خودآموز امنیت و حفاظت برای مدافعان حقوق بشر

انریکه ایگورن
و دفتر اروپایی سپاهیان صلح جهانی

فرانت لاین

بنیاد بین المللی
برای حفاظت از مدافعین حقوق بشر

سپاهیان
صلح جهانی

Peace Brigades International

FRONT LINE
Defenders of human rights defenders

خودآموز امنیت و حفاظت برای مدافعان حقوق بشر

تحقیق و نگارش توسط انریکه یگورن
سپاهیان صلح جهانی -دفتر اروپایی

منتشر شده توسط فرانت لاین
بنیاد بین المللی برای حفاظت
از مدافعین حقوق بشر

نمایه فصول

مقدمه

خودآموز امنیت و حفاظت برای مدافعان حقوق بشر

تهدیدات و مخاطراتی که متوجه مدافعان حقوق بشر می‌شود

قوانین بین‌المللی تضمین کننده حقوق بشر هستند، با این وجود فعالیت برای حصول اطمینان از رعایت این موازین و نیز بررسی پرونده افرادی که حقوق آنها نقض شده است متضمن مخاطرات متعددی است که مدافعان حقوق بشر را در سرتاسر جهان تهدید می کنند. مدافعان حقوق بشر اغلب تنها نیرویی هستند که میان مردم عادی و قدرت مطلقه و مهار نشده حکومت قرار گرفته‌اند. حضور و وجود این افراد برای توسعه فرآیندها و نهادهای دموکراتیک، پایان بخشیدن به فرار نقض کنندگان و متجاوزان حقوق بدیهی افراد جامعه از مجازات و در نهایت ارتقا حقوق بشر حیاتی است.

مدافعان حقوق بشر غالبا با آزار و اذیت،دستگیری و بازداشت، شکنجه و افترا، تعلیق از شغل،عدم آزادی در فعالیت و عدم شناسایی قانون انجمن‌ها و نهادی خود مواجه می‌شوند. در برخی از کشورها این افراد حتی "ناپدید" و یا کشته می‌شوند.

در چند سال اخیر، سطح آگاهی عمومی نسبت به خطرات عظیمی که مدافعان حقوق بشر در چارچوب فعالیت‌های خود با آن روبه‌رو می‌شوند، افزایش یافته است. شناسایی این تهدیدات و خطرات هنگامی که مدافعان در شرایط نامساعد مشغول به کار هستند -برای مثال در کشوری که مطابق قوانین آن برای افرادی که برخی فعالیت‌های خاص مرتبط با حقوق بشر را پیگیری می کنند، مجازات‌هایی تعیین شده است- به سادگی قابل شناسایی هستند. مدافعان حقوق بشر همچنین زمانی که از یک سو طبق قوانین، فعالیت‌های حقوق بشر مجاز شمرده نمی‌شود و از سوی دیگر افرادی که مدافعان حقوق بشر را در مورد تهدید و یا حتی تهاجم قرار می‌دهند از تعقیب مصون می‌مانند، نیز چنین مخاطراتی را متوجه خود می‌بینند. در میان درگیری‌های مسلحانه، این مخاطرات باز هم افزایش می‌یابد.

گذشته از برخی شرایط بحرانی خاص که طی آن جان مدافع حقوق بشر بستگی به عملکرد سربازی مستقر در ایست بازرسی پیدا می کند، خشونت اعمال شده علیه مدافعیت را نمی‌توان تصادفی و بدون هدف تلقی کرد. در اغلب موارد حملات خشت واکنشی کاملا برنامه‌ریزی شده و آگاهانه در قبال فعالیت‌های مدافعین بوده و با هدف سیاسی و نظامی معینی در ارتباط می‌باشند.

مجموعه این چالش‌ها باعث می‌شود تا اجرای یک سری استراتژی‌های امنیتی جامع و پویا از سوی مدافعین حقوق بشر در جریان فعالیت‌های روزمره، الزامی باشد. در چنین شرایطی دیگر اکتفا کردن به چند توصیه خیرخواهانه و پیشنهاد اینکه آنها "مراقب خود باشند" قطعا معقول نیست. بهینه‌سازی مدیریت امنیت در این جا کلید اصلی است. خودآموز حاضر هر چند دارای راهکارهای کاملا آماده شده‌ای که بتوان آنها در هر وضعیت و شرایطی اجرا کرد، نیست ولی با این وجود مجموعه‌ای از استراتژی‌ها را با هدف بهبود مدیریت امنیت مدافعین مطرح و بررسی می کند.

موثرترین درس‌های امنیتی در عمل حاصل تجارب خود مدافعین هستند؛ تاکتیک‌ها و استراتژی‌هایی که آنها در گذر زمان برای حفظ خود

و محیط کارشان در برابر تهدیدات ابداع کرده‌اند. با در نظر داشتن این موضوع، بدیهی است که باید خود آموز حاضر را عملا فرآیندی در حال تکمیل تلقی کرد که با جمع‌آوری و گردآوران تجارب و آموخته‌های سایر فعالان و مدافعان حقوق بشر روزآمد شده و امکان تطبیق راهکارهای ارائه شده در آن با دامنه گسترده‌تری از شرایط و وضعیت‌ها وجود خواهد داشت.

بدیهی است که در این میان می‌توان درس‌های بسیاری از سازمان‌های غیردولتی فعال در عرصه حقوق بشر و مسائل انساندوستانه که در سال‌های اخیر هر یک قواعد و راهکارهای خاص خود را برای تامین امنیت کارکنانشان تدوین کرده‌اند، آموخت.

مهمترین خطری که متوجه مدافعین حقوق بشر می‌شود- و باید به آن توجه کافی داشت به این واقعیت تلخ برمی‌گردد که تهدیدات غالبا به صورت حملاتی واقعی، عملی می‌شوند. مهاجمان در این میان با برخورداری از انگیزه، ابزار و نیز اطمینان از مصونیت خود، به راحتی تهدیداتشان را عملی می‌کنند. در چنین شرایطی بهترین وسیله برای حمایت از مدافعین، اقدام سیاسی برای حل یک مساله بزرگ است: ملزم ساختن دولت‌ها و جامعه مدنی برای اعمال فشار و یا اقدام علیه افرادی که هر روز مدافعین حقوق بشر را مورد آزار قرار داده، تهدید کرده و یا حتی به قتل می‌رسانند. توصیه‌های ارائه شده در این خودآموز به هیچ وجه نباید جایگزین و یا نافی مسوولیت دولت و یا دولت‌ها برای حمایت از مدافعان حقوق بشر تلقی شود.

بدیهی است که مدافعین نیز در این میان می‌توانند با به کار بستن چند دستورالعمل آزمایش پس داده، امنیت خود را به نحو قابل ملاحظه‌ای افزایش دهند.

این خودآموز تلاش فروتنانه‌ای است در راستای تحقق هدفی که سازمان‌های متعددی در آن مشترک هستند؛ حفاظت از فعالیت‌های غیرقابل ارزشگذاری مدافعین حقوق بشر. مدافعان حقوق بشری که در "خط مقدم" حضور دارند، موضوع اصلی این خودآموز هستند.

خودآموز

هدف اصلی این خودآموز فراهم آوردن و یا افزودن درک مدافعین حقوق بشر از امنیت و آشناسازی آنها با برخی ابزارهایی است که ممکن است در فرآیند تامین امنیت و حفاظت کاربرد داشته باشند. امیدی می‌رود که این خودآموز به ترویج آموزش‌های امنیتی و حفاظتی یاری رسانده و به مدافعین کمک کند که امکان شناسایی و برآورد میزان و نوع تهدیدات و تعریف قواعد و راهکارهای امنیتی، متناسب با شرایط خاص خود، را دارا شوند.

خودآموز حاضر حاصل پروژه‌ای طولانی مدت در مورد حفاظت میدانی مدافعان حقوق بشر است که از سوی سپاهیان صلح جهانی طراحی و اجرا شده است. در این میان فرصت یافته‌ایم که علاوه بر دسترسی به نتایج این پروژه، از تجارب و دانش صدها تن از مدافعین حقوق بشر در این حوزه نیز بهره بگیریم. این کار از طریق برگزاری کارگاه‌ها، جلسات و گردهمایی‌ها و مباحثات متعدد در حوزه مسائل امنیتی امکان‌پذیر شد. بخش غالب محتویات خودآموز بیش از این به صورت عملی- یا در شرایط واقعی و برای حفاظت از جان مدافعین و یا در جریان کارگاه‌های آموزشی و یا حضور مدافعین- اجرا شده‌اند. خودآموز حاضر بدین ترتیب ثمره و ماحصل تمامی این تجارب و تبادل دانش‌هاست و بدیهی است که باید قدردان تمامی مدافعین حقوق بشر باشیم که با مشارکت خود امکان تهیه این مجموعه را فراهم ساخته‌اند.

امنیت و حفاظت عرصه‌های دشواری هستند. این دو مفهوم نه تنها حول دانشی کاملا منسجم شکل می‌گیرند بلکه در عمل از رویکردهای فردی و رفتارهای سازمانی نیز تاثیر می‌پذیرند. یکی از کلیدی‌ترین پیام‌هایی که این خودآموز قصد رساندن آن به گوش مخاطبان را دارد این است که علی‌رغم فشار کاری، برنامه‌های فشرده فعالیت، تنش‌های فزاینده و شرایط هراس آفرینی که مدافعین و سازمان‌هایشان در آن به سر می‌برند، باز هم باید زمان، مکان و انرژی لازم به موضوع امنیت اختصاص یابد. این وضعیت نیازمند ارتقای سطح دانش عمومی و حرکت به سوی ایجاد فرهنگی سازمانی است که در آن امنیت تبدیل به امری ذاتی شده باشد.

آگاهی کافی از سناریوی درگیری و درک منطق سیاسی حاکم بر منطقه، در مدیریت امنیت مدافعان نقشی کلیدی ایفا می‌کنند. این خودآموز

شامل چارچوبی کلی و نیز دیدگاهی گام به گام برای مدیریت امنیت است. در مجموعه حاضر همچنین ایده‌ها و نظرات مختلف در مورد مفاهیمی بنیادین چون مخاطره، آسیب‌پذیری، تهدید و... منعکس شده و توصیه‌هایی چند در راستای بهبود و ارتقای امنیت مدافعین در جریان فعالیت‌های روزمره‌شان ارائه می‌شود. امیدواریم که موضوعات پرداخته شده این امکان را برای سازمان‌های غیردولتی و مدافعین فراهم‌آورند که با آمادگی بیشتری به‌مواجهه با چالش‌های فزاینده‌امنیتی، که‌هر روز بیش‌از پیش‌فعالان‌حقوق‌بشر را تهدید می‌کند، بپردازند. با در نظر گرفتن موارد فوق تنها یادآوری و تاکید بر این نکته باقی می‌ماند که مدافعین حقوق بشر سلامت و حتی حیات خود را به مخاطره می‌اندازند و تهدیداتی که متوجه آنها می‌شود بسیار جدی است. در این میان گاهی تنها راه نجات اختفاء و سپس فرار کردن است. به شدت و با کمال صراحت تاکید می‌کنیم که روش‌ها و توصیه‌های ارائه شده در این خودآموز را به هیچ وجه نباید پاسخگوی تمامی تهدیداتی دانست که متوجه مدافعین می‌شود. این خودآموز هر چند با تلاش فراوان و با اطمینان قلبی به صحت و کارآمدی مطالب آن نگاشته شده است، اما متاسفانه به هیچ وجه نمی‌توان مفاد آن را تضمین کننده موفقیت تلقی کرد.

فراخوان برای بهبود این خودآموز

این خودآموز را می‌توان فرآیندی در نظر گرفت که پیوسته در جریان است و باید در گذر زمان توسعه و بهبود یافته و تکمیل گردد. بدین ترتیب بدیهی است که بازخورد نظرات شما، به عنوان مدافع حقوق بشر – در مورد هر بخشی از این خودآموز – از ارزشی غیرقابل محاسبه برخوردار است. لذا خواهشمندیم نظرات و آرای خود را – به ویژه در مورد تجربه شما از به کارگیری عملی این خودآموز – در اختیار ما قرار دهید. تنها با کمک شماست که ما می‌توانیم این خودآموز را تبدیل به ابزاری کارآمد و موثر برای مدافعین حقوق بشر در سرتاسر جهان کنیم.

با هر یک از صندوق‌های پست الکترونیکی زیر می‌توانید تماس بگیرید:

Protectionmanual@frontlinedefenders.org

Pbibeo@biz.tiscali.be

و یا به نشانی‌های پستی زیر با مکاتبه کنید:

- **دفتر اروپا - سپاهیان صلح جهانی**

38, Rue Saint - Christophe, 1000 Bruxelles (Belgium)

Tel/Fax +32(0)2 511 14 98

- **فرانت لاین**

16 Idrone lane , Off Bath Place , Blackrock , County Dublin , Ireland

Tel: +353 1212 3750 Fax: +353 1212 1001

مقدمه‌ای کوتاه بر مدافعین حقوق بشر

"مدافع حقوق بشر" عبارتی است که برای توصیف افرادی که به صورت فردی و یا با همکاری دیگران اقدام و یا فعالیتی را برای ارتقای سطح و یا حفاظت از حقوق بشر انجام می‌دهند، به کار گرفته می‌شود.

مدافعین حقوق بشر عموما با توجه به فعالیت خود شناسایی می‌شوند. این واژه هم در واقع توصیف مناسبی از فعالیت اصلی آنان- دفاع از حقوق بشر- را در خود نهفته دارد.

در سال ۱۹۹۸، مجمع عمومی سازمان ملل "بیانیه حقوق و مسوولیت افراد، گروه‌ها و نهادهای جامعه‌ای، ارتقا و حفاظت از حقوق بشر و آزادی های بنیادین مورد وثوق جامعه جهانی" را تصویب کرد (این بیانیه از این پس بیانیه سازمان ملل در مورد مدافعین حقوق بشر خوانده می‌شود). این قطعنامه که ۵۰ سال پس از تصویب بیانیه جهانی حقوق بشر و ۲۰ سال پس از مذاکرات متمادی در مورد پیش نویس بیانیه‌ای در مورد مدافعین حقوق بشر، تصویب شد در حقیقت شناسایی واقعیتی است که همواره وجود داشته است. سازمان ملل در واقع پس از مدت‌ها حاضر به تایید واقعیت حضور هزاران فردی شد که برای ارتقا و حفاظت از حقوق انسان در سرتاسر جهان تلاش می کنند. بیانیه صادره به هر حال بیانیه‌ای جامع است که تنوع و تکثر افرادی که در فرآیند ارتقای سطح و حفاظت از حقوق بشر درگیر هستند، به رسمیت می‌شناسد.

نماینده ویژه دبیر کل سازمان ملل در امور مدافعین حقوق شر به موجب این بیانیه موظف شده است تا به جستجو، دریافت، بررسی و در نهایت پاسخ‌دهی به اطلاعات مربوط به شرایط و حقوق هر فردی که به صورت مستقل و یا مرتبط با دیگران به تلاش برای ارتقای سطح و یا محافظت از حقوق بشر و آزادی‌های بنیادین مشغول است، بپردازد.

فرانت لاین "مدافع حقوق بشر" را شخصی تلقی می کند که به گونه‌ای غیر خشونت‌آمیز در جهت تحقق یک یا همه حقوق مندرج در بیانیه جهانی حقوق بشر می کوشد. فرانت لاین خود می کوشد تا بیانیه سازمان ملل در مورد مدافعین حقوق بشر را هم تا حدی اصلاح کند (اصلاحات و متن بیانیه پیشنهادی فرانت لاین را در بخش پایانی مطالعه می کنید).

چه کسی مسوول حفاظت از مدافعین حقوق بشر است؟

بیانیه مدافعین حقوق بشر تاکید دارد که دولت در وهله نخست مسوول حفاظت از مدافعین حقوق بشر است. در این بیانیه "کار ارزشمند افراد، گروه‌ها و اتحادیه‌های مرتبط و تشریک مساعی آنان برای حذف موثر تمامی موارد نقض حقوق بشر و آزادی‌های بنیادین" و نیز "رابطه صلح و امنیت بین‌المللی و برخورداری جوامع از حوق بشر و آزادی‌های بنیادین" مورد تاکید قرار گرفته است.

با این وجود به استناد گفته‌های هینا جیلانی، نماینده ویژه دبیر کل سازمان ملل در امور مدافعان حقوق بشر "افشای موارد نقض حقوق بشر و تلاش برای تعقیب عاملین آنها، تا حد بسیار زیادی بستگی به درجه و میزان امنیتی است که مدافعین حقوق بشر از آن برخوردار هستند.۱ با نگاهی به هر یک از گزارشات مربوط به مدافعین حقوق بشر در سرتاسر جهان، با انبوهی از روایات مربوط به شکنجه، ناپدید شدن افراد، قتل، تهدید، دزدی و سرقت، ورود غیرقانونی به دفاتر کار، افترا، بازداشت غیرقانونی و در نهایت قرار گرفتن افراد در معرض بازجویی و استراق سمع و سایر موارد جاسوسی مشابه روبه‌رو می‌شویم یا متاسفانه تمامی این موارد برای مدافعان حقوق بشر به کرات روی می‌دهند و دیگر نمی‌توان آنها را استثنائاتی که در حین کار ممکن است با آنها مواجه شوند قلمداد کنیم.

برای کسب اطلاعات بیشتر در مورد مدافعین حقوق بشر به تارنماهای زیر مراجعه کنید

www.unhcr.ch/defender/about1.htm

کمیسیونر عالی سازمان ملل در مورد حقوق بشر

www.frontlinedefenders.org

فرانت لاین، بنیادی جهانی برای مدافعین حقوق بشر

www.peacebrigades.org/beo.html.org

دفتر اروپایی سپاهیان صلح جهانی در بروکسل

www.fidh.org www.omct.org

ناظرین حفاظت از مدافعین حقوق بشر، زیرمجموعه فدراسیون جهانی حقوق بشر و سازمان جهانی اقدام علیه شکنجه

http://web.amnesty.org/pages/hrd-index-eng www.amnesty.org

عفو بین‌الملل

www.ishr.ch

دفتر خدمات جهانی برای حقوق بشر در ژنو

www.humanrightsfirst.org

سازمان "اول حقوق بشر"

www.urgentactionfund.org

بنیاد اقدام عاجل برای حمایت از حقوق انسانی زنان

برای آموختن و کسب اطلاعات بیشتر از ابزارهای قانونی موجود و بیانیه سازمان ملل در مورد مدافعین حقوق بشر به تارنمای زیر مراجعه کنید.

www.unhcr.ch.org

تارنمای متعلق به کمیسیونر عالی سازمان ملل در حقوق بشر

www.frontlinedefenders.org/manual/en/index.htm

فرانت لاین ایرلند، خودآموز ابزارهای جهانی برای مدافعین حقوق بشر.

توصیه می‌شود از صفحه کارآمد و ارزشمند "پیوندها" نیز در این نشانی استفاده شود.

http://www.frontlinedefenders.org/links/

www.ishr.ch/index.htm

خدمت جهانی برای حقوق بشر، ژنو. در این مکان لیستی کامل از ابزارهای منطقه‌ای و جهانی برای حفاظت از مدافعین حقوق بشر یافت می‌شود.

فصل اول

اتخاذ تصمیمات آگاهانه درباره امنیت و محافظت

هدف:

آگاهی از اهمیت تحلیل محیط کار بنا به دلایل امنیتی.

آشنایی با روش‌های قضاوت برای بررسی شرایط و تحلیل وضعیت اشخاص دخیل.

محیط های کاری مدافعین حقوق بشر

مدافعین حقوق بشر معمولا در محیط‌های پیچیده‌ای فعالیت می کنند. ویژگی این محیط‌ها به تعدد فعالان و نیز تاثیرپذیری عمیق آنها از فرآیند تصمیم‌گیرهای سیاسی بازمی گردد. در این میان انبوه حوادثی که عموما به صورت همزمان نیز روی می‌دهند و هر یک بر دیگری تاثیر خاص خود را دارند نیز بر پیچیدگی شرایط می افزاید. در این میان دینامیک هر فعال یا شخص دخیل در این سناریو می تواند نقشی قایل توجه در رابطه میان آن فعال با سایرین داشته باشد. مدافعین حقوق بشر بدین ترتیب نیازمند اطلاعاتی هستند که تنها به موضوعاتی که مستقیما با فعالیت آنها در ارتباطند، محدود نمی‌شود، بلکه حوزه‌هایی چون موقعیت و موضع سایر فعالان کلیدی و حتی افراد دخیل را هم دربر می گیرد.

به عنوان یک تمرین ساده می توانید ترتیب یک جلسه "توفان نفری" گروهی را بدهید و سعی کنید تا با استفاده از انبوه ایده‌های ارائه شده لیستی از تمامی فعالان اقتصادی، سیاسی و اجتماعی که می توانند بر وضعیت امنیتی فعلی شما تاثیرگذار باشند را شناسایی کنید.

تحلیل محیط کاری شما

درک و شناسایی محیط فعالیت و شرایط آن تا حد امکان و کسب بیشترین اطلاعات ممکن در این عرصه، از اهمیت بسزایی برخوردار است. تحلیل مطلوب از شرایط محیط کار به شما این امکان را می‌دهد تا تصمیماتی آگاهانه در مورد قواعد و راهکارهای امنیتی مناسبی که باید اجرا شوند، اتخاذ کنید. از سوی دیگر پیش‌بینی سناریوهای احتمالی آتی نیز از اهمیت به سزایی برخوردار است چرا که به شما این امکان را می‌دهد که در صورت امکان اقدامات پیشگیرانه لازم را معمول دارید.

به هر حال، باید در نظر داشت که تحلیل ساده‌انگارانه محیط کاری کافی نیست. شما نیازمند بررسی موضوعاتی چون نحوه بر هم کنش حوادث و تاثیر آنها بر شرایط و حتی برآورد نحوه تعامل فعالان با یکدیگر هستید. محاسبه و لحاظ کردن سناریوهای کاری نیز از اهمیت به‌سزایی برخوردار است. شما می توانید تحلیل را ابتدا در سطح کلان با مطالعه منطقه و یا کشور آغاز کنید و سپس نحوه کارکرد

این دینامیک‌های کلان را در منطقه خاص که برای فعالیت خود انتخاب کرده‌اید، بررسی نمایید. به عبارت دیگر از دینامیک‌های کلان،در نهایت باید به دینامیک‌های خود برسید. برای مثال فرض کنید که شما تحلیلی از کارکرد شبه‌نظامیان در سطح کلان (کشوری) در دست دارید، اما همین شبه‌نظامیان ممکن است در منطقه‌ای خاص رفتار و کارکردی متفاوت از انتظار شما را ارائه دهند. بدیهی است که شما باید از چنین ویژگی‌های محلی و منطقه‌ای آگاهی داشته باشید. اجتناب از داشتن نگاهی ثابت در مورد سناریوی کار، امری حیاتی است چرا که شرایط دائما در حال تغییر و تکوین هستند. بدین ترتیب بدیهی است که باید سناروییهای کار را دائما مورد بازبینی قرار داد.
"**طرح پرسش**"، "**تحلیل میدان نیرو**" و "**تحلیل عاملان دخیل**" سه روش موثر برای تحلیل شرایط محیط کار هستند.

طرح پرسش

شما با طرح پرسش‌های صحیح قطعا بهتر می‌توانید محیط کار و فعالیت خود را درک کنید. طرح پرسش روشی موثر و کارآمد برای تولید مباحث و محورهای بحث در یک گروه کوچک است. البته بدیهی است که این روش تنها هنگامی نتیجه‌بخش خواهد بود که پرسش‌ها به‌گونه‌ای منسجم و هدفمند و در راستای رسیدن به راه‌حلی مطلوب، طرح شده باشند.
برای مثال شرایطی را در نظر بگیرید که مقامات محلی با مزاحمت‌های متعدد خود تبدیل به معضلی جدی شده‌اند. اگر پرسش‌خود را این‌گونه طرح کنید که "برای کاهش این مزاحمت‌ها چه باید کرد؟" عملا وقت و توان خود را صرف یافتن علاجی برای نمود بیرونی یک معضل کرده‌اید. در واقع شما تنها به دنبال تسکین درد و نه درمان بیماری هستید.
اما اجازه بدهید این پرسش را به‌گونه‌ای باز تعریف کنیم که امکان رسیدن به راه‌حلی واقعی وجود داشته باشد. برای مثال بهتر است بپرسید "آیا محیط اجتماعی- سیاسی ما به قدر کافی برای تعقیب فعالیت‌هایمان امن است؟". بدیهی است که پاسخ این پرسش به دو مورد "بلی" و "خیر" محدود می‌شود. اگر پاسخ مثبت باشد، آنگاه باید سوالی دیگر را مطرح کنید که به شما اجازه مشخص کردن دقیق معضل و درک مناسب مسائل حیاتی لازم برای تامین امنیت کاری را بدهد. اما از سوی دیگر اگر پس از بررسی و ملاحظه مناسب و دقیق تمامی فعالیت‌های ممکن، طرح‌ها و منابع و همچنین در نظر گرفتن قوانین، مذاکرات و مقایسه شرایط خود با شرایط سایر مدافعین حقوق بشر در منطقه، پاسخ شما به این پرسش منفی بود، این پاسخ منفی به نوبه خود می‌تواند به هدایت شما به سمت یافتن راه‌حلی برای معضل امنیتی موجود منتهی شود.

به کارگیری روش طرح سوال

- به دنبال پرسش‌هایی بگرید که به شما امکان شناسایی و رجوع دقیق به موضوع و درک مسائل حیاتی را بدهد.
- پرسش‌ها را به گونه‌ای هدفمند و در راستای یافتن راه‌حل طراحی کنید.
- این فرآیند را به دفعات لازم تکرار کنید (به صورت مباحثه و گفت‌وگو).

برخی پرسش‌های موثر و کارآمد برای طرح

- مهمترین مسائل منطقه در عرصه‌های اقتصادی، سیاسی و اجتماعی چیست؟
- عاملان دخیل کلیدی در ارتباط با این مسائل کلیدی چه کسانی هستند؟
- چگونه ممکن است فعالیت ما تاثیر مثبت و یا منفی بر منافع این عاملان دخیل کلیدی داشته باشد؟
- واکنش ما در صورتی که هدف تهاجم هر یک از این عاملان قرار بگیریم چه خواهد بود؟
- آیا محیط پیرامونی ما – از لحاظ سیاسی و اجتماعی- به قدر کافی برای فعالیت‌های ما امن است؟
- واکنش مقامات محلی و یا ملی در قبال فعالیت‌های پیشین مدافعین حقوق بشر در این عرصه چه بوده است؟

- واکنش عاملان دخیل به اقدامات مشابه مدافعین حقوق بشر و یا سایرین در این عرصه‌ها چه بوده است؟
- واکنش رسانه‌ها و جامعه در شرایط مشابه چه بوده است؟
- و موارد مشابه و متعدد دیگر

تحلیل میدان نیرو

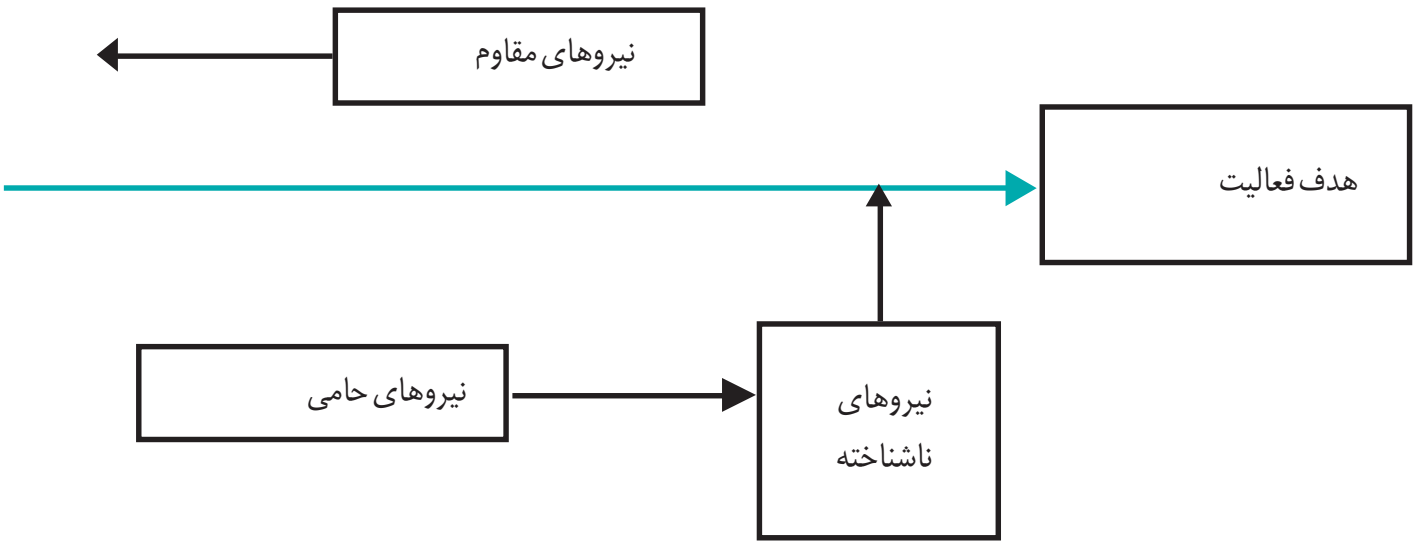
تحلیل میدان نیرو تکنیکی است که به شما اجازه می‌دهد به‌وضوح تاثیر نیروهای مختلف بر تسهیل و یا ممانعت از تحقق اهداف فعالیت خود را مشاهد کنید. در این روش نیروهای "حامی"، "مخالف" و فعالیت نمایش داده شده و فرض می‌شود که مشکلات امنیتی در زیرمجموعه نیروهای مخالف یا مقاوم قرار گیرند. بدیهی است که شما برای غلبه بر این مشکلات امنیتی از برخی نیروهای حامی هم بهره بگیرد. این روش می‌تواند توسط یک فرد اجرا شود و ماحصل آن مورد تحلیل قرار گیرد، هر چند شاید کار جمعی گروهی متکثر با هدفی واضح و تعیین شده و راهکارهای معین برای تحقق آن، نتیجه‌ای به مراتب بهتر را به ارمغان آورد.

برای شروع یک پیکان افقی بکشید که به سمت چارچوبه‌ای متوجه شده است. خلاصه‌ای از هدف فعالیت خود را در چارچوبه بنویسید. نگارش این خلاصه هدف به شما کمک می‌کند تا با وضوح بیشتری نیروهای حامی و مقاوم را شناسایی کنید.

بر بالای پیکان افقی، چارچوبه دیگری بکشید. در این چارچوبه لیستی از تمام نیروهای مقاوم و یا مخالفی که بر سر تحقق اهداف شما مشکل ایجاد می‌کنند را بنویسید.

در زیر پیکان افقی چارچوبه دیگری بکشید و این بار لیستی از نیروهای خود را در آن بنگارید. برای نیروهایی که هنوز نمی‌دانید حامی هستند یا مقاوم، چارچوبه‌ای دیگر رسم کرده و آنها را در درون آن ذکر کنید.

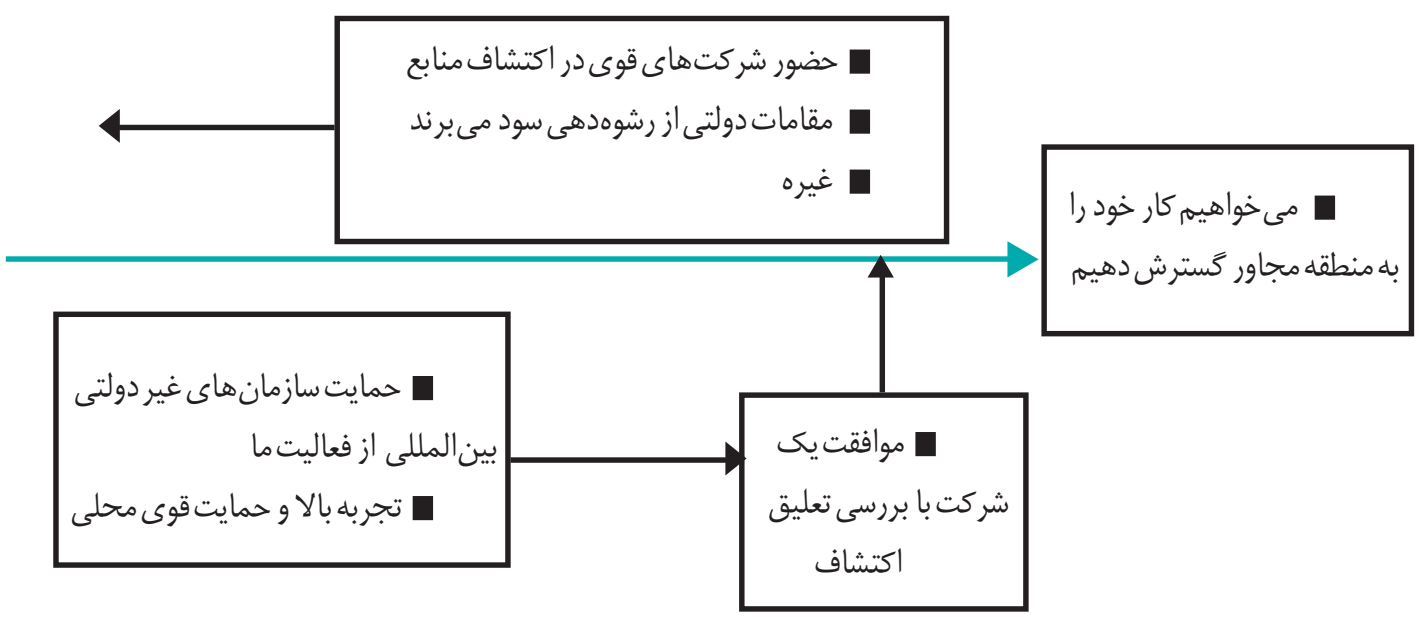
ترسیمه ۱ - تحلیل میدان نیرو برای بررسی محیط کاری



پس از تکمیل چارت زمان بررسی نتایج رسیده است. تحلیل میدان نیرو به شما کمک می‌کند تا به صورتی واضح نیروهایی را که شما با آن سروکار دارید را مجسم‌سازی کند. هدف اصلی یافتن راهی برای کاهش یا تقلیل و حذف مخاطراتی است که توسط نیروهای مقاوم آفریده می‌شوند. امر می‌تواند با بهره‌گیری از توان بالقوه نیروهای حامی موجود صورت گیرد. در مورد نیروهای ناشناخته هم یا می‌توانید فرض را بر حامی بودن آنها گذاشته و یا به صورت مستمر بر آنها نظارت داشته وسعی کنید تا کوچکترین علائمی را که می‌تواند در تعیین ماهیت آنها - حامی و یا مقاوم بودن نیروها - کمک کنند، شناسایی نمایید.

برای مثال:

تصور کنید شما به سازمانی تعلق دارید که به دفاع از حقوق بومیان نسبت به منابع طبیعی موجود در اراضی‌شان می‌پردازد. در این موارد معمولا چندین بازیگر و فعال دخیل حضور دارند که هر یک به نحوی خود را در اکتشاف و استخراج این منابع طبیعی صاحب حق می‌دانند. این امر در نهایت به شکل گیری نزاعی میان این افراد منتهی شده است. شما اکنون می‌خواهید دامنه فعالیت خود را به اراضی مجاور منطقه گسترش دهید. این منطقه نیز دارای معضلات مشابهی است.



تحلیل فعالان (یا عوامل دخیل)

تحلیل فعالان یا عوامل دخیل راهی مهم برای افزایش اطلاعات موجود و حیاتی در هنگام اتخاذ تصمیمات لازم برای حفاظت است. در این روش شناسایی و توصیف فعالان مختلف (یا عوامل دخیل) تکمیل شده و رابطه آنها براساس ویژگی‌ها و منافع آنها تحلیل می‌شود. این تحلیل و توصیف باید پیرامون یک موضوع حفاظتی معین صورت بگیرد.

عاملان دخیل در حفاظت به هر شخص، گروه و یا نهادی اطلاق می‌شوند که دارای منافع و یا سهمی در نتایج سیاسی حاصله در محدوده مورد حفاظت باشند.

تحلیل عوامل دخیل برای درک موارد زیر الزامی است:

- چه کسی را می‌توان عاملی دخیل تلقی کرده و تحت چه شرایطی "دخالت" آنها اهمیت می‌یابد
- رابطه میان عوامل دخیل در حفاظت، مشخصه‌ها و منافع آنان
- نحوه تاثیر فعالیت‌ها حفاظتی بر موارد ذکر شده در فوق
- تمایل هر عامل دخیل به مشارکت در فعالیت‌های حفاظتی مزبور

عوامل دخیل در حفاظت را می‌توان به صورت زیر گروه‌بندی کرد:

عوامل دخیل اولیه: در عرصه محافظت این عوامل را می‌توان **خود مدافعین و آنهایی که همراه و یا در خدمت این افراد به فعالیت مشغولند.** تمامی این افراد در حفاظت از "خود" نقش به‌سزایی را باید برعهده بگیرند.

عوامل دخیل مسوول: شامل **افرادی که مسوولیت دفاع از مدافعین را برعهده دارند.** در میان این عوامل می‌توان به موارد زیر اشاره کرد:

- دولت و حکومت (شامل نیروهای امنیتی، قاضی‌ها، قانونگذاران و ...)
- نهادهای بین‌المللی با دستورالعمل و یا هدفی که حفاظت از این افراد را دربر می‌گیرد، نهادهایی چون نهادهای وابسته به سازمان ملل، نیروهای صلح‌بان و ...
- در صورتی که اپوزیسیون تشکل از فعالان صلح باشد، باید آنها را کاملا توجیه کرد که از حمله به مدافعین حقوق بشر خودداری کنند (و آنان را غیرنظامی تلقی کنند) این امر به ویژه در مواردی که اپوزیسیون صلح کنترل منطقه‌ای را به دست گرفته است، از اهمیت به‌سزایی برخوردار است.

عوامل دخیلی که می‌توانند به صورتی آشکار بر حفاظت از مدافعین تاثیر بگذارند

این عوامل دخیل می‌توانند توانایی و یا ظرفیت سیاسی برای اعمال فشار بر عوامل دخیل مسوولی باشد که وظایف خود را به صورت مناسب انجام نمی‌دهند (برای مثال می‌توان از سایر دولت‌ها یا نهادهای وابسته به سازمان ملل به عنوان اهرم فشاری بر سایرین استفاده کرد). بدیهی است که در مواردی برخی از این عوامل دخیل ممکن است به صورت مستقیم و یا غیر مستقیم در حملات و یا اعمال فشار بر مدافعین هم‌مشارکت داشته و یا سهیم باشند (شرکت‌های خصوصی، وسایل ارتباط جمعی و یا حتی در مواردی دولت‌های دیگر را می‌توان گاه در این گروه مشاهده کرد). رویکرد این عوامل دخیل نسبت به مدافعین حقوق بشر و تاثیر آنها بر حفاظت این افراد متاثر از منافع و استراتژی‌های کلان آنها است. لیست زیر هر چند جامع و کامل نیست اما بهر حال شامل مواردی‌است که غالبا بر سطح حفاظت مدافعین حقوق بشر تاثیر گذارند.

- نهادهای وابسته سازمان ملل (به استثنای نهادهایی که دارای وظایف لازم‌الاجرا و از پیش تعیین شده هستند)
- کمیته بین‌المللی صلیب سرخ
- سایر دولت‌ها و نهادهای چندملیتی (چه به عنوان سیاستگذار و چه کمک کننده مادی)
- سایر فعالان مسلح
- سازمان‌های غیر دولتی (ملی یا بین‌المللی)
- کلیساها و نهادهای مذهبی
- سازمان‌های خصوصی
- رسانه‌های جمعی

یکی از مشکلات اصلی برای درک و تبیین استراتژی‌ها و اقدامات صورت گرفته توسط عوامل دخیل، به ابهام نوع رابطه میان آنها با یکدیگر و یا فقدان چنین رابطه‌ای بازمی‌گردد. بسیاری از عوامل دخیل مسوول همانند دولت‌ها، نیروهای امنیتی و نیروهای مسلح مخالف خود در موارد متعدد عامل نقض حقوق بشر بوده و یا با مشارکت و همراهی آنها چنین مواردی صورت می‌گیرد. در چنین شرایطی بدیهی است که نمی‌توان از این عوامل دخیل مسوول انتظار داشت که به صورت مناسب حفاظت از مدافعین را برعهده بگیرند.

در شرایطی که هر یک از عوامل دخیل به صورت انفرادی و در وضعیت عادی دارای نگرانی‌های امنیتی خاص خود هستند، اما هنگامی که این عوامل در محیطی به تعامل با یکدیگر می‌پردازند، این نگرانی‌های امنیتی عملا به حاشیه رانده شده و منافع متضاد و رقابت‌های متزاحم

جایگزین آنها می‌شوند. به عبارت دیگر در چنین شرایطی به جای اینکه امکان تاکید بر نگرانی‌های امنیتی خاص و غالبا مشترک وجود داشته باشد باید حداکثر تلاش به عمل آید تا تعارض و برخورد منافع عوامل دخیل به حداقل برسد. رقابت‌های سیاسی دولت‌ها، نهادهای تحت کنترل سازمان ملل و سازمان‌های غیردولتی و منافع گاه متعارض آنها شاهدی بر این مدعاست. مجموعه این شرایط، به همراه ویژگی‌های ذاتی بحران‌ها و درگیری‌ها باعث می‌شود تا تصویری پیچیده از محیط کاری (به عنوان یک مجموعه کلی) پیش روی شکل بگیرد.

تحلیل فرآیندها و ساختارهای متغیر

عوامل دخیل، عواملی ساکن و ایستا نیستند، آنها در سطوح مختلف با یکدیگر ارتباط داشته و بدین ترتیب انبوهی از روابط تودرتو و تارمانند را آفریده و شکل می‌دهند. در مورد حفاظت، توجه و برجسته‌سازی به روابطی که نیازهای حفاظتی افراد را شکل داده و یا گاه تغییر می‌دهند، ضروری است. ما می‌توانیم در این حالت از "**ساختارها و فرآیندها**" حرف بزنیم.

ساختارها بخش‌هایی از نهادهای خصوصی، جامعه مدنی و بخش عمومی هستند که از ارتباطاتی درونی با یکدیگر برخوردارند. ما در این جا از نقطه‌نظر حفاظتی به بررسی آنها می‌پردازیم. در بخش عمومی ما دولت را به عنوان مجموعه‌ای از فعالان که یا دارای یک استراتژی واحد هستند و یا استراتژی‌هایی با تعارضات درونی را تعقیب می‌کنند، درنظر می‌گیریم. برای مثال هنگامی که از موضوعی میان سیاست‌های دولت در قبال مدافعین حقوق بشر صحبت می‌کنیم تفاوت میان سیاست‌های مورد تعقیب و یا مطلوب وزارت دفاع و وزارت خارجه به وضوح آشکار می‌شود. ساختارها می‌توانند دارای مولفه‌های مرکب باشند، برای مثال یک کمیسیون میان‌بخشی (که شامل اعضایی از دولت، سازمان‌های غیردولتی، سازمان ملل و هیات‌های دیپلماتیک می‌شود) می‌تواند برای تعقیب وضعیت حفاظت از یک سازمان مدافع حقوق بشری معین تشکیل شود.

فرآیندها زنجیره‌هایی از تصمیمات و یا اقدامات هستند که توسط یک یا چند ساختار با هدف بهبود شرایط حفاظتی یک گروه خاص گرفته و یا اجرا می‌شوند. فرآیندها می توانند شمال فرآیندها در بهبود وضعیت حفاظتی موفق نیستند. در موارد متعدد، فرآیندهای حفاظتی در تضاد با یکدیگر را خنثی می کنند. برای نمونه مردمی که گفته می‌شود تحت حفاظت و حفاظت قرار گرفته‌اند، ممکن است عملا حاضر به پذیرش فرآیندهای "حفاظت سیاسی" دولت نباشند چرا که معتقدند هدف آنها به وضوح تنها آواره کردن مردم از یک منطقه معین و بیرون راندن آنها است. در چنین شرایطی سازمان ملل، سازمان‌های غیردولتی می توانند به مردم در این فرآیندها کمک کنند. اعتماد به کارکرد این سازمان‌ها می تواند جایگزین بی‌اعتمادی به دولت باشد.

راه‌های متعددی برای انجام تحلیل عوامل دخیل یا فعالان وجود دارد. در روش زیر از متدولوژی بررسی مستقیم استفاده شده است که رعایت آن می تواند نتایج مناسبی را در فرآیند تحلیل و تصمیم‌گیری حاصل کند.

هنگام پیش‌بینی و برآورد فرآیندهای حفاظت، باید کارکرد آنها در چشم‌انداز زمانی معقول را نیز مدنظر داشت. به عبارت دیگر حرف مناسب بودن فرآیندهای حفاظت در زمان حال کافی نیست. همواره باید این پرسش را مطرح کرد که آیا در آینده (زمانی معقول) هم این فرآیندها پاسخگو خواهند بود؟ درنظر داشتن منافع و اهداف تمامی عوامل دخیل در این میان از اهمیت ویژه‌ای برخوردار است.

تحلیل عوامل دخیل در چهار گام

۱ ◆ شناسایی مسائل حفاظتی در بستری گسترده‌تر (برای مثال بررسی شرایط امنیتی مدافعین حقوق بشر در منطقه‌ای مفروض در درون کشور)

۲ ◆ عوامل دخیل چه کسانی هستند؟ (به عبارت واضح‌تر چه نهادها، موسسات و گروه‌ها و یا افرادی مسوولیت حفاظت را بر عهده داشته

و یا از این اقدام سود می برند؟). شناسایی و تهیه فهرستی از این عوامل دخیل که امکان تهیه آن با برگزاری چند جلسه طوفان فکری و یا بحث گفت و گو وجود دارد.

۳ ◆ تحقیق و تحلیل مشخصه های عوامل دخیل و ویژگی های خاص آنها. مواردی چون مسوولیت هر یک از عوامل در حفاظت، قدرت تاثیرگذاری آنها بر شرایط حفاظتی، اهداف، استراتژی ها، مشروعیت و منافع آنها (از جمله اراده آنها بر تداوم حفاظت).

۴ ◆ بررسی و تحقیق در مورد رابطه میان عوامل دخیل

بعد از انجام این تحلیل ها و طی مراحل چهارگانه باید بتوانید از ماتریسی مانند آنچه در زیر شرح داده می شود، استفاده کنید:

لیست تمامی عوامل دخیل مرتبط با یک موضوع حفاظتی کاملا تعریف شده را در یک ماتریس قرار دهید (ترسیمه۲). همان لیست را در ستون نخست و سطر نخست تکرار کنید. اکنون می توانید دو روش تحلیلی را تعقیب کنید.

◆ برای تحلیل ویژگی های هر عامل دخیل (اهداف، منافع، استراتژی ها، مشروعیت و قدرت). باکس های نظری را (در حقیقت محل برخورد ستون و سطر متعلق به هر عامل با یکدیگر) پر کنید.

برای مثال

می توانید منافع و علایق و استراتژی های گروه های مخالف مسلح را در باکس **الف** قرار دهید.

◆ برای تحلیل رابطه میان عوامل دخیل، باکس هایی را که به تعریف مهمترین "رابطه" مرتبط با موضوع حفاظتی اختصاص یافته اند، پر کنید.

برای مثال باکسی که از تقاطع ارتش و کمیسیونر عالی سازمان ملل در امور پناهندگان)قزاندع) شکل می گیرد (باکس ذ) را پر کنید. به همین ترتیب ادامه بدهید.

پس از پر کردن مرتبط ترین باکس ها، شما تصویری از اهداف و استراتژی ها و نحوه برهم کنش مهمترین عوامل دخیل مرتبط با یک موضوع حفاظتی معین را پیش روی خواهید داشت.

ترسیمه۲: سیستم ماتریسی برای تحلیل عوامل دخیل

	دولت	ارتش	پلیس	مخالفین مسلح	گروه‌های ملی حقوق بشر	کلیساها	سایر دولت‌ها	آژانسهای سازمان ملل	سازمانهای غیردولتی بین‌المللی
دولت	عامل دخیل								
ارتش		عامل دخیل						B	
پلیس			عامل دخیل						
مخالفین مسلح				A					
گروه‌های ملی حقوق بشر					عامل دخیل				
کلیساها						عامل دخیل			
سایر دولت‌ها							عامل دخیل		
آژانسهای سازمان ملل								عامل دخیل	
سازمانهای غیردولتی بین‌المللی									عامل دخیل

باکس A

برای هر عامل دخیل

- اهداف و منافع
- استراتژی‌ها
- مشروعیت
- قدرت

باکس B

رابطه میان فعالان دخیل

رابطه متقابل فعالان دخیل در ارتباط با مسائل استراتژیک و موضوعات حفاظتی

فصل دوم

برآورد مخاطرات: تهدیدات آسیب‌پذیری و ظرفیت‌ها

هدف:

درک مفاهیم تهدیدات، آسیب‌پذیری و ظرفیت در مباحث امنیتی

آشنایی با برآورد مخاطرات

تحلیل‌ها مخاطرات و نیاز به محافظت

فعالیت مدافعین حقوق بشر می‌تواند بر منافع برخی فعالان خاص تاثیر منفی بگذارد. طبیعی است که این افراد یا گروه‌ها هم در واکنش به این امر، مدافعین را با مخاطراتی مواجه سازند. بدین لحاظ تاکید بر این موضوع که "**این مخاطرات بخشی تفکیک ناپذیر از زندگی مدافعین حقوق بشر در برخی کشورهای خاص است**" الزامی است.

برای برآورد مخاطراتی که متوجه مدافعین حقوق بشر می‌شود، می‌توان به صورت زیر عمل کرد:

تحلیل منافع و استراتژی‌های فعالان دخیل اصلی >> برآورد تاثیر فعالیت‌های مدافعین بر این منافع و استراتژی‌ها >> برآورد مخاطراتی که متوجه مدافعین می‌شود>> برآورد آسیب‌پذیری و ظرفیت مدافعین>>اثبات مخاطرات

به عبارت دیگر، فعالیت‌هایی که شما به عنوان مدافع حقوق بشر انجام می‌دهید ممکن است میزان مخاطراتی را که متوجه شما می‌شود، افزایش دهد.

- **آنچه** که شما انجام می‌دهید می‌تواند تهدیدات را به همراه آورد
- **نحوه، محل و زمان** فعالیت شما هم می‌تواند در میزان آسیب‌پذیری و ظرفیت شما تاثیر بگذارد

تاکنون هیچ تعریف واحدی در مورد مخاطرات صورت نگرفته است، اما می‌توانیم آن را به عنوان مجموعه‌ای از رویدادهای احتمالی- هر چند حدوث آنها قطعی نیست- که می‌توانند به آسیب و صدمه منجر شوند، در نظر بگیریم.

در هر شرایط مفروضی، افرادی که در حوزه حقوق بشر فعالیت دارند ممکن است در معرض سطح یکسانی از خطرات قرار گیرند، اما بدیهی است که تمام افراد، حتی اگر در مکان مشابهی به سر برند، از آسیب‌پذیری مشابهی در قبال مخاطرات عمومی برخوردار نیستند. به عبارت ساده‌تر با در نظر گرفتن مجموعه ای از **خطرات** معین و ثابت و با فرض اینکه جمعی از مدافعین در مکان مشابه، فعالیت مشابهی را پیگیری کنند، باز هم میزان آسیب‌پذیری هر شخص در قبال این مخاطرات با دیگری متفاوت خواهد بود.

میزان **آسیب‌پذیری**- یا احتمال صدمه و آسیب‌دیدن یک شخص یا گروهی از مدافعین در اثر حمله و یا هر اقدام خصمانه دیگر- برآیندی از چندین عامل است که ما اکنون آنها را مورد بررسی قرار خواهیم داد.

برای درک بهتر این عوامل مثال زیر را در نظر بگیرید

کشوری فرضی را در نظر بگیرید که در آن دولت تهدیدی عام را متوجه تمامی فعالان حقوق بشر در تمامی عرصه‌ها می کند. این امر بدان معناست که تمامی مدافعین در معرض تهدید قرار دارند. با این وجود ما می‌دانیم که برخی مدافعین بیش از دیگران در معرض تهدید قرار گرفته‌اند. برای مثال یک سازمان غیردولتی بزرگ و دارای ساختار مناسب که در پایتخت استقرار یافته و فعالیت می کند به مراتب کمتر از یک سازمان غیردولتی کوچک و محلی در معرض تهدید قرار می گیرد. ممکن است در ابتدا این موضوع را امری بدیهی و منطقی فرض کنیم، اما بررسی دقیق و موشکافانه علل این امر می تواند در درک بهتر نگرانی‌های امنیتی مدافعین در رفع آنها مفید باشد.

