مواد ناریه، عدم جداسازی بخش‌های نظامی و غیرنظامی صنایع از یکدیگر و ورود افراد غیرنظامی بدون رعایت ضوابط لازم، واگذاری امورات به پیمانکاران بخش‌های خصوصی در اماکن دارای طبقه‌بندی که صلاحیت آنها احراز نشده است و... .

۲-۳ تعریف لغوی آسیب

آسیب یعنی عارضه، علت، ضرر، زخم، عیب و یا نقصی که به‌سبب ضربه‌ای پدید آید.

آسیب در لغت به معنی زخم، کوب، ضرب، عیب و نقص یا شکستگی که به‌سبب ضربت و زخم پیدا شود، صدمه، تعب، رنج، مشقت، آفت، بلا، نکبت، مصیبت، گزند، آزار، زیان، ضرر و... است (معین، ۱۳۷۸).

برابر تعریف مندرج در دایره‌المعارف ویکی‌پدیا، آسیب به‌معنای زخم، جراحت و صدمه از حوزهٔ زیست‌شناسی به مباحث اجتماعی و سپس امنیتی وارد شده است.

۲-۴ تعریف اصطلاحی آسیب

ضربه، عارضه و یا نقصی که توسط عوامل خودی یا دشمن ایجادشده و زمینهٔ اعمال تهدیدات دشمنان را فراهم نماید مانند اخذ پورسانت، رشوه، مبادرت به اختلاس، عامل‌شدن برای دشمن، انحرافات اعتقادی یا جنسی، شایعه‌پراکنی و جوسازی با اهداف سیاسی، جعلیات (اوراق رسمی، مدارک، مهر و امضاء و...)، تبلیغات (عدم توزیع عادلانه امکانات سازمانی)، عدم رعایت ضوابط در مناقصه‌ها و مزایده‌ها، فرسودگی و غیراستانداردبودن دستگاه‌های تولیدی در برخی صنایع، حوادث ناشی از انفجار، آتش سوزی و...

«آسیب‌ها از لحاظ حفاظتی و اطلاعاتی جنبه‌های فیزیکی ندارند و بعضاً قابل‌مشاهده نیستند. به‌عنوان مثال، وجود نفوذی و جاسوس نوعی آسیب امنیتی برای تشکیلات محسوب می‌شود؛ درحالی‌که این ضرر و خسارت از نظر فیزیکی و مادی قابل رویت نیست و صرفاً آسیب‌های امنیتی از طریق قرائن و شواهد آن شناخته می‌شود» (علی‌زاده و همکاران، ۱۳۸۱: ۳۸).

در کل، نتیجهٔ اعمال تهدید و عوارض ناشی از آن در مجموعه را آسیب می‌گویند.

۲-۵ تعریف آسیب و آسیب‌پذیری

مقولهٔ آسیب و آسیب‌پذیری وجه مشترکی با امنیت سازمانی دارند. به‌طور کلی هر اقدام یا هر ابزاری که موجب کاهش توانایی و کارکرد سازمان شده و منشاء آن داخلی باشد، آسیب‌پذیری نامیده می‌شوند. در آسیب‌پذیری تعمّد و برنامه‌ریزی در کار نیست، لیکن نتیجه آن بروز خسارت و زمینه‌ساز تهدید و ایجاد شرایط مناسب برای اعمال تهدید با هزینه‌های پایین‌تر خواهند بود.

باتوجه به آنچه گفته شد؛ تعریف موردنظر در این سند از مقولات آسیب و آسیب‌پذیری را می‌توان به شرح زیر بیان نمود:

آسیب‌پذیری: ضعف‌های موجود در مجموعه و نقاط ضربه‌پذیری که زمینه بروز و فعلیّت‌یافتن تهدیدات بالقوه را فراهم نموده و یا موجب تشدید تهدیدات بالفعل می‌شود.

آسیب: اثرات اعمال تهدید بر منافع و موجودیت سیستم را آسیب می‌گویند.

۶-۲ زمینه‌های بروز آسیب

شناخت عوامل ایجاد و افزایش‌دهنده آسیب‌پذیری ضروری است، چون با کنترل و حذف این عوامل می‌توان صیانت و صحت سازمان را تضمین نمود. یکی از وظایف مهم مجموعه‌های حفاظتی تبیین و بررسی این عوامل است تا با آموزش و توجیه نیروی انسانی از بروز تهدیدات بعدی جلوگیری نماید.

به‌طور کلّی عواملی که در ادامه می‌توان زمینه‌ساز ایجاد و بروز تهدیدات امنیتی مهم تلقی نمود در سه دسته عمده قرار دارند که عبارتند از:

الف) عوامل درون‌سازمانی

این عوامل که به حوزه سازمانی برگشته و ناشی از ضعف یا نقص در سیستم می‌باشند را می‌توان با بررسی آثار آن در سازمان تشخیص داد و ترمیم نمود. به‌طور نمونه به چند عامل شایع‌تر که زمینه بروز آسیب و خسارت است اشاره می‌شود:

۱- عدم‌جامعیت قوانین و مقررات اداری: در بسیاری از موارد قوانین و مقررات در شرایط خاص تدوین شده‌اند و به مرور باتوجه به شرایط جدید نسبت به آنها تجدید نظر نشده است. این موضوع باعث شده است تا تمامی جوانب در مباحث مربوطه لحاظ نگردد. خلاءهای قانونی از جمله مواردی است که زمینه‌ساز بروز بعضی از آسیب‌پذیری‌ها شده است.

۲- ضعف دستگاه در توجیه و آموزش کارکنان مجموعه: از آنجا که در دستگاه‌های دولتی بخش معینی مسئول ارشاد و آگاهسازی کارکنان نسبت به قوانین نیست و در این حوزه به‌صورت مناسب نقش ایفاء نمی‌شود زمینه بروز نابسامانی‌های اداری افزایش می‌یابد. تذکر، آموزش، فرهنگ‌سازی و تقویت تعهد افراد ازجمله عواملی است که غفلت از آن، زمینه بروز ضعف در مجموعه را ایجاد می‌نماید.

عدم‌شناخت و اطلاع از تبعات قانونی بعضی از فعالیت‌ها، مبنای بسیاری از تخلفات اداری است و همواره بهانه‌های عدم آگاهی از سوی متخلفین به‌راحتی بیان و نزد مراجع قضایی پذیرفته می‌شود.

۳- فقدان سیستم کنترلی بر عملکرد کارکنان: یکی از عوامل بازدارنده در بروز آسیب‌پذیری‌ها، انجام نظارت مستمر بر فعالیت کارکنان مجموعه است که با تقویت نهادهای

نظارتی و تقویت کنترل‌های اداری، ضمن شناسایی مشاغل درمعرض آسیب، امکان اعمال اقدامات بازدارنده وجود دارد.

انجام اقدامات کنترلی معمولاً توسط سیستم مدیریتی و همچنین حفاظت اطلاعات یکی از نیازهای اصلی مجموعه‌های دولتی به‌خصوص مراکز مهمی مانند نیروهای مسلح می‌باشد.

ب) عوامل محیطی

دسته دوم از زمینه‌های بروز آسیب‌پذیری، شرایط محیطی است که در آن بسر می‌بریم. گاهی عامل بروز و گرایش کارکنان به فعالیت‌های خسارت‌بار و آسیب‌زا محیط زیست فکری و انسانی آنها است. در واقع گاهی افراد در بحران‌های ناشی از تربیت دوران گذشته، تغییرات فرهنگی زمان حاضر، مشکلات و ترس ناشی از آینده و... زندگی می‌کنند که این مشکلات منتج به رفتارهای خارج از ضوابط اداری شده و برای فرد و سازمان خسارت‌بار می‌باشد.

۱- محیط خانواده: یکی از عواملی که افراد را به‌سوی انجام فعالیت‌های غیرقانونی سوق داده و بروز فساد اداری را افزایش می‌دهد، توقعات خانواده است. اعضای خانواده تحت‌تاثیر رسومات اجتماعی و مقایسه خود با همکاران و...، فرد را برای تامین نیازهای بعضاً کاذب زندگی تحت‌فشار قرار داده که امکان بروز اختلال‌کاری و انحرافات (عموماً اقتصادی) متصور است.

۲- محیط اجتماعی: افزایش هزینه‌ها و فشارهای اقتصادی در جامعه و وجود تورم و افزایش هزینه‌های زندگی اجتماعی مخصوصاً برای افرادی که نگاهی تجمل‌گرا دارند و در عین‌حال در موقعیت شغلی مناسبی قرار گرفته‌اند، به‌عنوان عوامل تاثیرگذار مطرح است. این موارد صرفا انگیزه‌های اولیه بوده و در اثر استمرار بهره‌گیری از اموال دولتی یا اختیارات قانونی به‌صورت شخصی، فرد عادت نموده و به روند غلط زندگی خود ادامه می‌دهد.

۳- محیط اداری ـ کاری: همچنین تفاوت در زندگی فردی و اداری و داشتن شخصیت کاذب در محیط کاری فرد را به‌سوی تجمل‌گرایی سوق می‌دهد و نهایتاً فرد درصدد همگونی شخصیت اداری و شخصی خود خواهد رفت. در واقع تجمل‌گرایی از ناحیه محیط کاری به فرد تحمیل می‌گردد. این وضعیت برای افرادی که در بخش‌های تشریفات یا معاملات مالی و بازرگانی کار می‌کنند بیشتر اتفاق می‌افتد.

۴- تربیت غلط و ضعیف: جامعه هویت نسبتاً مستقلی از افراد دارد که واقعاً بر وجود افراد اضافه می‌شود، اما در وجود، قائم به افراد است.

فرد برای استفاده از امکانات اجتماعی لازم است بسیاری از ارزش‌ها و الزامات آن را بپذیرد و خود را با الگوهای فرهنگی آن هماهنگ سازد. حال اگر در جامعه‌ای سنت‌ها و قوانین الهی حاکمیت نداشته باشند یا ناقص اجرا شوند، طبیعی است که افراد، خود را منطبق با این وضعیت تربیت خواهند کرد و کم هستند کسانی که خود را از چنبرهٔ این تربیت، رها ساخته و دوام بیاورند.

ج) عوامل فردی

در مجموع عوامل فردی موثر در بروز تخلفات فردی را می‌توان به شرح زیر تبیین نمود:

۱- ضعف شخصیتی (تجمل‌پرستی و افزون‌طلبی): یکی از عواملی که در بروز آسیب‌پذیری امنیتی نقش مهمی را ایفا می‌کند ضعف شخصیتی افراد و تلاش برای پرنمودن این ضعف ازطریق توجه به ظواهر مادی است.

از آنجا که گرایش به تجملات و علاقه‌مندی افراطی به مادیات، با حقوق و درآمدهای معمول سازگار نیست، گرایش به اخذ پورسانت که یکی از معمول‌ترین جاذبه‌های مراودات اقتصادی است از همین ناحیه بروز می‌نماید.

۲- توجیه‌نبودن به‌وسیله قوانین و مقررات: معمولاً مقررات و قوانین در نزد برخی از کارکنان، دست و پاگیر تلقی می‌شوند و افراد سعی در فرار از محدودیت‌های قانونی دارند. به همین دلیل عدم‌توجه افراد به شناخت، یادگیری، اجرای قوانین و مقررات را باعث می‌گردد.

لذا در مجموعه‌هایی که توجیه کمتری نسبت به اعمال مقررات اداری وجود دارد و کنترل‌های لازم صورت نمی‌پذیرد زمینه را برای افراد نامنظم مهیا نموده و فرهنگ بی‌توجهی به اصول و مقررات و سهل‌انگاری در امور را در آن سازمان گسترش می‌دهد.

رابطه تهدید و آسیب در محیط امنیتی سازمان

در رابطه با نسبت تهدید و آسیب، دو رویکرد عمده وجود دارد:

در رویکرد اول، نتیجه و اثر وقوع تهدید بر موضوع مورد تهدید را آسیب می‌نامند. بنابراین، شاید بتوان آسیب امنیتی[1] را چنین تعریف نمود: «صدمه و ضرر به یک موضوع با ارزش که امنیت آن توسط اقدامات دشمن دچار خدشه گردد.»

در رویکرد دوم، آسیب‌پذیری، معطوف به نقاط ضعف داخلی سیستم بوده و زمینه‌ساز فعلیت یافتن تهدیدات و ضربه‌پذیربودن سیستم محسوب می‌شود.

معمولاً آسیب‌پذیری در مقابل تهدید به‌کار می‌رود و از یک جهت به تمایز داخلی یا خارجی‌بودن این دو توجه می‌شود. در این فرض، آسیب‌پذیری، نقایص، ضعف‌ها و مشکلات درونی و ساختاری، محیط مفروض را دربر می‌گیرد و تهدید، خطرات بیرونی نسبت به محیط می‌باشد (بوزان، ۱۳۷۸: ۱۳۶).

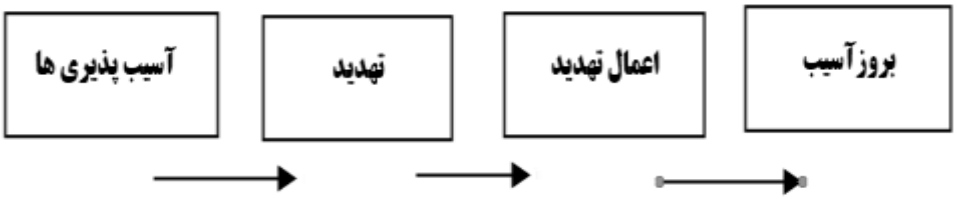
تهدیدات خارجی با آسیب‌پذیری‌های داخلی رابطهٔ مستقیم دارند، یعنی هرچه درجهٔ آسیب‌پذیری بالاتر باشد، احتمال وجود تهدیدات نیز افزایش می‌یابد. این یک قاعدهٔ منطقی است. دشمن به نقطه‌ای حمله می‌کند که با هزینهٔ کمتر، احتمال ورود خسارت و صدمه به آن نقطه بالاتر باشد.

اقدام به جنگ همواره با این تصور درست یا اشتباه صورت می‌گیرد که طرف مقابل در شرایط ضعف بسر می‌برد و دارای آسیب‌پذیری‌های جدی است (آزر و مون،۱۳۷۹: ۳۷۹).

از جهت دیگر، آسیب‌پذیری‌های یک سیستم از نظر کمّی و کیفی در حد یک تهدید جدی تلقی نمی‌گردند. بنابراین ممکن است گسترش آسیب‌پذیری‌ها به یک تهدید امنیتی تبدیل شوند (تریف، ۱۳۸۳: ۲۲۰-۲۱۷).

در محیط امنیتی سازمان نیز می‌توان باتوجه به تعاریف صورت‌گرفته، و با درنظرداشتن رویکردی که آسیب‌پذیری‌های موجود در سیستم را زمینه بروز و اعمال تهدید و متعاقب آن، بروز آسیب به سیستم می‌داند؛ می‌توان فرایند اعمال تهدید را در قالب شکل زیر ترسیم نمود:

1 - Security Vunerability



به‌عنوان مثال،آسیب‌پذیری‌های موجود در یک سیستم، تهدیدات اقتصادی را بر آن مترتب ساخته و در مرحله بعدی، موجب اعمال تهدید اقتصادی می‌گردد که به نوبهٔ خود، بروز آسیب‌هایی در حوزه اقتصاد را به‌دنبال خواهد داشت. این آسیب‌ها، خود به‌عنوان زمینه‌های تجدید اعمال تهدید محسوب شده و در مرحله بعدی، می‌تواند موجب بروز بحران اقتصادی شده و درصورت تکرار اعمال تهدید در حوزه اقتصادی، زمینه براندازی از بستر اقتصادی را فراهم نماید.

بخش ۳– عزت

مقام معظم‌رهبری در بیانات خود[1]عزت را به بارو تشبیه نموده و فرهنگستان زبان فارسی نیز دیوارهٔ آتش را به بارو تشبیه نموده‌اند. که می‌توان نتیجه چنین گرفت، در صورتی که بخواهیم دژی مستحکم در برابر نفوذ دشمن در عوامل انسانی ایجاد نماییم، مستلزم این است عوامل دفاعی و پدافندی در وجود آن و پیرامون آن ایجاد نمود. درخصوص ابنیه، تاسیسات، رایانه، اسناد و... می‌توان به‌صورت فیزیکی دیوارهٔ آتشی را ایجاد نمود ولی نمی‌توان در مورد عوامل انسانی این‌گونه عمل کرد. لذا دیوارهٔ آتش در عوامل انسانی نیز باید به‌گونه‌ای باشد که دائم همراه آن بوده تا در تمامی اوقات بتواند از صاحب خود محافظت نماید که باید در وجود عوامل انسانی این دیوارهٔ آتش ایجاد شود تا با دشمن و تهدیدات آن مقابله نماید. باتوجه به مطالعات علمی صورت‌گرفته و مطالب مندرج در تعالیم دین اسلام این وظیفه را عزت می‌تواند به خوبی انجام دهد.

---

۱ - مراسم گرامیداشت بیست و سومین سالگرد رحلت حضرت امام خمینی (ره) در تاریخ ۱۳۹۱/۰۳/۱۴

معنای لغوی و اصطلاحی «عزّت»

"عزت" در اصل آن حالتی است که انسان را مقاوم و شکست‌ناپذیر می‌سازد، و از آنجا که تنها خداوند است که شکست‌ناپذیر است، لذا تمام عزت از آن اوست، و هر کس عزتی کسب می‌کند از برکت دریای بی‌انتهای اوست.

معنای واژهٔ اصلی «عزّت» در کتب لغت آمده است: « واژهٔ عزّت بر شدّت، قدرت و آنچه که متضمّن معنای غلبه و قهر است، دلالت دارد». همچنین در جایی دیگر آمده است: «عزّت، در اصل، قدرت، شدّت و غلبه است» (ابن‌منظور: ۱۸۵).

از آنجا که شدّت و قوّت همواره با نوعی تفوّق و عدم‌چیرگی بر آن همراه است لذا «عزّت» را به‌معنای دست‌نایافتنی نیز معنا کرده‌اند. به‌طور مثال علامّهٔ طباطبایی در مورد معنای این واژه می‌نویسد:«کلمهٔ عزّت به‌معنای نایابی است، وقتی می‌گویند فلان چیز «عزیز الوجود» است، معنایش این است که به‌آسانی نمی‌توان بدان دست یافت و عزیز قوم به‌معنای کسی است که شکست‌دادنش و غلبه‌کردن بر او آسان نباشد؛ برخلاف سایر افراد قوم که چنین نیستند؛ زیرا عزیز در بین خودش مقامی دارد» (موسوی‌همدانی: ۲۰۶).

آیت ا...جوادی آملی نیز در این زمینه بیان می‌دارند: «عزّت، حالت نفوذ ناپذیری است که مانع مغلوب شدن است» (جوادی‌آملی: ۳۶۹).

پس باتوجه به تعاریف بالا می‌توان نتیجه گرفت که «عزّت» در اصل لغت به‌معنای به شدّت، قهر و غلبه است و لازمهٔ آن شکست‌ناپذیری و عدم چیره‌شدن در مقابل قوای دیگر است.

خداوند در قرآن کریم می‌فرماید: «من کان یرید العزّة فلله العزة جمیعاً» یعنی هر کس که خواهان عزّت است، همانا کلّ عزّت از آن خداست. از این‌رو عزّت حقیقی تنها در نزد خداوند متعال است و اوست که منشأ حقیقی همه عزّت‌هاست و هیچ‌س و هیچ موجودی بدون ارتباط با خداوند، حظّی از این کمال وجودی ندارد.

اصل صلابت و شکست‌ناپذیری، در معنای عزت است؛ در واقع نوعی بزرگ‌منشی و اتکاء به نفس و بی‌نیازی از غیر در این کلمه نهفته است، یعنی فردی که عزیز است، سلطه و سلطنت غیر را که معتقد به ذلیل‌بودن اوست، برخود نمی‌پذیرد و اگر در برابر کسی هم تسلیم شد یعنی

تسلیم به معنی واقعی کلمه، گویا او را عزیزتر از خود می‌داند و خود را در برابر وی ذلیل می‌یابد.

عزت از منظر قرآن و روایات

۱– عزّت در قرآن

در قرآن کریم واژهٔ عزّت به‌همان معنای لغوی به‌کار رفته است؛ یعنی شکست‌ناپذیری، توانایی و مغلوب‌نشدن. واژه «العزّة» ده‌بار و «عزیز» ۹۲ بار و مشتقات دیگر آن، بسیار در قرآن آمده و هرجا به‌معنای خاصی که گونه‌ای ارتباط با شکست‌ناپذیری دارد، اشاره دارد. چنان‌که این تعبیر، غالبا در معنای نیک و شایسته استعمال‌شده و ذات الهی را به «العزیز» یا «عزیز» توصیف می‌نماید: «و اللّه عزیز حکیم» (قرآن مجید، سوره توبه: آیه ۴۰).

معانی گوناگون واژه‌ی «عزّت» در قرآن مجید به شرح زیر است:

۱. تقویت کردن «**إِذْ أَرْسَلْنَا إِلَيْهِمُ اثْنَيْنِ فَكَذَّبُوهُمَا فَعَزَّزْنَا بِثَالِثٍ**» (قرآن مجید، سوره یس: آیه ۱۴) هنگامی که دو نفر از رسولان را به‌سوی آنها فرستادیم امّا آنان رسولان را تکذیب کردند پس برای تقویت آن دو، شخص سوّمی فرستادیم.

۲. چیره‌شدن و غلبه‌کردن «**فَقَالَ أَكْفِلْنِيهَا وَعَزَّنِي فِي الْخِطَابِ**» پس گفت مرا بر آن میش کفیل کن و در سخن گفتن بر من غلبه کرد.

۳. سربلندکردن و قدرت‌دادن «**... وَتُعِزُّ مَنْ تَشَاءُ وَتُذِلُّ مَنْ تَشَاءُ...**» (قرآن مجید، سوره آل‌عمران: آیه ۲۶) و هرکه را بخواهی عزّت می‌دهی و هرکه را بخواهی خوار می‌کنی.

۴. یکی از صفات خداوند به‌معنای نیرومندی و شکست‌ناپذیری «وَتَوَكَّلْ عَلَى الْعَزِيزِ الرَّحِيمِ» (قرآن مجید، سوره شعراء: آیه ۲۱۷) و بر خداوند عزیز و رحیم توکل کن.

۵. سخت و ناگوار «**لَقَدْ جَاءَكُمْ رَسُولٌ مِنْ أَنْفُسِكُمْ عَزِيزٌ عَلَيْهِ مَا عَنِتُّمْ**» (قرآن مجید، سوره توبه: آیه ۱۲۸) به یقین رسولی از خود شما به سویتان آمد که رنج‌های شما بر او سخت است.

۶. ممتنع و نشدنی «**وَمَا ذَلِكَ عَلَى اللَّهِ بِعَزِيزٍ**» (قرآن مجید، سوره ابراهیم: آیه ۲۰) و این کار برای خدا مشکل نیست.

۷. آسیب‌ناپذیری و چیزی که در آن تغییر و تبدیل راه ندارد «**إِنَّهُ لَكِتَابٌ عَزِيزٌ لَا يَأْتِيهِ الْبَاطِلُ**» (قرآن مجید، سوره فصلت: آیه ۴۱) و این کتابی است قطعاً آسیب‌ناپذیر که هیچ باطلی در آن راه ندارد.

۸. تکبّر و خود بزرگ‌بینی «**وَإِذَا قِيلَ لَهُ اتَّقِ اللَّهَ أَخَذَتْهُ الْعِزَّةُ بِالْإِثْمِ**» (قرآن مجید، سوره بقره: آیه ۲۰۶) و هنگامی که به آنها گویند: از خدا بترسید لجاجت و تعصّب آنها را به گناه می‌کشاند.

مفسّران نیز واژهٔ عزّت را به‌معنای: قوّت، قدرت، غلبه و شکست‌ناپذیری دانسته‌اند. در تفسیر کبیر ذیل آیه ۱۸، از سورهٔ منافقون، چنین آمده است: «لِلّهِ العزّ، ای، الغَلَبَةُ و القوّة...» (فخررازی، ۱۷) عزّت برای خداوند است یعنی غلبه و توانائی.

علاّمه طباطبائی نیز عزّت را به‌معنای: قوّت، غلبه و شکست‌ناپذیری، گرفته است (طباطبایی: ص ۳۱).

آیت‌الله مکارم شیرازی در تفسیر آیه ۱۸ از سورهٔ منافقون می‌گوید: «گرچه در فارسی روز مرّه عزّت به‌معنای احترام، آبرو و گران‌بها بودن است، ولی در لغت به‌معنای قدرت و شکست‌ناپذیری است.» (مکارم‌شیرازی: ۱۸۲).

بنابراین برتری و ارجمندی لازمه عزّت بوده و در مواردی که به‌معنای عظمت، ارجمندی، کرامت، سرافرازی و شرافت به‌کار رفته، از باب استعمال در لازم معنا است (شجاعی: ۱۷۶).

«در یک نگاه عمیق و تحلیلی، در تمام معانی یادشده می‌توان به نوعی همگرایی و اشتراک معنوی دست یافت و آن اینکه عزّت در موارد مختلف و ساختارهای گوناگون، به‌معنای قوّت، قدرت، غلبه و حالت شکست‌ناپذیری است» (شجاعی: ۱۷۵).

۲- عزّت در روایات

در روایات نیز کلمه عزّت به‌معنای صلابت و شکست‌ناپذیری آمده است. چنان که امام صادق علیه السّلام فرموده است: «**...انّ المؤمن أعَزّ من الجبل...**» (کلینی: ۵۳۳) مؤمن از کوه مقاوم‌تر و سخت‌تر است.

در روایتی دیگر می‌فرماید: «**إنّ المؤمن أشَدُّ مِنْ زُبَرِ الحَدِید...**» (محمدی‌ری‌شهری: ۲۲) مؤمن از پارهٔ آهن محکم‌تر است.

امام باقر[علیه‌السّلام] نیز فرموده است: «**المُؤْمِنُ أصْلَبُ من الجبل...**» (همان) مؤمن از کوه سخت‌تر است.

این دو روایت تأیید می‌کند این مطلب را که واژهٔ «اعزّ» در روایت اوّل به‌معنای صلابت، سرسختی و شکست‌ناپذیری است.

