ماهنامه اداره کل پدافند غیرعامل
شماره ۴۶/ تیر ماه ۱۳۹۹

ماهنامه دیجیتالی پدافند غیرعامل

استاندار آذربایجان شرقی:
عادی‌انگاری شرایط و شروع فعالیت‌های اجتماعی پس از یک دوره محدودیت را مهم‌ترین عامل افزایش آمار مبتلایان به کرونا عنوان کرد

معاون سیاسی، امنیتی و اجتماعی استانداری:
تجمع مردم و شنا و آب‌تنی در سواحل دریاچه ارومیه در آذربایجان شرقی ممنوع است

در این شماره می‌خوانید:

کشاورزی ارگانیک و غذای سالم

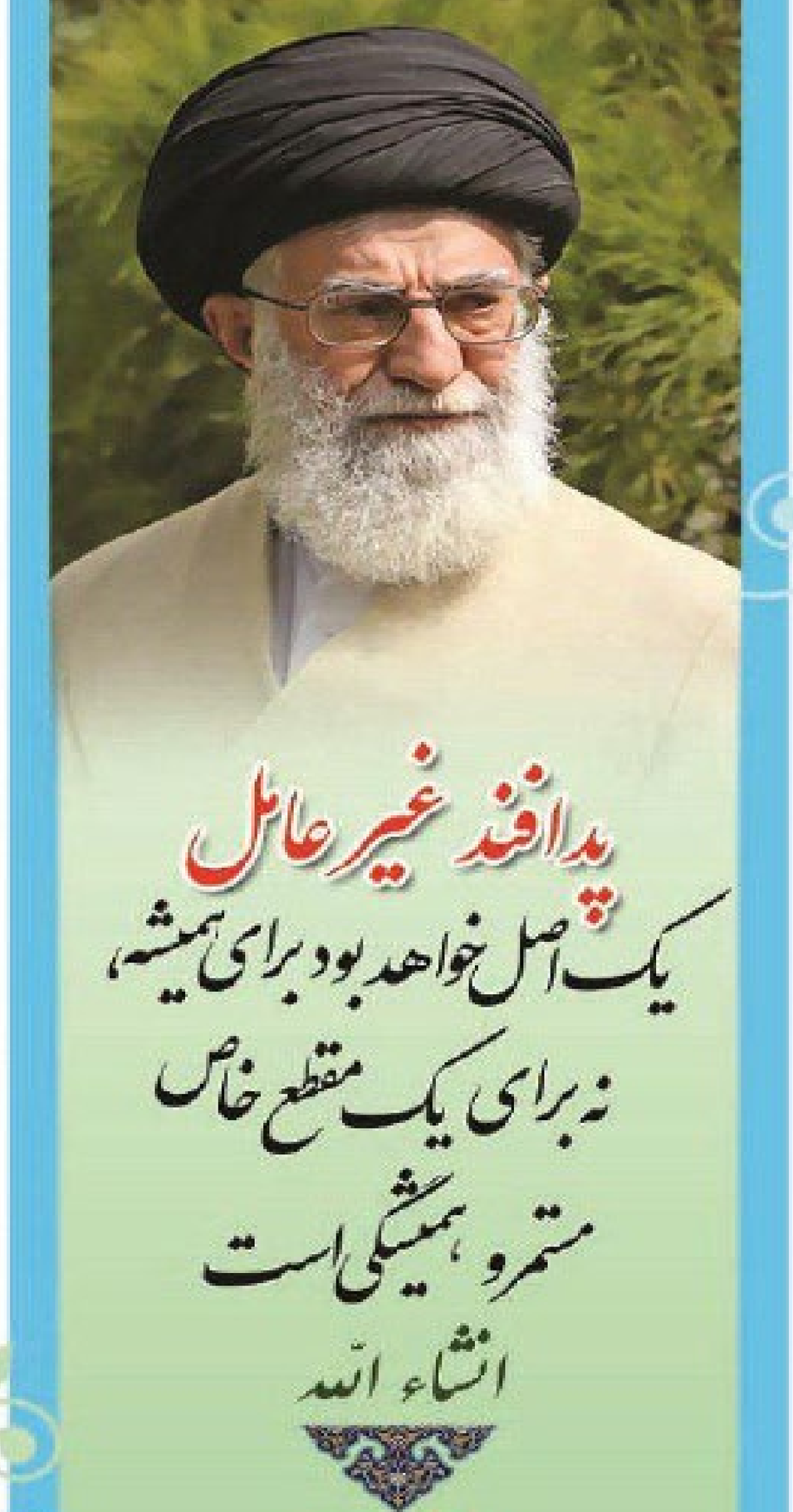
پایان پشتیبانی از Adobe Flash Player تا پایان سال میلادی