سطح مخاطراتی که گروهی از مدافعین با آن مواجه هستند متناظر با **تهدیداتی** که دریافت کرده اند و نیز سطح **آسیب‌پذیری** آنان در برابر این تهدیدات افزایش می‌یابد. این مساله را می‌توان به معادله زیر ۲ تبدیل کرد:

آسیب‌پذیری × تهدیدات = مخاطرات

تهدیدات در واقع نشانگر این احتمال هستند که شخصی ممکن است به انسجام معنوی، فیزیکی و یا مالی شخص دیگری از طریق اعمالی آگاهانه و با قصد و نیت مشخص- و غالبا همراه با خشونت-، صدمه بزند. "برآورد تهدیدات" به معنای تحلیل احتمال عملی شدن این احتمالات (تهدیدات) است.

مدافعین ممکن است در جریان یک سناریوی درگیری با تهدیدات متفاوت و بی‌شماری مواجه شوند. این تهدیدات ممکن است به اشکال "تهدیدات غیرمستقیم"، "حملات جنایی عام" و یا "هدف قرار دادن" بروز یابند.

رایج‌ترین نوع تهدید را می‌توان "**هدف‌قرار دادن**" دانست. در این نوع تهدید هدف توقف و یا تغییر فعالیت گروه و یا تاثیر گذاری بر رفتار افراد دخیل در فعالیتی مشخص است. این نوع تهددی معمولا ارتباطی نزدیک با فعالیتی دارد که توسط مدافعین در حال انجام است. در این میان منافع و نیازهای افراد مخالف اقدامات مدافعین را هم باید در نظر داشت.

مدافعین همچنین ممکن است با تهدیداتی از جنس "**حملات جنایی عام**" مواجه شوند. این احتمال به ویژه هنگامی که آنها در محیط‌های پرمخاطره فعالیت می کنند، به شدت افزایش می‌یابد: از سوی دیگر باید توجه داشت که بسیاری از تهدیدات هدفمندی که در بالا به آن اشاره شد، عموما تحت پوشش "حملات جنایی عام" صورت گرفته و عاملان سعی می کنند تا آنها را به صورتی حوادثی رایج جلوه دهند.

تهدیدات غیرمستقیم عموما ناشی از صدماتی است که در مناطق و حوزه‌هایی که در آنها درگیری‌های مسلحانه وجود دارد، به صورت بالقوه وجود دارند. این تهدیدات را معمولا به "بودن در مکان نادرست، در زمانی نادرست" تعبیر می کنند. این تهدیدات معمولا متوجه مدافعینی می‌شوند که در مناطقی که درگیری‌های مسلحانه در آن در جریان است، فعالیت می کنند.

تهدیدات هدفمند (یا قرار دادن) می‌توانند به صورتی دیگر نیز متوجه مدافعین شوند برای مثال مدافعین حقوق بشر ممکن است گاه با تهدیداتی "**بیان شده**" مواجه شوند. این نوع تهدیدات می‌توانند از طریق ارسال هشدارهایی در مورد "تهدید مرگ" متوجه مدافعین شوند. (برای آشنایی با برآورد "تهدیدات بیان شده" به فصل ۳ رجوع کنید).
از سوی دیگر همچنین مواردی از تهدیدات "**احتمالی**" را می‌توان برشمرد که در جریان آن یک مدافع حقوق بشر که در مجاورت محل فعالیت شما، به کار مشغول است هدف تهدید قرار می گیرد و بدین ترتیب این انتظار منطقی به وجود می آید که ممکن است هدف بعدی چنین تهدیداتی شما باشید.

آسیب‌پذیری‌ها

آسیب‌پذیری به معنای میزان احتمال لطمه دیدن، متحمل خسارت شدن، آسیب‌خوردن و در مواردی دیگر مرگ افراد در هنگام مواجهه با حمله است. بدیهی است این میزان برای هر مدافع و یا هر گروهی در مقایسه با شخص یا گروه دیگر متفاوت است. گذر زمان و تغییر شرایط هم این میزان را تغییر می‌دهد. آسیب‌پذیری همیشه امری نسبی است چرا که تمامی افراد و گروه‌ها به هر حال تا حدی آسیب‌پذیر هستند. با این وجود هر شخص دارای سطح و نوع آسیب‌پذیری خاص خود است. نوع و سطح آسیب‌پذیری هر فرد را شرایط تعیین می‌کند. بگذارید برای روشن شدن بهتر موضوع چند نمونه را در نظر بگیریم:

- آسیب‌پذیری می‌تواند با موقعیت مکانی در ارتباط باشد. برای مثال یک مدافع حقوق بشر هنگامی که برای انجام بازرسی میدانی در حال سفر به نقطه‌ای دیگر است، به مراتب از زمانی که در داخل دفتر شناخته شده خود قرار گرفته و هر حمله‌ای توسط سایرین مشاهده و گزارش خوهد شد، آسیب‌پذیرتر است.

- آسیب‌پذیری همچنانکه ممکن است ناشی از عدم دسترسی به تلفن یا سیستم حمل و نقل مطمئن زمینی و یا عدم وجود قفل و بست مناسب برای درهای خانه باشد، می‌تواند از فقدان وجود شبکه‌ها و یا واکنش‌های مشترک میان مدافعین نیز نشات بگیرد.

- آسیب‌پذیری ممکن است با کار تیمی و یا هراس مرتبط باشد. مدافعی که تهدیدی را دریافت می‌کند، ممکن است هراسان شده و این ترس به کار او هم اثر بگذارد. اگر در این شرایط دو راهی برای برطرف کردن ترس خود نداشته باشد ظ(برای نمونه دوستی برای صحبت کردن و یا تیمی از همکاران قابل اعتماد برای عنوان کردن موضوع و یاری خواستن از آنها وجود نداشته باشد) احتمال دارد که در اثر این ترس مرتکب اشتباهاتی شده و یا تصمیمات نه چندان مناسبی اتخاذ کند. هر دوی این موارد می‌توانند در نهایت به تشدید معضلات امنیتی او منتهی شوند.

(در پایان این فصل فهرستی از آسیب‌پذیری‌های احتمالی و ظرفیت‌ها ارائه شده است).

ظرفیت‌ها

ظرفیت‌ها در واقع همان توان (قدرت) یا منابعی هستند که یک گروه و یا حتی یک مدافع به صورت منفرد به آنها دسترسی داشته و با به کارگیری آنها می‌تواند تا حد معقولی امنیت خود را تضمین کند. مواردی چون آموزش‌های امنیتی و یا قانونی، کار گروهی به صورت تیم، دسترسی به تلفن یا حمل و نقل امن، دسترسی به شبکه‌ای مناسب از مدافعین و آشنایی با نحوه غلبه بر هراس و ... را می‌توان در ذیل عنوان ظرفیت‌ها گنجاند.

در اغلب موارد آسیب‌پذیری‌ها و ظرفیت‌ها
دو روی سکه هستند

برای مثال مورد زیر را در نظر بگیرید:

فقدان اطلاعات کافی در مورد محیط کار "آسیب‌پذیری" محسوب می‌شود در حالی که داشتن ای اطلاعات می‌تواند یک "ظرفیت" تلقی شود. در مورد عدم دسترسی و یا دسترسی به حمل و نقل امن و یا شبکه‌ای مدافعین هم می‌توان این موضوع را صادق دانست. در حالی که دسترسی به این موارد یک "ظرفیت" محسوب می‌شود، عدم دسترسی را باید یک "آسیب‌پذیری" قلمداد کرد.

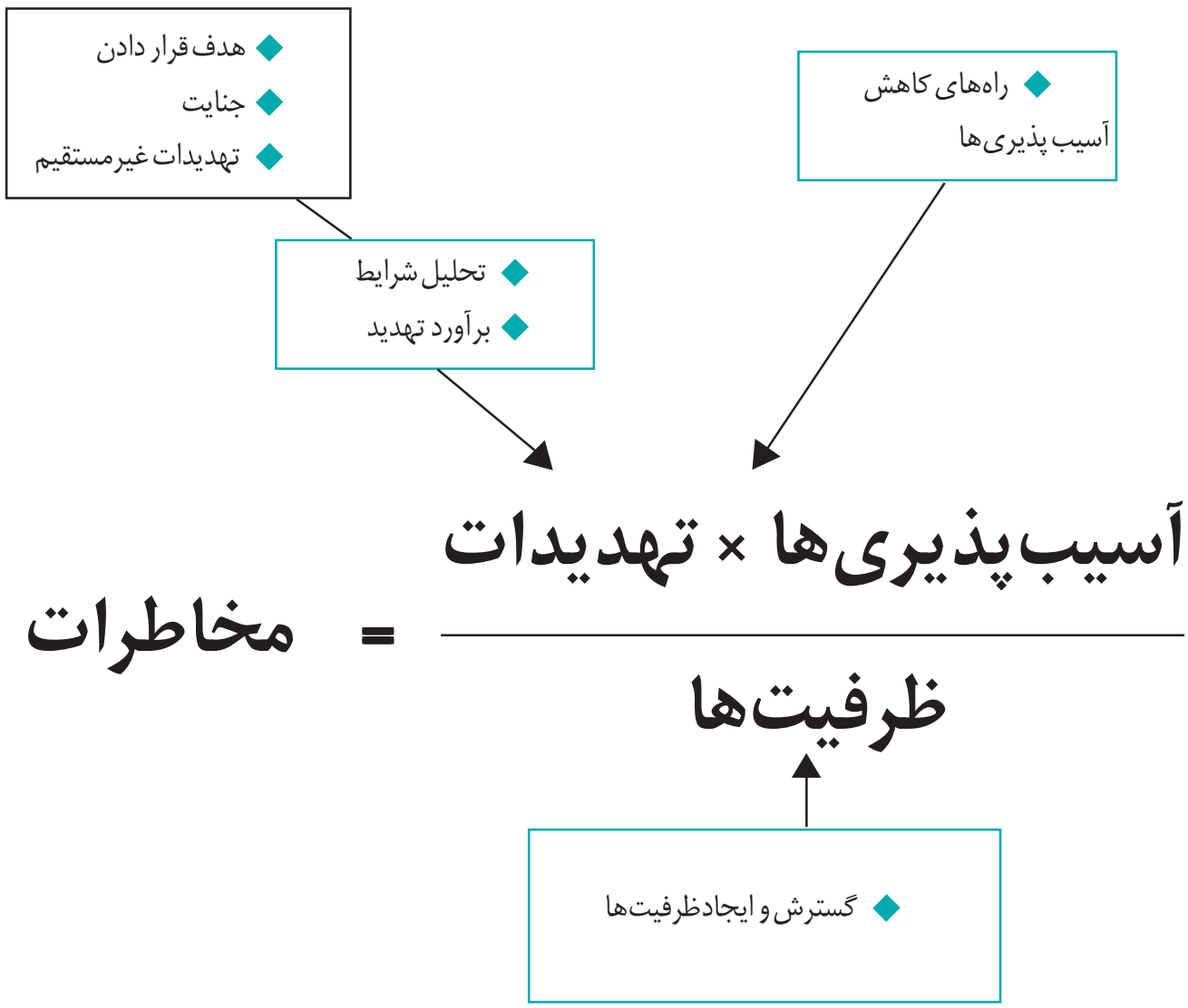
همان‌گونه که پیشتر هم ذکر شده در پایان فصل لیستی از ظرفیت‌ها و آسیب‌پذیری‌های رایج ارائه شده است.
مخاطرات ناشی از تهدیدات و آسیب‌پذیری‌ها در صورتی که مدافعین دارای ظرفیت لازم و کافی باشند، به میزان قابل توجهی کاهش می‌یابند. به عبارت ساده‌تر تعداد و میزان ظرفیت‌ها افزایش یابند، میزان و سطح مخاطرات کاهش خواهد یافت.

$$\text{مخاطرات} = \frac{\text{آسیب‌پذیری‌ها} \times \text{تهدیدات}}{\text{ظرفیت‌ها}}$$

خلاصه بحث

به منظور کاهش مخاطرات به یک سطح قابل قبول و در نهایت حفاظت از خود باید

- تهدیدات را کاهش دهیم
- فاکتورهای آسیب‌پذیری را کاهش دهیم
- و در نهایت ظرفیت‌های حفاظت را افزایش دهیم.



مخاطره، مفهومی دینامیک است که در گذر زمان و با تغییر طبیعت تهدیدات که آسیب‌پذیری‌ها و ظرفیت‌ها دچار تغییر می‌شود. بدین ترتیب بدیهی است که برآورد مخاطرات باید به صورت دوره ای صورت بگیرد. این برآورد دوره‌ای به‌ویژه در شرایطی که محیط کاری، تهدیدات و یا آسیب‌پذیری‌ها دچار تغییر شده‌اند، از اهمیت به سزایی برخوردار است. برای مثال در نظر بگیرید که چگونه با تغییری در رهبری گروه ممکن است مدافعین در موقعیت به مراتب ضعیف‌تری نسبت به قبل قرار بگیرند. بدیهی است در این شرایط آسیب‌پذیری تغییر کرده است. وجود یک تهدید آشکار و حاضر باعث می‌شود تا سطح مخاطرات به صورتی قابل توجه افزایش یابد. در چنین مواردی، تلاش برای کاهش سطح مخاطرات با افزایش ظرفیت‌ها منطقی و قابل توجیه نیست چرا که افزایش ظرفیت‌ها نیازمند صرف زمانی طولانی است و بدیهی است در شرایطی که سطح مخاطرات به حد هشدار دهنده‌ای رسیده باشد امکان بی تفاوتی نسبت به تهدیدات و آسیب‌پذیری‌ها و صرف وقت برای افزایش ظرفیت‌ها وجود ندارد.

رعایت و ارتقای معیارهای امنیتی مانند آموزش‌های قانونی یا موانع حفاظتی می‌توانند با کاهش فاکتورهای آسیب‌پذیری، سطح مخاطرات را هم تقلیل دهند. با این وجود چنین معیارهایی نمی‌توانند نافی منبع اصلی مخاطرات یا به عبارت بهتر همان تهدیدات باشند، همچنانکه از توانایی حذف و به حاشیه راندن تهدیدات هم برخوردار نیستند. رعایت و ارتقای معیارهای امنیتی، در شرایطی که متجاوزان مطمئن هستند به راحتی از دام مجازات خواهند گریخت و لازم نیست در قبال اقدامت خود بهایی پرداخت کنند، عملا نمی‌توانند باعث کاهش چشمگیر سطح مخاطرات شود. بدین ترتیب منطقی‌ترین رویکرد این است که در تمامی اقدامات حفاظتی تاکید و هدف اصلی بر کاهش تهدیدات قرار گیرد. کاهش آسیب‌پذیری و افزایش ظرفیت هم به ترتیب در مراحل بعدی می‌توانند مدنظر قرار گیرند.

مثال

گروهی کوچک از مدافعین در شهری سرگرم فعالیت پیرامون موضوع مالکیت زمین هستند. با آشکار شدن تاثیر اقدامات آنها بر منافع زمین‌داران محلی، آنها چندین تهدید آشکار به مرگ را دریافت می‌کنند. اگر قرار باشد معادله مخاطره به شرایط امنیتی آنها تعمیم داده شود، این امر به ویژه ناشی از تهدید به مرگی است که آنها دریافت کرده‌اند. اگر قرار باشد این مخاطرات کاهش یابند بدیهی است زمان تعویض قفل درهای محل کار نیست (چرا که این مخاطرات به هیچ‌وجه ارتباطی با ورود مخفیانه به محل کار ندارند)، حتی زمان خرید یک تلفن ماهواره‌ای برای هر مدافع هم نیست (چرا که هر چند "ارتباط" برای حفظ امنیت از اهمیت بالایی برخوردار است، اما قطعا زمانی که شخصی قصد کشتن شما را کرده است، نمی‌تواند مانع اجرای این تهدید شود). در چنین شرایطی یک استراتژی معقول و مرتبط کار بر روی ایجاد شبکه‌ها و برانگیختن واکنش‌های سیاسی برای مقابله مستقیم با این تهدید است. در نهایت اگر چشم‌انداز موفقی برای این تلاشش در بازه زمانی کوتاه مشاهده نشد، سریع‌ترین و موثرترین راه حل که می‌توان تهدید را به گونه‌ای قابل توجه تقلیل دهد، کاهش حضور مدافعین در ملاء عام و حتی در مرحله بعدی- و در صورت نیاز- خروج از منطقه برای مدت لازم می باشد. به خاطر داشته باشید که توانایی انتقال به محل امن هم خود یک ظرفیت محسوب می‌شود.

آسیب‌پذیری‌ها و ظرفیت‌ها، همانند تهدیدات، ممکن است بسته به سن و جنسیت تغییر یابند. بدین ترتیب بازبینی یافته‌ها بر اساس این دو فاکتور می‌تواند بسیار موثر باشد.

برآورد آسیب‌پذیری و ظرفیت‌ها

طراحی یک روش مناسب جهت برآورد آسیب‌پذیری‌ها و ظرفیت‌های متناظر با گروهی و یا فردی، معین و مفروض شامل مراحل زیر می‌شود:

- تعیین تعریف گروه (به صورت یک جامعه، مجموعه‌ای از افراد گرد هم آمده، سازمان غیردولتی و ...)

- تعیین موقعیت فیزیکی محل استقرار گروه و زمانبندی فعالیت‌های آن (با در نظر گرفتن اینکه ؟؟فایل آسیب‌پذیری شما در طول زمان دچار تغییر و تحول می‌شود).

پس از طی دو مرحله مقدماتی زیر اکنون می‌توانید آسیب‌پذیری‌ها و ظرفیت‌ها را برآورد کنید. برای این منظور می‌توانید از ترسیمه ۳ که در پایان این فصل ارائه شده است، به عنوان راهنما کمک بگیرید.

لطفا توجه داشته باشید که برآورد ظرفیت‌ها و آسیب‌پذیری‌ها را باید فعالیتی در نظر گرفت که به یک بازه زمانی خاص محدود نشده و نه تنها امکان بازبینی و تکمیل آن در گذر زمان همواره وجود دارد بلکه امری ضروری است. هدف از برآورد ظرفیت‌ها و آسیب‌پذیری‌ها ارائه تصویری دقیق- بر اساس اطلاعات موجود- از معضلی است که به صورت مستمر در حال تکامل و تکوین است. هنگام برآورد ظرفیت‌ها، باید توجه داشت که صرفا ظرفیت‌های عملی موجود در نظر گرفته شوند، نه ظرفیت‌های بالقوه و یا مواردی که ما آرزوی آن را داریم!

استراتژی‌هایی برای تعامل و واکنش

مدافعین و گروه‌های مورد تهدید از استراتژی‌های تعاملی متفاوتی برای مواجهه با مخاطراتی که انتظار حدوث آنها را دارند، بهره می‌گیرند. این استراتژی‌ها بسته به محیط پیرامونی (شهری یا روستایی)، نوع تهدید و منابع مالی، اجتماعی و قانونی موجود و ... متغییر هستند.
استراتژی‌های تعاملی را می‌توان غالبا به صورتی فوری، در واکنش به اهداف کوتاه‌مدت اجرا کرد. به همین دلیل استراتژی‌های تعاملی بیشتر کارکردی شبیه "تاکتیک" دارند تا استراتژی‌های واکنشی دقیق و جامع الاطراف. آنها غالبا متناظر با درک و سابژکتیو افراد از مخاطرات می‌باشند و بدیهی است در مواردی که این استراتژی‌ها بازگشت‌پذیر نباشند، ممکن است صدمات احتمالی محدودی را به گروه وارد سازند.
استراتژی‌های تعاملی معمولا از رابطه‌ای بسیار تنگاتنگ از یک سو با نوع و شدت تهدید و از سوی دیگر با آسیب‌پذیری‌ها و ظرفیت‌های گروه برخوردار هستند.

هنگامی که مساله امنیت و حفاظت را در نظر می گیرید باید علاوه بر استراتژی تعاملی خود، استراتژی های تعاملی سایرین را نیز مدنظر قرار دهید. با لحاظ کردن تمام موارد آنگاه باید استراتژی‌های موثر را تقویت کرده و استراتژی‌های مضر را تا حدامکان کمرنگ و محدود ساخته و به استراتژی‌های باقی‌مانده (به ویژه استراتژی‌های تعاملی مرتبط با باورهای مذهبی یا فرهنگی) احترام بگذارید.

برخی استراتژی‌های تعاملی

- تقویت موانع حفاظتی، اختفای اشیای قیمتی
- اجتناب از رفتارهایی که می‌تواند باعث برانگیخته شدن یا تحریک فعال دیگری شود. این امر به ویژه در مواردی که فعالیت‌های شما در مناطقی واقع شده است که اختلافات مسلحانه بر سر آن جریان دارد، از اهمیت بسیاری برخوردار است.
- اختفا و پنهان شدن در شرایطی که مخاطرات به شدت افزایش می‌یابند. مکان‌های مناسب نقاطی هستند که دسترسی به آنها به سادگی امکانپذیر نیست؛ مکان‌هایی چون کوه‌ها یا جنگل‌ها، در چنین شرایطی تغییر مستمر محل سکونت هم می‌تواند تا حدی مفید باشد. گاه لازم است تمام خانواده (علاوه بر شخص مدافع) مخفی شوند و در مواردی هم تنها اختفای خود مدافع کافی است. اختفا می‌تواند به ساعات شب محدود شده و یا در مواردی حتی چندین هفته به طول بینجامد و در طی یان مدت هیچ تماسی با خارج گرفته نشود.
- تلاش برای کسب حفاظت سیاسی، نظامی از سوی یکی از طرفین درگیری مسلحانه
- تعلیق فعالیت‌ها، بستن دفتر و تخلیه مکان، مهاجرت اجباری (آوارگی یا جابه‌جایی محدود داخلی) تبعید.

- تکیه بر "شانس مساعد" و یا توسل به باورهای سحرآمیز و جادویی
- پنهان کاری بیشتر، از جمله محدودسازی روابط با همکاران، انکار همه چیز با سرباز زدن از گفت‌وگو در مورد تهدیدات، نوشیدن مشروبات الکی به حد افراط، اضافه‌کاری‌های طولانی و رفتارهای آزاردهنده و منزجر کننده

مدافعین اما همزمان به استراتژی‌های واکنشی هم دسترسی دارند. این استراتژی‌ها می‌توانند شامل مواردی چون انتشار گزارشاتی برای اعلان عمومی یک موضوع، اعلام اتهام علیه شخص یا گروهی، برگزاری تظاهرات و ... گردند. در بسیاری از موارد این استراتژی‌های عملا به یک استراتژی ها عملا به یک استراتژی قابل اتکا در بلند مدت منتهی نشده و درنهایت تنها به تحقق اهداف و رفع نیازهای کوتاه مدت می‌انجامد. در برخی موارد استراتژی‌های واکنشی حتی ممکن است معضلات امنیتی بیشتری را هم بیافرینند. به عبارت دیگر این استراتژی‌های نه تنها گرهی از مشکلات و معضلات امنیتی باز نکرده که حتی بر بار آن هم ممکن است بیافزایند.

هنگام تحلیل استراتژی‌های تعاملی و واکنشی باید موارد زیر را لحاظ کرد:

- **حساسیت:** آیا استراتژی‌های مورد نظر شما می‌توانند به سرعت نیازهای امنیتی فرد یا گروه را برطرف کنند؟
- **سازگاری:** آیا این استراتژی‌ها قابلیت سازگاری سریع با شرایط جدید را پس از رفع خطر حمله دارا هستند؟ ممکن است مدافع دارای چند گزینه باشد برای‌مثال‌بتواند مخفی شود یا مدتی منزل دیگران ساکن شود. شاید چنین استراتژی‌هایی ضعیف و فاقد ثبات به نظر برسند اما اغلب از دوام و پایداری مناسبی برخوردارند.
- **پایداری:** آیا استراتژی‌های مورد نظر در گذر زمان علی‌رغم تهدیدات و حملات غیرکشنده، می‌توانند پایدار بمانند؟
- **تاثیر گذاری:** آیا استراتژی‌های شما می‌توانند به گونه‌ای موثر از افراد و یا گروه‌های مفروض حمایت کنند؟

بازگشت‌پذیری: در صورت عدم موفقیت استراتژی یا تغییر شرایط، آیا امکان بازگشت و یا تغییر استراتژی‌ها وجود دارد؟

تعامل با مخاطرات پس از ارزیابی

هنگامی که برآورد ارزیابی شما از مخاطرات تکمیل شد، زمان بررسی نتایج فرا رسیده است. با توجه به اینکه محاسبه و سنجش میزان مخاطراتی که با آن مواجه هستید، امکان‌پذیر نیست، باید "سطح مخاطره" را مدنظر قرار دهید.
مدافعین و سازمان‌های مختلف، ممکن است برآوردهای متفاوتی از سطح مخاطرات پیش روی خود داشته باشند. آنچه که از نظر برخی مدافعان غیرقابل‌پذیرش است، از نگاه جمعی دیگر ممکن است امری طبیعی و قابل‌پذیرش تلقی شود. گاه حتی نوع تلقی از سطح مخاطرات در میان اعضای یک سازمان هم متفاوت است. در این جا بهتر است به جای آنکه در مورد آنچه که "باید" انجام شود و یا اینکه آیا آماده مقابله با مخاطرات هستید یا خیر، در ابتدا برداشت‌های متفاوت افراد از مخاطرات مورد بررسی قرار گیرند. به عبارت بهتر باید در ابتدا به تعریفی قابل قبول و مورد اجماع در میان تمامی اعضای سازمان برسید.

به هر حال برای تعامل با مخاطرات راه‌های متفاوتی وجود دارند:

- می‌توانید مخاطرات را در شرایط فعلی "**قابل قبول**" توصیف کرده و سعی کنید با آنها کنار آمده و فعالیت خود را پیگیری کنید.
- می‌توانید سطح مخاطرات را **کاهش** دهید. این امر با کار بر روی تهدیدات، آسیب‌پذیری‌ها و ظرفیت‌ها امکان‌پذیر است.
- می‌توانید مخاطرات را با دیگران **سهیم** شوید. به عبارت واضح‌تر با همکاری و انجام اقدامات و فعالیت‌های به صورت مشترک با سایر مدافعین و یا سازمان‌های مدافع حقوق بشر، تهدیدات احتمالی به یک مدافع و یا یک سازمان خاص را کم‌اثرتر کنید.
- می‌توانید از مواجهه با مخاطرات **اجتناب** کنید. این امر با توقف فعالیت‌ها و تغییر رویکرد به نحوی که تهدیدات احتمالی کاهش یابند،

امکان‌پذیر خواهد بود.

◆ می‌توانیدبه مخاطرات **اعتنایی نداشته** و به کار خود ادامه دهید. بی‌توجهی به مخاطرات و روی‌گرداندن از آنها، قطعا بهترین گزینه پیشنهادی محسوب نمی‌شود!

باید توجه‌داشته‌باشید که‌سطح مخاطرات برای هر سازمان و یا فردی که‌در مسائل مربوط به حقوق بشر فعالیت‌دارد، متفاوت‌است. مهاجمان معمولا ترجیح می‌دهند ضعیف‌ترین بخش‌ها را هدف حمله قرار دهند. بدین ترتیب بررسی جامع موضوع و شناسایی این نقاط ضعیف که می‌توانند هدف بالقوه حمله مهاجمان قرار گیرند، از اهمیت بسزایی برخوردار است. برای مثال موردی را در نظر بگیرید که یک دهقان توسط شبه نظامیان یا عوامل مسلح مالک زمین کشته می‌شود. ممکن است چندین سازمان و یا فرد در بررس این موضوع و پیگیری آن دخیل باشند. برای نمونه شاید یک گروه‌از وکلای مستقر در شهری نزدیک پایتخت، اتحادیه دهقانان محلی و سه شاهد ماجرا (که‌در واقع دهقانان ساکن روستای مجاور هستند) در این قضیه عوامل دخیل شمرده شوند. در چنین شرایطی برآورد سطوح مختلف تهدیدی که متوجه هر یک از این افراد و یا گروه‌ها می‌شود، برای برنامه ریزی نحوه حفظ امنیت آنها ضروری است.

ترسیمه ۳- اطلاعات مورد نیاز برای برآورد ظرفیت‌ها و آسیب‌پذیری‌های یک گروه

نکته: اطلاعات درج شده در ستون سمت راست نشاندهنده آن است که موارد درج شده در ستون سمت چپ را باید جزو ظرفیت‌ها در نظر گرفته و یا از رده آسیب‌پذیری‌ها قلمداد کرد.

اطلاعات مورد نیاز برای ارزیابی آسیب‌پذیری‌ها و ظرفیت‌های مرتبط با هر مولفه	مولفه‌های آسیب‌پذیری‌ها و ظرفیت‌ها
مولفه‌های فنی، فیزیکی و جغرافیایی	
لزوم حضور و یا گذر از مناطق خطرناک برای انجام امور روزانه و یا فعالیت‌های محوله- تهدیدکنندگان حاضر در این مناطق	در معرض دید قرار گرفتن
مشخصه‌های ساختمانی (دفاتر- منازل- پناهگاه‌ها)، مواد ساختمانی جنس درها، پنجره‌ها و کمدها- موانع حفاظتی- روشنایی در شب	ساختارهای فیزیکی
آیا عامه مردم امکان دسترسی به دفاتر شما را دارند؟ آیا محلی خاص برای پرسنل در نظر گرفته‌شده‌است؟ آیا با مراجعین ناشناخته هم در طول حضور خود در دفتر مواجه می‌شوید؟	دفاتر کار و مکان‌های قابل دسترسی برای عامه
آیا مکان اختفایی وجود دارد؟ میزان و امکان دسترسی به این مکان چگونه است؟ چه کسانی به آن دسترسی دارند (افراد خاص یا تمام گروه)؟ آیا در صورت لزوم می‌توانید محل کار را ترک کرده و به آنجا بروید؟	مکان‌های اختفا، راه‌های فرار
امکان دسترسی بازدیدکنندگان خارجی (مقامات دولتی، اعضای سازمان‌های غیردولتی و ...) به محل کار شما چگونه است؟ آیا در منطقه پرخطری حضور دارید که دسترسی به شما را مشکل کند؟ دسترسی به محل کار شما تا چه میزان برای مهاجمان دشوار است؟	دسترسی به محل

اطلاعات مورد نیاز برای ارزیابی آسیب‌پذیری‌ها و ظرفیت‌های مرتبط با هر مولفه	مولفه‌های آسیب‌پذیری‌ها و ظرفیت‌ها
آیا مدافعین به حمل و نقل امن (حمل و نقل عمومی یا شخصی) دسترسی دارند؟ آیا این روش حمل و نقل مزایا یا معایب خاص دارد؟ آیا هنگام سفر به مسکن امن دسترسی دارند؟	حمل و نقل و مسکن
آیا امکانات ارتباطی (رادیو، تلفن در محل وجود دارد؟ آیا دسترسی به مدافعین به آنها ساده است؟ آیا این وسایل همواره سالم هستند؟ آیا امکان قطع ارتباط هنگام حمله مهاجمین (توسط آنان یا بر اثر حادثه) وجود دارد؟	ارتباطات
آیا مدافعان با طرف‌های درگیر ارتباطی دارند (وابستگی، هم‌محل بودن یا منافع مشترک) که امکان استفاده نادرست و سوء از آنها علیه سایر مدافعان وجود داشته باشد؟	ارتباط با طرف‌های درگیر
آیا فعالیت مدافعان تاثیر مستقیمی بر منافع یک فعال درگیری می گذارد (مواردی چون حفاظت از منابع طبیعی، حق زمین و یا موارد باارزش برای فعالان قدرتمند)؟ آیا موضوعی به شدت حساس برای یکی از فعالان در حوزه کاری شما قرار دارد؟	اقدامات مدافعان و تاثیر آنها بر یک طرف درگیری
آیا مدافعین دارای کالاها یا اشیایی هستند (مانند بنزین، باتری، کمک‌های اولیه، دستور العمل‌های پزشکی و یا اسناد مهم) که آنها را تبدیل به هدفی برای حمله مهاجمان کند؟	انتقال کالاها و اشیاء و اطلاعات مکتوب
آیا اطلاعات شما در مورد حوزه‌های درگیری ممکن است شما را در معرض خطر قرار دهد؟ آیا اطلاعاتی در مورد مناطق امن و به‌دور از درگیری دارید؟ آیا اطلاعات قابل اتکایی در مورد مناطق مین گذاری شده دارید؟	دانش در مورد حوزه درگیری‌ها و مناطق مین گذاری‌شده

مولفه‌های مربوط به سیستم قانونگذاری و سیاسی

آیا مدافعین می‌توانند از فرآیندهای قانونی برای استفاده از حقوق خود (دسترسی به وکیل و حضور فیزیکی او در مکالمات و ...) بهره گیرند؟ آیا امکان بهره گیری از کمک مقامات مرتبط برای حفظ امنیت و تداوم فعالیت خود را دارا هستند؟	دسترسی به مقامات و یا سیستمی قانونی برای استفاده از حقوق قانونی
آیا مدافعین از لحاظ قانونی امکان درخواست حقوق قانونی خود را دارند؟ آیا آنها در معرض قوانین داخلی سرکوبگرانه قرار می گیرند؟ آیا آنها می توانند حمایت کافی را برای جلب توجه مقامات نسبت به ادعاهای خود جلب کنند؟	مکان به نتیجه رسیدن اقدامات از طریق سیستم قانونی و یا مقامات

اطلاعات مورد نیاز برای ارزیابی آسیب‌پذیری‌ها و ظرفیت‌های مرتبط با هر مولفه	مولفه‌های آسیب‌پذیری‌ها و ظرفیت‌ها
آیا مدافعین از ثبت فعالیت خود (گروهی یا فردی) به صورت قانونی منع شده و یا با تاخیرهای طولانی مواجه می‌شوند؟ آیا سازمان آنها امکان افتتاح حساب و فعالیت مالی با توجه به استانداردهای قانونی را دارا است؟ آیا از نرم‌افزارهای رایانه‌ای خاص استفاده می‌کنند؟	استانداردهای قانونی، ثبت فعالیت و نگاهداری حساب

مدیریت اطلاعات

آیا مدافعین دارای منابع اطلاعاتی مستند برای متهم کردن مجرمان هستند؟ آیا اطلاعات از سوی مدافعان با دقت و به روش صحیح منتشر می شود؟	منابع و دقت اطلاعات
ایا مدافعین امکان نگاهداری اطلاعات در مکانی امن و قابل اطمینان را دارا هستند؟آیا امکان سرقت اطلاعات وجود دارد؟ آیا می توان آنها را از دسترسی هکرها و یا ویروس‌ها دور نگاه داشت؟ آیا امکان ارسال و دریافت داریم اطلاعات به صورت امن وجود دارد؟	نگاه‌داری،ارسال و دریافت اطلاعات
آیا مدافعین شاهدان رویدادهایی هستند که می توانند اتهاماتی علیه یک عامل قدرتمند را مطرح کنند؟ آیا مدافعان اطلاعات منحصربه‌فرد و ارزشمندی در مورد یک پرونده خاص، موضوعی خاص و یا فرآیندی مهم را دارا هستند؟	شاهد بودن و یا داشتن اطلاعات کلیدی
آیا مدافعان توصیفی جامع،قابل دوام (غیرمتغیر) و واضح در مورد فعالیت‌ها و اهداف خود دارند؟ آیا این شرح و توصیف از سوی همه یا اغلب فعالان دخیل (به ویژه فعالان مسلح) قابل قبول یا حداق قابل تحمل است؟ آیا تمامی اعضای گروه از توانای تشریح اهداف و فعالیت‌های خود در صورت لزوم برخوردارند؟	توضیح و تشریح جامع و قابل قبول فعالیت‌ها و اهداف

مولفه‌های سازمانی و اجتماعی

آیا گروه ساختار و سازماندهی مناسبی دارد؟ آیا این سازماندهی هماهنگی و وابستگی قابل قبولی را در گروه ایجاد می کند؟	وجود یک ساختار گروهی
آیا ساختار گروه نشانگر منافع خاص بوده و یا منافع گروه را در بر می گیرد (دامنه اعضا و گسترش آن)؟ آیا وظایف اصلی و یا اتخاذ تصمیمات صرفا به یک یا چند نفر محول می‌شوند؟ آیا سیستم‌های جایگزین برای تصمیم‌گیری و پذیرش مسوولیت‌ها وجود دارند؟ اتخاذ تصمیمات تا چه حد بر اساس اصول مشارکتی است؟ آیا ساختار گروه امکان :الف)تصمیم گیری و اجرای تصمیمات به صورت مشترک ب)بررسی و بحث‌های گروهی در مورد مسائل ج) جلسات غیرموثر و زاید و د) هیچ یک از موارد بالا را فراهم می‌سازد؟	توانایی اتخاذ تصمیمات مشترک

اطلاعات مورد نیاز برای ارزیابی آسیب‌پذیری‌ها و ظرفیت‌های مرتبط با هر مولفه	مولفه‌های آسیب‌پذیری‌ها و ظرفیت‌ها
آیا قوانین امنیتی و دستورالعمل‌ها مرتبط آن اجرا می‌شوند؟ آیا درک گسترده‌ای از دستورالعمل‌های امنیتی وجود دارد؟ آیا افراد از این قواعد امنیتی پیروی می‌کنند؟ (برای جزئیات بیشتر به فصل ۸ مراجعه کنید)	طرح‌های امنیتی و دستورالعمل‌ها
مدافعین چگونه زمان خود را در خارج از محیط کار می‌گذرانند؟ (خانواده و اوقات آزاد). الکل و مواد مخدر را باید آسیب‌پذیری‌های جدی در نظر گرفت. روابط هم می‌توانند آسیب‌پذیری (و البته همزمان نقطه قوت) محسوب شوند.	مدیریت امنیت در خارج از محیط کار (وقت آزاد و خانواده)
آیا تمامی افراد دارای قراردادهای کار هستند؟ آیا به منابع مالی اضطراری دسترسی دارید؟ آیا افراد بیمه هستند؟	شرایط کاری
آیا دستورالعمل مناسبی برای استخدام پرسنل، همکاران و یا اعضا وجود دارد؟ آیا در مورد داوطلبان موقتی (مانند دانشجویان) یا بازدیدکنندگان از سازمان هم رویکرد امنیتی خاص وجود دارد؟	استخدام افراد
آیا فعالیت شما در ارتباط مستقیم با مردم صورت می‌گیرد؟ آیا این مردم را به خوبی می‌شناسید؟ آیا سازمانی به عنوان واسطه ارتباطی شما با مردم عمل می‌کند؟	کار با افراد و یا موسسات واسطه
آیا مخاطراتی را که متوجه قربانیان و یا شاهدان مرتبط با موضوعی که ما مشغول فعالیت پیرامون آن هستیم، ارزیابی کرده‌اید؟ آیا معیارهای امنیتی خاصی هنگام ملاقات با آنها به دفترها معمول می‌شود؟ اگر آنها تهدیدی دریافت کنند، واکنش ما چگونه خواهد بود؟	حفاظت از شاهدان یا قربانیانی که با آنها کار می‌شود
آیا مدافعین از لحاظ اجتماعی به صورتی مناسب در منطقه جا افتاده‌اند؟ آیا گروه‌های اجتماعی خاصی وجود دارند که فعالیت‌های مدافعین را مناسب تشخیص دهند؟ آیا مدافعین توسط افرادی که به صورت بالقوه نسبت به فعالیت آنان رویکرد خصمانه‌ای دارند، محاصره شده‌اند؟ (وجود افرادی مانند خبرچین‌ها در همسایگی مدافعین و ...)	محیط پیرامونی و شرایط اجتماعی منطقه
آیا مدافعین از توانایی ایجاد انگیزه و تحرک در افراد برای فعالیت‌های اجتماعی برخوردارند؟	ظرفیت تحرک

مولفه‌های روان‌شناختی (افراد یا گروه)

ا افراد کلیدی، یا گروه به صورت یک مجموعه، در مورد کار خود احساس اطمینان دارند؟ آیا افراد به وضوح به حس اتحاد و هدف مشترک در مورد فعالیت‌های خود (در گفتار و رفتار) دست یافته‌اند؟ آیا سطح تنش ارتباط مناسب میان افراد یا روابط بین‌شخصی را تحت‌الشعاع قرار داده است!؟	توانایی مدیریت ترس و تنش

اطلاعات مورد نیاز برای ارزیابی آسیب‌پذیری‌ها و ظرفیت‌های مرتبط با هر مولفه	مولفه‌های آسیب‌پذیری‌ها و ظرفیت‌ها
آیا احساس افسردگی و سرخوردگی یا از دست دادن را می‌توان به وضوح در رفتار و گفتار افراد مشاهده کرد؟	احساس ناامیدی و یاس شدید

منابع فعالیت

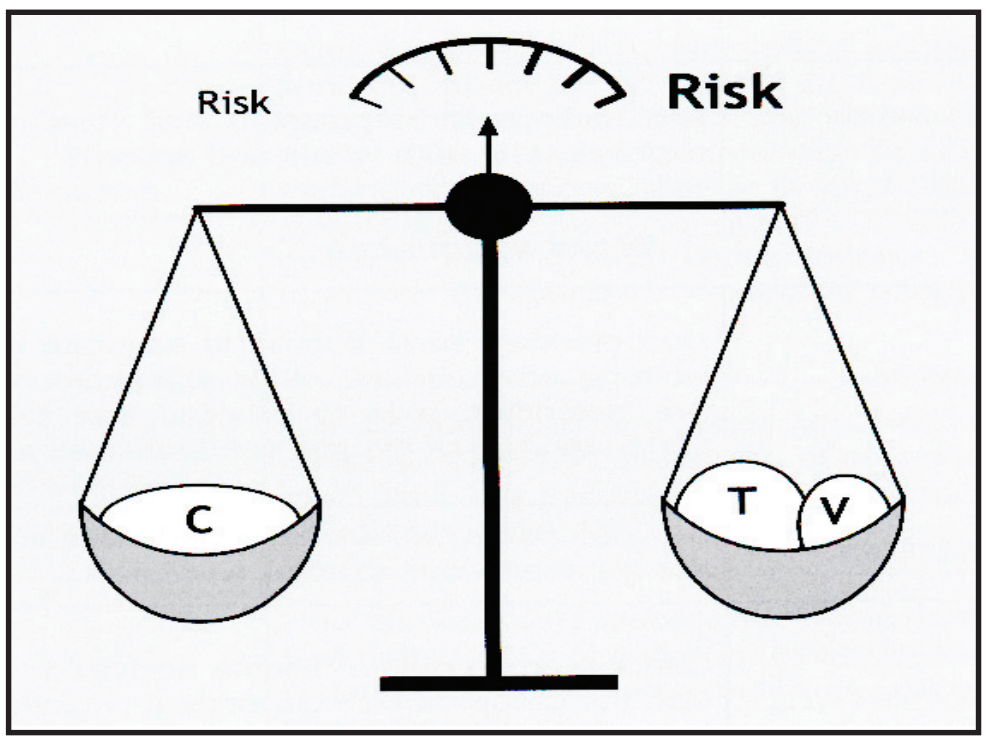
آیا مدافعین به اطلاعات دقیق در مورد محیط کاری خود، سایر فعالان دخیل و منافع آنان دسترسی دارند؟ آیا مدافعین از توانایی پردازش این اطلاعات و رسیدن به درکی از تهدیدات، آسیب‌پذیری‌ها و ظرفیت‌ها برخوردارند؟	توانایی درک بستر فعالیت و مخاطرات
آیا مدافعین می‌توانند طرح‌های عملیاتی را تعریف و از آن مهم‌تر اجرا کنند؟ آیا سابقه‌ای از چنین فعالیت‌هایی در گروه وجود داشته است؟	توانایی تعریف طرح‌های عملیاتی
آیا گروه می‌تواند راهنمایی و پیشنهادات قابل اطمینانی به دست آورد؟ آیا امکان کسب این موارد از منابع صحیح وجود دارد؟ آیا گروه می‌تواند به صورت مستقیم در مورد انتخاب منبع تصمیم‌گیری کند؟ آیا به سازمان‌های خاص که ظرفیت حفاظت شما را افزایش دهند دسترسی دارید؟ آیا در چنین سازمان‌هایی عضویت دارید؟	توانایی کسب راهنمایی از منابع مطلع
آیا افراد یا پرسنل موجود و در دسترس با حجم کار مورد نیاز متناسب هستند؟ آیا امکان این را دارید که برای بازدیدهای میدانی از تیم (حداقل دونفر) استفاده کنید؟ افراد و میزان فعالیت آیا منابع مالی لازم را برای تامین امنیت خود در اختیار دارید؟ آیا می‌توانید به صورتی مطمئن پول نقد به دست آورید؟	منابع مالی
آیا با زبانی که در منطقه فعالیت شما به آن صحبت می‌شود آشنایی دارید؟ آیا مشخصات مکانی منطقه فعالیت را شناسایی کرده‌اید؟ (مواردی چون جاده‌ها، روستاها، تلفن‌های عمومی، مراکز بهداشتی و ...)	دانش در مورد زبان‌ها و مناطق

منابع فعالیت

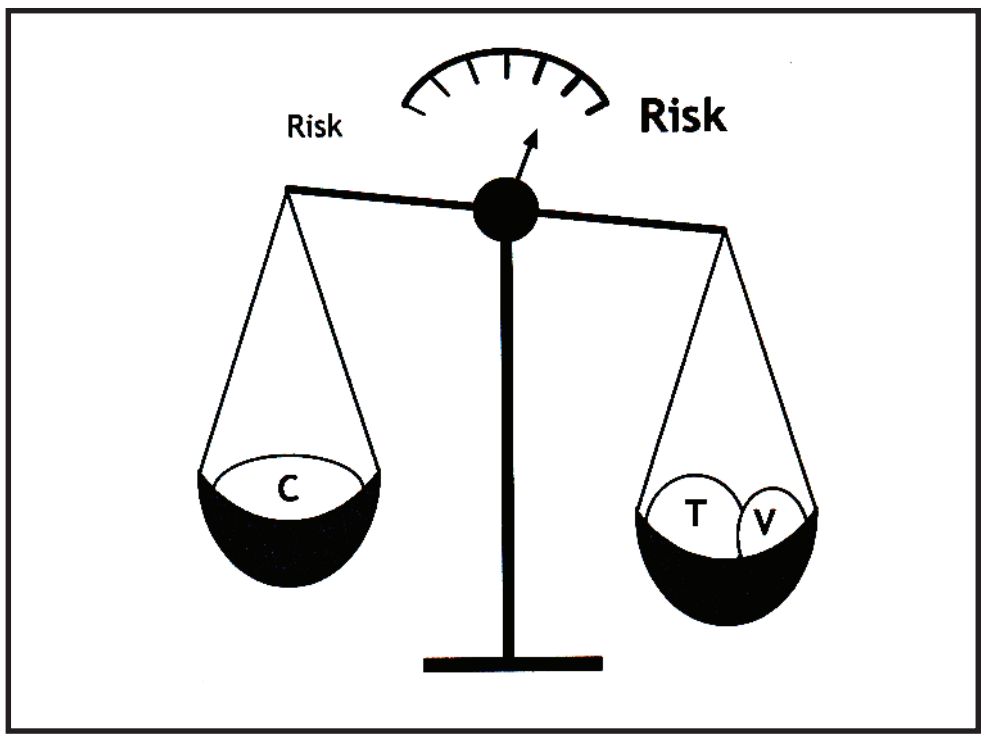
آیا مدافعین دارای رابطین ملی و یا بین‌المللی هستند؟ آیا با هیات‌های اعزامی، سفارتخانه‌ها و سایر دولت‌ها و ... ارتباط دارند؟ آیا با رهبران جوامع، رهبران مذهبی و سایر افراد تاثیرگذار ارتباط دارند؟ آیا در صورت نیاز می‌توانند اقدامی ضروری را از طریق سایر گروه‌ها انجام دهند؟	دسترسی به شبکه‌های ملی و بین‌المللی
آیا مدافعین به رسانه‌ها (ملی و بین‌المللی) دسترسی دارند؟ آیا با سایر رسانه‌ها (رسانه‌های مستقل) ارتباط دارند؟ آیا مدافعین می‌دانند چگونه ارتباطی مناسب با رسانه‌ها برقرار کرده و آن را مدیریت کنند؟	دسترسی به رسانه‌ها و توانایی کسب نتیجه

مقیاس مخاطرات: روشی دیگر برای درک مخاطرات

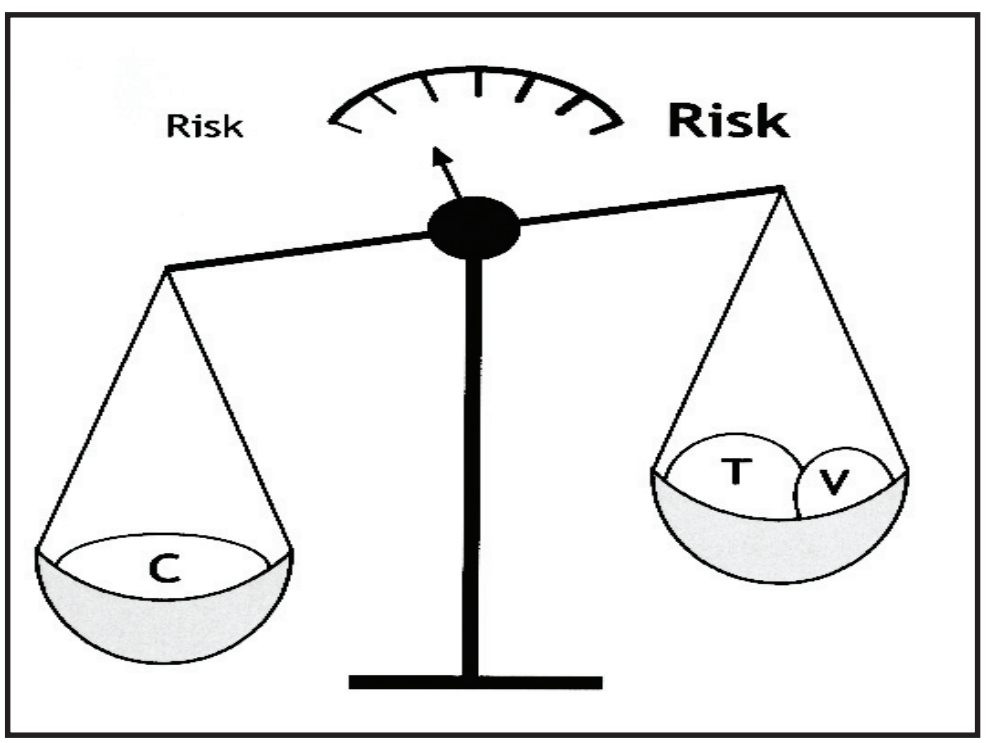
برای درک مفهموم مخاطره، می‌توان از ترازو استفاده کرد! استفاده نمادین از این ابزار که ما می‌توانیم آن را "مخاطره‌سنج" بخوانیم، درک بسیاری از مسائل را تسهیل خواهد کرد. اگر ما دو جعبه را که در یکی از آنها تهدیدات و آسیب‌پذیر های ما قرار گرفته و در دیگری ظرفیت‌هایمان را قرار داده‌ایم در دو کفه ترازو قرار دهیم، می‌توانیم به وضوح افزایش و یا کاهش مخاطرات را مشاهده کنیم.



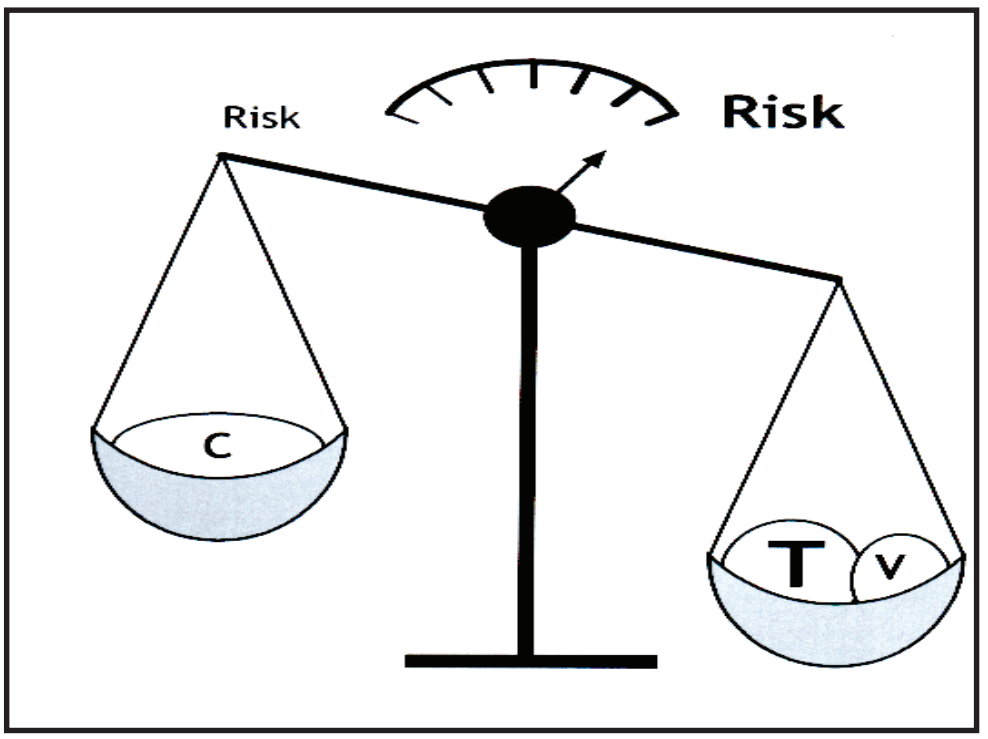
هر چه میزان تهدیدات و آسیب‌پذیری‌ها افزایش یابند ما با مخاطره بیشتری روبه‌رو می‌شویم.



