سال اقتصاد مقاومتی، اقدام و عمل

پدافند غیرعامل

استانداری آذربایجان شرقی
اداره کل پدافند غیرعامل

ماهنامه پدافند غیرعامل
شماره ۹ – فروردین ماه ۱۳۹۵

در این شماره خواهید خواند:

سخن سردبیر ماهنامه ۱
هشدار های بانکی پلیس فتای استان ۲
اصول اولیه امنیت اطلاعات برای شرکت ها و سازمان های کوچک ۳
نگاهی اجمالی بر شهرسازی مبتنی بر پدافند غیرعامل ۵
بیت کوین؛ طلای دیجیتال یا حباب روی آب؟ ۱۱
پاسخ ایران به حملات سایبری آمریکا ۱۶
عناوین رویدادهای مهم خبری ۲۰

مقام معظم رهبری در دیدار اعضای مجلس خبرگان تاکید کردند:

هدف دشمن از «نفوذ» تهی‌کردن نظام از عناصر درونی قدرت است. استکبار در راهبرد نفوذ چند هدف اصلی را دنبال می کند: «تأثیرگذاری در مراکز تصمیم ساز و تصمیم گیر»، «تغییر باورهای مردم» و «تغییر محاسبات و مواضع مسئولان».

سخن سردبیر ماهنامه

بِسم اللهِ الرّحمنِ الرّحیم

منّت خدای را عز و جل که طاعتش موجب قربتست و به شکر اندرش مزید نعمت. هر نفسی که فرو می رود ممدّ حیاتست و چون بر می آید مفرّح ذات پس در هر نفسی دو نعمت موجودست و بر هر نعمت شکری واجب.

حمد و ثنای بی قیاس خدای را که با استعانت از درگاه او، با مساعدت های فعالان پدافند غیرعامل ۸ شماره از ماهنامه پدافند غیرعامل را در سال گذشته منتشر کردیم. در این راه وامدار حمایت ها و ارشادات مسئولین محترم استان از جمله استاندار محترم استان جناب آقای دکتر جبارزاده، معاون محترم سیاسی و امنیتی استان جناب آقای دکتر شبستری و مدیرکل محترم پدافند غیرعامل استان جناب آقای سردار جهانسری هستیم. انتشار نشریه پدافند غیرعامل فرصتی ناب تعبیر می گردد که محلی برای نشر افکار، ایده ها و نظریه های اصحاب فکر و قلم استان است. اینک که به لطف خداوند بزرگ بزرگترین قدرت موشکی و نظامی و سایبری منطقه هستیم، پدافند غیرعامل نیز جزو ضروریات و تکمیل کننده این پازل افتخارآمیز است. اگر دیروز فرزندان این مرز و بوم با فداکردن جان و مال خود در جنگی نابرابر،حماسه آفریدند امروزه این جنگ به شکلی دیگر شروع شده و این بار اراده و باور مردم را نشانه گرفته و نیاز به حماسه ای از جنس دیگر دارد. حملات سایبری به زیرساخت های کشورمان، تحریم های ظالمانه، کارشکنی های غیرمتعارف، موج سواری روی مسائل مختلف اجتماعی، ایجاد تشتت و در نهایت ایجاد

جنگ روانی و تضعیف امنیت روانی مردم تنها بخشی از هجمه های دشمنان و مخالفان اسلام و نظام مقدس جمهوری اسلامی ایران در این روزهاست. بنابراین به روحیه ای انقلابی، عزمی راسخ ، اراده ای جدی و برنامه ای منسجم و گسترده برای خنثی سازی این تهدیدات نیازمندیم. در این راستا پدافند غیرعامل استانداری در دوسال گذشته برنامه ای گسترده برای نهادینه کردن و آموزش مفاهیم پدافند غیرعامل تدارک دیده که انتشار ماهنامه پدافند غیرعامل تنها بخشی از این برنامه است. این ماهنامه با هدف گسترش و نهادینه کردن مفاهیم پدافند غیرعامل، ترویج و انتشار یافته‌های پژوهشی و آثار اندیشمندان در حوزه های پدافند غیرعامل اعم از تهدیدشناسی، فرهنگی و مردم محور ، اقتصادی، سایبری،زیستی ، شیمیایی، هسته ای، کالبدی و ... با صاحب امتیازی اداره کل پدافند غیرعامل استانداری و به منتشر می‌شود. در سال گذشته بیشتر مسائل عمومی در این ماهنامه منتشر می شد و امسال برآنیم تا با همراهی صاحب‌نظران، استادان و پژوهشگران علاقه‌مند مطالب تخصصی را نیز در این نشریه اضافه کنیم و در این راستا نیازمند مطالب ارزشمندتان هستیم.

صالح و طالح متاع خویش نمودند	تا چه قبول افتد و چه در نظر آید

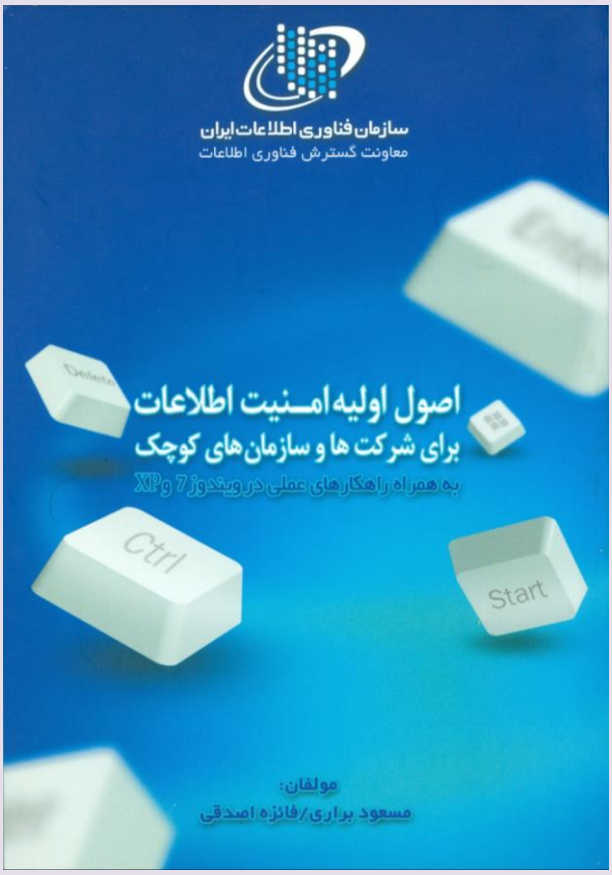
محمد بامدادی(سردبیرماهنامه پدافند غیرعامل استانداری آذربایجان شرقی)- آدرس پست الکترونیکی:padafand.gheyre.amel100@gmail.com

هشدار های بانکی پلیس فتای استان

سرهنگ محمودی، رئیس پلیس فتای استان
az.sh_fata@police.ir

- در تماس‌های تلفنی، پیامکی و نیز ارتباط از طریق پست الکترونیک، از بازگو کردن مشخصات محرمانه خصوصی کارت بانکی (رمزها، کد اعتبارسنجی و تاریخ انقضاء) برای دیگران خودداری شود
- تاکید می‌شود در مقاطع زمانی دلخواه برای تغییر رمزهای کارت خود اقدام کنید. این امر به ویژه در مواردی که احتمال می‌رود اشخاص ناشناس به هر طریقی از رمز عبور آگاهی یابند از ضرورت دو چندانی برخوردار می شود.
- نوشتن رمز عبور بر رو یا پشت کارت یا نگهداری آن در مجاورت کارت جداً خودداری شود.
- در مبادلات روزمره مالی تنها موردی که باید به طرف مقابل به منظور انجام انتقال وجه (کارت به کارت) اعلام شود صرفاً شماره کارت، حساب یا شبای مربوط به خود است.
- از پذیرش هرگونه درخواست افراد ناشناس به منظور استفاده از خدمات بانکی به واسطه کارت شما اکیداً خودداری شود.
- رمز های عبور خود را بصورت ترکیبی طراحی کرده و از کلمات متداول و شماره های شناسنامه ، تلفن همراه، شماره شناسنامه برای این موضوع استفاده نکنید.
- اطلاعات مهم کارت یا حساب بانکی خود بویژه رمز عبور را در اختیار افراد ناشناس قرار ندهید.
- هنگام وارد نمودن رمز اینترنت بانک حتماً از صفحه کلید امنیتی استفاده کنید. برخی برنامه های جاسوسی داده های وارد شده توسط صفحه کلید شما را کنترل می کنند.
- در زمان استفاده از پایانه های فروشگاهی pos رمز عبور کارت را خودتان وارد کنید.
- سعی کنید حتی الامکان برای پرداخت های اینترنتی از کافی نت ها، فرودگاه ها و اماکن عمومی استفاده نکنید.
- برای پرداخت های اینترنتی حتماً از سایت هایی که به آنها اطمینان دارید استفاده کنید. برای مثال از علامت قفل موجود در سایت که حاکی از صحت می باشد، اطمینان حاصل نمایید.
- در صورت مشاهده هر گونه تغییر در دستگاه ATM (تغییر در کارت خوان، تغییر صفحه کلید و یا دوربین نصب شده مشکوک) از دستگاه استفاده نکرده و سریعاً آن را به مسئول شعبه اطلاع دهید.

اصول اولیه امنیت اطلاعات برای شرکت ها و سازمان های کوچک



خلاصه ای از کتاب اصول اولیه امنیت اطلاعات برای شرکت ها و سازمان های کوچک،:«مولفان: مسعود براری، فائزه اصدقی، ناشر: انتشارات اندیکا، چاپ اول، ۱۳۹۰»

قسمت دوم – توصیه های ضروری در خصوص حفاظت از اطلاعات در ارتباط با شبکه و اینترنت

۲-۹- مسائل و مشکلات دانلود نرم افزار از اینترنت

از صفحات وب ناشناس نرم افزار دانلود نکنید.

اگر تصمیم به استفاده از نرم افزار رایگان یا اشتراکی را از یک منبع در وب دارید باید مراقب باشید بسیاری از این نرم افزارها بدون پشتیبانی فنی هستند.

۲-۱۰- چگونگی محافظت در برابر مهندسی اجتماعی

مهندسی اجتماعی تلاش شخصی و یا الکترونیکی برای بدست آوردن اطلاعات و یا دسترسی غیرمجاز به سیستم، امکانات و بخش های حساس سیستم و دستکاری آنهاست.

برای محافظت در برابر تکنیک های مهندسی اجتماعی:

باید به کارکنان آموزش های لازم داده شود تا زمانی که شخصی با آنها تماس می گیرد و تقاضای کمک، دریافت اطلاعات و یا دسترسی به سیستم خاص می کند هوشیار باشند. کارمند باید سوالاتی در مورد تایید هویت فرد بپرسد که مرتبط با سازمان باشد. همچنین کارمند باید کوششی که برای بدست آوردن اطلاعات یا دسترسی به سیستم صورت گرفته را به مدیریت اطلاع دهد.