هدف منافقان در پذیرش ولایت کافران، دستیابی به عزت و شکوه است، درحالی‌که تمامی عزت، تنها از آن خداوند است و پذیرش ولایت کفار، هرگز مایهٔ عزّت و سربلندی نیست، بلکه چون از عزت واقعی تهی‌اند، تکیه بر آنان، خسران است. این آیهٔ شریفه، دعوتی است ضمنی که برای دستیابی به عزت پایدار، به خداوند روی آورید! چرا که اعتقاد به عزت و قدرت مطلقه الهی، مانع گرایش به عزت و اقتدار موهوم کافران می‌گردد. اینکه منافقان، عزت را در ولایت کافران می‌جویند، نوعی نفاق سیاسی است که از نفاق عقیدتی آنان ناشی می‌شود (هاشمی‌رفسنجانی: ۱۱۰-۱۰۹) و مایه سرسپردگی و وابستگی سیاسی و روحی به بیگانگان و عدم استقلال در عرصه‌های بین‌المللی است. اما مؤمنان، چون به خدا ایمان می‌آورند، همهٔ عزت از آن آنهاست، از نظر سیاسی نیز عزتمند بوده و ولایت بیگانه را نمی‌پذیرند.

در واقع، کسب عزت، تنها در گرو پذیرش ولایت خداوند است: «یقولون لئن رجعنا إلی المدینهٔ لیخرجنّ الأعزّ منها الأذلّ، و للّه العزّهٔ و لرسوله و للمؤمنین و لکنّ المنافقین لایعلمون» (قرآن مجید، سوره منافقون: آیه ۸).

در سایه عزت الهی است که جامعه اسلامی بر کفار و منافقان پیروز می‌شود و همواره عزتمند و شرافتمند می‌زید: «و لینصرنّ اللّه من ینصره إنّ اللّه لقویّ عزیز» (قرآن مجید، سوره حج: آیه ۴۰)؛ «کتب اللّه لأغلبنّ أنا و رسلی إنّ اللّه قویّ عزیز» (قرآن مجید، سوره مجادله: آیه ۲۱).

اگر می‌بینیم در بعضی از آیات قرآن "عزت" را علاوه بر خداوند، برای پیامبر(ص) و مؤمنان قرار می‌دهد "وَ لِلَّهِ الْعِزَّةُ وَ لِرَسُولِهِ وَ لِلْمُؤْمِنِینَ" (قرآن مجید، سوره منافقون: آیه ۸).

به خاطر آن است که آنها نیز از پرتو عزت پروردگار کسب عزت کرده‌اند، و در مسیر طاعت او گام بر می‌دارند.

ضمنا مؤمن اجازه ندارد عزت نفس خود را جریحه‌دار نموده و خود را ذلیل و خوار کند. در روایت آمده: خداوند همه کارهای مؤمن را به او واگذار کرده جز اینکه به او اجازه نداده است که

خود را ذلیل و خوار کند، مگر نمی‌بینی خداوند در این‌باره فرموده: عزت مخصوص خدا، رسول او و مؤمنان است. سزاوار است مؤمن همیشه عزیز باشد، و ذلیل نباشد (نورالثقلین: ۳۳۶).

در روایتی از امام حسن(ع) آمده: "و اذا اردت عزا بلا عشیرهٔ، و هیبهٔ بلا سلطان، فاخرج من ذل معصیهٔ اللّه الی عز طاعهٔ اللّه"؛ هرگاه بخواهی بدون داشتن قبیله، عزیز باشی، و بدون قدرت حکومت، هیبت داشته باشی، از سایه ذلت معصیت خدا بدر آی و در پناه عزت اطاعت او قرار گیر! (بحارالانوار: ۱۳۹).

شاخصه‌های عزت

عزت به‌معنای چیزی که قاهر است و نه مقهور و غالب است و نه مغلوب، مختص خدای عزوجل است، چون غیر از خدای متعال هرکس را فرض کنیم در ذاتش فقیر و در نفسش ذلیل است و چیزی را که نفعش باشد، مالک نیست مگر اینکه خداوند به او ترحم کند و سهمی از عزت به او بدهد؛ مانند دیگر موهبت‌هایی که خداوند متعال به انسان عطا می‌کند و یا از صفات خودش مثل علم، قدرت و حکمت به او می‌بخشد.

در این کاوش چندین دستاویز مهم به‌چشم می‌خورد، که به تشریح هریک از آنها می‌پردازیم؛

الف) عبودیت و تقرب به خدا: «فان العزهٔ لله جمیعاً»، یعنی اگر عزت و سربلندی می‌خواهی نزد خود خداست و بر توست که از خود او درخواست کنی؛ بلکه اساساً خداوند متعال که خود عزیز است، عزت را برای مؤمنین و دوستان خودش هم می‌خواهد و به آنها اجازه نمی‌دهد که کاری بکنند تا عزت و سربلندیشان از بین برود.

ب) حذر کردن از کافرین: انسان برای رسیدن به هر هدفی باید یک سلسله کارها را انجام دهد و از یک دسته کارها بپرهیزد، یعنی اگر اموری مانع رسیدن او به مقصد می‌باشند که در واقع دشمنانِ هدف او هستند، باید آنها را از پیش پای خود بردارد؛ عزت مؤمن همان دین اوست" و سربلندی و افتخار او تحت سربلندی و عزت خدا شکل می‌گیرد، لذا می‌توان گفت که دشمنانِ عزت مؤمن، دشمنان دین و خدا هستند و خداوند متعال همان‌گونه که بایدهای ما را بیان نموده است، در باب نبایدها، نحوه رفتار مؤمنین با دشمنان را به‌گونه‌ای بیان کرده تا عزتشان پایمال نگردد.

ج) نفی هرگونه سلطه کافرین: خداوند متعال با سلطه کافرین بر مؤمنین موافق نیست و آن را به‌شدت نفی می‌کند و می‌فرماید: «و لن یجعل الله الکافرین علی المؤمنین سبیلاً» (قرآن مجید، سوره نساء: آیه ۱۴۱). پس بر مؤمنین واجب است که تا آنجا که می‌توانند دست زور و ستم کافرین را از سر خود کوتاه کنند و در هیچ یک از مسائل اعم از فرهنگی، سیاسی، اقتصادی، اجتماعی و... به کافرین اندک نرمش و ملایمتی که سبب ذره‌ای تسلط آنها بر خودشان شود، نشان ندهند.

د) حذر کردن از دوستی با کافرین: در مرتبه بالاتر دوستی با کافران را هم جایز ندانسته و آن را حجتی آشکار بر علیه مؤمنین می‌داند و می‌فرماید: «یا ایها الذین امنوا لاتتخذو الکافرین اولیاء اتریدون ان تجعلو الله علیکم سلطاناً جیناً» (قرآن مجید، سوره نساء: آیه ۱۴۴) و در آیه‌ای دیگر به دوستی‌گرفتن کافرین را نشانه عزت داشتن کافرین می‌داند و با بیان اینکه هیچ عزتی در نزد آنها نیست، مؤمنین را از موالات و دوستی با آنها برحذر می‌دارد و می‌فرماید: «الذین یتخذون الکافرین اولیاء من دون المؤمنین ایبتغون عندهم العزة فان العزة لله جمعیاً». اینکه کافرین هیچ عزتی ندارند به این دلیل است که عزت همواره از علم و قدرت سرچشمه می‌گیرد و آنها که هیچ علم و قدرتی ندارند، مسلم هیچ عزتی هم نخواهند داشت. خداوند در وصف آنها فرموده: «لهم قلوب لایفقعور لا یفقحون بها و لهم اعین لایبصرون بها و لهم اذان لایسمعون بها» (قرآن مجید، سوره اعراف: آیه ۱۷۹).

با استدلالی که بیان شد، معلوم گردید که کافرین هیچ عزتی ندارند، اما در هرصورت باز دوستی با آنها جایز نیست زیرا که قابل‌اعتماد نیستند؛ هرگاه منافعشان اقتضاء کند، بی‌درنگ صمیمی‌ترین دوستان و متحدان خود را رها کرده و به سراغ منافع و سودجویی خود می‌روند، چنان که گویی هرگز با هم آشنایی نداشته‌اند (کان لم تکن بینکم و بینه مودة)؛ چرا که کافران دینی ندارند که آنها را پایبند تعهدات خود کند. وفاکردن و نکردن به وعده برایشان یکسان است و بالطبع تعهدگرفتن و نگرفتن از آنها مساوی است و نمی‌توان براساس آنچه آنها تضمین کرده و تعهد داده‌اند، برنامه‌ریزی کرد و با تکیه بر آن کاری انجام داد. خداوند این مطلب را به زیبایی ضمن مثالی بیان می‌کند، آنجا که می‌فرماید: «مثل الذین اتخذوا من دون الله اولیاء کمثل العنکبوت اتخذت بیناً بیت‌الله و ان اوهن البیوت العنکبوت لو کانوا یعلمون» (قرآن مجید، سوره عنکبوت: آیه ۴۱). در آیه ۵۳ سوره مبارکه مائده این مطلب به وضوح بیان شده که

می‌فرماید: «و یقول الذین امنوا هؤالاء استموا بالله جهد ایمانهم انهم لمعکم». در این آیه، مراد از هولاء یهود و نصاری هستند و معکم خطاب به منافقین است. یعنی مؤمنان در آن روز به منافقان گویند که آیا این یهود و نصاری که سوگند موکد یاد کردند که با شما و حامی شما خواهند بود پس چرا به دادتان نرسیدند. «حبطت اعمالهم فاصبحوا خاسرین»، یعنی زحمتی که در موالات کفار کشیده و برای روز مبادا آنها را پشتیبان خود قرار داده‌اند، پوچ و بی‌فایده خواهد شد.

دوستی با کفار یعنی روآوردن به دشمن عزت و بزرگی، یعنی احساس نیاز و فقر، ذلیل‌تر و پست‌تر بودن و در یک کلام یعنی ذلت محض.

خداوند حتی در آیه ۵۱ سوره مبارکه مائده دوستی با کافرین را ارتداد دانسته و می‌فرماید: «یا ایها الذین امنوا لاتتخذو الیهود و النصاری اولیاء بعضهم اولیاء بعض و من یتولهم منکم فانه منهم». باتوجه به این آیات، دیگر جای تردید باقی نمی‌ماند که دوستی با کافرین چه ذلتی به دنبال خواهد داشت.

هـ) شدت و غلظت نسبت به کافرین: خداوند نسبت به دشمنِ عزت مؤمنین، تا همین حد هم بسنده نمی‌کند؛ بلکه قدم فراتر نهاده و از آنها می‌خواهد نسبت به کفار سختگیر و خشن بوده و از خود غلظت و درشتی نشان دهند.

خداوند عزیز و قادر از مؤمنین می‌خواهد، همان عزت و اقتداری را که در برابر دشمنان خود و خدا دارند (عزت و افتخاری را که در سایه دینداری بدست آورده‌اند)، هرگز و به هیچ قیمتی نفروشند.

عوامل دستیابی به عزّت حقیقی

حال که منشأ حقیقی عزّت مشخّص شد و معلوم گردید که تنها راه دستیابی به عزّت حقیقی اتّصال به منبع اصلی آن و جستجوی عزّت از جانب اوست، سئوال اصلی این است که راه عملی رسیدن به این عزّت چیست و اساساً قرآن کریم چه راه‌کارهایی را در این جهت ارائه داده است.

در جواب باید گفت که برای رسیدن به عزّت، راهی جز پیمودن طریق عبودیّت خداوند وجود ندارد و عبودیت نیز در دو چیز خلاصه می‌شود؛ یکی ایمان و دیگری عمل صالح.

خداوند در ضمن آیه‌ای با اشاره به منشأ حقیقی عزّت، راه‌کار عملی آن را نیز معرفی کرده است: «من کان یرید العزّة فلله العزّة جمیعا، الیه یصعد الکلم الطیّب و العمل الصالح یرفعه» (قرآن مجید، سوره منافقون: آیه ۸).

موجبات ذلت

با دقت در آنچه گذشت، اموری که موجب ذلت و خواری انسان است، معلوم می‌گردد، زیرا عمل‌نکردن و سازگارنبودن با موجبات عزت، سبب ذلت خواهد بود لکن برای توضیح بیشتر، برخی از عوامل ذلت را یاد آور می‌شویم:

۱- نفاق و دوستی با کافران

خداوند متعال در قرآن مجید بیان می‌فرماید: که عزت تنها از آن خدا، پیامبرش و مومنین می‌باشد ولیکن منافقین درک نمی‌کنند و در آیه دیگر به منافقین که کافران را دوست می‌دارند و در پی کسب عزت در پیش آنان هستند وعده عذاب می‌دهد. بشر المنافقین بان لهم عذابا الیما. الذین یتخذون الکافرین اولیاء من دون المومنین ایبتغون عندهم العزه لله جمیعا (قرآن مجید، سوره نساء: آیه ۱۳۹ و ۱۳۸) و مژده بدهید منافقین را به اینکه عذاب دردناک برایشان (مقرر) است. آنان که مومنان را ترک گفته و کافران را دوست گرفتند، آیا عزت را در پیش ایشان جستجو می‌کنند پس همانا تمام عزت برای خداست.

۲- عزت از غیرخدا

چنان که از آیه شریفه معلوم شد تمام عزت برای خداست پس هر کس غیر از خداوند متعال طلب عزت نماید و به‌خاطر کسب شرف و کرامت به‌سوی غیرخدا دست دراز کند، ذلیل خواهد شد.

امیرالمؤمنین(ع) در این باره می‌فرماید: من اعتز بغیر الله سبحانه ذل (الحکم الزاهره: ۲۶۵) هر کس به غیر خدا عزت یابد، ذلیل شود و به همین مضمون از رسول خدا(ص) نیز روایت شده است که: من اعتز بالعبید اذله الله (دانش‌پژوه: ۴۸) هر کس به بندگان عزیز گردد خدای تعالی وی را ذلیل کند.

۳- ترک جهاد

رسول خدا (ص) می‌فرماید: للجنه باب یقال له باب المجاهدین... قال: فمن ترک الجهاد البسه الله ذلا و فقرا فی معیشته و محقا فی دینه (آثارالصادقین: ۳۹۶). بهشت دری دارد که به آن باب مجاهدان گفته می‌شود... و فرمود: پس هرکس جهاد را ترک کند خداوند لباس مذلت را به او می‌پوشاند... چنان‌که جهاد تنها موجب عزت برای نسل جهادگر در هر عصر نیست، بلکه موجب سرافرازی نسل‌های آینده نیز می‌باشد، در مقابل ترک جهاد هم موجب ذلت و سرافکندگی برای نسل حاضر و آینده می‌شود. امیرالمؤمنین (ع) می‌فرماید:

فعاودوا الکر و استحیوا من الفر، فانه عار فی الاعقاب، و نار یوم الحساب (نهج‌البلاغه: خطبه ۶۶) پس پشت سرهم حمله آورید و از فرار شرم کنید که موجب سرافکندگی و عار در نسل‌های بعد و نیز سبب آتش در روز حساب است.

۴- سستی در جهاد و فرصت‌دادن به دشمن

باید به‌موقع و در اولین فرصت ممکن به جهاد اقدام کرد و فرصت را از دست دشمن خارج نمود و با ابتکار عمل، سرعت عمل و هوشیاری نظامی، دشمن را سرکوب کرد. در غیر این‌صورت اهمال در جهاد و فرصت‌دادن به دشمن، موجب ذلت خواهد شد. امیرالمؤمنین(ع) می‌فرماید: ...و قلت لکم اغزوهم قبل ان یغزوکم فوالله ما غزی قوم قط فی عقر دارهم الا ذلوا... (نهج‌البلاغه: خطبه ۲۷) ...و گفتم با آنان بستیزید پیش از آنکه بر شما حمله برند و به خدا سوگند با مردمی در آستانه خانه‌شان نجنگیدند جز که جامه‌خواری بر آن مردم پوشاندند.

۵- اختلاف و تشتت

اختلاف و تشتت هر ملتی موجب ذلت، هلاکت و اسارت آنان در بند دشمنان خواهد بود. قرآن کریم می‌فرماید: و لاتنازعوا فتفشلوا و تذهب ریحکم (قرآن مجید، سوره انفال: آیه ۴۶) راه نزاع و اختلاف نپیمایید که سست شوید و شوکت و قدرت شما از بین برود. در سخن معجزه‌آسای علی (ع) نیز درباره امت‌های گذشته و موجبات ذلت ایشان چنین آمده است: ...پس بنگرید که پایان کارشان به کجا کشید. چون میانشان جدایی افتاد و الفت به پراکندگی انجامید و سخن‌ها و دلهاشان متفرق گردید. ازهم جدا شدند و به حزب‌ها گراییدند و خدا لباس کرامت خود را از تنشان برون آورد و نعمت فراخ خویش از دستشان به دور کرد... (نهج‌البلاغه: خطبه ۱۹۲)

۶- زیر سلطه‌بودن

انسانی که خداوند او را آزاد آفریده، اگر به اختیار خود، طوق بندگی قلدران حاکم را به گردن افکند، شرافت انسانی خود را نابود کرده است. امیرمومنان(ع) می‌فرماید: ...و لاتکن عبد غیرک و قد جعلک الله حرا (میزان‌الحکمه: ۴۴۱) ...بنده دیگران مباش در حالی که خداوند تو را آزاد آفریده است و در بیانی دیگر می‌فرماید: کل عزیز داخل تحت القدره فذلیل (میزان‌الحکمه: ص ۲۸۶) هر ارجمندی که تحت سیطره قدرتی باشد ذلیل است.

۷- تجمل‌پرستی

تجمل‌پرستی و تشریفات‌گرایی موجب نیازمندی و وابستگی است؛ زیرا زندگی تشریفاتی حد و مرزی ندارد تا با رسیدن به آن نیاز مرتفع شود و از جهت همین نیاز، وابستگی پیش می‌آید. وابستگی به افراد یا منابعی که این نیازمندی را بتوانند برطرف کنند، موجب ذلت و خواری برای انسان می‌شود؛ زیرا تامین‌کنندگان این‌گونه نیازها به‌شرط تامین منافع خود و بهره‌بری از شخص وابسته، اقدام به این کار می‌کنند. اصولا وابسته‌شدن به زندگی و تشریفات آن، برای همه به ویژه نیروهای‌مسلح خطرناک است حتی اگر وابستگی به اشخاص زر اندوز و زورمند هم پیش نیاید، نفس دل بستن به جلوه‌های رنگارنگ زندگی مادی و پیوسته دنبال تجملات‌بودن انسان را از رسیدن به اهداف عالی باز می‌دارد و باعث تحقیر شخصیت انسان و در نتیجه ذلت خواهد شد و اگر فرهنگ اسراف و تجمل‌پرستی بر نیروهای‌مسلح حاکم گردد و نظامیان به آنها خو کنند، دیگر انتظار شجاعت، استواری مقاومت و دشمن‌ستیزی از چنین نیرویی بیهوده خواهد بود. چنان که تجربه نشان داده است.

خداوند متعال در قرآن‌کریم می‌فرماید: ای پیامبر بگو؛ - امت را - اگر شما پدران، فرزندان، برادران، زنان، خویشاوندان و اموالی که جمع آورده‌اید و تجارتی که از کسادی آن بیمناکید و منازلی را که به آن دل‌خوش داشته‌اید، بیش از خدا، رسولش و جهاد در راه او دوست می‌دارید، پس منتظر باشید تا امر خدا برسد - و دنیاطلبان بدکار از کار خویش پشتیبان شوند - و خداوند بدکاران را - به راه بهشت و سعادت - هدایت نخواهد کرد (قرآن مجید، سوره توبه: آیه ۲۴).

۸- اخلاق ناپسند

رفتارهای ناپسند و مذموم، موجبات ذلت انسان را فراهم می کند. امیرالمؤمنین(ع) می‌فرماید: ...و ایاکم و الاخلاق الدنیه فانها تضع الشریف و تهدم المجد (میزان‌الحکمه: ۱۴۶) برحذر باشید از اخلاق پست، چرا که انسان بزرگوار را پست می‌کند و مجد و کرامت را نابود می‌سازد و ازجمله اخلاق‌های زشت که انسان را به خواری دچار می‌کند تکبر و دروغگویی است. علی(ع) می‌فرماید: من تکبر علی الناس ذل (همان: ۳۱۶) هر کس با مردم با تکبر برخورد کند ذلیل می‌شود. امیرالمؤمنین(ع) می‌فرماید: و ان الکاذب لمهان ذلیل (همان: ۲۸۷) همانا دروغگو پست و خوار است.

بخش ۴- جهاد کبیر

جهاد در فرهنگ قرآن از بار معنایی خاصی برخوردار است و پیامبر اکرم(ص) در طی سال‌ها اقامت در مدینه، متناسب با شرایط دورهٔ هجرت و تشکیل حکومت اسلامی، به هر مناسبتی بخش‌هایی از این مفهوم متعالی را رونمایی می‌کردند و جامعه اسلامی را بدان توجه می‌دادند.

مفهوم عرفی و متبادر به ذهن از جهاد همان جنگ فیزیکی، درگیری و مقاتله با دشمن خارجی است که نهایتاً به فوز عظیم پیروزی ختم می‌گردد. برداشت جامعه جوان مدینه از جهاد، نبرد با دشمنان اسلام، کفار، مشرکین قریش و رومیان بود، مسلمانان پس از آن همه جان‌فشانی و تقدیم شهید، فکر می‌کردند که مسئولیت بزرگی را به سامان رسانده‌اند و با خوشحالی صحنه‌های نبرد را برای خود بازگو می‌کردند ولی پیامبر(ص) خطاب به این رزمندگان عرصه‌های سخت فرمود: «مرحباً بقوم فصواالاجهاد الاصغر و بقی علیهم الجهاد الاکبر»[1]: (آفرین به رزمندگانی که جهاد با دشمن خارجی و کفار و مشرکین را پشت سرگذاشتند و هم‌اکنون خود را برای رویارویی در جهاد اکبر آماده می‌سازند.)

رزمندگان خطاب به نبی خاتم(ص) عرض کردند یا رسول‌الله این جنگ‌های سخت و طاقت‌فرسا مگر جنگ و نبرد با دشمن نبود؟ حضرت پاسخ دادند: بلی این نبرد کوچک بود، هنوز کار شما تمام نشده و جهاد بزرگ‌تر باقی مانده است خود را برای آن آماده سازید. روش تربیتی

---

۱ - وسائل، ج۱۱، ص۱۲۲

پیامبر(ص) آماده‌سازی جامعه اسلامی برای صعود به قله‌های برتر ایمانی و اخلاقی است و پیامبر(ص) این روش‌ها را به آرامی در صحنه‌های گوناگون به‌صورت عملی و عملیاتی به پیروانش تعلیم می‌دهد.

در این واقعه پیامبر(ص) کلیت موضوع جهاد را در ذهن رزمندگان و مسلمانان به دو قسمت تقسیم می‌نماید و می‌فرماید: جهاد دو قسم است. جهاد اصغر - جنگ با دشمن خارجی و جهاد اکبر؛ یعنی جهاد و نبرد با دشمن درون، جنگ با نفس اماره، مقاتله با خواسته‌های نفسانی و میل به آرامش و خمودی که طبعاً پس از هر دوره‌ای پیش می‌آید و طبق فرمایش پیامبر اعظم(ص) ارزش و اجر جهاد با نفس یعنی جهاد تزکیه و خودسازی به‌دلیل ارتباط اصیل آن با بعثت انبیاء و اصل آفرینش انسان از همه جهادها برتر و بافضیلت‌تر است.

در این جمله کوتاه نبوی مسیر و نقشهٔ راه مسلمانان روشن شد که مسلمانان حق توقف و ایستایی ندارند. دائماً باید حرکات دشمن را؛ چه دشمن درونی (جنگ با نفس) و چه دشمن برونی، چه در جنگ نرم و چه در جنگ سخت زیرنظر داشته باشند. بدیهی است راه رسیدن به این قله با عظمت، اولاً کار هر کس نیست و ثانیاً بایستی موانع را از میان برداشت تا به پیروزی رسید.

دستور جامع دربارهٔ جهاد

قرآن کریم شش دستور در زمینهٔ جنگ و جهاد می‌دهد:

۱- هنگامی که با گروهی از دشمنان مواجه شدید، ثابت قدم باشید. «**یا ایّها الّذین امنوا اذا لقیتم فئهٔ فاثبتوا**»

۲- خداوندر ا فراوان یاد کنید تا پیروز شوید. «**و اذکروا اللّه کثیرا لعلّکم تفلحون**» (قرآن مجید، سوره انفال: آیه ۴۵)

۳- از خدا و پیامبر اطاعت کنید. «**و اطیعوا اللّه و رسوله**»

۴- نزاع و کشمکش نکنید مبادا سست شوید و قدرت و هیبت شما از میان برود. «**و لا تنازعوا فتفشلوا و تذهب ریحکم**»

۵- صبر و استقامت کنید که خداوند با صابران است. «**و اصبروا إنّ اللّه مع الصّابرین**» (قرآن مجید، سوره انفال: آیه ۴۶)

۶- مانند کسانی نباشید که از سرزمین خود از روی غرور و هوا پرستی و خودنمایی خارج شدند. «**و لا تکونوا کالّذین خرجوا من دیارهم بطرا و رئاء النّاس**» (قرآن مجید، سوره انفال: آیه ۴۷)

مجموع این امور شش‌گانه، دستور جامعی است که همهٔ امور نظامی را دربر می‌گیرد.

بنابراین اسلام جهاد را به‌عنوان نیروی بازدارنده دشمن از نبرد و خونریزی قرار داده و چنانچه بر اثر خیره‌سری دشمن، مسلمانان مجبور شوند دست به اسلحه ببرند، این کار تنها در حدّ ضرورت جایز است و هر زمان دشمن از کار خود پشیمان گردید و واقعاً طالب صلح بود، باید دست از جهاد کشید و صلح کرد.

نتیجه اینکه جهاد از منظر اسلام خشونت، خونریزی، کشتار، ویرانی، قتل و غارت نیست، بلکه درحقیقت سیستم دفاعی قوی و مستحکمی است که همچون سیستم دفاعی طبیعی نهادینه‌شده در بدن تمام موجودات، زندگی بدون آن امکان‌پذیر نیست و باعث جلوگیری از درگیری‌های نظامی و خشونت دشمن می‌گردد و چنین جهادی آن‌قدر ارزشمند و پربهاست که خداوند نه‌تنها به رزمندگان جان برکف آن و مرکب‌هایی که رزمندگان را حمل می‌کنند، بلکه به جرقّه حاصل از برخورد سمّ اسبان رزمندگان با سنگ‌های روی زمین سوگند یاد می‌کند.