هر چه میزان ظرفیت‌های ما افزایش یابد، با مخاطره کمتری مواجه شده برای کاهش مخاطرات باید یا تهدیدات آسیب‌پذیری‌های خود را کاهش داده و یا ظرفیت‌ها را افزایش دهیم.



اما ... توجه کنید وقتی که ما با تهدیدات بزرگی روبه‌رو می‌شویم،فارغ از آنکه بلافاصله به فکر افزایش ظرفیت‌هایمان بیافتیم، مخاطره منبع ما بهر حال سطح بالایی از مخاطره را نشان می‌دهد!



فصل سوم
درک و برآورد تهدیدات

هدف:

کسب درکی عمیق از تهدیدات و نحوه واکنش به آن

برآورد تهدیدات: درک عمیق تهدیدات

سرکوب مدافعین حقوق بشر عموما حول مسائل روانی شکل می‌گیرد. تهدیدات در این میان معمولا برای آن به کار گرفته می‌شوند که مدافعین را دچار احساس آسیب‌پذیری، اضطراب، سردرگمی و درماندگی کنند. درنهایت هدف از سرکوب درهم شکستن سازمان‌های است و سلب اعتماد مدافعین نسبت به رهبران و همکاران خود. مدافعین باید خط فاصل باریکی میان مدیریت دقیق و مناسب تهدیدات و رسیدن به حس امنیت در محیط کار بکشند. این موضوع اصلی فصل حاضر است.

در فصل ۲ تهدید به صورت "احتمال لطمه زدن به انسجام فیزیکی، روانی و یا مالی شخصی توسط فردی دیگر از طریق اعمال هدفمند و آگاهانه و معمولا خشن تعریف شد، همچنین در مورد تهدیدات "**احتمالی**" (هنگامی که یک مدافع در نزدیک محل فعالیت شما مورد تهدید قرار گرفته به همین علت منطقی است تصور کنیم که شما هم ممکن است نفر بعدی باشید که مورد تهدید قرار می گیرد) و تهدید "**اعلام شده**" (دریافت نامه تهدید مرگ و ...) صحبت کردیم. اکنون به بررسی نحوه تعامل با **تهدیدات اعلام شده** می‌پردازیم.

تهدید اعلام شده معمولا **اعلام یا نشانه‌ای از قصد برای آزاررسانی، تخریب، تنبیه و یا صدمه زدن به منظور تحقق امری معین** است. مدافعین حقوق بشر با چنین تهدیداتی به علت تاثیر فعالیت‌های خود روبه‌رو می‌شوند. اغلب این تهدیدات معمولا هدف خاصی را دنبال می‌کنند؛ بازداشتن مدافع از تعقیب فعالیت خود یا وادار کردن وی به انجام کاری.

تهدیدات همواره **مراجع** خاص خود را دارند. مرجع تهدید، گروه یا شخص خاصی است که از فعالیت مدافع تاثیر پذیرفته ولذا اکنون تهدیدی را متوجه وی می کند. تهدیدات همچنین اهداف خاص خود را دارند. هدف از تهدید معمولا بستگی به فعالیت مدافع داشته و براساس آن تعریف می‌شود. تهدیدات در نهایت "**ابزار بیان**" دارند. ابزار بیان نحوه آگاه کردن مدافع از تهدید است.

تهدیدات فریبنده هستند. شاید با درهم آمیختن کمی طنز بتوان گفت که تهدیدات معمولا اکولوژیک هستند! به عبارت دیگر هدف از تهدید کسب و تحقق حداکثر نتایج و با نتیجه‌ای حداکثری به حداقل صرف انرژی است. فردی که به تهدید روی می‌آورد، در حقیقت تهدید را جایگزین اقدام عملی- مستلزم صرف انرژی بیشتری است- می کند. چرا؟ ممکن است بتوان دلایل متعددی را برشمرد. آشنایی با این دلایل قطعا می‌تواند مفید باشد:

- شخص تهدید کننده دارای ظرفیت اقدام عملی است اما تا حدی نگران هزینه سیاسی اقدام آشکار علیه یک مدافع حقوق بشر است. در این شرایط معمولا از تهدیدات ناشناس استفاده می‌شود.
- شخص تهدید کننده دارای ظرفیت محدودی برای اقدام عملی است و قصد دارد با پوشاندن فقدان ظرفیت خود در پشت تهدیدات، اهداف بزرگتری را محقق کند. این ظرفیت محدود البته ممکن است موقتی و یا ناشی از اولویت‌بندی اهداف باشد، همچنانکه ممکن است دائمی باشد. بهر حال در هر دو حالت ممکن است وضعیت فعلی (کمبود ظرفیت) تغییر کرده و تهدید در آینده تبدیل به اقدام عملی علیه مدافع شود.

تهدید یک تجربه شخصی است و همواره بر انسان تاثیر خاص خود را می‌گذارد. به عبارت بهتر تهدیدات به هر حال بر افراد اثر می‌گذارند. یکی از مدافعین حقوق بشر می‌گفت: تهدیدات، حتی هنگامی که صرفا صحبت از تهدیدات می‌شود، باز هم بر انسان تاثیر می‌گذارند. در واقع تهدیدات دارای اثری دوگانه هستند؛ اثری عاطفی و اثری امنیتی. ما در اینجا بر اثرات امنیتی متمرکز می‌شویم، اما بدیهی است که به هیچ‌وجه نباید ابعاد عاطفی هر تهدیدی را فراموش کرد.

هر تهدیدی معمولا با تاثیر فعالیت‌های ما مرتبط است. بدین ترتیب دریافت تهدید را می‌توان بازخوردی از نحوه و میزان تاثیر فعالیت شما بر شخصی خاص دانست. اگر از این زاویه به مسائل بنگرید، تهدیدات منبعی گران‌قیمت و غیرقابل ارزشگذاری از اطلاعات هستند و باید به دقت مورد بررسی و تحلیل قرار گیرند.

"بیان" تهدید در برابر "اجرای" تهدید

مردم به دلایل متعدد و متفاوت مدافعین حقوق بشر را مورد تهدید قرار می‌دهند اما تنها برخی از آنها قصد و یا ظرفیت انجام عملی خشونت‌آمیز را دارا هستند. با این وجود برخی افراد بدون حتی بر زبان آوردن تهدید می‌توانند تهدیدی جدی را متوجه مدافعان کنند. بدین ترتیب تمییز قائل شدن میان بیان تهدید و اجرای آن بسیار حایز اهمیت است:

- برخی افراد تهدید کرده و در نهایت تهدید خود را اجرا می‌کنند.
- برخی افراد تهدید می‌کنند، اما تهدید خود را اجرا نمی‌کنند.
- برخی افراد که هرگز تهدیدی را بر زبان نمی‌آورند، عملا تهدید خود را اجرا می‌کنند.

تهدید را باید تنها در حالی جدی گرفت که شخص پشت آن دارای توانایی و ظرفیت اقدام علیه شما باشد. تهدید باید در خود نمادی از سطحی حداقل از نیرو و یا عنصری تهدید کننده برای برانگیختن هراس داشته باشد. شخص تهدید کننده می‌تواند ظرفیت خود را به سادگی به نمایش بگذارد. او برای مثال می‌تواند تهدیدی مکتوب را در داخل خودرویی قفل شده قرار دهد- به ویژه هنگامی که شما تنها برای چند لحظه خودروی خود را در مکانی پارک می‌کنید- و یا به محض رسیدن به منزل با تماس تلفنی شما را تهدید کند- و نشان دهد که شما تحت حفاظت او هستید-.

افراد می‌توانند با به کارگیری برخی عناصر نمادین در تهدیدات خود، هراس را در شما ایجاد کنند. برای نمونه ارسال دعوتنامه‌ای برای شرکت در مراسم تدفین خود و یا گذاشتن جسد بی‌جان حیوانی بر روی پلکان ورودی منزل و یا روی تخت شما، روش‌هایی برای القای هراس تلقی می‌شوند.
برخی تهدیدات دارای ترکیبی از مشخصه‌های فوق هستند. در این جا اهمیت تمییز قائل شدن میان انواع تهدیدات بیش از پیش می‌شود چرا

که برخی از افراد هنگام ارسال تهدید سعی می کنند تا با استفاده از عناصر نمادین و هراس آفرین تظاهر به داشتن ظرفیت عملی کردن تهدید خود نمایند.

همه می تواند تهدید کنند، اما هرکسی نمی تواند تهدید خود را اجرا کند

شما در پایان روز باید بتوانید به این برداشت برسید که آیا تهدیدی که شما با آن مواجه شده‌اید، عملی می‌شود یا خیر؟ اگر شما به صورت منطقی اطمینان حاصل کنید که عملی شدن تهدید دور از ذهن و بعید است، قطعا رفتار شما کاملا متفاوت از زمانی خواهد بود که فکر کنید این تهدید به هر حال تا حدی ریشه در واقعیات داشته یا به عبارت بهتر امکان عملی شدن آن وجود دارد.

دو هدف اصلی شما هنگام برآورد تهدید باید موارد زیر باشند:

- ☐ دسترسی به حداکثر اطلاعات ممکن در مورد علت و مرجع تهدید (هر دو مورد قطعا با فعالیت شما مرتبط هستند)
- ☐ رسیدن به نتیجه‌ای منطقی در مورد امکان عملی شدن یا نشدن تهدید

پنج گام برای برآورد تهدید

۱ ☐ شناسایی واقعیت پیرامون تهدید (یا تهدیدات)

دانستن آنچه که روی داده از اهمیت بسیاری برخوردار است. این امر می تواند با گفت‌و گوهای متعدد و یا با پرسیدن سوالاتی در مورد افراد کلیدی و یا گاه از طریق گزارشات مرتبط حاصل شود.

۲ ☐ شناسایی الگوی احتمالی تهدیدات

اگر با چندین تهدید متوالی مواجه شده‌اید (که معمولا این گونه است)، یافتن الگوهای مشابه اهمیت بسیاری دارد. برای نمونه ابزارهای تهدید (رساندن تهدید به شما)، زمان‌های تهدید، نمادها و سمبل‌های به کار گرفته شده و اطلاعاتی که به صورت شفاهی و یا کتبی از سوی تهدید کننده ارائه می‌شود، هر یک می توانند الگوی تهدیدات را شکل دهند. البته بدیهی است که همیشه امکان شناسایی چین الگوهایی وجود ندارد، اما به هر حال وجود احتمالی آنها می‌تواند در برآورد تهدیدات موثر باشد.

۳ ☐ شناسایی هدف تهدید

تهدید همواره هدف معینی را تعقیب می کند، هدف مرتبط با تاثیر فعالیت شما، با تعقیب آثار فعالیت خود، به عنوان یک سرنخ ممکن است هدف نهایی تهدید- یا هدفی را که قرار است تهدید شما آن را محقق کند- را شناسایی کنید.

۴ ☐ شناسایی تهدیدکننده

بدیهی است که این امر تنها پس از طی سه گام نخست امکان‌پذیر است. سعی کنید تا حد ممکن دقیق و واضح عمل کنید. برای مثال می‌توانید به این نتیجه برسید که "دولت" شما را تهدید می کند. اما با توجه به اینکه هر دولتی عملا مجموعه‌ای پیچیده از بازیگران است، بهتر است دریابید که چه بخشی از دولت عامل تهدید کننده شماست. فعالانی چون "نیروهای امنیتی" و "گروه‌های چریکی" نیز فعالان پیچیده‌ای هستند. به خاطر داشته باشید که حتی یک تهدید امضا شده عهم ممکن است جعلی و ساختگی باشد. این امر حتی می‌تواند به عنوان راهی موثر توسط شخصی که تهدیدات را متوجه شما کرده است، جهت فرار از هزینه‌های سیاسی و فراتر از آن تحقق هدف خود در برانگیختن هراس در درون مدافعین و در نهایت ممانعت و از تعقیب فعالیت‌هایش، مورد استفاده قرار می گیرد.

۵ ☐ تصمیم گیری منطقی در مورد عملی یا غیرعملی بودن تهدید

خشونت مشروط است. هرگز نمی‌توانید مطمئن باشید که یک تهدید عملی شده و یا هرگز عملی نمی‌شود. پیش‌بینی در مورد خشونت در واقع بررسی و تخمین احتمال اقدام خشن یک گروه یا شخص علیه هدفی معین، با درنظر گرفتن شرایط خاص موجود است.

مدافعین حقوق بشر قطعا پیشگو نیستند و نمی‌تواند تظاهر کنند که در مورد آنچه قرار است روی دهد اطلاع دارند. با این وجود ممکن است شما به این نتیجه منطقی برسید که آیا امکان عملی شدن تهدیی خاص وجود دارد یا خیر؟

اگر حتی پس از طی چهار گام شرح داده شده نتوانستید اطلاعات کافی در مورد تهدیدی که متوجه شما شده کسب کنید بالطبع قادر نبودید به نتیجه‌ای نهایی برسید و یا اگر در مورد میزان "واقعی" بودن تهدیدات یا به عبارت بهتر احتمال اجرا و عملی شدن آنها، به هیچ‌وجه مطمئن نبودید، باید با درنظر گرفتن بدترین سناریوی ممکن اقدام کنید.

مثال

یک فعال حقوق بشر با تهدید مرگ مواجه شده است، گروه تهدید را مورد تحلیل قرار داده و به دو نتیجه متضاد می‌رسد. برای اثبات هر دو نتیجه هم دلایل و شواهد کافی موجود است. برخی می گویند این تهدید کاملا ساختگی و غیرواقعی است در حالی که سایرین معتقدند علائم نگران کننده ای دال بر احتمال عملی شدن آن مشاهده می‌شود. در پایان جلسه، گروه تصمیم می گیرد بدترین سناریوی ممکن را در نظر بگیرد، حالتی که در آن تهدید عملی فرض می شود؛ و بر اساس این فرض اقدامات امنیتی را پیش بینی کنید.

این برآورد تهدید از بررسی واقعیات مسلم (گام اول) آغاز شده و به مرحله استدلال های منطقی ذهنی می‌رسد. گام دوم شامل تعبیر و تفسیر واقعیات است این مرحله در گام‌های ۳ تا ۵ هم به صورت فزاینده‌ای تکرار می‌شوند.

برای رعایت سلسله مراتب و حرکت منظم دلایل منطقی بسیاری را می‌توان مطرح کرد. برای مثال اگر قرار باشد ناگهان از گام دوم به گام چهارم جهش کنید، بخشی از اطلاعاتی را که در گام سوم به آنها دست می‌یافتید، از دست خواهید داد.

حفظ هوشیاری و خاتمه بخشیدن به تهدید

یک تهدید یا رویدادی امنیتی می‌تواند گروه مدافعین را هوشیار کند، اما معمولا حفظ این هوشیاری تا زمان خاتمه تهدید کاری دشوار است، نظر به فشارهای فزاینده خارجی که بر مدافعین تحمیل می‌شود، به صدا در آوردن مداوم زنگ خطر می‌تواند باعث بی‌توجهی تدریجی و بی‌اعتنایی فزاینده گروه به مسائل امنیتی شود.

بالا بردن سطح هوشیاری تنها باید با استناد به شواهد قابل تکیه و با تمرکز بر مسائل خاص صورت گیرد. این امر باید به گونه‌ای طراحی شود که تمامی اعضای گروه به فعالیت داشته شده و مجموعه‌ای پیش بینی شده و معین از اقدامات صورت گیرد. تحرکات و فعالیت‌های متناظر با این مساله باید به گونه‌ای معتدل طراحی شوند، تحرک پایین باعث می‌شود که افراد عملا توجهی به موضوع نکنند و تحرک بیش از اندازه هم باعث ازدیاد بار روانی و عاطفی افراد می‌شود. اگر قرار است تهدید نه به صورت مقطعی که به صورت مداوم متوجه گروه باشد، لازم است که به افراد در این مورد اطلاع داده شده باشد و نیز تصحیح راهکارها و توصیه‌های نادرست اولیه، اقدامات عاجل صورت گیرد. تصحیح اطلاعات و راهکارها و توصیه‌های نادرست و جایگزینی آنها با موارد صحیح می‌تواند باعث افزایش اعتماد گروه به موثر بودن اقدامات مشترک در مقابله با تهدیدات شود.

در نهایت اما اگر تهدید جنبه عینی به خود نگرفت، باید توضیحاتی در مورد علت این امر به گروه ارائه شده و افراد نسبت به علت کاهش تهدید

و یا رفع آن توجیه شوند.

شما هنگامی می‌توانید پرونده یک تهدید را خاتمه‌یافته تلقی کنید که مهاجم بالقوه اجرا کننده تهدید حضورش به شدت کمرنگ شده باشد به نحوی که عملا دیگر نتواند تهدید خود را اجرا کند. امکان خاتمه یافته تلقی کردن یک تهدید، در حالت ایده‌آل، هنگامی وجود دارد که شما بتوانید به صورت منطقی توجیهی برای رفع تهدید بیابید. به عبارت دیگر تنها هنگامی که بتوانید دلایل و یا شواهدی مستند در اثبات ادعای خود مبنی بر رفع تهدید یافته و ارائه کنید، می‌توانید پرونده تهدید را مختومه فرض کنید. هر چند حتی در این زمان هم باید از خود بپرسید که در چه شرایطی (یا به عبارت بهتر با چه تغییری در شرایط) ممکن است شخصی که پشت تهدیدات قرار داشته، بار دیگر به سمت اعمال خشن و اجرای تهدیدات خود حرکت کند.

واکنش به تهدیدات براساس تعاریف امنیتی

- ☐ هر تهدیدی را می‌توان رویداد امنیتی تلقی کرد. برای کسب اطلاعات بیشتر در مورد واکنش به رویدادهای امنیتی به فصل چهارم مراجعه کنید.
- ☐ برآورد تهدیدات بیان شده شاید شما را به این نتیجه برساند که ممکن است مورد حمله قرار گیرید. برای کسب اطلاعات بیشتر در زمینه ممانعت از حمله به فصل پنجم مراجعه کنید.

فصل چهارم

رویدادهای امنیتی: تعریف و تحلیل

هدف:

آشنایی با نحوه شناسایی و واکنش در برابر رویدادهای امنیتی

رویداد امنیتی چیست؟

یک رویداد امنیتی را می‌توان به سادگی به صورت **هر رویداد یا واقعیتی که به باور شما بر امنیت شخصی شما و یا سازمان متبوعه‌تان تاثیر می‌گذارد** تعریف کرد.

مواردی از این رویدادهای امنیتی را می‌توان در مشاهده یک خودروی ثابت و مشکوک که روزهای متعدد در مقابل منزل یا دفتر کار شما پارک شده است، تلفن‌های بدون پاسخ شبانه به محل اقامت شما، حضور شخصی که در نزدیکی محل کار و یا زندگی شما- یا حتی روستای مجاور- در مورد شما پرسش‌هایی را مطرح کرده است، ورود مخفیانه افراد به محل کار یا منزل شما و ... یافت.

بدیهی است که هر رویدادی که توجه شما را به خود جلب کند را نمی‌توان یک رویداد امنیتی تلقی کرد. بدین ترتیب شما با مشاهده رویدادی که احساس می‌کنید معنا و مفهوم خاصی برای امنیت شما و یا سازمانتان دارد آن را "**ثبت**" کنید و سپس نسبت به "**تحلیل**" آن اقدام کنید. در مورد تحلیل این حوادث حضور همکاران می‌تواند در برآورد منطقی از تاثیر چنین رویدادهایی بر امنیت شما تاثیرگذار باشد. پس از تحلیل نوبت "**واکنش**" رویداد می رسد. سیر اقدامات در برابر یک رویداد امنیتی را بدین ترتیب می‌توان به صورت زیر خلاصه کرد.

باور شما مبنی بر اینکه می‌توان آن را رویدادی امنیتی تلقی کرد<< جلب توجه شما به چیزی << رسیدن به این نتیجه که با یک رویداد امنیتی مواجه هستید<< ثبت رویداد یا در میان گذاشتن آن با دیگران<< واکنش متناسب در قبال رویداد

بدیهی است هر چقدر رویداد جدی‌تر باشد باید سلسله مراتب با سرعت بیشتری صورت گرفته و از هر نوع تاخیری در انجام آن پرهیز شود.

تفاوت میان رویدادهای امنیتی و تهدیدات

اگر شما در انتظار اتوبوس هستید و شخص مجاور، شما را به خاطر کار و فعالیت‌تان تهدید می‌کند، این امر را گذشته از تهدیدی که دربردارد، باید یک رویداد امنیتی قلمداد کرد، اما اگر کشف کرده‌اید که دفتر شما توسط ماشین پلیس پارک شده در روبه‌روی ساختمان تحت نظر قرار دارد، یا تلفن همراه شما به سرقت رفته است، این موارد را باید رویدادهای امنیتی- و نه الزاما تهدید- تلقی کرد. به خاطر داشته باشید که تهدیدات هدفمند هستند (فصل دوم) ولی رویدادها معمولا پیشامدهایی هستند که اغلب بی‌هدف اتفاق می‌افتند.

تمامی تهدیدات را باید رویدادهای امنیتی تلقی کرد اما تمامی رویدادهای امنیتی، تهدید نیستند.

علت اهمیت رویدادهای امنیتی

توجه به رویدادهای امنیتی برای تامین امنیت ضروری است چرا که **این رویدادها حاوی اطلاعات گران بهایی در مورد نحوه تاثیرگذاری فعالیت شما بوده و همزمان سرنخ‌هایی از این اقدامات احتمالی که ممکن است علیه شما برنامه‌ریزی و یا اجرا شوند**، می‌باشند. رویدادهای امنیتی همزمان به شما امکان می‌دهند رفتار و یا نوع فعالیت‌هایتان را تغییر داده و از مناطقی که می‌توانند خطرپذیر- و یا پرخطرتر از حد معمول- باشند، پرهیز کنید.

فرض کنید شما پس از مشاهده چندین رویداد امنیتی متوجه می‌شوید که تحت حفاظت قرار گرفته‌اید. اکنون باید واکنش مناسب و متناسب در قبال این حفاظت نشان دهید.

رویدادهای امنیتی نشاندهنده میزانی حداقلی از "معیارهای امنیتی" هستند و به عبارت دیگر چنین رویدادهایی حاکی از آن هستند که فعالیت‌های شما با مقاومت روبه‌رو شده و یا شما تحت فشار قرار گرفته‌اید.
هرگز بدون توجه و به سادگی از کنار این رویدادها نگذرید!

چه زمانی و چگونه باید به رویدادهای امنیتی توجه کرد؟

همه چیز بستگی به میزان آشکار بودن- یا جدی بودن- رویداد دارد. گاه ممکن است نیازی به توجه خاص به رویدادی وجود نداشته باشد. به هر حال توانایی شما در شناسایی رویدادهای امنیتی و میزان توجهی که باید به آن معطوف شود، از میزان آموزش‌های امنیتی، تجارب و سطح هوشیاری شما نشات می‌گیرد.

هر چه سطح هوشیاری و آموزش شما بالاتر باشد، رویدادهای کمتری ممکن است از چشم شما دور بماند

رویدادهای امنیتی در اغلب موارد جدی گرفته نمی‌شوند، توجه چندانی به آنها معطوف نمی‌شود و با نگاهی گذرا و اجمالی با آنان برخورد می‌شود. در نقطه مقابل اما گاهی افراد واکنش‌هایی بسیار شدید در برابر آنچه که باورشان رویدادی امنیتی است، نشان می‌دهند.

چگونه ممکن است رویدادی امنیتی از نظر شما دور بماند؟

مثال

شرایطی را در نظر بگیرید که یک مدافع حقوق بشر رویدادی امنیتی را پشت‌سر می‌گذارد، اما سازمان متبوعه او در برابر این رویداد هیچ واکنشی نشان نمی‌دهد. علت را می‌توان در میان موارد زیر جست‌و جو کرد:

- مدافع خود آگاه نیست که رویدادی امنیتی حادث شده است
- مدافع در این مورد آگاه است اما آن را جدی نمی‌گیرد
- مدافع به سازمان اطلاع نداده است (فراموش کرده، این کار را لازم تلقی نمی‌کند یا چون این حادثه را ناشی از اشتباه خود می‌داند، می‌خواهد با سکوت بر آن سرپوش بگذارد)
- سازمان پس از ارزیابی گروهی رویداد- پس از ثبت آن توسط مدافع در دفترچه رویدادها- اقدامی را ضروری نمی‌داند.

چرا گاهی افراد در برابر رویدادهای امنیتی واکنش بیش از حد نشان می‌دهند

مثال

شرایطی را در نظر بگیرید که همکار شما دائما در مورد رویدادهای امنیتی و یا مسائل مشابه صحبت می‌کند اما ارزیابی گفته‌های وی در نهایت نشان می‌دهد که یا این موارد ارزش چندانی نداشته- شک در ماهیت رویداد- و یا در تعریف رویدادهای امنیتی نمی‌گنجند. در چنین وضعیتی رویداد امنیتی واقعی را باید این واقعیت دانست که همکار شما دارای مشکلی است که باعث می‌شود او دچار توهم رویدادهای امنیتی غیر موجود شود. به عبارت دیگر او رویدادهایی عادی را رویداد امنیتی تلقی می‌کند. این امر می‌تواند ناشی از ترس بیش از حد او و یا تنش‌های تحمیل شده بر او باشد. این مشکل با ارائه کمک قابل حل است.

فراموش نکنید که در اغلب موارد افراد از کنار رویدادهای امنیتی، بدون توجه لازم گذشته و یا با نگاهی گذرا و اجمالی با آن برخورد می‌کنند.

تعامل با رویدادهای امنیتی

برای تعامل با رویدادهای امنیتی باید سه گام زیر را طی کنید:

۱ ☐ ثبت رویدادها:

رویدادهای امنیتی که توسط هر یک از مدافعین مشاهده می‌شوند، باید ثبت شوند. ثبت رویدادها می‌تواند در دفترچه‌های عادی صورت گیرد. نکته مهم این است که تمامی افراد باید امکان دسترسی به دفترچه را داشته باشند.

۲ ☐ تحلیل رویدادها:

تمامی رویدادهای امنیتی ثبت شده باید بلافاصله- یا در فواصل زمانی معین و منظم- مورد تحلیل قرار بگیرند. بهتر است کار تحلیل به صورت گروهی انجام شود تا فردی. در این شرایط امکان عدم توجه به ابعاد مختلف رویداد را به حداقل می‌رسد. باید شخصی مسوول حصول اطمینان از بررسی دقیق تمامی رویدادهای امنیتی شود.

همچنین باید در مورد اینکه آیا لازم است در مورد برخی رویدادهای خاص (مانند تهدیدات) مخفیکاری کرده و آنها را سری قلمداد کرد یا خیر، تصمیم گیری شود. آیا پنهان کردن تهدید از همکاران و یا افرادی که مرتبط با شما فعالیت می‌کنند، اخلاقی و یا واقع گرایانه است؟ بدیهی است نمی‌توان قاعده‌ای یکسان و ثابت را برای تمامی حملات توصیه کرد، اما بهر حال عموما بهتر است در چنین مواردی تا حد امکان باز برخورد کرد و همزمان با تشریک اطلاعات، نگرانی‌های منطقی و هراس‌ها را هم با سایر اعضا در میان گذاشت.

۳ ☐ واکنش به رویدادها:

- با توجه به اینکه رویدادهای امنیتی بازخورد خاص خود را بر فعالیت شما خواهند داشت می‌توان یکی از موارد زیر را محتمل دانست:

واکنش به خود رویداد

- بازخورد رویداد یا به عبارت دیگر تاثیر آن بر نحوه کار، طرح‌ها و یا استراتژی فعالیت

مثال

موردی را در نظر بگیرید که بازخورد یک رویداد امنیتی باعث می‌شود تا شرایط فعالیت شما به صورت امن‌تر مورد توجه قرار گیرد. برای

سومین باز یکی از اعضای سازمان شما به علت همراه نداشتن اوراق لازم، هنگام عبور از ایست‌بازرسی پلیس با مشکل روبه‌رو می‌شود. این امر به علت اینکه اعضا اغلب حمل این اوراق را فراموش می‌کنند، روی می‌دهد. شما تصمیم می‌گیرید تا چک‌لیستی فراهمی کنید که کلیه اعضای سازمان قبل از خروج از شهر باید آن را کامل کنند - و بدین ترتیب مانع بروز رویدادهای مشابه شوید - ممکن است همچنین مسیری را که اعضا برای این گونه مسافرت‌ها طی می‌کنند، تغییر دهید.

مثال

موردی را در نظر بگیرید که بازخورد یک رویداد بر نحوه برنامه‌ریزی شما برای تامین امنیت تاثیر می‌گذارد: در همان ایست‌بازرسی، شما مدت نیم ساعت بازداشت شده و به شما گفته می‌شود که نظر مساعدی در مورد فعالیت‌های شما وجود ندارد. تهدیداتی نه چندان جدی هم به عمل می‌آید. هنگامی که خواهان توجیح در مورد علت چنی رفتاری می‌شوید، بار دیگر همه چیز از اول آغاز می‌شود. پس از پایان بازداشت و برگشت به محل کار، شما درخواست جلسه‌ای گروهی می‌کنید تا برنامه‌های کاری خود را بازبینی نمایید چرا که مشخص است برای تداوم فعالیت‌هایتان باید در آن تغییراتی بدهید. تصمیم می‌گیرید یک‌سری دیدار با بخش خدمات اجتماعی وزارت کشور داشته باشید و همزمانی برخی از ابعاد فعالیت‌های خود را تغییر دهید. در نهایت قرار می‌شود جلساتی هفتگی برای نظارت بر شرایط برگزار شود.

مثال

موردی را در نظر بگیرید که بازخورد رویدادی باعث تغییر استراتژی امنیت شما می‌شود :هنگامی که فعالیت خود را به عنوان مدافعین حقوق بشر در منطقه‌ای جدید آغاز می‌کنید، به‌سرعت تهدید به مرگ می‌شوید. این تهدیدات چند بار تکرار شده و یکی از همکاران شما مورد حمله فیزیکی قرار گرفته و مجروح می‌شود. شما انتظار چنین مخالفتی با فعالیت‌های خود را نداشته‌اید و لذا در استراتژی‌های کلی خود هم آن را مدنظر قرار نداده‌اید. بدین ترتیب مجبورید که استراتژی خود را برای افزایش سطح تحمل فعالیت‌های خود (در منطقه) و همچنین متوقف کردن حملات و تهدیدات بعدی تغییر دهید. برای انجام این کار باید فعالیت خود را برای مدتی تعلیق کرده، از منطقه خارج شده و کل پروژه را مورد بازبینی قرار دهید.

واکنش اضطراری به یک رویداد امنیتی

برای واکنش قطعی به رویدادهای امنیتی چندین راه وجود دارد. مراحل زیر برحسب زمان و نحوه واکنش به یک رویداد، از لحظه گزارش آن، هنگام حدوث و پس از پایان آن، تنظیم شده‌اند.

گام نخست- گزارش رویداد

- ☐ چه چیزی در حال روی دادن است یا روی داده است؟ (ظسعی کنید بر واقعیت‌های موجود تمرکز کنید)
- ☐ این رویداد چه زمان و چه مکانی حادث شده است؟
- ☐ چه کسی در آن دخیل بوده است؟ (در صورت امکان اثبات و یا اطمینان)
- ☐ آیا لطمه و یا صدمه‌ای به افراد یا اموال وارد شده است؟

گام دوم- تعیین زمان واکنش

- ☐ در این جا دو احتمال را باید بررسی کرد

- نیاز به **اقدامی فوری** برای رسیدگی به افراد زخمی شده و یا توقف حمله
- نیاز به **اقدامی سریع** (ظرف چند ساعت یا چند روز آینده) برای ممانعت از بروز رویدادهای امنیتی احتمالی متعاقب رویداد رخ داده
- **واکنش متعاقب** (در چند روز، هفته و یا حتی ماه آینده). اگر شرایط به حالت ثبات رسیده باشد ممکن است نیازی به اقدام فوری یا سریع نباشد. با این وجود پس از هر نوع رویداد امنیتی که نیازمند اقدامی فوری یا سریع است باید "واکنشی متعاقب" نیز با هدف بازگرداندن شرایط کاری به وضعیت اولیه و یا تغییر در محیط فعالیت صورت گیرد

گام سوم- تصمیم گیری در مورد نحوه واکنش و اهداف آن

- اگر واکنش قرار است فوری باشد، اهداف آن مشخص هستند. رسیدگی به حال مجروحین و یا ممانعت از بروز حمله‌ای دیگر
- اگر واکنش قرار است سریع باشد، اهداف توسط تیم مدیریت بحران (یا تحت هر عنوان دیگری) تعیین می‌شوند. در این حالت باید تمرکز بر روی بازگرداندن امنیت لازم برای تاثیرپذیرفتگان از رویداد مزبور باشد

واکنش‌های متعاقب از طریق مکانیسم‌های عادی تصمیم گیری در سازمان بررسی و هدفگذاری می‌شوند. هدف اصلی ما باید بازگرداندن شرایط محیط کاری خارجی به وضعیت امن، بازتعریف دستورالعمل‌های درون‌سازمانی و آمادگی برای واکنش‌های متعاقب به رویدادهای امنیتی باشد.

در هر واکنشی باید امنیت و حفاظت از سایر افراد، نهادها و یا سازمان‌هایی که با شما رابطه کاری دارند، مدنظر قرار گیرد.

اهداف خود را قبل از انجام هر گونه عملی، کاملا مشخص کنید.
کنش قاطعانه مهم است اما مهم‌تر از آن دانستن این موضوع است که چرا باید چنین عملی صورت گیرد.
با تعیین آنچه که می خواهید محقق سازید (اهداف) می توانید نحوه تحقق آن (نحوه عمل) را معین کنید.

مثال

برای نمونه موردی را در نظر بگیرید که گروهی از مدافعین اخباری را کسب کرده‌اند مبنی بر اینکه یکی از همکاران گروه در زمان مقرر به مقصد خود نرسیده‌است. آنها می‌توانند واکنش خود را با تماس با بیمارستان و یا رابطین خود در سازمان‌های غیردولتی و یا مقر سازمان ملل در مجاور خود و یا دفتر پلیس آغاز کنند. اما قبل از شروع، باید بدانند که چه می‌خواهند به‌دست آورند و چه قرار است بگویند، در غیر این صورت ممکن است تنها باعث ایجاد یک "وضعیت هشدار" بی جهت شده باشند. برای مثال فرض کنید علت تاخیر در رسیدن مدافع مزبور به مقصد، از دست دادن اتوبوس و یا عدم تماس وی با دفتر در اثر فراموشی باشد. عدم آگاهی و اطمینان نسبت به هدف و نحوه عمل می‌تواند باعث شکل گیری واکنشی مخالف آنچه مطلوب آنهاست، بشود.

فصل پنجم

ممانعت و واکنش به حملات

هدف:

برآورد احتمال وقوع انواع گوناگون حملات

ممانعت از حملات مستقیم احتمالی علیه مدافعین

اقدام به عملیات ضد جاسوسی

حملات علیه مدافعین حقوق بشر

خشونت یک فرآیند است، همچنانکه می‌توان آن را یک عمل هم در نظر گرفت. حمله‌ای خشونت‌بار علیه یک مدافع در خلاء صورت نمی‌گیرد. تحلیل دقیق حملات اغلب نشان می‌دهد که آنها ماحصل و نتیجه اختلافات، نزاع‌ها، تهدیدات و اشتباهاتی هستند که در گذر زمان شکل گرفته‌اند و می‌توان ردپای آنها را تشخیص داد.

حملات علیه مدافعین حاصل حداقل سه فاکتور متصل هستند:

۱ ☐ شخصی که عمل خشونت‌آمیز را انجام می‌دهد

حملات علیه مدافعین اغلب محصول فرآیندهایی از فکر و عمل هستند که ما با بررسی آنها می‌توانیم موضوعات مهمی را درک کنیم. این اقدامات هر چند شامل افکار و اعمال غیرقابل قبول هستند اما باز هم حاوی درس‌های مهمی برای مدافعین می‌باشند.

۲ ☐ پس‌زمینه و عامل تسریع کننده‌ای که باعث شده است مهاجم خشونت را به عنوان یک گزینه تلقی کند

اغلب افرادی که مدافعین را هدف حمله قرار می‌دهند، حمله و هجوم را راهی برای تحقق یک هدف و یا حل مشکل شخصی خود قلمداد می‌کنند.

۳ ☐ بستر و مجموعه عوامل تسهیل کننده

مجموعه عوامل و شرایطی که خشونت را تسهیل کرده و امکان وقوع آن را فراهم می‌آورد و یا از وقوع آن ممانعت نمی‌کند.

چه کسی برای مدافعین خطرناک است؟

به صورت عام می‌توان گفت هر شخصی که تصور می‌کند حمله به مدافعین عملی مطلوب، قابل قبول و یا به صورت بالقوه راهی موثر برای تحقق هدف است را می‌توان یک مهاجم بالقوه محسوب کرد. بدیهی است در صورتی که چنین شخصی دارای ظرفیت حمله به مدافعین بوده- و یا قادر به کسب آن باشد- تهدید جدی‌تر می‌شود.

پیش از وقوع برخی حملات، تهدیداتی صورت می‌گیرد و در برخی موارد نیز شاهد چنین تهدیداتی نیستیم. با این وجودرفتار افرادی که در حال برنامه‌ریزی برای حمله خشونت آمیز و هدفمند هستند اغلب نشانه های آشکاری با خود دارد چرا که این افراد نیازمند جمع‌آوری اطلاعات در مورد زمان مناسب حمله، برنامه‌ریزی برای رسیدن و دستیابی به هدف خود و در نهایت تعیین نحوه فرار هستند.

تهدیدات متناظر با تغییر ظرفیت مهاجمین بالقوه برای عملی کردن طرح خود برای حمله تلقی آنها از میزان قابل قبول بودن حمله و در نهایت برآورد آنها از احتمال دستگیری و مجازات می تواند کاهش یابند

با توجه به این نشانه‌ها بدیهی است که شناسایی و تحلیل هر نشانه‌ای که بتواند حاکی از حمله‌ای احتمالی باشد ضروری است. برای این منظور باید

- احتمال عملی شدن تهدیدات را ارزیابی کرد. (فصل ۳)
- رویدادهای امنیتی را شناسایی و تحلیل کرد.

رویدادهای امنیتی که دربرگیرنده جاسوسی در مورد مدافعین و محیط کار آنها هستند، اغلب با هدف جمع‌آوری اطلاعات صورت می گیرند. این اطلاعات هر چند اغلب ممکن است برای طراحی حمله به مدافعین استفاده نشوند اما به هر حال باید این احتمال را هم در نظر گرفت (فصل ۴).

جاسوسی در مورد کارکنان و دفاتر با هدف جمع‌آوری اطلاعات در مورد آنها صورت گرفته و ممکن است برای اهداف متعددی به خدمت گرفته شود:

- شناسایی نوع فعالیت‌های انجام شده، زمان و شخص انجام‌دهنده هر فعالیت
- استفاده از این اطلاعات در زمانی دیگر برای حمله به شخص یا سازمان
- جمع‌آوری اطلاعات مورد نیاز برای اجرای حمله
- جمع آوری اطلاعات برای اقدامی قانونی و یا ایجاد مزاحمت برای فعالیت‌های مدافعین ظ(بدون خشونت مستقیم)
- مرعوب کردن حامیان و یا افرادی که با شما کار می کنند و یا ارائه اطلاعات با هدف مرعوب کردن شما و توقف متعاقب فعالیت‌ها

به یاد داشتن این موضوع که هر چند جاسوسی و کسب اطلاعات معمولا برای اجرای هر حمله‌ای ضروری است اما به صرف خود نمی تواند حمله تلقی شود از اهمیت به‌سزایی برخوردار است. همچنین باید توجه داشت که تمامی اعمال جاسوسی و کسب اطلاعات الزاما به حمله ختم نمی‌شوند. خشونت‌های هدفمند گاه هنگامی روی می‌دهند که مهاجم ناگهان با شرایط مساعد و فرصت مطلوب برای حمله مواجه می‌شود، اما حتی در چنین مواردی هم برخی تمهیدات اولیه (از جمله کسب اطلاعات) بیشتر به صورت نسبی انجام شده‌اند.

اطلاعات چندانی برای کمک به شما در شناسایی و تشخیص آماده شدن مهاجمان برای حمله، وجود ندارد. فقدان مطالعه و تحقیق در مورد این موضوع، در حالی است که در نقطه مقابل شاهد انبوهی از حملات علیه مدافعین هستیم. علیرغم این تناقض (کمبود تحقیق‌ها در قبال انبوه حملات) باز هم معدود مطالعات صورت گرفته می توانند حاوی اطلاعاتی گران‌قیمت و کاربردی باشند. ۳

☐ حمله به مدافعین ساده نیست و نیازمند منابع است

برای تعیین و شناسایی مسیر حرکت فرد و بهترین مکان حمله نیاز به جاسوسی و کسب اطلاعات است. تعیین نحوه رسیدن و دستیابی به هدف و فرار سریع و مطمئن از محل حمله هم ضروری است (به هر حال اگر مکان شرایطی مطلوب مهاجم داشته باشد، حمله با سهولت بیشتری صورت می گیرد).

□ **افرادی که به مدافعین حمله می کنند معمولا ارتباط نسبی با آنان دارند**

اغلب حملات به مدافعین توسط افرادی صورت می گیرد که به شدت در فعالیت‌های آنها ذی‌نفع محسوب می‌شوند. به عبارت دیگر معمولا این حملات بی‌هدف و یا تصادفی نیستند بلکه متناظر با منافع مهاجمین می‌باشند.

□ **عوامل جغرافیایی اهمیت دارند**

برای مثال حملات به مدافعین در مناطق روستایی کمتر در کانون توجهات عامه مردم قرار گرفته و طبیعی است که در سطوح انتظامی و حتی سیاسی واکنش‌های کمتری را در مقایسه با حملات صورت گرفته در مناطق شهری، برانگیزاند. حمله به مقر سازمان‌های غیر دولتی و یا سازمان‌های شناخته شده در مناطق شهری معمولا با بیشترین واکنش‌ها همراه است.

□ **انتخاب‌ها و تصمیم گیری‌ها قبل از حمله صورت گرفته‌اند**

افرادی که در حال بررسی حمله به یک سازمان مدافع هستند باید ابتدا تصمیم بگیرند که آیا قرار است به رهبران آن حمله کنند یا اعضا را ریشه‌کن کنند. آنها همچنین باید میان یک حمله نفوذ (علیه یک چهره کلیدی، کارآمد و سرشناس) که قطعا هزینه سیاسی عمل را افزایش خواهد داد و یا یک‌سری حملات (با هدف گرفتن اعضای سازمان) انتخاب کنند. مطالعات معدود صورت گرفته در این زمینه نشان می‌دهد که مهاجمان با توجه به شرایط از هر دو گزینه استفاده می‌کنند و نمی‌توان هیچ‌یک را نسبت به دیگری دارای احتمال بیشتری تلقی کرد.

شناسایی امکان‌پذیری حمله

برای تعیین احتمال وقوع یک حمله، باید فاکتورهای مرتبط و دخیل را تحلیل کنید. برای شناسایی این فاکتورها باید ابتدا انواع مختلف حملات را از یکدیگر تفکیک کرد: جرایم عام، حملات غیرمستقیم (حضور در مکان نادرست در زمان نادرست) و حملات مستقیم (هدفمند). برای این منظور می‌توان از سه جدولی که در صفحات بعد ارائه شده‌اند کمک گرفت.

جدول ۱ - تعیین سطح تهدید در حملات مستقیم (هدفمند)

سطح تهدید برای حملات مستقیم (هدفمند)			
تهدید شدید	تهدید متوسط	تهدید پایین	فاکتورها
مناطق فعالیت شما تحت کنترل کامل مهاجمین احتمالی قرار دارند	مهاجمین احتمالی دارای ظرفیت عملیاتی در مجاورت مناطق فعالیت شما هستند	مهاجمین احتمالی توانایی محدودی برای حمله در مناطق فعالیت شما دارا هستند	ظرفیت حمله
مهاجمین به شدت نیازمند تجهیزات و یا منابع مالی هستند	نیاز به تجهیزات، پول نقد و یا سایر راه‌های کسب درآمد (آدم‌ربایی) وجود دارد	مهاجمین احتمالی به تجهیزات و یا پول شما برای فعالیت خود نیاز ندارند	انگیزه مالی
اقدامات شما به وضوح تحقق اهداف آنها را به خطر انداخته و یا به رقبای آنان سود می‌رساند	ارتباط نسبی- فعالیت شما اهداف سیاسی و یا نظامی آنها را محدود می‌کند	وجود ندارد- فعالیت شما ارتباطی با اهداف آنها ندارد	انگیزه سیاسی و نظامی
موارد متعدد و پرشمار در گذشته	مواردی معدود (نه آنچنانکه بتوان آنها را نادر خواند)	وجود نداشته یا نادر است	سابقه حملات پیشین
تهاجمی با تهدیدات واضح و آشکار	بی‌تفاوتی، تهدیدات گاه‌به‌گاه و هشدارهای متعدد	بی‌تفاوتی یا همراهی	رویکرد یا قصد
وجود نداشته یا نیروهای امنیتی هم با مهاجمین احتمالی همکاری می‌کنند	پایین است	وجود دارد	ظرفیت نیروهای امنیتی برای ممانعت از حمله
محدود است (با توجه به شرایط) و یا اصلا وجود ندارد	متوسط یا پایین	خوب است	سطح نفوذ سیاسی شما در مقایسه با مهاجمین احتمالی

مثال

برای روشن شدن سطح تهدید برای حملات مستقیم (هدفمند)

حالتی را در نظر بگیرید که مهاجمین احتمالی منطقه فعالیت شما را تحت کنترل دارند اما هیچ انگیزه اقتصادی برای حمله به شما وجود ندارد. فعالیت شما تنها تا حدی مقاصد نظامی و سیاسی آنها را متاثر از خود کرده و هیچ سابقه‌ای هم از حملات مشابه در این شهر وجود ندارد. رفتار آنها همراه با بی‌تفاوتی است و آنها به وضوح خواهان معطوف شدن توجه ملی به منطقه و وضعیت خود و یا تحمیل فشاری در اثر حمله به شما نیستند.

در این سناریو سطح تهدید برای حمله را می‌توان کم تا متوسط تلقی کرد.

جدول ۲- تعیین سطح تهدید در جنایت

سطح تهدید برای جنایت			
تهدید شدید	تهدید متوسط	تهدید پایین	فاکتورها
مهاجمان جنایتکار در هر نقطه‌ای، روز یا شب فعالیت می‌کنند	مهاجمان جنایتکار معمولا شبانه وارد سایر مناطق می‌شوند (در مجاورت محدوده فعالیت می‌کنند)	مهاجمان جنایتکار معمولا در منطقه خاص خود، به‌دور از محدوده فعالیت سازمان باقی می‌مانند	تحرک و موقعیت مکانی مهاجمان جنایتکار
مهاجمان جنایتکار به صورت آشکار سرقت‌های خیابانی انجام داده و با ورود به محوطه ساختمان‌ها مرتکب جنایت می‌شوند	مهاجمان جنایتکار در خیابان مرتکب جنایت می‌شوند (اما نه در دفاتر مملو از کارکنان)	مهاجمان جنایتکار معمولا از مقابله می‌گریزند (عمدتا در مناطقی که سازمان‌های غیردولتی حضور ندار ند مرتکب جنایت می‌شوند)	وضعیت تهاجمی مهاجمان جنایتکار
سلاح‌های گرم و گاه قوی‌تر به کار می‌گیرند	سلاح‌های ابتدایی همانند قمه و ساطور در اختیار دارند	غیرمسلح و یا مسلح به اسلح‌های غیرکشنده هستند	دسترسی و یا استفاده از سلاح
به صورت گروهی عمل می‌کنند	۴-۲ نفر در یک تیم عمل می‌کنند	به صورت منفرد و یا زوج عمل می‌کنند	ابعاد و سازمان
پلیس معمولا حتی با حداقل کارآیی هم واکنش نشان نمی‌دهد	واکنش کند، موفقیت ناچیز در دستگیری جنایتکاران هنگام ارتکاب جرم	واکنش سریع با توانایی بازدارندگی	واکنش و بازدارندگی پلیس
پلیس یا عملا وجود نداشته و یا فاسد است (همکاری با مهاجمان)	آموزش منظم، حقوق پایین، منابع محدود	کاملا آموزش‌دیده و حرفه‌ای اما فاقد منابع لازم	آموزش و سطح حرفه‌ای نیروهای امنیتی
حقوق به هیچ‌وجه رعایت نمی‌شود	فقدان امنیت	فقدان اقتدار قانون، اما شرایط نسبتا امن است	وضعیت عام امنیت

مثال

برای برآورد سطح تهدید برای جنایت

موردی را در نظر بگیرید که در شهری جنایتکاران در نقاط مختلف به صورت زوج یا گروه‌های کوچک، برخی اوقات حتی در طول روز فعالیت می‌کنند. آنها اغلب رفتار تهاجمی داشته و تفنگ حمل می‌کنند. پلیس در قبال این جنایات واکنش نشان می‌دهد اما واکنش پلیس آرام و غیر موثر است، نیروی پلیس هم غیرحرفه‌ای و فاقد منابع لازم می‌باشد. با این وجود فرماندهی پلیس کاملا منظم انجام می‌شود. در شهر با فقدان امنیت روبه‌رو هستیم. در مناطق حاشیه شهر هم با توجه به اینکه تمامی شاخص‌ها در سطح بالا قرار دارند، تهدید جنایت در بالاترین حد خود قرار دارد.

احتمال حدوث حمله‌ای جنایتکارانه در مرکز شهری با چنین مشخصاتی، متوسط تا بالا ارزیابی می‌شود.

جدول ۳- تعیین سطح تهدید برای حملات غیرمستقیم

سطح تهدید برای حملات غیرمستقیم			
تهدید شدید	تهدید متوسط	تهدید پایین	فاکتورها
آگاهی کم در مورد محل وقوع درگیری‌ها	تقریبی	خوب	دانش شما در مورد محدوده‌های درگیری
فعالیت‌های شما در مناطق درگیری صورت نمی‌گیرد	محل فعالیت شما در نردیکی این مناطق است و شما گاه وارد این مناطق می‌شوید	محل فعالیت شما دور از این مناطق است	فاصله تا محل نزاع
تغییر محل‌های درگیری چنان دائمی و مستمر می باشد که احتمال پیش بینی آن وجود ندارد	محل های درگیری غالبا به صورت نسبی تغییر می کنند	درگیری‌ها ثابت بوده و محل آنها به ندرت و به آرامی تغییر می‌یابد. تغییر محل قابل پیش بینی است	تغییر محل‌های درگیری
در مورد مکان‌ها هیچ نمی‌دانید	اطلاعاتی تقریبی در دست دارید	آگاهی مناسبی دارید و یا اصلا محل مین گذاری شده‌ای وجود ندارد	دانش شما در مورد موقعیت مناطق مین گذاری شده
فعالیت‌های شما در مناطق مین گذاری شده صورت می‌گیرند	محل فعالیت شما در نزدیکی این منطقه است و یا تنها گاه وارد این مناطق می‌شوید	فعالیت شما در فاصله‌ای دور از این مناطق انجام می‌شود یا اصلا محل مین گذاری شده‌ای وجود ندارد	فاصله میان محل فعالیت شما و مناطق مین گذاری شده
بدون قائل شدن تفکیک: بمباران، توپخانه سنگین، حملات تروریستی و بمب گذاری	قائل به تفکیک به همراه استفاده متناوب از توپ، کمین و تک تیراندازها	قائل به تفکیک (میان طرف‌های درگیر و غیرنظامیان)	تاکتیک‌های مبارزه و تسلیحات

مثال

برای برآورد سطح تهدیدهای حملات غیرمستقیم

موردی را در نظر بگیرید که شما با محدوده‌های درگیری آشنایی دارید. این محدوده‌ها به آرامی تغییر می کنند و امکان شناسایی و پیش بینی آنها وجود دارد. محل فعالیت شما در نزدیکی مناطقی است که درگیری در آنها روی می‌دهد و شما اغلب به بازدید از این منطقه رفته و یا در محدوده درگیری مدتی را سپری می کنید، با این وجود محل فعالیت شما در نزدیکی مناطق مین گذاری شده قرار ندارد. تاکتیک‌های مبارزه مورد استفاده قائل به تفکیک بوده و لذا چندان شهروندان را به خطر نمی‌اندازد.

فعالیت در چنین منطقه‌ای متضمن سطح پایینی از تهدید حملات غیرمستقیم است.

ممانعت از حمله مستقیم احتمالی

شما اکنون باید به این برداشت رسیده باشید که همزمان با تغییر ظرفیت بالقوه یک مهاجم برای اجرای طرح حمله خود، تلقی آنها در مورد قابل قبول بودن حمله و یا احتمال دستگیری و مجازات، سطح تهدید هم تغییر یافته و کاهش پیدا می کند.