قسمت سوم- راهکارهای کاهش هزینه های وقوع رخداد

باید تدابیری اندیشید که هزینه های ناشی از وقایع را به حداقل رساند.

۳-۱- ملاحظه و برنامه ریزی بازیابی اطلاعات برای وقایع احتمالی و فاجعه آمیز

در صورت بروز یک فاجعه چه اتفاقی می افتد؟

آیا احتمال وقایعی همچون قطع برق، روشن شدن آب پاش های ضدحریق به صورت تصادفی را پیش بینی کرده اید؟

آیا یک طرح مناسب برای بازیابی اطلاعات سازمانتان در زمان حادثه و یا بعد از آن را دارید؟

در مورد قطع برق، برای کامپیوترها و اجزای حساس شبکه از برق اضطراری (UPS) استفاده کنید.برق اضطراری این امکان را می دهد تا از طریق آن بتوان اطلاعات خود را قبل از قطع کامل برق ذخیره کنید.

آیا فهرستی از تمام اطلاعات مورد استفاده و در حال اجرا در سازمانتان دارید؟

آیا می دانید که هر نوع از اطلاعات در کجا و برروی کدام کامپیوتر و یا سرور واقع شده است؟

آیا اولویت بندی برای اطلاعات سازمان انجام داده و می دانید که چه نوع از اطلاعات دارای اهمیت بیشتری و در چه نقاطی قرار دارند؟

اگر فهرستی از اطلاعات مهم موجود در سازمان را ندارید اینکار را کنید، مراحل زیر را دنبال کنید:

در مورد اطلاعات مورد استفاده سازمان باید به دقت فکر کرد و یک لیست از تمام اطلاعات مورد استفاده در سازمان تهیه کرد. (اطلاعات برای سازمان مفید باشد). در لیست نوشته شده در مورد بالا، ۵ اولویت اول انواع اطلاعات مورد استفاده در سازمان را مشخص کند.

بخشی را که در آن هر یک از این انواع اطلاعات ذخیره می شوند را مشخص کنید.

در نهایت یک جدول کامل برای انواع اطلاعات سازمان به صورت اولویت بندی شده ایجاد می شود.

اولویت نوع داده کدام بخش ذخیره می شود

اولویت	نوع داده	کدام بخش ذخیره می شود
۱		
۲		

بعد از کامل شدن فهرست، مطمئن شوید که اطلاعات بر اساس اهمیت اولویت بندی شده اند. سه ستون به این صفحه اضافه می شود که نشان دهنده نوعی از حفاظت است که اطلاعات به آن نیاز دارد.

برخی از اطلاعات نیاز به حفاظت از لحاظ محرمانه بودن، برخی از لحاظ جامعیت و برخی نیاز به حفاظت از لحاظ دسترسی دارند. برخی هم هر سه نوع را نیاز دارند. برای مشخص کردن میزان حفاظت مورد نیاز مراحل زیر را انجام دهید:

در مورد اطلاعات سازمان فکر کنید.

۵ نوع داده که بالاترین اولویت در سازمان را دارند در جدول وارد کنید.

سطح حفاظت که برای هر نوع داده لازم است در ستون چپ وارد کنید.

جدول را برای کلیه انواع داده تکمیل کنید.

اولویت	نوع داده	محرمانه بودن	جامعیت	دسترسی
۱				
۲				

باید از بالاترین اولویت اطلاعات شروع کرد. در صورت بروز رخداد امنیتی که منجر به بروز حادثه و از دست دادن داده ها شود باید روش هایی برای گزارش دادن رخداد به کارمندان و یا مشتریان داشته باشید. اکثر کشورها قوانینی دارند که طبق آن اطلاع رسانی به مشتریان خود را دارند.

۳-۲- هزینه های اجتناب از رسیدگی به امنیت اطلاعات

داشتن روش در زمانی که مشکلی برای اطلاعات رخ دهد مهم است. هر اتفاق بدی ممکن است باعث از بین رفتن محرمانگی اطلاعات شود یک ویروس یا برنامه مخرب که وارد سیستم شده و یک کپی از اطلاعات حساس سازمان را می دزدد.

۳-۳- سیاست های سازمان در زمینه امنیت اطلاعات و موضوعات مرتبط

هر سازمانی نیاز به نوشتن و داشتن سیاست هایی برای شناسایی شیوه های قابل قبول و انتظارات سازمان در انجام کارها دارد. سیاست هایی که مدیریت سازمان برای اطلاعات، کامپیوتر، شبکه و امنیت در فضای تبادل اطلاعات دارند باید به وضوح برای کارکنان مشخص گردد. این سیاست ها که کدام اطلاعات و چه منابعی برای مدیریت مهم است و انتظارات مدیریت سازمان از کارکنانی که از این منابع استفاده می کنند باید به روشنی مشخص شود و انتظارات مدیریت از همه کارکنان برای حفاظت و استفاده از این اطلاعات توضیح داده شود. سیاست ها برای هر یک از کارمندان روشن باشد و بدانند در صورت نقض این سیاست ها چه مجازات هایی برای آنها در نظر گرفته می شود.

ادامه دارد...

تهیه و خلاصه کتاب: لیدا رسول اهری – کارشناس آموزش و پژوهش اداره کل پدافند غیرعامل استانداری

نگاهی اجمالی بر شهرسازی مبتنی بر پدافند غیرعامل

کمال ترابی کارشناس ارشد شهرسازی شهرداری کلانشهر تبریز
اسد ذالی کارشناس امورهویتی اداره ثبت و احوال شهرستان کلیبر

چکیده

پدافند غیرعامل، حرکتی عکس العملی و واکنشی است. در مواقع غافل گیری، دفاع غیرعامل به طور ذاتی باید جوابگو باشد. با پیشرفت روزافزون دانش بشری و استفاده از سلاح‌های پیشرفته برای تصرف و ضربه زدن به کشور حمله شده، استفاده از راهکارهای غیرنظامی در شهرسازی تاثیر زیادی در مقاومت کشور خواهد داشت. به کارگیری اقدامات پدافند غیرعامل، باعث ایجاد اهداف مستحکمی می‌گردد که انهدام آن‌ها، برای دشمن مشکل‌تر و پرهزینه‌تر خواهد بود. این امر در بدترین شرایط، هزینه جنگ دشمن رابالا برده و به عنوان یک اهرم بازدازنده قوی عمل خواهد کرد. کاربری زمین، ساخت و بافت شهر، فضای باز شهرها، ساخت پناهگاه، پراکندگی تاسیسات و ساختمانهای مهم، وجود و استوار نمودن تأسیسات باارزش در مواقع اضطراری در کاهش و یا افزایش آسیب‌ها و خسارت‌های ناشی از جنگ تاثیر بسزایی دارند. با مطالعه درست آن‌ها آسیب ناشی از جنگ در یک شهر را تا حدودی کاهش داده و امکان برنامه ریزی درست را فراهم می‌آورد.
واژه‌های کلیدی: :پدافند غیرعامل، شهرسازی

۱- مقدمه

انجام اقدامات دفاع غیرعامل در جنگ‌های امروزی در جهت مقابله با تهاجمات خصمانه و تقلیل خسات ناشی از حملات هوایی، زمینی و دریایی کشور مهاجم، در مجموعه شهری و کلانشهرها موضوعی بنیادی است که وسعت و گستره آن تمامی زیرساخت و مراکز حیاتی و حساس، مبادی ارتباطی و مواصلاتی، فرودگاه‌ها و زیرساخت‌های کلیدی نظیر پالایشگاه‌ها، نیروگاه‌ها، مجتمع‌های بزرگ صنعتی، مراکز هدایت و فرماندهی و جمعیت مردمی را در برمی گیرد تا حدی که حفظ امنیت ملی و اقتصادی، به نحو چشمگیری وابسته به برنامه ریزی و سامان دهی همه جانبه در موضوع حیاتی دفاع غیرعامل به خصوص در شهرهای بزرگ کشور می‌باشد (صراف جوشقانی، ۱۳۸۶: ۱۲).

شهر دارای کالبدی است که این کالبد فعالیت‌های متعددی را در خود جای داده است. مجموع این فعالیت‌ها فضاهای شهری را می‌سازد و به آن هویت می‌بخشد. همه مقوله‌های فوق، جمعیت وابسته‌ای را به دنبال خود دارند که در صورت وقوع جنگ به شدت از آنهاتأثیر می‌پذیرند. شناسایی خطر آسیب‌های احتمالی نقش مهمی در پیش گیری و آمادگی برای مواجهه و مقابله با کم و کیف آثار منفی حملات نظامی به مناطق شهری دارد. اگر شناخت ابعاد خطر حملات نظامی به مناطق شهری و آسیب‌های محتمل در نتیجه آن به درستی حاصل شود، می‌توان سطح و نوع اقدامهای مقابله با این آسیب‌ها را نیز تا مقیاس تک تک افراد به طور گسترده تعریف نموده و توسعه بخشید. بدین منظور بایستی شناختی از عوامل مؤثر در حمله به شهرها حاصل گردد. در نتیجه‌ی مطالعات انجام شده از جمله عوامل مؤثر در حمله به شهرها تمرکز نیروهای انسانی، مراکز سیاسی، اداری و نظامی می‌باشد. همچنین انباشت سرمایه‌های کلان مادی و غیرمادی کشورها در مراکز شهری، انگیزه بالایی در جهت تخریب و یا دست یابی به آنهابرای دشمن فراهم می‌کند. علاوه بر آن شهرها به عنوان حلقه ارتباطی و کانون انسجام منطقه‌ای و پسگرانه های روستایی خود هستند که با مقاومت یا سقوط آن‌ها، سرنوشت منطقه نیز مشخص می‌گردد. بدین ترتیب شهرها اغلب هدف اصلی در درگیری‌های بوده و پیوسته باید فشارهای ناشی از جنگ را تحمل نمایند. از سوی دیگر، اهدافی نیز درون شهرها وجود دارد که حملات دشمن به شهر را توجیه می‌سازد. از آن جمله می‌توان به وجود پادگان‌های نظامی در شهرها، صنایع، نیروگاه‌ها، پالایشگاه‌ها و پست‌های فشار قوی، تصفیه خانه‌ها، مخازن ذخیره سوخت و آب، فرودگاه‌ها، پایانه‌ها، راه آهن، بنادر، جاده‌ها، پل‌ها

و شبکه مخابراتی اشاره کرد. از این رو نوعی سیاست تمرکززدایی برای آن دسته از تأسیسات شهری که حضور آن‌ها در بدنه‌های شهری ضرورتی ندارد، می‌تواند ایمنی نسبی شهرها را افزایش و ضریب آسیب پذیری آن‌ها را کاهش دهد (ناطقی الهی، ۱۳۸۰).