آسیب‌پذیری بحرانی SigRed در ویندوز سرور

مهم‌ترین به‌روزرسانی‌های ماه جاری شرکت‌های تولید کننده سخت افزار و نرم افزار

اهمیت خودکفایی

خودکفایی و خود اتکایی تنها مؤلفه های دستیابی به امنیت غذایی و دستیابی به زنجیره ی پایدار می باشند.



بسم الله الرحمن الرحیم

فهرست مطالب:

مدیر مسئول:
محمد باقر آقایی

سردبیر:
لیدا رسول اهری

نشانی:
تبریز، میدان شهدا، استانداری آذربایجان شرقی، اداره کل
پدافند غیرعامل
تلفن: ۰۴۱-۳۵۲۹۱۳۱۸
دورنگار: ۰۴۱-۳۵۲۹۱۳۵۹

استادان، پژوهشگران و دانشجویان علاقمند، می‌توانند مقاله‌های آموزشی، پژوهشی و ترویجی خود را برای درج در نشریه پدافند غیر عامل به نشانی زیر ارسال کنند.

passivedefense@ostan-as.gov.ir

جلسه ستاد استانی مدیریت و مقابله با کرونا

دکتر محمدرضا پورمحمدی در بیست و سومین جلسه ستاد استانی مدیریت و مقابله با کرونا، اظهار داشت: در روزهای گذشته شاهد ارتقای میزان رعایت پروتکل‌های بهداشتی از سوی مردم هستیم و همه به این آگاهی رسیده‌اند که چاره‌ای جز رعایت این پروتکل‌ها نداریم.

وی عادی‌انگاری شرایط و شروع فعالیت‌های اجتماعی پس از یک دوره محدودیت را مهم‌ترین عامل افزایش آمار مبتلایان به کرونا در هفته‌های اخیر دانست و گفت: خوشبختانه ما در قسمت سخت‌افزاری کار یعنی بخش درمان و تأمین اقلام بهداشتی، مشکل خاصی نداریم و با همت بخش‌های مختلف، توان مواجهه و مقابله با بیماری افزایش یافته است.

مشکل اصلی در قسمت نرم‌افزاری است که طی یکی دو هفته اخیر با ازسرگیری برخی فعالیت‌های اقتصادی و اجتماعی ایجاد شده است، رسانه‌ها و تشکل‌های اجتماعی باید ارتقای آگاهی مردم و فرهنگ‌سازی را جدی بگیرند و اطلاعات لازم را در این خصوص به جامعه منتقل کنند.

همواره از انعکاس شفاف اخبار و اطلاعات استقبال می‌کنیم، اما در شرایطی که جامعه نیاز به آرامش دارد انتشار اخبار کذب شایسته نیست. اطلاعاتی که مسئولان درباره بیماری کرونا ارائه می‌کنند به هیچ وجه دارای ملاحظات سیاسی نیست، چرا که این موضوع با سلامت مردم در ارتباط است.

دستگاه‌های مسئول وظایف خود را به خوبی انجام داده‌اند و بیشتر مردم هم انصافاً همکاری خوبی دارند؛ اما باید بر این نکته تأکید کنیم که در حال حاضر ابتکار عمل به دست خود شهروندان است.

وی از همکاری دستگاه قضایی و نیروی انتظامی استان در برخورد با تخلفات بهداشتی قدردانی کرد و گفت: در حال حاضر برخوردها نسبت به روزهای ابتدایی شیوع کرونا سخت‌تر است و اعمال قانون باید با در نظر گرفتن ملاحظات اجتماعی انجام شود، در عین حال بر تشدید نظارت‌ها در حوزه رعایت پروتکل‌های بهداشتی تأکید کرد.

همچنین بر نظارت جدی دستگاه‌های مسئول بر تولید و توزیع اقلام بهداشتی، رعایت پروتکل‌های بهداشتی و صرفه‌جویی در مصرف آب و برق در ادارات و ممنوعیت تشکیل هرگونه تجمع نیز تأکید کرد.