برای ممانعت از وقوع یک حمله، لذا ضروری است که :

- مهاجم بالقوه و یا شخص تهدیدکننده متقاعد شود که هر حمله‌ای هزینه‌های غیرقابل قبول و عواقب نامطلوبی دربر خواهد داشت
- امکان عملی شدن حملات- و یا عملی به نظر رسیدن آنها- به حداقل برسد

این نوع ممانعت از وقوع حملات را می‌توان مشابه تحلیلی دانست که در فصل۲ صورت گرفت و به استناد آن مخاطرات بستگی به آسیب‌پذیری‌ها و ظرفیت‌های مدافعین داشت. در آن تحلیل ذکر شده بود که برای حفاظت از خود و به صورت طبیعی کاهش مخاطرات، باید در برابر تهدید اقدامی عملی انجام داده، آسیب‌پذیری‌ها را کاهش داده و ظرفیت‌ها را گسترش داد.

جدول ۴- ممانعت از حمله مستقیم- نتایج روش‌های حفاظتی متفاوت

ممانعت از حمله مستقیم- نتایج روش‌های حفاظتی متفاوت	
مقابله و کاهش تهدیدات (اقدام مستقیم علیه مرجع تهدید یا علیه هر نوع اقدام صورت گرفته از سوی مرجع تهدید)	**تغییر در رفتار مقصرین:** بازداشتن مهاجمین با افزایش هزینه‌های احتمالی حمله **تغییر در میزان تبعیت عوامل دخیل مسوول از بیانیه سازمان ملل در مورد مدافعین حقوق بشر:** افزایش احتمال اقدام جدی مقامات مسوول علیه مقصران حمله و یا حفاظت از مدافعین می‌تواند باعث مایوس شدن مهاجمان و صرف‌نظر آنها از عملی کردن طرح خود شود
کاهش **آسیب‌پذیری‌ها** و افزایش **ظرفیت‌ها**	**کاهش امکانپذیری حمله:** کاهش میزان در معرض تهدید قرار گرفتن مدافعین به بهبود شرایط محیط فعالیت، مدیریت هراس و تنش به صورت مناسب، تهیه و تدوین طرح‌های امنیتی و ...

هنگامی که تهدیدی متوجه شما شده و می خواهید مخاطرات مرتبط با آن را کاهش دهید، باید توجه داشته باشید که نه تنها باید نسبت به خود تهدید واکنش نشان داده و عمل کنید بلکه باید در مورد **آسیب‌پذیری‌ها** و **ظرفیت‌های متناظر با تهدید** هم عملی انجام دهید. در هنگامی که تحت فشار زیادی قرار گرفته و می خواهید که با حداکثر سرعت ممکن واکنش نشان دهید، اغلب بهتر است توجه خود را صرف آسیب‌پذیری‌هایی کنید که امکان رفع و یا برطرف کردن آنها ساده‌تر است. در این حالت گاه ممکن است مجبور باشید از آسیب‌پذیری‌های مرتبط‌تر با تهدید- که امکان برطرف کردن آنها چندان ساده نیست- صرف‌نظر کرده و وقت خود را صرف سایر آسیب‌پذیری‌های مرتبط کنید.

مراقب باشید

اگر خطر حمله بالاست (یا به عبارت دیگر تهدید قوی و واقعی بوده و در شرایطی که ظرفیت‌های شما محدود است، از آسیب‌نیروهای متعددی رنج می‌برید) معطوف کردن توجه به رفع آسیب‌پذیری‌ها و افزایش ظرفیت چندان عقلانی نیست، چرا که برای موثر واقع شدن هر نوع تغییری در این بخش‌ها نیازمند گذر زمان هستید. اگر مخاطراتی که با آن مواجه هستید، بسیار بالا هستند (تهدید و یا حمله شدیدی قطعا در راه است) برای اجتناب از مخاطرات، تنها سه راه پیش‌رو دارید:

الف) ■ مقابله موثر و بلافاصله با تهدید با علم به اینکه شما می‌توانید نتیجه‌ای فوری و معین را به‌دست آورید؛ نتیجه‌ای که بتواند مانع حمله شود (اغلب اطمینان از اینکه می‌توان به نتیجه‌ای فوری و موثر دست یافت بسیار دشوار است چرا که به هر حال هر واکنشی نیازمند زمانی برای تاثیرگذاری است و در چنین شرایطی هم‌زمان عنصری بسیار ارزشمند است).

ب) ■ کاهش حضور خود به حداقل (در صورت امکان به صفر)، از طریق اختفاء و یا ترک محل ۶

ج) ■ تلاش برای قرار دادن خود تحت حفاظت مسلحانه یا به خدمت گرفتن محافظان مسلح. آگاهی مهاجمان از وجود مراقبی مسلح و یا در دست بودن سلاحی برای دفاع باعث می‌شود آنها از اقدام خود منصرف شده و مدافع در میان‌مدت یا طولانی‌مدت با خطرات دیگری مواجه نشود. (در عمل اما کسب سلاح جهت محافظت و یا محافظ مسلح چندان ساده نیست و مستلزم گاه صرف زمانی طولانی است). گاه ممکن است دولت اسکورت مسلحی را برای مدافع در نظر بگیرد. این امر اغلب در شرایطی عملی می‌شود که فشاری ملی یا بین‌المللی بر دولت جهت حفاظت از جان مدافع اعمال می‌شود. در چنین شرایطی پذیرش و یا رد اسکورت دولتی از سوی مدافعین هر چند بر میزان مسوولیت دولت تاثیرگذار است اما نافی این واقعیت نیست که دولت مسوول مستقیم حفظ امنیت مدافعین- ولو در صورت سر باز زدن آنها از پذیرش اسکورت مسلح- است. مداخله شرکت‌های امنیتی و حفاظتی خصوصی در چنین مواردی، به ویژه اگر آنها ارتباطاتی غیررسمی با دولت و نیروهای دولتی داشته باشند، باعث افزایش مخاطرات می‌شود (به فصل ۹ رجوع کنید). از سوی دیگر باید در نظر گرفت که حمل سلاح از سوی مدافعان معمولا تاثیری در پیشگیری از حمله‌ای سازماندهی شده نداشته و حتی ممکن است به نوبه خود باعث شود سطح آسیب‌پذیری مدافعین افزایش یابد چرا که دولت می‌تواند از مسلح بودن مدافعین به عنوان توجیهی برای حمله به آنها- با بهانه مبارزه با تروریسم یا شورشیان- استفاده کند.

برطرف کردن تهدیدات و شرایط تهدید کننده در صورتی که سایر فعالان مربوطه و فعالان دخیل هم حاضر به همکاری و اقدام مشترک باشند، با سهولت بیشتری امکان‌پذیر است. برای مثال می‌توان به سیستم قضایی کارآمد و شبکه‌های حمایتی (داخلی و یا بین‌المللی) اشاره کرد که می‌توانند فشار قابل توجهی را بر عوامل دخیل مسوول اعمال کنند. شبکه‌های اجتماعی (درون‌سازمانی یا میان‌سازمانی)، شبکه‌های شخصی و یا خانوادگی، صلح‌بانان بین‌المللی یا سازمان ملل و ... هم می‌توانند در این میان نقش ویژه خود را ایفا کنند.

جاسوسی و ضد جاسوسی

عملیات ضد جاسوسی می‌تواند به شما در تعیین این موضوع که آیا تحت حفاظت قرار دارید یا خیر، کمک کند. درک این موضوع که آیا تماس‌های شما - در تمامی اشکال ارتباطی- تحت کنترل قرار گرفته و یا شنود می‌شوند یا خیر، معمولا ساده نیست. لذا بهتر است فرض را بر این قرار دهید که تمامی ارتباطات شما تحت کنترل هستند.۷ حفاظت از دفاتر کار و یا تعقیب فعالیت‌ها و رفت‌و آمدها را می‌توان با سهولت بیشتری تعیین کرد.

چه کسی ممکن است مراقب شما باشد؟

افرادی که معمولا در محدوده شما حضور دارند؛ کسانی مانند دربان‌ها، باربرهای ساختمان، دست‌فروشا دوره‌گردی که در نزدیکی ورودی ساختمان‌ها بساط خود را پهن می‌کنند، افرادی که در وسایط نقلیه مجاور یا روبه‌روی دفتر شما حضور دارند، بازیدکنندگان و ... همگی می‌توانند به صورت بالقوه مراقب حرکات شما باشند.

این افراد ممکن است برای کسب پول به جاسوسی شما بپردازند یا تحت فشار قرار گرفته باشند، گاه جاسوسی این افراد تنها ناشی از همراستایی آنها با اهداف مخالفان شماست و در مواقعی هم ترکیبی از هر سه انگیزه مزبور می‌تواند باعث شود افراد عادی جاسوسی شما را بکنند. افرادی که در پشت جاسوسی از شما قرار دارند، در مواردی ممکن است همکار و یا عضوی از سازمان خود را در منطقه فعالیت شما مستقر کنند.

افراد ممکن است گاهی شما را از فاصله دور تحت حفاظت قرار دهند. در این موارد، افراد مزبور اغلب اعضای سازمانی خاص هستند و قطعا از روش‌های حفاظت و جاسوسی ویژه‌ای استفاده می‌کنند که به آنها امکان می‌دهد بدون "دیده شدن" شما را تحت نظر بگیرند این امر به معنای حفظ فاصله مراتب با شماست، افراد متعدد و متفاوتی می‌توانند به نوبت از موقعیت‌های مکانی متفاوت شما را تحت نظر بگیرند و یا از وسایط نقلیه متفاوت استفاده کنند. روش‌های متعددی برای عدم برانگیخته شدن شک شما وجود دارد.

چگونه می‌توانید مطمئن شوید که تحت نظر قرار دارید؟

شما می‌توانید با تحت نظر قرار دادن افرادی که ممکن است مراقب شما باشند، مطمئن شوید که آیا تحت نظر هستید یا خیر؟ این کار را می‌توانید با به کار بستن قواعد زیر انجام دهید (البته بدیهی است که نباید به هیچ‌وجه مضطرب و هیجان‌زده شوید):

- اگر بنا به دلایلی منطقی به این باور رسیده‌اید که شخصی ممکن است مراقب شما باشد، باید به تمام حرکات افراد در محدوده خود توجه داشته و تغییرات رفتار آنها را مدنظر قرار دهید. برای مثال اگر آنها ناگهان به فعالیت‌های شما علاقه‌مند شده و شروع به پرسش در مورد فعالیت‌های شما کردند، باید آن را نشانه‌ای مهم تلقی کنید. به خاطر داشته باشید همان‌گونه که مردان و زنان می‌توانند جاسوسی شما را بکنند، هیچ محدوده سنی هم برای جاسوسان وجود ندارد. مراقبان شما ممکن است افرادی بسیار جوان یا بسیار پیر باشند.
- اگر به‌این باور رسیده‌اید که تحت تعقیب قرار دارید، می‌توانید از راهکارهای ضد جاسوسی استفاده کنید. برای مثال می‌توانید از شخص ثالثی که مورد اعتماد شما است اما برای افرادی که ممکن است مراقب شما باشند ناشناخته است، کمک بخواهید. این شخص می‌تواند با حضور خود در محل پیش از رسیدن شما و از فاصله‌ای مطمئن، تحرکاتی را که هنگام رسیدن شما، ترک محل و یا رفتن به نقطه‌ای دیگر صورت می‌گیرد، تحت نظر قرار دهد. افرادی که مراقب شما هستند معمولا فعالیت‌های شما را در مکان‌هایی که غالبا در آن جا به سر می‌برید، مانند منزل، دفتر کار و یا نقاطی که غالبا به آنجا رفت و آمد می‌کنید، تحت نظر قرار می‌دهند.

مثال

موردی را در نظر بگیرید که شما پیش از رسیدن به منزل می‌توانید از یکی از اعضای خانواده یا همسایه‌های مورد اعتماد بخواهید که در نقطه‌ای نزدیک منزل شما مستقر شود (برای مثال به تعمیر خودرو یا تعویض لاستیک مشغول شود)، تا بتواند حضور احتمالی شخصی را که منتظر رسیدن شما به منزل است، تشخیص دهد. هنگام خروج از اداره- به صورت پیاده- هم می‌توانید روش مشابهی را پیگیری کنید. در صورتی که از وسیله نقلیه شخصی استفاده می‌کنید باید خودوری دیگری پس از خودروی شما به حرکت دربیاید تا بدین وسیله به مراقب‌های احتمالی فرصت کافی جهت نزدیک شدن به خود را بدهید.

حداقل سود حاصل از ضد جاسوسی این است که شخص مراقب شما نمی‌فهمد که شما نسبت به حضور او آگاهی دارید. به همین دلیل باید برای تمام کسانی که در این عملیات ضد جاسوسی حضور دارند روشن ساخت که به هیچ‌وجه با شخص مراقب مواجه نشوند و با وی برخورد نکنند. مواجهه با این افراد آنها را متوجه می‌کند که شما نسبت به فعالیت آنها آگاهی یافته‌اید و این امر ممکن است به نوبه خود به واکنش خشن آنها منتهی شود. در صورتی که مطمئن هستید شخصی مراقب شما است باید حداکثر حفاظت و دقت را معمول داشته و فاصله مناسب را با جاسوسان داشته باشید. هنگامی که نسبت به عملیات جاسوسی و حفاظت مطمئن شدید، می‌توانید اقدامات پیشنهاد شده در این خودآموز را پیگیری کنید (به فصل ۹ رجوع کنید).

اغلب توصیه‌های ضد جاسوسی منحصرا مربوط به مناطق شهری و یا نیمه‌شهری هستند. در مناطق روستایی با شرایطی به مراتب دشوارتر مواجه هستیم، با این وجود مدافعین و جوامع ساکن در این مناطق از هوشیاری بیشتری نسبت به حضور بیگانه‌ای در اطراف خود برخوردارند. به عبارت دیگر حضور هر بیگانه‌ای به سرعت مشخص می‌شود. شرایط منطقه‌ای باعث می‌شود تا شخصی که خواهان حفاظت از شمایت از شانس چندانی برای به خدمت گرفتن ساکنان منطقه‌ای روستایی برخوردار نباشد، مگر در مواردی که ساکنان منطقه نسبت به فعالیت‌های شما احساس خصومت عمیقی داشته باشند.

نکته: برقراری رابطه با نیروهای امنیتی ناظر بر فعالیت‌های شما می‌تواند در برخی شرایط مفید واقع شود و در برخی موارد خیر. به خاطر داشته باشید در مواردی آشکار کردن جاسوسی علیه شما و نظارت بر فعالیت‌هایتان به صورت عاملانه و با هدف مرعوب کردن شما صورت می‌گیرد. به هر حال مدافعین ممکن است حتی در مواردی برخی افراد درون نیروهای امنیتی را به خدمت بگیرند تا در مواردی که قرار است آنها تحت حفاظت قرار گرفته و یا طرحی علیه آنها اجرا شود، از آن مطلع شوند.

چه زمانی باید احتمال تحت نظر بودن را بررسی کرد؟

منطق می‌گوید اگر دلایل منطقی برای باور این موضوع که تحت نظر قرار گرفته‌اید را دارید، باید این احتمال را مورد بررسی قرار داد. برای مثال اگر متوجه رویدادهایی امنیتی شدید که می‌توانند مرتبط با عملیات جاسوسی باشند، باید این احتمال را بررسی کرد. اگر فعالیت‌های مدافعین حقوق بشر با مخاطراتی خاص و معین همراه باشد، انجام برخی عملیات ضد جاسوسی- به صورت متناوب و گاه به گاه- نه تنها ایده بدی نیست، حتی در مواردی هم ممکن است به کشف موارد مهمی منجر شود.

شما همزمان باید مخاطراتی که ممکن است جاسوسی از شما برای دیگران به همراه بیاورد را هم مدنظر قرار دهید. فرض کنید شما تحت نظر هستید، این امر مخاطرات به مراتب بیشتری را متوجه شاهدان یا اعضای خانواده یک قربانی- که با شما ملاقات دارند- می‌کند تا شخص شما. بدین ترتیب بدیهی است که باید تعیین مکان امن برای ملاقات با این افراد را هم مدنظر قرار دهید. شاید حتی لازم باشد به آنها در مورد اینکه فعالیت‌های شما تحت نظارت قرار دارند، هشدار دهید.

واکنش به حملات

هیچ قاعده نفوذ و ثابتی را نمی‌توان برای تمامی حملات صورت گرفته علیه مدافعین قابل اعمال و صادق دانست. حملات را نیز باید رویدادهای امنیتی تلقی کرد. در فصل چهارم با دستورالعمل‌هایی برای نحوه واکنش در برابر رویدادهای امنیتی آشنا شدید.

در هنگام مواجهه با هر نوع حمله‌ای باید دو موضوع اساسی را به خاطر داشت:

- همیشه در مورد امنیت فکر کنید! هیچ وقت، چه هنگام حمله و چه پس از آن، امنیت را از ذهن خود دور نکنید. (اگر با حمله‌ای مواجه شدید و باید میان دو گزینه، یکی را انتخاب کنید، بی‌درنگ گزینه‌ای که متضمن امنیت بیشتر است را برگزینید).
- متعاقب یک حمله، باید از لحاظ فیزیکی و روانی خود را بازسازی کرده، برای حل شرایط اقدام نموده و محیط کاری امنی را برای خود و سازمان‌تان فراهم کنید. گردآوری حداکثر اطلاعات ممکن در مورد حمله حیاتی است. مواردی چون آنچه که روی داده است، تعداد افراد دخیل در حمله و شناسایی آنها، شماره پلاک خودروها و هر نوع توصیف از رویداد و مسائل پیرامونی آن، حائز اهمیت هستند. ثبت این موارد برای مستندسازی پرونده حائز اهمیت بوده و باید با حداکثر سرعت مورد بررسی قرار گیرند. رونوشتی در تمامی اسنادی که به عنوان مستندات پرونده به مقامات مسوول تحویل داده‌اید را نگاهداری کنید.

فصل ششم

آماده‌سازی استراتژی و طرح امنیتی

هدف:

آشنایی با نحوه آماده سازی پیش نویس یک استراتژی امنیتی

آشنایی با نحوه آماده‌سازی یک طرح امنیتی

فعالیت مدافعین حقوق بشر در محیط‌های خصمانه

در اغلب موارد مدافعین در محیط‌های خصمانه فعالیت می‌کنند. دلایل وجود یا شکل گیری این خصومت علیه فعالیت‌های آنان را می‌توان در موارد متعددی برشمرد. اصلی‌ترین علت را باید ناشی از این واقعیت دانست که فعالیت‌های مدافعین حقوق بشر ممکن است به مقابله آنها با فعالان قدرتمندی که ناقض قوانین جهانشمول حقوق بشر هستند منتهی شود. این فعالان قدرتمند می‌توانند شامل دولت یا مقامات دولتی، نیروهای امنیتی، گروه‌های اپوزیسیون مسلح و یا گروه‌های خصوصی مسلح باشند. این فعالان ممکن است در واکنش به اقدامات صورت گرفته از سوی مدافعان، سعی کنند مانع تداوم فعالیت‌های آنان شوند. این امر می‌تواند از راه‌های مختلف، از سرکوب و محدودسازی آزادی بیان گرفته تا تهدیدات اعلام شده و حملات مستقیم صورت بگیرد. سطح تحمل فعالان بستگی به نوع فعالیت مدافعین دارد؛ ممکن است برخی فعالیت‌ها قابل قبول تلقی شده و برخی فراتر از سطح تحمل قلمداد گردند.
ابهام در سطح تحمل فعالان نسبت به فعالیت مدافعین، گاه آگاهانه ایجاد می‌شود.

بدیهی است در اینجا باید دو نکته مهم را مدنظر داشت:
در بسیاری موارد تنها چند عنصر خاص در **درون** مجموعه پیچیده فعالان حضور دارند (عناصری مانند آنچه در بالا به آن اشاره شد) که نسبت به مدافعین وضعیتی خصمانه دارند. برای نمونه برخی عناصر در درون یک دولت ممکن است حتی نسبت به محافظت از مدافعین رویکردی نسبتا جدی داشته باشند در حالی که سایر عناصر خواهان حمله و تهاجم به این مدافعین باشند. مدافعین ممکن است در طول دوران آشوب‌های سیاسی- بازه‌های زمانی برگزاری انتخابات یا سایر رویدادهای سیاسی- با خصومت بیشتری مواجه شوند.

فضای فعالیت سیاسی- اجتماعی مدافعین

در این دستورالعمل علاوه بر تمرکز بر حفاظت‌و حفظ امنیت مدافعین حقوق بشری که در شرایط و محیط‌های خصمانه مشغول فعالیت هستند، معیارها و راهکارهای بهبود امنیت آنها نیز مورد بررسی قرار می‌گیرد. بدیهی است که اقداماتی را می‌توان در سطوح سیاسی- اجتماعی برای بهبود و ارتقای احترام به حقوق بشر و بهینه‌سازی محیط فعالیت برای آنان انجام داد. فعالیت‌های تبلیغاتی و اعتراضی مدافعان حقوق بشر اغلب با هدف حصول اطمینان از مقبولیت و پذیرش گسترده‌تر حقوق بشر در سطح جامعه و یا انجام اقداماتی جدی‌تر از سوی فعالان سیاسی برای اطمینان از رعایت حقوق بشر شکل می‌گیرند. بدیهی است نمی‌توان این اقدامات را اقداماتی هدفمند و در راستای افزایش امنیت مدافعین تلقی کرد اما با این وجود چنین اقداماتی در صورت موفقیت می‌توانند تاثیری مثبت بر حفاظت و حفاظت از فضای

فعالیت اجتماعی- سیاسی مدافعین حقوق بشر داشته باشند.

فضای فعالیت اجتماعی- سیاسی را می‌توان به عنوان **مجموعه‌ای از اقدامات احتمالی که هر مدافعی نمی‌تواند با تقبل سطحی قابل قبول از مخاطرات شخصی انجام دهد**، تعریف کرد. به عبارت دیگر، هر مدافع مجموعه‌ای گسترده از اقدامات سیاسی احتمالی را فرض کرده و متناظر با هر یک عواقب یا هزینه‌های معین را برآورد کرده و به آن ارتباط می دهد. پس از این ارزیابی مدافع برخی از این اقدامات را با توجه به عواقب و هزینه‌های مترتب بر آن، "قابل قبول" تلقی کرده و برخی دیگر را "غیرقابل قبول" برآورد می‌کند. با این برآورد در واقع محدوده‌های یک "فضای سیاسی" متمایز و خاص تعریف می شوند.

برای مثال گروهی از مدافعین ممکن است پرونده‌های حقوق بشر را تا آنجا دنبال کنند که یکی از اعضای گروه با تهدید مرگ روبه‌رو شود. در صورتی که برآورد این گروه حاکی از در اختیار داشتن فضای سیاسی- اجتماعی باشد، ممکن است تصمیم گرفته شود با افشا و اعلام عمومی این تهدید، به تعقیب پرونده ادامه دهند اما اگر به این باور برسند که فضای سیاسی آنها محدود است، شاید بی‌توجهی به تهدید را متناظر با پرداخت هزینه‌های گزاف تلقی کرده و در نهایت تصمیم بگیرند که از پیگیری پرونده برای یک برهه زمانی خودداری کرده و در این فاصله به افزایش ظرفیت امنیتی خود بپردازند.

صفت "قابل قبول" در مورد مخاطرات، با توجه به شرایط زمانی و حتی تفاوت‌های میان افراد و گروه‌ها با یکدیگر ممکن است تغییر یابد. برای برخی شاید شکنجه و یا مرگ یک عضو خانواده حد نهایت مخاطرات تلقی شود. برخی مدافعین ممکن است اعتقاد داشته باشند که به زندان افتادن، در صورتی که به تحقق اهداف آنها منجر شده و یا در این راه موثر باشد مخاطره‌ای قابل قبول است. برای دیگران اما ممکن است ظرف تحمل آنها با اولین تهدید لبریز شود.

فضای سیاسی فعالیت، علاوه بر آنکه معمولا به صورت سابژکتیو توسط افراد دخیل و فعال در آن محدوده تعریف می‌شود، در برابر تغییرات صورت گرفته در محیط پیرامونی سیاسی (در سطح ملی) هم به شدت تاثیرپذیر است. بدین ترتیب بدیهی است که باید این فضا را به عنوان فضایی نسبی و قابل تغییر در نظر گرفت.

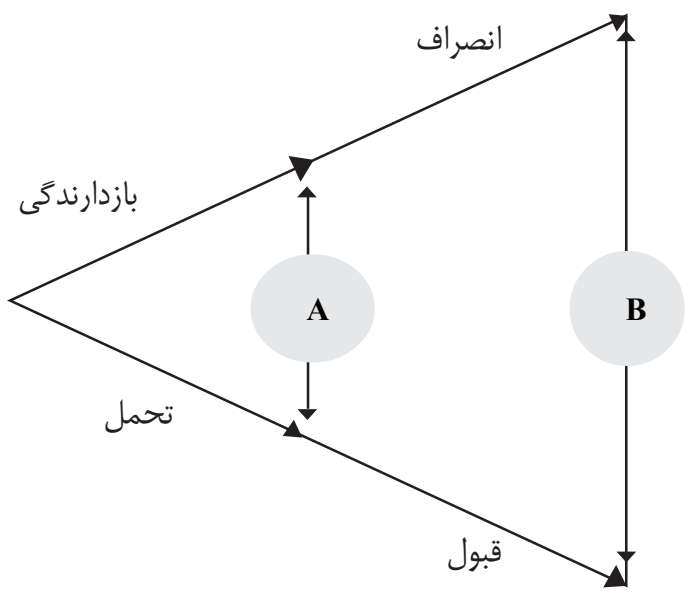
امنیت و فضای فعالیت مدافعین

تمامی استراتژی‌های امنیتی را می‌توان در چند کلمه خلاصه کرد: شما می خواهید فضای خود را گسترش داده و همزمان آن را پایدار سازید. اگر قرار باشد از واژگان و ادبیات امنیتی استفاده کنیم باید بگوییم که فضای فعالیت مدافعین نیازمند سطحی حداقلی از رضایت فعالان اصلی موجود در منطقه است- به‌ویژه در شرایطی که ممکن است مقامات سیاسی یا نظامی و یا گروه‌های مسلح حاضر در منطقه از فعالیت مدافعین تاثیر پذیرفته و در نقطه مقابل سعی کنند تا علیه آنها وارد عمل شوند-.

این رضایت می‌تواند به صورتی **صریح** ابراز شود، برای مثال به صورت صدور مجوز رسمی فعالیت از سوی مقامات مسوول و یا به صورت **ضمنی**، از سوی گروه‌های مسلح. این رضایت در صورتی که فعال مورد نظر از فعالیت‌های مدافعین سود ببرد، پایدارتر و قابل اتکاتر خواهد بود و در صورتی که فعال مزبور در اثر فعالیت‌های مدافعین ملزم به تحمل هزینه شود، قطعا باید شکننده تلقی شود. در چنین شرایطی سطح رضایت فعالان حاضر بستگی به هزینه سیاسی خواهد داشت که آنها در صورت تقابل و یا حمله به مدافعین باید پذیرا باشند. این امر به‌ویژه در مورد نزاع‌های مسلحانه‌ای که مدافعین با بیش از یک فعال مسلح روبه‌رو هستند، صدق می کند. در چنین وضعیتی ممکن است یک فعال مسلح فعالیت مدافعین را به نفع رقیب خود فرض کند. بدین ترتیب قبول و رضایت یکی از طرفین درگیری نسبت به فعالیت مدافعین می‌تواند به بروز خصومت از سوی طرف دیگر بیانجامد.

فضای فعالیت مدافعین را می‌توان توسط دو محور نمایش داد:

- محور نخست نشانگر گستره‌ای است که هر فعال حاضر به تحمل یا قبول کار شماست. این سطح تحمل بستگی به نوع و میزان تاثیر فعالیت شما بر اهداف و یا منافع استراتژیک هر فعال دارد. (پویستار تحمل- قبول).
- محور دیگر نشان‌دهنده گستره‌ای است که شما می‌توانید مانع حملات شوید. این سطح بستگی به هزینه بالای سیاسی اقدام علیه شما داشته و به میزانی که شما بتوانید فعالان را بر مبنای توجیهات منطقی- اخلاقی از اقدام علیه خود منصرف کرده و یا حتی آنها را نسبت به مزایای عدم حمله به شما و یا نقض حقوق بشر توجیه کرده و آنها را ترغیب به چنین رفتاری کنید، افزایش می‌یابد (پویستار بازدارندگی- انصراف).



توسعه فضای فعالیت در گذر زمان امکان‌پذیر است. تحقق "قبول" فعالیت مدافعین از طریق استراتژی انصراف نیازمند مدنظر قرار دادن فعالیت متناظر با نیازهای جمعیت، تصویر شما، دستورالعمل‌ها، همگرایی و ... است. این امر در فضا ی **B** قابل تحقق است. اما در نواحی که نزاعی مسلحانه در حال جریان است، فضای فعالیت معمولا تنها محدود به فضایی است که در آن امکان جلب رضایت فعالان مسلح وجود دارد. این فضا غالبا در اثر هزینه حمله به مدافعین (انصراف) ایجاد می‌شود. بدین ترتیب فضای فعالیت مدافعین به سطح **A** تقلیل می‌یابد.

گسترش فضای فعالیت با افزایش تحمل و قبول

فعالیت‌های شما ممکن است بر اهداف یا منافع استراتژیک اشخاصی که چندان اهمیتی به حقوق بشر نمی‌دهند، تاثیر گذاشته و در نتیجه در محیط فعالیت مدافعین شرایطی خصمانه حکمفرما گردد. برای رسیدن به وضعیت "قبول" فعالیت‌های مدافعین و یا حداقل رضایت نسبت به این فعالیت‌ها، کاهش برخوردها به حداقل میزان ممکن حائز اهمیت است. برای انجام این امر می‌توان توصیه‌های زیر را به کار بست:

- **فراهم آوردن و ارائه اطلاعات و آموزش در مورد ذات و مشروعیت فعالیت مدافعین**

مقامات دولتی و سایر فعالان در صورتی که ماهیت فعالیت شما و دلایل پیگیری آن را درک کنند، ممکن است تمایل بیشتری به همکاری نشان بدهند. در این شرایط تنها آگاه نمودن مقامات ارشد نسبت به فعالیت‌های خود کافی نیست چرا که مدافعین در جریان فعالیت‌های روزانه خود با انبوهی از مقامات دولتی در سطوح متفاوت و در نهادهای مختلف مواجه می‌شوند. برای تحقق این سطح از آگاهی باید تلاش

پیگیر و مدام برای مسطح کردن و آموزش دادن تمامی مقامات در تمامی سطوح داشته باشید.

◘ روشن کردن اهداف فعالیت مدافعین

در تمامی مواردی که فعالیت شما در محدوده درگیری صورت می گیرد، بهتر است حوزه و اهداف فعالیت‌های خود را مشخص کرده و محدوده آن را نیز به‌وضوح تعیین نمایید. این امر می تواند سوءبرداشت و یا تقابل‌های غیرضروری که ممکن است به ممانعت از تحقق اهداف مدافعین منجر شود را به میزان قابل توجهی کاهش دهد.

◘ محدودسازی اهداف متناظر و مطابق با فضای اجتماعی- سیاسی فعالیت

هنگامی که فعالیت مدافعین بر منافع استراتژیک معین یک فعال مسلح تاثیر می گذارد، فعال مزبور ممکن است با خشونت بیشتری واکنش نشان داده و چندان نگران خدشه‌دار شدن تصویر خود نباشد. برخی از انواع فعالیت‌ها، بیش از سایر فعالیت‌ها، مدافعین را در معرض آسیب قرار می‌دهد بنابراین باید مطمئن شوید که اهداف شما تا حد امکان با سطح مخاطرات و ظرفیت‌های حفاظتی‌تان همخوانی دارند.

◘ در استراتژی خود امکان "ترمیم وجهه" را قائل شوید

اگر می‌بایست با یک فعال در زمینه سوءاستفاده و نقض حقوق بشر مواجه شوید (یا به عبارت بهتر امکان دارد در این مورد تقابلی صورت گیرد) سعی کنید برای آنها این امکان را فراهم کنید که با تصحیح شرایط اعتبار خود را بازیابند.

◘ جذب متحد

تا حد امکان با تمامی بخش‌های اجتماعی متحد و همراه شوید

◘ ایجاد تعادل

باید میان شفاف‌سازی کلیه فعالیت‌های خود- با هدف اثبات این موضوع که مدافعین هیچ چیزی برای پنهان کردن نداشته و فعالیت‌های آنها کاملا مشروع است- و ممانعت از افشای اطلاعاتی که می تواند فعالیت یا امنیت شما را دچار تهدید کند، تعادل ایجاد کنید.

◘ و در نهایت

به خاطر داشته باشید که مشروعیت و کیفیت کار شما هر چند شروط لازم باز نگاه‌داشتن فضای فعالیت بر روی شما هستند، اما شروط کافی نیستند. ممکن است نیاز داشته باشید تا برخی مهاجمان بالقوه را از اقدام علیه خود منصرف کنید (به بخش ذیل رجوع کنید).

گسترش فضای فعالیت از طریق افزایش بازدارندگی و انصراف

مدافعین حقوق بشری که در فضاهای خصمانه فعالیت می کنند باید بتوانند به مهاجمین چنین القا کنند که در صورت هر گونه حمله به آنان مجبور به پرداخت هزینه گزاف سیاسی هستند. این هزینه باید چنان گزاف و بالا به تصویر کشیده شود که مهاجمین را متقاعد به عدم اقدام علیه مدافعین کند. این فرآیند را "**بازدارندگی**" می نامند.

بهتر است میان بازدارندگی "**عام**" و "**فوری**" تفکیک قائل شد. بازدارندگی عام شامل ترکیبی از تاثیر تمامی تلاش‌های ملی و بین‌المللی برای حفاظت از مدافعین است. به عبارت دیگر بازدارندگی عام دربرگیرنده هر چیزی است که بتواند در شکل‌دهی به این برداشت عام که حمله به مدافعین عواقب ناگواری دربر خواهد داشت، سهمی ایفا کند.
این امر می تواند از طریق کمپین‌های موضوعی یا آموزش و آگاهی‌دهی در مورد حفاظت از مدافعین صورت گیرد. در نقطه مقابل اما بازدارندگی فوری، هنگامی که بازدارندگی عام موثر واقع نشده و یا کافی نیست و یا مواردی که تلاش‌های محافظتی بر روی مواردی خاص و مشخص

متمرکز شده‌اند، می‌تواند مفید واقع شود.

انصراف اما موضوعی به مراتب فراگیرتر است. انصراف را می‌توان به عنوان نتیجه اقداماتی که در نهایت حریف را متقاعد به عدم انجام یک اقدام خصومت‌آمیز مورد انتظار کند، تلقی و تعریف نمود. بحث‌های منطقی، درخواست‌های اخلاقی، افزایش مشارکت، درک انسانی بهتر، انحراف توجه، به کارگیری سیاست‌های غیرتهاجمی و بازدارندگی، از جمله اقداماتی هستند که می‌توانند برای حصول "انصراف" به کار گرفته شوند. مدافعین حقوق بشر در سطوح ملی یا بین‌المللی به صورت مداوم از چنین تاکتیک‌هایی بهره می‌گیرند. بدیهی است که مدافعین نمی‌توانند چندان از تهدید سیستم برای منصرف کردن حریف استفاده کنند، در چنین حالتی استراتژی آنها بر این پایه استوار است که به دیگران گوشزد کنند که متناظر با تصمیماتشان باید در انتظار "عواقبی" باشند.

اجرایی کردن بازدارندگی

برای اطمینان از اینکه آیا توانسته‌اید سطح بازدارندگی مطلوب را محقق کنید، باید شرایط زیر ارضا شوند:

۱■ **مدافعین باید به صراحت نوع اقداماتی را که غیرقابل قبول می‌دانند مشخص کرده و به اطلاع مهاجمان برسانند.** بازدارندگی در صورتی که مهاجم نداند چه نوع عملی با واکنش مواجه خواهد شد، هرگز موثر نخواهد بود.

۲■ **سازمان مدافعین باید تعهد خود به بازدارندگی از تهاجم را چنان واضح و آشکار بیان کنند که مهاجمین نسبت به آن آگاهی یابند.** سازمان باید در عمل دارای استراتژی برای تحقق بازدارندگی باشد.

۳■ **سازمان مدافعین باید دارای توانای اجرای اقدامات بازدارنده مبسوط مهاجمین را نسبت به این امر آگاه کند.** اگر تهدید شما برای برانگیختن واکنش ملی یا بین‌المللی از سوی مهاجمان مستند و معتبر تلقی نشود، بدیهی است که آنها به هیچ دلیل نباید آن را جدی تلقی کنند. شما هم نباید انتظار داشته باشید که تهدید بی‌پشتوانه شما بر افزایش امنیت‌تان تاثیرگذار باشد.

۴■ **مدافعین باید مهاجمان را شناسایی کنند.** گروه‌های ضربت معمولا در تاریکی شب فعالیت کرده و به ندرت مسوولیت اقدامات خود را می‌پذیرند. بدین ترتیب شناسایی عاملین غالبا محدود به تحلیل این موضوع می‌شود که چه کسانی از چنین حملاتی متنفع می‌شوند. برای افزایش سطح تاثیرگذاری واکنش ملی یا بین‌المللی، استناد به فرض "مسوولیت دولت" - هر چند صحیح است- اما چندان موثر نیست. در چنین شرایطی باید اطلاعات بیشتری در مورد گروه‌هایی که در دستگاه‌های حکومتی در پس پرده هدایت و اجرای حملات را برعهده داشته‌اند، گردآوری شود.

۵■ **مهاجمین باید به صورت جدی حمله را مورد ارزیابی قرار داده و سپس نسبت به عدم انجام آن تصمیم بگیرند.** این امر زمانی حاصل می‌شود که هزینه‌ها- ناشی از تعهد مدافعین به بازدارندگی- به مراتب بیشتر از منافع حمله احتمالی باشد.

در شرایطی که مهاجمین چندان از تعهد و التزام مدافعین به بازدارندگی متاثیر نمی‌شوند، متقاعد کردن آنان نسبت به انصراف از اقدام خود، دشوار است. برای درک بهتر این امر شرایطی را در نظر بگیرید که جامعه جهانی می‌تواند دولتی را به خاطر حملات صورت گرفته به مدافعین حقوق بشر مجازات کند، اما دولت به نوبه خود امکان تنبیه و مجازات مجرمان اصلی و ناقضین واقعی حقوق بشر را ندارد. برای مثال ارتش‌های خصوصی معمولا در خارج از حیطه تسلط دولت هستند و منافع مشترکی هم با دولت ندارند. در چنین شرایطی ممکن است مهاجمین حتی از حمله به مدافعین حقوق بشر سود هم ببرند چرا که چنین حملاتی دولت را در موقعیتی دشوار قرار داده و وجهه آن را تخریب می‌کند.
مدافعین هرگز نمی‌توانند از پیش مطمئن باشند که "تعهد و التزام آنها به بازدارندگی" آن‌قدر قوی است که می‌تواند باعث انصراف مهاجمین

از حمله‌های بالقوه شود یا خیر. مهاجمین ممکن است از حمله خود به دنبال تحقق منافعی باشند که مدافعین نسبت به آنها آگاهی ندارند. برآورد شرایط با حداکثر دقت ممکن چالشی دائمی فراروی مدافعین است، چالشی که گاه حل و فصل آن را با توجه به فقدان اطلاعات ضروری و حائز اهمیت، غیرممکن می‌نماید. سازمان‌های مدافعین بدین ترتیب باید طرح‌های جایگزین کاملا منعطفی در اختیار داشته و از توانایی واکنش سریع در قبال رویدادهای پیش‌بینی نشده برخوردار باشند.

پیش نویس یک طرح امنیتی

تهیه پیش نویس یک طرح امنیتی نباید چندان مشکل باشد. فرآیندی که به منظور تهیه این پیش نویس باید طی شود، در اینجا طی چند گام؟؟ مورد و شرح داده می‌شود:

۱ ■ مولفه‌های طرح

هدف از طرح امنیتی کاهش مخاطراتی است که متوجه شما شده یا خواهند شد. لذا حداقل باید سه هدف مشخص، براساس برآورد مخاطرات صورت گرفته، وجود داشته باشند. این اهداف سه گانه عبارتند از:

- کاهش سطح مخاطراتی که متوجه شما شده است
- کاهش آسیب‌پذیری‌ها
- افزایش ظرفیت‌ها

لحاظ موارد زیر در طرح‌های امنیتی می‌تواند به کارآیی آن کمک کند:

- طرح‌ها یا پروتکل‌های پیشگیرانه، برای حصول اطمینان از اینکه فعالیت‌های روزمره در چارچوب استانداردهای امنیتی انجام می‌شوند. برای مثال تعیین نحوه اعلام جرم به صورت عمومی و یا دیدار از منطقه‌ای دورافتاده.
- طرح‌های اضطراری برای مقابله با معضلات خاص، برای مثال مواردی چون بازداشت یا ناپدید شدن اعضا.

۲ ■ وظایف و منابع برای اجرای طرح

برای حصول اطمینان از اینکه طرح اجرا شده است، باید اقدامات امنیتی روزمره را در چارچوب فعالیت‌های روزانه گنجاند.

- لحاظ کردن برآورد شرایط و نکات امنیتی در دستور کار روزانه
- ثبت و تحلیل رویدادهای امنیتی
- تقسیم و احاله وظایف
- تخصیص منابع لازم (زمانی یا مالی) برای امنیت

۳ ■ تهیه پیش نویس طرح- چگونگی آغاز

اگر پیش از این برآورد و مخاطرات را در ارتباط با یک مدافع و یا سازمان انجام داده باشید، اکنون لیست بلندی از آسیب‌پذیری‌ها، چندین نوع تهدید و مقداری ظرفیت در اختیار دارید. بدیهی است که عملا نمی‌توان همه چیز را در یک زمان پوشش داد. پس از کجا باید شروع کرد؟ پاسخ ساده است:

◆ چند تهدید معدود را گزینش کنید

تهدیدهایی را که فهرست‌وار ذکر کرده‌اید الویت‌بندی کنید، خواه این تهدیدات ذاتی باشند و خواه بالقوه. اولویت با تهدیدهایی است که دارای حداقل یکی از این مشخصه‌ها باشند: جدی‌ترین تهدید (برای مثال تهدیدات واضح مرگ)، یا محتمل‌ترین و جدی‌ترین تهدیدات (برای مثال اگر سازمان‌هایی مشابه شما مورد حمله قرار گرفته‌اند، باید آن را تهدیدی بالقوه برای خود محسوب کنید) و یا تهدیداتی که بیشترین تناظر را با آسیب‌پذیری‌های شما دارند (چرا که امکان ضربه خوردن شما از چنین تهدیداتی به مراتب بیشتر است).

◆ لیستی از آسیب‌پذیری‌های متناظر با تهدیدات گزینش شده را تهیه کنید

این آسیب‌پذیری‌ها باید در وهله نخست رفع شوند. البته به خاطر داشته باشید که همه آسیب‌پذیری‌ها با همه تهدیدات مرتبط نیستند. برای مثال اگر شما تهدید به مرگ شده‌اید، بدیهی است ایمن‌سازی قفسه‌های دفتری که در مرکز شهر واقع شده است، نباید اولویت نخست شما باشد مگر در شرایط بسیار غیرمحتملی که مطمئن باشید در محل کار خود مورد حمله قرار خواهید گرفت! در این شرایط بهتر است حضور خود در ملاء عام را- هنگام رفت و آمد به محل کار و یا منزل و یا تعطیلات پایان هفته- تا حد امکان کاهش دهید. ایمن‌سازی قفسه‌ها و کشوها امری "غیر مهم" نیست، قطعا آسیب‌پذیری شما در قبال تهدید به مرگ را کاهش نخواهد داد.

◆ لیستی از ظرفیت‌های خود را متناظر با تهدیدات گزینش شده تهیه کنید

شما اکنون در موقعیتی قرار دارید که می‌توانید تهدیدات گزینش شده، آسیب‌پذیری‌ها و ظرفیت‌های موجود را در طرح امنیتی خود قید کنید. بدین ترتیب می‌توانید مطمئن باشید که از همان گام نخست در مسیری صحیح برای کاهش مخاطرات قرار گرفته‌اید.

لطفا توجه داشته باشید که روش ذکر شده سهل‌ترین روش تهیه پیش نویس یک طرح امنیتی- البته با در نظر گرفتن دقت و جامعیت مطلوب- است. بدیهی است که راه‌های "رسمی" متعددی برای این امر وجود دارند، اما روش ارائه شده ساده و قابل درک بوده و همزمان شما را از توجه به جدی‌ترین و فوری‌ترین مسائل امنیتی مطمئن می‌کند- هر چند موفقیت این روش عملا در گروی برآورد صحیح شما از مخاطرات است- . با پیگیری این روش شما در نهایت طرحی "واقعی" و "به‌روز" در اختیار خواهید داشت. چنین ویژگی‌هایی را می‌توان مشخص‌های اصلی و بارز یک طرح امنیتی تلقی کرد. (برای مشاهده مجموعه‌ای مفصل در مولفه‌های دیگری که می‌توانید در طرح امنیتی خود قید کرده و یا حتی هنگام برآورد مخاطرات آنها را مدنظر قرار دهید، به بخش انتهایی این فصل مراجعه کنید).

کنار آمدن با چالش‌های امنیتی: مدیریت امنیتی گام به گام

مدیریت امنیت هرگز پایان نیافته و همواره به صورت نسبی و گزینشی صورت می‌گیرد. این مر را می‌توان ناشی از دلایل زیر دانست:

- همیشه حدی برای میزان اطلاعاتی که شما می‌توانید با آنها سروکار داشته باشید، وجود دارد، به عبارت دیگر تمامی فاکتورهای موثر بر امنیت را نمی‌توان در زمانی واحد طبقه‌بندی کرده و به آنها رسیدگی نمود.
- مدیریت امنیت فرآیندی پیچیده است. در طول این فرآیند به زمان و تلاش برای ایجاد آگاهی، ایجاد رضایت، آموزش افراد، رسیدگی به عملکرد نیروها، اجرای فعالیت‌ها و... نیازمند است.

مدیریت امنیت امری عملگرایانه است

مدیریت امنیت به ندرت می‌تواند کارکردی طولانی‌مدت و جامع داشته باشد. کارکرد مدیریت امنیت، تواناسازی مجموعه برای ممانعت از حملات و برجسته کردن نیاز به تدوین استراتژی‌های سازمانی برای کنار آمدن با این شرایط نهفته است. ممکن است در نگاه اول این وضعین

چندان ترغیب‌کننده (یا راضی‌کننده) به نظر نرسد و با بلندپروازی‌های ذهنی ما سازگار نباشد اما نباید فراموش کنیم که معمولا منابع بسیار محدودی برای مسائل امنیتی اختصاص می‌یابند!

هنگام بازبینی فعالیت‌های امنیتی یک سازمان یا یک مدافع ممکن است برخی دستورالعمل‌ها، طرح‌ها، راهکارها و یا الگوهای رفتاری- که پیش از این در درون سازمان وجود داشته و یا توسط مدافع اجرا می‌شدند- را کشف کنید. ممکن است همچنین به برخی نیروهای متضاد موجود، از ایده‌های سنتی و رایج در مورد اقدامات امنیتی گرفته تا مقاومت در برابر افزایش بار کاری موجود با به کارگیری و اعمال فعالیت‌های امنیتی جدید، برخورد کنید.

مدیریت امنیتی گام به گام راه را به سوی فرآیندی غیررسمی گشوده و فضایی برای پاگیری اقدامات جدید ایجاد می‌کند. تعامل با حوادث ناگهانی و غیرمترقبه، مانند رویدادهای امنیتی ممکن است مستلزم اتخاذ تصمیمات کوتاه‌مدت و نوری باشند که در صورت وجود مدیریت مناسب، به نوبه خود می‌توانند به اقداماتی امنیتی بلند مدت برای کل سازمان تبدیل شوند.

اجرای یک طرح امنیتی

طرح‌های امنیتی مهم هستند، اما اجرای آنها ساده نیست. اجرای این طرح‌ها بسیار فراتر از یک فرآیند تکنیکی صرف است. در واقع اجرای آنها را می‌توان نوعی فرآیند سازمانی تلقی کرد. این امر بدان معناست که در حین اجرا باید در جست‌وجوی نقاط ؟//؟ و فرصت‌ها و همزمان موانع و مشکلات بود.

یک طرح امنیتی باید حداقل در سه سطح اجرا شود:

- **سطح فردی:** هر فرد باید ملزم به اجرای طرح باشد تا امکان تاثیرگذاری آن فراهم شود
- **سطح سازمانی:** سازمان به عنوان یک مجموعه باید از طرح تبعیت کند
- **سطح میان‌سازمانی:** برای کسب امنیت معمولا به سطحی از مشارکت میان‌سازمان‌های مختلف نیاز است.

نمونه‌هایی از نقاط ورودی و فرصت‌ها هنگام اجرای یک طرح امنیتی

- چند رویداد امنیتی جزئی در سازمان شما و یا سازمان دیگری روی داده و نیروهای کارمندان شما نسبت به آنها ابراز نگرانی می‌کنند.
- به علت شرایط حاکم بر کشور، نوعی نگرانی عام در مورد امنیت حاکم است.
- نیروهای جدیدی به سازمان الحاق شده‌اند و امکان آموزش آنها برای رعایت معیارهای امنیتی، با سهولت بیشتری وجود دارد.
- یک سازمان دیگر پیشنهاد می‌کند که آموزش امنیتی نیروهای شما را برعهده بگیرد.

نمونه‌هایی از موانع و سدهای موجود بر سر راه اجرای یک طرح امنیتی

- برخی افراد ممکن است بر این باور باشند که اقدامات امنیتی باعث افزایش فشار کار آنها می‌شود.
- برخی دیگر ممکن است تصور کنند که موسسه در شرایط فعلی هم دارای امنیت کافی است.
- "ما برای این جور کارها فرصت نداریم".
- "خیلی خب! صبح روزهای یکشنبه وقت اضافی رو به بحث در مورد امنیت اختصاص می‌دهیم. اما فقط همین ؟؟؟ نه اوقات دیگر"
- "ما باید بیشتر مراقب مردمی باشیم که قرار است به آنها کمک کنیم نه این که به خودمان فکر کنیم".

راه‌های بهبود اجرای یک طرح امنیتی

- **بهره‌گیری از فرصت‌ها و نقاط ورودی** برای مواجهه با مشکلات و عبور از سد موانع
- **پیشرفت گام به گام.** لازم نیست تظاهر کنیم که همه کارها را می‌توان در یک آن انجام داد
- **تاکید بر اهمیت امنیتی برای پیشرفت کارها به نفع قربانیان.** تاکید بر این موضوع که امنیت شاهدان و اعضای خانواده برای افزایش کارآیی فعالیت های اصلی گروه حیاتی است و این امر هم با اعمال معیارهای مناسب امنیتی در تمامی عرصه‌های فعالیت قابل حصول است. می‌توانید از مثال‌هایی در جریان مباحثات و یا دوره‌های آموزشی استفاده کنید تا تاثیرات منفی بالقوه و فقدان امنیت بر شاهدان و قربانیان با وضوح بیشتری قابل درک شوند.
- طرحی که توسط دو "کارشناس" تدوین شده و سپس به کل مجموعه "تحمیل" شود، به احتمال قریب به یقین شکست خورده و موثر واقع نخواهد شد. در مورد مسائل امنیتی، **مشارکت همگانی امری کلیدی است.**
- **طرح باید واقع گرایانه و قابل اجرا باشد.** لیستی طولانی از اعمالی که باید قبل از هر بازدید میدانی انجام شوند، قطعا با مخالفت اعضا روبه‌رو شده و عمل نخواهد شد. باید برای حفظ امنیت، به حداقل معیارهای لازم بسنده کرد. این امر شاید دلیلی دیگر به ضرورت مشارکت افرادی باشد که در عمل با فعالیت‌های سازمان سر و کار دارند (نه صرفا متخصصان امنیتی). برای مثال افرادی که معمولا به بازدیدهای میدانی می‌روند باید در تدوین طرح مشارکت داشته باشند.
- **طرح را نباید به عنوان "فعالیتی اضافه" تلقی کرد بلکه باید آن را "راهی بهتر برای فعالیت" قلمداد نمود.** افراد باید امکان درک فرد یا طرح را بیابند. برای مثال باید از باز نویسی گزارش‌ها اجتناب کرد. مطمئن شوید که در گزارشات مربوط به بازدیدهای میدانی ابعاد امنیتی هم در نظر گرفته شده‌اند. مسائل امنیتی را بخشی از جلسات عادی گروهی کنید، بررسی ابعاد امنیتی را هم در دل آموزش‌ها بگنجانید و ...
- **تاکید کنید که امنیت یک گزینه شخصی نیست.** تصمیمات فردی، رفتارها و رویکردهایی که بر امنیت تاثیرگذار هستند، می‌توانند برای امنیت شاهدان، اعضای خانواده قربانیان و حتی همکاران عواقبی در بر داشته باشند. بدین ترتیب لازم است تا تعهدی جمعی برای اجرای اقدامات امنیتی مطلوب وجود داشته باشد.
- **زمان و منابع لازم باید تخصیص یابند.** برای اجرای طرح باید زمان، منابع لازم اختصاص یافته باشند. بهبود سطح امنیت با استفاده از "اوقات فراغت" افراد امکان‌پذیر نیست. اگر قرار است فعالیت‌های امنیتی مهم تلقی شوند، باید جایگاهی مشابه سایر فعالیت‌های مهم برای آنها قائل شد.
- **باید بر رعایت طرح از سوی تمامی افراد نظارت شود.** این امر به‌ویژه در مورد مدیران و افرادی که مسوول فعالیت‌های دیگران هستند صادق است. باید برای افرادی که به صورت مداوم از اجرای طرح و تطبیق فعالیت‌های خود با آن سر باز می‌زنند، عواقبی در نظر گرفته شود.