۲- شاخص های شهرسازی مرتبط با پدافند غیرعامل

مؤلفه‌های شـهری شامل بافت مناطق شهری، ساختار شهر به طور جزء و ساختار هر منطقه به طور کل، فرم شهر، موقعیت مکانی کاربری اراضـی شـهری، شبکه حمل و نقل شهری و تأسیسات زیربنایی موجود در شهرها می‌باشد. در ادامه مختصری به هر یک از این مؤلفه‌ها و ویژگی‌های آن‌ها در هنگام رویارویی با بحران نظامی و جنگ پرداخته می‌شود.

۲-۱- ساختار منطقه و شهر

ساختار فضایی شهر در تأثیر متقابل با منطقه‌ای که شهر به لحاظ اقتصادی، اجتماعی، سیاسی و ... با آن کار می‌کند، شکل می‌گیرد. در واقع شـهر در شـبکه یا سـلسله مراتبی از روابط کالبدی، عملکردی با محیط پیرامونی قرار گرفته است. اساسی‌ترین و کلی‌ترین طرحی که جهت دفاع از شـهر در برابر هر نوع تهدیدی مطرح است، طرح آمایش سرزمین است چرا که اساسی‌ترین مؤلفه‌های این طرح رابطه مابین انسـان، فضا و فعالیت‌های آن است که به تثبیت و پایداری توسعه هم می انجامد در واقع علاوه بر محتوای نظامی و سیاسی دفاع در مقیاس شـهری، ملی و منطقه‌ای، دفاع از موجودیت‌های تثبیت یافته فضـا نیز مورد نظر اسـت. رویکرد آمایشـی به ساماندهی بحث دفاعی در پهنه منطقه‌ای و ملی باعث می‌شـود که شهر به گونه‌ای در فضا استقرار یابد که حداکثر امنیت و قابلیت دفاعی را داشته باشد (قرارگاه پدافند هوایی خاتم الانبیا، ۱۳۸۴).

توزیع فضـای عناصر، ترکیب عناصر و عملکردهای اصلی شهر که تشکیل دهنده ساختار شهر هستند، نقش مهمی در میزان آسیب پذیری شـهر در برابر حوادث مختلف دارند. تقسیمات کالبدی شهر، مانند کوی، محله، ناحیه، برزن و منطقه، تک مرکزی یا چند مرکزی بودن و... نیز وجوه دیگری از سـاختار شـهر محسـوب می‌شـوند که هر یک به لحاظ مقابله در برابر حوادث دارای اسـتعداد خاص خود است. مثلاً در سـاختار تک مرکزی شـهر و تمرکز امکانات اقتصـادی و انسانی در یک قسمت از شهر نسبت به شهرهای دارای چند مرکز، امکان آسیب پذیری بیشتر می‌شود (عبدالهی،۱۳۸۰، ۷۶-۷۵).

۲- ۲- بافت شهر

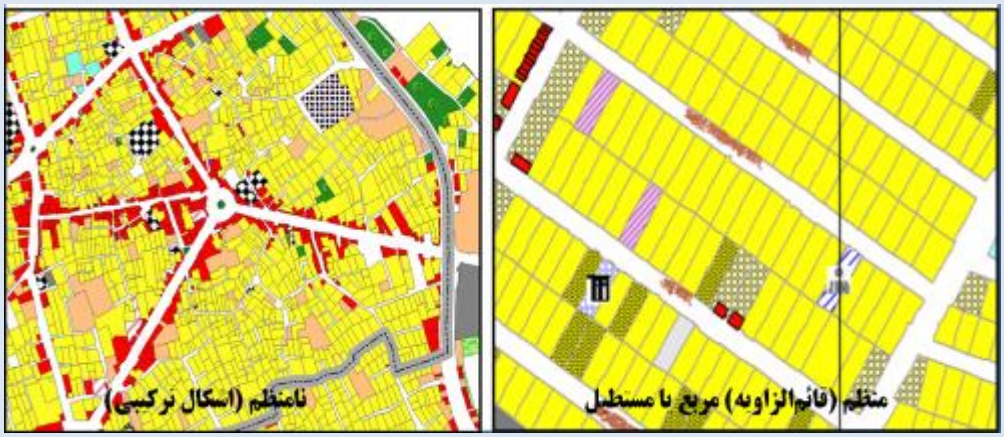
واکنش هر نوع بافت شهری در هنگام وقوع زلزله و جنگ در قابلیت‌های گریز و پناه گیری ساکنان، در امکانات کمک رسانی، در چگونگی پاکسـازی و بازسـازی و حتی اسـکان موقت، دخالت مستقیم دارد. الگوی ترکیب فضاهای باز و بسته و نسبت سطح ساخته شده به فضای باز، مهم‌ترین ملاک کارآیی و سـنجش خواهد بود. در یک بافت شـهری غیر از سـلول‌هایی که همان قطعات اراضـی و سـاخت و سـازها هسـتند. شبکه‌ی راه‌های فرعی الگوی راه و مشخصات فیزیکی آن شامل طول و عرض مطرح است. چگونگی ترکیب و انتظام قطعات، در تشـکیل انواع بافت و مشـخصـات آسـیب پذیری آن مطرح می‌گردد. غیر از الگوی ترکیب قطعات در یک بافت شهری، الگوی همجواری ساخت و سازها و فضاهای باز قطعات مجاور نیز از شاخص‌های دیگر در ارزیابی آسیب پذیری و قابلیت بافت، ترکیب راه‌ها و قطعات زمین و سـاخت و سـازها اسـت. با این مشخصه، نحوه مجاورت قطعات تفکیکی با گذر، همجواری فضای باز و ساخته شده‌ی هر قطعه با گذر و نیز درجه‌ی محصـوریت معابر مورد بررسـی قرار می‌گیرد. از دیگر شـاخص‌های بخشـی، قابلیت بافت، الگو و اندازه‌ی بلوک‌های شهری و الگوی ترکیب راه‌ها و بلوک‌های شـهری اسـت. این شـاخص به همراه سـطح قطعه بندی‌ها و راه‌های فرعی درون بلوک‌های شهری، در میزان فشـردگی یا نظم سـاخت و سـازهای درون آن موثر بوده و به همین لحاظ در میزان آسیب پذیری بافت تاثیر دارند. الگوی فضاهای

باز در کل سطح بافت بخش‌های مسکونی، عامل دیگری در افزایش کارآیی بافت، هنگام سوانح طبیعی است. موقعیت و سطح قرارگیری فضاهای باز و همجواری با ساختارها یا عوارض طبیعی با توجه به وسعت آن می‌تواند موجب آسیب پذیری فضاهای باز شود (حمیدی،۱۳۷۱، ۲۱۹-۲۱۱).

با افزایش نسبت ساخته شده‌ی به کل سطح زمین و یا به فضای باز، آسیب پذیری فضای باز ناشی از ریزش آوار ساختمان‌ها و غیر قابل استفاده شدن بافت افزایش می‌یابد. میزان افت کارآیی فضای باز با ارتفاع ساختمان‌ها نیز ارتباط مستقیم دارند. در جدول ۱ ارزیابی قطعه‌بندی مختلف هنگام و بعد از وقوع بحران نشان داده شده است.

جدول ۱- ارزیابی قطعه‌بندی مختلف هنگام و بعد از وقوع بحران(حمیدی،۱۳۷۱: ۲۲۲)

الگوی قطعه بندی	وضعیت از نظر آسیب پذیری
منظم، مربع یا مستطیل	احتمال نظم بیشتر در فرم ساختمان‌ها و آسیب پذیری کمتر به دلیل باقی ماندن فضای باز مفید و کارایی بیشتر در پناه گرفتن و اسکان موقت
مربع چند ضلعی (زوایای منفرجه و حاده)	تاثیر در بی نظمی فرم ساختمان و احتمال آسیب پذیری بیشتر، خرد شدن فضای باز و غیر قابل استفاده بودن برای گریز، پناه، امداد و اسکان
نا منظم (اشکال نا ترکیبی)	موثر در بی نظمی ساختمان‌ها و افزایش ضریب آسیب پذیری، بی نظمی و خرد شدن فضای باز قطعه و لذا کارایی در پناه گرفتن، امدادرسانی در اسکان موقت



شکل ۱- دو نوع بافت متفاوت شهری از منظر نظام تفکیک قطعات ساختمانی(حبیبی ،۱۳۸۸: ٦٠)

به طور کلی بافت پیوسته و منظم در اراضی هموار که راه‌های آن نیز از درجه‌ی محصوریت متوسط یا کم برخوردارند و به ویژه نسبت سطح ساخته شده به فضای باز آن‌ها متوسط یا کم است و دارای بلوک‌هایی با یک یا دو ردیف منظم ساختمان هستند، آسیب پذیری کمتر و کارآیی بیشتر بعد از وقوع سانحه هستند. نظم شبکه‌ی راه‌ها و طول کم و شطرنجی بودن کوچه‌های فرعی به دلیل تعداد دسترسی، از فلج شدن بافت جلوگیری می‌کند." (حمیدی،۱۳۷۱، ۲۲-۲۲۱). رابطه‌ی درجه‌ی آسیب پذیری و انواع بافت‌های شهری در جدول ۲ مشخص است.

جدول ۲- رابطه‌ی درجه‌ی آسیب پذیری و انواع بافت‌های شهری (حمیدی،۱۳۷۱: ۲۲۲)

نوع بافت	درجه‌ی آسیب پذیری
پیوسته و منظم	کم
ناپیوسته ونا منظم	متوسط
پیوسته و نامنظم	زیاد

۲-۳- فرم شهر

هر شهری ممکن است با هدفی طراحی شود. اما هیچ شهری با این هدف ساخته نشده که خطرهای ناشی از بحران‌ها را به حداقل برساند و این سوال مطرح می‌شود که آیا می‌توان کالبد شهر را به صورتی تغییر داد که از صدمات موشکباران جلوگیری کرده و یا آن را به حداقل برساند؟ آیا خصوصیات ذاتی برای فرم شهر وجود دارد که انعطاف پذیری آن را افزایش دهد. سینگر (۱۹۵۲) و لینچ (۱۹۵۸) هر دو معتقدند که فرم‌های باز برای تغییرات انعطاف‌پذیری بیشتری نسبت به فضاهای متراکم دارند. علاوه بر انعطاف‌پذیری، امکانات زیاد نیز خصیصه‌ی دیگری است که می‌تواند فرمی را نسبت به دیگری برتری دهد(حبیب،۱۳۷۱، ۲۱).