مفهوم‌شناسی جهاد و انواع آن

واژه جهاد از واژه عربی جَهد و جُهد به‌معنای مشقت و سختی بسیار (معجم مقاییس‌اللّغه: ۴۸۶)، کوشش، تلاش سخت و کامل است. البته به زمین سخت که در آن گیاه نروید نیز جَهَاد می‌گویند که جمع آن جُهُد است. واژه جُهْد نیز به‌معنای نیرو و توانایی به‌کار می‌رود. از همین‌روست که گفته می‌شود: بَذَلَ جُهْدَهُ: تمام نیروی خود را به‌کار بُرد. یا گفته می‌شود: أجْهَدَ الدابّةَ: ستور را بیش از طاقتش بار کرد.

پس واژهٔ جهاد نیرو و توان فوق‌العاده‌ای را در کاری سخت و مشقت‌بار هزینه‌کردن است. زمین سخت را نیز به‌خاطر آنکه غیر قابل‌نفوذ است جُهد می‌گویند تا سخت‌کاری و مشقت آن را بیان کنند. اینکه می‌گویند: جهدالحق به‌معنای آشکارشدن حق است که البته به سختی از درون باطل و شبهات آشکار می‌شود؛ و یا جهدالمال به‌معنای هزینه بیهوده است؛ یعنی مشقت

مالی و توان و نیروی خود را در جایی صرف‌کردن که هیچ سودی ندارد؛ چنانکه کسی در زمین سخت و بی‌حاصل با مشقت بخواهد گیاهی برویاند یا آبی را به چنگ آورد.

به هرحال، به هر کوشش و تلاشی جهاد گفته نمی‌شود؛ بلکه تلاش و کوششی تمام و کامل همراه با سختی و مشقت را جهاد می‌گویند.

در اصطلاح فقهی جهاد تنها به جهاد با مال، جان در برابر متجاوزان و دشمنان، دفاع از سرزمین، مال و جان مسلمانان گفته می‌شود، اما در فرهنگ قرآنی جهاد اصطلاحی فراگیرتر است. از این‌روست که صاحب جواهر، جهاد در مفهوم شرعی را که همان مفهوم برگرفته از قرآن است، به بذل جان، مال و توان خویش در راه اعتلای کلمه اسلام و اقامه شعائر ایمان تعریف و تفسیر کرده است (جواهرالکلام: ۳).

باتوجه به‌معنای پیش‌گفته که جهاد به‌معنای هرگونه تلاش مشقت‌آمیز برای ارتقای نفس، اعتلای کلمه اسلام و اقامه شعائر اسلامی دانسته شد، باید گفت که جهاد دارای اقسامی است. براساس یک تقسیم‌بندی می‌توان گفت که جهاد در قرآن و روایات سه گونه است: اصغر، کبیر و اکبر.

در ادامه به اقسام جهاد اشاره می‌شود:

الف) جهاد اصغر

مقاتله و جنگ در جبهه و رزم با دشمنان اسلام است. «**فیقتلون و یقتلون**» (قرآن مجید، سوره توبه: آیه ۱۱۱).

جهاد یعنی مبارزه یعنی تلاش برای مقابله با دشمن

قبلا نیز به‌صورتی دیگر بیان گردید که معیار جهاد، شمشیر و میدان جنگ نیست. معیار جهاد، همان چیزی است که امروز در زبان فارسی، در کلمه «مبارزه» وجود دارد. فلانی آدم مبارزی است؛ فلانی آدم مبارزی نیست. نویسندهٔ مبارز و نویسندهٔ غیرمبارز، عالِم مبارز و عالِم غیرمبارز، دانشجوی مبارز و دانشجوی غیرمبارز، طلبهٔ مبارز و طلبهٔ غیرمبارز. جامعهٔ مبارز و جامعهٔ غیرمبارز؛ پس جهاد یعنی "مبارزه". در مبارزه، دو چیز حتماً لازم است؛ اینکه در آن جدّ، جُهد و تحرکی باشد (بیانات مقام معظم‌رهبری در شروع درس خارج فقه، تاریخ۲۰/ ۰۶/ ۱۳۷۳).

جهاد، فقط به‌معنای حضور در میدان جنگ نیست، زیرا هرگونه تلاش در مقابله با دشمن، می‌تواند جهاد تلقّی شود. البته بعضی افراد ممکن است کاری انجام دهند، زحمتی بکشند و از آن، تعبیر به جهاد کنند، اما این تعبیر، درست نیست چون یک شرط جهاد، این است که در مقابله با دشمن باشد. این مقابله، یک‌وقت در میدان جنگِ مسلّحانه است که «جهاد رزمی» نام دارد، یک‌وقت در میدان سیاست است که «جهاد سیاسی» نامیده می‌شود، یک‌وقت در میدان مسائل فرهنگی است که به «جهاد فرهنگی» تعبیر می‌شود و یک‌وقت هم در میدان سازندگی است که به آن «جهاد سازندگی» اطلاق می‌گردد. البته جهاد، با عنوان‌های دیگر و در میدان‌های دیگر هم هست. پس، شرط اوّلِ جهاد این است که در آن تلاش و کوشش باشد و شرط دومش اینکه، در مقابل دشمن صورت گیرد (بیانات مقام معظم‌رهبری در دیدار فرماندهان لشکر ۲۷ محمد رسول‌الله(ص)، ۱۳۷۵/۰۳/۲۰).

ب: جهاد کبیر

جهاد علمی و فرهنگی است که به‌وسیلهٔ معارف قرآن کریم با کژی‌ها و انحرافات در جامعه مبارزه می‌شود. قرآن کریم در این زمینه به پیامبر اکرم(ص) می‌فرماید: «**فلا تطع الکافرین و جاهدهم به جهادا کبیرا**» (قرآن مجید، سوره فرقان: آیه ۵۲). پس تو هرگز از کافران فرمان مبر و در راه حق، عدالت و خشنودی خدای یکتا، به‌وسیلهٔ این کتاب پرشکوه با آنان به جهادی بزرگ بپرداز و روشنگری کن. برترین و پرشکوه‌ترین جهادها و تلاش‌ها در پیشگاه خدا، جهاد علمی، فکری و فرهنگی است. جهاد کسانی است که با روشنگری خویش بافته‌ها، ساخته‌ها و شبهات بد اندیشان و گمراه‌گران را از اذهان و افکار می‌زدایند و مردم را با روح و جان دین خدا و هدف‌های بلند آن آشنا می‌سازند. زیرا جهادی است که گفتمان درست فکری و فرهنگی را به جامعه ارائه می‌دهد و اجازه نمی‌دهد تا گفتمان باطل مستبدانه با سرکوب افکار و فرهنگ‌های عقلانی و عقلایی دیگر بر جامعه مسلط شود.

در روایات جوهر سیاه قلم عالم از خون سرخ شهید برتر دانسته شده است. «**مداد العلماء افضل من دماء الشهدا**» (گفتار فلسفی: ۱۴۲). این تفضیل از آن‌روست که جهادهای مالی و جانی، زمینه‌ساز فرصتی برای گفتمان علمی و فرهنگی در جوامع بشری و رهایی بشر از گفتمان ستمگرانی است که با استبداد رای و خودکامگی، هرگونه اندیشه‌های رقیب را سرکوب

کرده و ضدارزش‌ها را جایگزین ارزش‌ها و هنجارهای رفتاری می‌کنند. تلاشی که انسان در جهاد کبیر می‌کند، رهایی خود و دیگران از تسلط فکری و فرهنگی است و اجازه نمی‌دهد تا گفتمان باطل، بینش و نگرش او را سامان دهد و رفتارش را تحت‌کنترل درآورد و او را بنده فکری و فرهنگی خود سازد. در جهاداکبر، انسان به خودش اجازه نمی‌دهد تا هواهای نفسانی بر او چیره شود.

تعریف جهاد کبیر

نفوذناپذیری مؤمنان در برابر کافران یا به عبارت دیگر: مقاومت و تسلیم‌ناپذیری اهل ایمان در مقابل دشمنان قرآن.

الزامات جهاد کبیر

برای آمادگی و ورود به این نبرد جدید دو شرط اساسی لازم است که عبارتند از:

۱- شناخت دشمن و راهبردهای جدید او

۲- افزودن بصیرت و آگاهی عمومی

الف) دشمن شناسی:

اگرچه ظاهر قضیه مشخص است که استکبار جهانی و در رأس آن دولت آمریکا که امام بزرگوار به حق او را شیطان بزرگ نامید با همهٔ امکانات خود و سازکار لازم و با وجود ناکامی‌ها و شکست‌های پی‌درپی که در مصاف با انقلاب اسلامی و نظام جمهوری‌اسلامی داشته است نه‌تنها مأیوس نگردیده بلکه خشمگینانه‌تر و غضبناک‌تر وارد مرحله دیگری از جنگ با انقلاب که فوق‌العاده خطرناک‌تر و پیچیده‌تر می‌باشد گردیده است و به طراحی و تهیه راهبرد برای شکست انقلاب اسلامی و در واقع پایان همیشگی این پدیده نوظهور وارد صحنه عملیات جدید گردیده است و تمام عِده و عُده خود را به‌کار گرفته و صحنه جنگ و مبارزه را آن‌قدر توسعه داده است به‌گونه‌ای که همه ابزارهای خود را در سطح جهانی، منطقه‌ای در غرب آسیا و در داخل کشور به‌کار گرفته است.

اگر به گذشته ۴ دهه تهاجمات دشمن بعد از پیروزی انقلاب اسلامی مراجعه کنیم ملاحظه می‌گردد که دولت آمریکا در سه مرحله تهاجمات خود را به انقلاب ارتقاء داده است.

در طول ۱۰ ساله اول انقلاب، با یک جنگ سخت همه‌جانبه در درون کشور وارد این جنگ گردید، به‌گونه‌ای از ۱۷توطئه براندازانه همچون راه‌اندازی منازعات قومی، فعال‌کردن گروه‌های تروریستی، جنگ‌های تجاوزکارانه، منازعات تجزیه‌طلبانه قومی و فتنه‌ها دست زد که با نصرت الهی و حضور ملت انقلابی در صحنه، تمامی این توطئه‌ها خنثی گردید و دشمن از برخورد و رویارویی سخت‌افزارانه با این انقلاب الهی مأیوس گردید (کتاب مدیریت بحران در جمهوری اسلامی، ۱۳۹۴).

در نتیجه راهبرد و روش خود را تغییر داده و وارد مرحله دیگری از جنگ با انقلاب که به آن جنگ نرم می‌گویند گردید. در این مرحله از جنگ و با این تفاوت که اگر جنگ سخت، جنگ افزار است، در این جنگ نرم، جنگ با افکار می‌باشد (شکست دولت آمریکا و اذنابش در این مرحله از جنگ نرم).

و مرحله سوم از این جنگ بی‌امان را تحت‌عنوان نفوذ پایه‌ریزی نموده‌اند. در این مرحله از نبرد می‌بایست با هدف تغییر اساسی در ادراکات، افکار، رفتار و سبک زندگی عموم مردم انقلابی (به‌ویژه جوانان) و با کمک شبکه‌های نفوذی خود در داخل کشور سیاست‌های جدیدی را دنبال می‌کنند که عبارتند از:

- با بزک‌کردن دشمن از او چهره‌ای نه در جایگاه دشمن، بلکه دوست ساخته و در عین‌حال آن را صاحب قدرت و جایگاه عظیم جهانی تعریف کنند.

- مهم‌ترین هدف آن ایجاد تحول و تغییر در افکار، اندیشه‌ها، تغییر رفتار نسل چهارم انقلاب و زمینه‌سازی برای نسل‌های بعدی می‌باشد. در این مسیر باید منبع اقتدار انقلاب که همانا افکار عمومی، توده‌های مؤمن و انقلابی، به‌ویژه جوانان را آن‌چنان به تباهی کشاند و اندیشه‌ها و فرهنگ غربی را به‌جای افکار و اندیشه‌های اسلامی در قلب و روح آنها جایگزین کرد تا به سهولت دروازه‌های کشور را بر روی دشمنان باز نموده و تسلیم بی‌قید و شرط جمهوری اسلامی در مقابل آنها فراهم گردد.

ب) بصیرت‌افزایی:

برای آمادگی و مبارزه در این جهاد کبیر بعد از شناخت دشمن موضوع بصیرت‌افزایی باید در سرلوحه برنامه‌های ما قرار گیرد. تاریخ صدر اسلام نشان می‌دهد ضرباتی که اسلام و مسلمین

خورده‌اند ناشی از بی‌بصیرتی، عدم‌شناخت و درک و تشخیص میان حق و باطل به‌ویژه در میان تودهٔ مردم ناآگاه بوده است.

چه باید کرد؟

ملت انقلابی باید به این باور برسد که در این جنگ درصورت توفیق دشمن بلیه‌ای عظیم و خانمان‌برانداز بر انقلاب و کشور وارد گردیده و حرث و نسل انقلاب را نابود و عرض و ناموس ملت را به مخاطره خواهد افکند و به قول مقام معظم‌رهبری: «اینها می‌خواهند هم اسلام و هم انقلاب را یکجا از این ملت بگیرند.»

ملت نباید منتظر اقدام دولتمردان و حکومت باشد بلکه خود با هر وسیله‌ای که می‌توانند برای این جهاد کبیر و این جنگ بی‌امان علیه دشمن و نفوذی‌های آن آماده باشند. برای مقابله با آن در حوزه‌های فرهنگ، اقتصاد و سیاست به‌صورت فردی و جمعی قیام کنند.

در مرحله اول باید جوانان و فرزندان خود را که دشمن آنها را نشانه گرفته و خطر بزرگی آنها را تهدید می‌کند از این گرداب ولنگاری فرهنگی نجات داد و در مقابل توطئه‌های دشمن به‌ویژه در فضای مجازی واکسینه نمود (محمدی، تاریخ ۱۳۹۵/۳/۲۹).

شرائط تحقق جهاد کبیر

به‌نظر می‌رسد دست‌کم باید دو شرط حاصل شود تا جهاد کبیر تحقق پیدا کند:

۱- شرط قصد قربت (دارای ویژگی‌های درونی؛ هدف‌شناسانه، انگیزه و نیت تقرب به خدا) این همان قیدی است که در جهاد مطرح است و اگر جهاد برای رضای خدای متعال انجام نشود و به اصطلاح "فی‌سبیل‌الله" نباشد، دیگر جهاد نیست و چنین جهادی دیگر از نظر اسلام، ارزشی ندارد.

۲- برهم‌زدن نقشه دشمن (ویژگی‌های بیرونی: عملکردی در جهت عکس خواست دشمنان قرآن) این شرط به صراحت در قرآن کریم آمده است: «**فلاتطع الکافرین و جاهدهم به جهادا کبیرا**» (قرآن مجید، سوره فرقان: آیه ۵۲).

پس کسی که پازل دشمن را کامل کند هرچند فرض کنیم قصد قربت هم داشته باشد؛ ندانسته درحال خدمت به شیطان و دشمنان خدا است.

ابزارهای جهاد کبیر

از آنجایی که جهاد کبیر، جهاد علمی، فکری و فرهنگی است، برخلاف جهادهای فیزیکی و سخت، ابزارهای نرمی لازم است که مورد استفاده قرار گیرد. در جنگ نرم، ابزارهای سخت چون قتل و شکنجه کارایی ندارد و حتی نتیجه عکس می‌دهد و بجای اینکه موجب تسلط فکری و فرهنگی گفتمانی شود، موجب نابودی و تزلزل آن می‌شود. از آنجایی که هدف در جهاد کبیر، تسلط بر اذهان و قلوب است، لازم است تا از ابزارهایی استفاده شود که موجبات تسلط بر قلوب می‌شود. جهادگر در جهاد کبیر و جنگ نرم نمی‌خواهد تا جانی را بستاند و مالی را به غارت ببرد و یا کسی را برده کند؛ بلکه در این فکر است که کسی یا جامعه‌ای را بنده خود کند تا بنده با همه وجودش در خدمت رب و یا ارباب باشد.

جهادگران فرهنگی در گفتمان باطل برای تسلط بر ذهن و قلب بشر از هر ابزار باطل و حقی استفاده می‌کنند؛ زیرا هدف وسیله را برای آنان توجیه می‌کند. آنان از ابزارهای ضداخلاقی و ضدانسانی چون تمسخر، استهزاء، تهمت، افترا و نیز متشابهات و خرافات بهره می‌گیرند تا ذهن و قلب بشر را در اختیار گیرند. اما از آنجایی که مؤمنان در جهاد کبیر در اندیشهٔ تسلط خوبی‌ها، هنجارها، افکار و اندیشه‌های عقلانی و عقلایی هستند، تنها مجاز می‌باشند تا از این ابزارها استفاده کنند و مجاز نیستند از امور خرافی و باطل یا رفتارهای ضداخلاقی و هنجاری برای تبیین و تسلط بر ذهن و قلب استفاده کنند، لذا با محدودیت‌های ابزاری مواجه هستند.

در جهاد فرهنگی و علمی، لازم است تا باتوجه به استعداد و قابلیت‌های مخاطبان، از برهان عقلانی، موعظه‌ها و پندهای عقلایی استفاده کرد و با جدال احسن و گفتمان مناسب خردپسند و مقبول عقلایی، دیگران را نسبت به حقایق آگاه کرد و ایشان را از بندگی ارباب به بندگی خداوند یکتا و یگانه خواند. (قرآن مجید، سوره نحل: آیه ۱۲۵) هدف از جهاد فکری، علمی و فرهنگی آن است که مؤمنان را از تهاجم فکری و فرهنگی دشمن حفظ کرد و با پاسخگویی به شبهات، روشنگری و بصیرت‌زایی یا بصیرت‌افزایی، اجازه نداد تا رفتارهای نابهنجار آنان به شکل فرهنگ بر جامعه مسلط شود و با تخریب حقایق و هنجارهای ارزشی، فکری و فرهنگی؛ جامعه را دچار تردید کند.

پس از کادرسازی و تقویت مبانی فکری، فرهنگی و اخلاقی جامعه ایمانی با بهره‌گیری از عالمان و اندیشمندان، می‌بایست نسبت به افکار، اندیشه‌ها و رفتارهای ضدبشری و اخلاقی کافران و دشمنان واکنش نشان دهد و با برهان، استدلال و جدال احسن دشمن را خلع سلاح کند. بهره‌گیری از گفتمان سالم در همه حال (قرآن مجید، سوره نساء: آیه ۶۳) مراعات اعتدال و میانه‌روی در ارتباط با مردم، هدایت و راهنمایی آنان[۱] (قرآن مجید، سوره اعراف: آیه ۱۹۹) تأکید بر امور فطری و فطریات ازجمله منفعت‌طلبی و ضررگریزی[۲] (قرآن مجید، سوره مائده: آیه ۷۶)، بهره‌گیری از برهان و دلیل عقلانی و عقلایی[۳] (قرآن مجید، سوره آل‌عمران: آیه ۸۶)، بیان فلسفه زندگی و احکام (قرآن مجید، سوره نحل: آیه ۱۲۵)، صراحت‌گویی[۴] (قرآن مجید، سوره حجر: آیه ۹۴) و مانند آن از ابزارها و روش‌هایی است که می‌بایست در جهاد نرم، جهاد کبیر فکری، فرهنگی و عملی به‌کار گرفت.

اخیراً مقام معظم‌رهبری در جلسات مختلف و با یک تحلیل همه‌جانبه از شرایط و اوضاع احوال جهانی، منطقه‌ای و ملی به یک جمع‌بندی جدید رسیده‌اند که ملت و امت انقلابی در داخل کشور و حتی در سراسر جهان باید خود را آماده نموده و جهادی کبیر که، بسیار پیچیده‌تر و حساس‌تر از زمان‌های قبل می‌باشد با دشمنان قسم‌خورده انقلاب (یعنی استکبار جهانی به رهبری آمریکا) وارد کارزار شوند.

جهادی که در قرآن بیان شده است در یک تقسیم‌بندی به دو نوع جهاد اکبر و جهاد اصغر تقسیم می‌شود که یک نوع از انواع جهاد اصغر، «جهاد کبیر» نام دارد. جهاد کبیر در عرصه سیاست شامل فریب‌نخوردن از دشمن و آگاهی از نقشه‌های اوست، در میدان اقتصاد نیز اجرای کامل اقتصاد مقاومتی و هضم‌نشدن در هاضمه اقتصاد جامعه جهانی است. همچنین این جهاد در عرصه اجتماع در به میدان‌آمدن همه استعدادهای موجود در خدمت پیشرفت کشور تعریف می‌شود و در حوزه فرهنگ و هنر نیز امر به انجام کارهای فرهنگی خودجوش توسط جوان‌های مومن و حزب‌اللهی و انقلابی شده است (مقام معظم‌رهبری: تاریخ ۱۳۹۷/۴/۲۸).

---

۱ - سوره انبیاء، آیه ۱۰۹

۲ - سوره انعام، آیه ۷۱

۳ - سوره محمد، آیه ۱۴

۴ - سوره مائده، آیه‌های ۹۲ و ۹۹

پایه‌هایی که پیغمبر(ص) گذاشتند (پایه‌های ایمان، عقلانیت، مجاهدت و عزت) پایه‌های اصلی جامعهٔ اسلامی است. ایمانمان را در دل‌های خود و در عمل خود تقویت کنیم. از خرد انسانی، که هدیهٔ بزرگ الهی به بشر است، استفاده کنیم؛ جهاد فی‌سبیل‌الله را چه در میدان‌های نبرد نظامی (آن وقتی که لازم باشد)، چه در میدان‌های سیاست، اقتصاد و... دنبال کنیم و حس عزت، کرامت انسانی و اسلامی را برای خودمان مغتنم بشماریم (مقام معظم‌رهبری: تاریخ ۱۳۹۰/۴/۹).

تفاوت به‌کارگیری نوع ابزار و تجهیزات در جهاد اصغر و جهاد کبیر

برای پیروزی در هر نوع عملیاتی در هر سطح و میدانی باتوجه به شرایط محیطی و منطقه‌ای نیازمند به‌کارگیری سلاح خاص و تجهیزات مختص آن نبرد است. جهاد اصغر جنگ سخت است و نیازمند جنگ‌افزارهای مخصوص خود، ولی جهاد کبیر از نوع جهاد علمی، فکری و فرهنگی است و برای پیروزی در این جبهه نیازمند نرم‌افزارهای است که توانایی مقابله با تهاجم فکری و فرهنگی دشمن را داشته باشد.

هدف در جهاد کبیر تقویت مبانی فکری و اعتقادی جبهه توحید است. ایجاد آمادگی ذهنی و روانی در مردم است که مرعوب و فریفته برنامه‌ها و سیاست‌های مزورانه دشمن نشوند، هدف ساختن ظرفیت اجتماعی، تولید ابزار و نرم‌افزاری است که بتواند پیوندهای فکری، عاطفی و فرهنگی جامعه را قوام بخشد و ارتقا دهد.

چرا جهاد کبیر از جهاد اصغر با فضیلت‌تر است؟

در پاسخ باید گفت: جهاد اکبر افضل است چون تنها راه رسیدن بشر به مقام خلافت الهی و بدست‌آوردن بار امانت الهی است و این دقیقاً همان مسیر تکامل و تعالی بشر است که انبیاء الهی در طول تاریخ، انسان‌ها را بدان دعوت می‌کردند. در جهاد اکبر انسان به تزکیه و خودسازی می‌پردازد و با اعتدال نفس مانع گرایش آن به فجور و پلیدی می‌گردد و اجازه تسلط هوای نفس را نمی‌دهد و اما در رتبه دوم که نوبت به جهاد کبیر می‌رسد. در این جبهه موضوع جهاد علمی و فرهنگی مطرح است. در جهاد کبیر رزمنده مجاهد در پی تلاش برای رهایی خود و جامعه از تسلط فکری و فرهنگی است می‌جنگد که دشمن او را مخاطره نکند و بینش و رفتار او را تحت‌تأثیر قرار ندهد و لذا جهاد کبیر نشان‌دهنده تقابل علمی و فرهنگی جبهه حق در مقابله با تسلط و حاکمیت سلطه باطل می‌باشد.

جهاد کبیر در مقابل دشمنان یعنی ظرفیت‌سازی، ایجاد آمادگی و تجهیز پیروان جبهه حق به‌صورت عملی در دوران پس از جهاد اصغر که احتمالاً رزمندگان جبهه توحید احساس می‌کنند در پایان جنگ و فرارسیدن دوران صلح، وقت استراحت و آرامش است که این تفکر رفاه و آسودگی خیال؛ عامل اساسی غفلت در جامعه و فراموشی دشمن است.

ارتباط جهاد اصغر با جهاد کبیر چیست؟

عموما پنداشته می‌شود که جهاد اصغر فقط جهاد نظامی با دشمن خارجی است در حالی‌که این پندار درست نیست و هرگونه جهاد و مقابله با دشمنان بیرونی جهاد اصغر است و بنابراین هرگونه جهاد (فرهنگی، اقتصادی، سیاسی و...) با کافران و منافقان نیز از مصادیق جهاد اصغر است که خدای حکیم در قرآن کریم نام آن را جهاد کبیر گذاشته است.

براساس معارف قرآن کریم، دشمنان اسلام هرگز از مسلمانان راضی نخواهند شد، مگر آنکه مسلمین اسلام را رها کنند و پیرو کافران شوند؛ در نتیجه فرمان الهی این است که هرگز نباید در برابر آنان کوچک‌ترین نرمشی نشان دهید و باید در برابرشان محکم و استوار همچون کوه باشید و مقاومت کنید و تسلیم‌ناپذیر باشید.

هرگز یهود و نصاری از تو راضی نخواهند شد تا به‌طور کامل تسلیم خواسته‌های آنها شوی و از آئین (تحریف‌یافته) آنان پیروی کنی بگو هدایت تنها هدایت الهی است و اگر از هوی و هوس‌های آنها پیروی کنی، بعد از آنکه آگاه شوی هیچ سرپرست و یاوری از ناحیه خدا برای تو نخواهد بود. کسانی که کتاب آسمانی، به آنها داده‌ایم (یهود و نصاری) و آن را از روی دقت می‌خوانند، به پیامبر اسلام ایمان می‌آورند و کسانی که به او کافر شوند زیانکارند (قرآن مجید، سوره بقره: آیه ۱۲۰ و ۱۲۱).

برای پی‌بردن به عمق موضوع و بحث جهاد کبیر باید ویژگی‌های این جهاد را شناخت: (بیانات مقام معظم‌رهبری، تاریخ ۱۳۹۵/۳/۳)

۱- برخلاف جهاد اصغر (هرگونه مقابله با دشمن)، که عرصه میدان نظامی و سرشار از شور و هیجان است در جهاد کبیر دارای شور و هیجان‌ها خاموش هست.

۱-درجهاد کبیر به کسی مدال افتخار نمی‌دهند، برای اینکه نتایج بدست‌آمده از این جهاد ملموس نیست.