عناصر احتمالی برای لحاظ کردن در یک طرح امنیتی

در این بخش لیستی جامع از عناصری که می‌توانند در یک طرح امنیتی لحاظ شوند، ارائه شده است. پس از انجام برآورد مخاطرات، می‌توانید از میان این ایده‌ها، تعدادی را گزینش کرده و برای تکمیل طرح امنیتی خود به خدمت بگیرید.

- اهداف و ماموریت سازمان
- بیانیه سازمان در مورد سیاست امنیتی
- امنیت باید در تمامی ابعاد فعالیت‌های روزانه حاکم باشد: ارزیابی بستر فعالیت‌ها، ارزیابی مخاطرات و تحلیل رویدادها و تحلیل امنیت باید مدنظر قرار گیرد.
- نحوه حصول اطمینان از آموزش مطلوب تمامی کارکنان در مورد مسائل امنیتی (تا سطح مورد نیاز) و تبادل وظایف اطلاعاتی میان کارکنان، هنگام خروج آنها از سازمان
- تعیین و تخصیص مسوولیت‌ها: چه کسی قرار است چه کاری را در چه شرایطی انجام دهد.
- نحوه حل و فصل یک بحران امنیتی: تشکیل یک کمیته بحران و یا گروه کاری، مسوولیت برقراری ارتباط در مدیریت آن با رسانه‌ها، ارتباط با بستگان و ...
- مسوولیت‌های امنیتی درون‌سازمانی: برنامه‌ریزی، اقدامات متعاقب، بیمه، مسوولیت‌ها مدنی و ...
- مسوولیت‌های امنیتی فردی: کاهش مداوم مخاطرات، نحوه گذران اوقات فراغت یا فعالیت‌های خارج از برنامه کاری، گزارش و ثبت رویدادهای امنیتی، اعمال ممنوعه (برخی از این موارد در صورت امکان می‌توانند در قراردادهای کاری لحاظ شوند).
- تعیین سیاست‌های سازمانی در موارد زیر:

۱ -مدیریت تنش، اوقات فراغت و استراحت ۲ - رویدادهای جدی همانند آدم‌ربایی، ناپدیدشدن و یا مصدومیت شخصی و ... ۳ - امنیت شاهدان ۴ - ممانعت از حدوث حوادث و مشکلات بهداشتی ۵ - ارتباط با مقامات مسوول، نیروهای امنیتی و گروه‌های مسلح ۶ - مدیریت اطلاعات، نگهداری اطلاعات و اسناد محرمانه و ذخیره کردن آنها در مکانی امن ۷ - تصویر سازمان متناظر با ارزش‌های مذهبی، اجتماعی و فرهنگی ۸ - مدیریت امنیتی، در دفاتر و منازل (از جمله در مورد بازدیدکنندگان).

- تعیین پروتکل‌ها و طرح‌های پیشگیری

۱ -آمادگی برای بازدیدهای میدانی ۲ - نقل و انتقال پول و یا موارد با ارزش ۳ - پروتکل‌ها و وسایل ارتباطی ۴ - تعمیر وسایل نقلیه ۵ - مین‌های ضد نفر ۶ - کاهش خطر درگیر شدن در جنایات عام، رویدادهای مسلحانه و یا حملات و تعرضات جنسی ۷ - کاهش خطر بروز حوادث در هنگام مسافرت و یا در مناطق پرمخاطره.

- تعیین پروتکل‌ها و طرح‌ها برای واکنش در برابر بحران‌های امنیتی

مواردی چون ۱ - موارد اضطراری پزشکی و روان‌شناسی (با در نظر گرفتن موارد محتمل میدانی) ۲ - حملات، از جمله تعرضات جنسی ۳ - سرقت ۴ - واکنش هنگامی که شخصی در زمان معین در مکان تعیین شده حاضر نمی‌شود ۵ - دستگیری یا بازداشت ۶ - آدم‌ربایی ۷ - آتش‌سوزی و سایر رویدادهای مشابه ۸ - تخلیه ۹ - فجایع طبیعی ۱۰ - جست و جوهای قانونی و یا غیرقانونی و یا ورود مخفیانه به منازل و دفاتر ۱۱ - در صورت حمله به یک شخص (به‌ویژه حمله مسلحانه) ۱۲ - در صورت قتل شخصی ۱۳ - در صورت بروز کودتا.

فصل هفتم

برآورد عملکرد امنیتی سازمان: چرخ امنیت

هدف:

بررسی راه‌های مدیریت امنیت

ارزیابی میزان ادغام ضوابط امنیتی در فعالیت‌های حقوق بشر

چرخ امنیت

اجازه بدهید از ساده‌ترین بخش شروع کنیم. یک چرخ برای گردش دست باید کاملا گرد باشد. قطعا در این موضوع هیچ شک و شبهه‌ای وجود ندارد. اما اگر برخی سپرهای چرخ از بقیه بلندتر باشند، چه روی خواهد داد؟ بدیهی است که چرخ کاملا گرد نبوده و لذا به صورت مناسب به دوران در نمی‌آید. به عبارت دیگر چرخ کارآیی مورد انتظار را از دست می‌دهد.

در مدیریت امنیت در یک گروه یا سازمان هم وضعیت مشابهی را شاهد هستیم. اگر مولفه‌های اصلی امنیت همزمان تکامل نیابند، استراتژی امنیتی کلی قطعا کارکرد مورد انتظار را نخواهد داشت. بر اساس چنین شباهتی شما می‌توانید "چرخ امنیت" را ترسیم کنید. شما همچنین می‌توانید نحوه مدیریت امنیت را مورد بررسی قرار داده و میزانی که ضوابط امنیتی در فعالیت‌های مدافعین ادغام و اجرا شده‌اند را بررسی کنید.

این ارزیابی را می‌توان به صورت گروهی انجام داد. شما می‌توانید گستره‌ای از ایده‌ها را حول بخش‌های مختلف چرخ- به صورت متناسب تاکنون تکامل نیافته‌اند- جمع‌آوری و لیست کنید و سپس راه‌های پیشنهادی متعددی را برای حل مشکلات متناظر با هر بخش بیابید. هنگامی که تمامی راه‌حل‌های ممکن را لیست کردید، می‌توانید شروع به کار کرده و موردی را که مناسب‌تر و جامع‌تر- البته تحقق‌پذیر- است را انتخاب کنید.

هنگامی که ارزیابی چرخ امنیت را انجام دادید، نباید نتایج و دیاگرام حاصله را از نظر دور کنید. با تکرار این فرآیند در فواصل چند ماه می‌توانید دیاگرام‌های جدید و قدیم را با یکدیگر مقایسه کرده و به این ارزیابی برسید که آیا در بخش‌های مورد نظر موفق به بهبود اوضاع شده‌اید یا خیر؟

مولفه‌های چرخ امنیت

چرخ امنیت دارای ۸ پره یا مولفه است

- **تجربه عملی**

دانش اکتسابی عملی در مورد امنیت و محافظت. مکان عظیمت و مقصد

- **آموزش**

شما می‌توانید آموزش‌های امنیتی را در طی دوره‌های ویژه و یا حتی به صورت خودآموز در حین کار روزانه بگذرانید.

- **آگاهی و رویکرد در قبال امنیت**

آیا هر شخص و یا مجموعه سازمانی واقعا حفاظت و امنیت را الزامی و ضروری می‌پندارند و حاضر به کار و تلاش جهت اطمینان از تامین امنیت و حفاظت خود هستند یا خیر؟

- **برنامه‌ریزی**

ظرفیت برنامه‌ریزی برای امنیت و برنامه‌ریزی کاری با در نظر گرفتن مسائل حفاظتی

- **احاله وظایف**

چه کسی در کدامیک از ابعاد امنیتی و حفاظتی مسوولیت دارد؟ در شرایط اضطراری چه کسی مسوول است؟

- **میزان وجود قواعد امنیتی و رعایت آنها**

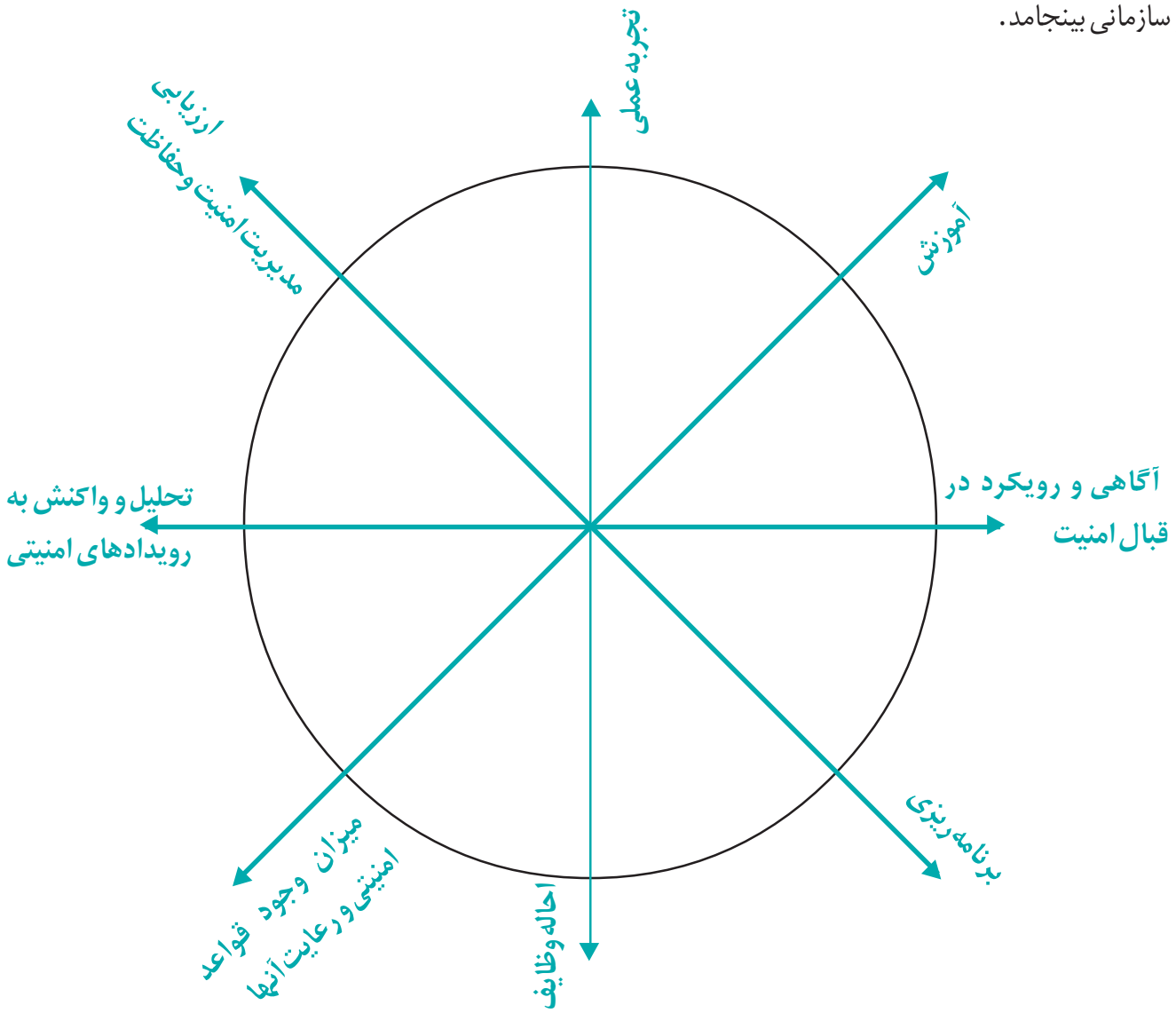
تا چه میزان افراد از قواعد و دستورالعمل‌های امنیتی پیروی می کنند؟

- **تحلیل و واکنش به رویدادهای امنیتی**

تا چه میزان رویدادهای امنیتی مورد تحلیل قرار می گیرند؟ آیا سازمان در قبال این رویدادها واکنش مناسب را نشان می‌دهد؟

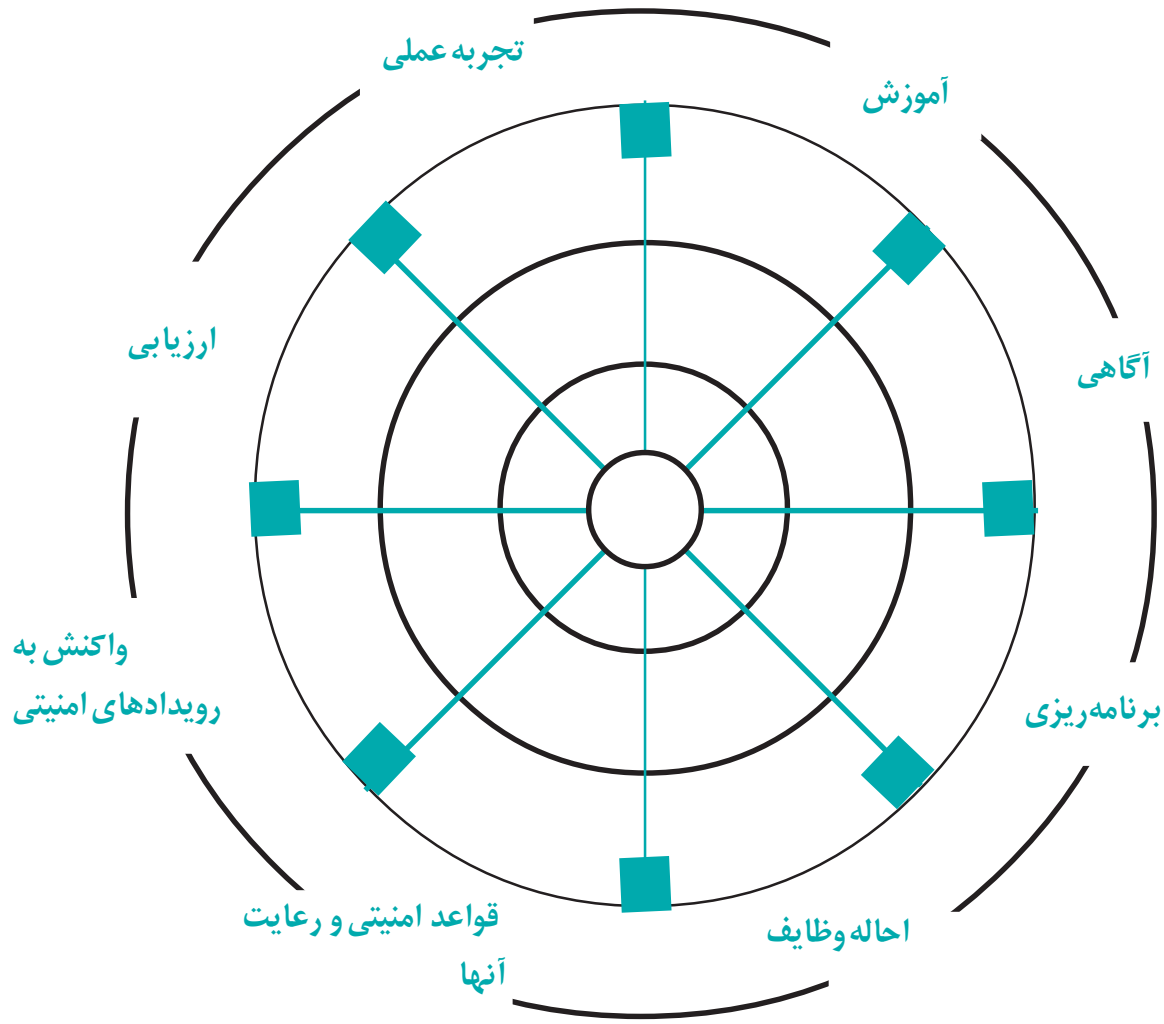
- **ارزیابی مدیریت امنیت و حفاظت**

اگر فعالیت‌های روزانه شما و نیز واکنش‌های صورت گرفته به رویدادهای امنیتی ارزیابی شوند، این امر می‌تواند به ارتقای دانش و تجربه فردی و سازمانی بینجامد.



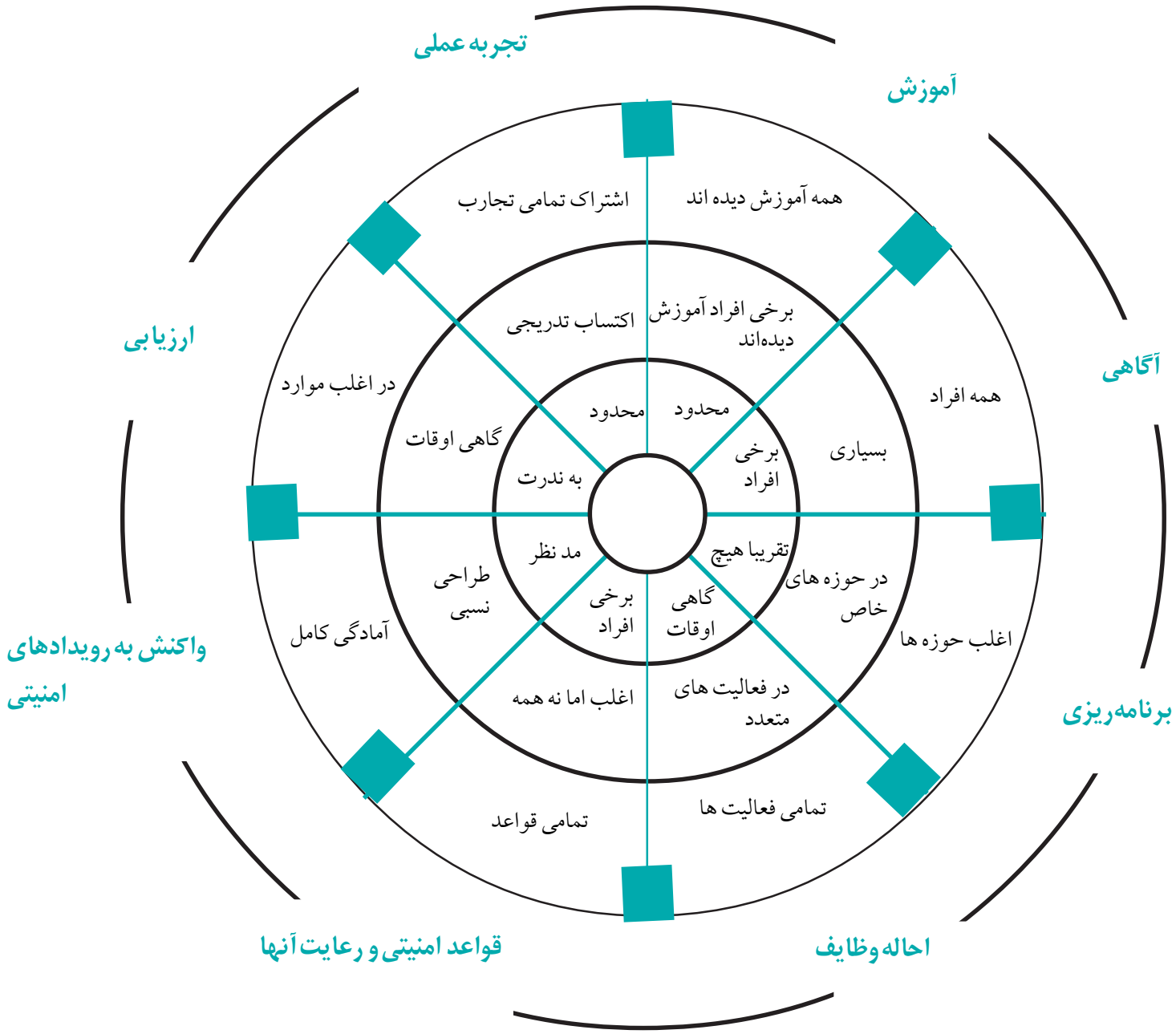
اکنون با مولفه‌های چرخ امنیتی بیشتر آشنا شدید، سعی کنید دیاگرامی با برخی اطلاعات تکمیلی ترسیم کنید. دیاگرام ترسیمی شما می‌تواند شبیه مورد زیر باشد.

چرخ امنیت و هشت قسمت (یا هشت پره) آن



چرخ امنیت هرگز ایده‌آل نیست

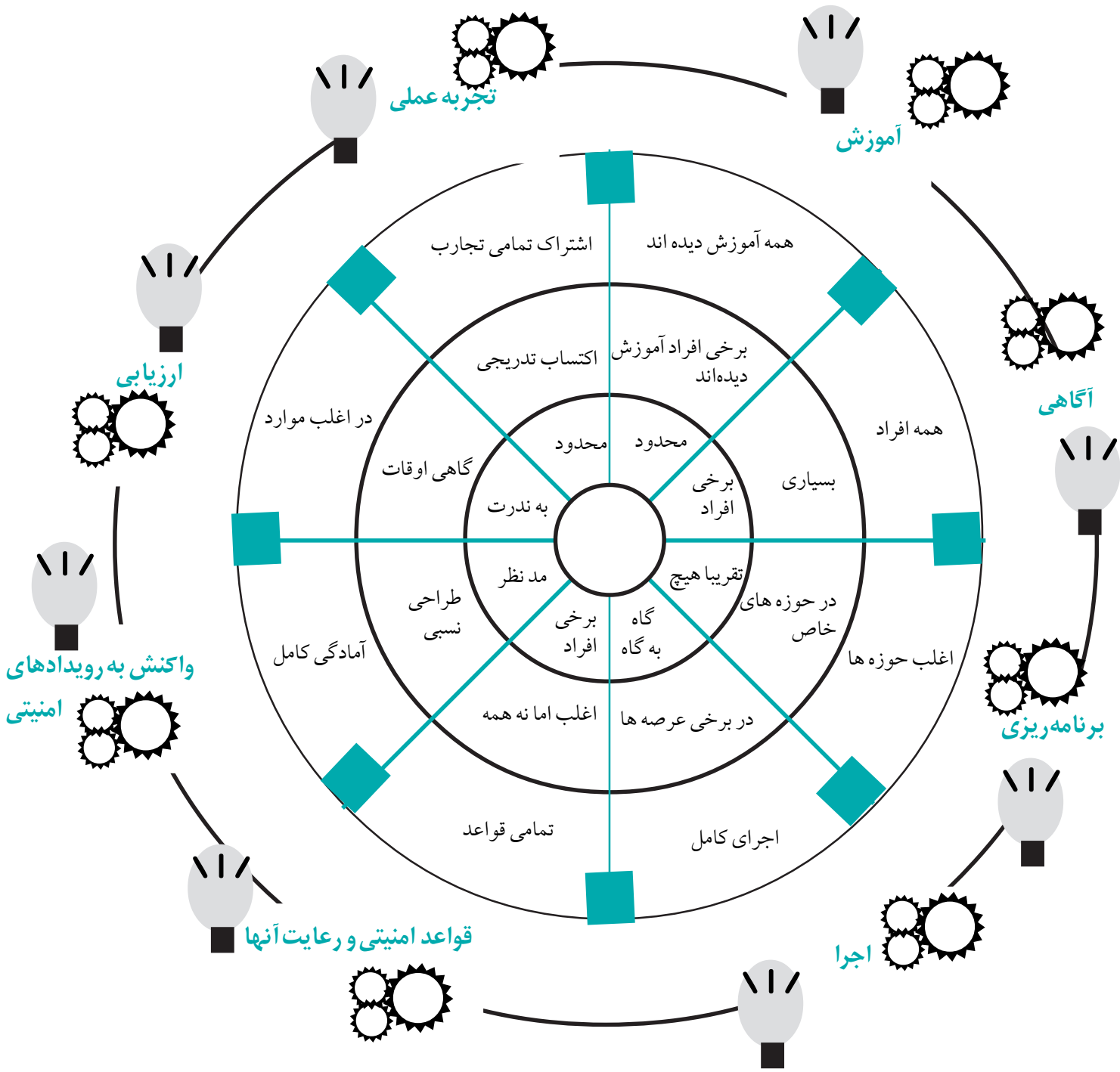
معمولا برخی از بخش‌ها بیش از بخش‌های دیگر تکامل یافته‌اند. بدین ترتیب بررسی میزان تکامل هر بخش می‌تواند موثر باشد. با انجام این امر شما می‌توانید به‌این نتیجه برسید که چه نوع اعمالی را باید برای بهبود امنیت و حفاظت خود اولویت دهید. هر خط باریکی که از مرکز دایره به سمت بیرون کشیده می‌شود نشان‌دهنده میزان تکامل آن مولفه از چرخ است.



می‌توانید این چرخ را فتوکپی گرفته یا ترسیم کنید، سپس فضاهای میان پره‌ها را رنگ کنید تا شکل واقعی چرخ گروه یا سازمان به‌وجود بیاید. در این صورت با راحتی بیشتری میزان تکامل هر بحث را بررسی می‌کنید.

شناسایی نقایص موجود در هر یک از هشت پره

چراغ نشان‌دهنده مشکلات در هر بخش از چرخ است
و **چرخ‌دنده‌ها** نشانه راه‌حل مشکلات هستند



فصل هشتم

حصول اطمینان از اجرای قواعد و دستورالعمل‌های امنیتی

هدف:

بررسی علت عدم رغبت یا توانایی پرسنل و یا سازمان برای تعقیب و اجرای طرح‌ها و دستورالعمل‌های امنیتی و یافتن راه‌حل‌های مناسب

امنیت به همه مرتبط است

تعیین اینکه آیا افراد و یا سازمان‌ها در عمل دستورالعمل‌ها و قواعد امنیتی را رعایت می‌کنند، مساله‌ای پیچیده است. ممکن است شما یک طرح امنیتی خوب داشته و تمامی دستورالعمل‌های مرتبط با مواد ضروری و یا قواعد پیشگیری را هم تدوین کرده و برای تکمیل طرح به آن افزوده باشید، حتی مساله امنیت را در اولویت دستور کار تمامی جلسات بزرگ و اصلی قرار داده باشید و ... اما در نهایت افراد باز هم از اجرای قواعد امنیت سازمانی سر باز زنند.

شاید وقوع چنین شرایطی با توجه به فشار فزاینده و مداومی که بر مدافعین حقوق بشر اعمال می‌شود، دور از ذهن باشد، اما رد عمل شاهد چنین وضعیتی هستیم.

بدیهی است اگر شخصی بخواهد در مورد فعالیت شما اطلاعاتی را کسب کند، هرگز سعی نخواهد کرد این اطلاعات را از "حفاظترین" شخص درون سازمان کسب کند بلکه در عوض سعی می‌کند که به کسی نزدیک شود و با او ارتباط برقرار کند که معمولا شنبه‌شب‌ها با زیاده‌روی در مصرف مشروبات الکلی، مست می‌کند. به صورت مشابه اگر قرار باشد شخصی به سازمان شما هشداری جدی بدهد (با ضربه زدن به یک عضو)، قطعا به فردی که تمامی پیش‌بینی‌های امنیتی را مد نظر قرار داده است، حمله نخواهد کرد، بلکه در عوض شخصی را هدف می‌گیرند که غالبا نسبت به امنیت خود بی‌توجه است، هر چند در مواردی اثرات این بی‌توجهی تنها به خود شخص محدود نمی‌شود. ممکن است شخصی مراقب هدف حمله قرار گیرد چرا ک شخصی بی‌توجه در را باز گذاشته است. مساله مهم این است که بی‌توجهی یک نفر می‌تواند همه را در معرض مخاطرات فزاینده‌ای قرار دهد.

بنا به دلایل فوق، بدیهی است که باید امنیت را به صورت مساله‌ای مربوط به کل سازمان تعریف کرد (علاوه بر مساله‌ای فردی برای تمامی کارکنان). اگر قرار باشد تنها سه نفر از مجموع ۱۲ عضو یک سازمان قواعد امنیتی را رعایت کنند، تمامی سازمان از جمله افراد رعایت کننده قواعد، در معرض خطر قرار دارند. بدیهی است اگر شرایط بهبود یافته و ۹ نفر از ۱۲ نفر به رعایت دستورالعمل‌های امنیتی روی آورند میزان مخاطرات کاهش می‌یابد. با این وجود اگر هر ۱۲ نفر دستورالعمل ها و قواعد امنیتی را رعایت می‌کردند، میزان مخاطرات به شدت تقلیل می‌یافت.

امنیت نه تنها مساله‌ای فردی است بلکه مساله‌ای است گروهی و مرتبط با تمام سازمان

داشتن یک طرح امنیتی تا زمانی که افراد خود را ملزم به رعایت آن ندانند، هیچ معنا و مفهومی ندارد. بگذارید واقع‌نگر باشیم: بسیاری ار افراد در عمل قواعد و دستورالعمل‌ها را رعایت نمی‌کنند. این فقدان تبعیت ناشی از خوش‌بینی افراد و یا تاثیر این قواعد بر زندگی واقعی آنها است. به هر حال باید به خاطر داشته باشیم که مواجهه با مشکلات- دشواری‌های احتمالی رعایت قواعد- بسیار ساده‌تر از مواجهه با عواقب احتمالی عدم رعایت آنها است.

علت عدم تبعیت افراد در قواعد امنیتی و نحوه رفع آن

قبل از خرید هر چیز باید به این موضوع توجه داشت که واژه "تبعیت" دارای بار ناخوشایند "فرمانبرداری" و "اطلاعات" است و لذا باید از به کار بردن آن اجتناب کرد. افراد تنها زمانی قواعد را تعقیب و اجرا می‌کنند که آنها را درک کرده و قبول نمایند، چرا که تنها در این صورت است که می‌توانند آن قواعد را از آن خود دانسته و یا به عبارت دیگر "مالک" آنها شوند. لغت کلیدی در اینجا "مالکیت" است.

به منظور تعقیب و اجرای دستورالعمل‌های امنیتی، تمامی افراد سازمان باید به آن ایمان داشته باشند. بدیهی است که این امر نمی‌تواند به صورت سریع و لحظه‌ای روی دهد. اگر قرار است کارکنان یک دستورالعمل امنیتی را باور داشته باشند باید به آنها امکان مشارکت در ترسیم و اجرای آن را داد. در این شرایط آموزش، درک و قبول دستورالعمل مورد نظر حایز اهمیت هستند.

جدول ۱ - رابطه میان افراد و سازمان‌ها از لحاظ امنیت

رویکرد: سازمان و فرد در مورد قواعد به توافق رسیده‌اند!	رویکرد: همه باید از قواعد پیروی کنند!	مفهوم
مبتنی بر نیازهای امنیتی شخص و سازمان	متمرکز بر قواعد	رویکرد
مبتنی بر گفتمان	آمرانه یا بر اساس الگوی منظم	نوع رابطه میان فرد و سازمان
برای رعایت توافق، با امکان نقد و بهبود قواعد (ما با هدف یا نیاز موافقیم و برای کمک به حفاظت از همکاران و افرادی که به آنها و یا برای آنها کار می‌کنیم)	بر اساس اجبار یا برای ممانعت از قرار گرفتن در معرض تحریم یا اخراج	چرا قواعد را رعایت می‌کنیم؟
در مسوولیت سهیم است	سهمی از مسوولیت ندارد	مسوولیت در برابر امنیت

"مالکیت" تنها به موضوع "تعقیب قواعد" باز نمی گردد بلکه پیرامون رسیدن و شکل دهی به توافقی است در مورد قواعدی که باید افراد آنها را رعایت کنند. افراد باید با درک، مناسب تلقی کردن و موثر دانستن قواعد و احساس سهم کردن نسبت به رعایت آنها اقدام کنند. به همین دلیل است که قواعد باید با شرایط اخلاقی و مذهبی افراد و نیز نیازهای اولیه آنها مطابقت و یا حداقل همراستایی داشته باشد.

"مالکیت" را نمی توان تنها به "تعقیب قواعد" تقلیل داد.
مالکیت به معنای احترام گذاشتن به توافقی میان سازمن و کارکنان پیرامون امنیت است.

برای رسیدن به توافقی میان کارکنان و سازمان، ضروری است که **فرد یا افراد مسوول امنیت سایر کارکنان را به صورت مداوم، از طریق جلسات تشریحی، یادآوری ها در مورد ابعاد توافق و یا جویا شدن نظرات افراد در مورد مناسب و یا موثر بودن قواعد در هنگام اجرا، در مسائل امنیتی مشارکت دهد.**

این نوع مشارکت در صورت فقدان **فرهنگ سازمانی امنیت** که باعث تقویت و استحکام دستورالعمل ها یا برنامه های کاری رسمی و غیر رسمی می شود، از ارزش چندانی برخوردار نیست.

بستر لازم برای اینکه افراد ضرورت دستورالعمل ها و قواعد امنیتی را مشاهده و درک کنند را می توان با طی گام های زیر فراهم نمود:

- ایجاد این درک و برداشت که امنیت برای حفاظت از قربانیان، شاهدان، اعضای خانواده و همکاران مهم بوده و امکان تداوم فعالیت های بنیادین و اساسی سازمان را فراهم می آورد.
- توسعه و ارزش دهی به فرهنگ امنیت سازمانی
- ایجاد "مالکیت" قواعد و دستورالعمل های امنیتی
- حصول اطمینان از مشارکت تمامی کارکنان در طراحی و بهبود قواعد و دستورالعمل های امنیتی
- آموزش افراد در عرصه های امنیتی
- حصول توافقی میان افراد و سازمان ها در مورد قواعد و دستورالعمل های امنیتی
- مشارکت افراد مسوول در امنیت برای در جریان گذاشتن و آموزش دادن به سایرین یا در یادآوری موضوعات مورد توافق به کارکنان و جویا شدن نظرات آنها در مورد مناسب و یا موثر بودن این قواعد در عمل

علت عدم اجرای قواعد و دستورالعمل های امنیتی

قطعا نمی توان در عمل هیچ نمونه ای از مدافعین حقوق بشر را یافت که هیچ یک از قواعد امنیتی را رعایت نکنند، بسیاری از افراد در یک سازمان به هر حال برخی قواعد – نه الزاما تمامی آنها – را رعایت می کنند و یا قواعد را به صورت متناوب و نه دائمی و منظم مورد توجه قرار می دهند.

دلایل بسیاری را برای عدم رعایت قواعد و دستورالعمل های امنیتی از سوی افراد می توان یافت. برای تغییر این وضعیت و حصول اطمینان از "مالکیت"، باید این علل را شناسایی کرده و سپس راه هایی را با کمک سایر افرادی که در این نگرانی سهیم هستند، یافت. در این میان تفکیک قائل شدن میان دلایل متفاوتی که هر یک از افراد برای عدم رعایت قواعد امنیتی دارند، موثر است.

برخی دلایل احتمالی برای عدم توجه به قواعد و دستورالعمل‌های امنیتی

ناآگاهانه:

- مدافع نسبت به قواعد آگاه نیست
- قواعد را به صورت مناسب اجرا نمی‌کند

آگاهانه:

مشکلات عام:

- قواعد بسیار پیچیده بوده و اجرای آنها دشوار است
- دستورالعمل‌ها عملا در محیط کار در دسترس قرار ندارند و یا به گونه‌ای عرضه شده‌اند که امکان به کارگیری آنها به صورت روزانه و مستمر دشوار است.

مشکلات فردی:

- قواعد در تضاد با نیازها یا منافع فرد قرار داشته و این تضاد حل نشده باقی‌مانده است
- فرد با برخی یا تمامی قواعد موافق نیست، آنها را بر اساس تجارب شخصی،اطلاعات قبلی، آموزش‌ها و یا باورهای فردی زاید و غیرضروری، نامناسب و غیرموثر تلقی می‌کند.

مشکلات گروهی:

- اغلب کارکنان قواعد را رعایت نمی‌کنند، همچنانکه رهبران گروه هم آنها را رعایت نکرده و یا به صورت کافی نسبت به رعایت آنها توجه ندارند. علت این امر را باید فقدان فرهنگ سازمانی امنیت دانست.
- فقدان انگیزه فعالیت (به صورت عام) می‌تواند باعث بی‌توجهی افراد به قواعد امنیتی شود.

مشکلات سازمانی:

- منابع فنی و یا مالی لازم برای تسهیل رعایت قواعد از سوی کارکنان وجود ندارد.
- ممکن است تناقضی میان قواعد و برخی حوزه‌های فعالیت وجود داشته باشد. برای مثال ممکن است قواعد توسط افراد مسوول امنیت تدوین شده باشند اما توسط افراد شاغل در بخش برنامه ریزی و حسابداری مورد توجه قرار نگرفته یا به صورت کامل اجرا نشوند. برخی قواعد ممکن است تنها برای یک حوزه فعالیت مناسب باشند و با شرایط حاکم بر حوزه دیگر تعارض داشته باشند.
- کارکنان مجبور هستند فشار کاری بالایی را تحمل کنند و لذا برای برخی یا تمامی قواعد اولویت قائل نیستند.
- فقدان انگیزه (به صورت عام) به شکل تنش، اختلافات در محل کار تبلور می‌یابد و در نهایت به عدم رعایت قواعد منجر می‌شود.

فرهنگ سازمانی، را می‌توان هم امری رسمی و هم غیررسمی تلقی کرد. این فرهنگ نه تنا باید در سازمان (به عنوان یک مجموعه) حاکم باشد بلکه حتی در درون گروه‌های همکار (تیم‌ها) هم باید جاری شده باشد. نشانه‌های یک فرهنگ سازمانی مطلوب را می‌توان در گپ‌زدن‌های غیررسمی، شوخی کردن‌ها، میهمانی‌ها و ... یافت.

نظارت بر ملاحظه قواعد و دستورالعمل‌های امنیتی

نظارت مستقیم:

رعایت قواعد و دستورالعمل‌های امنیتی را می‌توان در ارزشیابی‌های عام صورت گرفته از فعالیت‌ها و یا در چک‌لیست‌ها لحاظ کرد. جلسات

برگزار شده پیش و یا پس از عملیات میدانی، گزارش‌های فعالیت و یا دستور کارهای جلسات هم دیگر فرصت‌هایی هستند که می توان برای نظارت بر ملاحظه قواعد و دستورالعمل‌های امنیتی از آنها استفاده کرد.

بازبینی‌های دوره‌ای را نیز می توان با مشارکت گروه‌هایی (تیم‌هایی) که به نظر می‌رسد نحوه رعایت قواعد از سوی آنها زیر سوال است، با هدف بررسی مسائل مورد نظر مانند امنیت نگهداری اطلاعات حساس، رونوشت برداری و دستورالعمل‌های امنیتی، پروتکل‌های امنیتی برای بازدیدکنندگان از مقر سازمان، نحوه آماده‌سازی برای عملیات میدانی و موارد مشابه دیگر، صورت داد.

نظارت غیرمستقیم :

جویا شدن نظرات افراد در مورد قواعد و دستورالعمل‌ها، مناسب بودن و سهولت اجرای آنها و ... می‌تواند به شما کمک کند تا به این ارزیابی برسید که آیا کارکنان در مورد قواعد اصولا آگاهی دارند، آیا آنها را به صورت کامل پذیرا شده‌اند و یا اینکه آیا میزان مخالفت آنها با این قواعد چنان است که می تواند اجرای آنها شود. در این روش می توان استفاده کارکنان از راهنمای امنیت و یا پروتکل‌ها و قواعد موجود را نیز بررسی کرد.

بررسی و تحلیل نظرات افراد و ارزیابی قواعد و دستورالعمل‌های امنیتی با مشارکت گروه‌هایی که به نظر می‌رسد نحوه رعایت قواعد از سوی آنها زیر سوال است، بسیار ارزشمند است. این امر می‌تواند حتی به صورت غیررسمی، مخفیانه و یا از طریق شخص ثالث صورت گیرد.

نظارت از طریق بازنگری:

بازبینی امنیت با تحلیل رویدادهای امنیتی واقع شده، امکان‌پذیر است. این امر باید با دقت ویژه‌ای صورت بگیرد چرا که افرادی که با رویدادهای امنیتی مواجه می‌شوند ممکن است حدوث این رویدادها را ناشی از قصور خود دانسته و نگران باشند که تحلیل این رویدادها ممکن است به اعمال تنبیهات علیه آنان منجر شود. افراد در چنین شرایطی ممکن است تمایل به مخفی کردن رویداد داشته و از گزارش رویداد و یا ابعادی از آن خودداری کنند.

چه کسی مسوول نظارت است؟

بر اساس نحوه کارکرد و فعالیت سازمان، هر شخصی که مسوول سازماندهی امنیت، حوزه‌های خاصی از عملیات در چارچوب مسائل امنیتی و مدیریت امنیت کارکنان است، مسوول نظارت بر امنیت هم خواهد بود.

اگر قواعد و دستورالعمل‌های امنیتی رعایت نشدند، چه می توانیم بکنیم؟

۱ ◆ علت‌ها را شناسایی کرده، راه‌حل‌ها را یافته و نسبت به برطرف کردن علت عدم رعایت مسائل امنیتی اقدام کنید. لیست گزینه‌های ارائه شده در جدول ۱ را می‌توان به عنوان راهنما مد نظر قرار داد.

۲ ◆ در صورتی که شکل آگاهانه است و توسط تنها یک شخص ایجاد شده است، سعی کنید :

- ◇ الف) با شخص مزبور وارد گفت‌وگو شده و علت یا انگیزه او را از عدم رعایت موارد مزبور بیابید.
- ◇ ب) با کل تیم- که این فرد هم عضوی از آن است- کار کنید. توجه داشته باشید که با توجه به موضوع این امر ممکن است در موارد مناسب نباشد.
- ◇ ج) از سیستم هشداردهی استفاده کنید تا شخص کاملا نسبت به شکل آگاه شود.
- ◇ د) از روش تنبیهات تدریجی استفاده کنید. این تنبیهات در نهایت با اخراج شخص می‌تواند به نقطه اوج برسد.

۳ ◆ در تمامی قراردادهای کاری، شرطی را در مورد لزوم رعایت قواعد و دستورالعمل‌های امنیتی بگنجانید تا کارمندان نسبت به میزان

اهمیت این موضوع برای سازمان آگاه شوند.

در نهایت:

برخی ممکن است بر این باور باشند که بحث در مورد علت عدم رعایت قواعد امنیتی از سوی افراد، هدر دادن وقت است چرا که همواره فعالیت‌های مهم‌تر و ضروری‌تری برای انجام دادن وجود دارند. افرادی که بر این باور هستند معمولا به سادگی اعتقاد دارند "قوانین باید رعایت شوند، فقط همین!". این در حالی است که به باور بسیاری دیگر جهان معمولا همواره بر وفق مراد و انتظار نمی‌چرخد.

باور و نظر شما هر چه که هست، ما شما را دعوت می کنیم که گامی به عقب برداشته و میزان رعایت قواعد و دستورالعمل‌های امنیتی در سازمانی که در آن شاغل هستید را بررسی و تحلیل کنید. نتایج ممکن است حیرت‌آور باشند و شما را به این باور برسانند که بهتر است برای اجتناب از عواقب احتمالی، دقت و توان لازم را جهت اصلاح وضعیت فعلی اختصاص دهید.

فصل نهم

ارتقای امنیت در منزل و محل فعالیت

هدف:

ارزیابی امنیت در منزل و محل فعالیت

طراحی، ارتقا و سنجش میزان امنیت در منازل و دفاتر

امنیت در محل کار و منزل

امنیت مقرهای سازمان، دفاتر کار و منازل کارکنان در انجام بهینه فعالیت های مدافعین حقوق بشر از اهمیتی بنیادین برخوردار است. بدین ترتیب بهتر است در ابتدا به صورت عمقی نسبت به نحوه تحلیل و ارتقای امنیت دفاتر یا منازل بپردازیم (برای تسهیل امر از این پس فقط دفاتر را مدنظر قرار می‌دهیم، هر چند اطلاعات ارائه شده برای منازل هم صدق خواهد کرد).

ابعاد عام امنیت دفتر

هدف ما از ارتقای امنیت دفاتر را می‌توان در یک جمله ساده خلاصه کرد: **ممانعت از دسترسی غیرمجاز**. در موارد بسیار معدود ممکن است نیاز باشد دفتر در برابر حملات احتمالی (برای مثال بمب‌گذاری) محافظت شود.

برای رسیدن به هدف مزبور، باید نخستین گام را برداریم. این گام چیزی نیست جز شناسایی آسیب‌پذیری‌های دفتر. این آسیب‌پذیری‌ها، بسته به تهدیداتی که متوجه شما شده و یا می‌شوند، سطح مخاطرات را افزایش می‌دهند. برای مثال اگر شما با این خطر روبه‌رو هستید که کسی ممکن است قصد به سرقت بردن تجهیزان و یا اطلاعات شما را داشته باشد، باید آسیب‌پذیری‌های متناظر با این امر را برطرف کنید. دزدگیری‌های شبانه در صورتی که کسی قرار نباشد برای سرکشی و بررسی آنچه روی داده است، به محل مراجعه کند، ارزش چندانی ندارند. از سوی دیگر قرار است حمله و یا سرقتی خشونت‌بار در طول روز صورت بگیرد، نرده‌های مستحکم و تقویت شده بر روی درها و یا حتی زنگ‌های خطر هم چندان موثر نخواهد بود. به عبارت ساده‌تر، باید اقدامات خود را متناسب و متناظر با تهدیداتی که متوجه شما شده و همچنین بستری که در آن مشغول فعالیت هستید، انجام دهید.

آسیب‌پذیری‌های دفتر را
باید متناظر با تهدیداتی که متوجه شما شده است
ارزیابی کرد

به هر حال بدیهی است که ایجاد تعادلی میان تدارک اقدامات امنیتی مناسب و القای این تصور به افراد خارجی که شما با افزایش اقدامات امنیتی قصد "پنهان کردن" و یا "حفاظت" از چیزی باارزش را دارید، الزامی است. القای چنین تصوری به افراد خارج سازمان می‌تواند مخاطراتی را که متوجه شما شده است، به مراتب افزایش دهد، در مواردی همین حس القا شده، خود می‌تواند مخاطراتی را متوجه شما کند.

در مورد امنیت دفتر اغلب باید میان رضایت دادن به حداقل ها و یا انجام اقداماتی آشکار (در صورت نیاز) دست به انتخاب بزنید.

میزان امنیت یک دفتر، بستگی به نقطه ضعف آن دارد.
به عبارت صحیح تر این نقطه ضعف یک دفتر است که میزان امنیت آن را تعیین می کند.

اگر قرار باشد کسی بدون اطلاع شما وارد دفترتان شود، طبیعی است که سراغ دشوارترین مکان ورود و سخت‌ترین شرایط نخواهد رفت. به خاطر داشته باشید که ساده‌ترین روش دسترسی به یک دفتر و مشاهده آنچه که در درون آن در جریان است، گاه به صدا درآوردن در و داخل شدن است!

موقعیت دفتر

فاکتورهایی که هنگام تاسیس یک دفتر باید مدنظر قرار گیرند، عبارتند از: همسایگی، آیا ساختمان در گذشته با افراد خاص و یا فعالیت‌های خاصی مرتبط بوده است، دسترسی به حمل و نقل مشخص و عمومی، میزان خطر روی دادن حوادث، مناسب بودن ساختمان برای تعبیه ابزارها و وسایل امنیتی لازم و ... (برای اطلاع از سایر موارد به برآورد ریسکی که در ادامه ارائه شده است، رجوع کنید).

بررسی اقدامات ایمنی که در سایر ساختمان های منطقه پیرامونی معمول داشته شده‌اند، مفید است. اگر این تدابیر امنیتی شدید باشند، آن را می‌توان نشانه‌ای از ناامن بودن منطقه از لحاظ حدوث "جرایم عام" در نظر گرفت. گفت‌وگو با ساکنان منازل و دفاتر مجاور در مورد امنیت منطقه هم از اهمیت ویژه‌ای برخوردار است. به هر حال، در نهایت باید مطمئن شوید که اقدامات و تدابیر امنیتی که برای دفتر خود اندیشیده اید را می‌توانید بدون جلب توجه بی‌مورد دیگران اجرا کنید، آشنا شدن با ساکنان محلی هم می‌تواند مفید باشد چرا که این افراد می‌توانند اطلاعاتی در مورد حوادث مشکوکی که ممکن است در محله روی دهد، در اختیار شما قرار دهند.

آشنایی با صاحب ملک هم از اهمیت خاص خود برخوردار است. باید او را بشناسید. آیا به چیزی شهرت دارد؟ آیا دلیل وجود دارد که مقامات بتوانند به بهانه آن او را تحت فشار قرار دهند؟ آیا با اجرای اقدامات امنیتی اندیشیده شده از سوی شما مشکلی وجود نخواهد داشت؟

در انتخاب دفتر افرادی که قرار است به آن رفت و آمد داشته باشند را هم باید مد نظر قرا داد. دفتری که در آن قرار است قربانیان برای دریافت توصیه‌های قانونی به آن مراجعه می کنند در مقایسه با دفتری که صرفا مکان فعالیت کارکنان است، قطعا باید تفاوت‌هایی داشته باشد. نحوه دسترسی به دفتر با استفاده از وسایل نقلیه عمومی و لزوم گذر از مناطق ناامن برای رسیدن به دفتر (از منزل کارکنان و یا محل تمرکز اغلب فعالیت‌ها و ...) از جمله مواردی هستند که باید در انتخاب مکان دفتر به آنها توجه شود. ارزیابی مناطق مجاور به ویژه با هدف ممانعت و پیشگیری از اجبار کارکنان برای عبور از محدوده‌ای ناامن، نیز از اهمیت ویژه‌ای برخوردار است.

هنگامی که موقعیت دفتر انتخاب شد، بررسی متناوب و دوره‌ای ابعاد مختلف موقعیت دفتر – که ممکن است در گذر زمان تغییر کرده باشند – نباید به فراموشی سپرده شود. برای مثال ممکن است "عنصری نامطلوب" در همسایگی شما ساکن باشد. این فاکتور می‌تواند شرایط محیطی را متاثر از خود کند و اقدامات و تدابیر امنیتی جدیدی را الزامی سازد.

چک‌لیست مرتبط با انتخاب موقعیت مکانی مناسب برای دفتر	
آمار جنایت و جرم، نزدیکی به اهداف بالقوه مهاجمان مسلح (مناطقی مانند مراکز دولتی یا نظامی)، وجود منطقه‌ای امن برای پناه بردن به آنجا و وجود سازمان‌های ملی یا بین‌المللی که با آنها رابطه دارید	همسایگی
نوع افراد ساکن منطقه، صاحب یا مالک زمین، ساکنین قبلی، کاربردهای قبلی مکان	روابط
یک یا چند مسیر دسترسی مناسب (هر چه تعداد مسیرها بیشتر باشد، باید آن را مزیت تلقی کرد) امکان دسترسی به محل با وسایل نقلیه عمومی یا شخصی	دسترسی
آب ، برق و تلفن	خدمات اولیه
در محوطه پیرامونی	روشنایی خیابان
آتش‌سوزی، سیل، رانش زمین، نگهداری مواد خطرناک، کارخانه‌های دارای فرآیندهای مضر و ...	در معرض حوادث یا مخاطرات طبیعی
استحکام بنا، امکان تعبیه تجهیزات ایمنی، درها و پنجره‌ها، نرده‌ها و موانع امنیتی، نقاط دسترسی (به زیر مراجعه کنید)	ساختار فیزیکی
وجود یک گاراژ یا حداقل یک حیاط یا محوطه سرپوشیده با نرده و یا حفاظ پارکینگ	برای وسایل نقلیه

دسترسی اشخاص ثالث به دفتر: موانع فیزیکی و دستورالعمل مربوط به بازدیدکنندگان

بدیهی است که اولین هدف از اندیشیدن تدابیر امنیتی برای یک دفتر ممانعت از دسترسی افراد غیرمجاز است. فرد یا افراد می‌توانند پس از ورود به دفتر نسبت به سرقت، کسب اطلاعات، قرار دادن چیزی در نقطه‌ای که بعدها بتوانند آن را علیه شما استفاده کنند - مانند مواد مخدر یا اسلحه- و یا حتی به تهدید شما اقدام کنند. آنها ممکن است اقدامات متفاوتی را انجام دهند، اما هدف شما همواره یکسان است: ممانعت از بروز این حوادث.

دسترسی به ساختمان به وسیله **موانع فیزیکی** (نرده‌ها، درها، دروازه‌ها)، یا از طریق **روش‌های فنی** (زنگ خطر به همراه روشنایی) و **دستورالعمل‌های پذیرش بازدیدکننده**، کنترل می‌شود. هر مانع یا دستورالعمل را در این مورد می‌توان یک **فیلتر** تلقی کرد که افراد مایل به ورود به دفتر باید از میان آنها عبور کنند. وضعیت ایده‌آل هنگامی است که این فیلترها با یکدیگر ترکیب شده و چندین لایه محافظ که دارای توانایی ممانعت از انواع و اقسام ورودهای غیرمجاز هستند، شکل دهند.