۲-٤- کاربری اراضی شهری

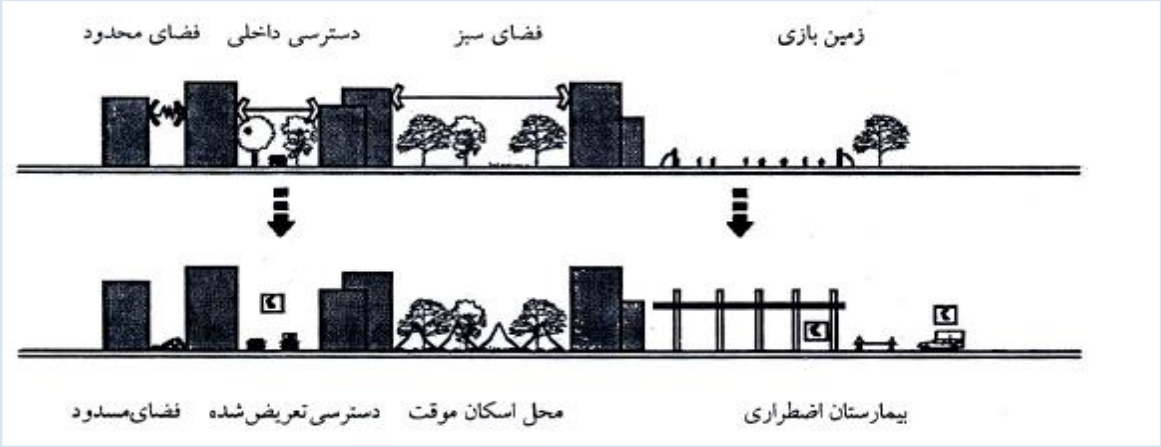
بعضی از کاربری‌ها در شهر وجود دارند که نقش بسیار حساسی در آسیب پذیری شهر دارند. این کاربری‌ها به «کاربری‌های ویژه» معروفند و شامل مدرسه‌ها، دانشگاه‌ها، بیمارستان‌ها مراکز امدادرسانی، مراکز مدیریت شهری، کارخانه، مخازن سوخت و ... می‌باشند. بدیهی است که آسیب دیدن مراکزی نظیر مدرسه‌ها و دانشگاه‌ها به علت انبوهی جمعیت آن‌ها، کارخانه‌ها و مخازن سوخت، به دلیل ایجاد خطر برای نواحی اطراف خود، بیمارستان‌ها و مراکز امدادرسانی و مدیریت شهری به دلیل عملکرد حساسی که به هنگام وقوع بحران دارا می‌باشند، از حساسیت فوق العاده ای برخوردارند و ضروری است در مکان یابی این گونه کاربری‌ها دقت فراوان صورت گیرد تا حداقل به این مراکز آسیبی وارد نشود(احمدی،۱۳۷۶: ۶۵ و ۶۶). به عنوان مثال با توزیع صحیح مراکز امدادی در سطح شهر، طراحی ساده کاربری‌های ویژه و مکان یابی آن‌ها در زمین‌های صاف بدون شیب و در ارتباط با شبکه معابر و عدم همجواری با مناطق آسیب پذیر می‌توان آسیب پذیری این کاربری‌ها در برابر بحران‌ها را تا حد ممکن کاهش داد و در نتیجه درجه ایمنی شهر را افزایش داد. مسکن نیز یکی از کاربری‌های مهم در شهر می‌باشد که باید سعی شود هنگام وقوع بحران، این بخش دچار آسیب نشود. بدین منظور می‌بایست از طرح‌های ساده برای ساخت مسکن استفاده نمود و همجواری ها را رعایت کرد، خصوصا مسکن باید از کاربری‌های خطر آفرین نظیر کارگاه‌های صنعتی به دور باشد. استفاده از مصالح ساختمانی سبک و برقراری امکان تخلیه سریع مناطق مسکونی در کاهش آسیب پذیری این مناطق بسیار موثر است. در واقع کاربری‌های مسکونی شهرها، آزمایشگاهی است که شرایط تمام عیار آزمایش را دارد و در فرآیند تنش‌های شدید زمینی و آسیب پذیری محیط مصنوع شهری به دو شکل «تلفات» و «تخریب» تاثیر می‌پذیرد. این در حالی است که سایر کاربری‌های موجود نظیر آموزشی، بهداشتی، مذهبی و ... از آثار دوگانه زلزله صرفا بخش تخریب را منعکس می‌سازند(احمدی،۱۳۷۶: ۷).

۲-۵- فضاهای باز

عوامل بسیاری در آسیب پذیری و کارآیی فضای باز شهری در زمان بحران موثر می‌باشد. در زیر به تعدادی از این عوامل اشاره شده است:

- هر چه سطوح فضای باز در شهر وسیع‌تر باشد، آسیب پذیری کمتر است.
- توزیع مناسب فضای باز شهری به منظور تامین سطوح پناه‌گیری و اسکان قبل و بعد از وقوع بحران در سطح شهر باعث کاهش آسیب پذیری شهر می‌شود.
- هر چه وسعت فضای باز بیشتر باشد، آسیب پذیری و کارآیی آن بیشتر می‌شود.
- هر چه دسترسی‌های فضای باز بیشتر و مناسب‌تر باشد، کارآیی آن افزایش و آسیب پذیری شهر کاهش می‌یابد.
- هر چه محصوریت و ارتفاع ابنیه مجاور و فضای باز شهری بیشتر باشد، خطر آسیب پذیری و آسیب رسانی افزایش می‌یابد.
- هر چه سازگاری کاربری‌های اطراف فضای باز با آن بیشتر باشد، آسیب پذیری کمتر است.
- وجود عملکردهای خطرزا در اطراف فضای باز شهری سبب افزایش آسیب پذیری می‌شود.

- هر چه فرم فضای شهری هندسی‌تر و منظم‌تر باشد، قابلیت استفاده از آن در زمان بحران افزایش می‌یابد.
- مکانیابی مناسب فضای باز شهری با توجه به ویژگی‌های بستر طبیعی سبب کاهش آسیب پذیری می‌شود.. (مرکزمطالعات مقابله با سوانح طبیعی ایران،۱۱،۱۳۷۳)
- در فضای باز لبه‌هایی به عنوان جان پناه می‌توان ایجاد کرد. به عنوان مثال در فاصله بین فضای باز و ساختمان‌ها، با استفاده از گلدان‌های طولی یک لبه مستحکم می‌توان ایجاد نمود که در مواقع اضطراری به عنوان جان پناه نیز قابل استفاده باشد(مرکز تحقیقات ساختمان و مسکن، ۱۳۸۸: ۱۸). اجزای فضاهای باز می‌تواند براساس اصل انعطاف پذیری و با عملکردهای چند منظوره طراحی شود تا در شرایط معمول امکان غنا بخشیدن به فعالیت‌های عادی را فراهم نموده و در شرایط اضطراری حفاظهای قابل قبول ایجاد نمایند(مرکز تحقیقات ساختمان و مسکن، ۱۳۸۸: ۱۹).
- تا حد امکان لبه‌های تیز و گوشه دار از فرم کلیه عناصر حذف شده و از فرم‌های نرم و گرد گوشه استفاده شود. بدین منظور زاویه لبه‌ها (توده ساختمان، جوی آب، آبنما، سکو، گلدان، حفاظ میله‌ای یا عناصر و تجهیزات نوک تیز) تا حدود ارتفاع سه متر از کف محل استقرار، راست گوشه نباشد.
- در فضاهای باز و محوطه تا حد امکان نباید از عناصر و مبلمان صلب و نرده‌ها و حفاظهای میله‌ای استفاده شود. این امر به ویژه در محل‌های تجمع و بازی و دیگر سطوح نسبتا وسیع حائز اهمیت است(مرکز تحقیقات ساختمان و مسکن، ۱۳۸۸: ۱۹-۲۰). اصل انعطاف پذیری و طراحی چند منظوره در شکل ۲ نشان داده شده است.



شکل۲-اصل انعطاف پذیری و طراحی چند منظوره(مرکز تحقیقات ساختمان و مسکن، ۱۳۸۸: ۱۹)

سطوح فضاهای باز شهرها شامل پارک‌های جنگلی، پارک‌های بزرگ و متوسط و کوچک، میادین، فضاهای سبز موجود در شهر، محیط باز ساختمان‌ها، تاسیسات ورزشی و ... می‌باشند. با تداوم برخی سیاست‌ها و اقدامات کلان اقتصادی نظیر تمرکز منابع و امکانات در شهرها (به ویژه تهران) و به تبع آن افزایش جمعیت شهرهای بزرگ و نیز ورود حساب نشده ی خودرو به سطح شهرها و ایجاد تقاضا در جهت تولید ساختمان‌های مسکونی و خدماتی بیشتر، روند ساخت و سازها و توسعه فضاهای ساخته شده باعث کاهش فضاهای باز و مفید شهری که می‌توانند در زمان تهدیدات عملکردهای گوناگونی از جمله تخلیه یا اسکان جمعیت، فرود بالگرد و غیره داشته باشند، می‌گردد. به عبارتی افزایش گسترش کالبدی شهرها منجر به کاهش شدید فضای باز شهرها طی دو دهه گذشته گردیده است (عشق آبادی، ۱۳۹۰).

۳- روش‌های استفاده از پدافند غیر عامل در شهر

از مهم‌ترین اقدامات استفاده از روش‌های پدافند غیرعامل در شهر در قالب الگوهای ذیل می‌گنجد.

۳-۱- پراکندگی تأسیسات و ساختمان‌ها

۳-۲- استوار نمودن تأسیسات باارزش

۳-۳- ساختن پناهگاه

٤- راهبردهای دفاع غیر عامل در شهرسازی

موارد زیر را می‌توان به عنوان راهبردهای پدافند غیر عامل در موضوع شهر و شهرسازی برشمرد:

- بهسازی و ایمن سازی وضع موجود ساختمان‌های عمومی و مسکونی مردم
- پیش بینی ذخیره سازی نیازهای ضروری و اضطراری (مانند سوخت، آب و...) در داخل محدوده شهر
- تامین فضاهای امن مورد نیاز بخشی از شهروندان با استفاده از عملکردهای دومنظوره خدمات شهری
- آماده سازی زیرساخت‌های لازم جهت اسکان موقت بخشی از شهروندان در فضاهای باز شهری و پیرامونی
- جلوگیری از ایجاد و یا گسترش مراکز حیاتی و حساس جدید در داخل شهرهای بزرگ
- ایجاد حریم امنیتی مراکز حیاتی و حساس واقع در شهر
- دو منظوره شدن فضاهای عمومی با قابلیت بهره برداری در شرایط بحران
- ضرورت تدوین ضوابط فنی وملاحظات دفاع غیر عامل در حوزه شهرسازی، ساختمان و زیرساخت‌های شهری
- ایجاد و ساماندهی شبکه معابر با ویژگی تخلیه و امداد رسانی سریع به مردم
- اعمال اصول و مبانی پدافند غیرعامل در طرح‌های جامع و تفضیلی شهر
- مکان یابی و پیش بینی فضاهای امن مدیریت بحران(مهندسین مشاور یادگار طرح، ۱۳۹۱).