۳- در جهاد کبیر پیچیدگی وجود دارد، دشمن را به راحتی نمی‌توان دید، در جهاد کبیر صف بندی‌ها و تشخیص‌دادن جهت‌ها و اهداف نیاز به تخصص و بصیرت دارد.

۶-عده‌ای در جهاد کبیر انگیزه‌ها را خشک می‌کنند و خود را مهره دشمن قرار می‌دهند و در عرصه‌های مختلف، روحیه مردم و جهادگران را تضعیف می‌کنند.

پس از تبیین جهاد کبیر و ویژگی‌های این جهاد نیاز است که این موضوع را در زمینه‌های مختلف ازجمله فرهنگی، سیاسی، اقتصادی و فکری بررسی کنیم:

فرهنگ:

تقریبا از دهه ۷۰ و بعد از اتمام جنگ تحمیلی علیه ایران رهبر معظم انقلاب چندین بار بحث شبیخون فرهنگی و ناتوی فرهنگی دشمن علیه فرهنگ کشور را بیان فرمودند. که متاسفانه عده‌ای باور نداشتند و آن را سرسری گرفتند.

اما در زمان فعلی، با ملموس‌شدن این واقعیت، به‌خود آمده‌اند. از موارد تبعیت‌نکردن از دشمن که سبک زندگی اسلامی- ایرانی ما را در امر فرهنگ نشانه رفته است، می‌تواند تدوین و فرهنگ‌سازی تولیدات و همچنین توجه به سبک‌های اسلامی- ایرانی باشد، تا با تکیه بر آن در بحث فرهنگی بتوانیم نقشه‌های دشمنان را خنثی کنیم.

اقتصاد:

در بحث اقتصاد دشمن با طراحی تحریم‌های اقتصادی، القای ناامیدی معیشتی به مردم و باور ناتوانی در اداره امور اقتصادی به بعضی مسئولین کشور، توانسته است در این موضوع نیز بر مردم و تفکرات اقتصادی بعضی از مسئولین تاثیرات منفی بگذارد. نکته‌ای که در این مبحث، عدم‌تبعیت از دشمن (جهاد کبیر) را به ما نشان می‌دهد، تکیه بر توان درون، شناختن استعدادهای جوانان انقلابی و همچنین اجرای سیاست‌های اقتصاد مقاومتی می‌باشد.

سیاست:

امر سیاست مهمترین اقدامات دشمن براندازی های نرم ، القای تفکرات ضد انقلاب اسلامی، ناتوان کردن ایران در سیاست خارجی، منزوی کردن کشور در مجامع بین المللی و... می باشد.

امر جهاد کبیر که همان عدم تبعیت از دشمن است زمانی در امور سیاست کشور خنثی می‌شود که همه افراد جامعه و نخبگان سیاسی کشور دارای وحدت سیاسی باشند و حضور

دشمن در میدان های مختلف این سیاست را درک کنند و همچنین به اصول و اهداف انقلاب اسلامی در سیاست خارجی پایبند بوده و خطوط قرمز آن را بدانند.

فکر و اندیشه:

برای این امر دشمن تمام تلاش خود را بر تغییر باورها، آداب و رسوم، اعتقادات ظاهری، درونی و رفتاری مردم قرار داده است و سعی در استحاله فکری ما را دارد. اندیشه‌های برخواسته از دانشگاه و حوزه‌های علمی ما را به چالش می‌کشد و گاها از مسیر اصلی و هدف خود دور می‌کند. جهاد کبیر و عدم‌تبعیت واقعی از دشمن در این حوزه، هم می‌تواند تدوین علوم اسلامی ایرانی به‌جای متون غربی دانشگاه‌ها، بازسازی علوم انسانی و در آخر کادرسازی و تربیت جوانانی برای انقلاب اسلامی است که با اندیشه انقلاب رشد کرده باشند.

کار جهادی و عدم‌تبعیت از دشمن در مرتبه اول باید از روی اخلاص و نیت برای خدا باشد، در مرتبه دوم همراه با سختی، کوشش دقیق و حساب‌شده باشد و در مرتبه سوم با شناخت و بصیرت در مورد دشمنی (داخلی و خارجی) باشد که در آن حوزه فعالیت می‌کند.

رهبر انقلاب اسلامی خاطرنشان کردند: البته اگر در این جنگ دچار غفلت شویم مغلوب خواهیم شد و اگر دچار ساده‌اندیشی شویم ضربه خواهیم خورد.

حضرت آیت‌الله خامنه‌ای با اشاره به ابعاد جنگ پیچیده اطلاعاتی، فرموده‌اند: در این جنگ، شیوه‌ها و روش‌های مختلفی همچون از «نفوذ و سرقت اطلاعات» و «تغییر محاسبات تصمیم‌گیران» و «تغییر باورهای مردم» تا «ایجاد نابسامانی مالی و اقتصادی» و «ایجاد آشفتگی‌های امنیتی» در دستور کار است.

معظم‌له یکی دیگر از راه‌های مقابله با تهاجم جبهه مقابل را جدی‌گرفتن موضوع نفوذ دانستند و افزودند: فردی که می‌خواهد در نظام جمهوری‌اسلامی، امانت‌دار کشور و مردم باشد باید صلاحیت داشته باشد، لذا کوچک‌ترین تردید درباره صلاحیت افراد باید منعکس شود و دستگاه‌ها نیز موظف به عمل براساس نظر وزارت اطلاعات هستند (بیانات مقام معظم‌رهبری در دیدار با وزارت اطلاعات، تاریخ ۲۹ /۰۱/ ۹۷).

رابطه عزت و جهادکبیر

عزت به‌معنی شکست‌ناپذیری است و جهاد کبیر نیز به مفهوم تسلیم‌ناپذیری اهل ایمان در مقابل دشمنان قرآن و تبعیت‌نکردن از دشمن است. لذا به‌منظور رسیدن به عزت نیز باید به جهاد کبیر پرداخته شود. به‌عبارتی دروازه رسیدن به عزت، جهاد کبیر است. زیرا درصورتی که فردی از دشمن تبعیت نماید، شکست‌پذیرشده و عزتی دیگر باقی نخواهد ماند و این‌گونه می‌توان جمع‌بندی نمود که راه رسیدن به دیوارهٔ آتش انسانی تقویت عزت درونی است، اگر در ابتدای راه با جهاد کبیر آغاز نماییم در جهت ایجاد دیوارهٔ آتش انسانی پیش خواهیم رفت و در غیر این‌صورت، چنین دیواره‌ای تشکیل نشده و راه ذلت ایجاد خواهد شد.

ج: جهاد اکبر

جهاد با نفس است که در حدیث معروف نبوی آمده است: آفرین بر گروهی که جهاد اصغر را انجام دادند که منظور جهاد با دشمن ظاهری است و برعهدهٔ آنها جهاد اکبر؛ یعنی مجاهدت با نفس باقی مانده است.

تفاوت جهاد اصغر با جهاد اکبر

منظور از جهاد اصغر، جنگ ظاهری بین دو گروه است و مقصود از جهاد اکبر مبارزه و مجاهدت با نفس است «**و جاهدوا فی اللّه حق جهاده**» (قرآن مجید، سوره حج: آیه ۷۸) و میان این دو جنگ و جهاد تفاوت‌هایی به شرح ذیل وجود دارد:

۱ - در جهاد اصغر دشمن ظاهر است؛ **قاتلوا الّذین یقاتلونکم** (قرآن مجید، سوره بقره: آیه۱۹۰)، در جهاد اکبر مخفی و پنهان است. امام کاظم(ع) می‌فرماید: «**أخفاهم لک شخصا مع دنّوه منه**».

۲ - در جهاد اصغر مدت کوتاه است، در جهاد اکبر مدت طولانی، بلکه همیشگی است.

۳ - در جهاد اصغر مرگ یکبار است(آن هم احتمالا)، ولی در جهاد اکبر و مبارزه با نفس، در هر کاری انسان با مرگ معنویت خود مواجه می‌شود؛ «**فی حدیث المعراج فی صفهٔ اهل الخیر و الاخرهٔ یموت النّاس مرّهٔ و یموت احدهم فی کلّ یوم سبعین مرّهٔ من مجاهدهٔ انفسهم و مخالفهٔ اهوائهم**» (فیض‌کاشانی: ۱۴۲)

۴ - در جهاد اصغر و جنگ ظاهری، زمان و مکان مشخص است، در جهاد اکبر چون نفس انسان خارج از منطقه جغرافیایی است، هیچ مکان، زمان، سنگر و دژ کارسازی نیست، حتی در شب تاریک و در حال اشک و سجده، نفس، انسان را رها نمی‌کند.

۵ - در جنگ ظاهری و جهاد اصغر، شکست از دشمنان زود پدیدار می‌شود، ولی در جهاد اکبر گاهی انسان هشتاد سال از نفس و هوس خود شکست می‌خورد، ولی توجه ندارد.

۶ - در جهاد اصغر، هجوم دشمن ظاهری زمان، برنامه و بودجه لازم دارد، لیکن در جهاد اکبر وسوسه نفس فوری و مجّانی صورت می‌گیرد.

۷ - در جهاد اصغر از دشمن ظاهری فرار ممکن است، ولی در جهاد اکبر از دشمن باطنی (نفس) فرار ممکن نیست.

۸ - در جهاد اصغر صلح و سازش با دشمن ممکن است، ولی در جهاد اکبر صلح و سازش با دشمن درون ممکن نیست.

۹ - در جهاد اصغر، مریض، لنگ، کور، زن و پیرمرد معاف هستند، ولی در جهاد اکبر هیچ‌کدام معاف نیستند.

۱۰- هر کس در جهاد اکبر بر دشمن نفس پیروز شود، در جهاد اصغر نیز شرکت می‌کند، لیکن هرکس در جهاد اصغر شرکت کرد، معلوم نیست در جهاد اکبر پیروز شود.

۱۱ - حفظ و تداوم جهاد اصغر به‌وسیله جهاد اکبر است (هم قبل، هم بعد و هم در حین جهاد اصغر)، جهاد اکبر لازم است؛ اما حفظ و تداوم جهاد اکبر وابسته به جهاد اصغر نیست.

۱۲ - در جهاد اکبر، درگیری و مبارزه با خود شیطان است، در جهاد اصغر با پیروان شیطان.

۱۳ - در جهاد اکبر مباشرت لازم است، ولی در جهاد اصغر با مال هم می‌توان جبهه را کمک کرد.

۱۴ - پیروزی در جهاد اصغر نیاز به تجهیزات مادی دارد؛ «**و أعدّوا لهم ما استطعتم من قوّة و من رباط الخیل**» (قرآن مجید، سوره انفال: ۱۶۰)، پیروزی در جهاد اکبر نیاز به اشک و ناله در درگاه الهی دارد؛ «**و سلاحه البکاء**» (قمی[الف]: دعای کمیل) و «**و أعنّی بالبکاء علی نفسی**» (قمی[ب]: دعای ابوحمزه ثمالی).

۱۵ - در جهاد اصغر، همهٔ مردم موظف به شرکت نیستند؛ «**و ماکان المؤمنون لینفروا کافّةً**» (قرآن مجید، سوره توبه: آیه ۱۱۲) در جهاد اکبر همهٔ مردم شرکت دارند.

در شرایطی که جهاد کبیر مطرح است ممکن است با جهاد اصغر همزمان باشد و یا ممکن است با جهاد اکبر همراه باشد. یعنی در برخی شرایط ممکن است جنگ و جهاد نباشد ولی جهاد کبیر و جهاد اکبر وجود داشته باشد و در حقیقت کسی که در جبهه جهاد کبیر به دفاع از کیان اسلام و مسلمین می‌پردازد در همان‌حال به‌خاطر دل‌مشغولی به نفس، جهاد در راه خدا، گذشتن از رفاه و آرامش، انتخاب سختی و مجاهده در راه خدا، فرد مجاهد فی سبیل‌الله و درحال تزکیه نفس و خودسازی شناخته شود.

نتیجه اینکه در برخی شرایط جهاد کبیر شامل جهاد اصغر و جهاد اکبر نیز می‌باشد ولی هر رزمنده جهاد اصغر و هر تلاشگر جهاد اکبر، لزوماً مجاهد عرصه جهاد کبیر نیست ولی می‌توان گفت مجاهد عرصه جهاد کبیر می‌تواند با قصد قربت به خدا، مجاهد با دشمن خارجی و مجاهد با نفس (جبهه درون) نیز باشد.

جهاد کبیر و جنگ نامتقارن از دیدگاه رهبر معظم انقلاب

رهبر انقلاب برای جهاد کبیر ابعادی برمی‌شمارند و به بعد اقتصادی (مقاوم‌کردن اقتصاد)، بعد فرهنگی (کارهای فرهنگی خودجوش و تبعیت نکردن از فرهنگ دشمن) و بعد اجتماعی (به صحنه‌آوردن استعدادهای موجود کشور) آن اشاره می‌کنند (بیانات رهبر معظم‌انقلاب در دانشگاه افسری و تربیت پاسداری امام حسین(ع)، تاریخ ۰۳/ ۰۳/ ۱۳۹۵)

دو شاخص "جنگ نامتقارن" و "جهاد کبیر" از مهم‌ترین شاخص‌هایی است که رهبر معظم انقلاب در این بیانات بر آنها تاکید دارند. رهبر معظم انقلاب، معنای جنگ نامتقارن را برخورداری از منابع مختلف با هویت‌های مختلف می‌دانند و ضمن تاکید بر "درحال جنگ نامتقارن‌بودن ایران با استکبار جهانی"، ابزارهای جنگ نامتقارن ایران را "توکّل"، "اعتماد به خدا"، "اعتماد به پیروزی نهایی" و "اعتماد به قدرت انسان" بر می‌شمارند. ایشان همچنین جنگ نامتقارن را "جنگ اراده‌ها" می‌دانند.

رهبر معظم انقلاب همچنین از شاخص "جهاد کبیر" نام می‌برند و آن را "تبعیت‌نکردن از کفار در میدان‌های مختلف سیاست، اقتصاد، فرهنگ، هنر و..." می‌دانند. ایشان ضمن نام‌بردن

جهاد اصغر، تاکید می‌کنند که جهاد کبیر با جهاد اکبر متفاوت است. رهبر انقلاب با اشاره به توصیه مکرر خداوند به پیامبر در سورهٔ احزاب درخصوص تبعیت‌نکردن از کفار، تاکید می‌کنند جهاد کبیر به‌معنای قطع رابطه با دنیا نیست. رهبر انقلاب برای جهاد کبیر ابعادی برمی‌شمارند و به بعد اقتصادی (مقاوم‌کردن اقتصاد)، بعد فرهنگی (کارهای فرهنگی خودجوش و تبعیت‌نکردن از فرهنگ دشمن) و بعد اجتماعی (به صحنه‌آوردن استعدادهای موجود کشور) آن اشاره می‌کنند. به عقیده رهبر معظم انقلاب، هوشمندی و اخلاص لازمه جهاد کبیر و این جهاد نیازمند تبیین است.

جهاد کبیر چه ارتباطی با جهاد اکبر دارد؟

در حقیقت، تهذیب نفس و مبارزه با خواهش‌های نفسانی یعنی جهاد اکبر، زیربنای همه انواع جهاد اصغر و جهاد کبیر است. کسی می‌تواند جهاد کبیر کند که در مبارزه با نفس پیروز شده باشد.

مهم‌ترین تجهیزات و نرم‌افزارهایی که برای پیروزی در جبهه حق کاربرد دارد عبارتند از:

الف) وحدت و همدلی حقیقی بین مؤمنان در همه سطوح و عرصه‌های جامعه متشتت، شایعه‌پذیر و احساسی؛ توان مقابله و شناخت برنامه‌های رنگارنگ دشمن را نخواهد داشت.

ب) ایجاد حس اعتماد، اطمینان، محبت و عاطفه در بین تمام اقشار جامعه به‌عنوان سنگ زیرین سرمایه اجتماعی

سیمای جهادگران واقعی

قرآن کریم پس از بیان معامله سودمند با خداوند و خریدن جان آنان در برابر بهشت، جهادگران واقعی را با نُه صفت می‌ستاید: «**انّ اللّه اشتری من المؤمنین اءنفسهم ... التائبون العابدون الحامدون السائحون الراکعون الساجدون الامرون بالمعروف و الناهون عن المنکر و الحافظون لحدود اللّه و بشّر المؤمنین**» (قرآن مجید، سوره توبه: آیه‌های ۱۱۲ و ۱۱۱).

۱- توبه‌کنندگان

۲- عبادت‌پیشگان

۳- ستایشگران

۴- تلاشگران
۵- رکوع‌کنندگان
۶- ساجدان
۷- آمران به معروف
۸- ناهیان از منکر
۹- حافظان حدود الهی

دو رکن جهاد متقوم

پس، جهاد متقوّم دو رکن است: یکی اینکه در آن جدّ و جُهد باشد؛ دیگر اینکه در مقابل دشمن باشد. اگر کسی علیه دوست جدّ و جُهد کند، این جهاد نیست؛ بلکه فتنه و اخلال است (بیانات مقام معظم‌رهبری در شروع درس خارج فقه، تاریخ ۲۰/ ۰۶/ ۱۳۷۳).

بخش ۵– بارو

کلمهٔ بارو در منابع بسیار کهن به دورهٔ ساسانیان باز می‌گردد. دیوارهای دفاعی و خاکریزهای متعلق به آغاز سکونت انسان در ایران هنوز برجاست. شکل آنها به موازات پیشرفت سلاح‌های تهاجمی و تدافعی تکامل یافته است.

در گذشته نوع استحکامات عموماً تابع مقتضیات ناشی از محل قلعه یا دهکده و اوضاع طبیعی سرزمین بود. در همهٔ دوره‌ها، استحکامات را در دورافتاده‌ترین و مرتفع‌ترین نقطه بنا می‌کردند تا به‌سبب وجود شیب‌های تند تپه یا کوه، دستیابی به آن دشوار باشد و مدافعان نیز در بالا قرار بگیرند و از لحاظ دید مسلّط باشند. طرح‌های ساختمانی بیشتر براساس معلومات و تجربهٔ کلّی نسبت به حمله و دفاع طراحی می‌شد تا سنت‌های محلّی. در هر دوره‌ای، روش‌های آزموده و

مقبول برای ایجاد استحکامات انتخاب می‌شد. همین آمادگی برای پذیرش فنون کار، که در موارد دیگر مؤثر افتاده است، در سراسر تاریخ معماری ایران، تا رسیدن به اقتباس «سبک فرانسوی» در معماری قلاع و حصارهای شهر در اوایل قرن سیزدهم، خصوصاً در خوی و تهران، می‌توان ردیابی کرد .(Kleiss and Kellner, ۱۹۷٦: p ١٦٧)

عامل دیگری که در طراحی استحکامات تأثیر داشته مواد و مصالح محلی است. در نواحی کویری فلات ایران و همچنین دشت خوزستان که مجاور بین‌النهرین بود، بیشتر از خشت یا آجر استفاده می‌شد و حال آنکه در مناطق کوهستانی استفاده از سنگ، دست‌کم برای پی بنا، رواج داشت، هرچند که در دورهٔ پیش از تاریخ و اوایل دوران تاریخی، حتی در این‌گونه مناطق نیز، قسمت‌های بالای حصارهای دفاعی غالباً از خشت خام بوده است. خاکریزها به‌معنای دقیق آن در دوران متأخر و تحت‌تأثیر اروپا در اواخر قرن دوازدهم و اوایل قرن سیزدهم پدید آمد (همان). استفاده از الوار و ترکیب آن با گِل و سنگ، در استحکامات پیش از تاریخ و اوایل دوران تاریخی در اروپا به‌کار می‌رفت.

در طول تاریخ ایران، استحکامات بیشتر برای محافظت از قلعه‌ها ساخته می‌شد، زیرا قلعه هم اقامتگاه شاه و درباریان بود و هم مردم محل می‌توانستند با وسایل و احشام خود در آنجا پناه بگیرند. از آغاز دوران پیش از تاریخ در هزارهٔ اول پیش از میلاد، پیرامون دهکده‌ها نیز حصار کشیده می‌شد. این کار، نخست برای مصون‌ماندن از حملهٔ راهزنان و جانوران وحشی بود، ولی بعدها عمدتاً برای دفاع در مقابل هجوم دشمنان صورت می‌گرفت. در سراسر این سرزمین، بقایای حصارهای محکم دهکده‌ها و قلعه‌های مسکونی را می‌توان یافت که متعلق به هزارهٔ سوم پیش از میلاد است (Kleiss and Kellner, 1976: p 27).

باروها را تا حدّ امکان بر روی ارتفاعات صخره‌ای می‌ساختند تا هم از خطر نقب‌زدن مهاجمان محفوظ باشند و هم حمل ادوات محاصره‌ای به پای دیوار توسط دشمن دشوار باشد. کندن خندق از شیوه‌های دیگری بود که برای مقابله با حملهٔ مهاجمان به باروها به‌کار می‌رفت. به روایتی، سلمان فارسی در سال پنجم هجری، به مسلمانان آموخت که برای دفع هجوم دشمن از سمت غربی مدینه خندقی حفر کنند.

علاوه براین، ایرانیان در چندین ناحیهٔ سوق‌الجیشی، مانند دربند در کرانهٔ غربی دریای خزر، در برابر قبایل بیگانه و همچنین در چالوس و قزوین در مقابل چپاول‌های دیلمیان، باروهای دفاعی بنا کرده بودند (مسعودی، ۱۸۶۱-۱۸۷۷: ۱۹۷-۱۹۶).

در شبه جزیرهٔ عربستان، تنها طائف دارای باروهای دفاعی بود. اعراب بادیه ـ مانند سایر اقوام چادرنشین ـ با حصار دائمی، میانه‌ای نداشتند. ولی با پیشروی به‌سوی مشرق و داخل جهان اسلام خصوصاً ایران، فراگرفتن باروسازی را لازم دیدند.(Spuler, 1952: 499)

بخش ۶– نتیجه‌گیری

همان‌گونه که در بخش‌های قبلی این کتاب به آن اشاره شد، وقتی قصد بررسی تهدید، آسیب‌پذیری و ایجاد امنیت وجود دارد باید بستری که درنظر است این اقدام در آن انجام شود و یا دیوارهٔ آتش در آن ایجاد گردد شناسایی شود تا با شناخت کافی از آن، گستره و بررسی نقاط قوت و ضعف آن، دیوارهٔ آتش متناسب را ایجاد نمود و آسیب‌پذیری‌ها را نیز شناسایی و رفع نمود که از آن ناحیه ضربه‌پذیر نباشیم و تهدید نتواند صدمه‌ای وارد نماید.

پس از اینکه گستره یا زمین بازی مشخص گردید باید به‌دنبال ایجاد دیوارهٔ آتش مناسب بود. دیوارهٔ آتش سازمان‌ها می‌بایست متناسب با حوزه‌های فعالیت (فرایندهای سازمانی) و در دو بعد؛ انسانی و غیرانسانی ایجاد گردد. بُعد غیرانسانی یعنی همان پدافند غیرعامل و حفاظت فیزیکی و بُعد انسانی اقداماتی است که برای ایجاد دیوارهٔ آتش در وجود عوامل انسانی می‌باشد، تا عوامل انسانی در موقعیت‌های مختلف و در مواجهه با مسائل و تهدیدات مختلف بتواند دفاعی متناسب انجام دهد که نه خود و نه اطلاعاتی که به او به امانت سپرده شده به خطر بیفتد. حوزه نرم باتوجه به تاثیرگذاری بیشتر از اهمیت بالاتری برخوردار است. زیرا برابر مستندات بدست‌آمده در تحقیقات صورت‌گرفته حدود ۸۰٪ از مشکلات امنیتی به‌وجود آمده در مجموعه‌ها توسط عوامل انسانی رخ می‌دهد و ۲۰٪ آن به‌دلیل سایر مولفه‌ها است

انتخاب عوامل انسانی مناسب (یعنی بررسی صلاحیت امنیتی) پس از گذشتن از اولین دیوارهٔ آتش، انجام می‌شود، تا با استفاده از این ابزار بتوان از نفوذ دشمن و عوامل انسانی نامناسب جلوگیری نمود. پس از آن تهدیداتی که در کمین این عوامل انسانی قرار می‌گیرد تهدیداتی از جمله ترور، جاسوسی و تهدید خرابکاری در محصولات و ادواتی است که این عوامل انسانی با آنها سر و کار دارند، یا در ابنیه‌ای که فعالیت می‌نمایند و یا تاسیساتی که رفاهی را ایجاد می‌نمایند، است و برای اینکه بتوان امنیت کاملی را ایجاد نمود می‌بایست در مقابل این تهدیدات دیوارهٔ آتش مناسب ایجاد نمود. دیوارهٔ آتش در بعد غیرانسانی پیرامون بخش‌های ابنیه و تاسیسات، رایانه و شبکه، سلاح و مهمات و تجهیزات، اسناد و اطلاعات است و همچنین محل نگهداری رسوب دانش آن مجموعه که باتوجه به طبقه‌بندی آن دیوارهٔ آتش مناسب ایجاد خواهد شد.

باتوجه به نقش بسیار زیاد عوامل انسانی در ایجاد و برقراری امنیت، نیاز است که دیوارهٔ آتش برای عوامل انسانی ایجاد گردد که زیر چتر امنیتی ایجادشده عوامل انسانی بتوانند به فعالیت خود ادامه دهند و گزندی به آنها نرسد. لذا دیوارهٔ آتشی که برای عوامل انسانی باید ایجاد شود، نمی‌تواند همچون بارو، دیواره آتشی از جنس سخت باشد و به نوعی باید باشد که دائم همراه او باشد. زیرا اگر چنین نباشد و یا از جنس سخت باشد، در زمانی که عامل انسانی از آن محل خارج گردیدند، دیگرهیچ حاشیهٔ امنی پیرامون آن وجود نخواهد داشت.

در اثر آموزش در عوامل انسانی می‌توان بصیرت را در عوامل انسانی ایجاد و تقویت نمود تا شکست‌ناپذیر، نفوذناپذیر و مقاوم گردند و در این‌صورت صاحب عزت خواهند شد و وقتی عوامل انسانی به این مرحله ارتقاء یابند دیوارهٔ آتش در وجود آنها ایجاد خواهد گردید. وقتی بتوان چنین قابلیتی را در عوامل انسانی ایجاد نمود، عوامل انسانی متناسب با عزت ایجادشده، از گزند سرویس‌های اطلاعاتی که در کمین او نشسته‌اند، مصون خواهند ماند.

در هرحال یک دیوارهٔ آتش قادر است درجهت بالارفتن سطح امنیتی سازمان اقدامات مفیدی را انجام دهد.