موانع فیزیکی

موانع به صورت فیزیکی مانع ورود بازدیدکنندگان غیرمجاز می‌شوند. میزان کارآیی و سودمندی مدافع بستگی به استحکام و توانایی پوشاندن

تمامی منافذ ممکن دارد.

شما می‌توانید در سه محدوده برای دفتر خود موانع فیزیکی نصب کنید

۱ محوطه **خارجی**: نرده‌ها، دیوارها و یا سایر موانع که در بیرون باغ یا حیاط نصب می‌شوند

۲ محوطه **ساختمانی یا بنا**

۳ محوطه **درونی**: موانع متعددی را می‌توان در درون هر دفتری برای محافظت از یک، یا چند اتاق تعبیه کرد. این امر به ویژه در مورد دفاتری که تعداد بازدیدکنندگان و میزان آمد و شد آنها بالا است، می‌تواند موثر واقع شود. این موانع فضای عمومی را از فضای خصوصی‌تر جدا کرده و می‌توان این فضای خصوصی را با موانع اضافی باز هم مورد حفاظت بیشتری قرار داد.

محوطه خارجی

دفتر باید به وسیله یک محوطه خارجی واضح و آشکار احاطه شود و از فضای پیرامون (خیابان و ...) جدا شود. استفاده از نرده‌های کوتاه یا بلند، ترجیحا یکپارچه و بلند، امکان دسترسی غیرمجاز را تقلیل می‌دهد. سیم‌های خاردار و یا نرده‌هایی که امکان مشاهده فعالیت‌های درون‌سازمان از میان آنها وجود دارد، چندان مناسب نیستند. توصیه می‌شود از دیوارهای آجری و یا موارد مشابه برای جداسازی محوطه خارجی از فضای عمومی (خیابان و ...) استفاده شود.

محوطه ساختمان یا بنا

این بخش شامل دیوارها، درها، پنجره‌ها و سقف‌ها و بام‌ها می‌شود. اگر دیوارها صلب و استوار باشند، تمامی فضاهای باز و سقف هم صلب و استوار خواهند بود. درها و پنجره‌ها باید دارای قفل و بست‌های کافی بوده و با تعبیه نرده‌هایی متشکل از میله‌های افقی و عمودی که به درون دیوار محکم شده‌اند، تقویت شوند. اگر ساختمان دارای بام است، باید دارای حفاظت مناسبی باشد، یک ورقه فلزی یا لایه‌ای از سرامیک حفاظت لازم را فراهم نمی‌آورد. در صورتی که امکان تقویت بام خانه وجود ندارد، تمامی راه‌های دسترسی ممکن به سطح فوقانی بام را – چه از زمین و چه از ساختمان‌های مجاور – مسدود کنید.

در مناطقی که احتمال حملات مسلحانه وجود دارد، ایجاد مناطق امن در درون دفتر حایز اهمیت است (برای مطالعه در مورد امنیت در محدوده‌های درگیری مسلحانه به فصل ۱۱ مراجعه کنید).

محوطه درونی

در مورد محوطه درونی و یا ساختمان هم موارد مشابه صدق می‌کنند. داشتن مکانی با امنیت مضاعف در داخل دفتر بسیار حایز اهمیت است. ایجاد چنین مکان‌هایی هم معمولا چندان دشوار نیست. برای مثال حتی یک گاوصندوق را هم می‌توان یک محوطه امن درونی محسوب کرد.

نکاتی در مورد کلیدها

- هیچ کلیدی نباید در معرض دسترسی و یا حتی دید بازدیدکنندگان قرار داشته باشد. تمامی کلیدهای را در کمد و یا کشویی که دارای قفل ترکیبی ساده است نگاه دارید. تنها کارکنان باید رمز این قفل را بدانند. برای امنیت بیشتر هر چند مدت، افراد را تغییر دهید.
- اگر کلیدها هر یک دارای برچسب هستند، برای شناسایی و جداسازی آنها هرگز از توصیف و یا نام اتاق مربوطه و یا کشو و یا کمد متناظر با آنها استفاده نکنید. این امر باعث سهولت سرقت می‌شود. از سیستم کدگذاری مبتنی بر اعداد، حروف و یا رنگ استفاده کنید.

اقدامات فنی: روشنایی و زنگ‌های خطر

اقدامات فنی باعث تقویت موانع فیزیکی یا دستورالعمل‌های لحاظ شده برای پذیرش بازدیدکنندگان می‌شوند. تعبیه چشمی در درها، دوربین‌های مدار بسته و یا ارتباطات داخلی و ... از جمله این موارد هستند. (برای لیست جامعی از این اقدامات به بخش‌های بعدی مراجعه کنید).

اقدامات فنی تنها هنگامی موثر هستند که برای ممانعت و بازداشتن متجاوزان به کار گرفته شوند. اقدامات فنی،هنگامی کارآیی دارند که در نهایت به واکنش معین منتهی شوند. برای مثال زنگ خطر باید باعث جلب توجه همسایگان،پلیس و یا یک شرکت خصوصی حفاظت و امنیت شود. اگر این امر روی ندهد و متجاوز نسبت به آن آگاه باشد، این اقدامات دارای ارزش چندانی نبوده و تاثیر آنها تنها به بازداشتن دزدان تازه‌کار و یا ثبت افراد وارد شده به محل، محدود می‌شود.

- روشنایی محوطه پیرامونی ساختمان (برای مثال حیاط،باغ و پیاده‌رو) و فضای مجاور الزامی است.
- زنگ‌های خطر می‌توانند دارای اهداف متعددی باشند، از جمله شناسایی متجاوزین و بازداشتن متجاوزان بالقوه از ورود و یا ادامه تلاش برای دسترسی.

زنگ خطر می‌تواند صدایی هشداردهنده را از درون ساختمان فعال کند، چراغی امنیتی را روشن کرده و یا صدایی بلند (زنگ یا سروصدا) را ایجاد کند یا سیگنالی به یک مرکز امنیتی واقع در خارج ساختمان ارسال کند. زنگ خطرهای صوتی برای جلب توجه مفید هستند اما در شرایط درگیری و یا اگر انتظار نمی‌رود ساکنان منطقه و یا دیگران نسبت به آن واکنش نشان دهند، حتی ممکن است تاثیر ناخوشایند و مضری هم بر جای بگذارد. میان زنگ‌های خطر صوتی و یا فوری (یک نور قوی ثابت و یک نور قرمز منقطع) باید انتخابی هوشمندانه صورت بگیرد. مورد اخیر برای بازداشتن یک مهاجم از ادامه تلاش کافی است چرا که نشان می‌دهد پس از شناسایی اولیه، اقدامی دیگر صورت خواهد گرفت.

زنگ‌های خطر باید در نقاط ورودی (حیاط‌ها،درها، پنجره‌ها و محوطه‌های حساس مانند اتاق‌های حاوی اطلاعات حساس و ذی‌قیمت) نصب شوند. ساده‌ترین و موثرترین زنگ‌های خطر آنهایی هستند که به حسگرهای حرکتی منجر هستند، این حسگرها با درک هر نوع حرکت بلافاصله چراغی را روشن کرده،صدایی را ساطع کرده و یا دوربینی را فعال می‌کنند.

زنگ‌های خطر باید:

- دارای باتری باشند تا حتی در هنگام قطع برق هم بتوانند فعالیت کنند
- دارای تاخیر زمانی باشند تا در صورتی که بر اثر اشتباه کارکنان فعال شدند امکان غیرفعال کردن آنها وجود داشته باشد
- امکان فعال سازی دستی آنها وجود داشته باشد تا در مواردی خاص که کارکنان نیازمند آن هستند بتوانند آن را فعال کنند
- نصب و تعمیر آنها ساده باشد
- امکان تفکیک آنها از هشداردهنده‌های آتش وجود داشته باشد.

دوربین‌های ویدیویی

دوربین‌های ویدیویی در بهبود دستورالعمل‌های پذیرش مراجعین موثر هستند (به موارد زیر توجه کنید). آنها همچنین می‌توانند ورود افراد را ثبت کنند. با این وجود ثبت تصاویر باید در منطقه‌ای صورت گیرد که دور از دسترس متجاوزان قرار داشته باشد، چرا که در غیر این صورت مهاجمان می توانند محفظه دوربین را شکسته و نوار ویدیویی را نابود کنند.

شما ممکن است مجبور به تصمیم‌گیری در مورد استفاده از دوربین‌های ویدیویی باشید. آیا این دوربین‌ها ممکن است به عنوان کالایی باارزش به جلب نظر سارقان بیانجامد؟ در صورتی که از دوربین‌های ویدیویی استفاده می کنید، بهتر است هشداری در این زمینه بر دیوار نصب شود. (فراموش نکنید که حق حریم خصوصی، یکی از حقوق بشر است)

شرکت‌های خصوصی تامین امنیت

در این مورد باید به شدت مراقب باشید. در بسیاری از کشورها شرکت‌های خصوصی تامین امنیت توسط ماموران امنیتی سابق اداره می‌شوند.

موارد مستندی وجود دارد که چنین افرادی در جاسوسی از مدافعین و یا حملات به آنها دست داشته‌اند. در صورتی که نگران جاسوسی نیروهای امنیتی و یا حملات آنها هستید، بنا به دلایل منطقی بهتر است به این شرکت‌های خصوصی تامین امنیت هم اعتماد نکنید. اگر یک شرکت خصوصی تامین امنیت به دفتر شما دسترسی داشته باشد، به سادگی می‌تواند میکروفون‌هایی را برای شنود در دفتر شما کار گذاشته و یا امکان ورود به دفتر را برای اشخاص غیرمجاز فراهم کند.

اگر احساس می‌کنید که به حضور چنین شرکتی نیاز دارید باید مطمئن شوید که در مورد اقداماتی که پرسنل این شرکت از طرف شما مجاز به انجام آن هستند و اقداماتی که مجاز به انجام آن نیستند، به توافقی واضح رسیده‌اید. همچنین باید مناطقی از ساختمانی را که آنها حق دسترسی به آن را دارند با مناطقی که مجاز به دسترسی به آن نیستند، به وضوح مشخص کنید. در نهایت باید این امکان را داشته باشید که بر اجرای این توافقات نظارت کنید.

برای مثال

موردی را در نظر بگیرید که شما از خدمات امنیتی شرکتی بهره می‌گیرید که در صورت فعال شدن سیستم هشداردهنده ماموری را به محل دفتر شما اعزام می‌کند. این مامور ممکن است به برخی بخش‌های حساس دفتر شما دسترسی داشته و تجهیزات استراق سمع را در آن منطقه- در اتاق ملاقات شما برای مثال- تعبیه کند.

بهتر است در صورت امکان در مورد شخص خاصی که قرار است مسوولیت رسیدگی به مسائل امنیتی مرتبط با دفتر شما را بر عهده گیرد، به توافق رسیده و بر ایفای این وظیفه، صرفا توسط او نظارت کنید. این امر اما در اغلب موارد امکان‌پذیر نیست.

در صورتی که ماموران امنیتی شرکت مزبور سلاح حمل می‌کنند، برای یک سازمان حقوق بشر بسیار مهم است که نسبت به شرایطی که این ماموران از سلاح استفاده می‌کنند، کاملا توجیه و مطلع شده باشند. فارغ از این موضوع بررسی مزایای احتمالی وجود مامور مسلح با امکان استفاده از سلاح در مقابل نقاط ضعف آن حایز اهمیت است. بدیهی است سلاح‌های کوچک در مقابل مهاجمین با قدرت آتش بالاتر (موردی که معمولا روی می‌دهد) کارآیی چندانی ندارند اما اگر مهاجمان بدانند که در محوطه ساختمان شما افرادی هستند که سلاح حمل می‌کنند (سلاح سبک)، ممکن است تصمیم بگیرند هنگام ورود اجباری به محل برای حفاظت از خود، آماده گشودن آتش شوند. به عبارت دیگر ظرفیت تسلیحاتی کم (سلاح‌های سبک) ممکن است به احتمال قوی منجر به این شود که مهاجمان از توان آتش به مراتب بالاتر خود استفاده کنند. در چنین شرایطی شاید بهتر باشد از خود بپرسید که آیا برای حفظ امنیت خود به محافظین مسلح به مسلسل و تیربار نیاز دارید، آیا اصولا فضای سیاسی- اجتماعی لازم برای تداوم فعالیت شما وجود دارد؟

فیلترهای ورودی

موانع فیزیکی باید با دستورالعمل‌ها یا فیلترهای ورودی ترکیب شوند چنین دستورالعمل‌هایی تعیین‌کننده این هستند که چه هنگام و چگونه، چه کسی به هر بخشی از دفتر دسترسی پیدا می‌کند. دسترسی به حوزه‌های حساس، همانند کلیدها، اطلاعات و یا پول، باید تا حد امکان محدود شود.

ساده‌ترین راه برای ورود به دفتر محل فعالیت مدافعین حقوق بشر، به صدا در آوردن در و وارد شدن به دفتر است! افراد بسیاری هر روزه به همین روش وارد دفاتر مدافعین حقوق بشر می‌شوند. برای ایجاد هماهنگی میان ویژگی "گشوده بودن درهای دفتر مدافعین حقوق بشر بر روی همگان" با نیاز به کنترل افرادی که به دلایل مختلف قصد ملاقات با شما را دارند، به تدوین و اجرای دستورالعمل‌های مناسب پذیرش نیاز دارید.

به طور کلی، مردم باید دلیل خاص برای ورود به یا به صدا در آوردن در محل کار شما داشته باشند. آنها اغلب خواهان طرح پرسش و یا انتقال چیزی، بدون اینکه الزاما اجازه گرفته باشند، هستند. بگذارید این موضوع را به صورت مورد به مورد بررسی کنیم.

شخصی مراجعه کرده و خواهان ورود، به دلیلی خاص می‌شود.

در چنین شرایطی باید سه گام ساده را طی کنید:

۱ ◆ بپرسید که چرا شخص مزبور خواستار ورود است

اگر او خواهان دیدار با شخصی در دفتر است، با شخص مورد نظر تماس بگیرید. اگر وی حضور نداشت از مراجع بخواهید زمانی دیگر بازگشته و یا در خارج از محدوده دفتر منتظر باشد. استفاده از چشمی‌ها، دوربین‌ها و یا آیفون برای اجتناب از گشودن در و یا نزدیک شدن به آن بسیار مهم است، به ویژه اگر قصد دارید مانع ورود کسی شده و یا احتمال ورود همراه با خشونت و درگیری را می‌دهید، بهتر است محیط انتظاری که به صورت فیزیکی مجزا از ورودی داخلی دفتر است، ایجاد کنید. اگر الزاما باید فضایی با دسترسی عام در داخل دفتر داشته باشید، مطمئن شوید که با موانع فیزیکی به صورتی موثر آن را از مناطق مهم دفتر جدا کرده‌اید.

ممکن است فردی به منظور چک و یا تعمیر آب، الکتریسیته و یا سایر کارهای تعمیراتی تقاضای ورود کند. او می‌تواند حتی ادعا کند که نماینده یک رسانه است یا یک مقام دولتی و ... همواره بیش از صدور اجازه ورود هویت این افراد را با شرکت، سازمان و یا موسسه‌ای که ادعا می‌کنند از سوی آن اعزام شده‌اند، چک کنید. به خاطر داشته باشید که نه یونیفورم و نه کارت شناسایی، هیچ یک تضمین کننده مطمئنی برای هویت شخص نیستند. این امر به ویژه در مواردی که با سطح متوسط یا بالایی از مخاطرات روبه‌رو هستید، باید جدی‌تر تلقی شود.

۲ ◆ تصمیم گیری در مورد صدور یا عدم صدور اجازه دسترسی

هنگامی که دلیل درخواست و رد بازدیدکننده مشخص شد، شما باید تصمیم بگیرید که آیا باید به او اجازه ورود بدهید یا خیر. اگر شخصی دلیلی برای درخواست ورود خود عنوان می‌کند، این بدان معنی نیست که شما باید الزاما به او اجازه ورود بدهید. اگر مطمئن نیستید که قصد آنها از ورود چیست، به آنها اجازه ورود ندهید.

۳ ◆ نظارت بر بازدیدکنندگان تا هنگام ترک محل

هنگامی که بازدیدکننده‌ای وارد دفتر شد، مطمئن شوید که شخصی در تمام اوقات، تا هنگام ترک ساختمان، بر آنها نظارت دارد. داشتن محوطه‌ای برای ملاقات با بازدیدکنندگان، خارج از محدوده حساس (با دسترسی محدود) بسیار موثر است.

در مورد تمامی بازدیدکنندگان باید اطلاعات آنها، مواردی چون نام، سازمان، هدف و علت دیدار، شخص ملاقات شونده، هنگام ورود و هنگام خروج، ثبت و نگاهداری می‌شود. این اطلاعات به ویژه هنگامی که قرار است پس از یک رویداد امنیتی، اقدامات اشتباهی که به بروز آن منجر شده‌اند شناسایی و برطرف گردند، از اهمیتی به‌سزا برخوردار می‌گردند.

شخصی تماس گرفته یا به دفتر آمده و پرسش های متعددی را مطرح می کند

فارغ از آن چه که تماس گیرنده یا بازدید کننده ممکن است بگوید شما تحت هیچ شرایطی نباید به آنها موقعیت مکانی و با اطلاعات شخصی مرتبط با همکار و یا سایر افراد در ارتباط با مجموعه را بدهید. اگر شخص پرسش کننده سماجت به خرج داد از او بخواهید تا پیامی برای شخص مورد نظرش بگذارد، یا چند ساعت بعد برگردد و یا بالاخره زمانی را برای ملاقات تعیین کند تا شما به اطلاع شخص مورد نظر برسانید.

افراد همیشه ممکن است بر اثر اشتباه وارد مکانی شوند و پرسش هایی چون آیا فلانی و فلانی اینجا زندگی می کنند یا آیا فلان چیز برای

فروش گذاشته شده است را مطرح کنند. گدایان هم برای درخواست کمک می توانند وارد محلی شوند. درصورتی که مانع دسترسی این افراد به اطلاعات و یا مکان های حساس شده و اطلاعاتی هم به آن ها ندهید سطح مخاطرات امنیتی خود را به شدت کاهش خواهید داد.

شخصی می خواهد شی یا بسته ای را به دست شخصی برساند

خطری که بسته ها یا اشیا متوجه شما می کنند در این واقعیت ساده نهفته است که محتوی آن ها می تواند به شما صدمه برساند مصداق این امر ار می توان در بمب های نامه ای یا بسته ای مشاهده کرد. به هر حال گذشته از این که یک بسته تا چه میزان عادی و بی گناه! به نظر برسد هرگزپیش از طی سه گام اولیه زیر نه به آن دست بزنید و نه آن را جابجا کنید:

۱ ◆ اطمینان حاصل کنید که شخصی که قرار است بسته به دست او برسد انتظار دریافت چنین بسته ای را داشته است.

شناسایی فرستنده از سوی گیرنده (فرد درون سازمان) کافی نیست چرا که هویت فرستنده به سادگی قابل جعل است. اگر مشخص شد که گیرنده انتظار بسته ای را ندارد وی باید با فرستنده ای که نام و یا مشخصاتش بر روی بسته درج شده است تماس گرفته و تایید ارسال بسته از سوی آن ها را بگیرد. اما اگر بسته مخاطب مشخص نداشته و برای سازمان فرستاده شده است باید هویت فرستنده تایید شده و سپس بعد از بررسی و بحث در مورد بازکردن آن تصمیم گیری شود.

۲ ◆ تصمیم بگیرید که آیا بسته ای را قبول کنید یا خر ؟

اگر نمی توانید هویت فرستنده را تایید کنید و یا اگر این امر مستلزم صرف زمانی طولانی است بهترین گزینه عدم دریافت بسته است. این گزینه در مناطقی با سطح مخاطه بالا و یا متوسط اهمیت و کاربرد بیشتری دارد. یادتان باشد که همیشه می توانید بسته مورد نظر راپس از تایید هویت فرستنده از اداره پست دریافت کرده و یا از خود شخص بخواهید مجددا آن را برایتان ارسال کند

۳ ◆ بسته را در داخل اداره ردیابی کنید

مطمئن شوید که مکان بسته در داخل اداره را تا زمان رسیدن آن به دست دریافت کننده نهایی در هر لحظه می دانید.

درجریان گردهمایی ها و میهمانی ها

در این شرایط یک قاعده ساده وجود دارد : در وهله اول اجازه ورود به اشخاصی که نمی شناسید را ندهید. تنها افرادی که توسط همکاران معتمد شما مورد تایید و شناسایی قرار می گیرند امکان ورود خواهند یافت آن هم در شرایطی که شخص تایید کننده خود در مکان حاضر بوده و شخصا هویت میهمانش را تایید کند. اگر افرادی مراجعه کرده و خود را از آشنایان شخصی در دفتر شما معرفی کردند و شخص مزبور در محل حضور نداشت ، به آنها اجازه ورود ندهید.

ثبت تماس های تلفنی و بازدیدکنندگان

نگاهداری سابقه تماس های تلفنی ، شماره های تلفن و نیز افرادی که از دفتر شما بازدید کرده اند ممکن است مفید باشد. در برخی ادارات و سازمان ها از بازدید کنندگان خواسته می شود تا سند و یا مدرکی برای احراز هویت خود یا کارت شناسایی ارائه دهند . مشخصات این مدرک نیز توسط متصدی مربوطه ثبت می شود.

اضافه کاری در دفتر :

برای کلیه کارکنانی که در ساعاتی فراتر از ساعات عادی مشغول به کار هستند باید دستورالعملی وجود داشته باشد. افرادی در سازمان که قصد دارند ساعات اضافی در طی شب به کار بپردازند باید در فواصل زمانی مخصوص به فردی معین شده گزارش بدهند و همزمان هنگام ترک محوطه نز مراقبت های لازم را به عمل آورند.

چک لیست : شناسایی نقاط ضعف در دستورالعمل های مربوط به بازدید کنندگان
چه کسی وبه **چه علت** دسترسی منظم به **چه محدوده هایی** را داراست؟ دسترسی ها را مگر در موارد مطلقا ضروری محدود کنید.
میان **انواع گوناگون** بازدید کنندگان تفاوت قائل شوید (پیک ها، تعمیرکاران فنی، اعضای سازمان های غیر دولتی، میهمانان مهم و مدعوین برای جلسات و ...) **برای هر گروه باید دستورالعمل ورودی خاص تدوین شود**. تمامی کارکنان سازمان باید با این دستورالعمل ها آشنا بوده و در قبال اجرای آن ها احساس مسئولیت کنند.
آیا بازدید کننده هنگام ورود می تواند به نقاط ضعف شما دسترسی داشته باشد؟ اگر پاسخ مثبت است با تدوین استراتژی مانع این امر شوید
چک لیست : دسترسی به کلیدها
چه کسی به **چه** کلیدهایی و **چه زمانی** دسترسی دارد؟
کلیدها و **کپی آن ها** کجا و چگونه **نگهداری** می شوند؟
آیا سابقه ای از کپی های موجود در دست افراد و اعضا وجود دارد؟
آیا این خطر وجود دارد که شخصی **بدون کسب مجوز** از کلید کپی بسازد؟
درصورتی که **شخصی کلیدی را گم کند**، چه روی می دهد؟ قفل متناظر با آن کلید باید عوض شود، مگر اینکه کاملا مطمئن باشید که کلید به صورت تصادفی در مکانی نامعلوم جا گذاشته شده است و هیچ کس به هیچ نحوی نمی تواند صاحب کلید و یا آدرس وی را بیابد. به خاطر داشته باشید که ممکن است کلیدها به سرقت بروند ، برای مثال ممکن است برای سرقت کلیدها و فراهم آوردن امکان دسترسی بعدی به مناطق از دفتر ، حتی یک سرقت نمایشی هم صورت بگیرد.

تمامی اعضای دفتر وظیفه برخورد با افرادی را دارند که دستورالعمل های مربوط به ورود افراد را به درستی اجرا نمی کنند. افراد همچنین باید در دفترچه های اختصاص یافته به رویدادهای امنیتی هر نوع حرکت مشکوک افراد و یا حضور غیر معمول وسایل نقلیه را نیز درج کنند. این امر در مورد اشیای غیرعادی که در بیرون محوطه دفتر قرار داده شده اند هم صادق است چرا که بدینوسیله می توان احتمال انفجار بمب را به شدت کاهش داد. اگر مظنون هستید که شی یا بسته ای محتوی بمب است از کنار آن بی تفاوت نگذرید، به آن دست نزنید و باپلیس تماس بگیرید.

هنگام تعویض مکان دفتر و یا هنگام گم شدن یا به سرقت رفتند کلیدها ، باید حداقل تمامی قفل های ورودی ها را تعویض کنید.

چک لیست: دستورالعمل های عام برای امنیت دفتر

- کپسول های اطفای حریق و چراغ قوه (با باتری قبل تعویض) در اختیار داشته باشید. مطمئن شوید که تمامی کارکنان با نحوه کار با آن ها آشنا هستند.

- اگر احتمال قطع برق زیاد است باید ژنراتور برق داشته باشید. قطع برق می تواند امنیت شما را به ویژه در مناطق روستایی به خطر بیاندازد(قطع سیستم های هشدار دهنده، نور ، تلفن و ...)

- لیستی از شماره تماس های اضطراری مربوط به ادارات‌پلیس و آتش نشانی محلی ، آمبولانس و بیمارستان نزدیک به محل کار را برای موارد اضطراری تهیه کنید.
- اگر امکان بروز درگیری در آن نزدیکی وجود دارد ذخیره ای از آب و مواد غذایی را نگاه دارید.
- موقعیت مکان های امن خارج از دفتر خود را برای موارد اضطراری شناسای کنید(برای مثال دفاتر سایر سازمان ها)
- هیچ شخصی از خارج سازمان نباید در مکانی آسیب‌پذیر و یا با امکان دسترسی به کلید ها اطلاعات و یا چیزهای ارزشمند، **تنها** باقی بماند.
- **کلیدها :** هرگز کلیدها را در مکانی که ممکن است بازدیدکنندگان به آنها دسترسی داشته باشند قرار ندهید .پنهان کردن کلیدها بیرون ورودی دفتر، اصلا باعث‌پنهان ماندن آن ها نمی شود بلکه میزان احتمال دسترسی به آنها را افزایش می دهد.
- **دستورالعمل های ورودی:** اگر مهاجمی بالقوه وارد دفتر شود موانع امنیتی عملا باعث حفاظت از شما نمی شوند. به همین جهت باید موراد زیر را در ذهن داشته باشید:
  - تمامی کارکنان به صورت مشابه و مساوی در کنترل بازدید کنندگان و ورود افراد مسئول هستند
  - بازدیدکنندگان مادام حضور در دفتر نباید به حال خود رها شوند. آن ها باید همراه داشته باشند.
- اگر بازدیدکننده ای غیر مجاز را در درون دفتر یافتید:
  - هرگز با کسی که به نظر می رسید آماده استفاده از خشونت برای رسیدن به‌خواسته خود است(برای مثال افراد مسلح) درگیر نشوید. در این موارد به همکاران خود هشدار داده ، مکانی امن برای اختفا بیابید و سعی کنید ازپلیس کمک بگیرید.
  - با دقت به شخص مورد نظر نزدیک شده و از افراد داخل دفتر و یاپلس طلب کمک کنید.
- در شرایطی با مخاطره بالا ، همیشه کنترل چیزهای باارزش را در اختیار داشته باشید(برای مثال اطلاعات ذخیره شده بر روی دیسک سخت) تا بتوانید در وضعیت های اضطراری آن ها را از دسترس مهاجمین دور کنید.
- به خاطر داشته باشید که به هر حال در هر مقابله ای با افراد مهاجم، کارکنان دفتر در خط مقدم درگیری قرار می گیرند. مطمئن شوید که کارکنان آموزش های لازم را دیده و آماده تعامل با چنین شرایطی ، بدون آن که خود را در معرض مخاطره ای جدی قرار دهند، هستند.

بازبینی منظم و امنیت دفتر

بازبینی و یا بازرسی مداوم امنیت دفتر از اهمیت ویژه‌ای برخوردار است چرا که شرایط امنیتی و دستورالعمل‌های مرتبط با آن در گذر زمان تغییر می‌یابند چرا که برای مثال ممکن است تجهیزات نصب شده از کار بیافتد و یا میزان بازدیدکنندگان و یا تعداد کارکنان تغییر یابند. به هر حال باید در نظر داشت که در میان کارکنان باید نوعی احساس مالکیت نسبت به قواعد امنیتی دفتر شکل بگیرد.

فرد مسوول امنیت باید حداقل **هر شش ماه یک بار** امنیت دفتر را مورد بازبینی و بررسی قرار دهد. با کمک لیست زیر این امر می‌تواند به سادگی و با صرف زمانی حداکثر یک یا دو ساعته صورت گیرد. فرد مسوول امنیت باید اطمینان حاصل کند که پرسنل و کارکنان نظرات خود را پیش از مکتوب شدن گزارش نهایی ارائه کرده‌اند. پس از این است که او می‌تواند گزارش امنیتی را برای اتخاذ تصمیمات مقتضی و یا اقدامات لازمه به سازمان ارائه کند. گزارش باید برای مقایسه با گزارش آتی، ثبت و نگاهداری شود.

چک‌لیست : بازنگری امنیت دفتر

بازبینی :

انجام شده توسط:

تاریخ:

۱- تماس اضطراری:

- آیا لیست به روز شده و قابل دسترسی از شماره تلفن‌ها و نشانی‌های سایر سازمان‌های غیردولتی، اورژانس‌ها و بیمارستان‌ها، پلیس، آتش‌نشانی و آمبولانس وجود دارد.

۲- موانع فنی و فیزیکی (خروجی،داخلی و درونی):

- بررسی شرایط و نحوه عملکرد درهای خروجی، نرده‌ها، درهای ساختمان، پنجره‌ها، دیوارها و سقف
- بررسی شرایط و نحوه عملکرد روشنایی خارجی، سیستم‌های هشداردهنده، دوربین‌ها یا آیفون‌های تصویری
- بررسی دستورالعمل‌های کلیدی مانند نگاهداری کلیدها در مکان امن و کدگذاری آنها، احاله وظایف برای کنترل کلیدها و ساختن کلیدهای یدک، حصول اطمینان از کارکرد درست کلیدها و کلیدهای یدک، حصول اطمینان از عوض شدن قفل‌ها پس از گم شدن یا دزدیده شدن کلیدها و در نهایت حصول اطمینان از ثبت چنین رویدادهایی

۳- دستورالعمل‌های ورود بازدیدکنندگان و فیلترها :

- آیا برای تمامی انواع بازدیدکنندگان دستورالعمل‌های متناظر اجرا می‌شود؟ آیا تمامی کارکنان با این دستورالعمل‌ها آشنا هستند؟
- بازبینی تمامی رویدادهای امنیتی ثبت شده در ارتباط با دستورالعمل‌های ورودی و یا فیلترها
- پرس‌وجو کردن از کارمندان مسوول اجرای این دستورالعمل‌ها در مورد کارآیی و یا لزوم ارتقای آنها

۴- امنیت در برخورد با حوادث:

- شرایط و وضعیت آتش خاموش‌کن‌ها، شیرفلکه‌ها یا لوله‌های گاز، شیرهای آب، کابل‌ها، پریزهای برق و ژنراتورها (در صورت وجود) بررسی شوند.

۵- مسوولیت و آموزش:

- آیا مسوولیت امنیت دفتر به افراد خاص محول شده است؟ آیا این امر موثر بوده است؟
- آیا برنامه آموزشی در مورد امنیت دفتر وجود دارد؟ آیا تمامی موارد ذکر شده در این فهرست در آن گنجانده شده‌اند؟ آیا تمامی کارکنان جدید آموزش‌های لازم را به نحو موثری پشت‌سر گذاشته‌اند؟

فصل دهم

امنیت و مدافعین زن حقوق بشر

هدف:

بررسی نیازهای امنیتی ویژه مدافعین زن حقوق بشر

در این بخش سعی می‌شود تا برخی از نکات کلیدی در مورد نیازهای خاص مدافعین زن حقوق بشر بررسی شوند. بررسی این موضوع نیازمند تحلیل عمیق تجارب عملی مدافعین زن حقوق بشر است. به همین جهت مباحث مفصل تری درباره این موضوع در جلسه مشاوره بین‌المللی در مورد مدافعین زن حقوق بشر که در سال ۲۰۰۵ برگزار شده، ارائه گردیده است.

زنان به عنوان مدافعین حقوق بشر

زنان همواره در ارتقا و حفاظت از حقوق بشر بازیگرانی مهم و تاثیرگذار بوده‌اند، با این وجود نقش آنان هرگز آن گونه که شایسته بوده، مورد توجه قرار نگرفته است. زنان به صورت منفرد و یا در کنار مردان برای دفاع از حقوق بشر فعالیت می کنند.[۸] اکنون تعداد بی‌شماری از زنان در سازمان‌هایی فعالیت می کنند که به امور افراد مفقود شده و یا زندانیان رسیدگی می کنند. سایرین در دفاع از حقوق گروه‌های اقلیت و یا قربانیان خشونت‌های جنسی فعالند و جمعی هم در کسوت فعالان اتحادیه‌های تجاری، وکلا و فعالان حقوق بشر در زمینه "حقوق زمین" فعالیت می کنند.

حملات به مدافعین زن حقوق بشر

هینا جیلانی نماینده ویژه دبیرکل سازمان ملل در امور مدافعین حقوق بشر در گزارش سالانه خود (۲۰۰۲) به کمیسیون حقوق بشر می گوید: "مدافعین زن حقوق بشر همراه همکاران مرد، خود را در خط مقدم ارتقا و حفاظت از حقوق بشر قرار داده‌اند. در چنین وضعیتی، مدافعین زن با توجه به جنسیت خود، عملا با مخاطراتی افزون‌تر از همکاران مرد خود مواجه هستند".

زنان در وهله نخست، بیش از مردان مورد توجه قرار می گیرند. به عبارت دیگر زنان به عنوان مدافعین حقوق بشر در فعالیت‌های خود با واکنش‌های خصومت‌آمیز بیشتری مواجه می‌شوند چرا که ممکن است فعالیت‌های آنها برخلاف باورها و هنجارهای فرهنگی، مذهبی و یا اجتماعی موجود در مورد زنانگی و نقش زنان در برخی جوامع و یا کشورها تلقی گردد.

در چنین بستری، نه تنها آنها ممکن است به علت فعالیت‌های خود به عنوان مدافع حقوق بشر با نقض حقوق بشر و تجاور به حقوق خود مواجه شوند که حتی ممکن است در مقایسه با همکاران مرد خود مجبور به پذیرش مخاطرات بیشتری گردند چرا که اقدامات آنها عملا با

باورهای جامعه در مورد طبیعت فرمانبردار زن همخوانی نداشته و حتی تلقی جامعه در مورد وضعیت زنان را به چالش بکشد.

در وهله دوم، نمی توان این امکان را از نظر دور داشت که خصومت، آزار و اذیت و سرکوب مدافعین زن، ممکن است به اقتضای جنسیت آنها شکل و شیوه خاصی به خود بگیرد. به صورت نمونه می توان به سوءرفتار لفظی با زنان (با توجه به جنسیت آنان) و یا مواردی چون آزار و اذیت جنسی و یا حتی تجاوز اشاره کرد. در این ارتباط موقعیت حرفه‌ای و جایگاه زنان در جامعه ممکن است مورد تهدید قرار گیرد. این تهدیدات عموما متناظر با جنسیت آنها است. موارد آشنایی چون زیر سوال بردن پاکدامنی زنان هنگامی که آنان می خواهند از حق خود برای برخورداری از سلامت جنسی و بارداری دفاع کرده و یا همانند مردان زندگی عاری از خشونت و تبعیض را بگذرانند، از جمله این تهدیدات به شمار می روند. گاه مشاهده می شود که فعالان زن حقوق بشر به استناد قوانینی که فعالیت در جهت بهره برداری از حقوق طبیعی و یا دفاع از حقوق بشر را عملی مجرمانه تلقی می کنند، محکوم می شوند. این زنان تنها به خاص باورها و دیدگاهایشان و پایداری در دفاع از حقوق بشر محکوم می شوند.

در وهله سوم، باید در نظر داشت که نقض حقوق بشر در مورد مدافعین زن ممکن است پیامدهای خاص و متناظر با جنسیت آنها را در برداشته باشد. برای مثال سوءاستفاده جنسی از یک فعال زن حقوق بشر که در بازداشت به سر می برد و تجاوز به او می تواند به بارداری و انتقال بیماری آمیزشی- چون ایدز- منجر شود.

ارتقا و دفاع از برخی از حقوق خاص زنان تنها به وسیله مدافعین زن امکان پذیر است. ارتقا و دفاع از حقوق زنان می تواند عاملی برای افزایش سطح مخاطرات باشد چرا که اعمال برخی از این حقوق تهدیدی نسبت به نظام مرد سالار حاکم محسوب شده و همزمان هنجارهای فرهنگی، مذهبی و اجتماعی را هم به هم می ریزد. دفاع از حق حیات و آزادی زنان در برخی کشوها به بهای حیات و آزادی خود مدافعین تمام شده است. به صورت مشابه اعتراض به اعمال تبعیض آمیز علیه زنان گاه به محاکمه یک فعال زن برجسته حقوق بشر به اتهام "ارتداد" منتهی شده است.

عواملی چون سن، قومیت، پس زمینه تحصیلی، وضعیت تاهل و تمایلات جنسی را نیز باید در بررسی مخاطراتی که متوجه مدافعین زن حقوق بشر می شوند، لحاظ کرد، چرا که گروه‌های مختلف مدافعین زن، هر یک با چالش های متفاوتی روبه‌رو شده و لذا نیازهای امنیتی و حفاظتی آنها هم متفاوت هستند.

ارزیابی نیازهای حفاظتی مدافعین زن اغلب در تعیین و آشکار شدن نیازهای متفاوت و خاص هر یک از گروه‌ها، آسیب پذیری ها و استراتژی‌های متناظر آنان نیز مفید است. بدین ترتیب شرایط و موقعیت آنان را به صورتی جامع تر و مناسب تر می توان در شرایط اورژانس و یا روزمره مد نظر قرار داد.

امنیت برای مدافعین زن حقوق بشر

مدافعین زن حقوق بشر برای فعالیت‌های خود در محافظت و ارتقای حقوق انسانی دیگران، بهایی سنگین پرداخت می کنند. مدافعین زن باید با مخاطراتی مختص جنس خود مواجه شده و بدین ترتیب امنیت آنها مستلزم در نظر داشتن رویکردی خاص است چرا که:

زنان ممکن است ناخواسته جلب توجه کنند

مدافعین زن ممکن است خصومت‌ها را علیه خود برانگیزند چرا که زن بودن و فعالیت کردن به عنوان یک مدافع حقوق بشر، به صورت توامان ممکن است باعث نقض هنجارهای اجتماعی، مذهبی و یا فرهنگی جامعه و باورهای افراد در مورد زنانگی و نقش زنان شود. مدافعین زن بدین ترتیب ممکن است با مواردی از نقض حقوق بشر مواجه شوند که علت آن تنها در فعالیت‌های آنان خلاصه نمی شود بلکه گاه ریشه در

این مساله دارد که فعالیت زن و یا ایفای نقش مدافع حقوق بشر از سوی یک زن، باورهای جامعه در مورد طبیعت فرمانبردار و موقعیت زنان را بر هم می‌ریزد.

مدافعین زن ممکن است مجبور به شکستن قوانین مردسالارانه و یا تابوهای اجتماعی شوند

در برخی کشورها دفاع از حق حیات و آزادی زنان به بهای نقض حق حیات و آزادی خود مدافعین حقوق بشر منتهی شده است. به صورت مشابه گاه اعتراض در مورد اقدامات تبعیض‌آمیز علیه زنان باعث شده است تا یک مدافع برجسته حقوق بشر به اتهام ارتداد محاکمه شود. در بسیاری از فرهنگ‌ها، این الزام که زن باید در ملاء عام تسلیم خواست و اراده مردان باشد، ممکن است مانعی جدی بر سر راه زیر سوال بردن موارد نقض حقوق بشر از سوی مردان، توسط فعالان زن در ملاء عام باشد. در برخی موارد تعابیر تبعیض‌آمیز و یا جنسیتی از متون مذهبی، اغلب برای تثبیت و یا تصویب قوانین و یا رفتارهایی که بر حقوق زنان تاثیری جدی دارند، به کار گرفته می‌شوند.

گونه‌های خاصی از حمله به مدافعین زن وجود دارد

رفتار خصومت‌آمیز، آزار و اذیت و سرکوبی که مدافعین زن با آن مواجه می‌شوند ممکن است منحصر به جنسیت آنها باشد، مواردی چون سوء استفاده لفظی نسبت به آنان و یا آزار و اذیت جنسی و تجاوز نمونه‌هایی از این حملات خاص هستند. عواقب این قبیل حملات هم ممکن است منحصر به جنسیت آنان باشد؛ مواردی چون حاملگی و یا طرد از اجتماع.

مدافعین زن برای اثبات استحکام شخصیت خود تحت فشار قرار می‌گیرند

موقعیت حرفه‌ای زنان و جایگاه آنان در جامعه هم ممکن است به روش‌های معتبر زیر سوال رفته و یا تهدید شود. زیر سوال بردن استحکام شخصیت و ثبات آنان (با توجه به برخی باورها در مورد زنان) از جمله این روش‌هاست.

همکاران مرد ممکن است فعالیت‌های مدافعین زن را درک نکرده و یا حتی رد کنند

همکاران مرد مدافعین زن ممکن است دارای همان تعصبات اجتماعی باشند که افراد بیرونی که به مدافعین زن حمله می‌کنند، از آن برخوردارند. مردان همچنین ممکن است از رقابت‌های حرفه‌ای با یک زن احساس تهدید کنند. این امر می‌تواند باعث به حاشیه رانده شدن و یا بی‌توجهی و نادیده گرفته شدن مدافعین زن شده و حتی در مواردی به آزار و اذیت و خشونت علیه مدافعین زن، از سوی همکارانشان منتهی شود.

مدافعین زن ممکن است با خشونت‌های داخلی مواجه شوند

خشونت‌های داخلی ناشی از تغییر ساختار قدرت در درون خانواده هستند. افزایش و پر رنگ شدن نقش حرفه‌ای یک مدافع زن و قدرت گرفتن او، ممکن است همسر، شریک و یا سایر اعضای خانواده را دچار احساس تهدید کرده و باعث شود آنان سعی کنند تا مانع فعالیت‌های وی شده و یا حتی در مواردی روی به خشونت بیاورند. خشونت‌های داخلی علیه زنان تمامی انواع فیزیکی و صدمات روانی و جنسی که در درون خانواده روی می‌دهد – مواردی مانند ضرب و شتم، رابطه جنسی بدون رضایت، معلولیت و صدمه زدن به اندام‌های جنسی زنانه و سایر روش‌های سنتی که علیه زنان به کار گرفته می‌شوند – را در بر می‌گیرند. (توضیحات بیشتر در بخش‌های بعدی ارائه می‌شود).

الزامات اضافی خانوادگی

بسیاری از مدافعین زن علاوه بر فعالیت‌های روزمره باید از فرزندان و سایر بستگان خود نیز حفاظت کنند. این وظایف به ویژه اگر شامل حفاظت از کودکان خردسال نیز باشد، بر بسیاری از تصمیمات امنیتی که یک مدافع زن مجبور است در وضعیتی که با مخاطرات بالایی روبه‌رو است، تاثیر می‌گذارد.

حرکت به سوی امنیت

شناسایی این موضوع که مدافعین زن حقوق بشر دامنه گسترده‌ای از افراد را که با مشکلات متعدد روبه‌رو هستند، دارای سوابق و پس‌زمینه‌های متفاوت بوده و نیازمند راه‌حل‌های متفاوت هستند، شامل می‌شوند. مهمترین نکته‌ای که باید به خاطر داشت این است که در هر شرایط مفروضی، زنان مدافعین حقوق بشری هستند که می‌توانند مشکلات را شناسایی کرده و برای آنها راه حل‌های مناسبی بیاندیشند. برای یافتن این چاره‌ها، ترکیبی از هدایت مشارکت فزاینده زنان و همزمان حصول اطمینان از لحاظ شدن نیازهای امنیتی خاص زنان (با توجه به جنسیت آنها) باید مورد بررسی قرار گیرند. در این شرایط آموزش زنان در حوزه‌های زیر ضروری است:

هدایت مشارکت زنان

به صورت خلاصه، این امر بدان معناست که از مشارکت کامل زنان دوشادوش مردان در فرآیند تصمیم‌گیری‌ها، در دستور کار قرار گرفتن مسائل امنیتی زنان و تلقی مساوی از زنان و مردان در فرآیند لحاظ کردن پیش‌بینی‌ها و اقدامات احتیاطی لازم، اطمینان حاصل شود. در این وضعیت ضروری است که تجارب زنان و رویکرد آنها به مسائل لحاظ شود تا از این امر که زنان خود در تعریف قواعد امنیتی و دستورالعمل‌ها و همزمان نظارت و ارزیابی آنها نقش دارند اطمینان حاصل شود.

حصول اطمینان از بررسی نیازهای حفاظتی و امنیتی متناظر با مسائل جنسیتی

گذشته از سایر نیازهای امنیتی، احاله وظایف و مسوولیت‌ها برای حصول اطمینان از مد نظر قرار گرفتن خشونت‌های مبتنی بر جنسیت و یا مخاطرات امنیتی که مدافعین زن با آن روبه‌رو می‌شوند، در درون ساختار هر سازمان یا گروه مدافعی حیاتی است. اگر افراد مسوول امنیت دارای درکی مناسب از نیازهای ویژه مدافعین زن باشند، وضعیت ایده‌آلی را شاهد خواهیم بود. در برخی موارد ممکن است شخصی دیگر را به کار گفت که دانش خاص و درک لازم برای حل فصل مسائل ویژه این حوزه را دارا باشد. برای مثال ممکن است در سازمان شخصی به عنوان مسوول امنیت معرفی شده باشد، اما سازمان مدتی بعد تصمیم بگیرد تا شخصی را با دانش و مهارت‌های لازم مسوول تمرکز بر خشونت‌های مبتنی بر جنیست مدافعین کند، در برخی موارد هم هر دو ممکن است به صورت مشترک و هماهنگ با یکدیگر کار کرده و از اجرای مطمئن تمامی دستورالعمل‌های امنیتی و متناظر بودن آنها با نیازهای متفاوت افراد اطمینان حاصل کنند.

آموزش

آموزش تمامی افرادی که در کنار یکدیگر یک سازمان حقوق بشری فعالیت می‌کنند، کلید بهبود امنیت و حفاظت تلقی می‌شود. این آموزش باید شامل ارتقای سطح آگاهی نسبت به نیازهای خاص مدافعین زن نیز باشد.

خشونت‌های مرتبط با جنسیت اغلب به ندرت گزارش می‌شوند. آگاهی عمومی نسبت به خشونت‌های مرتبط با جنسیت در درون سازمان یا گروه ممکن است شرایط را برای گفت‌وگو و ابراز تهدیدات خاص جنسیتی یا رویدادهای متناظر با آن مساعدتر شود. اعضای داوطلب می‌تواند به عنوان "نقاط ورودی" جهت مراجعه مدافعین مرد و یا زنی که خواهان یافتن راه‌حل‌هایی برای تهدیدات و یا خشونت‌های متناظر با جنسیتی هستند که علیه آنان و یا دیگران در درون سازمان و یا جامعه صورت گرفته، عمل کنند.

به صورت خلاصه:

تفاوت در نیازهای امنیتی زنان متناظر با نقش های متفاوت آنان، گونه‌های متفاوت تهدید و تفاوت میان شرایط مختلف (بازداشت، فعالیت میدانی و ...) است.

هدف ایجاد واکنش‌های متناظر با جنسیت در برابر خشونت علیه زنان و سایر مدافعین است.

تجاوز جنسی و امنیت شخصی

ممانعت و پیشگیری از تجاوز جنسی می تواند مشابه فعالیت از بروز سایر حملات باشد، به‌ویژه در مواردی که این حملات را بتوان در دسته"جنایات عام" طبقه‌بندی کرد. تجاوزات جنسی ممکن است به صورت روشی برای سرکوب فعالیت مدافعین تلقی شده و در این میان قربانیان ممکن است از پیش تعیین‌شده بوده و یا به صورت تصادفی هدف حمله قرار گیرند.

هر شخصی- مرد یا زن- می‌تواند قربانی بالقوه تجاوز جنسی باشد اما زنان بخش اعظم قربانیان را تشکیل می‌دهند. تجاوز جنسی جنایتی از نوع قدرت و خشونت است و تماس جنسی تنها راهی دیگر برای اثبات و نمایش قدرت و سلطه مهاجم بر قربانی است.

به خاطر داشته باشید در اغلب موارد زنانی که به همراه یک مهاجم بالقوه به مکانی متفاوت می‌روند، مورد تجاوز قرار می گیرند (و در مواردی ضرب و شتم‌شده و حتی به‌قتل می‌رسند)، لذا زنان باید همراه با تمام عزم و اراده خود از رفتن به همراه مهاجمی بالقوه به مکانی دیگر خودداری کنند، مگر به استثنای مواردی که چنین مقاومتی به شدت جان مدافع و یا دیگران را به خطر بیاندازد.

واکنش در برابر تجاوز جنسی

گزینه‌های موجود برای واکنش نشان دادن به تجاوزات جنسی محدود بوده و اختیار کردن هر یک از آنها بستگی به قربانی دارد. بدیهی است در این میان هیچ واکنشی را نمی توان درست و یا غلط تلقی کرد. گزینه‌های موجود و فراروی قربانیان تجاوزات جنسی را می توان در میان موارد زیر جست:

۱◆ **تسلیم**

اگر قربانی از جان خود در هراس باشد، ممکن است تسلیم جنایت شود

۲◆ **مقاومت منفعلانه**

انجام عمل و یا گفتن چیزهایی ناخوشایند و نامطلوب برای از بین بردن تمایل مهاجم به تماس جنسی. می توانید به متجاوز بگویید که به‌ایدز مبتلا هستید، دچار خونریزی شده‌اید، استفراغ کنید و ... .

۳◆ **مقاومت فعال**

استفاده‌از هر نوع مقاومت فیزیکی برای رهایی از مهاجم؛ مواردی مانند حمله به‌او، لگد زدن، گاز گرفتن، ناخن کشیدن، فریاد زدن و یا فرار کردن.

در تمامی شرایط، هر آنچه را که برای زنده ماندن لازم‌است انجام دهید. به غرایزتان اطمینان کنید. هیچکس نمی تواند پیش بینی کند که در چنین شرایطی چه رفتاری را در پیش خواهد گرفت بنابر این روش واکنش شما هم هر چه که باشد، با توجه به موقعیت مفروض، برای شما بهترین حالت ممکن است.

پس از تجاوز جنسی

تمامی **سازمان‌های مدافع حقوق بشر و گروه‌های مشابه باید طرح‌های پیشگیرانه و واکنشی برای مواجه با چنین شرایطی را که در آن عضوی از آنها مورد تجاوز قرار گرفته است، آماده کرده باشند**. طرح‌های واکنشی در شکل حداقلی خود باید شامل مواردی چون ارائه مراقبت‌های پزشکی موثر و لازم- از جمله مراقبت‌های روانی- (آزمایش‌های فوری و منظم برای حصول اطمینان از عدم ابتلای

قربانی به بیماری‌های مقاربتی و قرص‌های پیشگیری بارداری) و اقدامات قانونی لازم باشند.

ایجاد تعادل میان حصول اطمینان از دسترسی بیمار به حمایت و مراقبت تخصصی متناظر با نوع تهاجم و نیز اطمینان از عملکرد حمایت‌گرایانه و مناسب سازمان، ضروری است.

مطالعه بخش پنجم در مورد ممانعت و واکنش در قبال حملات می‌تواند مفید باشد.

بیانیه حذف خشونت علیه زنان (۱۹۹۳)، خشونت علیه زنان را به صورت زیر تعریف می‌کند:

هر نوع اقدام خشن مبتنی بر جنسیت منجر به ایراد صدمه و یا رنج فیزیکی، جنسی و یا روانی زنان (یا احتمال بروز چنین لطمات و صدماتی)، تهدید به ارتکاب چنین اقداماتی و یا محروم ساختن زنان از آزادی، در زندگی خصوصی و یا در عرصه عمومی (ماده۱)

خشونت علیه زنان را برای درک بهتر می‌توان در گروه‌های زیر گنجاند (بدیهی است که خشونت علیه زنان محدود به موارد ذکر شده نمی‌شود):

الف) ◆ خشونت فیزیکی، جنسی و یا روانی که در درون خانواده روی می‌دهد، شامل مواردی چون ضرب و شتم، سوءاستفاده جنسی از فرزندان مونث خانواده می‌شود، خشونت به علت کمبود جهیزیه، رابطه زناشویی بدون رضایت زن، ختنه اعضای تناسلی زنانه و سایر اقدامات سنتی مضر برای زنان، خشونت‌های غیر مرتبط با مسائل زناشویی و خشونت‌های مرتبط با استثمار و سوء استفاده از زنان.