٥- نتیجه گیری

توزیع فضـای عناصر، ترکیب عناصر و عملکردهای اصلی شهر که تشکیل دهنده ساختار شهر هستند، نقش مهمی در میزان آسیب پذیری شـهر در برابر حوادث مختلف دارند. تقسیمات کالبدی شهر، مانند کوی، محله، ناحیه، برزن و منطقه، تک مرکزی یا چند مرکزی بودن و... نیز وجوه دیگری از ساختار شهر محسوب می‌شوند. در ارزیابی و قطعه بندی اراضی، شکل هندسی قطعه (منظم یا نامنظم)، مساحت قطعه و ابعاد و اندازه‌ی قطعه، تناسـبات طول و عرض قطعه در رابطه با کاربری زمین و نوع مالکیت (اختصـاصـی یا مشـاع) ملاک سنجش قرار می‌گیرد. مشخصات ساخت و ساز درون هر قطعه زمین، شاخص دیگر در ارزیابی قطعه بندی طراحی بافت خواهد بود.

هرگاه در تعیین کاربری زمین‌های شـهری، همجواریهای ناسـازگار در کنار یکدیگر قرار داده نشـوند، اماکن تخلیه سـریع فراهم گردد. اگر کاربری‌ها در شـهرها به گونه‌ای توزیع شوند که سبب عدم تمرکز گردند، می‌توان انتظار داشت آسیب پذیری شهرها در برابر به حرام تا حد زیادی کاهش یابد. کمیت و کیفیت فضـاهای باز شهر در سطح شهر و نحوه توزیع آن‌ها نقش مهمی در آسیب پذیری شهر دارد. فضاهای باز شـهری می‌تواند به عنوان فضـاهایی امن جهت گریز، پناه‌گیری، امدادرسانی، اسکان موقت و جمع آوری کمک‌ها درزمان بحران باشد. پراکنده تاسـیسـات و بناهای حیاتی در شـهرها باعث می شود در صورت هدف قرار گرفتن آنها، شهرها بتوانند پاسخگوی نیازهای حداقلی ساکنین خود باشند. همچنین این امر باعث افزایش هزینه جنگ شده و عامل بازدارندگی مهمی در جلوگیری از جنگ خواهد بود. همچنین توجه به نحوه سـاخت پناهگاهها در بناهای شهر و ساختن پناهگاههای چندمنظوره می تواند ساکنین شهرها را برابر حوادث ناشی از جنگ بیمه کند.

منابع و مآخذ

۱- احمدی، حسن(۱۳۷۶)، نقش شهرسازی در کاهش آسیب پذیری شهر، مسکن و انقلاب، تهران
۲- حبیب، فرح(۱۳۷۱)، نقش فرم شهر در به حداقل رساندن خطرات ناشی از زلزله، مجموعه مقالات اولین کنفرانس بین المللی بلایای طبیعی در مناطق شهری، دفتر مطالعات و برنامه ریزی شهر تهران، تهران
۳- حبیبی، کیومرث (۱۳۸۸)، امنیت شهری و GIS، انتشارات دانشگاه امام حسین، تهران
۴- حمیدی، ملیحه(۱۳۷۱)، ارزیابی الگوهای قطعه بندی اراضی و بافت شهری در آسیب پذیری مسکن، مجموعه مقالات سمینارسیاستهای توسعه مسکن در ایران، تهران.
۵- داعی نژاد، فرامرز(۱۳۸۵) اصول و رهنمودهای طراحی و تجهیز فضای باز مجموعه‌های مسکونی به منظور پدافند غیرعامل، مرکز تحقیقات ساختمان و مسکن، تهران
۶- صراف جوشقانی، حسن، (۱۳۸۶)، تعیین و اولوین گذاری اقدامات در دفاع غیرعامل کشور، اولین کنفرانس هسته رزم زمینی، دانشگاه مالک اشتر
۷- عبدالهی، مجید(۱۳۸۰)، مدیریت بحران در نواحی شهری، انتشارات انوار، تهران
۸- عشق آبادی، فرشید(۱۳۹۰)، تحلیل نظام برنامه ریزی شهری از منظر پدافندغیرعامل، اولین همایش علمی- پژوهشی شهرسازی و معماری با رویکرد پدافند غیرعامل، دانشگاه صنعتی مالک اشتر
۹- قرارگاه پدافند هوایی خاتم الانبیاء(۱۳۸۴)معماری و طراحی شهری در ایران؛ نشریه شماره ۴
۱۰- مرکز تحقیقات ساختمان و مسکن (۱۳۸۸)، پیش نویس مبحث بیست و یکم مقررات ملی ساختمان (پدافند غیرعامل)، مرکز تحقیقات ساختمان و مسکن، تهران
۱۱- مرکز مقابله با سوانح طبیعی ایران(۱۳۷۳)، کاربرد مدیریت بحران درکاهش ضایعات ناشی از زلزله، بنیاد مسکن انقلاب اسلامی، تهران
۱۲- ملکی سعید و احمدی، رضا (۱۳۹۰)، جایگاه پدافند غیر عامل در شهرهای ایران باستان، اولین همایش علمی- پژوهشی شهرسازی و معماری با رویکرد پدافند غیرعامل، دانشگاه صنعتی مالک اشتر
۱۳- مهندسین مشاور یادگار طرح (۱۳۹۱)، طرح جامع - تفصیلی شهر میامی- اداره کل راه و شهرسازی استان سمنان
۱۴-ناطقی الهی، فریبرز (۱۳۸۰)، سناریوهای آسیب پذیری لرزهای شهرها و استفاده از آن در ایمن سازی کشور، نشریه آبادگران؛ شماره ۲۰۱.

بیت کوین؛ طلای دیجیتال یا حباب روی آب؟

محسن محمودی[۱] – نوید غلامزاده[۲]

۱. کارشناس ارشد پیشگیری از جرایم- دانشگاه علوم انتظامی امین (رئیس پلیس فتای استان آذربایجان شرقی)
۲. کارشناس ارشد مهندسی تجارت الکترونیک، دانشگاه آزاد اسلامی واحد قزوین، دانشکده مهندسی برق و کامپیوتر

چکیده

در سال های اخیر پول و سکه های مجازی زیادی از جمله لایت کوین ،داج کوین ،پی پل و ... به وجود آمده اند که سر آمد آنها بیت کوین می باشد. بیت کوین امروزه در ادبیات اغلب مقالات مدیریتی و اقتصادی دیده شده واهمیت روز افزونش به خوبی نمایان است.در این تحقیق در مرحله اول در مورد هستی بیت کوین صحبت می کنیم و در مرحله دوم امنیت بیت کوین را از زوایای مختلف بررسی کرده ودر مرحله سوم اصلاحات مهم بیت کوین را معرفی می کنیم. سپس مزایا و معایب بیت کوین را بررسی کرده و در مرحله چهارم وضعیت بیت کوین

در ایران را بررسی کرده و در انتها در مورد آینده بیت کوین مطالبی را گوش زد خواهیم کرد.

کلمات کلیدی : بیت کوین–امنیت بیت کوین– کیف پول مجازی– تراکنش بیت کوین– امضای دیجیتال

مقدمه

در سال های اخیر پول های الکترونیک و مجازی نظر همگان را به خود جلب کرده است.امروزه افراد و سازمانهای دولتی و خصوصی زیادی در سراسر دنیا تبادلات مالی خود را از طریق پول های الکترونیک انجام می دهند.در این مقاله ما سعی کرده ایم یکی از سرشناس ترین این پول ها را بررسی کنیم.بیت کوین پول مجازی است که در این سال ها طرفداران بی شماری را به سمت خود جلب کرده است.هر پولی که امروزه تبادل می شود دارای مزایا و معایبی است.در اینجا هدف آشنایی با بیت کوین وچند اصطلاح مهم، بررسی امنیت خود بیت کوین و تراکنش های آن می باشد.امیدواریم با شناخت دقیق این پول الکترونیک، استفاده مناسب از آن را بدست آوریم.

✓ بیت کوین و دیدگاه تئوری به عنوان پول

پاسخ به این سوال که آیا بیت کوین پول است یا نه به این صورت است که با بیت کوین به مانند پول می توان ارزش هر نوع کالا یا خدماتی را پرداخت کرد.با این دیدگاه به پول می توان بیت کوین را به عنوان پول در نظر گرفت.

✓ بیت کوین و دیدگاه تجربی به عنوان پول

تعریف بیت کوین از دیدگاه تجربی به عنوان پول ارتباط دارد با رابطه بین توسعه و پیشرفت مقداری(ارزشی) پول با دیگر متغیر های بزرگ اقتصادی.می دانیم که ارزش پول در طی زمان به دلایل اقتصادی و سیاسی دچار نوسان می شود.با در نظر گرفتن این مساله و اینکه ارزش بیت کوین نیز در طول زمان تغییر می کند،می توان از نظر تجربی هم بیت کوین را با پول یکی دانست.

✓ بیت کوین و دیدگاه قانونی به عنوان پول

در تعریف قانونی بیت کوین به عنوان پول مهم ترین مساله قوانین اختصاصی هر مملکت در تعریف پول می باشد.بعضی کشور ها بیت کوین را به عنوان پول تایید می کنند و بعضی کشور ها قبول نکرده و حتی یک تهدید جهانی برای جایگاه پول (دلار) می پندارند.در تعریف قانونی بعضی کشور ها پول الکترونیک این ویژگی ها را دارد:

۱- دارنده یا صاحب این پول باید مشخص باشد.

۲- پول الکترونیک باید در یک ابزار پرداخت الکترونیک ذخیره شود.مثلا درایو،پوشه،کیف اکترونیک و...

۳- ارزش وجوه دریافتی در مقابل خارج شده نباید از ارزش پول الکترونیکی خارج شده کمتر باشد.

٤- مورد پذیرش دیگران به عنوان یک وسیله پرداخت پولی باشد.

با توجه به اینکه دارنده بیت کوین مخفی است و می تواند در هر تراکنش جهت ناشناس ماندن ،آدرس خود را تغییر دهد،بیت کوین از لحاظ قانونی مورد تایید نیست.

✓ تعریف بیت کوین

بیت کوین یک ارز رمزی و مخفی نو ظهور است که باجنجال و در رمز و راز پیچیده شده است. هر بیت کوین یک کد طولانی از اعداد و حروف است که توسط عملیات ریاضی طولانی توسط کامپوتر های با قدرت پردازش بالا طی چندین روز به وجود آمده و در کامپیوتر یا کیف

پول مجازی ثبت و ذخیره می شود. پول مجازی و رمز نگاری شده که کاربران و تولید کنندگان آن،آن را به خوبی درک می کنند.بیت کوین یک نوآوری در شبکه پرداخت و یک نوع جدید از پول است. تنها تفاوت بیت کوین با پول در این است که بیت کوین هنوز به صورت جامع عمومی نشده است.بیت کوین بدون هیچ مرجع و یا بانک مرکزی کار کرده و تراکنش ها را مدیریت می کند.هیچکس مالک آن نیست و آن را کنترل نمی کند و همه می توانند در آن شراکت داشته باشند.بیت کوین مرزها را شکافته و یک ارز بین المللی است.یعنی برای انتقال به فردی در هر جای دنیا کافیست فقط یک کلیک انجام داده شود.