- دیواره آتش می‌تواند اجرای تصمیمات امنیتی را در یک نقطه متمرکز کند.
- دیواره آتش می‌تواند سیاست امنیتی را به اجرا درآورد.
- در دیوارهٔ آتش فعالیت‌ها را ثبت می‌شود.
- دیواره آتش قادر است سطوح مختلفی از امنیت را برای بخش‌های مختلف پیاده‌سازی کند.
- دیواره‌های آتش از مهم‌ترین ابزارهای تدافعی محسوب می‌شوند و باوجود تصور عمومی دارای ویژگی‌ها و امکانات متفاوتی هستند.
- دیوارهٔ آتش، یکی از راه‌های حفاظت مجموعه خودی از مجموعه غیرقابل‌طمینان است.
- دیوارهٔ آتش برای مقابله با خطرات شناخته‌شده طراحی شده است.

- نیاز است که دائم ترفندهای جدید دشمن رصد شده و در پیکره‌بندی، اصلاحات لازم انجام شود و کارکنان نیز نسبت به آن و اهمیت به‌کارگیری آن به‌طور کامل و مطمئن توجیه شوند.

استراتژی امنیتی می‌بایست بر مبنای زیر باشد: (www.iranictnews.ir)

- دادن حداقل امتیاز: فقط مجوزهایی که مورد نیاز هستند می‌بایست اعطاء گردند.
- دفاع عمقی: سیستم‌های دفاعی دیگری (بغیر از دیوارهٔ آتش) نیز می‌بایست مورد استفاده قرار گیرد و در تمامی لایه‌هایی که وجود دارد پیاده‌سازی شود.
- بی‌خطر به‌هنگام بروز خطا: هنگامی که دیوارهٔ آتش دچار اختلال گردد نباید امنیت دچار نقصان شود. لذا در این مورد می‌بایست برنامه‌ریزی دقیقی صورت پذیرد.

باتوجه به مطالب فوق مشخصات دیوارهٔ آتش می‌تواند به شرح زیر باشد:

مولفه‌ها: مولفه‌های این دیوارهٔ آتش عبارتند از کارکنان، اسناد و اطلاعات، رایانه و شبکه، سلاح و مهمات و تجهیزات، ابنیه و تاسیسات. باتوجه به مستندات بدست‌آمده، کارکنان اهمیت و تاثیرگذاری بیشتری در ایجاد امنیت، نسبت به بقیه دارند.

شاخص‌ها: شاخص‌های ما، استانداردها، اصول و دستورالعمل‌هایی است که اگر این شاخص‌ها رعایت نگردد، مورد تهدید قرار خواهیم گرفت.

ویژگی‌ها: ویژگی این دیوارهٔ آتش باید این باشد که غیر از داخل سازمان، در کل گستره‌ای که با سازمان مرتبط است نیز گسترده خواهد شد. (چه در داخل کشور و چه خارج از کشور) دشمن از هیچ طریقی نتواند نزدیک شود و هرگونه اقدامی از سوی دشمن؛ گرفتاری در دام دیوارهٔ آتش باشد ولی محدودیتی برای آنهایی که باید وارد شوند نیز ایجاد ننماید.

ابعاد: این دیوارهٔ آتش در دو بعد انسانی و غیرانسانی است بدین‌گونه که یک بعد دیوارهٔ آتش فیزیکی می‌باشد که از کل مولفه‌ها غیراز عوامل انسانی محافظت نماید و بعد دیگر، دیوارهٔ آنش انسانی[1] است که باید در وجود عوامل انسانی ایجاد شود تا در هر موقعیتی بتواند از عوامل انسانی در برابر تهدیدات دشمن محافظت نماید.

1 - Human firewall

چالش‌ها: چالش‌ها در پیاده‌سازی اصول، مقررات و دستورالعمل‌های سازمان در مراکزی است که با سازمان مرتبط هستند و چون بخشی از اطلاعات سازمان در اختیارشان قرار می‌گیرد درصورتی که الزامات را رعایت ننمایند، باعث بروز آسیب می‌گردند.

گسترش: راه گسترش این دیوارهٔ آتش این است که کلیه مرتبطین بپذیرند که اصول و ضوابط را رعایت نمایند و برای اینکه ظاهری زیبا به آن بدهیم، در قالب یک استاندارد می‌توان ارائه نمود تا قبل از برقراری تعامل این استاندارد پیاده‌سازی شود.

پویایی: برای پویایی و به‌روز بودن این مدل نیز نیاز است که طی یک فرایند، سلسله اقداماتی انجام شود تا دائم کلیه تعاملات رصد گردد و نقاط ضعف و آسیب، شناسایی شده و سریعا نسبت به رفع آن اقدام شود.

لذا این دیوارهٔ آتش باید در تمامی ابعاد، تا پایین‌ترین لایه، برای مقابله با تمامی تهدیدها، در بعد انسانی و غیرانسانی (فیزیکی)، در هر مکان که عوامل انسانی در آن حضور دارد (چه در داخل سازمان و چه خارج از آن و چه در داخل کشور و چه خارج از آن) و در هر لحظه که تهدید در کمین آن است کارآیی داشته باشد.

۲

فصل دوم
ارائه الگو

بخش ۱– پیشینه موضوع

در این بخش پیشینه موضوع کتاب مورد بررسی قرار می‌گیرد. در ادامه این بخش، به تشریح یافته‌ها پرداخته خواهد شد:

پایان‌نامه‌ها و مقالات

در موضوع دیوارۀ آتشی که در رایانه و شبکه به‌کار گرفته می‌شود منابع فارسی زیادی وجود دارد ولی در موضوع دیوارۀ آتش انسانی[1] منابع فارسی یافت نشد. مقالات و پایان‌نامه‌های بدست آمده بیشتر خارجی می‌باشد که به شرح زیر می‌باشد:

الف– پایان‌نامه Jamison W.Scheeres با عنوان:

Establishing the human firewall: reducing an individual’s vulnerabiliy to social engineering attacks [2]

1 - Human fierwall

2- Jamison W.Scheeres; Establishing the human firewall: reducing an individual’s vulnerailiy to social engineering attacks; master thesis in Department of the air force; air university, ohio, 2008.

در این پایان‌نامه به تهدیداتی که از طریق مهندسی اجتماعی ایجاد می‌شود و در کمین کارکنان است پرداخته و راه مقابله با آن را آگاهسازی کارکنان معرفی نموده و در ادامه ذکر شده است که در اثر این اقدام (آگاهسازی)، کارکنان با شناخت کامل می‌توانند در مقابل درخواست‌های ناصحیح حمله‌کنندگان پاسخ منفی بدهند.

نقطه ضعف این پایان‌نامه در عدم ارائه مدل می‌باشد و دیوارهٔ آتش انسانی کامل با این اقدام ایجاد نخواهد شد و نکته اصلی اینکه محتوا و منابعی که در آگاهسازی باید استفاده شود را نیز معرفی نکرده است.

ب– پایان‌نامه Evans, Nathaniel Joseph با عنوان:

Establishing the human firewall: reducing an individual’s vulnerabiliy to social engineering attacks [1]

در این پایان‌نامه به تهدیداتی که ازطریق مهندسی اجتماعی ایجاد و در کمین کارکنان است پرداخته و راه مقابله با آن را آگاهسازی کارکنان معرفی نموده و در ادامه ذکر شده است که در اثر این اقدام (آگاهسازی)، کارکنان با شناخت کامل می‌توانند در مقابل درخواست‌های ناصحیح حمله‌کنندگان پاسخ منفی بدهند.

نقطه ضعف این پایان‌نامه در عدم ارائه مدل می‌باشد و دیوارهٔ آتش انسانی کامل با این اقدام ایجاد نخواهد شد و نکته اصلی اینکه محتوا و منابعی که در آگاهسازی باید استفاده شود را نیز معرفی ننموده است.

ب– پایان‌نامه Evans, Nathaniel Joseph با عنوان:

Information technology social engineering: an academic definition and study of social engineering -analyzing the human firewall[2]

1- Jamison W.Scheeres; Establishing the human firewall: reducing an individual’s vulnerailiy to social engineering attacks; master thesis in Department of the air force; air university, ohio, 2008.

2-*Evans, Nathaniel Joseph, "Information technology social engineering: an academic definition and study of social engineering -analyzing the human firewall". Graduate Theses and Dissertations. (2009)*

در این پایان‌نامه به خطر مهندسی اجتماعی پرداخته و یک مدل برای نحوه انجام مهندسی اجتماعی ارائه نموده و تهدید اصلی دیوارۀ آتش انسانی را مهندسی اجتماعی معرفی کرده است و راه مقابله با این تهدید را رعایت سه عامل محرمانگی[۱]، تغییرناپذیری[۲] و دسترس‌پذیری[۳] توسط کارکنان، معرفی نموده است.

در پایان‌نامه‌های بررسی‌شده تنها به پایان‌نامه‌های مرتبط با کارکنان پرداخته شده است.

ج – مقاله Charles jenninge با عنوان:

Building human firewalls[4]

در این مقاله به حفره‌هایی که در لایه‌های دفاعی وجود دارد و دشمن از آن طریق سعی در ضربه واردنمودن می‌کند، پرداخته است. در این مقاله ذکرشده که اطلاعات ما توسط تهدیدکنندگان زیرنظر است و ازطریق حفره‌هایی که بین حد قابل‌قبول و حد واقعی در سیستم‌ها وجود دارد، در ایجاد آسیب تلاش می‌نمایند، حمله‌کنندگان امنیت را تهدید می‌کنند و این تهدید پس از مورد شناسایی قرارگرفتن حفره‌ها در لایه دفاعی، امنیت را تهدید می‌نماید. برای اینکه این حفره‌ها را به حداقل رسانید و همچنین تهدیدها را بی‌اثرتر نمود، می‌بایست کارکنان نسبت به این امور آگاه‌تر شده و سیاست‌های امنیتی قوی‌تر، مقبول‌تر و پیشرفته‌تری را به‌کار برد تا بتوان نیروی کار مناسب را تربیت نمود.

نقطه قوت این مقاله تاکید بر آگاه‌سازی و به‌کارگیری سیاست‌های امنیتی است و نقطه ضعف این مقاله این است که هیچ مدلی را ارائه ننموده است و دوم اینکه تنها با آگاه‌نمودن کارکنان، دیوارۀ آتش ایجاد نخواهد شد (هرچند تاثیر زیادی دارد) و سایر موضوعات تاثیرگذار را نیز باید از گزند تهدید خرابکاری و جاسوسی دشمن دور نگاه داشت.

د– مقاله Andrew Breakwell با عنوان:

The human firewall creating a security[5]

---

1 - confidential
2 - integrity
3 - availability
4 - *Charles jenninge, Building human firewalls, ceo,swan island, network,inc. , 2013*
5 - *Andrew Breakwell, The human firewall creating a security, Sai global, 2007*

نویسنده در این مقاله برای استقرار دیوارهٔ آتش انسانی ۵ مرحله را معرفی نموده و معتقد است با اجرای این مراحل می‌توان امنیت را برقرار نمود. مراحل اشاره شده عبارتند از: احساس نیازنمودن، وجود تهدید عمومی، برنامه‌ریزی، متعهدشدن و ارزیابی.

نقطه قوت این مقاله متعهدشدن است و نقطه ضعف آن معرفی‌ننمودن چگونه متعهدشدن، می‌باشد.

هـ – مقاله Strphen ndonga kariuki با عنوان:

The human firewall creating a security aware workforce [1]

در ابتدای این مقاله ذکر شده است که حفاظت از اطلاعات، نیازمند انجام التزام در کارکنان یا مرتبطین است. در ادامه اشاره شده است که کارکنان مسئول ۸۰٪ از رخنه‌های امنیتی در سیستم می‌باشند، لذا همیشه کارکنان توسط تهدیدکنندگان مورد هدف قرار می‌گیرند. در مدل مفهومی که بدین‌منظور ارائه نموده است، برای هر لایه، حفاظت‌کننده (دیوارهٔ آتش) قرارداده است. برای کارکنان نیز معتقد است که باید دیوارهٔ آتش ایجاد شود و عنوان می‌کند که یک دیوارهٔ آتش انسانی، اطلاعات او را حفظ می‌کند و از دسترسی غیرمجاز و استفاده غیرمجاز از آن اطلاعات جلوگیری می‌نماید.

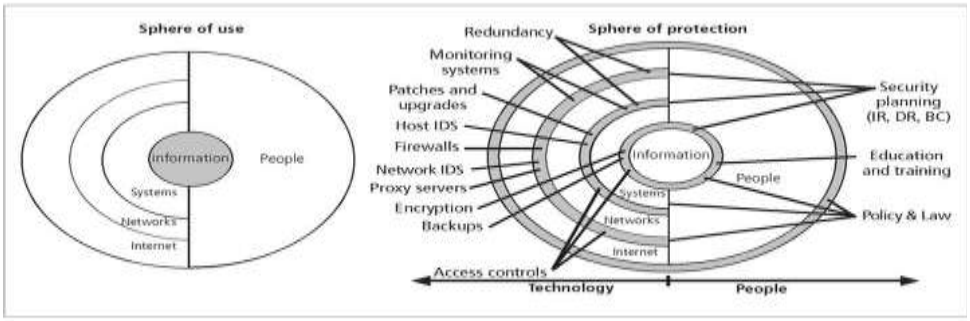


FIGURE 6-16 Spheres of Security

1- *Strphen ndonga kariuki, The human firewall creating a security aware workforce, harmony solutions limited,2011.*

برای اینکه در کارکنان التزام عملی ایجاد نمود که همچون دیوارۀ آتش عمل نمایند می‌بایست تعهد آنها را نسبت به اصول، دستورالعمل‌ها و قوانین محل کار بالاتر برد و این کار را می‌توان با آگاهسازی امنیتی انجام داد. آگاهسازی امنیتی شامل اطلاعاتی درباره چگونه حفاظت‌کردن، کشف کردن، واکنش نشان‌دادن است تا دانش و مهارت امنیت فرد را ارتقاء دهد تا بر رفتار او تاثیر گذاشته و بهبود ببخشد و بداند که چه چیزی را و چگونه باید حفظ نماید.

در ادامه مقاله به تعریف دیوارۀ آتش و دیوارۀ آتش انسانی پرداخته و در نهایت فرمولی برای دیوارۀ آتش ارائه نموده است.

تعریف دیواره آتش: طراحی سیستمی است برای پیشگیری از دسترسی غیرمجاز داخلی و خارجی در یک سیستم محافظت‌شده.

تعریف دیواره آتش انسانی:[1] استفاده از روش‌های گوناگون توسط کارکنان برای مقابله با تهدیدهای خارجی و پیشگیری از بروز آسیب را دیوارۀ آتش انسانی می‌گویند.

این مقاله نسبت به باقی منابع بدست‌آمده کامل‌تر بوده ولی نقطه ضعف آن در مدل مفهومی آن می‌باشد که سلاح، مهمات و تجهیزات را در این مدل مفهومی مشخص ننموده است.

در بررسی مقالات و پایان‌نامه‌ها، موضوعی که به‌طور مشترک در تمامی آنها تاکید گردیده است آگاهسازی امنیتی کارکنان می‌باشد.

جدول جمع بندی یافته‌ها در پایان‌نامه‌ها و مقالات

	سیاست امنیتی	آگاهسازی امنیتی	متعهد نمودن	اقدام تدافعی	مدل دیواره آتش
پایان نامه Jamison W.Scheeres		❋			
پایان نامه Evans, Nathaniel Joseph	❋				
مقاله Charles jenninge	❋	❋			
مقاله Andrew Breakwell			❋		
مقاله Strphen ndonga kariuki	❋	❋	❋	❋	**ناقص**

همان‌گونه که اشاره شد مقالۀ Strphen ndonga kariuki نسبت به باقی منابع کامل‌تر بود ولی مدلی را که ارائه نموده ناقص است. در این تحقیق تلاش‌شده در مدلی که ارائه

1 - Human firewall

می‌گردد، با مبنا قراردادن این مدل و رفع نقایص آن مدلی کاربردی برای ایجاد دیوارهٔ آتش در سازمان ارئه گردد.

تدابیر و بیانات فرماندهی معظم کل‌قوا درخصوص دشمن

	اتحاد	دانستن ایمان و اعتقاد	عزت	پافشاری بر اصول	دانستن بصیرت	–تلاش‌بودن –هوشیاری –شناسایی حرکات او	هشداردادن	پیشرفت	از بین‌بردن خاکریز نرم	مقابله با حیله‌گری دشمن • حمله به دشمن و مقابله هوشیارانه و با برنامه‌ریزی	ثبت تحرکات دشمن
دیدار پاسداران در روز پاسدار) ۱۳۷۵/۹/۲۴								*	*	*	
دیدار جهادگران ۱۳۷۷/۷/۱۵							*			*	
دیدار پاسداران، جانبازان، دانشجویان ۱۳۷۹/۸/۱۱	*	*	*						*	*	
دانشگاه افسری ۱۳۸۵/۶/۲۹										*	
مراسم سالگرد ارتحال بنیانگذار انقلاب(ره) ۱۳۸۶/۳/۱۴			*			*		*		*	
دیدار مجلس خبرگان ۱۳۸۸/۷/۴					*	*		*			
دیدار کارگزاران نظام ۱۳۸۹/۵/۲۷	*									*	
در اجتماع مردم گیلان شرب ۱۳۹۰/۷/۲۳										*	
بیانات ۱۳۹۰/۱۱/۱۴				*		*					
در اجتماع دانش‌آموزان ۱۳۹۱/۸/۱۰	*					*				*	
دیدار مردم آذربایجان ۱۳۹۱/۱۱/۲۸	*										
در حرم مطهر رضوی ۱۳۹۲/۱/۱						*				*	
دیدار فرماندهان و پرسنل نیروی هوایی ارتش ۱۳۹۲/۱۱/۱۹						*		*		*	*
دیدار جمعی از مداحان ۱۳۹۳/۱/۳۱						*				*	
	سیاست امنیتی						آگاه‌سازی امنیتی	اقدام تدافعی			
	اقدام در حوزه خود						اقدام تدافعی				

مقام معظم رهبری در ۱۴ سخنرانی فوق درخصوص دشمن، بیاناتی را ارائه فرموده‌اند که با تجزیه متن بیانات، ۱۱ کلیدواژه از آن استخراج شده که به دو بخش تقسیم شده‌است. بخش اول اقدماتی است که نیروهای‌مسلح و مردم شریف ایران در مقابل دشمن باید عمل نمایند تا تقویت‌شده و دشمن نتواند در بین آنها نفوذ نموده و اهداف خود را به‌ثمر برساند.

در بخش دوم اقدامات تدافعی است که مشخص می‌فرمایند در مقابل دشمن چگونه باید به‌صورت تدافعی اقدام نمود.

در بخش اقدام در حوزه خود شش عنوان از مطالب مربوط به سیاست امنیتی و یک عنوان مربوط به آگاهسازی امنیتی و یک عنوان مربوط به اقدام تدافعی است و وزن بیانات به‌ترتیب بیشترین تا کمترین به کلید واژه‌های زیر اختصاص داشت:

اول: غافل‌نبودن از دشمن و شناسایی حرکات او با هوشیاری

دوم : اتحاد و پیشرفت

سوم: عزت

چهارم: هشداردادن، داشتن ایمان و اعتقاد، داشتن بصیرت و پافشاری بر اصول

در بخش اقدام تدافعی، وزن بیانات به‌ترتیب بیشترین تا کمترین به کلید واژه‌های زیر اختصاص داشت:

اول: مقابله با حیله‌گری دشمن، حمله به دشمن و مقابلهٔ هوشیارانه و با برنامه‌ریزی

دوم: از بین‌بردن خاکریز نرم

سوم: ثبت تحرکات دشمن

- در بازدید از نمایشگاه تحقیقاتی جهادی ن.م در تیرماه ۱۳۹۰

برخی از کارها دارای طبقه‌بندی بالاست، این را باید رعایت کنید. در همه بخش‌ها طبقه‌بندی را بدون ملاحظه رعایت کنید، نگذارید که دشمن از بی‌مبالاتی ما در مورد حفاظت از کارهای طبقه‌بندی‌شده و اسناد طبقه‌بندی‌شده، سوءاستفاده کند؛ یعنی بی‌اعتنایی و بی‌مبالاتی به‌کار حفاظت و رعایت‌نکردن طبقه‌بندی‌ها هیچ‌هنری نیست، این بی‌هنری است که آدم خودش را رها کند تا دشمن بتواند سوءاستفاده کند؛ به این هم توجه کنید.

- در شرفیابی مسئولین (تاریخ ۱۳۹۰/۱۰/۱۸) فرموده:

(تلاش کنید که یک دیوارهٔ آتش درست کنید که کسی نتواند نزدیک شود. البته سخت است چون در بخش‌های مختلف همهٔ نیروها فنی و علمی هستند و کارهای مهم و حساس هم دستشان است. مشکل است اما با تدبیر و با ظرافت می‌شود خیلی کارها را انجام داد. به‌طور جدی این مسئله را دنبال کنید.)

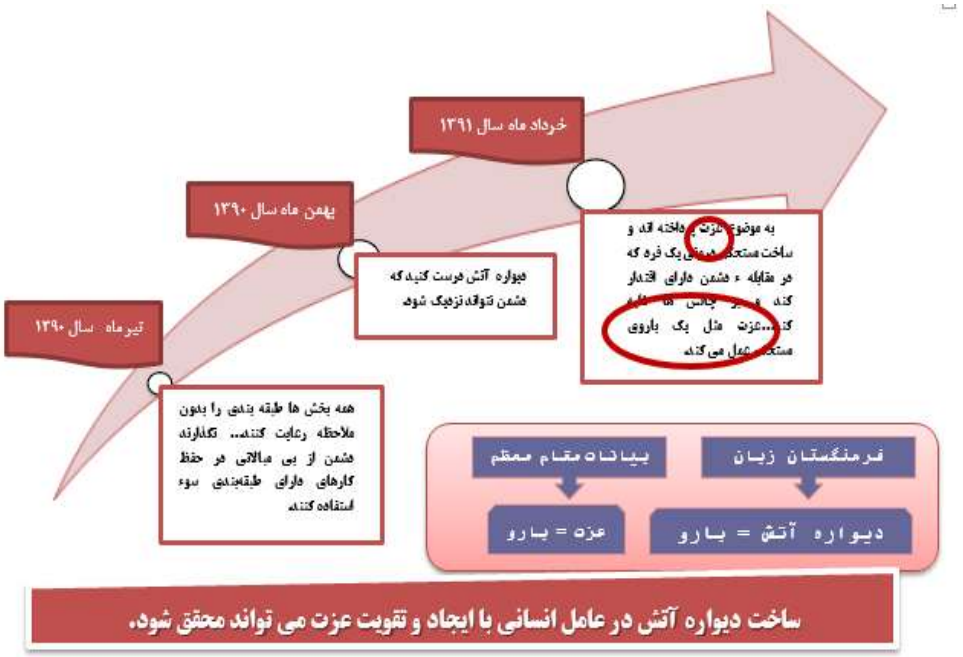
- در تاریخ ۱۳۹۱/۰۳/۱۴ در مراسم گرامیداشت بیست‌وسومین سالگرد رحلت حضرت امام خمینی(ره):

(...عزت یعنی چه؟ عزت به‌معنای ساخت مستحکم درونی یک فرد یا یک جامعه است که او را در مقابلهٔ با دشمن، در مقابلهٔ با موانع، دارای اقتدار می‌کند و بر چالش‌ها غلبه می‌بخشد... وقتی که عزت شامل حال یک انسان، یک فرد و یا یک جامعه می‌شود، مثل یک حصار عمل می‌کند، مثل یک باروی مستحکم عمل می‌کند؛ نفوذ در او، محاصرهٔ او، نابودکردن او برای دشمنان دشوار می‌شود؛ انسان را از نفوذ و غلبهٔ دشمن محفوظ نگه می‌دارد. آن‌وقت هرچه این عزت را در لایه‌های عمیق‌تر فرد و جامعه مشاهده کنیم، تأثیرات این نفوذناپذیری بیشتر می‌شود، کار به‌جائی می‌رسد که همچنان که انسان از نفوذ و غلبهٔ دشمن سیاسی و اقتصادی محفوظ می‌ماند، از غلبه و نفوذ دشمن بزرگ و اصلی، یعنی شیطان هم محفوظ باقی می‌ماند...).

در بیانات خود به مفهوم عزت پرداخته‌اند و راه را برای ایجاد یک دیوارهٔ آتش، مشخص‌تر نموده است در مفهوم عزت مقام معظم‌رهبری عزت را به بارو تشبیه نموده‌اند. فرهنگستان زبان فارسی نیز کلمه بارو را اعلام نموده است که می‌توان بجای دیوارهٔ آتش به‌کار برد.[1] لذا باتوجه به بیانات مقام معظم‌رهبری و همچنین یافته‌های ذکرشده در پیشینه، دیوارهٔ آتش در تمامی حوزه‌های تاثیرگذار باید مستقر شود تا بتواند با اقتدار عمل نماید. قبل از اینکه حوزه‌های تاثیرگذار، بازیگران و یا درگاه‌هایی که دشمن می‌تواند ازطریق آنها وارد شود، نیاز است در آن درگاه‌ها دیوارهٔ آتش متناسب را به‌کار برد، و بستری که درنظر است تمامی این بازگیران، درگاه‌ها و حوزه‌ها در آن مستقر شوند را در یک مدل مفهومی ارائه نمود.

---

۱ - دانشنامه آزاد ویکی پدیا



بخش ۲– سرمایه‌های اطلاعاتی و مبادی افشاء اطلاعات

سرمایه‌های اطلاعاتی موجود در سازمان

مهم‌ترین و با ارزش‌ترین سرمایه‌های سازمان را می‌توان چنین برشمرد:

- پروژه‌های دارای طبقه‌بندی
- محققین و نخبگان دفاعی
- دانش و فناوری
- اسناد و اطلاعات دارای طبقه‌بندی (سری و بالاتر)
- صادرات و واردات کالاهای نظامی و تحریمی

مبادی اصلی افشاء اطلاعات در سازمان

الف) ورود شبکهٔ همکاران صنایع‌دفاعی به ستاد و سازمان‌های تابعه در راستای رویکرد هسته و شبکه

از محورهای اصلی برنامه‌های سازمان‌ها عدم انحصارطلبی در امر تحقیق و نوآوری؛ استفاده از ظرفیت‌های تحقیقاتی موجود در کشور، استفاده از ظرفیت صنعت کشور و پرهیز از ایجاد واحدهایی که تولیدات آن توسط بخش غیردولتی (عدم تصدی‌گری) قابل انجام است می‌باشد. سازمان‌ها نیز در راستای این خط‌مشی‌ها، سیاست‌ها و تدابیر ابلاغی رویکرد هسته دانا و شبکه توانا را در دستور کار و اولویت قرارداده است.