ب) ◆ خشونت‌های فیزیکی، جنسی و یا روانی که در درون جامعه رخ می‌دهند شامل مواردی چون تجاوز، سوء استفاده جنسی، آزار و اذیت و ارعاب جنسی در محل کار، موسسات آموزشی وسایر اماکن، قاچاق زنان و روسپی گری اجباری.

ج) ◆ خشونت‌های فیزیکی، جنسی و یا روانی که دولت در هر مکانی مرتکب آنها شده و یا نسبت به ارتکاب آنها چشم‌پوشی می‌کند. (بند ۲).

فصل یازدهم

امنیت
در مناطق درگیری مسلحانه

هدف:

کاهش ریسک ذاتی موجود در مناطق درگیری مسلحانه

مخاطره در شرایط درگیری

فعالیت در مناطق درگیری مدافعین حقوق بشر را در معرض مخاطرات خاصی قرار می‌دهد، این امر به‌ویژه در شرایط درگیری‌های مسلحانه صادق است. بسیاری از قتل‌عام‌های شهروندان در شرایط فعلی ناشی از اعمال جنگ‌طلبانه کور است، در این میان بسیاری از شهروندان هم به صورت مستقیم هدف قرار گرفته و به قتل می‌رسند. ما باید تمامی این موارد را شناسایی و بررسی کنیم. اقدامات سیاسی برای جلب توجهات به چنین اقداماتی و تلاش برای پایان دادن به آنها الزامی هستند.

گر چه شما نمی‌توانید کنترلی بر عملیات نظامی در حال حدوث داشته باشید، اما می‌توانید رفتار و عملکرد خود را با آن همسان کرده و بدین ترتیب از تاثیرپذیری خود در اثر درگیری اجتناب ورزید و یا در صورت وقوع حادثه‌ای واکنشی مناسب نشان دهید.

اگر شما در منطقه‌ای مستقر شده‌اید که در آن درگیری‌های نظامی به صورت منظم روی می‌دهد، قطعا تاکنون بسیاری از ارتباطات لازم را برای حفاظت از خود، خانواده و افرادی که با آنها فعالیت می‌کنید، برقرار کرده‌اید. برقراری این ارتباطات برای تداوم فعالیت ضروری است.

با این وجود اگر در منطقه درگیری مسلحانه فعالیت می‌کنید، اما در آن منطقه مستقر نشده‌اید، باید **مواردی را همواره در ذهن داشته باشید:**

الف ◆ چه سطحی از مخاطرات را قابل قبول می‌دانید؟ آیا برای پذیرش این سطح از مخاطرات آماده هستید؟ این امر در مورد افراد و یا سازمان‌هایی که با شما همکاری دارند نیز صادق است.

ب ◆ آیا منافع حضور شما در چنین مناطقی بر مخاطرات آن سنگینی می‌کند؟ فعالیت‌های حقوق بشر در شرایطی که سطح مخاطرات بر منافع آن فزونی یافته باشد، پایدار و قابل تداوم نیستند.

ج ◆ "آشنایی با محل" یا "اطلاعات بسیار در مورد تسلیحات" برای حفاظت از شما کافی نیست. اگر قرار باشد هدف آتش قرار گرفته و یا با نارنجک و یا توسط تک‌تیراندازها تهدید شوید، صرفا آشنایی با چنین مواردی نمی‌تواند باعث محافظت شما شود.

مخاطرات قرار گرفتن زیر آتش

انواع آتش

شما ممکن است هدف آتش تفنگ، مسلسل، نارنجک، راکت، بمب و موشک‌های زمین به زمین، هوا به زمین و یا دریا به زمین قرار گیرید. این آتش ممکن است کم و بیش هدفمند باشد، می‌تواند از سوی یک تک‌تیرانداز یا هلی‌کوپتری که دارای دید مناسب و تسلط بر شماست، شلیک شده و یا توسط خمپاره و گلوله‌های توپ شما را هدف قراردهد. سطح و شدت آتش ممکن است متفاوت باشد، در برخی موارد هدف با خاک یکسان کردن کل سطح یک منطقه است.

هر چه آتش هدفمند تر باشد، شما با مخاطرات کمتری روبه‌رو خواهید بود(البته به شرطی که هدف آتش مشخصا شما یا محل استقرارتان نباشد). در چنین شرایطی با عقب‌نشینی و دور شدن از منطقه مخاطرات هم کاهش می‌یابند. **در هر حال باید به خاطر داشته باشید هنگامی که زیر آتش قرار گرفته‌اید، تعیین اینکه آیا هدف شما هستید و یا خیر دشوار است. به همین جهت اصولا تعیین این موضوع، چنانکه در زیر نشان خواهیم داد، اولویت ندارد.**

انجام اقدامات پیشگیرانه: کاهش آسیب‌پذیری در قبال آتش

۱ ◆ دوری از مناطق خطرناک

در مناطق درگیری و یا محدوده اقدامات تروریستی مستقر نشوید. در این مناطق دفتری تاسیس نکرده و یا مدت زیادی را در نزدیکی اهداف احتمالی حملات باقی نمانید. پادگان‌های و یا تاسیسات ارتباطاتی اهداف بالقوه برای حمله هستند. همین امر در مورد مناطق استراتژیک مانند مبادی ورودی و خروجی شهر، فرودگاه‌ها و یا نقاط مسلط بر محدوده افراط (به دلیل وضعیت جغرافیایی) نیز صادق است.

۲ ◆ تلاش برای کسب حفاظت مناسب در قبال حملات

شیشه‌های خردشده‌ای که پس از انفجار به‌اطراف پرتاپ می‌شوند، یکی از عوامل اصلی جراحات و صدمات هستند. پوشاندن پنجره‌ها با تخته‌های چوبی و یا چسباندن نوارچسب می‌تواند این صدمات احتمالی را به حداقل برساند. در شرایطی که مورد حمله قرار گرفته‌اید، از پنجره‌ها فاصله گرفته و به سرعت به سوی زمین، زیر میز یا در اتاقی مرکزی که دارای دیوارهای کلفت‌است و یا حتی از آن بهتر در درون یک زیرزمین، پناه بگیرید.

کیسه‌های شن و ماسه گاه می‌توانند بسیار کارآمد باشند، البته در صورتی که سایر ساختمان‌ها هم از آن استفاده کرده باشند. در غیر این صورت استفاده از این کیسه‌ها خطر جذب توجهات غیرضروری را افزایش می‌دهد.

اگر هیچ چیزی برای حفاظت در دسترس ندارید کف زمین و یا هر فرورفتگی در سطح زمین می‌تواند حفاظتی حداقلی را برای شما فراهم کند.

یک دیوار ساده آجری و یا در خودرو نمی‌تواند شما را در برابر گلوله تفنگ و یا آتش تسلیحات سنگین‌تر حفاظت کند. خمپاره‌ها و راکت‌ها می‌توانند تا فواصل چندین کیلومتری قربانی بگیرند. بنابراین برای اینکه هدف قرار بگیرید، الزاما نباید چندان نزدیک محل درگیری باشید.

انفجار بمب‌ها و خمپاره‌ها می‌توانند به گوش‌های شما صدمه بزنند. گوش‌های خود را با دستانتان پوشانده و دهانتان را نیمه‌باز بگذارید.

مشخص کردن مقرهای فعالیت، موقعیت حضور و یا وسایل نقلیه‌تان می‌تواند مثمرثمر باشد، اما هوشیار باشید که تنها در صورتی ثمربخش است که مهاجمان برای فعالیت‌های شما اهمیت و احترام قائل باشند.

در صورتی که وضعیت چنین نیست، متمایز کردن محل استقرار و یا وسایل، شما را بدون هیچ دلیلی در معرض توجه قرار می‌دهد. اگر باز هم می‌خواهید چنین اقداماتی را انجام بدهید با نصب پرچم یا رنگ‌آمیزی و ترسیم علائمی بر روی دیوارها و سقف (در صورت خطر حمله هوایی) این امر را انجام دهید.

۳ ◆ مسافرت با وسایل نقلیه

اگر در خودرویی هستید که مستقیما زیر آتش قرار گرفته‌است، باید وضعیت را بررسی کنید، هر چند برآورد دقیق شرایط معمولا بسیار دشوار است. به صورت عام بهتر است در نظر بگیرید که وسیله نقلیه شما ممکن است "هدف" تلقی شود. در این شرایط اقدام مناسب پیاده شدن از خودرو و یافتن پناهگاهی در اسرع وقت است. وسایل نقلیه اهدافی واضح هستند. حضور در خودرو در هنگام حمله شما را در معرض آسیب‌پذیری بیشتری قرار می‌دهد. امکان صدمه دیدن شما از خرد شیشه‌های پرتاب شده و یا انفجار باک بنزین به علاوه آتش مستقیم از حمله مواردی هستند که آسیب‌پذیری شما را افزایش می‌دهند. اگر آتش از فاصله‌ای چندان نزدیک متوجه شما نشده‌است، به رانندگی ادامه دهید تا اینکه در مکانی مناسب پناهگاهی برای خود بیابید.

مین‌ها و مهمات منفجر نشده

مین‌ها و مهمات منفجر نشده تهدیداتی جدی را متوجه شهروندان حاضر در مناطق درگیری می‌کنند. این تهدیدات را می‌توان به صورت زیر تقسیم‌بندی کرد:

□ مین‌ها

- ◆ مین‌های ضدتانک در مسیر جاده‌ها و گذرگاه‌ها کاشته شده‌اند و می‌توانند حتی خودرویی عادی را نابود کنند.
- ◆ مین‌های ضدنفر کوچکتر بوده و امکان وجود آنها در هر منطقه‌ای که احتمال می‌رود محل رفت و آمد افراد باشد، وجود دارد.

مین‌های ضدنفر اغلب در دل خاک کاشته می‌شوند. فراموش نکنید افرادی که محوطه جاده‌ای را مین‌گذاری کرده‌اند، ممکن است مزارع مجاور حتی گذرگاه‌های نزدیک را هم مین‌گذاری کنند.

□ تله‌های انفجاری

- ◆ تله‌های انفجاری مواد منفجره کوچکی هستند که در درون اشیایی عادی و یا جذاب (رنگ‌آمیزی شده) جاسازی شده و به محض اینکه شخصی آنها را لمس کند، منفجر می‌شوند. این واژه برای مین‌هایی که به اشیای دیگر متصل شده‌اند و به محض حرکت و یا فعال شدن آن اشیاء، منفجر می‌شوند (از یک جسد گرفته تا خودرویی ترک شده)، نیز به کار می‌رود.

□ مهمات منفجر نشده

- ◆ این مورد شامل تمامی جنگ‌افزارهایی که شلیک شده اما منفجر نشده‌اند، می‌شود.

پیشگیری در قبال مین‌ها و مهمات منفجر نشده

تنها راه برای اجتناب از محدوده‌های مین گذاری شده، اطلاع و آگاهی از محل آنهاست. اگر شما در منطقه‌ای مستقر نشده و یا در آن زندگی نمی‌کنید، می‌توانید محل میدان‌های مین را با پرسش مداوم و پیگیرانه از ساکنان و یا کارشناسان موضوع جویا شوید. این امر در صورتی که انفجارها و یا درگیری‌هایی در منطقه صورت گرفته باشد، اهمیت بیشتری می‌یابد. بهتر است از شاهراه‌های آسفالت‌شده و جاده‌هایی که به صورت مداوم برای رفت و آمد مورد استفاده قرار می‌گیرند، استفاده کرده و مسیر حرکت در سایر وسایل نقلیه را دنبال کنید. **هرگز بدون وسیله نقلیه خود از بزرگراه خارج نشوید، حتی برای رفتن به شانه‌های خاکی جاده و یا جدول‌های کناری.** مین‌ها و یا سایر مهمات منفجر نشده می‌توانند تا سال‌ها پنهان اما آماده انفجار باقی بمانند.

مهمات منفجر نشده ممکن است در مناطق درگیری و یا تبادل آتش یافت شوند و حتی امکان مشاهده آنها وجود داشته باشد (این مهمات با توجه به اینکه با قصد اصابت و انفجار شلیک شده‌اند، معمولا قابل مشاهده بوده و پنهان نشده‌اند). **به این مهمات نزدیک نشوید، آنها را لمس نکنید، در صورت امکان محل را نشانه گذاری کرده و بلافاصله موضوع را به اطلاع دیگران برسانید.**

تله‌های انفجاری معمولا در مناطقی یافت می‌شوند که یکی از طرفین درگیر از آنها عقب‌نشینی کرده است. در چنین مناطقی عدم لمس یا حرکت دادن اشیاء و دور ماندن از ساختمان‌های متروکه الزامی است.

در صورت انفجار مین زیر و یا نزدیک شخص یا وسیله‌ای نقلیه

دو قاعده طلایی را به خاطر داشته باشید:

- جایی که یک مین وجود دارد، مین‌های دیگری هم وجود خواهند داشت.
- هرگز هیجان‌زده و عصبی رفتار نکنید، ولو اینکه برخی افراد مجروح شده باشند.

اگر می‌خواهید از منطقه انفجار دور شوید، در صورتی که جای گام‌های پیشین خود را می‌توانید مشاهده کنید، دقیقا از همان مسیر استفاده کنید. اگر با وسیله‌ای نقلیه مسافرت می‌کنید و تصور می‌کنید ممکن است مین‌های ضدتانک هم در منطقه کار گذاشته شده باشند، خودرو را ترک کرده و با تعقیب اثر لاستیک‌ها در امتداد آنها به عقب بازگردید.

اگر باید به سمت یک قربانی رفته و یا از منطقه‌ای مین گذاری شده دور شوید، تنها راه زانو زدن و یا دراز کشیدن بر روی زمین و "سیخ زدن" زمین است. برای سیخ زدن، یک سیخ (تکه چوب یا فلزی بسیار باریک) را با دقت در زاویه‌ای ۳۰ درجه‌ای به درون زمین فرو کرده و در جست‌وجوی هر حجم سخت و یا صلبی مسیر حرکت و پیرامون خود را بکاوید اگر به حجمی سخت برخوردید، به آرامی و دقت بسیار اطراف آن را پاک کنید تا بتوانید آن را مشاهده کنید.

مین‌ها گاهی توسط سیم‌های نامریی فعال می‌شوند. در صورتی که به سیمی برخورد کردید، آن را به هیچ‌وجه قطع نکنید. انجام این اعمال احتیاطی برای خروج از محدوده خطر قطعا نیازمند صرف وقتی قابل توجه است.

فصل دوازدهم

امنیت، ارتباطات و فناوری اطلاعات

مطالب این بخش با مشارکت پرایواترا تهیه شده‌اند

هدف:

شکاف‌های عظیم موجود در فناوری اطلاعات که در سرتاسر جهان، مدافعی حقوق بشر را هم از خود متاثر می‌کنند. این فصل عمدتا بر فناوری اطلاعات (رایانه‌ها و اینترنت)۴ متمرکز شده است. مدافعینی که به اینترنت و یا رایانه دسترسی ندارند ممکن است برخی از مطالب این بخش را چندان مرتبط با خود تلقی نکنند. البته بدیهی است این گروه به شدت نیازمند دسترسی به ابزار لازم و گذراندن دوره‌هایی آموزشی هستند تا بتوانند فناوری اطلاعات را در خدمت دفاع از حقوق بشر به کار گیرند.

راهنمایی در مورد مسائل امنیتی در عرصه ارتباطات و نحوه اجتناب از آنها

آگاهی قدرت است. اگاهی نسبت به اینکه مشکلات امنیتی بالقوه شما در عرصه ارتباطات، چیست و در کجا نهفته است، در حین فعالیت احساس امنیت بیشتری می‌کنید. لیست حاضر نشاندهنده راه‌های متعددی است که ممکن است افراد به صورت غیرقانونی به اطلاعات و ارتباطات شما دسترسی یافته و یا آنها را دستکاری کنند. در این لیست همچنین راه‌های پیشگیری و اجتناب از وقوع چنین رویدادهایی نیز ارائه شده‌اند.

مکالمه

دستیابی غیرقانونی دیگران به اطلاعات مستلزم انتقال این اطلاعات از طریق اینترنت نیست. به عبارت بهتر نباید تصور کنید افراد تنها در هنگام انتقال اطلاعات از طریق اینترنت است که می‌تواند به صورت غیرقانونی به آنها دسترسی یابند، هنگامی که در مورد مسائل حساس در حال گفت‌وگو هستید، سوالات زیر را در نظر بگیرید:

۱. آیا به افرادی که مخاطب گفتار شما هستند، اعتماد دارید؟

۲. آیا این افراد نیازی به اطلاعاتی که شما در حال دادن به آنها هستید، دارند؟

۳. آیا در محیطی امن قرار دارید؟ وسایل شنود و استراق سمع اغلب در مکان‌هایی تعبیه می‌شوند که افراد احساس می‌کنند در آنجا در امنیت کامل به سر می‌برند، مکان‌هایی مانند دفاتر شخصی، خیابان‌های شلوغ، اتاق خواب منازل و یا در درون خودروها.

ممکن است یافتن پاسخ پرسش سوم چندن ساده نباشد چرا که میکروفون‌ها و یا سایر ابزار شنود ممکن است انتقال هر نوع گفتاری

و یا ثبت آن در هر مکانی مخفی شده باشند. میکروفون‌های لیزری ممکن است از فواصل بسیار دور برای استراق سمع و شنیدن مکالمات درون یک ساختمان به سمت پنجره آن نشانه رفته باشند. شیشه‌های دوجداره و پرده‌های سنگین در این شرایط می‌توانند تا حدی مانع دقت عملکرد میکروفون‌های لیزری شوند. در برخی از ساختمان‌های امن، از تعبیه دوسری پنجره برای به حداقل رساندن کارکرد وسایل استراق سمع لیزری استفاده می‌شود.

چه می‌توان کرد؟

◆ همواره فرض کنید که شخصی در حال استراق سمع است

با داشتن رویکرد بازبینانه و وسواسی (البته در سطحی سالم و نه بیمارگونه) هنگامی که پای مسائل مهم و حساس در میان است، شما دقت بیشتری را اعمال خواهید کرد.

◆ تجهیزات پاکسازی وسایل استراق سمع و شنود می‌توانند مفید باشند

دسترسی به این وسایل و یا اجاره آنها- با توجه به بهای بالایشان- دشوار است. از سوی دیگر گاهی اوقات افرادی که برای شناسایی استراق سمع استخدام می‌شوند، در عمل خود مسوول اصلی آن هستند. آنها که خود در نصب و تعبیه استراق سمع اصلی در محل مورد نظر شما دست داشته‌اند، در حین عملیات پاکسازی چند "آت و آشغال" (وسایل ارزان‌قیمتی که در اصل با هدف کشف شدن، تعبیه شده‌اند) را کشف کرده و یا به صورت حیرت آوری به هیچ مورد مشکوکی برخورد نمی‌کنند. این افراد در نهایت در حالی که مکان مورد نظر همچنان تحت کنترل وسایل استراق سمع است، آنها را "پاک" اعلام می‌کنند.

◆ هر یک از نظافت‌کاران می‌توانند یک تهدید امنیتی جدی باشند

این افراد پس از پایان ساعات کار و حضور افراد در دفتر، به محل کار شما دسترسی داشته و در نهایت هم هر شب زباله‌ها را به خارج منتقل می‌کنند. تمامی این کارکنان باید به صورت کامل از لحاظ مسائل امنیتی- و عدم وابستگی به گروه‌های خاص- مورد بررسی قرار گیرند. این بررسی‌ها به صورت منظم باید تکرار شوند چرا که ممکن است این افراد پس از پیوستن به جمع شما و یا آغاز همکاری با شما، در گذر زمان برای چنین مقاصدی به کار گرفته و استخدام شده باشند.

◆ تا حد امکان اتاق‌های ملاقات را تغییر دهید

هر چه از تعداد اتاق‌ها و یا مکان‌های بیشتری برای بحث، گفت‌وگو یا تبادل اطلاعات استفاده کنید، تعداد نفرات و تجهیزات لازم برای شنود مکالمات شما هم افزایش می‌یابد.

◆ مراقب هدایایی باشید که به گونه‌ای طراحی شده‌اند که همیشه همراه شما باشند

قلم‌های گران‌قیمت یا مواردی که ممکن است به صورت دائم در دفتر شما قرار گیرند مانند سوراخ‌کن کاغذ، گیره‌های نگاه‌دارنده کاغذ و یا تصاویر بزرگ در گذشته بارها برای شنود و استراق سمع مکالمات مورد استفاده قرار گرفته‌اند.

◆ تصور کنید که بخشی از اطلاعات شما افشا شده است

همیشه باید این تصور را واقعی بپندارید. به همین جهت شاید بهتر باشد طرح‌ها و کدها را هر از چندی تغییر داده و برای مخاطبان خود تنها بخشی از اطلاعات واقعی را بازگو کنید. در برخی موارد می‌توانید از دادن اطلاعات غلط برای بررسی اینکه چه کسی از آنها استفاده کرده و یا نسبت به آنها واکنش نشان می‌دهد، استفاده کنید.

◆ مسائل حساس را در زیرزمین و یا اتاق‌های بدون پنجره مطرح کنید

این امر تاثیرگذاری و کارکرد سیستم‌های شنود لیزری را به حداقل می‌رساند. برخی ادوات شنود در هنگام بارش باران و یا تغییرات جوی ناگهانی کارآیی خود را به شدت از دست می‌دهند.

◆ **صدایی غیریکنواخت و یا موسیقی عامه پسندی پخش کنید**

پخش این صداهای مزاحم باعث اخلال در شنود می‌شود. تنها تجهیزات گران‌قیمت می‌توانند صداهای مزاحم تصادفی (غیرمنظم) را فیلتر کرده و گفت‌وگو را شنود کنند.

◆ **فضاهای باز و وسیع هم مفید هستند و هم مضر**

ملاقات در فضای پرت و دورافتاده می‌تواند مفید باشد، چرا که به سادگی متوجه می‌شوید که آیا مورد تعقیب قرار گرفته و یا تحت نظارت هستید یا خیر. اما در این فضاها فرار کردن و پنهان شدن ساده نیست. در میان جمعیت می‌توان با راحتی بیشتری خود را گم کرد اما بدیهی است که شنود و یا تعقیب شما هم به همان میزان ساده‌تر است.

تلفن‌های همراه

امکان شنود تمامی تلفن‌ها وجود دارد، مشروط به اینکه شخص استراق سمع کننده دارای ظرفیت لازم از لحاظ امکانات و دسترسی به فناوری باشد. هیچ تماس تلفنی را نمی‌توان امن تلقی کرد. تلفن‌های همراه آنالوگ در مقایسه با تلفن‌های همراه و دیجیتال از امنیت به مراتب کمتری برخوردار هستند و هر دو مورد در مقایسه به خطوط ثابت امنیت به مراتب کمتری دارند.

جاسوسی ماهواره‌ای به راحتی مکالمات و حتی موقعیت شما را فاش می‌کند. شما حتی لازم نیست سرگرم مکالمه‌ای باشید تا مکان‌تان افشا شود. فقط کافی است شما تلفن همراه خود را روشن کنید تا موقعیت شما شناسایی شود.

هرگز اطلاعات حساس همانند نام‌های خاص و یا شماره های مهم را در حافظه تلفن خود نگاهداری نکنید. اگر تلفن همراه شما به سرقت رود از این اطلاعات ممکن است برای شناسایی و اقدام علیه افرادی که شما خواهان حفاظت از آنها هستید، استفاده شود.

امنیت فیزیکی اطلاعات در دفتر

در تمام اوقات در دفتر را بسته نگاه دارید. پنجره‌ها را هم ببندید. از کلیدهایی استفاده کنید که تکثیر آنها نیازمند مجوز خاصی است. وضعیت تمامی نسخه‌های تکثیر شده را هم دنبال کنید. هرگز کلیدها را در اختیار شخص ثالث قرار ندهید ولو این شخص تعمیرکار و یا نظافتچی باشد. هنگام حضور چنین افرادی مطمئن شوید که خود شما و یا شخصی مورد اعتمادتان در دفتر حضور دارد. اگر امکان این امر وجود ندارد، اتاقی با دسترسی محدود را به نگاهداری اسناد آسیب‌پذیر و حساس اختصاص دهید. بهتر است تمامی درهای دفتر را قفل کرده و زباله‌های غیرسری (زباله‌هایی که حاوی نامه‌ها، شماره‌ها و یا اسناد سری یا مهم و باارزش، ولو پاره شده، نیستند) را شب‌ها در راهرو قرار دهید.

برای نابود کردن هر سندی از دستگاه‌های پودرکننده کاغذ استفاده کنید. خردکننده‌هایی که اسناد را به صورت نواری خرد می‌کنند عملا بی‌فایده هستند. برای نابود کردن اسناد بسیار محرمانه، آنها را پودر کرده، سپس پودر را سوزانده، خاکستر و آسیاب کرده و در نهایت آنها را به درون فاضلاب خالی کنید.

مسائل ابتدایی در امنیت رایانه و اسناد

- در صورت امکان رایانه‌ها را هنگام ترک دفتر قفل کنید. صفحه رایانه‌ها را مقابل پنجره‌های قرار ندهید.
- از محافظ افت فشار برق برای تمامی پریزهای برق استفاده کنید (تغییر جریان برق می‌تواند به رایانه شما صدمه بزند).
- از اطلاعات خود- از جمله اسناد کاغذی- پشتیبان تکیه کنید و آنها را در مکانی امن محافظت کنید. اطمینان حاصل کنید که این پشتیبان‌ها امن هستند. برای این کار می‌توانید آنها را بر روی یک دیسک سخت ظ (هارد دیسک) مجزا و قفل شده در داخل یک سازمان امنیت اطلاعات پشتیبان نگهداری کرده و یا با قفل‌های پیچیده فیزیکی از امنیت آن اطمینان حاصل کنید.
- برای کاهش خطر دسترسی افراد به رایانه شما، از رمزهای عبور عبارت مانند- و نه کلمه‌ای- استفاده کنید. همواره هنگام ترک دفتر رایانه خود راخاموش کنید.
- فایل‌های خود را قفل گذاری کنید تا حتی در صورت دسترسی شخصی به رایانه و کشف رمزهای عبور بازهم امکان دسترسی به فایل‌های شما وجود نداشته باشد.
- در صورتی که به طور منظم و روزانه از فایل‌های خود پشتیبان تهیه کرده باشید (با رعایت نکات ایمنی) حتی در صورت سرقت و یا نابودی رایانه خود هم می‌توانید فایل‌هایتان را در اختیار داشته باشید. نسخه‌ای قفل شده‌را در نقطه‌ای دور از دفتر و در مکانی امن نگاه دارید.
- فایل‌های حذف شده در صورتی که با نرم‌افزارهایی مانند pgpwipe و یا موارد مشابه پاک شده باشند، قابل بازیابی نیستند. فایل‌هایی را که می‌خواهید حذف کنید هرگز در "سطل آشغال" رایانه قرار ندهید.
- رایانه شما می‌تواند به نحوی برنامه‌ریزی شده باشد که بدون اطلاع شما فایل‌هایتان را برای دیگران ارسال کرده و یا به نحوی شما را آسیب‌پذیر نماید. برای ممانعت از این امر رایانه خود را از منبعی مطمئن خریداری کرده، دیسک سخت را به محض خرید فرمت کنید و سپس تنها نرم‌افزارهایی را که لازم دارید نصب کنید. تنها به متخصصان مورد اعتماد اجازه تعمیر رایانه خود را بدهید و در تمام مدت هم مراقب آنها باشید.
- هنگامی که از دفتر خارج می‌شود ارتباط اینترنتی رایانه خود را قطع کرده، آن را از سیم تلفن و یا مودم جدا کنید. قطع ارتباط اینترنتی باید به صورت فیزیکی صورت بگیرد. در این شرایط پس از ترک دفتر، در نیمه‌های شب، مهاجمان با برنامه‌های راه‌انداز رایانه نمی‌توانند وارد رایانه شخصی شما شوند.
- هرگز در طول روز هنگام ترک محل کار، رایانه خود را روشن نگذارید. نرم‌افزاری را نصب کنید که پس از گذشت مدت زمانی معین و عدم فعالیت رایانه، آن را خاموش کرده و یا دسترسی به آن را مستلزم ارائه رمز ورود می کند. بدین ترتیب زمانی که برای نوشیدن قهوه و یا تهیه یک برگ فتوکپی اتاق را ترک می‌کنید، رایانه شما در معرض خطر قرار ندارد.
- در تنظیمات برنامه‌های مرورگر خود گزینه‌ای را که با نمایش extension فایل به شما امکان شناسایی نوع آن را، بیش از باز کردن و یا ذخیره کردن می‌دهد، فعال کنید. قطعا شما علاقه‌ای ندارید که با بازکردن فایلی اجرایی که با ظاهری چون فایل‌های متنی برای شما ارسال شده‌است، ویروسی را بر روی رایانه خود فعال کنید. برای انجام این تنظیمات در برنامه Internet Explorer به منوی Tools رفته و گزینه folder options را انتخاب کنید. بر روی view کلیک کرده و مطمئن شوید که چارچوبه مجاور Hide Extensias For Known File Type? انتخاب نشده‌است.

معضلات امنیتی اینترنت

نامه‌های الکترونیکی شما قطعا از رایانه‌تان به رایانه مقصد(دریافت‌کننده) پرواز نمی‌کنند! این نامه‌ها از چندین گروه گذشته و در هنگام عبور اطلاعاتی را از خود به جای می‌گذارند. بدین ترتیب **هر نامه الکترونیکی در سرتاسر مسیر گذر خود (و نه الزاما در کشور شما) می‌تواند قابل دسترسی باشد.**

شخصی ممکن است در حینی که شما سرگرم تایپ نامه هستید از فراز سر شما محتویات آن را بخواند. این امر به ویژه در کافی‌نت‌ها معضلی آشناست. اگر شما به شبکه‌ای متصل هستید، نام الکترونیکی شما ممکن است برای سایر افراد اداره هم قابل دسترسی باشد. مدیر فنی سیستم‌های شما یا همان Adminstrator ممکن است با تعریف برخی مزیت‌های خاص برای خود، امکان دسترسی به تمامی نام‌های الکترونیکی شما را داشته باشد.

شرکت ارائه دهنده خدمات اینترنتی به تمامی نامه‌های الکترونیکی شما دسترسی دارد و هر شخصی که بتواند نفوذ خود بر این شرکت را اعمال کند، می‌تواند مسوولان آن را وادار به ارسال رونوشتی از نامه‌های الکترونیکی شما کند. هکرها در این میان می‌توانند به نامه‌های الکترونیکی شما در میانه راه دسترسی پیدا کنند.

تمامی این شرایط برای دریافت کنندگان نامه‌های الکترونیکی به شما هم صدق می‌کند. ممکن است شرکت خدمات‌دهنده اینترنت به آنها تحت فشار قرار گرفته باشد یا نامه‌های دریافت شده توسط وی در دسترس دیگران هم قرار گیرد. معضلات نام برده شده در این قسمت همزمان مربوط به هر دو سوی یک ارتباط اینترنتی است.

مسائل پایه امنیت در اینترنت

ویروس‌ها و سایر موارد مشکل‌آفرین مانند تروجان‌ها- اسب‌های تروا و ... می‌توانند از هر جایی شما را هدف حمله قرار دهند. دوستان شما هم گاه می‌توانند ناآگاهانه باعث گسترش ویروس‌ها شده و در نهایت شما را در معرض مخاطره قرار دهند. همواره از یک برنامه ضدویروس مناسب استفاده کرده و با استفاده از امکان به روزسازی خودکار از طریق اینترنت، برنامه خود را به روز کنید. ویروس‌های جدید به صورت مداوم خلق و کشف می‌شوند. بنابریان برای مجهز شدن به آخرین روش‌های حفاظتی در برابر آنها می‌توانید از پایگاه اینترنتی www.vil.nai.com استفاده کنید.

ویروس‌ها معمولا از طریق نامه‌های الکترونیک منتشر می‌شوند بنابراین قطعا دقت لازم را برای ارسال دریافت"امن" نامه‌های الکترونیک معمول دارید (به بخش زیر رجوع کنید). ویروس‌ها ممکن است مخرب باشند و گاه هم مخرب نیستند. تروجان‌ها (یا اسب‌های تروآ) برنامه‌هایی هستند که هدف از طراحی آنها فراهم آوردن امکان دسترسی شخص ثالث (و یا هر شخصی!) به رایانه شماست.

یک فایروال مناسب می‌تواند باعث شود شما در برابر هکرها نامریی به نظر برسید و لذا مهاجمین حتی به فکر حمله و تلاش برای ورود به رایانه شما نیفتند. فایروال در عمل تنها به برنامه‌های مجاز و تعیین‌شده‌ای امکان وصل شدن به اینترنت را داده و مانع آن می‌شود که برنامه هایی چون تروجان‌ها، اطلاعات شما را به صورت اتوماتیک برای شخص ثالثی ارسال کرده و یا "درهای پشتی" رایانه شما را به روی هکرهای منتظر ورود بگشاید.

برنامه‌های "ثبت کلید" یا به عبارت دیگر key logger می‌توانند فشردن هر کلیدی را توسط شما ثبت کنند. تکثیر و گسترش این برنامه‌ها یا معمولا توسط شخصی صورت می‌گیرد که با استفاده از غیبت شما این برنامه را بر روی رایانه‌تان نصب کرده است و یا از طریق

تروجان و یا ویروسی که از طریق اینترنت به رایانه شما حمله کرده است، به صورت خودکار و بدون آگاهی شما، نصب می‌شوند. برنامه‌های ثبت کلید، سابقه فشردن کلیدها و هر فعالیتی که بر روی دستگاه نصب شود را ثبت و نگهداری کرده و معمولا از طریق اینترنت به شخص ثالث ارسال می‌کنند. استفاده از رمزهای عبور برای حفاظت از رایانه، به کار بستن اصول ارسال و دریافت امن نامه‌های الکترونیک، استفاده از ضدویروس و یا به کارگیری برنامه‌هایی که به شما این امکان را می‌دهند با استفاده از ماوس کلمات رمز و عبارات مهم را تایپ کنید (صفحه کلیدهای مجازی) می‌تواند مانع فعالیت این برنامه‌ها شده و یا کارآیی آنها را به حداقل برساند. برنامه‌های ثبت کلید همچنین با قطع فیزیکی ارتباط رایانه با اینترنت غیرفعال می‌شوند. برای این کار کافی است هنگامی که با رایانه کاری ندارید، سیم تلفن را از مودم نصب‌شده در داخل دستگاه قطع کرده و یا مودم خارجی را قطع کنید.

نشانی صندوق اینترنتی ممکن است "جعل" شده و یا توسط شخصی غیر از صاحب واقعی آن استفاده شود. این امر با دسترسی به رایانه و رمز ورود شخص دیگر و یا هک کردن ارائه‌دهنده خدمات ارتباط اینترنتی و یا استفاده از آدرسی که بسیار شبیه آدرس معین شخص مورد نظر است، امکان‌پذیر است. برای مثال با عوض کردن حرف l (**ال** کوچک) با رقم " ۱ " شما می‌توانید آدرسی مشابه آدرس اصلی ایجاد کنید و اغلب افراد هم متوجه این تغییر نخواهند شد. برای اجتناب از فریب خوردن توسط آدرس‌های جعلی، از موضوعات با معنی استفاده کنید. به عبارت دیگر در بخش مربوط به موضوع عبارتی با معنی و مرتبط را بنویسید. به صورت متناوب پرسش‌هایی را مطرح کنید که تنها اشخاص واقعی (اشخاص مورد نظر شما) بتوانند پاسخ دهند. برای هر نوع درخواست برای کسب اطلاع را به روشی دیگر تایید بگویید. (به عبارت دیگر با استفاده از سایر روش‌های ارتباطی، مانند تلفن، موضوع را با شخص مورد نظر مطرح کنید).

از آشکار شدن فعالیت‌های خود در فضای اینترنت با عدم قبول کوکی ها و حذف فایل‌های ذخیره‌شده پس از هر بار اتصال به اینترنت، جلوگیری کنید. در صورتی که از مرورگر اینترنت اکسپلورر استفاده می‌کنید، به منوی سمخخف رفته و زیرمجموعه سدخهفخ را انتخاب کنید.

در صورتی که مرورگر نت‌اسکیپ را به کار می‌گیرید به منوی Edit رفته و Preferences را انتخاب کنید. هنگامی که در هر یک از این منوهای فرعی قرار گرفتید، تاریخچه فعالیت خود یا همان History را پاک کرده و تمام کوکی‌هایی را که ممکن است دریافت کرده باشید و نیز نسخه ذخیره‌شده صفحات مرور شده توسط خود را بر روی رایانه (Cache) حذف کنید. به خاطر داشته باشید که یادآوری‌ها یا همان Book mark را هم حذف کنید. برنامه‌های مرورگر معمولا سابقه‌ای از سایت‌هایی را که به آن مراجعه کرده‌اید در فایل‌های (Cache) ذخیره می‌کنند. بنابراین با جست‌وجوی ساده فایل‌هایی را که باید حذف کنید بیابید.

مرورگرهای خود را به روزرسانی کنید تا امکان استفاده از کدگذاری‌های ۱۲۸ بیتی را داشته باشید. این ویژگی باعث می‌شود تا حداکثر مراقبت و حفاظت ممکن نسبت به اطلاعاتی که شما می خواهید به صورت امن از طریق اینترنت منتقل کنید، از جمله کلمات عبور و یا سایر اطلاعات حساسی که هنگام پر کردن نرم‌ها در آنها درج می‌کنید، حاصل شود . .

آخرین دنبالک های امنیتی (patches) را برای برنامه‌های خود، به‌ویژه مایکروسافت آفیس، مایکروسافت اینترنت اکسپلورر و نت‌اسکیپ نصب کنید.

اصول پایه برای ارسال و دریافت امن نامه‌های الکترونیک

اصول زیر می‌تواند باعث ایمن‌سازی ارتباطات الکترونیک شما شده و یا میزان مخاطراتی را که با آن روبه‌رو هستید، به حداقل برسانند. این اصول باید علاوه بر شما، توسط تمامی دوستان و افراد مرتبط با شما هم رعایت شوند. برای این منظور به آنها صراحتا بگویید در صورت

عدم رعایت این اصول، نامه‌های ارسالی‌شان را باز نخواهید کرد.

۱ ◆ **هرگز** نامه‌ای را که از سوی شخصی ناشناس برایتان ارسال شده است باز نکنید

۲ ◆ **هرگز** نامه‌ای را که از شخصی ناشناس برایتان ارسال شده و یا منبع اصلی آن (شخص ایجادکننده) برایتان ناشناخته است، برای دیگران ارسال نکنید. تمامی نامه‌هایی که افراد برای یکدیگر (معمولا به صورت دسته‌جمعی، به تمامی آدرس‌های موجود در دفترچه نشانی‌شان) با مضامینی چون "فکرهای خوب" یا "الهام‌بخش" و ... می‌توانند حاوی ویروس باشند. با ارسال چنین نامه‌هایی به دوستان و یا افراد مرتبط با خود، ممکن است رایانه آنها را آلوده به ویروس کنید. در مواردی که واقعا به متن احساسی درون این نامه ها علاقه پیدا کرده و می‌خواهید احساس خود را با کسی دیگر شریک شوید، پیام یا متن مورد نظر را شخصا بار دیگر تایپ کرده و آن را به صورت نامه‌ای جداگانه برای دریافت‌کننده مورد نظرتان ارسال کنید. از ارسال متن اولیه به نشانی دوستانتان بپرهیزید. اگر احساس می کنید متنی ارزش زمانی را که باید صرف تایپ آن کنید را ندارد، به احتمال قریب به یقین آن متن یا پیام ارزش چندانی برای ارسال هم ندارد!

۳ ◆ **هرگز** فایل ضمیمه نامه را باز و یا دانلود نکنید مگر اینکه از محتویات و امنیت آن مطمئن باشید. گزینه دانلود اتوماتیک را در برنامه دریافت و ارسال نامه‌های الکترونیک خود غیرفعال کنید. بسیاری از ویروس‌ها و تروجان‌ها به صورت "کرم" خود را تکثیر می کنند. کرم‌های پیشرفته غالبا به نظر می‌رسد که از سوی دوست و یا آشنایی برای شما ارسال شده‌اند. کرم‌های هوشمند به درون دفترچه نشانی‌ها شما خزیده و به‌ویژه در مواردی که از نرم‌افزارهایی چون مایکروسافت اوت‌لوک‌و یا اوت‌لوک اکسپرس استفاده می کنید، نامه الکترونیک ایجاد کرده و خود به ایمیل‌های ایجاد شده به صورت فایلی ضمیمه چسبانده و به نشانی‌های موجود ارسال می‌شوند. دریافت‌کننده در این شرایط نام آلوده را نامه‌ای از سوی شخصی آشنا تصور می کند.

استفاده از نرم‌افزارهایی چون PGP برای کدگذاری کردن نامه‌های الکترونیک- چه دارای فایل‌های ضمیمه باشند و چه خیر- تا حد بسیار زیادی امکان شناسایی نامه‌های عاری از ویروس را فراهم می‌آورند. همکاران شما در این شرایط می‌توانند نامه‌های کاذب و آلوده را از نامه‌های سالم تشخیص داده و فایل ضمیمه را با خیال راحت دانلود کنند. (لطفا به بخش کدگذاری مراجعه کنید).

۴ ◆ از فرمت‌های Rich Text, HTML,MIM در نامه‌های خود استفاده نکنید. متن ساده و یا همان Plain Text بهترین انتخاب است. نامه‌های دارای فرمت‌های دیگر ممکن است محتوی برنامه‌های مخفی شده و پنهانی باشند که فایل‌های موجود در رایانه شما را تخریب کرده و یا امکان دسترسی به آن را برای دیگران فراهم آورند.

۵ ◆ در صورتی که از برنامه‌های اوت‌لوک یا اوت‌لوک اکسپرس استفاده می کنید، گزینه صفحه پیش‌نمایش را غیرفعال کنید.

۶ ◆ تا حد امکان نامه‌های خود را کدگذاری کنید. یک نامه کدگذاری نشده همانند کارت‌پستالی است که همه امکان خواندن محتوای آن را داشته یا به محتوای آن دسترسی دارند. نامه های الکترونیکی کدگذاری شده اما همانند نامه‌ای هستند در درون یک پاکت که در داخل گاوصندوق قرار داده شده است.

۷ ◆ موضوع نامه‌های خود را مرتبط با آن انتخاب کنید تا دریافت‌کننده بداند شما از ارسال آن هدفی را دنبال می کنید یا به عبارت دیگر تفاوت آن با نامه‌های کاذب مشخص شود. از دوستان و همکاران خود بخواهید که در موضوع نامه، مطلبی شخصی را بازگو کنند تا مطمئن شوید که نامه از سوی آنان ارسال شده است. این امر می تواند باعث شناسایی نامه‌های واقعی از نامه‌های جعل شده و یا نامه‌هایی که تروجان‌ها برای گسترش دامنه آلودگی خود به صورت انبوه و گروهی برای تمامی افراد حاضر در دفتر چه‌های نشانی فرستاده‌اند، بشود. اگر

قرار است در بخش موضوع اطلاعات شخصی را بنویسید، به خاطر داشته باشید که از درج اطلاعات امنیتی و حایز اهمیت در آن باید خودداری شود. بخش موضوع، کدگذاری نشده و ممکن است باعث آشکار شدن ماهیت و محتوی نامه شده و بدین ترتیب میزان احتمال حمله را افزایش دهد. بسیاری از برنامه‌ها "محرمانه"، "خصوصی" و یا هر کلمه دیگری که نشانگر جذابیت و یا مهم بودن پیام درون نامه باشد را تعقیب و از آن نسخه برداری می کند.

۸◆ هرگز هنگام ارسال نامه برای گروهی کثیر، نام آنها را در بخش‌های To یا CC قرار ندهید. در عوض نام خود را به عنوان گیرنده در بخش To درج کرده و آدرس سایر افراد را در بخش Bcc درج کنید. این امر علاوه بر اینکه روشی مناسب و مطمئن محسوب می‌شود، نشانگر احترام شما برای سایرین است. چرا که در غیر این صورت نشانی هر یک از آنها را برای انبوهی از افراد که برایشان ناآشنا هستند، ارسال می کنید. قرار دادن آدرس شخصی افراد در دسترس دیگران عملا ناخوشایند، رنجش آفرین و حتی خطرناک است.

۹◆ هرگز به نامه‌های ناخواسته پاسخ ندهید ولو برای اینکه بخواهید از آنها درخواست کنید که شما را از لیست دریافت کنندگان تبلیغات یا خدمات خود حذف کنند. ارسال کنندگان این نامه‌ها از سرورهایی استفاده می کنند که به انبوهی از آدرس‌های تصادفی نامه ارسال می کنند. آنها هرگز نمی توانند مطمئن باشند که آیا آدرسی که به آن نامه‌ای ارسال شده است، عملا وجود داشته و فعال است یا خیر. پاسخ به این نامه‌ها باعث می‌شود سرور آنها نشانی شما را به عنوان "نشانی فعال" شناسایی کرده و به احتمال قریب به یقین شما در فاصله‌ای کوتاه با انبوهی از نامه‌های مشابه مواجه خواهید شد.

۱۰◆ در صورت امکان برای دریافت نامه‌های الکترونیک عمومی از رایانه‌ای جداگانه استفاده کنید که به سایر رایانه‌ها وصل نبوده و دارای هیچ فایل اطلاعاتی نباشد.

کدگذاری؛ پرسش‌ها و پاسخ‌ها

در این بخش مجموعه‌ای از پرسش‌ها و پاسخ‌های مرتبط با کدگذاری را مشاهده می کنید. در صورتی که نیاز به اطلاعات بیشتری داشتید برای طرح پرسش خود درنگ نکرده و با سازمان غیردولتی privaterra در نشانی www.privaterra.org آن را در میان بگذارید.

پرسش: کدگذاری چیست؟

پاسخ: کدگذاری به معنای به هم ریختن داده‌ها و چینش آنها به صورت کدی رمزی است که توسط شخصی جز طرف مورد نظر قابل رمزگشایی نیست. بدیهی است که تمامی پیام‌های کدگذاری شده با صرف وقت و برخورداری از قدرت محاسباتی مناسب قابل بازیابی هستند، اما به هر حال طبیعی است که این امر نیازمند صرف زمان و هزینه بالایی است. کدگذاری به عبارت ساده‌تر روشی است برای امن‌سازی و پنهان کردن فایل‌ها و نامه‌های الکترونیک شما از دید جاسوسان. در این فرآیند قایل‌های شما تبدیل به کد می‌شوند، کدهایی که ترکیبی تصادفی از ارقام و حروف بوده و برای سایر افرادی که آن را مشاهده می کنند هیچ معنا و مفهومی در بر ندارند. برای کدگذاری یک فایل، در حقیقت شما آن را با کلیدی قفل می کنید، این کلید در حقیقت همان رمز عبور است. هنگام کدگذاری یک پیام، شما پیام مزبور را با استفاده از یک جفت کلید قفل می کنید. یکی از این کلیدها - یا در واقع رمزهای عبور - در اختیار دریافت کننده پیام است. پیام بدین ترتیب تنها توسط دریافت کننده مورد نظر و با به کارگیری کلید مخصوص (رمز عبور) قابل بازگشایی است.

پرسش: چرا باید گروه‌های حقوق بشری از کدگذاری استفاده کنند؟

پاسخ: همه باید از کدگذاری استفاده کنند چرا که ارتباطات دیجیتال ذاتا ناامن هستند. با این وجود، فعالان حقوق بشر اغلب بیشتر از اکثر افراد در معرض مخاطرات مختلف قرار می‌گیرند و طبیعی است که اسناد و ارتباطات آنها هم از حساسیت بیشتری برخوردار باشد. استفاده از کدگذاری توسط مدافعین حقوق بشر برای حفاظت از خود و افرادی که تلاش خود را صرف کمک به آنها کرده‌اند، ضروری است.

فناوری دیجیتال برای مدافعین حقوق بشر مزیت محسوب می‌شود چرا که به آنها اجازه می‌دهد از ارتباطاتی سهل‌تر با تاثیر بیشتر و فرصت‌های افزون‌تر برخوردار شوند. با این وجود طبیعی است که هر مزیتی، خطرات خاص خود را هم به همراه دارد. بدیهی است بستن کمربند ایمنی بدان معنا نیست که شما هر بار که رانندگی می‌کنید، قرار است تصادف کنید. رانندگی در شرایط خطرناک، برای مثال در مسابقه، در این میان حتی باید شما را بیش از پیش به استفاده از کمربند ایمنی، جهت حفظ امنیت خود، ترغیب کند.

مدافعین حقوق بشر اهداف شناخته شده فعالیت‌های جاسوسی هستند. از آنجا که نامه های الکترونیکی کد نشده به راحتی توسط اغلب افراد قابل دسترسی و خواندن هستند، قاعدتا باید باور داشته باشید که پیام‌های کد نشده شما به هر حال در مکانی کشف و مورد بررسی قرار می‌گیرند. ممکن است رقبای شما از مدت‌ها پیش کلیه پیام‌هایتان را تحت نظر گرفته‌اند و شما همچنان از آن بی‌خبر هستید. به خاطر داشته باشید مخالفان افرادی که شما فعالیت‌های خود را صرف کمک به آنها کرده‌اید را هم باید مخالفان خود محسوب کنید.

پرسش: آیا استفاده از کدگذاری غیرقانونی است؟

پاسخ: گاهی اوقات. در اغلب کشورهای جهان اما استفاده از کدگذاری کاملا قانونی است. با این وجود استثنائاتی هم وجود دارند. برای مثال در چین سازمان‌هایی که می‌خواهند از کدگذاری استفاده کنند باید درخواست صدور مجوز کتبی کنند. همچنین اگر بر روی رایانه قابل حمل شما نرم‌افزار کدگذاری نصب شده و یا برنامه آن وجود داشته باشد، باید هنگام ورود به کشور آن را اعلام کنید. سنگاپور و مالزی اما قانون‌هایی را به تصویب رسانده‌اند که به موجب آن افرادی که خواهان استفاده از کدگذاری هستند باید رمزهای شخصی خود را گزارش کنند – در واقع کلید رمز را در اختیار مقامات مسوول قرار دهند –. در هندوستان نیز قوانین کم و بیش مشابهی وجود دارد. استثنائات دیگری نیز می‌توان در این میان یافت.

مرکز اطلاعات حریم الکترونیک بررسی جامع و فراگیری در مورد سیاست‌ها در قبال کدگذاری در سرتاسر جهان انجام داده است. در این تحقیق قوانین اغلب کشورها مورد بررسی قرار گرفته‌اند. این تحقیق جامع الاطراف را می‌توانید در نشانی اینترنتی:
http://www2.epic.org/reports/crypto2000 یافته و مطالعه کنید. این لیست آخرین بار در سال ۲۰۰۰ میلادی به روزرسانی شده است. در صورتی که همچنان نگران غیرقانونی بودن استفاده از کدگذاری در کشوری خاص هستید با پرایواترا تماس گرفته و موضوع را جویا شوید.

پرسش: برای امن نگاه داشتن سیستم‌های ای‌تی خود به چه احتیاج داریم؟

پاسخ: این موضوع بستگی به سیستم‌های موجود فعالیت‌های شما دارد، اما به صورت عام هر شخصی باید دارای موارد زیر باشد:

- یک فایروال
- کدگذار دیسک
- کدگذار نامه‌های الکترونیکی که امکان امضای دیجیتال را نیز فراهم می‌سازند
- نرم‌افزار شناسایی
- پشتیبان گیری مطمئن: ارسال تمامی مواد موجود از طریق نامه الکترونیک به سایتی امن و گرفتن نسخه‌های پشتیبان هفتگی برروی لوح‌های فشرده و نگاهداری آنها در مکانی مجزا و امن.

- کلمات عبوری که هرچند به یاد آوردن آنها باید ساده باشد اما امکان حدس زدن آنها توسط دیگران نباید وجود داشته باشد.
- تعریف سلسله مراتب دسترسی: بدیهی است تمامی افراد یک سازمان نیازی به دسترسی به تمامی فایل‌ها ندارند.
- مداومت: هیچ‌یک از این ابزارها و روش‌ها در صورتی که شما به صورت مداوم و دائمی آنها را به کار نگیرید، ثمربخش نخواهند بود.

به خاطر داشته باشید در اختیار داشتن نرم‌افزار مناسب و دوست، تمام راه‌حل نیست. معمولا این افراد هستند که حلقه ضعیف زنجیره محسوب می‌شوند نه فناوری. بدیهی است در صورتی که افراد به صورت مداوم از روش های کدگذاری استفاده نکنند و یا رمزهای عبور خود را در اختیار همگان قرار داده و یا حتی آن را بر روی کاغذ یادداشت و یا برچسبی نوشته و به مونیتور خود الصاق کنند، کدگذاری عملا بی‌نتیجه خواهد بود. نسخه‌های پشتیبان اگر در محلی مجزا و امن نگاهداری نشوند، در وصرت وقوع آتش‌سوزی و یا حمله مهاجمان ممکن است نابود شوند. در این صورت تلاش‌های شما برای تهیه نسخه‌های پشتیبان هیچ حاصلی نداشته و در عمل بودن و یا نبودن آنها به حال شما تاثیری نخواهد داشت. اطلاعات حساس باید تنها در اختیار افرادی که نیاز به دانستن آنها دارند قرار گیرند، نه اینکه به اطلاع تمامی اعضای سازمان برسد. ایجاد و تعیین سلسله مراتب و یا پروتکل‌ها باعث خواهد شد تا هر کس به‌اندازه نیاز خود، اطلاعات در اختیار داشته باشد، به طور کلی باید فقط حریم خصوصی و امنیت را در تمامی فعالیت‌های روزانه‌تان دخیل کنید. این طرز فکر و تلقی به"بدبینی سالم" مرسوم است.