✓ بیت کوین چگونه تولید می شود؟

بیت کوینها در فرایندی رقابتی و تمرکز زدایی شده که "استخراج" نام دارد، تولید می شوند. استخراج بیت کوین به این صورت است که استخراج کننده باید آنقدر تلاش کند تا یک کدطولانی را که همان بیت کوین است را به دست بیاوردکه تا به امروز این کد تولید نشده است.این کار مستلزم صرف زمان بسیار طولانی است و برنامه تولید این کد توسط منطق ریاضی خیلی قوی ،پیچیده و امن کنترل می شود.برای ساخت یک بیت کوین شاید حدود یک ماه تا ۵۰ روز وقت نیاز باشد.و در این مدت سیستم پردازش گر باید شبانه روز کار کند.این فرایند مستلزم آن است که افراد از شبکه برای خدمات خود، جایزه دریافت کنند. استخراج کنندگان بیت کوین تراکنش ها را پردازش کرده و با استفاده از سخت افزار تخصصی، شبکه را ایمن کرده و در عوض آن بیت کوینهای جدید جمع آوری می نمایند. طراحی پروتکل بیت کوین به گونه ایست که بیت کوینهای جدید را با نرخ ثابتی تولید می کند. به این ترتیب استخراج بیت کوین یک کسب و کار رقابتی خواهد شد. اگر استخراج کنندگان بیشتری به شبکه بپیوندند، سودآوری مرتباً دشوار خواهد شد و استخراج کنندگان باید بدنبال بازده برای کاهش هزینه های استخراج باشند. هیچ مرجع مرکزی یا توسعه دهنده ای، اختیار آنرا ندارد تا سیستم را برای افزایش سود، کنترل یا دستکاری کند.هر نُد بیت کوین در جهان، هر آنچه را که در تطابق با قوانینی که انتظار میرود سیستم از آن پیروی کند، نباشد حذف خواهد کرد. بیت کوینها با نرخی کاهنده و قابل پیش بینی، تولید می شوند. تعداد بیت کوینهای جدیدی که هر سال تولید می شود، بطور اتوماتیک در طول زمان نصف می شود تا اینکه مجموع بیت کوینهای موجود به ۲۱ میلیون برسد. از این هنگام به بعد، دیگر بیت کوینی صادر نخواهد شد. در این نقطه، احتمالاً بطور اختصاصی به استخراج کنندگان بیت کوین مقدار کمی کارمزد تراکنش پرداخت خواهد شد.

✓ امنیت بیت کوین

با توجه به مجازی بودن شبکه بیت کوین،استفاده از کامپیوتر و البته اینترنت،امنیت بیت کوین هر لحظه شکننده است و هیچ گونه امنیتی ندارد.در سال های قبل مبلغ قابل توجهی از بیت کوین توسط هکر ها ربوده شده و شرکت های زیادی را به کام مرگ کشانده است.در نتیجه حفظ و ذخیره بیت کوین کاملا خطرناک است.تحقیقات نشان میدهد که بیت کوین از زمان اولین میزان ارزش تا به امروز نوسانات ارزشی رو به رشدی داشته و دارندگان بیت کوین تنها در چند برهه زمانی کوتاه ضرر کرده اند. ارزش اولین بیت کوین ها از یک دلار کمتر بوده که امروزه برای یک بیت کوین باید صد ها دلار پول پرداخت کرد.روند رو به رشد بیت کوین همگان را برای خرید و ذخیره وسوسه می کند اما بیت کوین شما که صد ها دلار و شاید هزاران دلار ارزش دارد،ممکن است در یک چشم به هم زدن توسط هکر ها نابود شود و هیچ مرجع قانونی هم هرگز مدافع شما نخواهد بود.حامیان بیت کوین که منتقد پول های دولتی هستند ،خطر ((چاپ پول))(تقلب) و در نتیجه از دست دادن ارزش پول خود را در نظر می گیرند. اما آیا در بیت کوین این امکان وجود ندارد؟

✓ امنیت بیت کوین جهت ذخیره ارزش

Jerons در کتاب معروف خود ((پول و مکانیسم تبادل پول)) در سال ۱۸۷۵ چهار نقش برای پول تعریف کرده است که شامل ۱.وسیله مبادله و دادوستد ۲.مقیاس عمومی از ارزش ۳.استاندارد ارزش و ۴.ذخیره ارزش می باشد.او اظهار داشت که پول باید قابلیت حمل،امنیت و قابل ذخیره شدن باشد. اما یا بیت کوین ویژگی سوم را دارد؟

در یک تحقیق که در حوزه پول و ذخیره بیت کوین انجام شده بود،محققین نوسانات ارزشی ۴ دارایی را بررسی کرده اند.این ۴ دارایی

شامل دلار،طلا،سیب و واحد پولی کشور جمهوری چک بود.مطابق تابع محاسبه نوسانات $S=\sqrt{\frac{1}{N-1}\sum(Xi-M)^2}$ که در این فرمول Sانحراف استاندارد،Nتعداد بازگشت های مداوم،Xi خود بازگشت مداوم و M تغییر قیمت می باشد، مشاهده شد که بیشترین تغییرات بین سال های ۲۰۱۱ تا ۲۰۱۳ مربوط به بیت کوین است.از ۲۰۱۳ تا ۲۰۱۴ نیز تغییرات زیادی در ارزش بیت کوین وجود داشته که با این نتایج و درک اینکه بیت کوین نوسانات ارزشی بالایی دارد،ذخیره آن کاری بسیار خطرناک می باشد.

✓ امنیت تراکنش های بیت کوینی

- ✓ برای انتقال بیت کوین به هر آدرس دلخواه،شما باید آدرس خود را وارد کنید و سپس مبلغ مورد نظر را وارد کرده و انجام تراکنش را تایید کنید.سپس باید منتظر باشید تا ۱۰ تایید از مرکز(بلاک چین) دریافت کنید.در طول این مدت اگر به هر دلیلی ارتباط شما قطع شود،بیت کوین شما از دست رفته است و احتمال برگشت بیت کوین وجود ندارد.همچنین اگر در طول مدت تایید ها اگر هکری شما را زیر نظر داشته باشد و بتواند به آدرس شما دسترسی پیدا کند بیت کوین های شما ربوده خواهد شد. با توجه به تنها دو مورد خیلی عمومی و سطح پایین ازضعف امنیت در بیت کوین ذخیره و استفاده از این پول و شبکه پرداخت آن توصیه نمی شود. مزیت های بیت کوین.

۱.بیت کوین متن باز است،طراحی آن عمومی است و هیچ کس مالک آن نسیت. این ویژگی می تواند کسانی که علاقه دارند از بیت کوین استفاده کنند امنیت خود پول را به خوبی درک کنند.

۲.بیت کوین یک شبکه پرداخت است.شما می توانید هر مبلغی را با استفاده از کیف پول دیجیتال به هر کسی در هر جای دنیا پول انتقال دهید بدون اینکه از خانه خارج شوید.

۳.کارمزد شبکه پرداخت بیت کوین خیلی کم است.در هر نقل و انتقال بیت کوین شما یک مبلغ به عنوان کارمزد پرداخت می کنید که در مقابل کارمزد بانک ها خیلی ناچیز است.

٤.بیت کوین اشتباهات چاپی را تشخیص می دهد.اگر به اشتباه به یک آدرس دیگر بیت کوین انتقال دهید در حال انتقال اشتباه در آدرس دهی را به شما می گوید.

۵.حفاظت از حریم خصوصی.بیت کوین با شفافیت بالا کار می کند و تمام تراکنش ها توسط گره ها بررسی شده و قابل پیگیری است.

٦.آزادی زمانی پرداخت.در هر لحظه از شبانه روز و در هر جایی از دنیا شما می توانید تذاکنش بیت کوین انجام دهید.

✓ معایب بیت کوین

۱.میزان پذیرش و عدم اعتماد مردم تا به امروز.

۲.ناپایداری ارزش بیت کوین.بیت کوین با اینکه طلای دیجیتال است اما مانند حبابی است که هر لحظه امکان دارد که بترکد.و کسی جرات ذخیره و سرمایه گذاری روی بیت کوین را ندارد.

۳.در حال توسعه بودن بیت کوین

۴.عدم امکان استفاده در تجارت های دولتی و خیلی سازمان ها و بخش های خصوصی در دنیا

۵.پول شویی

٦.استفاده موسسه ها و شرکت های زیر زمینی و متخلف برای انتقال پول و دادوستد

٧.عدم امکان پرداخت مالیات و فرار از مالیات

٨.نبود امنیت در حفظ بیت کوین در کیف پول دیجیتال و احتمال سرقت توسط هکر ها

٩.وسوسه شدن کاربران بیت کوین و وارد شدن آنها به فهرست های آنلاین ناشناس.

١٠. و ....

✓ بیت کوین در ایران

همانند دیگر کشور ها خرید و فروش و تبادل بیت کوین در ایران هم انجام می شود و شبکه ها و صرافی های آنلاین زیادی بیت کوین را پشتیبانی می کنند.از صرافی ها و سایت های آنلاین می توان موارد زیر را عنوان کرد:

١. http://exchanging.ir/

٢. https://farhadexchange.net/

٣. http://iranbitcash.com/

٤. http://irchange.org/

٥. http://www.coinava.com/

٦. http://elmodars.ir/exchanging

٧. و....

✓ نتیجه گیری و بحث آخر

اینکه بیت کوین در آینده می تواند به عنوان پول رایج خیلی کشور ها بشود قابل تامل است، اما با توجه به اینکه امروزه پول شویی و استفاده موسسه های متخلف از بیت کوین به اوج خود رسیده نشان می دهد که بیشتر از دولت مردان این افراد متخلف هستند که به بیت کوین روی آورده اند و از آن استفاده می کنند.با توجه به این مطالب اگر در آینده دولت ها بتوانند از پول شویی و تبادلات غیر مجاز و حمله هکر ها جلوگیری کنند، می توانند با وضع قوانین مناسب بیت کوین را نیز به واحد های پولی اضافه کنند.در غیر این صورت هرگز بیت کوین عمومی نخواهد شد.