اما رویکرد هسته و شبکه چنانچه با نواقص حفاظتی چون؛ عدم تقلیل طبقه‌بندی، خردنکردن پروژه‌ها و فعالیت‌های قابل‌واگذاری، فقدان پیوست حفاظتی برای پروژه‌ها و فعالیت‌های واگذارشده به پیمانکاران، عدم نظارت کافی حفاظتی و امنیتی بر فعالیت‌ها و پروژه‌های برون‌سپاری، عدم طبقه‌بندی مناسب فعالیت‌ها و پروژه‌های قابل‌واگذاری به پیمانکاران، عدم اهتمام مسئولین و مدیران برای تأمین امنیت پروژه‌های واگذارشده به پیمانکاران، عدم امکان الزام پیمانکاران به اجرای کامل قرارداد در زمان بحران، تردد افراد فاقد صلاحیت به اماکن دارای‌طبقه‌بندی سازمان و عدم کنترل‌های حفاظتی و امنیتی لازم، واگذاری اطلاعات دارای‌طبقه‌بندی از سوی پیمانکار به افراد غیر بدون مجوز کارفرما و عدم رعایت گفتار توسط افراد پیمانکار همراه باشد موجب کاهش ضریب امنیتی و حفاظتی، از دست‌دادن استقلال و حقوق مالکیت معنوی خواهد گردید.

لذا ضرورت دارد در راستای تقویت بنیهٔ دفاعی، با ایجاد سازوکارهای لازم جهت حفظ اسرار نظامی و جلوگیری از دسترسی‌های غیرمجاز و عدم افشاء اطلاعات دارای طبقه‌بندی، الزامات و ملاحظات حفاظتی و امنیتی ازقبیل: نظارت‌های مستمر از محل اجرای پروژه‌های نیروهای‌مسلح در بخش خصوصی، استعلام صلاحیت شرکت‌های پیمانکار مطابق سطح طبقه‌بندی اطلاعات واگذارشده به آنان، ارزیابی حفاظتی شرکت‌ها مطابق شاخص‌های تهیه‌شده و سطح‌بندی حفاظتی برای واگذاری سطح طبقه‌بندی اطلاعات، اخذ تعهدهای لازم از شرکت‌های پیمانکار، درج تعهدات در قراردادها و گرفتن وثیقه مناسب جهت اجرای تعهدات،

در فرآیند برون‌سپاری مدنظر قرارگرفته و شرکت‌های همکار صنایع دفاعی ملزم به رعایت گردند.

ب) همکاری سازمان‌ها با محققین، دانشجویان، مراکز علمی و دانشگاهی و واگذاری پروژه‌های دارای طبقه‌بندی

سازمان‌های تابعه براساس تدبیر فرماندهی معظم‌کل‌قوا مبنی بر استفاده از مراکز تحقیقاتی دانشگاهای کشور، اقدام به برقراری ارتباط و همکاری‌گسترده با معاونین پژوهشی، هیئت‌های علمی و دانشجویان دانشگاه‌های کشور در جوانب مختلف نموده‌اند. همکاری‌های اشاره‌شده عبارتند از: طرح پژوهانه (تعریف و واگذاری پروژه‌های رساله دکتری به دانشجویان کشور در قالب پژوهانه)، هیئت‌های مشترک همکاری فنی ـ تحقیقاتی با دانشگاه‌ها، تعریف پروژه‌های تحقیقاتی برای دانشگاه‌ها، استفاده بخش دفاع از ظرفیت دانشجویان بورسیه خارج از کشور، استفاده بخش ملی از ظرفیت آزمایشگاه‌های سازمان‌های دفاعی، محورهای نوظهور، بدیع و پارک‌های علم و فناوری.

فرایند فوق با مشکلاتی چون: درج عناوین پروژه‌های دارای طبقه‌بندی اعلامی ازسوی سازمان در سایت دانشگاه‌ها، آشکارشدن ضعف‌ها و نیازمندی‌های دفاعی برای سرویس‌های اطلاعاتی، تردد استادان و دانشجویان به اماکن دارای طبقه‌بندی سازمانی برای استفاده از آزمایشگاه‌ها و اطلاع از فعالیت‌های درحال انجام، واگذاری تولید یک سامانه به یک دانشگاه خاص بجای ارجاع اجزای فناوری و ماژول‌ها (خردننمودن پروژه)، انجام مکاتبات توسط سازمان‌های تابعه با سربرگ سازمانی با دانشگاه‌های طرف قرارداد و افشای ماهیت همکاری و نیازمندی‌های فناورانه هر صنعت.

برای اطمینان از ارتباط امن با محققین و مراکز علمی لازم است مواردی چون: خودداری از ارسال موضوعات دارای طبقه‌بندی و اطلاعات غیرضروری به دانشگاه‌ها در قالب طرح پژوهانه، جلوگیری از واگذاری کامل یک سامانه به یک دانشگاه خاص و خُردنمودن پروژه‌ها تا پایین‌ترین اجزا و واگذاری به دانشگاه‌های مختلف، اخذ صلاحیت امنیتی استادان دانشگاه و نخبگان علمی برای همکاری‌های علمی و فناورانه، جلوگیری از تردد اعضای هیئت علمی و دانشجویان در واگذاری آزمایشگاه‌های صنایع به ایشان در اماکن دارای طبقه‌بندی و غیرمرتبط، تاکید بر

رعایت محرمانگی اطلاعات در قراردادهای همکاری و ضرورت عدم درج سوابق اقدامات مشترک با بخش دفاعی در رزومه‌ها، مقالات علمی و عدم طرح موضوعات در زمان تدریس، سخنرانی در همایش‌های داخلی و خارجی، خودداری از مکاتبه با سربرگ‌های سازمان‌ها که بیانگر نیازمندی‌های سازمان مزبور می‌باشد در اعلام نیازمندی‌های فناورانه با دانشگاه‌ها، تاکید بر اجتناب معاونین پژوهشی دانشگاه‌ها از قراردادن عناوین نیازمندی‌های فناورانه بخش دفاع در دسترس عموم و درج در مجلات و سایت‌ها.

ج) ارائه رزومه و مقالات به مراجع بین‌المللی توسط محققین سازمان‌ها برای کسب فرصت‌های مطالعاتی و شرکت در سمپوزیوم‌های بین‌المللی

دانشجویان، محققین، استادان و نخبگان برای ارتقای رتبهٔ علمی خود باید مقالاتی را به همایش‌ها، جشنواره‌ها، مجلات و نشریات داخلی و خارجی ارائه نمایند و یا برای انجام فعالیت‌هایی خارج از سازمان نسبت به ارائه رزومه خود اقدام نمایند که این اقدامات منجر به بروز مخاطرات متعدد حفاظتی و امنیتی از حیث افشای اطلاعات مربوط به تحقیق، فعالیت‌ها، افراد مرتبط با موضوعات علمی، اطلاعات مراکز تحقیقاتی و پژوهشی سازمان خواهد شد و در خوش‌بینانه‌ترین حالت اینکه اطلاعات طبقه‌بندی‌شده حفاظتی در مقالات و رزومه‌ها نباشد، در افشای اسامی و مشخصات افراد تردیدی وجود نخواهد داشت و احتمال نشان‌گذاری کارکنان سازمان برای تقرب، جذب، تطمیع و حذف ازسوی سرویس‌های بیگانه وجود دارد و ضروریست به‌منظور رعایت و اعمال تمهیدات حفاظتی اقداماتی اعم از ایجاد مرکزی در سازمان به‌منظور ارزیابی علمی مقالات برتر و صدور تأییدیه مورد پذیرش وزارت علوم، تعامل با وزارت علوم برای پیش‌بینی سازوکار لازم برای ممیزی و ارزیابی مقالات علمی نیروهای‌مسلح در مراکز علمی اختصاصی ن.م، انجام هماهنگی لازم با وزارت‌علوم مبنی بر اختصاص شرایط ویژه به دانشجویان و اعضای هیئت علمی سازمان برای حذف لزوم درج مقالات در نشریات داخلی و بین‌المللی و اصلاح مقررات موجود در مورد ارتقای سطح علمی اعضای هیئت علمی سازمان، بررسی و تحقیق در مورد چگونگی تأمین حقوق و حفظ منزلت و ارتقای سطح علمی نخبگان، محققین و اعضای هیئت علمی مرتبط با سازمان صورت پذیرد.

د) تجمیع اطلاعات مربوط به سازمان‌ها در مراجع بیرونی

از آنجاکه سازمان‌ها جهت ارائه تسهیلات و خدمات به کارکنان از مراکز خدماتی اعم از بانک‌ها، بیمه‌ها، آموزشگاه‌ها و... استفاده می‌نماید و در تعامل با آنها ملزم به ارائه اطلاعاتی می‌گردند. باتوجه به عدم نظارت و کنترل حفاظتی بر اطلاعات واگذارشده به دستگاه‌های دولتی، دسترسی افراد فاقد صلاحیت به اطلاعات ارائه‌شده به مراجع دولتی و غیردولتی، سرقت و مفقودشدن اطلاعات دارای طبقه‌بندی سازمان که به مراجع مذکور ارائه گردیده، انتشار اطلاعات دارای‌طبقه‌بندی سازمان توسط مراجع دریافت‌کننده اطلاعات فارغ از ملاحظات حفاظتی و امنیتی، اتصال رایانه‌های مراجع دولتی به شبکهٔ جهانی اینترنت، تبعاتی را برای کارکنان سازمان در آینده در پی خواهد داشت.

بنابراین برای حفاظت بهتر و بیشتر اسناد و اطلاعات طبقه‌بندی‌شده باید اسناد و اطلاعات بین سازمان‌های کمتری توزیع شود و تنها سازمان‌هایی مطلع گردند که برای انجام وظایف محول‌شده نیاز به آگاهی از مفاد آنها داشته و قابلیت اطمینان آنها تحقیق و تأیید شده باشد و از افراد حائز صلاحیت امنیتی در تکمیل و بهره‌برداری از بانک‌های اطلاعاتی مربوط به نیروهای‌مسلح و دارای دسترسی مطابق باسطح طبقه‌بندی اطلاعات نیروهای‌مسلح استفاده گردد.

ه) تمایل سازمان‌ها به استقرار سیستم‌های مدیریتی با استفاده از نمایندگان شرکت‌های خارجی

گرایش سازمان‌ها و صنایع تابعه به اخذ استانداردهای بین‌المللی مدیریت و کیفیت از نمایندگی شرکت‌های خارجی (CB)، مستلزم ارائه اطلاعات دارای طبقه‌بندی مجموعه بوده و شرکت‌های خارجی و سرویس‌های اطلاعاتی بیگانگان به‌راحتی و بدون پرداخت هزینه موفق به جمع‌آوری و کسب جدیدترین اطلاعات مربوط به محصولات و بعضاً پروژه‌های دارای طبقه‌بندی می‌گردند. همچنین سازمان‌ها برای تهیه اظهارنامه و مشاوره، آموزش، ممیزی و استقرار سیستم‌های مدیریتی از مشاوران بیرونی و ممیزان شرکت‌های خصوصی استفاده و یادشدگان از تمامی فرآیندها و جدیدترین فعالیت‌های هر سازمان مطلع می‌گردند.

برای جلوگیری از این اتفاق لازم است مواردی چون؛ کنترل و نظارت مستمر بر عملکرد سازمان‌ها در استقرار سیستم‌های مدیریتی، نظارت مناسب بر عملکرد مرکز استاندارد دفاعی ایران و ارتباط مرکز با پیمانکاران و بخش‌های خصوصی، توجیه حفاظتی ممیزان سازمان به‌منظور رعایت حیطه‌بندی و حفاظت گفتار در همکاری با شرکت‌ها، تمرکز مشاوره، آموزش، اخذ گواهینامه‌های بین‌المللی و استقرار سیستم‌های مدیریتی ازطریق مرکز استاندارد دفاعی سازمان، ساماندهی ممیزان سازمان و برگزاری کلاس‌های آموزشی و آگاه‌سازی حفاظتی برای حفظ اطلاعات دارای طبقه‌بندی مجموعه‌ها و عدم طرح مسایل مربوط به سازمان در شرکت‌های دیگر مدنظر قرار گیرد.

و) شرکت سازمان‌های تابعه در جشنواره‌ها، نمایشگاه‌ها و همایش‌های بین المللی

همه ساله واحدهای تابعه جهت انجام تبلیغ، کسب مقام در جشنواره‌ها، نمایشگاه‌ها، همایش‌های مختلفی شرکت می‌کنند و ارائه اطلاعات و توانمندی‌ها (لزوم این کار)، موجب افشای اطلاعات و مقالات دارای طبقه‌بندی از طریق اینترنت، انتشار چهره و مشخصات فردی برگزیدگان نیروهای‌مسلـــح، تحریم، تطمیع، تهدید و حذف فیزیکی احتمالی نخبگان سازمان توسط بیگانگان، دسترسی شرکت‌کنندگان و برگزارکنندگان به اطلاعات دارای طبقه‌بندی فراتر از میزان دسترسی آنها، سرقت و یا مفقودشدن اسناد و مدارک دارای طبقه‌بندی در فرایند برگزاری می‌گردد. بنابراین ضروریست از ارائه هرگونه اطلاعات دارای طبقه‌بندی به جشنواره‌ها و همایش‌های خارج از نیروهای‌مسلح خودداری و صرفاً پروژه‌های فاقد طبقه‌بندی و ضرورتاً طبقه‌بندی پایین و با رعایت مقررات حفاظتی و امنیتی و دستورالعمل‌های موجود شرکت داده شود و پروژه‌های دارای طبقه‌بندی در جشنواره‌ها و همایش‌های داخلی نیروهای‌مسلح مطرح شود و در آینده ترتیبی اتخاذ تا جشنواره‌ها و همایش‌های دارای امکانات و مؤلفه‌های برابر با جشنواره‌ها و برگزاری همایش‌های ملی در سطح نیروهای‌مسلح به‌منظور ایجاد فضایی برای جبران کاستی‌ها و محدودیت‌های مطرح‌شدن نخبگان دفاعی در رسانه‌ها برگزار گردد و درصورتی که این‌گونه فعالیت‌ها با رعایت ملاحظات حفاظتی همراه نباشد می‌تواند محل و مکان‌های خوبی برای جمع‌آوری اطلاعات توسط سرویس‌های اطلاعاتی حریف باشد.

ز) مصاحبه‌ها

یکی از شگردهای ساده و بدون هزینه سرویس‌های اطلاعاتی بیگانه از کشورهای موردنظر، جمع‌آوری آشکار اطلاعات می‌باشد که روزانه در رسانه‌ها، روزنامه‌ها و سایت‌های اینترنتی منتشر می‌گردد. یکی از مبادی انتشار اطلاعات انجام جاسوسی تلفنی کارکنان (شنود مکالمات و تخلیه اطلاعاتی)، عدم رعایت گفتار از سوی کارکنان در مکالمات تلفنی، جلسات با بیگانگان، عدم کنترل و نظارت کافی حفاظت اطلاعات‌ها بر مصاحبه‌ها، سخنرانی‌ها و شرکت در کنفرانس‌های خبری مسئولین و مدیران واحدهای تابعه سازمان می‌باشد. بنابراین ضروریست هرگونه مصاحبه نظامی با هماهنگی سیستم امنیتی بوده و نمایندهٔ آن در جلسات و ملاقات با بیگانگان حضور داشته و قبل از تشکیل جلسات مسئولین را توجیه نمایند و کلیه کارکنان نسبت به عدم ارائه اطلاعات دارای طبقه‌بندی توجیه شده تا انجام مصاحبه، گفتگوهای خبری و سازمان با رعایت ملاحظات حفاظتی صورت پذیرد.

ح) دفاتر ویژه (محل‌های نگهداری اسناد سری و بالاتر)

بهترین نوع نگهداری و کنترل اسناد سری و بالاتر تشکیل بایگانی ویژه (مرکزی) خواهد بود. بدین‌طریق که کلیه اسناد سری و بالاتر یک سازمان یا صنعت به‌صورت متمرکز نگهداری شده و متصدی کنترل اسناد، عهده‌دار نگهداری و حسابداری اسناد آن سازمان یا صنعت خواهد بود و کلیه اقدامات از قبیل بررسی، اقدام، تایپ، بسته‌بندی و لاک‌ومهر اسناد مذکور باید در داخل بایگانی ویژه صورت پذیرد. مطابق آیین‌نامه حفاظت اسناد و مدارک طبقه‌بندی‌شده نیروهای‌مسلح مصوب ستادکل نیروهای‌مسلح به جزء مجموعه ستاد سازمان که مجاز به تشکیل بایگانی ویژه نیمه‌متمرکز می‌باشد، سایر سازمان‌ها و صنایع که گردش اسناد سری و بالاتر در آنها وجود دارد موظف به تشکیل بایگانی ویژه متمرکز می‌باشند. درحال‌حاضر در اکثر بایگانی‌های ویژه ممیزی اسناد سری و بالاتر صورت نگرفته و تعداد دقیق اسناد موجود در آنها مشخص نمی‌باشد. ضمن اینکه هیچگونه تقلیل یا امحایی درخصوص اسناد قدیمی موجود در بایگانی‌های ویژه صورت نپذیرفته است. بایگانی‌های ویژه فاقد درب‌های مجهز به قفل رمز و سیستم اعلام خطر می‌باشند و در اکثر موارد اسناد جهت رؤیت، اقدام رؤسا و مدیران از بایگانی ویژه خارج می‌شوند. عدم تشکیل بایگانی ویژه جهت نگهداری اسناد و مدارک سری و بالاتر،

عدم طبقه‌بندی و علامت‌گذاری صحیح اسناد و مدارک طبقه‌بندی‌شده، عدم رعایت حیطه‌بندی در مکان‌های حاوی اسناد و اطلاعات دارای طبقه‌بندی، دسترسی کارکنان فاقد صلاحیت امنیتی به اسناد و اطلاعات دارای طبقه‌بندی، فقدان تجهیزات ایمنی و اطفای حریق در محل‌های نگهداری اسناد و مدارک دارای طبقه‌بندی نیز از جمله تهدیدات و آسیب‌پذیری‌ها در این زمینه می‌باشد.

ط) ارسال و مراسلات اسناد به خارج از مجموعه‌ها:

نقل و انتقال اسناد دارای طبقه‌بندی از یک محل به محلی دیگر باتوجه به خطراتی که در مسیر انتقال وجود دارد، موجب پایین‌آمدن درجه حفاظت آن اسناد و اطلاعات می‌گردد. ارسال از طریق دبیرخانه خطرات سرقت، مفقودیت و دسترسی‌های غیرمجاز و از طریق وسایل مخابراتی تهدید جاسوسی و شنود را به‌دنبال دارد. لذا ضروریست برای ارسال و مراسلات اسناد و مدارک طبقه‌بندی‌شده از پیک‌های ورزیده و باهوش که آموزش‌های لازم را طی نموده‌اند استفاده شده و اسناد در داخل کیف‌های مجهز به قفل رمز و خودروهای مطمئن منتقل شوند. درحال‌حاضر بیشتر سازمان‌ها فاقد پیک مشخص می‌باشند و اسناد توسط افراد مختلف جابجا می‌شود. ضمن اینکه در برخی موارد پیک‌ها فاقد کیف مجهز به قفل رمز بوده و در مورد مأموریت خود و نحوه برخورد با شرایط اضطراری آموزش کافی ندیده‌اند. علاوه بر این اکثر سازمان‌ها و صنایع به منظور نقل و انتقال اسناد سری و بالاتر فاقد پیک ویژه مسلح می‌باشند.

ی) تاسیس دفاتر در خارج از کشور

برخی از سازمان‌ها به‌منظور ایجاد سهولت در برقراری ارتباط با بیگانگانی که همکاری دارند اقدام به تاسیس دفاتری در کشور متبوع بیگانگان می‌نمایند ولی بدلیل عدم رعایت کامل اصول و مقررات حفاظتی و امنیتی، حفظ اطلاعات به‌طور کامل انجام نشده و منجر به افشاءِ کامل یا بخشی از اطلاعات می‌گردد و تبعات زیانباری را برای سازمان‌ها ایجاد می‌نماید.

ک) جلسات مجامع سازمان‌ها و صنایع و هیئت‌های امنا

همه ساله واحدهای تابعه سازمان نسبت به تشکیل مجامع و هیئت‌های امناء اقدام نموده و گزارش‌های کاملی از عملکرد سازمان‌ها و صنایع در این جلسات که بعضاً افرادی خارج از سازمان نیز در آن شرکت می‌کنند ارائه می‌گردد که این عمل موجب افشاء اطلاعات دارای

طبقه‌بندی مجموعه‌ها می‌گردد. بنابراین ضروریست به‌منظور حفظ اطلاعات دارای طبقه‌بندی قبل از تشکیل جلسات، تأیید صلاحیت امنیتی افراد خارج از سازمان متناسب با سطح طبقه‌بندی جلسه تعیین شده باشد، طبقه‌بندی اطلاعات ارائه‌شده متناسب با دسترسی افراد حاضر در جلسه باشد، حیطه‌بندی و حفاظت گفتار در جلسات رعایت گردد، کلیه اعضای شرکت‌کننده در جلسات، بالاخص افراد خارج از نیروهای‌مسلح به‌منظور حفاظت از اسناد و اطلاعات دارای طبقه‌بندی توجیه حفاظتی شده باشند.

بخش ۳– مدل پیشنهادی و چگونگی ایجاد دیوارهٔ آتش در سازمان

دیواره آتش مناسب، دیواره آتشی خواهد بود که بتواند ضمن مقابله با افشاء اطلاعات، لختی در تعاملات نیز ایجاد ننماید. باتوجه به مدل‌های بررسی‌شده و تدابیر مقام معظم‌رهبری چنین نتیجه‌گیری می‌گردد، مدلی که درنظر است در سازمان‌ها پیاده‌سازی شود می‌بایستی دارای خصوصیات زیر باشد:

- ❖ برای ایجاد امنیت ابتدا می‌بایست آن گستره‌ای که درنظر است در آن امنیت برقرار گردد شناسایی شود.
- ❖ تهدیدات رصد شده و راه‌های مقابله با آن دائم تقویت‌شده و ضمن نو به نو شدن راه‌های مقابله با تهدید قدیمی نیز ادامه یابد.
- ❖ آسیب‌پذیری‌های آن گستره، شناسایی شود.
- ❖ در آن گستره برای اینکه تهدید نتواند اثر خود را بگذارد در تمام لایه‌ها دیوارهٔ آتش متناسب خود را باید ایجاد نمود.
- ❖ این دیوارهٔ آتش حتما باید به روز شود.

مدلی که ارائه خواهد شد در سه بخش خواهد بود:

۱- چیستی دیوارهٔ آتش در سازمان در برابر دشمن

۲- چگونگی اجرای دیوارهٔ آتش در سازمان در برابر دشمن

۳- فرایند پویایی دیوارهٔ آتش

چیستی دیوارهٔ آتش

باتوجه به مستندات بدست‌آمده در بخش‌های قبلی کتاب، برای یافتن چیستی دیوارهٔ آتش باید مراحل زیر را طی نمود:

۱- ابتدا باید گستره‌ای از تمامی و یا بخشی از مولفه‌های سازمان که در آنجا وجود دارند را مشخص نمود.

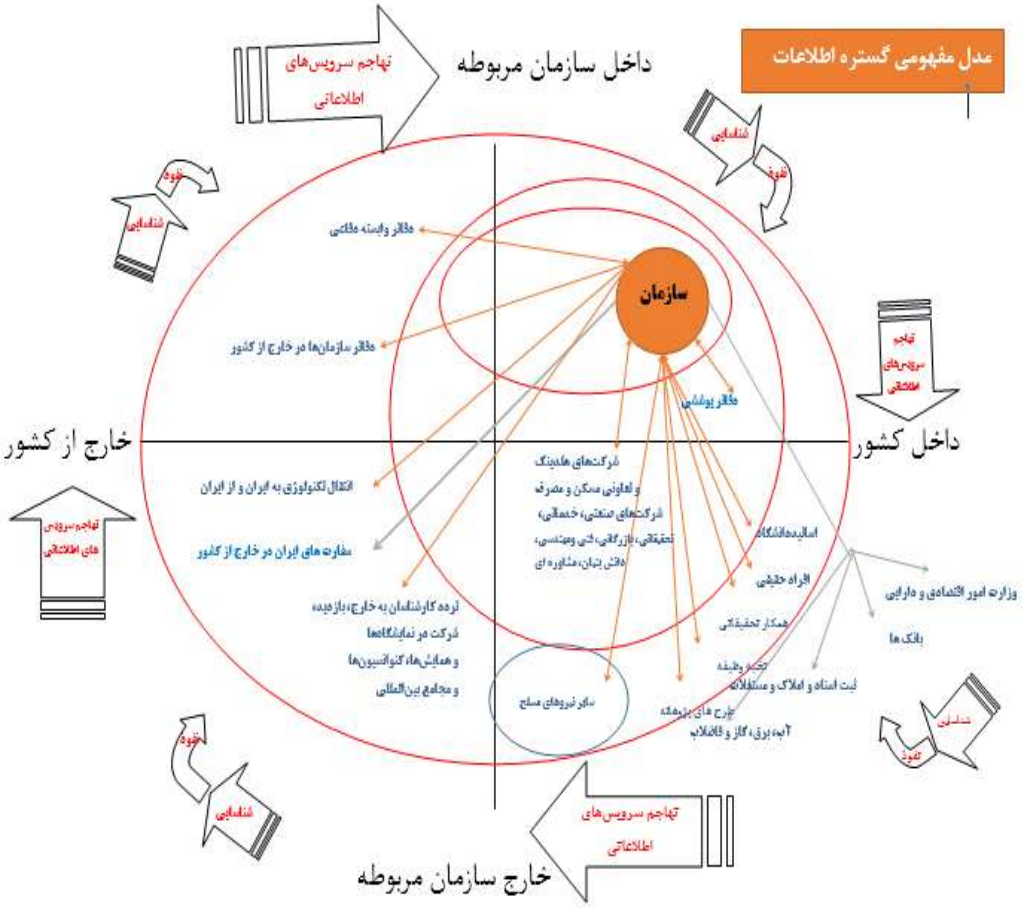
۲- نحوه فعالیت سازمان مشخص گردد.

۳- بازیگرانی که در گستره سازمان فعال هستند، شناسایی شوند.

۴- تهدیدات آن بازیگران مشخص گردد.

۵- دیوارهٔ آتش متناسب با هر تهدید معرفی شود.