پرسش: چگونه نرم‌افزار کدگذاری مناسب را انتخاب کنیم؟

پاسخ: معمولا می‌توانید از دوستانتان نظر خواسته و در نهایت تایید ما را بگیرید. شما قطعا باید با افراد و یا گروه‌هایی خاص ارتباط داشته باشید، بنابریان اگر آنها از سیستم کدگذاری خاصی استفاده می‌کنند، شما هم بهتر است برای تسهیل ارتباطات از همان سیستم استفاده کنید. به هر حال باز هم فراموش نکنید که قبل از انتخاب سیستم کدگذاری با ما مشورت کنید چرا که برخی بسته‌های نرم‌افزاری عملا کارکرد مناسبی ندارند و دیگران هم مانند "کوزه‌های عسل" هستند. "کوزه‌های عسل" نرم‌افزارهایی رایگان با ظاهر و کارکردی عالی هستند که تنها یک نقص دارند؛ این نرم‌افزار ها توسط همان افرادی تهیه و به شما عرضه می‌شوند که خواهان جاسوسی و کنترل ارتباطات شما هستند! واقعا راهی بهتر از اینکه برای کسب اطلاعات شخصی و سازمانی در قالب ارائه‌دهنده نرم‌افزار کدگذار فرو رفته و در نهایت با خیال راحت بر تمامی ارتباطات نظارت، اشراف داشته باشید، سراغ دارید؟ علیرغم این موضوع اما در نظر داشته باشید که هنوز هم انواع گوناگونی از نرم‌افزارهای رایگان با مارک‌های معتبر وجود دارند که از کارآیی مناسبی هم برخوردار هستند. فقط به خاطر داشته باشید که قبل از استفاده از هر یک از آنها با ما مشورت کنید.

پرسش: آیا استفاده از کدگذاری احتمال برخورد با من را افزایش نمی‌دهد؟

پاسخ: هیچ‌کس متوجه نمی‌شود که شما از روش کدگذاری استفاده می‌کنید مگر اینکه از مدتی پیش کلیه مبادلات الکترونیکی شما را تحت نظر گرفته باشد. اگر این امر صحت داشته باشد، طبیعی است که باید فرض کنید اطلاعات خصوصی شما از مدت‌ها پیش در اختیار دیگران قرار گرفته و خوانده شده‌است. به عبارت دیگر برخورد با شما از مدت‌ها پیش توسط افرادی که شما را تحت نظر گرفته‌اند، آغاز شده است. در این جا شاید باید نگران این موضوع بود که افرادی که در حال مراقبت و جاسوسی هستند در صورتی که نتوانند دیگر نامه‌های الکترونیک شما را بخوانند، ممکن است به گزینه‌های دیگر روی آورند. در این شرایط، هنگامی که قصد دارید از سیستم کدگذاری استفاده کنید باید نسبت به شناسایی همکارانتان مطمئن بوده، سیاست‌های پشتیبان گیری امن و مطمئنی را اجرا کرده و مدیریت منطقی و یکنواخت دفتر را در دستور کار خود قرار دهید.

نکته: هیچ اطلاعاتی در مورد مواردی که استفاده از کدگذاری و نرم‌افزارهای مربوطه باعث بروز مشکلاتی برای مدافعین حقوق بشر شده باشد، در دست نیست. با این وجود باز هم باید پیش از آغاز به کارگیری سیستم کدگذاری احتمالات این گونه را جدی گرفت. این امر

به‌ویژه هنگامی شما در کشوری با درگیری‌های مسلحانه به سر می‌برید بیشتر صدق می‌کند، چرا که ممکن است بخش‌های امنیتی و یا اطلاعاتی نیروهای نظامی در مورد احتمال انتقال اطلاعات مهم- از لحاظ نظامی- به شما مشکوک شوند.

پرسش: چرا باید نامه‌های الکترونیک و اسناد را همواره کدگذاری کرد؟

پاسخ: طبیعی است اگر قرار باشد تنها در موارد بسیار حساس کدگذاری را مورد استفاده قرار داد، افرادی که سرگرم مراقبت و نظارت بر رفتار شما هستند و یا حتی موکلین شما می‌توانند وقوع فعالیت‌های مهم را حدس زنند. در چنین شرایطی امکان شناسایی شرایط و اقدامات حساس افزایش یافته و به تبع آن امکان اعمال فشار بر شما نیز فزونی می‌یابد. مراقبان هر چند شاید قادر به خواندن مواد و مطالب کدگذاری شده نباشند، اما می‌توانند تشخیص دهند که آیا فایلی کدگذاری شده است یا خیر. افزایش ناگهانی در حجم و تعداد مطالب کدگذاری شده ممکن است باعث واکنش آنها- به صورت حمله و یورشی ناگهانی شود. بدین ترتیب شاید بهتر باشد تا استفاده از سیستم کدگذاری مدتی پیش از شروع پروژه‌های مهم آغاز شود تا از جلب توجه غیرضروری به این پروژه‌ها اجتناب شود. در عمل باید تلاش کرد تا انتقال اطلاعات به صورت جریانی آرام و ملایم (بدون فراز و نشیب) صورت گیرد. ارسال نامه‌های الکترونیکی کدگذاری شده در فواصل زمانی معین- حتی اگر هیچ چیز جدیدی برای گزارش وجود نداشته باشد، می‌تواند به شکل‌گیری جریان آرام اطلاعات کمک کند. در این شرایط هنگامی که نیازمند ارسال اطلاعات حساس از طریق نامه الکترونیکی کدگذاری شده هستید، توجه کمتری به آن جلب خواهد شد.

پرسش: من فایروال دارم، پس چرا باید نامه‌های الکترونیکی را کدگذاری کنم؟

پاسخ: فایروال‌ها مانع دستیابی هکرها به دیسک سخت و یا شبکه شما می‌شوند اما هنگامی که نامه‌های الکترونیکی را در فضای اینترنت ارسال می‌کنید، این نامه می‌تواند در معرض دسترسی همگان قرار بگیرد. بنابراین بدیهی است که پیش از ارسال نامه باید تمامی تدابیر امنیتی ممکن را به کار بگیرید.

پرسش: هیچ کس نمی‌خواهد به دفتر من نفوذ کند، چرا باید از نرم‌افزارهای حافظ حریم خصوصی استفاده کنم؟

پاسخ: شما قطعا در مورد نفوذ و یا تلاش شخصی برای نفوذ به سیستم‌های شما و یا به سرقت بردن اطلاعات نمی‌توانید چنین مطمئن باشید. بدون ارتباطات کدگذاری شده، پروتکل‌های حریم خصوصی و یا امنیت فیزیکی، هر کسی می‌تواند به فایل‌های شما دسترسی پیدا کرده، نامه‌های الکترونیک شما را خوانده و اسناد شما را بدون اطلاعتان دست‌کاری و تحریف کند. آشکار شدن ارتباطات شما ممکن است در مواردی دیگران را هم به مخاطره بیاندازد. این امر به‌ویژه در مناطقی که حملات متاثر از انگیزه‌های سیاسی رایج هستند، بیش‌تر صادق است. بگذارید ساده‌تر دلیل لزوم استفاده از نرم‌افزارهای حافظ حریم خصوصی و یا کدگذاری را شرح دهیم. اگر شما پس از خروج از دفتر، درها را قفل می‌کنید پس بدیهی است که باید فایل‌هایتان را هم کدگذاری کنید، به همین سادگی!

پرسش: ما دسترسی به ارتباطات اینترنتی نداشته و مجبور به استفاده از کافی‌نت هستیم. چگونه می‌توانیم در شرایطی که از رایانه‌های خارجی استفاده می‌کنیم، ارتباطات خود را به صورت امن انجام دهیم؟

پاسخ: شما حتی در این شرایط هم می‌توانید نامه‌های الکترونیک و فایل‌های خود را کدگذاری کنید. پیش از رفتن به کافی‌نت می‌توانید فایل‌های خود را کد کنید و سپس آنها را به همان صورت کد شده، بر روی فلاپی دیسک یا لوح فشرده کپی کنید. در کافی‌نت هم می‌توانید از ارائه‌دهنده خدمات کدگذاری و یا یک ارائه‌دهنده خدمات مرور ناشناس اینترنت مانند استفاده کنید و نامه های الکترونیک خود را ارسال کنید. فقط به خاطر داشته باشید افرادی که دریافت کننده نامه‌های شما هستند هم برای دریافت خدمات مزبور (در سایت‌هایی که شما مورد استفاده قرار داده‌اید) ثبت‌نام کرده و از خدمات آنها استفاده کنند.

پرسش: اگر حفظ امنیت فایل‌ها و ارتباطات تا این حد حایز اهمیت است، پس چرا همه نباید نسبت به آن اقدام کنند؟

پاسخ: هر چند این فناوری نسبتا جدید است اما گسترش آن به نحو قابل توجهی سریع و شتابان صورت می گیرد. اکنون بانک‌ها، شرکت‌های چندملیتی، خبرگزاری‌ها و دولت‌ها همگی از کدگذاری استفاده می کنند. هزینه های مترتب بر کدگذاری هم در واقع نوعی سرمایه‌گذاری ضروری و هزینه‌ای است که برای تجارت باید پرداخت. سازمان‌های غیردولتی در این میان به مراتب بیشتر از شرکت‌ها در معرض خطر قرار دارند. شرکت‌ها معمولا مورد حمایت دولت‌ها هستند در حالی که سازمان‌های غیردولتی عملا اهداف معمول جاسوسی و کسب اطلاعات قلمداد می‌شوند. بدین ترتیب بدیهی است که سازمان‌های غیردولتی باید نسبت به کار گرفتن این فناور مشتاق باشند. مدافعین حقوق بشر هم اغلب با مواردی چون حفاظت و مراقبت از گروه‌ها و افراد مورد شکنجه و آزار و اذیت روبه‌رو هستند. آنها برای حسن اجرای وظایف خود باید فایل هایی را نگاهداری کنند که هر یک از آنها متناظر با مشخصات و موقعیت گروه و یا فرد آزاردیده هستند. اگر این فایل‌ها در دسترس برخی قرار گیرد، ممکن است افرادی که اطلاعات آنها در این فایل‌ها موجود است شناسایی شده و پس از آن مورد شکنجه قرار گرفته، ربوده شده و حتی به قتل برسند. در خوشبینانه‌ترین حالات این افراد چنان تحت فشار قرار می گیرند که در نهایت "متقاعد" می‌شوند با سازمان های غیردولتی هیچ همکاری نداشته باشند. اطلاعات موجود در این فایل‌ها می تواند به عنوان شواهد و یا مدارکی علیه سازمان‌های غیردولتی و یا موکلان آنها در محاکمات سیاسی مورد استفاده قرار می گیرند.

پرسش: یکی از اصول کار ما، شفافیت است. ما خواهان شفافیت بیشتر دولت بوده و برای آن تلاش می کنیم. چگونه ممکن است در این شرایط خود از فناوری‌های حفظ حریم خصوصی استفاده کنیم؟

پاسخ: حفظ حریم شخصی در همان راستای شفافیت قرار دارد. اگر دولت تمایل دارد به صورت آشکار از شما بخواهد که فایل هایتان را در اختیارش بگذارید، می تواند این کار را از روش‌های مناسب و شناخته شده انجام دهد. فناوری‌های مرتبط با حفظ حریم شخصی عملا مانع آن می‌شود که برخی افراد به صورت مخفیانه و غیرآشکار به اطلاعات شما دست یابند.

پرسش: ما تمامی پروتکل‌های امنیتی و خصوصی را رعایت می کنیم، اما اطلاعات ما باز هم به بیرون درز پیدا می کند. چگونه این امر ممکن است؟

پاسخ: ممکن است در داخل سازمان شما جاسوسی وجود داشته باشد و یا شخصی که ناآگاهانه از آنجا که نمی تواند اطلاعات شما را محرمانه نگاه‌دارد، باعث افشای آنها می شود. در این شرایط باید سلسله مراتب اطلاعاتی را بازنگری و بازسازی کرده و سعی کنید تا کمترین تعداد ممکن از افراد به اطلاعات حساس دسترسی داشته باشند. این چند تن معدود را آن گاه تحت مراقبت جدی قرار دهید. شرکت‌های بزرگ و سازمان‌های عظیم معمولا به صورت متناوب، اندکی اطلاعات نادرست را در اختیار برخی افراد – افرادی که نسبت به نقش آنها در انتقال اطلاعات به خارج از مجموعه ظن وجود دارد – قرار می‌دهند و به انتظار می نشینند، اگر این اطلاعات نادرست به بیرون نشت کند، به راحتی می توان رد و مسیر انتشار این اطلاعات را تعقیب کرده و به کارمندی رسید که در ابتدا این اطلاعات غلط عامدانه در اختیار وی گذاشته شده بود.

بایدها و نبایدهای استفاده از کدگذاری

- باید کدگذاری به طور مداوم صورت گیرد. اگر تنها مطالب حساس را کدگذاری کنید هر کس که ناظر انتقال و جریان نامه‌های الکترونیکی شما باشد، قطعا به این باور خواهد رسید که حادثه‌ای مهم در شرف روی دادن است. افزایش "ناگهانی" از کدگذاری حتی ممکن است به وقوع حمله‌ای "ناگهانی" منجر شود.

- نباید اطلاعات حساس را در بخش موضوع نوشته و ذکر کرد. مطالب این بخش حتی اگر کل نامه کدگذاری شده باشد، به همان

صورت عادی و کدگذاری نشده باقی می‌مانند.

◆ باید از عبارتی برای رمز ورود استفاده نکنید که شامل حروف، ارقام، فضا، علائم مجازی و ... باشد و تنها شخص شما امکان یادآوری آن را داشته باشید. برخی ار روش‌های ایجاد رمزهای ورودی امن استفاده از الگوهای قرارگیری کلیدها بر روی صفحه‌کلید و یا کلماتی تصادفی با ترکیبی از نمادها در میان حروف هستند. به طور کلی هر چه رمز ورود طولانی‌تر باشد، امنیت آن هم بیشتر خواهد بود.

◆نباید از یک کلمه‌واحد و منفرد مانند نام، عبارات متداول و یا آدرسی موجود در دفترچه نشانی‌ها به‌عنوان رمز ورود استفاده کنید. چنین رمزهایی ظرف چند دقیقه شناسایی می‌شوند.

◆ باید از "کلید خصوصی" (فایلی که حاوی کلید خصوصی شما برای راه‌اندازی نرم‌افزار کدگذاری است) در مکانی مجزا و امن پشتیبان تهیه کنید. برای مثال فایل را می‌توانید به صورت کدگذاری شده بر روی فلاپی‌دیسک یا بر روی حافظه‌های ع.نس قابل انتقال کوچک ثبت و نگاهداری کنید.

◆ نباید اطلاعات حساس را تنها به صرف اینکه یک نامه الکترونیک کدگذاری شده از سوی شخصی آشنا برای شما ارسال شده است، برای فرستنده ارسال کنید. ممکن است هویت فرستنده نام جعلی- و تنها شبیه نام و نشانی الکترونیکی که شما می‌شناسید- باشد. همیشه پیش از انتقال چنین اطلاعاتی هویت مشخص را احراز کنید. می‌توانید برای این کار با شخص مذبور- که تصور می‌کنید نامه از سوی وی ارسال شده- تماس تلفنی بگیرید و یا حتی با ارسال یک نامه الکترونیک مجزا- نه پاسخ دادن به نامه ارسالی وی- هویتش و درخواستش را مورد پرسش قرار دهید.

◆ باید به سایر افراد هم نحوه استفاده از کدگذاری را بیاموزید. هر چه تعداد افراد بیشتری این روش را به کار گیرند، همگی احساس امنیت بیشتری خواهیم کرد.

◆ نباید فراموش کنید که نامه‌ها را علاوه بر کدگذاری امضا کنید. این گونه می‌توانید دریافت‌کننده را نسبت به تغییر احتمالی مفاد پیام در حین انتقال به مقصد هوشیار کنید.

◆ باید فایل‌هایی را که می‌خواهید به‌عنوان ضمیمه همراه نامه‌ای کدگذاری شده ارسال کنید را باید جداگانه کدگذاری کنید چرا که این فایل‌ها هنگامی که شما نامه‌ای کدگذاری شده را می‌فرستید، به صورت اتوماتیک کدگذاری نمی‌شوند.

راهنمایی برای مدیریت امن‌تر دفتر و اطلاعات

مدیریت امن‌تر دفتر

مدیریت امن‌تر محل کار به معنای خلق برخی عادات است. عادات مدیریت دفتر می‌توانند مفید باشند و یا مضر. برای خلق عادات مفید مدیریت دفتر، درک منطق پشت‌سر هر عادت می‌تواند مفید باشد. ما در اینجا لیستی از عاداتی که می‌توانند در مدیریت امن‌تر اطلاعات به شما کمک کنند، ارائه نموده‌ایم. این عادات البته تنها زمانی کارآیی خواهند داشت که شما نه‌تنها در عمل آنها را اجرا کرده بلکه دلیل اهمیت آنها را هم درک کنید.

چه چیز در مدیریت دفتر در جهت تحقق امنیت و حریم خصوصی از اهمیت بیشتری برخوردار است؟

- آگاهی و اشراف نسبت به اطلاعات و افرادی که به آن دسترسی دارند
- ایجاد عادات امن و به کارگیری مدام آن
- استفاده مناسب از ابزار

مدیریت فنی

بسیاری از سازمان‌های دارای مدیر فنی یا مدیر سیستم‌ها هستند. مدیر فنی شخصی است که دارای مزیت‌های مدیریتی ظ (دسترسی‌های مدیریتی) بوده و امکان دسترسی به صندوق‌های پستی الکترونیک، رایانه‌های شبکه و یا نظارت بر نصب هر نوع نرم‌افزار جدیدی را دارا است. اگر کسی سازمان را ترک کرده و یا در دسترس نباشد، مدیر فنی می‌تواند به اطلاعات وی دسترسی داشته و فعالیت‌ها بدون توقف (و احساس خلاء غیبت شخص) ادامه یابند. مدیر فنی همچنین عهده‌دار حصول اطمینان از اینکه نرم‌افزارهای سیستم "پاک" بوده و از منبعی معتبر و قابل اعتماد به‌دست آمده‌اند، می‌باشد.

معضل در این مورد اما زمانی روی می‌دهد که برخی سازمان‌ها نقش مدیر فنی را صرفا نقشی فنی و منحصر با ارائه خدمات فنی تلقی کرده و لذا اجازه می‌دهند یک مقاطعه‌کار ثالث از امتیازهای مدیر فنی برخوردار باشد. این در حالی است که مدیر فنی دارای کنترل موثر تمامی اطلاعات درون سازمان بوده و لذا باید شخصی کاملا قابل اعتماد باشد. در برخی سازمان‌ها نقش مدیریت فنی را مدیر سازمان و یک شخص قابل اعتماد دیگر، به صورت مشترک عهده‌دار می‌شوند.

در برخی سازمان‌ها ترجیح داده می‌شود تا کلیدهای خصوصی و رمزهای عبور را جمع‌آوری کرده و کدگذاری کنند و آنها را به صورت مطمئن و امن از طریق یک سازمان مورد اعتماد، مورد حفاظت قرار دهند. این امر باعث می‌شود تا در صورتی که افراد رمز عبور خود را فراموش کرده و یا کلید خصوصی خود را از دست بدهند، از بروز مشکلاتی که فعالیت کلی سازمان را متاثر از خود کند، ممانعت شود. به هر حال بدیهی است که موقعیت مکانی محل نگاهداری فایل‌ها باید کاملا مخفی باقی بمانند. دستیابی به این فایل‌ها نیز باید توسط پروتکل‌های ویژه و فراگیر به شدت محدود شوند.

قواعد

- هرگز امتیازات مدیریت فنی را به یک مقاطعه‌کار ثالث واگذار نکنید. این افراد نه تنها به مراتب در مقایسه با افراد درون سازمان کمتر قابل اعتماد هستند بلکه دسترسی به شخصی در خارج از سازمان، در شرایط اضطراری به مراتب دشوارتر از شخصی درون سازمان است.

- تنها قابل اعتماد ترین افراد می‌توانند دارای امتیازات مدیر فنی باشند.

- میزان اطلاعاتی که باید در اختیار مدیر فنی قرار گیرد را مشخص کنید: دسترسی به تمامی رایانه‌ها، رمزهای ورود رایانه‌های، رمزهای ورود به شبکه، کلیدهای حل‌ح و رمزهای ورود متناظر با آنها و ...

- در صورتی که قصد دارید کپی‌هایی از رمزهای ورود و کلیدهای خصوصی را در سازمانی دیگر نگهداری کنید باید پروتکل‌هایی جامع برای دسترسی به آنها تعریف و اعمال کنید.

- اگر شخصی سازمان را ترک می کند، باید بلافاصله رمزهای ورود و کدهای دسترسی او تغییر یابند.
- در صورتی که شخصی با امتیازات مدیر فنی، سازمان را ترک می کند، تمامی رمزهای عبور و کدهای دسترسی باید بلافاصله تغییر یابند.

مدیریت نرم‌افزار

استفاده از نرم‌افزارهای سرقت شده یا قفل شکسته سازمان را در برابر آنچه که به"پلیس نرم‌افزار" موسوم است، آسیب‌پذیر می کند. مقامات می‌توانند به بهانه استفاده از نرم‌افزارهای غیرمجاز بر سازمان فشار اعمال کرده و یا با در نظر گرفتن جرایم سنگین، عملا فعالیت آنها را به تعطیلی بکشانند. در این شرایط سازمان تحت فشار عملا از همدردی و یا حمایت نشریات و رسانه‌های غربی هم برخوردار نمی‌شود چرا که در این جا دیگر فشاری بر یک سازمان غیردولتی داده نشده بلکه به"سارقان" حمله شده است. بدین ترتیب باید به شدت مراقب مجوز نرم‌افزارهای مورد استفاده بوده و هرگز اجازه ندهید تا نرم‌افزارهایی مورد استفاده توسط کارمندان و بنا به میل آنها تکثیر شوند. از سوی دیگر در نظر داشته باشید که نرم‌افزارهای سرقتی و غیرمجاز ممکن است حاوی ویروس باشند. هر زمانی که قصد نصب نرم‌افزاری را دارید، آن را در ابتدا با برنامه‌های ضدویروس بررسی کنید.

مدیر فنی باید بر روی کلیه نرم‌افزار های جدیدی که قرار است نصب شوند، کنترل داشته و از انجام بررسی های لازم بر روی آنها مطمئن شود. اجازه نصب نرم‌افزارهایی که به صورت بالقوه"ناامن" تلقی می‌شوند را ندهید. تنها نرم‌افزارهایی را نصب کنید که به آنها نیاز دارید.

در مورد تمامی نرم‌افزارهای مورد استفاده، آخرین دنبالک های امنیتی را هم نصب کنید(به‌ویژه در مورد مایکروسافت آفیس، مایکروسافت اینترنت اکسپلورر و نت‌اسکیپ). بزرگترین آسیب‌پذیری‌هایی که متوجه امنیت یک سیستم رایانه‌ای می‌شوند معمولا مربوط به نقایص نرم‌افزاها و یا سخت‌افزارهاای شناخته شده هستند. پیشنهاد می‌شود به استفاده از نرم‌افزارهای"متن باز" روی بیاورید. در حالی که اغلب نرم‌افزارها امنیت را در ممانعت از دسترسی دیگران به شاکله درونی خود می‌دانند، نرم‌افزارهای"متن باز" از تلاش و مجادله دائمی هکرها و کارشناسان امنیتی برای رفع نقایص خود استقبال می کنند. استفاده از نرم‌افزارهای"متن باز" و هر نرم‌افزاری جز نرم‌افزارهای ارائه شده از سوی مایکروسافت، این مزیت را برای شما به همراه خواهد داشت که کمتر در معرض حمله ویروس‌های استاندارد و هکرهای غیرشخصی قرار می گیرید. تعداد ویروس‌های ایجاد شده برای سیستم‌های عامل لینوکس و یا مک‌اینتاش به مراتب کمتر از ویندوز هستند چرا که کاربران ویندوز به مراتب بیشتر هستند. برنامه اوت لوک، پرطرفدارترین برنامه مرتبط با صندوق‌های پست الکترونیک است و بدین ترتیب پرطرفدارترین هدف برای هکرها محسوب می‌شود.

عادات مربوط به نامه‌های الکترونیک

کدگذاری نامه‌های الکترونیک باید تبدیل به یک عادت شود. ترویج عادت کدگذاری تمامی نامه‌ها به مراتب ساده‌تر از توجیه و نظارت بر اجرای سیاست‌های امنیتی سازمان برای کدگذاری نامه‌های دارای محتوای خاص است. به خاطر داشته باشید که اگر تمامی نامه های الکترونیک شما کدگذاری شوند، کسانی که بر رد و بدل شدن نامه‌های شما نظارت دارند هرگز نخواهند توانست رد و بدل شدن اطلاعات مهم حایز اهمیت را تشخیص دهند.

چند نکته مهم دیگر

◆ نامه‌های کدگذاری شده را همواره به همان شکل کدگذاری شده ثبت و نگاهداری کنید. همیشه می‌توانید این نامه‌ها را هنگام لزوم"کدگذاری" کنید اما به خاطر داشته باشید که نگاه داشتن سابقه کدگذاری نشده نامه‌ای ارسال شده باعث می‌شود تا هنگام دسترسی شخصی به رایانه شما، با مخاطراتی جدی روبه‌رو شوید. در این شرایط عملا دیگر تفاوتی نمی‌کند که نامه خود را به صورت عادی ارسال کرده یا کدگذاری کرده باشید.

◆ با سماجت و پیگیری از اینکه دریافت‌کنندگان نامه‌های کدگذاری شده شما، نامه‌تان را کدزدایی نکرده و برای دیگران ارسال نمی‌کنند و یا اینکه بدون متحمل شدن زحمت کدگذاری به شما جواب نمی‌دهند، اطمینان حاصل کنید، تنبلی افراد، مهمترین تهدیدی است که متوجه ارتباطات شما می‌شود.

◆ شاید بخواهید چند نشانی پستی الکترونیک برای فعالان میدانی سازمان ایجاد کنید. این نشانی‌ها معمولا چندان مورد استفاده قرار نگرفته و لذا توسط سرورهای س ئشح شناسایی نمی‌شوند. این نشانی‌های باید به صورت مداوم چک شوند، اما به استثنای ماموران میدانی شخص دیگری از آنها استفاده نکند. بدین ترتیب می‌توانید نشانی‌های پستی را که بیش از حد با ئشحس روبه‌رو هستند، بدون در خطر انداختن مبنای ارتباطی سازمان، حذف کنید.

نکاتی عام برای کافی نت‌ها و موارد دیگر

نامه‌های الکترونیکی که به صورت متن ساده و یا بدون کدگذاری ارسال می‌شوند ممکن است در فضای اینترنت توسط گروه‌های متفاوت خوانده شوند. تحقق این احتمال تنها بستگی به میزان علاقه‌مندی و صرف تلاش از سوی آنها است. در میان این گروه‌ها می‌توان به شرکت ارائه دهنده خدمات ارتباطات اینترنتی محلی و یا شرکت‌هایی که نامه شما از طریق آنها به مقصد می‌رسد (شرکتی که گیرنده نامه از خدمات ارتباطات اینترنتی آن استفاده می‌کند) اشاره کرد. یک نامه الکترونیک برای رسیدن به مقصد، از زمان ارسال از رایانه‌های متعددی می‌گذرد، مرزهای جغرافیایی در ارتباطات اینترنتی بی‌معنی هستند. به عبارت دیگر حتی اگر شما برای شخصی در همان محل استقرار خود نامه‌ای ارسال کنید ممکن است این نامه از سرورهای واقع در کشوری دیگر گذشته و سپس به مقصد برسد.

برخی نکات عام در مورد مسائلی که غالبا کاربران اینترنت در مورد آن درک اشتباهی دارند، عبارتند از:

◆ محافظت از یک فایل با رمز عبور، اصولا تاثیر چندانی در محافظت از فایل‌ها ندارد. میزان این تاثیر چنان ناچیز است که در مورد اسناد حاوی اطلاعات ذی‌قیمت و حساس بهتر است اصلا زحمت قرار دادن رمز عبور بر فایل‌ها را متحمل نشوید. این رمزهای ورود تنها نوعی حس کاذب امنیت را به شما القا می‌کنند.

◆ زیپ کردن فایل‌ها مانع آن نمی‌شود که افراد محتویات درونی آن را مشاهده کنند. به عبارت دیگر زیپ کردن فایل‌ها مانع به ثمر نشستن کنجکاوی دیگران نمی‌شود.

◆ در صورتی که می‌خواهید از ارسال امن یک فایل یا نامه الکترونیک مطمئن شوید از کدگذاری استفاده کنید. (به سایت www.privaterra.org مراجعه کنید).

◆ در صورتی که می‌خواهید نامه‌ای الکترونیک و یا سندی را به صورت امن منتقل کنید، در تمامی مراحل تا رسیدن به مقصد نهایی

از کدگذاری استفاده کنید. ارسال یک نامه الکترونیکی کدگذاری شده از دفتری واقع در محل انجام فعالیت‌های میدانی به نیویورک، لندن و یا هر جای دیگر و سپس ارسال همان نامه الکترونیک (این بار بدون کدگذاری و به صورت متن ساده) برای شخصی دیگر می تواند کل فرآیند را بی‌اثر کند.

◆ اینترنت فی‌نفسه پدیده‌ای جهانی است. هیچ تفاوتی میان ارسال پیامی الکترونیک میان دو دفتر واقع در مانهاتان و یا از یک کافی نت واقع در آفریقای جنوبی به دفتری در لندن وجود ندارد. تا حد امکان، همیشه از کدگذاری استفاده کنید، حتی اگر پیام و یا اطلاعاتی که می‌فرستید به هیچ وجه حساس نباشند.

◆ از نصب بودن نرم‌افزارهای ضدویروس بر روی رایانه مورد استفاده خود اطمینان حاصل کنید. بسیاری از ویروس‌ها با هدف استخراج اطلاعات از رایانه شما نوشته می‌شوند، اطلاعات می‌تواند بر روی دیسک سخت رایانه شما ذخیره شده یا فایل‌های صندوق پست الکترونیک شما بوده و یا حتی نام‌ها و نشانی‌های موجود در دفترچه نشانی‌های پست الکترونیک شما باشند.

◆ از مجاز بودن نسخه نرم‌افزاری مورد استفاده خود اطمینان حاصل کنید. اگر از نرم‌افزارهای غیرمجاز استفاده می کنید، از نگاه دولت و رسانه‌ها شما و سازمانتان دیگر مدافع حقوق بشر نیستید بلکه "دزد نرم‌افزار" محسوب می‌شوید. بهترین راه‌حل در این یمان استفاده از نرم‌افزارهای "متن باز" است. آنها رایگان هستند!

◆ در صورتی که از اینترنت استفاده می کنید، به خاطر داشته باشید که هیچ راه‌حلی برای تضمین امنیت شما به صورت صددرصد وجود ندارد. نسبت به مواردی که برخی افراد با استفاده از روش‌های مرسوم به "هک اجتماعی" یا "" به داخل سیستم شما نفوذ می کنند، هوشیار باشید. در این موارد هکرها گاه از طریق تلفن یا ارسال نامه‌های الکترونیکی خود را در پوشش فردی دیگر - غالبا مورد اعتماد شما - معرفی می‌کنند. قدرت تشخیص و شعور خود را به کار بگیرید.

اعلامیه سازمان ملل
در مورد مدافعین حقوق بشر

A/SER/53/144
۸ مارس ۱۹۹۹
پنجاه و سومین جلسه مجمع عمومی
مورد شماره ۱۱۰ - در دستورکار

قطعنامه مصوب مجمع عمومی
بر اساس گزارش کمیته سوم
A/53/625/53/2

۵۳/۱۴۴ اعلامیه حقوق و مسئولیت افراد، گروه‌ها و نهادهای جامعه در ترویج و حمایت از حقوق بشر و آزادی‌های اساسی شناخته شده جهانی

مجمع عمومی،

- با تاکید مجدد بر اهمیت رعایت اهداف و اصول منشور سازمان ملل متحد برای ترویج و حمایت کلیه حقوق بشر و آزادی‌های اساسی برای همه افراد در همه کشورهای جهان،

- با توجه به قطعنامه ۷/۱۹۹۸ کمیسیون حقوق بشر در ۳ آپریل ۱۹۹۸ ، که در آن کمیسیون متن پیش نویس اعلامیه حقوق و مسئولیت افراد، گروه‌ها و نهادهای جامعه در ترویج و حمایت از حقوق بشر و آزادی‌های اساسی شناخته شده جهانی را تصویب نموده است،

- با توجه به قطعنامه ۳۳/۱۹۹۸ شورای اقتصادی و اجتماعی در ۳۰ ژوئیه ۱۹۹۸، که در آنجا شورا به مجمع عمومی توصیه می‌نماید که پیش نویس قطعنامه را تصویب نماید،

- با آگاهی از اهمیت تصویب پیش‌نویس قطعنامه همزمان با پنجاهمین سالگرد اعلامیه جهانی حقوق بشر،

۱ - اعلامیه حقوق و مسئولیت افراد، گروه‌ها و نهادهای جامعه در ترویج و حمایت از حقوق بشر و آزادی‌های اساسی شناخته شده جهانی را که به پیوست این قطعنامه آمده است تصویب می نماید؛

۲ - از دولت‌ها، سازمان‌ها و نهادهای وابسته به سازمان ملل و سازمان‌های غیردولتی و بین‌دولتی دعوت می نماید که تلاش‌های خود را برای نشر و گسترش اعلامیه و افزایش احترام و درک جهانی نسبت به آن شدت بخشیده و از دبیرکل درخواست می‌نماید که متن اعلامیه را در چاپ جدید [حقوق بشر : مجموعه‌ای از اسناد بین‌المللی] بگنجاند .

هشتاد و پنجمین جلسه عمومی

۹ دسامبر ۱۹۹۸

اعلامیه حقوق و مسئولیت افراد، گروه‌ها و نهادهای جامعه در ترویج و حمایت از حقوق بشر و آزادی‌های اساسی شناخته شده جهانی

مجمع عمومی،

- با تاکید مجدد بر اهمیت رعایت اهداف و اصول منشور سازمان ملل متحد برای ترویج و حمایت کلیه حقوق بشر و آزادی‌های اساسی برای همه افراد در همه کشورهای جهان،

- همچنین با تاکید مجدد بر اهمیت اعلامیه جهانی حقوق بشر و میثاق‌های بین‌المللی حقوق بشر به‌عنوان عناصر پایه‌ای تلاش‌های بین‌المللی برای پیشبرد احترام جهانی و رعایت حقوق بشر وآزادی‌های اساسی و اهمیت دیگر اسناد حقوق بشر که در سیستم سازمان ملل متحد، و همچنین در سطح منطقه‌ای، به تصویب رسیده است،

- با تکیه بر اهمیت این که همه اعضای جامعه بین‌المللی باید، همراه با یکدیگر یا جداگانه، وظیفه خطیر خود را در ارتقاء و تشویق احترام برای حقوق بشر و آزادی‌های اساسی برای همه بدون هیچگونه تمایز، از جمله تمایز بر اساس نژاد، رنگ، جنس، زبان، مذهب، عقیده سیاسی یا عقاید دیگر، خاستگاه اجتماعی یا ملی، مالکیت، تولد یا مشخصه‌های دیگر، و با تاکید مجدد بر اهمیت ویژه دستیابی به همکاری بین‌المللی برای انجام این وظیفه بر اساس منشور،

- با توجه به اهمیت نقش همکاری بین‌المللی در، و کار ارزشمند افراد، گروه‌ها و سازمان‌ها در یاری رسانی به، حذف موثر همه اشکال نقض حقوق بشر و آزادی‌های اساسی مردمان و افراد، از جمله در رابطه با نقض سیستماتیک، آشکار و گسترده‌ای که حاصل آپارتائید، هرگونه تبعیض نژادی، استعمار، اشغال یا حاکمیت خارجی، تجاوز یا تهدید حاکمیت ملی، یکپارچگی ملی یا تمامیت ارضی و خودداری از برسمیت شناختن حق مردمان بر حاکمیت بر خویش و حق هر مردمی بر اعمال حاکمیت تام بر ثروت و منابع خویش،

- با در نظر گرفتن ارتباط امنیت و صلح بین‌المللی و برخورداری از حقوق بشر و آزادی‌های اساسی، و با این نگاه که نبود امنیت و صلح بین‌المللی عذری برای عدم رعایت نیست،

- با تصریح مجدد بر اینکه کلیه حقوق بشر و آزادی‌های اساسی جهانی، غیرقابل تفکیک و درهم آمیخته و وابسته به‌همدیگر بوده و بایستی به شیوه‌ای هم‌ارز، عادلانه و بدون تبعیض دراعمال هیچیک از این حقوق و آزادی‌ها با همدیگر ترویج و اعمال شود،
- با تکیه‌بر اهمیت اینکه مسئولیت اصلی و وظیفه ترویج و حمایت حقوق بشر و آزادی‌های اساسی بر دوش حکومت است،
- با تصریح اینکه حق و مسئولیت افراد، گروه‌ها و سازمانها در افزایش احترام و ترویج شناخت حقوق بشر و آزادی‌های اساسی در سطوح ملی و بین‌المللی،

اعلام می دارد :

ماده ۱

هر فردی حق دارد، به طور فردی یا همراه با دیگران، در راه ترویج و حمایت و تحقق حقوق بشر و آزادی‌های اساسی در سطوح ملی و بین‌المللی بکوشد .

ماده ۲

۱ - هر حکومتی مسئولیت اصلی و وظیفه حمایت، ترویج و تحقق کلیه حقوق بشر و آزادی‌های اساسی را، در میان وظایف دیگر، بر عهده دارد به این شکل که از طریق انجام اقدام‌های موردنیاز همه شرایط لازم اجتماعی، اقتصادی، سیاسی و دیگر زمینه‌ها را فراهم نموده و نیز با تامین تضمین حقوقی لازم، به همه افراد تحت قلمرو خویش اطمینان دهد که می‌توانند، بطور فردی یا همراه با دیگران، از همه این حقوق و آزادیها در عمل بهره ببرند .

۲ - هر حکومتی باید چنان اقدامات قانونگذاری، دولتی و دیگر گامهای ضروری را اجرا نماید تا بتواند تضمین کند که حقوق و آزادی‌های اساسی را که در اعلامیه حاضر بدانها اشاره می‌شود، در عمل دارای ضمانت اجرایی است .

ماده ۳

قوانین داخلی همخوان با منشور سازمان ملل متحد و دیگر وظایف بین المللی حکومت در زمینه حقوق بشر و آزادی‌های اساسی، چارچوب قضایی است که در آن حقوق بشر و آزادی‌های اساسی بایستی رعایت شده و مورد بهره‌وری قرار گرفته و همه فعالیت‌هایی که در زمینه ترویج، حمایت و تحقق عملی آن حقوق و آزادی‌ها در اعلامیه حاضر بدانها اشاره می‌شود، باید انجام پذیرد .

ماده ۴

هیچ چیزی در اعلامیه حاضر نباید به گونه‌ای تفسیر شود که در تناقض یا فروکاستن اهداف و اصول منشور سازمان ملل بوده و یا تمهیدات اعلامیه جهانی حقوق بشر، میثاق‌های بین‌المللی حقوق بشر و دیگر سندها و تعهدهای بین‌المللی مربوط به‌این زمینه را محدود یا تحریف نماید .

ماده ۵

برای هدف ترویج و حمایت حقوق بشر و آزادی‌های اساسی، هر کسی حق دارد، به طور فردی یا همراه با دیگران، در سطوح ملی و بین‌المللی :

(آ) بطور مسالمت‌آمیز ملاقات یا گردهمایی داشته باشد؛

(ب) به ایجاد، عضویت و همکاری با گروه، انجمن یا سازمان‌های غیردولتی بپردازد؛

(پ) با سازمان‌های غیردولتی یا بین دولتی ارتباط برقرار کند .

ماده ۶

هر کسی حق دارد، به طور فردی یا همراه با دیگران:

(آ) اطلاعات مربوط به کلیه حقوق بشر و آزادی‌های اساسی را، از جمله حق دسترسی به اطلاعات مربوط به چگونگی اجرای این حقوق و آزادی‌ها در سیستم‌های دولتی، قضایی و قانونگذاری داخلی را بداند، جستجو کند، بدست آورد، دریافت کند و نگهداری نماید .

(ب) چنانچه در حقوق بشر و دیگر سندهای بین‌المللی مربوطه آمده است، دیدگاه‌ها، اطلاعات و آگاهی درباره حقوق بشر و آزادی‌های اساسی را آزادانه به دیگران انتشار داده و آشکار سازد و در اختیار دیگران قرار دهد .

(پ) به مطالعه، بحث، پایه‌گذاری و هواداری عقاید درباره رعایت کلیه حقوق بشر و آزادی‌های اساسی، هم در قانون و هم در عمل، پرداخته و، و بوسیله اینها و دیگر شیوه‌های مناسب، به جلب توجه عموم به این مسائل بپردازد .

ماده ۷

هر کسی حق دارد، به طور فردی یا همراه با دیگران، اصول و ایده‌های نوین حقوق بشر را مورد بحث قرار داده و پرورش دهد و برای پذیرفته شدن آنها تبلیغ کند .

ماده ۸

۱ . هر کسی حق دارد بدور از هرگونه تبعیض و به گونه‌ای موثر، به طور فردی یا همراه با دیگران، در اداره امور کشور و در پیشبرد امور جامعه شرکت داشته باشد .

۲ . این شامل این حق، در میان دیگر حقوق، می‌شود که هر کسی، بطور فردی یا همراه با دیگران، پیشنهادها و انتقاداتی به نهادهای دولتی و موسسات و سازمان‌هایی که در رابطه با امور اجتماعی هستند، به منظور بهبود عملکرد آنها و یا جلب توجه به جنبه‌هایی از کار آنها که ممکن است مانعی در ترویج، حمایت و تحقق حقوق بشر و آزادی‌های اساسی باشد، ارائه نماید .

ماده ۹

۱ . در استفاده از حقوق بشر و آزادی‌های اساسی، از جمله ترویج و حمایت از حقوق بشری که در اعلامیه حاضر بدانها اشاره می‌شود، هر کسی حق دارد، بطور فردی یا همراه با دیگران، از گزیر موثر بهره‌مند شده و در صورت نقض این حقوق محافظت شود .

۲ . بدین منظور، هر کسی که گفته می‌شود حقوق و آزادی‌های وی نقض شده، این حق را دارد که، شخصا یا از طریق نماینده حقوقی رسمی، شکایت کرده و این شکایت را در اسرع وقت در یک جلسه علنی درمقابل یک مقام قضایی یا مقام قانونی دیگر که مستقل، بیطرف و دارای صلاحیت است، مورد بررسی گذارده و از آن مقام تصمیمی، بر اساس قانون، دریافت دارد که شامل دادخواهی وی از جمله هر گونه غرامت لازم، در جاییکه موردی از نقض حقوق بشر یا آزادی‌های فرد وجود داشته، و همچنین اجرای سریع تصمیم نهایی و پرداخت غرامت باشد .

۳ . به همان منظور، هر کسی این حق را، در میان دیگر حقوق، دارد که بطور فردی یا همراه با دیگران:

(آ) از سیاست‌ها و عملکردهای افراد مسئول و نهادهای دولتی در مورد نقض حقوق بشر و آزادی‌های اساسی، از طریق ارائه درخواست‌نامه یا دیگر شیوه‌های مناسب، به مقامات قضایی، دولتی یا قانونگذاری داخلی یا هر مقام دارای صلاحیت دیگری که توسط قانون تعیین شده، شکایت کند و این مقام باید تصمیم خود را در مورد شکایت هرچه سریعتر اعلان نماید؛

(ب) در جلسه‌های علنی، روند پیشرفت و دادرسی شرکت نماید تا بتواند نظر خود را درباره همخوانی آنها با قوانین کشور و میزان هماهنگی با وظایف و تعهدات بین‌المللی تعیین کند.

(پ) یاری حقوقی در سطح تخصصی و شایسته یا دیگر توصیه‌ها و یاری‌رسانی را در دفاع از حقوق بشر و آزادی‌های اساسی ارائه دهد.

۴. به همان منظور، و در راستای اسناد و مقررات بین‌المللی مربوطه، هر کسی این حق را دارد که، بطور فردی یا همراه با دیگران، دسترسی بلامانع و ارتباط با نهادهای بین‌المللی دارای صلاحیت ویژه یا عمومی داشته باشد تا درباره امور مربوط به حقوق بشر و آزادی‌های اساسی ارتباط برقرار کرده و اطلاعات دریافت نماید.

۵. حکومت بایستی هرگاه که دلایل کافی برای باور به اینکه نقض حقوق بشر و آزادی‌های اساسی در جایی از قلمرو تحت حاکمیت آن انجام پذیرفته وجود دارد، تحقیقات فوری و بیطرفانه‌ای را انجام دهد یا تضمین نماید که چنین تحقیقاتی انجام خواهد گرفت.

ماده ۱۰

هیچکس نباید با انجام عملی، یا بی‌عملی درهنگام ضرورت عمل، در نقض حقوق بشر و آزادی‌های اساسی مشارکت جوید و هیچکس نباید بخاطر خودداری از مشارکت در نقض حقوق بشر و آزادی‌های اساسی مورد مجازات یا آزار قرار گیرد.

ماده ۱۱

هر کسی این حق را دارد که، بطور فردی یا همراه با دیگران، به شیوه قانونی به شغل یا حرفه خویش بپردازد. هر کسی که بخاطر حرفه خویش، می‌تواند بر کرامت انسانی، حقوق بشر و آزادی‌های اساسی دیگران تاثیرگذار باشد، بایستی این حقوق و آزادی‌ها را محترم شمرده و مطابق با اصول اخلاق یا استانداردهای شغلی و حرفه‌ای بین‌المللی مربوطه رفتار نماید.

ماده ۱۲

۱. هرکسی این حق را دارد که، بطور فردی یا همراه با دیگران، درفعالیت‌های مسالمت آمیز بر علیه نقض حقوق بشر و آزادی‌های اساسی شرکت نماید.

۲. حکومت بایستی کلیه اقدامات لازم را به عمل آورد تا تضمین نماید که از هر کسی، بطور فردی یا همراه با دیگران، در مقابل هرگونه خشونت، تهدید، انتقام جویی، تبعیض منفی واقعی یا حقوقی، فشار یا هرگونه عمل سرخود که پیامد استفاده برحق از حقوقی است که در اعلامیه حاضر بدانها اشاره شده، توسط مقامات دارای صلاحیت حمایت خواهد شد.

۳. در این رابطه، هر کسی دارای این حق است که، بطور فردی یا همراه با دیگران، هنگامی که با روش‌های مسالمت‌آمیز در مقابل اعمال و فعالیت‌های منسوب به حکومت از جمله شیوه‌های حذفی که به نقض حقوق بشر و آزادی‌های اساسی می‌انجامد، و همچنین با اعمال خشونت‌باری که گروه‌ها یا افراد مرتکب می‌شوند که در بهره‌وری از حقوق بشر و آزادی‌های اساسی تاثیر می‌گذارد، واکنش نشان می‌دهد یا مخالفت می‌کند، توسط قانون کشور در عمل مورد حمایت قرار گیرد.

ماده ۱۳

هر کسی این حق را دارد که، بطور فردی یا همراه با دیگران، در جلب، دریافت و استفاده از منابع برای هدف مشخص ترویج و حمایت از حقوق بشر و آزادی‌های اساسی به شیوه‌های مسالمت آمیز، در راستای ماده ۳ اعلامیه حاضر، اقدام نماید.

ماده ۱۴

۱ . حکومت این مسئولیت را بر عهده دارد که با اقدامات قانونگذاری، قضایی، دولتی یا دیگر اقدامات مناسب درک همه افراد تحت حاکمیت خود را از حقوق مدنی، سیاسی، اقتصادی، اجتماعی و فرهنگی شان ارتقاء دهد .

۲ . چنین اقداماتی باید از جمله شامل و نه محدود به اقدامات زیر باشد :

(آ) انتشار و در دسترس عموم قرار دادن قوانین کشور و مقررات و اسناد پایه‌ای حقوق بشر بین‌المللی .

(ب) اجازه دسترسی کامل و برابر به اسناد بین‌المللی در زمینه حقوق بشر، از جمله گزارش‌های دوره‌ای حکومت به عنوان عضو به نهادهایی ایجاد شده توسط عهدنامه‌های حقوق بشر بین‌المللی، و خلاصه گزارش مذاکرات و گزارش‌های رسمی آن نهادها .

۳ . حکومت بایستی، بهنگام لزوم، ایجاد و گسترش سازمان‌های مستقل برای ترویج و حمایت از حقوق بشر و آزادی‌های اساسی در همه قلمرو تحت حاکمیت خود را، از تلاشگران حل اختلاف گرفته تا کمیسیون‌های حقوق بشر یا دیگر اشکال سازمان‌های ملی، تضمین نموده و تقویت نماید .

ماده ۱۵

حکومت این مسئولیت را بر عهده دارد که آموزش حقوق بشر و آزادی‌های اساسی را در همه سطوح تحصیل فراهم نموده و ترویج دهد و تضمین نماید که همه کسانی که مسئولیت تربیت وکیل‌ها، مامورین اجرای قانون، افراد نیروهای مسلح و مقامات دولتی را برعهده دارند، بخش‌های مناسبی از تدریس حقوق بشر را در برنامه آموزشی خود قرار دهند .

ماده ۱۶

افراد، سازمان‌های غیر دولتی و موسسه‌های مربوطه نقش مهمی در عمل برای کمک به افزایش آگاهی عمومی از پرسش‌های مربوط به همه حقوق بشر و آزادی‌های اساسی از راه فعالیت‌هایی همچون آموزش، تربیت و پژوهش در این زمینه‌ها بر عهده دارند تا، از جمله، با در نظر گرفتن پیشینه‌های گوناگون جوامع و محله‌هایی که فعالیت‌های خود را در آنجا انجام می‌دهند، هر چه بیشتر تفاهم، مدارا، صلح و روابط دوستانه میان ملت‌ها و میان همه گروه‌های نژادی و مذهبی را تقویت نمایند .

ماده ۱۷

در استفاده از حقوق و آزادی‌هایی که در اعلامیه حاضر بدانها اشاره می‌شود، هر کسی، که بطور فردی یا همراه با دیگران فعالیت می‌کند، بایستی تنها در آن زمینه‌هایی با محدودیت مواجه شود که در راستای انجام تعهدات بین‌المللی بوده و فقط به منظور تضمین احترام و رعایت حقوق و آزادی‌های دیگران و تامین ضروریات اخلاق، نظم عمومی، و رفاه عام در یک جامعه دمکراتیک توسط قانون مقرر شده است .

ماده ۱۸

۱ . هر کسی وظایفی درقبال و درون اجتماعی که رشد کامل و آزاد شخصیت وی تنها در آن امکان‌پذیر است، دارد .

۲ . افراد، گروه‌ها، موسسات و سازمان‌های غیر دولتی نقشی مهم در عمل و وظیفه‌ای در امر تضمین دمکراسی، ترویج حقوق بشر و آزادی‌های اساسی و کمک به ترویج و پیشبرد جوامع، سازمان‌ها و روندهای دمکراتیک دارند .

۳ . افراد، گروه‌ها، موسسات و سازمان‌های غیردولتی همچنین نقش مهمی و و ظیفه‌ای در یاری‌رسانی، به هنگام مناسب، به ترویج حق هر فرد به نظم اجتماعی و بین‌المللی که در آن حقوق و آزادی‌های برشمرده شده در اعلامیه جهانی حقوق بشر و دیگر اسناد

حقوق بشر بطور کامل تحقق یابد، دارند .

ماده ۱۹

هیچ چیز در اعلامیه حاضر نباید به عنوان حقی برای هیچ فرد، گروه یا نهاد اجتماعی یا حکومتی در انجام فعالیت یا عملی در جهت تخریب حقوق و آزادی‌های بیان شده در اعلامیه حاضر تفسیر شود .

ماده ۲۰

هیچ چیز در اعلامیه حاضر نباید چنان تفسیر گردد که به حکومت‌ها اجازه دهد از فعالیت‌های افراد، گروه‌هایی از افراد، موسسه‌ها یا سازمان‌های غیردولتی که مخالف با مواد منشور سازمان ملل متحد است، حمایت نموده یا به پیشرفت آنها کمک کند .