منابع

1. A lightweight protocol to enforce trust preferences in mobile Person-to-Person payments- Available from: Ngoc Tran-Retrieved on: 19 April 2016

2. Analyzing the deployment of Bitcoin's P2P network under an AS-level perspective-Sebastian Feld∗, Mirco Sch¨onfeld, Martin Werner –Procedia Computer Science 32 (2014) 1121 – 112

3. An Architectural Assessment of Bitcoin Using the Systems Modeling Language - Nicholas Roth - Procedia Computer Science 44 (2015) 527 – 536

4. Virtual currency bitcoin in the scope of money definition and store of value –Max Kubát – Procedia Economics and Finance 30 (2015) 409 – 416

پاسخ ایران به حملات سایبری آمریکا

با افشای بخشی از عملیات سایبری آمریکا علیه ایران به نام «نیترو زئوس»، لزوم طراحی "سلاح سایبری" جهت بازدارندگی و پاسخ متوازن به حمله احتمالی آمریکا و تدوین «استراتژی امنیت ملی سایبری» توسط ایران اقدامی ضروری محسوب می‌شود .

به گزارش افکارنیوز،آمریکا دومین سلاح سایبری (cyberspace weapon) خود را به طور کامل عملیاتی کرد؛ نیروی هوایی فرماندهی فضایی آمریکا در یک بیانیه اعلام کرد: «یک سلاح جدید سایبری ساخت آمریکا به اسم ارزیاب/شکارچی فضای سایبر (Cyberspace Vulnerability Assessment/Hunter) به وضعیت عملیاتی کامل رسیده است.

Second US Cyberspace Weapon Becomes Fully Operational - Space Command

19:31 26.02.2016 1017 0 0
(updated 20:08 26.02.2016)

A new US cyberspace weapon system, the Cyberspace Vulnerability Assessment/Hunter (CVA/H), has reached the status of full operational capability (FOC), US Air Force Space Command said in a press release on Friday.

به گزارش اسپوتنیک این سلاح در امور پرواز، مبارزه و پیروز شدن در آسمان ، فضا و فضای مجازی کاربرد دارد؛ این در حالی است که اوایل ژانویه امسال، اولین سلاح فضای سایبری نیروی هوایی آمریکا به وضعیت عملیاتی کامل رسیده بود.

سایت روسی اسپوتنیک خبر عملیاتی شدن دومین سلاح سایبری آمریکا را اعلام کرد.

آمریکایی‌ها خیلی پیش‌تر نیز برای حمله به کشورها و سازمان‌هایی که مغایر منافع خود می‌نامد، از قوای سایبری استفاده کرده‌اند. ماه گذشته در جشنواره فیلم برلین مستندی به نام «روزهای صفر» (Zero Days) برای اولین بار به نمایش گذاشته شد که نشان می‌داد پروژه اصلی آمریکایی‌ها و رژیم صهیونیستی به نام «نیترو زئوس» (NITRO ZEUS) برای حمله به زیرساخت‌های ایران بوده که استاکس‌نت (Stuxnet) تنها بخش کوچکی از این عملیات گسترده بود.

بر اساس این فیلم مستند که منبع اطلاعات برای ساخت آن، گفتگو با مقامات نظامی و امنیت سایبری آگاه اعلام شده، در روزهای نخست دولت باراک اوباما، آمریکا برنامه‌ای برای حمله سایبری به ایران در صورتی که تلاش‌های دیپلماتیک برای محدود کردن برنامه هسته‌ای این کشور شکست بخورد و به درگیری نظامی منجر شود، طراحی کرد؛ هدف از این طرح که «نیترو زئوس» نام داشت، فلج کردن سامانه‌های دفاع هوایی، سامانه‌های حمل و نقل و بخش‌های مهمی از شبکه برق ایران بود. این مستند ادعا می‌کند که پس از به دست آمدن توافق هسته‌ای میان ایران و شش کشور دیگر در تابستان گذشته، دست کم تا آینده‌ای قابل پیش‌بینی، این طرح به تعویق افتاده است.

پروژه «نیترو زئوس» بزرگ‌ترین حمله سایبری آمریکا به یک کشور (ایران) در جهان بوده که رژیم صهیونیستی نیز به این عملیات کمک کرده است.

یکی از مقامات آمریکایی –در حالی که خواست نامش فاش نشود– در مصاحبه با «نیویورک تایمز» اعلام کرد: «این برنامه پیچیده‌ترین برنامه تاکنون بوده و قبل از توسعه این برنامه، آمریکا هرگز یک طرح حمله سایبری را در این حجم ایجاد نکرده بود.»

محتوای این این فیلم مستند با وجود عملیات روانی که علیه ایران دارد، اما در لایه‌های خود می‌تواند پیام هشداردهنده‌ای برای جمهوری اسلامی داشته باشد.

ارتش آمریکا برنامه‌هایی احتیاطی را برای هر نوع درگیری احتمالی، همچون حمله کره شمالی به جنوبی، جنگ افزارهای هسته‌ای مهار نشده در جنوب آسیا و شورش در آفریقا یا آمریکای لاتین، طراحی می‌کند. بخش زیادی از این برنامه‌ها نگهداری و هر چند سال یک بار به روز می‌شوند؛ روزنامه «نیویورک تایمز» در همین رابطه در یادداشتی به قلم "دیوید سنجر" در ۱۶ فوریه می‌نویسد: «در حالی که پنتاگون سرگرم چنین تمهیداتی است، مراکز اطلاعاتی آمریکا برنامه سایبری جداگانه و محدودتری را برای از کار انداختن مرکز غنی‌سازی هسته‌ای "فردو" طراحی کردند. ایران این مرکز را در زیر کوهی در نزدیکی قم ساخته است. این حمله عملیاتی سری بوده و رئیس جمهور (آمریکا) حتی در نبود مناقشه‌ای مداوم (مانند مسئله هسته‌ای) می‌تواند مجوز آن را صادر کند».

آمریکا با حمله سایبری به‌دنبال فلج کردن سامانه‌های دفاع هوایی، سامانه‌های حمل و نقل و بخش‌های مهمی از شبکه برق ایران است

همکاری رژیم صهیونیستی با آمریکا برای حمله سایبری به ایران

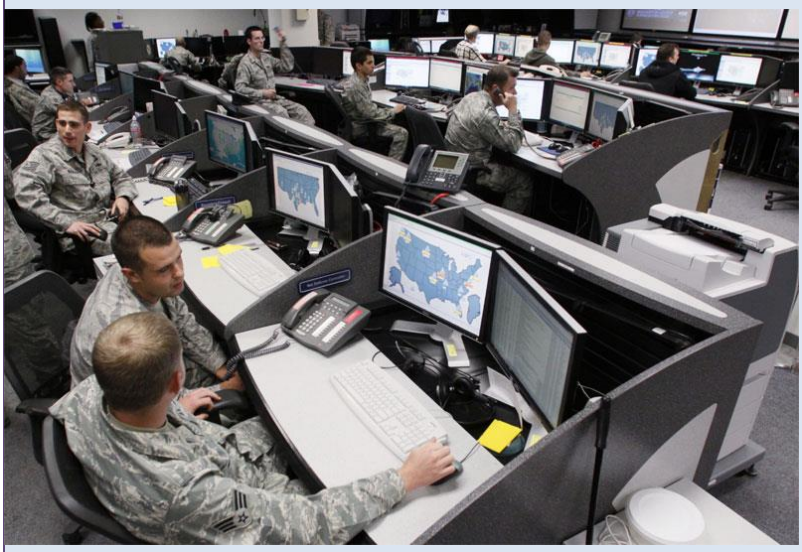
البته آمریکایی‌ها برای حمله سایبری به ایران همیشه تنها نبودند و رژیم صهیونیستی نیز در کنار آمریکایی‌ها و با همکاری آنان در این حملات شرکت می‌کند. هفته گذشته رسانه‌های این رژیم از سفر محرمانه ژنرال "مایک راجرز" رییس «آژانس امنیت ملی امریکا» (NSA) به اراضی اشغالی (تل آویو) و دیدار با سران سازمان جاسوسی این رژیم، خبر دادند. روزنامه «هاآرتص» به نقل از یک مقام این رژیم اعلام کرد: «این سفرِ کاری به منظور تحکیم همکاری‌ها بین سازمان اطلاعاتی امریکا و یگان اطلاعات سایبری موسوم به ۸۲۰۰ وابسته به مرکز اطلاعات نظامی ارتش اسرائیل، به ویژه هماهنگی در زمینه حمله سایبری علیه ایران و جنبش مقاومت حزب‌الله لبنان صورت گرفته است». در ایام این سفر بود که «هرتسی هلیفی» رئیس واحد اطلاعات ارتش رژیم صهیونیستی اعلام کرد این رژیم وارد یک جنگ سخت سایبری با ایران شده است.

در همین رابطه خبرگزاری روسی اسپوتنیک (sputnik news) در مقاله‌ای نوشت هدف سفر رئیس آژانس امنیت ملی آمریکا (NSA) به اراضی اشغالی تنها پروژه‌های دفاعی نبوده و عملیات‌های تهاجمی شبیه به ویروس استاکس‌نت نیز در دستور کار واشنگتن و تل‌آویو قرار دارد.

هفته گذشته ژنرال "مایک راجرز" رییس «آژانس امنیت ملی امریکا» به منظور تحکیم همکاری‌ها بین سازمان اطلاعاتی امریکا و یگان اطلاعات سایبری موسوم به ۸۲۰۰ وابسته به مرکز اطلاعات نظامی ارتش رژیم صهیونیستی، به ویژه هماهنگی در زمینه حمله سایبری علیه ایران و جنبش مقاومت حزب‌الله لبنان، به اراضی اشغالی (تل آویو) سفر کرده است. این اتفاق‌ها نشان می‌دهد که مسئله برجام و توافق هسته‌ای هیچ تضمینی برای قطع حملات سایبری علیه تاسیسات هسته‌ای ایران از سوی آمریکا نمی‌تواند باشد؛ این درحالی است که حملات سایبری به تاسیسات هسته‌ای، یکی از مجموع حملات علیه زیرساخت‌های ایران محسوب می‌شود.

آمریکا یک تروریست سایبری است

امروزه «سایبر تروریسم» (Cyberterrorism) خطرناکتر از تروریسم سنتی است؛ این امر به دلیل رشد روز افزون ساختار اقتصادی و خدمات‌رسانی بسیاری از کشورها مبتنی بر فناوری‌های اطلاعاتی و ارتباطی می‌باشد. سایبر تروریسم را می‌توان این گونه تعریف کرد: «اقدامات برنامه‌ریزی شده و هدفمند با اغراض سیاسی و غیرشخصی که علیه رایانه‌ها و امکانات و برنامه‌های ذخیره شده در درون آن‌ها از طریق شبکه جهانی صورت می‌گیرد و هدف از چنین اقدامی نابودی یا وارد آوردن آسیب‌های جدی به آنهاست».