به‌منظور ایجاد دیوارهٔ آتش نیاز به شناسایی بستری است که درنظر است دیوارهٔ آتش مستقر شود، بدین‌منظور ابتدا باید گستره‌ای که سازمان در آن قرار دارد و اطلاعات آن پخش شده است را شناسایی نمود و سپس سایر اقدامات را انجام داد. لذا در ادامه به ارائه مدل مفهومی گستره اطلاعات می‌پردازیم که در چهار حوزه مطرح می‌باشد:



مدل مفهومی گسترهٔ اطلاعات، بستری که دیوارهٔ آتش در آن باید استقرار یابد به چهار قسمت تقسیم می‌شود:

۱- داخل سازمان و داخل کشور

۲- داخل کشور و خارج از سازمان

۳- داخل سازمان و خارج از کشور

۴- خارج از کشور و خارج از سازمان

در این چهار بخش، ارگان‌ها، سازمان‌ها، موسسات و مراکز داخلی و خارجی مستقر می‌باشند که تمامی آنها ضمن اینکه با سازمان به‌صورت مستقیم و یا غیرمستقیم در ارتباطند، مورد هدف سرویس‌های اطلاعاتی جهان نیز قراردارند.

۱- در بخش اول که اصلی‌ترین بخش این مدل می‌باشد سازمان و کلیه مجموعه‌های مرتبط با آن قراردارد. شرکت‌های پوششی داخلی سازمان نیز در این بخش قرار دارد و سطح طبقه‌بندی اطلاعات سازمانی این بخش، از خیلی‌محرمانه تا بکلی‌سری است. لازم به ذکر است که گستره بخشی از اطلاعات سری به بخش ۳ این مدل نیز مربوط می‌شود، ولی اطلاعات خیلی‌محرمانه در حوزهٔ مختصری از چهار بخش، گسترش یافته است و اطلاعات محرمانه به بخش‌هایی که وسیع‌ترند تعلق دارد.

۲- در بخش دوم مراکز زیادی قراردارند که از سطح فاقد طبقه‌بندی تا خیلی‌محرمانه با سازمان مرتبط می‌باشند و هرکدام خصوصیات متفاوتی به شرح زیر با دیگر مراکز دارند:

الف) در این بخش نیروهای‌مسلح قراردارند که اکثر آنها مشتریان تولیدات سازمان یا شرکت هستند.

ب) بخشی از وزارتخانه‌ها: که سازمان از آنها خدماتی را دریافت می‌نمایند و بالطبع اطلاعاتی از سازمان را دریافت می‌نمایند. در اثر مرتبط‌شدن کارکنان با یکدیگر، اگر دیوارهٔ آتش مناسبی استفاده نگردد و دیوارهٔ آتش به دلایل مختلف تضعیف گردد، می‌تواند زمینه‌ساز تاثیرگذاری تهدید در داخل سازمان شده و سازمان آسیب‌پذیر می‌گردد.

ج) برخی دیگر از وزارتخانه‌ها خدمات خاصی به سازمان نمی‌دهند ولی سازمان موظف است که اطلاعات شرکت‌ها و موسساتی را که با آنها در تعامل است را ارائه نماید که اطلاعات ارزشمندی در این قالب ارائه می‌شود.

د) طیف دیگری که در این بخش با سازمان مرتبط می‌باشند شرکت‌های ایرانی داخل کشور است که سازمان پیرو سیاست برون‌سپاری، خدماتی را از این شرکت‌ها دریافت می‌نماید. لذا در اثر این ارتباط بخش زیادی از اطلاعات با ارزش سازمان نیز در اختیار این بخش قرار می‌گیرد.

ه) دانشگاه‌ها، دانشجویان و فارغ‌التحصیلانی نیز هستند که هرکدام با بخشی از سازمان مرتبطند تا خدماتی را ارائه داده و تسهیلاتی را دریافت نمایند که در اثر این ارتباط و تردد به مراکز دارای طبقه‌بندی سازمان، از اطلاعات سازمان مطلع می‌گردند.

و) مجموعه‌های تابعه سازمان جهت ارائه خدمات به کارکنان خود شرکت‌هایی را تاسیس نموده‌اند و مدعی استقلال از سازمان هستند ولی برخی از آنها در داخل مراکز سازمان مستقر هستند و برخی بیرون از سازمان، همچون شرکت‌های تعاونی مصرف، مسکن و...

۱- ارزش طبقه‌بندی اطلاعات در این بخش، از سطح فاقد طبقه‌بندی تا سری را شامل می‌شود همچون دفاتری که سازمان‌ها در خارج از کشور تاسیس نموده‌اند و با بیگانگان و شرکت‌های آن کشور مرتبط می‌باشند و برخی از آنها نیز کارمندان محلی استخدام می‌نمایند.

۲- در بخش آخر (خارج از سازمان و خارج از کشور) کلیه کشورها و شرکت‌های خارج از کشور را دربر می‌گیرد. کارکنان سازمان نیز با آنها مرتبط می‌شوند و در اثر برخی تعاملات (انتقال تکنولوژی و...) از طریق سفارتخانه‌های ایران در خارج از کشور ارتباط برقرار می‌کنند.

طبق مدل مفهومی، گسترهٔ اطلاعات می‌تواند شامل کارکنان و یا افرادی باشد که با سازمان مرتبط می‌باشند و به چهار دسته تقسیم می‌شوند:

۱- کسانی که خارج از کشور و خارج از سازمان شاغلند.
۲- کسانی که خارج از کشور ولی داخل سازمان شاغلند.
۳- کسانی که داخل کشور و خارج از سازمان شاغلند.
۴- کسانی که داخل کشور ولی خارج از سازمان شاغلند.

همه این چهار دسته در شرایط یکسانی نیستند. گروه‌های اول و سوم و همچنین گروه‌های دوم و چهارم شباهت‌هایی با یکدیگر دارند ولی شرایط و زمین بازی آنها باهم متفاوت است، لذا تهدیدات و آسیب‌پذیری‌های آنها نیز متفاوت است و باتوجه به تهدید و آسیب‌پذیری‌ها، نوع و چگونگی فعالیت دیوارهٔ آتش آنها نیز متفاوت خواهد شد.

چند بخش در چگونگی فعالیت دیوارهٔ آتش و موفق‌بودن دیوارهٔ آتش بسیار موثر خواهند بود زیرا نتیجه فعالیت آنها و پیاده‌سازی نتایج بازخورد آنها در دیوارهٔ آتش، می‌تواند آن دیوارهٔ آتش

را هوشیار، پویا و مشغول به‌کار نگاه دارد تا تهدیدی نتواند از آن عبور نموده و آسیب‌پذیری را ایجاد نماید.

همان‌گونه که در مدل مفهومی، گستره اطلاعات سازمان مشاهده می‌شود سرویس‌های اطلاعاتی، گروهک‌ها، فرقه‌ها و... دائم درحال رصدنمودن فعالیت‌های سازمان و مرنبطین داخلی و خارجی آن و همچنین مراکزی هستند که با سازمان در ارتباط می‌باشند و سعی و تلاش آنها بر این است که نفوذ نموده و تا هر سطحی از اطلاعات که در توان آنها است را جمع‌آوری و مورد بهره‌برداری قرار دهند و به حیثیت سازمان‌ها و نظام جمهوری‌اسلامی‌ایران لطمه وارد نمایند.

سازمان طی فرایندهای مختلفی فعالیت می‌نماید تا پروژه‌های متعهدشده را به نتیجه برساند و در این راستا تعامل و همکاری با شبکه همکاران را مدنظر دارد. لذا در هرجا از مدل منظور از کارکنان، کلیه کسانی می‌باشند که در داخل سازمان و یا خارج از سازمان با پروژه‌های سازمان مرتبط می‌باشند و اطلاعات آن را در اختیار می‌گیرند که در منحنی تعهد این کارکنان تقسیم‌بندی شده‌اند.

باتوجه به مطالب فوق، دیوارهٔ آتشی باید ایجاد و این دیواره به‌گونه‌ای باید عمل نماید که هم مانع برای فعالیت سازمان ایجاد ننماید و هم منجر به برقراری امنیت گردد و اثر تهدیدهای دشمنان را نیز به حداقل برساند.

طبق مدل مفهومی، گستره اطلاعات سازمان در داخل و خارج از سازمان (اطلاعات، اسناد و تجهیزات آن) وجود دارد و دیوارهٔ آتش باید تمامی اینها را در چتر حمایتی خود قرارداده تا بتواند امنیت آن را تامین نماید.

حال باید ببینیم که چگونه باید هم فعالیت خود را در سازمان ادامه داده و هم بارویی بسازیم که امنیت ایجاد شود و دشمن نتواند تهدیدی ایجاد کند. بارو چگونه می‌تواند حاکم شود؟ بخشی از پیاده‌سازی بارو به‌صورت سخت‌افزاری و فیزیکی است و بخشی از آن نیز باتوجه به بیانات مقام معظم رهبری با حفظ عزت می‌تواند، بدست آید.

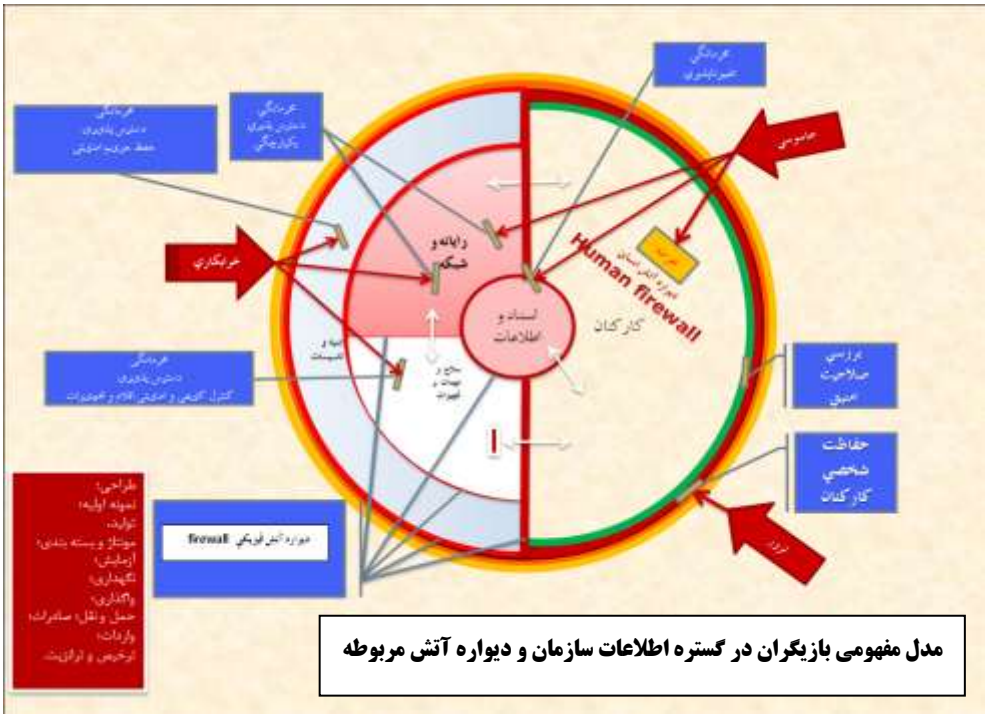
با بررسی معانی کلمه عزت، متوجه می‌شویم که شکست‌ناپذیری نیز یکی دیگر از معانی این کلمه است، لذا دیوارهٔ آتش در این گستره‌ای که اطلاعات سازمان پراکنده شده است می‌بایست طوری عمل نماید که شکست‌ناپذیر نیز باشد.

غیر از اقدامات فیزیکی برای اینکه بتوانیم عزت خود را خوب حفظ کنیم باید بصیرت نیز داشته باشیم که موضوع دیگری است که در بیانات مقام معظم رهبری در برابر دشمن ذکر شده است. لذا برای اینکه بصیرت را افزایش دهیم باید اصولی را تهیه کنیم که در هر بخش، بازیگران آن بخش هم به آن واقف باشند و با تسلط بر آن بتوانند عزت خود را حفظ کنند.

هرجا که فیزیک اطلاعات یعنی سندی وجود داشت، باید با امکانات فیزیکی، دیوارهٔ آتش را ایجاد نمود و قوانین خاص خودش را در آن دیوارهٔ آتش حاکم نمود و هرجا به کارکنان مرتبط می‌شود با تقویت عزت آنها دیوارهٔ آتش را در وجود کارکنان ایجاد نمود.

اصل کلی در قوانین و دستورالعمل‌هایی است که در هر دو دیوارهٔ آتش حاکم است یکی از راه‌ها حفظ عزت است که باید بصیرت خود را در این خصوص بالا برد.

باتوجه به مطالب فوق، در هر بخش از مدل مفهومی گستره اطلاعات، بازیگران و تاثیرگذاران آن با دیگر بخش‌ها فرق می‌کند، در مدل زیر که باعنوان مدل مفهومی بازیگران و میزان نقش آنها در تبادل اطلاعات در گستره اطلاعات است، به بازیگران و تاثیرگذاران پرداخته می‌شود.



مدل مفهومی بازیگران در گستره اطلاعات سازمان و دیواره آتش مربوطه

اولین لایه در این دیوارهٔ آتش پدافند غیرعامل است که هم در بعد انسانی و هم در بعد غیرانسانی می‌تواند حاکم شود و آن این است که تلاش کنیم که دشمن ما را نبیند. این لایه اول است و لایه دوم این است که اگر دیده شدیم شناسایی نشویم و لایه سوم اینکه اگر شناسایی شدیم مورد هدف قرار نگیریم و لایه چهارم اینکه اگر مورد هدف قرار گرفتیم، هزینه دشمن را بالا ببریم. هر لایه از دیوارهٔ آتش سعی دارد این چهار اقدام را انجام دهد و آخرین خاکریز در دیوارهٔ آتش ما در برابر جاسوسی، ترور و خرابکاری (که سه تهدید مهم است) مواردی است که در ادامه تشریح شده است.

در این مدل ۵ مولفه وجود دارد که هرکدام به نوعی بازیگر عرصه اطلاعات می‌باشند که به‌ترتیب اولویت به تشریح هر یک از آنها خواهیم پرداخت.

برای ایجاد یک مجموعه در سازمان می‌بایست ابنیه و تاسیساتی را در یک بستری که توام با امنیت است ایجاد کرد و باتوجه به ماموریت آن مجموعه، سلاح، مهمات و تجهیزات مرتبط را تهیه نمود و برای اینکه با تکنولوژی‌های روز پیش رفت نیاز به راه‌اندازی شبکهٔ رایانه‌ای و

رعایت الزامات امنیتی خاص آن می‌باشد. در این مرحله، کارکنان مجموعه پس از گذشتن از فیلتر تعیین صلاحیت وارد مجموعه می‌شوند تا در راستای ماموریت محوله فعالیت نمایند. در ابتدای کار اطلاعات، اسناد و دانش نیز وجود دارد که با شروع فعالیت‌ها این دانش نیز گسترده‌تر می‌گردد که رسوب آن در بخش اسناد و اطلاعات ایجاد می‌شود.

هر یک از بخش‌ها یک دیوارهٔ آتش مخصوص به‌خود را دارد. هرچه میزان اهمیت اسناد و اطلاعات باتوجه به اهمیتش، افزایش می‌یابد، در شرایط محفوظ‌تری نگهداری می‌گردد که از افشاء آن جلوگیری شود.

رایانه و شبکه، دیوارهٔ آتش سخت‌افزاری و نرم‌افزاری خاص خود را خواهند داشت و سلاح، مهمات و تجهیزات نیز در شرایط مناسبی نگهداری می‌گردد تا به سهولت دردسترس باشد و در زمان نیاز به آن با اطمینان به‌کارگیری شود که این خود نوعی دیواره آتش محسوب می‌شود.

ابنیه، خود حفاظت و بارویی است برای مجموعه‌های سازمان، که تاسیسات و سلاح و... در داخل آن قرار می‌گیرند. این دیوارهٔ آتش ایجاد می‌گردد که در مقابل تهدیداتی چون خرابکاری و جاسوسی مقابله کند. اما عنصر مهمی که کلید این بخش‌ها را به‌کار می‌گیرد تا به ماموریت محوله خود برسد، تهدیداتی همچون ترور و یا گرفتارشدن در دام جاسوسی است که هرکدام از آنها نیز می‌تواند دیوارهٔ آتشی داشته باشد. برای مقابله با تهدید ترور، دیوارهٔ آتش مناسب، اجرای صحیح و کامل حفاظت شخصی موردنیاز است.

تهدید مهم دیگری که در کمین کارکنان است، جاسوسی می‌باشد. باتوجه به بیانات مقام معظم رهبری، بهترین دیوارهٔ آتش برای کارکنان حفظ عزت آنها می‌باشد که در مقابل این‌گونه تهدیدات شکست‌ناپذیرشده و مانعی برای فعالیت‌های دشمن شوند.

تهدید جاسوسی در سایر حوزه‌ها نیز وجود دارد که یا بر اثر عدم اجرای الزامات، منجر به نفوذ دشمن می‌گردد و یا از طریق عامل انسانی (کارکنان)، دشمن به هدف خود می‌رسد که هرکدام از حوزه‌ها (رایانه و شبکه، سلاح و مهمات، تجهیزات، ابنیه و تاسیسات) الزامات خاص خود را دارد که رعایت آن دیوارهٔ آتش را ایجاد خواهد نمود.

به‌طور مثال در صورتی‌که تهدید در کمین اسناد، اطلاعات و دانش رسوب‌کرده در مجموعه‌ها باشد، با رعایت دو عامل محرمانگی و تغییرناپذیری می‌توان دیوارهٔ آتش مناسب آن را ایجاد

نمود و کارکنان نیز در کنار حفظ عزت خود و رعایت این دو عامل (دیوارهٔ آتش) مانع تحقق جاسوس می‌شوند.

سه حوزه دیگر غیر از اینکه مورد تهدید جاسوسی می‌باشند، مورد تهدید خرابکاری نیز هستند که درصورت رعایت الزامات خاص هر یک از حوزه‌های ذکرشده، می‌توان با آن تهدید نیز مقابله نمود.

درکل چهار بخش مدل مفهومی؛ شامل گستره اطلاعات عوامل کارکنان، اسناد و اطلاعات، سلاح، مهمات و تجهیزات، رایانه و شبکه می‌باشد که در هر بخش وزن آنها با بخش دیگر تفاوت دارد. برای اینکه تهدید آنها را آسیب‌پذیر ننماید باید طبق اصول و استانداردها حفظ شوند و تنها در اختیار کسانی قرار گیرند که صلاحیت دانستن آن و نیاز به دانستن آن را دارند و طبق این مدل مفهومی، کارکنان در هر محیط، حداقل ۵۰ درصد دخیل می‌باشند و به‌همین نسبت تهدیدها و آسیب‌پذیری‌ها در کمین آنها می‌باشند. ۵۰ درصد دیگر در بین باقی عوامل تقسیم می‌شود که بسته به نوع مکان، زمان و وزن هر یک و در موقعیت‌های مختلف، متفاوت است. ولی تهدید و آسیب‌پذیری هر موضوع در هر مکان می‌تواند وجود داشته باشد. به‌طور مثال کارکنان در معرض تهدید ترور و جاسوسی قراردارند و اسناد، اطلاعات، سلاح، مهمات و تجهیزات نیز مورد هدف جاسوسی می‌باشند که از طریق کارکنان و یا کارکنان نفوذی اقدام به جاسوسی می‌نمایند. رایانه و شبکه نیز به‌عنوان ابرازی در جاسوسی مورد استفاده قرار می‌گیرد. باتوجه به گسترش رایانه در تمام امور، یکی از ابزارهای اساسی برای انجام جاسوسی و جمع‌آوری اطلاعات رایانه می‌باشد.

باقی عوامل ازجمله حفاظت فیزیکی، ابنیه، تجهیزات، سلاح و... هدف تهدید دیگری به نام خرابکاری قراردارند.

منظور از کارکنان، تنها کارکنان سازمان نمی‌باشد، بلکه کلیه افرادی که به هردلیل با سازمان مرتبط و در این بخش قراردارند. همه در قبال سازمان مسئول می‌باشند ولی سهم آنها بایکدیگر به‌دلیل میزان دسترسی به اطلاعات دارای طبقه‌بندی، تفاوت خواهد داشت و این میزان سهم هر قشر در منحنی زیر به نام منحنی تعهد مشخص شده است.

در بخش سلاح، مهمات و تجهیزات؛ فعالیت‌های زیادی صورت می‌پذیرد که هر یک از این حوزه‌های کاری، خود می‌تواند مورد تهدید هریک از موضوعات مطرح‌شده(جاسوسی، خرابکاری)

قرار گیرد که در طراحی دیوارهٔ آتش می‌بایستی این فعالیت‌ها را درنظر گرفت. فعالیت‌هایی که در این بخش صورت می‌پذیرد عبارتند از: طراحی، تهیه نمونه اولیه (پایلوت)، تولید، مونتاژ و بسته‌بندی، آزمایش، نگهداری، واگذاری، حمل و نقل، صادرات، واردات، ترخیص و ترانزیت.

فرایندها برای تحقق اهداف سازمان در هر یک از این حوزه‌های ذکر شده اقدامات زیادی انجام می‌دهند و در همین راستا با شبکهٔ همکاران دفاعی مرتبط می‌گردند و در برخی از این موارد با بیگانگان نیز مرتبط می‌شوند.

چگونگی اجرای دیوارهٔ آتش

- باتوجه به ابعاد دیوارهٔ آتش در سازمان
- در بعد غیرانسانی اصول حفاظت فیزیکی، حفاظت شخصی و گزینش نیروی انسانی این وظیفه را به‌عهده دارند.
- در بعد انسانی باتوجه به بخش‌های قبلی کتاب، با ایجاد و ارتقاء عزت (Human firewall) در کلیه عوامل انسانی می‌توان دیوارهٔ آتش را اجرا نمود.
- اجرای دیوارهٔ آتش باتوجه به نقش و تاثیرگذاری عوامل انسانی و متناسب با چالش‌های سازمان به اجرا گذاشته خواهد شد.

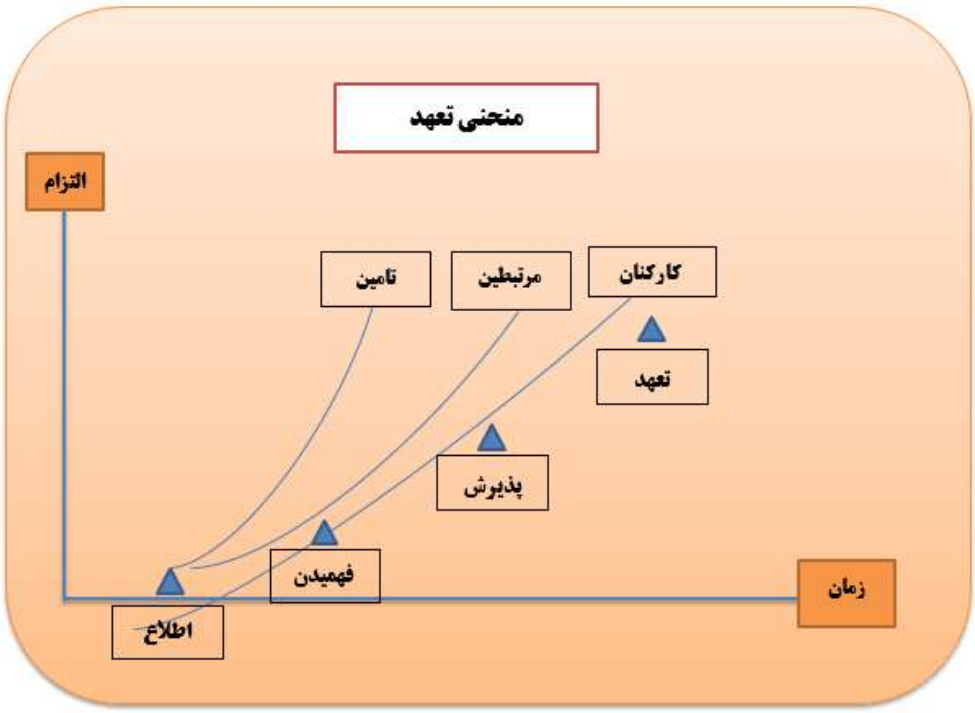
فرمول ایجاد دیوارهٔ آتش برای کارکنان

فرمول فوق با تدوین استانداردها، اصول، قوانین، رویه‌ها و سیاست‌های شایسته در قالب چارچوب پسندیده رفتاری شروع می‌شود.

پس از اینکه در سازمان این موارد تدوین و مصوب گردید می‌بایست هر یک از کارکنان که در منحنی تعهد تقسیم‌بندی شده‌اند به میزان سهم خود مورد آموزش قرارگیرند و دانش پسندیده رفتاری در آنها ایجاد شود.

پس از انجام آموزش‌ها؛ ایجاد دانش و بصیرت در وجود هر یک از کارکنان به میزانی که لازم است ایجاد خواهد شد و در نتیجه باعث ایجاد عزت و تقویت آن در وجود کارکنان می‌شود و این عامل همچون دیوارهٔ آتش در برابر دشمن و عوامل دشمن عمل خواهد نمود.

منحنی تعهد



در منحنی تعهد دو محور و سه منحنی ترسیم شده است و این سه منحنی نشان‌دهنده کارکنان در مدل مفهومی بازیگران در گستره اطلاعات سازمان را نشان می‌دهد.

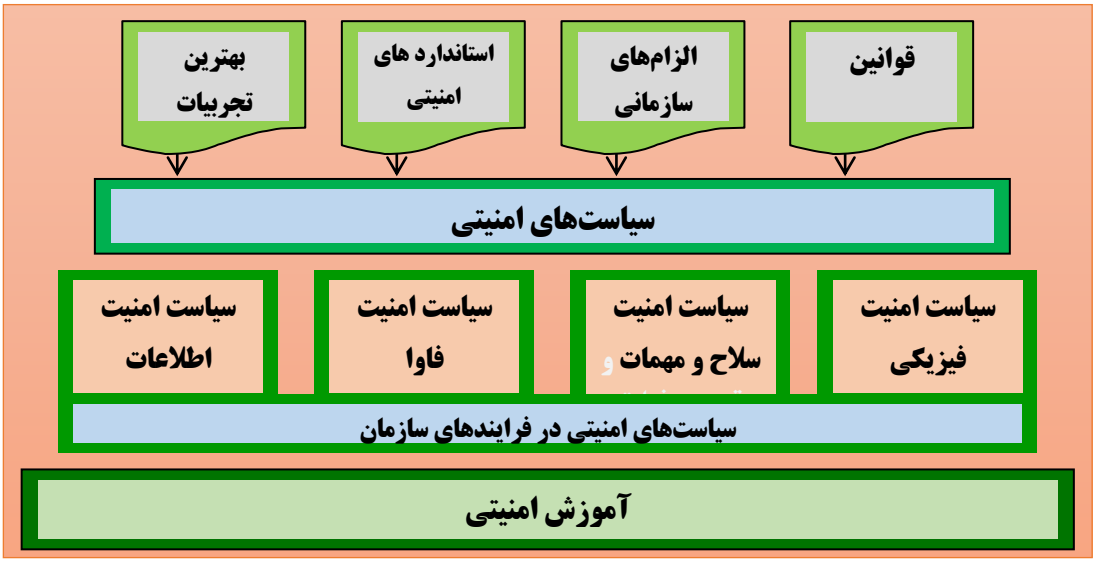
یک منحنی تامین‌کنندگان هستند. میزان اطلاعاتی که در اختیار تامین‌کنندگان قرار می‌گیرد در حد نیازمندی‌های سازمان می‌باشد.

منحنی دوم مرتبطین هستند. مرتبطین کلیه کسانی هستند که با سازمان ارتباط و تعامل برقرار می‌نمایند و به محیط‌های سازمان تردد داشته و با کارکنان سازمان به واسطه قراردادی که منعقد نموده‌اند مرتبط هستند و منحی سوم کارکنان سازمان می‌باشد.

در این نمودار در منحنی تعهد چهار شاخص وجود دارد که یکی از شاخص‌ها جنبه عمومی داشته و به‌عنوان شاخص اطلاع و باقی شاخص‌ها؛ شاخص‌هایی هستند که حداقل به یکی از منحنی‌ها مرتبط می‌باشد. به‌طور مثال شاخص فهمیدن مخصوص تامین‌کنندگان است ولی

مرتبطین و کارکنان نیز این شاخصه را دارا می‌باشند. پس از این، شاخص پذیرش است که مرتبطین باید این شاخصه را بدست آورند و کارکنان نیز غیر از این شاخصه، شاخصه بعدی یعنی تعهد را نیز باید بدست آورند.

معماری محتوی آموزش امنیتی



به‌منظور تهیه محتوی آموزش‌های امنیتی می‌بایست در ابتدا چهار موضوع را تهیه کرد که عصاره این چهار موضوع سیاست‌های امنیتی نام خواهند گرفت.

- بهترین ابتکارات عملی: بهترین ابتکارات و تجربیاتی را که بیشتر دانش و اندوختهٔ سال‌های گذشته و تلاش نخبگان می‌باشد جمع‌آوری و دسته‌بندی نموده تا در مواردی که کاربرد دارد مورد استفاده قرارگیرد.
- استانداردهای امنیتی: مجموعه الزام‌هایی که در زمینهٔ کاری مرتبط با سازمان می‌باشد و در امنیت تاثیرگذار است در این بخش جمع‌آوری می‌گردد.
- الزام‌های سازمانی: در هر سازمان الزام‌هایی خاص آن سازمان وجود دارد که باتوجه به موقعیت و یا شاخصه‌هایی که آن سازمان وجود دارد، تعیین می‌گردد و برآیند آن در امنیت نیز

تاثیرگذار خواهد بود. به‌طور مثال عدم ارتباط با بیگانگان، موضوعی است که در اثر این‌گونه ارتباط‌ها، احتمال بروز مشکلات امنیتی برای فردی که در سازمان شاغل است وجود دارد، ولی اگر در محیطی که به سازمان ارتباطی نداشته و یا شغلی است که سرویس‌های امنیتی دشمن را مورد طمع قرار نمی‌دهد، شاغل باشد، ارتباط‌گیری با بیگانگان خطری برای او نخواهد داشت و چنین الزامی در آن محیط وجود نخواهد داشت.

- قوانین: کلیه قوانین حقوقی و... که در امنیت سازمان تاثیرگذار بوده و یا مرتبط می‌باشد دراین بخش می‌بایست جمع‌آوری گردد.

همان‌گونه که اشاره گردید با گردآوری موارد فوق سیاست‌های امنیتی (در زمینه آموزش امنیتی) را می‌توان تهیه نمود.

در مرحله بعد باتوجه به فرایندهای موجود در سازمان و فعالیت‌هایی که در آن فرایندها انجام می‌شود که مرتبط با پروژه‌های سازمان می‌باشد در زمینه‌های امنیت اطلاعات؛ امنیت فاوا؛ امنیت سلاح، مهمات و تجهیزات؛ امنیت فیزیکی و پدافند غیرعامل، سیاست‌های لازم استخراج می‌گردد تا مطالبی که نیاز است کارکنان در این زمینه‌ها بدانند و طبق منحنی تعهد نسبت به آن متعهد باشند، تهیه شود.

راهبرد آموزش امنیتی

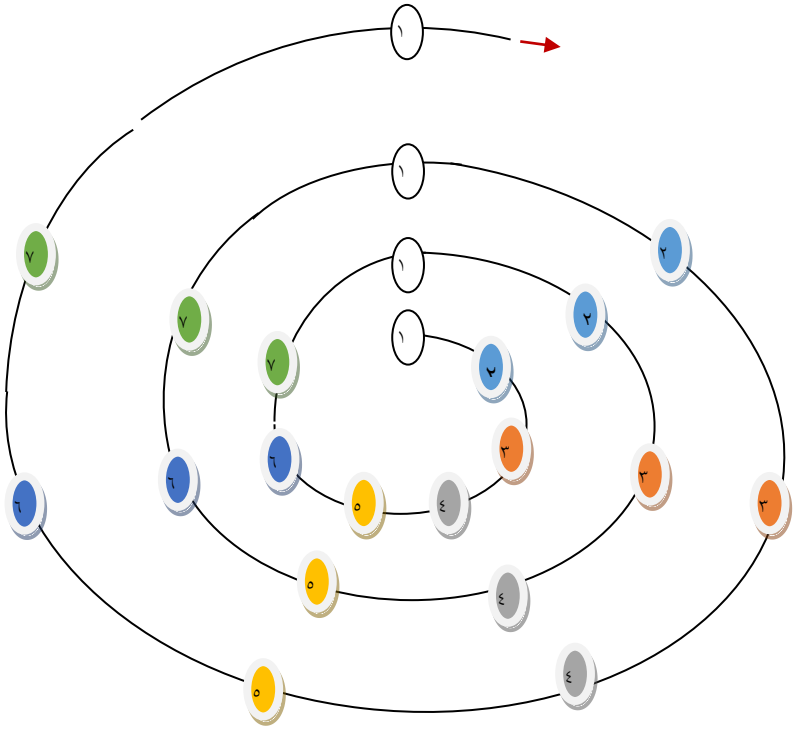
آموزش امنیتی در ۷ مرحله و طی یک فرایند مارپیچی به‌هم پیوسته، می‌تواند انجام شود و باتوجه به پیشرفت علم، تکنولوژی و تغییر نحوه بروز تهدید می‌بایست آموزش‌ها نیز به‌روزشده و گسترش یابد تا به راهبردی که در چشم‌انداز آینده سازمان داریم بتوانیم برسیم. یعنی در هر بخش باتوجه به پیشرفت علم و تکنولوژی مطالب به روزتر به مخاطب ارائه گردد،

به‌طور مثال در مرحله اول فرایند؛ اگر مخاطب به اندازهٔ حلقه اول از فرایند، مطالب را کسب نمود تحت‌عنوان مسئول‌سازی. در حلقه دوم که دو بعدی آموزش است با همان محور آموزشی ولی متناسب با نیازمندی مخاطب، آخرین موارد آموزشی ارائه گردد تا شاخصه‌های مسئول‌سازی در مخاطب ایجاد شود و در باقی مراحل فرایند نیز همین‌گونه باید عمل شود. باتوجه به منحنی تعهد، می‌بایست آموزش‌های لازم به عوامل انسانی طبق این فرایند ارائه گردد تا دیوارهٔ آتش مربوطه (عزت) در وجود عوامل انسانی ایجاد گردیده و در آموزش‌های بعدی که

طبق این فرایند مارپیچی ادامه‌وار خواهد بود دائم درحال تکمیل‌شدن باشد تا باتوجه به پیشرفت علم و تکنولوژی، خللی به امنیت عوامل انسانی وارد نگردد و تهدید نتواند گزندی را وارد نماید.

در فرایند مارپیچی که راهبرد آموزشی را نشان می‌دهد، هر مرحله با یک رنگ مشخص شده که در جدول زیر مراحل معرفی شده است.

۱	۲	۳	۴	۵	۶	۷
آگاهسازی	هوشیارسازی	مصون‌سازی	مسئول‌سازی	همراه سازی	توانمندسازی	ظرفیت سازی



فرایند پویایی دیوارهٔ آتش

باتوجه به مدل‌های مفهومی فوق و فرمول ایجاد دیوارهٔ آتش برای کارکنان و همچنین متغیربودن نوع و نحوه ایجاد تهدید و آسیب، نیاز است که فرایند دائم و مستمر، مشغول به‌کار باشد تا بتواند دیوارهٔ آتش را پویا، زنده و فعال نگاه دارد تا گزندی به سازمان و مرتبطین آن وارد نگردد.

مقام معظم رهبری در دیدار خود با جهادگران جهاد سازندگی در تاریخ ۱۳۷۷/۰۷/۱۵ فرموده‌اند: (...لحظه‌ای نباید متوقف شد باید دائم درحال پیشرفت بود، چون دشمن منتظر خاکریز نرم است که نفوذ کند...)، لذا برای اینکه لایه‌هایی که در مدل مفهومی معرفی شد به مرور زمان و با پیشرفت تکنولوژی دشمن به خاکریز نرم تبدیل نشود، باید دائم کل گستره را رصد نموده و نقاط ضعف و آسیب‌پذیر را شناسایی و برطرف نمود تا دشمن نتواند از آن طریق نفوذ نماید.

- با استفاده از فرایند فوق می‌توان پویایی و به‌روزبودن دیوارهٔ آتش را دنبال نمود. این فرایند با تهیه گزارش ۷ بندی که گزارشی از بروز تهدیدها و آسیب‌پذیری‌ها می‌باشد آغازشده و خروجی این بخش به دفتر مطالعات استراتژیک و یا آینده‌پژوهی ارسال می‌گردد و پس از تجزیه، تحلیل و بررسی، نتیجه به اتاق فکر تحویل می‌گردد. در اثر بررسی؛ درصورتی که نیاز به اقدام بیشتر و یا مستندات بیشتری باشد به همان دفتر اعلام می‌گردد و درصورتی که تمامی جوانب بررسی‌شده و مستندات به‌حدی باشد که قابل تصمیم‌گیری به‌وسیله آنها باشد در دو زمینه؛ اینکه نیاز به اصلاح قوانین، مقررات و ضوابط باشد و یا نیاز به آموزش و یا رفع آسیب‌پذیری‌ها؛ به هر بخش ارجاع داده می‌شود.
- مرکز فرماندهی می‌بایستی اقدامات زیر را انجام داده و اطلاعات اولیه در اختیار دفتر مطالعات استراتژیک و یا آینده‌پژوهی قرار گیرد تا ادامه فرایند ایجاد شود:

تهدیدات هر بخش نوشته شود:

۱- تهدید هر بخش با بخش دیگر فرق می‌کند.

۲- میزان اهمیت آسیب‌پذیری در یک مکان، احتمال دارد در مکانی دیگر به همین اندازه اهمیت نداشته باشد.

۳- برای شناسایی سریع آسیب‌پذیری‌ها، سیستم عصبی طراحی شود که این سیستم می‌تواند تهدیدات را بشناسد و آسیب‌پذیری‌ها را شناسایی نموده و برای تصمیم‌گیری به‌طور کامل، صحیح و سریع گزارش دهد.

۴- یادآوری یا یادگیری در بازخورد باید مشخص شود.

۵- غیر از اینکه یک دیوارهٔ آتش کلی وجود دارد، در پیرامون هر موضوع نیز یک دیوارهٔ آتش وجود دارد و حتی هریک از زیر بخش‌ها و کاراکترها، کارکنان هر بخش نیز نوعی دیوارهٔ آتش دارند.
۶- در هر موضوع بخش‌های مختلفی داریم (سطح مدیریتی، کارشناسی، کارکنان عادی یا خدماتی، مراجعین یا ارباب رجوع)
۷- خصوصیات، اصول و قوانین ارباب رجوع هر بخش با بخش‌های دیگر احتمالا متفاوت است. (برای هرکدام تمهیدات خاصی باید پیش‌بینی شود (نحوه تماس، نحوه ورود به اماکن، نحوه ارائه و دریافت اطلاعات و...).
۸- همیشه به یاد داشته باشیم که، هرچیز که حساس‌تراست محافظت از آن باید بیشتر باشد.

بخش ۴– نتیجه‌گیری و پیشنهادات

باتوجه به بررسی‌های بعمل‌آمده و تجزیه و تحلیل یافته‌ها، به این نتیجه می‌رسیم که نحوه ایجاد دیوارهٔ آتش انسانی، آگاه‌نمودن عوامل انسانی است و هرچه این آگاهی بیشتر شود، استقامت دیوارهٔ آتش انسانی نیز تقویت خواهد یافت. بالاترین درجهٔ عوامل انسانی که به آن دست خواهند یافت، شکست‌ناپذیری (عزت) خواهد بود. این آگاهی هرچه در رفتار و عملکرد فرد تاثیرگذارباشد، شکست‌ناپذیری او تقویت بیشتری خواهد یافت.

برای ایجاد دیوارهٔ آتش انسانی در یک جامعه هدف، در ابتدا نیاز به شناخت آن جامعه و میزان آگاهی از آن است تا آنها را به‌سمت ایجاد دیوارهٔ آتش انسانی سوق داد. در مرحله دوم باید آنها را ترغیب نمود تا عمل آنها مصداق جهاد کبیر باشد. در جهاد کبیر ابتدا باید دشمن‌شناسی را به عوامل انسانی آموزش داد و پس از آن نحوه انجام جهاد کبیر تعلیم داده شود. در اسلام ابتدا فرد ایمان می‌آورد و بعد مومن، باتقوا و پرهیزکار می‌شود و سپس می‌تواند به مراتب بالاتری در اسلام نائل شود که مصداق مفهوم این بیت زیر است؛

رسد آدمی به جایی که به جزء خدا نبیند

در ارائه آگاهی و آموزش کارکنان نیز باید بدین‌گونه عمل کرد که از ابتدای استخدام ملزم گردند که آموزش‌هایی که لازم است را ببینند و با طی‌نمودن سنوات، آموزش‌های مختلف را فرا بگیرند و شرط و لازمه تصدی هر شغلی دیدن اموزش‌های خاص باشد که فرد بتواند با دانش کامل، به جهاد کبیر بپردازد و با این توضیح؛ فرایند یادگیری را می‌توان به صورت زیر ترسیم نمود:

۱- کسب مهارت

۲- کسب آگاهی و درک

۳- توانایی تجزیه و تحلیل و به‌کارگیری آن

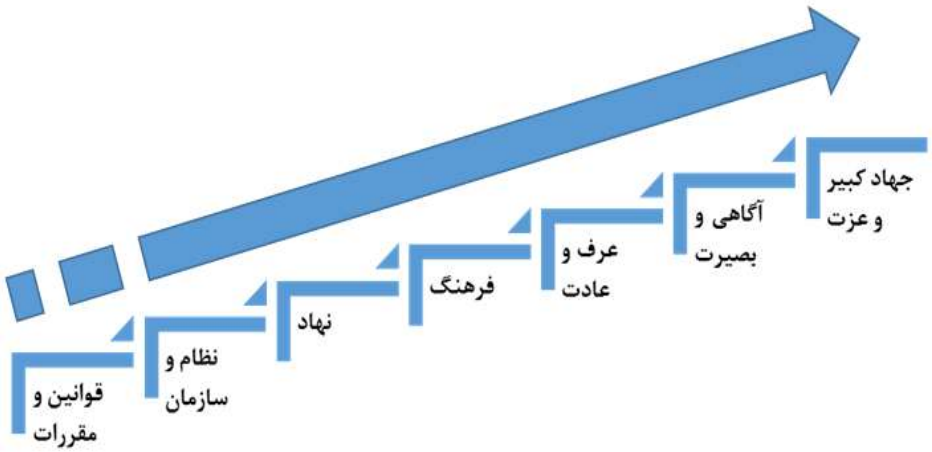
۴- توانایی نظریه‌پردازی، تولید و نوآوری در امور

در جهاد کبیر آن عوامل انسانی به این مهم دست خواهند یافت که کارهای خود را طوری انجام دهند که دشمن نتواند از آن بهره‌ای ببرد و یا در جهتی اقدام نکنند که به نفع دشمن باشد.

وقتی این روحیه تقویت شود و این ظرفیت در عوامل انسانی ایجاد گردد در آنها خصلتی می‌تواند ایجاد شود که در برابردشمن و توطئه‌های آنها شکست‌ناپذیر گردند و این یعنی به درجه عزت رسیده‌اند، لذا می‌توان مدل زیر را ترسیم نمود.

در شناسایی جامعه هدف و میزان آگاهی آنها نیز می‌توان شاخص‌هایی را تعیین نمود. به‌طور مثال رفتار عوامل انسانی چه قدر در ارتقاء امنیت تاثیرگذار است و دوم اینکه در ایجاد خلل در ارتقاء امنیت چقدر تاثیرگذر می‌تواند باشد.

در پایان براساس مطالبی که کل این کتاب ارائه گردیده روند توسعه‌یافتگی و پیشرفت را می‌توان چنین ترسیم نمود. (که اجزای آن در مدل‌های مختلف تشریح شده است).



فهرست منابع

منابع فارسی

۱- ابن فارس، **معجم مقاییس‌اللّغه**، نشر دار الفکر، ج۱، ص۴۸۶.
۲- ابن‌منظور، **لسان‌العرب**، ج۹، ص ۱۸۵.
۳- احسان بخش شیخ صادق، **آثارالصادقین**، انتشارات دارالعلم قم، سال ۱۳۷۷ جلد ۲.
۴- اکبر هاشمی رفسنجانی و دیگران، **تفسیر راهنما**، ج۴.
۵- بشری‌راد بابک و حبیبی‌لشکری آرش؛ **ویروس‌ها و بدافزارهای کامپیوتری**. تهران: انتشارات ناقوس. سال ۱۳۹۱.
۶- بیانات مقام معظم رهبری در مراسم گرامیداشت بیست و سومین سالگرد رحلت حضرت امام خمینی(ره) در تاریخ ۱۳۹۱/۰۳/۱۴
۷- بیانات مقام معظم رهبری در دیدار مسئولان نظام در روز عید مبعث، تاریخ ۱۳۹۰/۰۴/۰۹
۸- بیانات مقام معظم رهبری در شروع درس خارج فقه؛ تاریخ ۲۰/ ۰۶/ ۱۳۷۳.
۹- بیانات مقام معظم رهبری در دیدار با فرماندهان لشکر ۲۷ محمدرسول‌الله(ص)، تاریخ ۱۳۷۵/۰۳/۲۰.
۱۰- بیانات مقام معظم رهبری در شروع درس خارج فقه؛ تاریخ ۲۰/ ۰۶/ ۱۳۷۳.
۱۱-بیانات مقام معظم رهبری در تاریخ سوم خرداد ۱۳۹۵.
۱۲- بیانات مقام معظم رهبری، دیدار با واجا، تاریخ ۲۹ /۱۳۹۷/۰۱.
۱۳-جوادی‌آملی، **توحید در قرآن**، ص ۳۶۹.

۱۴- رهبر معظم انقلاب در دانشگاه افسری و تربیت پاسداری امام حسین(ع) در تاریخ ۰۳/ ۰۳/ ۱۳۹۵.
۱۵- رهبر معظم انقلاب، روزنامه کیهان، تاریخ ۱۳۹۷/۰۴/۲۸.
۱۶- شجاعی محمّدصادق، **توکّل به خدا**، نشر موسسه آموزشی و پژوهشی امام خمینی (ره)، سال ۱۳۸۷.
۱۷- شیخ حر عاملی، **وسائل الشیعه الی تحصیل مسائل الشریعه**، چاپ آل البیت الاحیاء التراث قم، سال ۱۴۱۴ قمری، ج۱۱.
۱۸- صابری یزدی علیرضا، **الحکم‌الزاهره**، نشر سازمان تبلیغات اسلامی، سال ۱۳۷۵.
۱۹- طباطبایی سیدمحمّدحسین، **تفسیر المیزان**، ج۱۷.
۲۰- طباطبائی منوچهر، **آزادی‌های عمومی و حقوق بشر**، تهران: انتشارات دانشگاه تهران، سال ۱۳۷۵، صفحه ۵۰.
۲۱- علوی‌فر سیدناصر، **راهکارهای تامین و توسعه امنیت**، تهران: نشر جهانگیر، سال ۱۳۸۵، صفحات ۲۰ الی ۲۲.
۲۲- عبدالله‌خانی علی، **رویکردها و طرح‌های آمریکایی دربارهٔ ایران**،تهران: موسسه فرهنگی مطالعاتی و تحقیقاتی بین‌المللی ابرار معاصر، سال ۱۳۸۶، صفحه ۲۱.
۲۳- عروسی حویزی عبد علی بن جمعه، **تفسیر نور الثقلین**، جلد ۵، نشر موسسه مطبوعاتی اسماعیلیان، سال ۱۴۵قمری.
۲۴- فخررازی، **تفسیر کبیر**، جزء ۳۰، ص ۱۷.
۲۵- فیض‌کاشانی، **الوافی**، ۱۴۰۶ ق، ج ۲۶، صفحه ۱۴۲.
۲۶- فلسفی محمد تقی، **گفتار فلسفی**، نشر فرهنگ اسلامی، سال ۱۳۹۴، ج ۳.
۲۷- قرآن مجید
۲۸-قمی شیخ‌عباس(الف)، **مفاتیح‌الجنان**، دعای کمیل
۲۹- قمی شیخ‌عباس(ب)، **مفاتیح‌الجنان**، دعای ابوحمزه ثمالی.
۳۰- قضاعی محمدبن سلامه، **شرح شهاب‌الاخبار**، انتشارات علمی و فرهنگی وزارت فرهنگ و آموزش عالی، سال ۱۳۶۱.
۳۱- کلینی محمّدابن‌یعقوب، **فروع کافی**، نشر قدس، سال ۱۳۹۳، ج۵.

۳۲- مجلسی محمد باقر، **بحارالانوار**، چاپ الاسلامیه، سال ۱۳۹۳، جلد ۴۴.
۳۳- موسوی‌همدانی، **ترجمهٔ المیزان**، ج۳، ص ۲۰۶.
۳۴- مکارم‌شیرازی ناصر، **تفسیر نمونه**، ج۲۴.
۳۵- محمّدی‌ری‌شهری محمّد، **منتخب میزان‌الحکمه**، سال ۱۳۹۲، ص ۲۲، ح ۶۶۱.
۳۶- محمدی منوچهر، خبرگزاری فارس، تاریخ۹۵/۰۳/۲۹
۳۷- مسعودی علی‌بن‌حسین، **مروج‌الذهب و معادن‌الجوهر**، چاپ باربیه دمینار و پاوه دکورتل، پاریس ۱۸۶۱-۱۸۷۷، ج ۲.
۳۸- محمدی منوچهر، **مدیریت بحران در جمهوری‌اسلامی** ایران؛ بحران های سیاسی- اجتماعی، نشر معارف، سال۱۳۹۴.
۳۹- مطهری هادی و عمادی ابوالفضل، **دیواره آتش XP** ، فصلنامه تخصصی ثبت برتر – شماره ۳، سال ۱۳۸۸.
۴۰- محمدی ری شهری محمد، **میزان‌الحکمه**، چاپ ونشر دارالحدیث، سال ۱۳۹۲، ج ۳.
۴۱- مجیدی‌نظامی سیدمهدی، **بایسته‌های امنیت اطلاعات در شبکه‌ها و سایت‌های اطلاع‌رسانی**، سایت مرکز اطلاعات و مدارک اسلامی،۲۴ خرداد ۱۳۹۱.
۴۲- ملکیان احسان، **نفوذگری در شبکه و روش‌های مقابله**، چاپ ششم، تهران: نشر نص، ۱۱ آذر، سال ۱۳۹۱.
۴۳- موسسه فرهنگی فاطمی، **سیستم‌عامل دو (رشته‌های فنی و حرفه‌ای)**، صفحه ۱۵۳- سال ۱۳۸۶- تهران: انتشارات موسسه فرهنگی فاطمی، سال ۱۳۸۶.
۴۴- نجفی محمدحسن، **جواهرالکلام** فی شرح شرایع الاسلام، ناشر دار الکتب الاسلامیه، سال ۱۳۹۶، ج۲۱.
۴۵-**نهج‌البلاغه**، ترجمهٔ شهیدی، نشر علمی و فرهنگی، سال ۱۳۹۲.
۴۶- ویکی پدیا، **دانش‌نامه آزاد**

سایت‌ها

۱- http://wiki-network.ir
۲- http://www.gooyait.com,۱۳۹۳ چهارشنبه , ۲۴ اردیبهشت
۳- http://vista.ir سایت شبکه فن‌آوری اطلاعات ایران
۴- http://fa.wikipedia.org
۵- http://www.ircert.com
۶- http://www.loghatnameh.com
۷- https:// rasekhoon.net موسسه فرهنگی و هنری نور راسخون
۸- www.iranictnews.ir
۹- www.ito.gov.ir منبع سایت فناوری اطلاعات ایران

منابع انگلیسی

۱- Andrew Breakwell, The human firewall creating a security, Sai global, ۲۰۰۷
۲- “Comp TIA Security”, ™ Study Guide ,Third Edition, Mike Pastore, Emmett Dulaney, p. ۱۳-۱۴
۳- Charles jenninge, Building human firewalls, ceo,swan island, network,inc. , ۲۰۱۳
۴- Dawn Kawamoto , Human Firewall gets new owner, Staff Writer, CNET News, ۲۰۰۴
۵- Evans, Nathaniel Joseph, "Information technology social engineering: an academic definition and study of social engineering -analyzing the human firewall". Graduate Theses and Dissertations. (۲۰۰۹)
۶- Jamison W.Scheeres; Establishing the human firewall: reducing an individual’s vulnerailiy to social engineering attacks; master thesis in Department of the air force; air university, ohio, ۲۰۰۸.
۷- Kleiss .W, in H.J. Kellner, ed., Uras ¤ tu , ein wiederentdeckter Rivale Assyriens , Munich ۱۹۷۶, ۲۸f .
۸- Spuler .B, Iran in fruh-islamischer Zeit , Wiesbaden ۱۹۵۲, .
۹- Strphen ndonga kariuki, The human firewall creating a security aware workforce, harmony solutions limited,۲۰۱۱.