آمریکا به عنوان مالک اینترنت و صاحب بزرگ‌ترین سازمان جاسوسی سایبری دنیا (NSA) در کنار ایجاد «فرماندهی سایبری» در ساختار ارتش خود، از این قدرت برای اقدامات تروریستی و ضربه‌زدن به بسیاری از سازمان‌ها و کشورهای جهان استفاده می‌کند

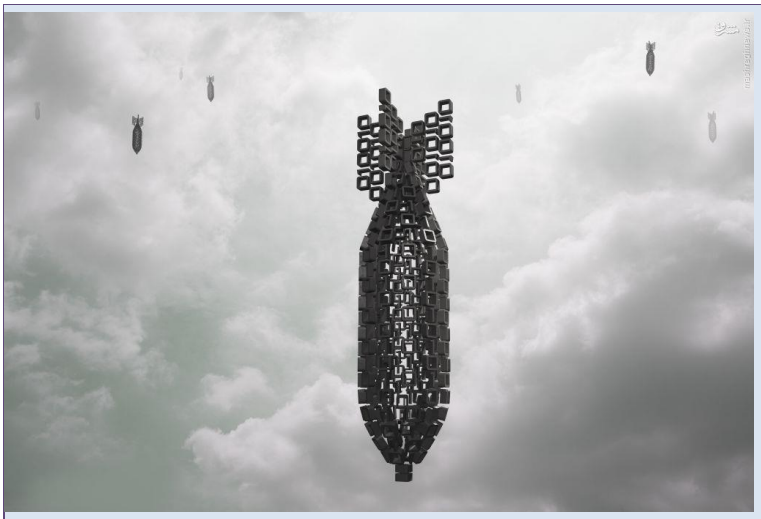
آمریکا به عنوان مالک اینترنت و صاحب بزرگ‌ترین سازمان جاسوسی سایبری دنیا (NSA) در کنار ایجاد «فرماندهی سایبری» در ساختار ارتش خود، توانسته حوزه «سایبر» را به یکی از مولفه‌های قدرت خود تبدیل و از این قدرت برای ضربه‌زدن به بسیاری از سازمان‌ها و کشورهای جهان استفاده کند. آمریکا تا کنون حملات تروریستی سایبری زیادی از جمله هک نمودن کامپیوترهای ارتش قذافی قبل از حمله هوایی علیه لیبی، قطع اینترنت و اختلالات ایجاد شده در شبکه تلفن همراه کره شمالی و حملات متعدد سایبری به زیرساخت‌های ایران با ویروس‌هایی مانند استاکس‌نت (Stuxnet)، استارس (STARS)، دوکو (Duqu)، فلیم یا شعله آتش (Flamer) و اکوئیشن (Equation) انجام داده است. البته به این موارد می‌توان تلاش برای دستیابی به شبکه‌های کامپیوتری زیرساخت‌های حساس کشور، ارسال تجهیزات سخت‌افزاری جاسوسی در بازار مصرف ایران و تعیین ایران به عنوان اولین و مهم‌ترین هدف حملات آژانس امنیت ملی آمریکا (NSA) را اضافه کرد که همگی در راستای تروریسم سایبری آمریکا علیه ایران تعریف می‌شود و تا کنون خسارات سنگینی را در ابعاد مختلف به منافع مادی و معنوی کشور وارد کرده است.

حملات سایبری آمریکا به ایران تا کنون خسارات سنگینی را در ابعاد مختلف به منافع مادی و معنوی کشور وارد کرده است:

با توجه به سابقه اقدامات تروریستی سایبری آمریکا علیه ایران و اینکه این حملات متوقف نشده و در آینده نیز ادامه خواهد داشت، ایران در برابر این حملات چه کارهایی باید انجام دهد؟

لزوم طراحی "سلاح سایبری قدرت‌مند" توسط ایران

یکی از بهترین شیوه‌های بازدارندگی، اقدام متقابل است که با اصطلاح «مقابله به مثل» از آن یاد می‌شود؛ همان‌طور که آمریکا در پروتکل‌های امنیت سایبر خود به‌طور صریح ابراز داشته که: «آمریکا در مقابل اعمال خصمانه در فضای مجازی به عنوان تهدیدی بر علیه منافع کشور پاسخ خواهد داد. همه کشورها دارای حق ذاتی برای دفاع از خود هستند، و به اعمال خصمانه‌ای که از طریق فضای مجازی صورت می‌گیرد با توجه به تعهدات ما در قبال هم‌پیمانان نظامی خود با اقدامات نظامی به آنها پاسخ خواهیم داد»، ایران نیز این حق را برای خود باید



محفوظ بدارد تا بتواند حمله سایبری قدرتمندی را جهت آسیب جدی به زیرساخت‌های آمریکا انجام دهد که این امر نیازمند نوآوری در طراحی یک سلاح سایبری قدرت‌مند است تا دشمنان ایران را از فکر حمله سایبری بیرون بیاورد.

ایران در اقدامی بازدارنده و در جهت آسیب جدی رساندن به زیرساخت‌های آمریکا، باید با نوآوری دست به طراحی "سلاح سایبری قدرت‌مند" بزند تا دشمنان را از فکر حمله سایبری بیرون بیاورد .

تدوین استراتژی امنیت ملی سایبری؛ ضرورتی استراتژیک در کنار طراحی یک سلاح سایبری قدرت‌مند سایبری، ایجاد واحدهای عملیاتی سایبری در نیروهای مسلح کشور و دستگاه‌های "اطلاعاتی-امنیتی- انتظامی"، تحت تدوین «استراتژی امنیت ملی سایبری» ضرورت دیگری است که این نیاز باتوجه به وابستگی روزافزون زیرساخت کشور به فضای سایبر، بسیار استراتژیک محسوب می‌شود. در حالی که دشمنان و رقبای ایران اسلامی در تلاش برای تکمیل حلقه‌های امنیت سایبری داخلی همچون تدوین استراتژی امنیت سایبری آمریکا و نظام‌سازی برای امنیت سایبری بین‌المللی در راستای اهداف خود هستند، تدوین «استراتژی امنیت ملی سایبری» دربرگیرنده ۴ حوزه امنیت ملی: سیاسی-امنیتی، فرهنگی-اجتماعی، اقتصادی و نظامی که نحوه تصمیم‌گیری، هدایت و کنترل امور را از سطح تکنیک تا استراتژیک در حوزه های سلبی- ایجابی ، آفندی- پدافندی و خارجی-داخلی کشور را پوشش دهد، بسیار ضروری به نظر می‌رسد.

تدوین «استراتژی امنیت ملی سایبری» دربرگیرنده ۴ حوزه امنیت ملی :سیاسی-امنیتی، فرهنگی-اجتماعی، اقتصادی و نظامی که نحوه تصمیم‌گیری، هدایت و کنترل امور را از سطح تکنیک تا استراتژیک در حوزه های سلبی- ایجابی ، آفندی- پدافندی و خارجی-داخلی کشور را پوشش دهد، بسیار ضروری به نظر می‌رسد.

این طرح باید ماموریت‌ها، وظایف، الزامات و اصول و فرمول‌های هدایت راهبردی، ایجاد ساختارهای نوین، خط مشی‌ها، رویه‌ها، پروتکل‌ها و چارچوب چینش و هماهنگی و هدایت یکپارچه عناصر را از بالا به پایین پوشش دهد و توسعه تاکتیک‌ها و تسلیحات ویژه این جنگ را در دستور کار قرار دهد. با تدوین و اجرایی نمودن این طرح در ذیل و راستای "استراتژی بزرگ" کشور است که می‌توان کنش‌ها و واکنش‌های کشور را در حوزه سایبر و تمامی حوزه‌های مربوط تنظیم نمود.

لزوم تشکیل فرماندهی سایبری در ایران

تشکیل یگان هوانیروز مستقل در سپاه نشان داد که جمهوری اسلامی نگاه سیالی به تامین امنیت دارد و حاضر است برای تحقق این موضوع، ساختارهای قبلی را شکسته تا ساختار جدیدی طراحی کنند. باتوجه به وجود این نگاه نوآور در مسئولان ارشد نظامی-امنیتی، انتظار می‌رود که هرچه زودتر فرماندهی سایبری در ایران تاسیس شود تا این نهاد جدید بتواند در تحقق ساخت سلاح‌های سایبری، تدوین استراتژی امنیت ملی سایبری و تقویت زیرساخت‌های کشور در قبال حملات سایبری در راستای امنیت بیشتر کشور عمل کند.

ساختار و اجزای فرماندهی سایبری آمریکا

ایران باید تهیه روندی که در آینده منجر به افزایش ضریب امنیت سایبری شود را هرچه سریع‌تر دنبال کند تا جلوی نفوذ سایبری آمریکا و هم‌پیمانانش مانند رژیم صهیونیستی گرفته شود و با تهیه دکترین فعالیت‌های فضای سایبری، از سرمایه‌های کشور همانند مرزهای فیزیکی محافظت نماید.منبع: سایت پایداری ملی:http://paydarymelli.ir

عناوین رویدادهای مهم خبری

«برای مشاهده متن کامل خبرها روی آنها کلیک کنید»

❖ نجات زمین از معضل زباله‌های پلاستیکی با یک باکتری جدید	❖ ۱۰ نکته اساسی درباره محصولات تراریخته
❖ تشخیص ویروس ابولا و زیکا با یک سیم!	❖ سناریوهای آمریکا برای مقابله با جمهوری اسلامی ایران (برجام ۱، ۲ و ....)
❖ بررسی وضعیت میزان مصرف سم در ایران/ تکذیب سرطان زا بودن محصولات تراریخته	ایران و عراق به روایت سرویس تحقیقاتی آمریکا؛ ❖ اسناد ویکی‌لیکس از پشت‌پرده فتنه‌انگیزی آمریکا میان ایران و عراق چه می‌گویند
❖ کری: مشکل تجارت با بانکهای اروپایی متوجه ایران است	یک کارشناس بیان کرد؛ ❖ لزوم کنترل واردات و حرکت به سمت اقتصاد مقاومتی با استفاده از اصول پدافند غیرعامل

سایت های مرتبط با پدافند غیرعامل

❖ وب سایت پایداری ملی	http://www.paydarymelli.ir/
❖ مرکز مطالعات پدافند غیر عامل	http://www.pdrc.ir
❖ پورتال پدافند غیرعامل استانداری آذربایجان شرقی	http://padafand.eaz.gov.ir/
❖ استانداری آذربایجان شرقی – دفتر پدافند غیرعامل	http://ostan-as.gov.ir/?PageID=42
❖ پلیس فتا	http://www.cyberpolice.ir/

صاحب امتیاز: اداره کل پدافند غیرعامل استانداری آذربایجان شرقی
مدیر مسئول: سردار احمد جهانسری
سردبیر: محمد بامدادی
دبیر تحریریه: رامین زارعی
شماره تماس : ۰۴۱-۳۳۳۳۶۲۰۹