ارتباط تصویری با جلسه ستاد ملی مقابله با کرونا

دکتر محمدرضا پورمحمدی در این ارتباط تصویری اظهار داشت: از ابتدای شیوع بیماری کرونا تاکنون ۵۰ هزار نفر در آذربایجان شرقی مشکوک به بیماری کرونا تشخیص داده شده‌اند که نتیجه تست ۳۵ درصد از این افراد معادل ۱۵ هزار نفر مثبت بوده است.

۹۲ درصد از مبتلایان قطعی به کرونا بهبود یافته یا در حال بهبودی هستند. ۸ درصد از مبتلایان نیز بستری شده یا فوت کرده‌اند که تعداد بستری‌شدگان ۷۵۰ نفر و تعداد فوت‌شدگان ٦۳۰ نفر است.

وی با اشاره به افزایش تعداد مبتلایان به کرونا در استان در دو سه هفته گذشته گفت: در این مدت روزانه به طور متوسط ۳۰۰ تا ٤۰۰ مورد جدید کرونا شناسایی شده است که این افزایش نگران‌کننده، سه علت عمده دارد. افزایش تست‌های انجام‌شده یکی از علت‌های افزایش تعداد مبتلایان شناسایی‌شده است. در حال حاضر روزانه یک‌هزار تست کرونا در استان انجام می‌شود که البته نسبت تعداد مبتلایان به تعداد تست‌ها، نسبت به ماه‌های گذشته ثابت است اما نسبت فوت‌شدگان کاهش یافته است.

دومین علت افزایش تعداد مبتلایان به کرونا در استان، بیماریابی هدفمند است، قبلاً از کسانی که به مراکز سلامت یا مراکز درمانی مراجعه می‌کردند تست گرفته می‌شد اما در حال حاضر روند بیماریابی کاملاً هدفمند شده و بیشتر از گروه‌های هدف مانند اطرافیان بیماران یا سالمندان تست گرفته می‌شود.

عادی‌انگاری و عدم رعایت پروتکل‌های بهداشتی، سومین و مهم‌ترین دلیل افزایش مبتلایان به کرونا در استان است.

پیش‌بینی می‌کنیم که روند بیماری در ماه‌های آینده نیز با کیفیت کنونی ادامه یابد و امیدواریم با همکاری مردم و رعایت پروتکل‌های بهداشتی به یک وضعیت تثبیت‌شده و مدیریت‌شده در استان برسیم.

تجمع مردم، شنا و آب‌تنی در سواحل دریاچه ارومیه در آذربایجان شرقی ممنوع است

معاون سیاسی، امنیتی و اجتماعی استانداری آذربایجان شرقی از تصویب ممنوعیت تجمع مردم، شنا و آب‌تنی در ساحل دریاچه ارومیه توسط ستاد استانی مقابله با کرونا خبر داد.

علیار راستگو با اعلام این خبر افزود: این ممنوعیت در راستای اعمال محدودیت‌های جدید برای مقابله با شیوع کرونا تصویب شده و در تمامی سواحل دریاچه ارومیه در آذربایجان شرقی اجرا می‌شود.

دستورهای لازم برای ممانعت از حضور شهروندان در سواحل دریاچه ارومیه از سوی ستاد استانی مقابله با کرونا به فرمانداران شبستر و اسکو ابلاغ شده است.

وی با تأکید بر رعایت جدی پروتکل‌های بهداشتی گفت: تجمع مردم و تشکیل اجتماعات یکی از عوامل اصلی شیوع کروناست، بر این اساس تشکیل هرگونه تجمع تحت هر عنوان ممنوع است.

راستگو با بیان اینکه حضور مردم در اماکن تفریحی و گردشگری معمولاً با تجمع همراه است، افزود: از مردم استان می‌خواهیم که فعلاً به خاطر سلامت خود و خانواده‌شان از تجمع و اتراق در پارک‌ها، بوستان‌ها، حاشیه جاده‌ها و سایر اماکن تفریحی اجتناب کنند.

جنگ سایبری

تهیه و تنظیم: میر رسول حسینی اقدم (کارشناس امریه اداره کل پدافند غیرعامل)

منابع:
۱. مارتی لهتو، پکا نیتامَاکی، کتاب امنیت سایبری (تجزیه و تحلیل‌ها، فناوری و اتوماسیون)، مترجم علیرضا زحلی، چاپ اول، تهران: بهار ۱۳۹۵
۲. هیتر هریسون دنیس، کتاب جنگ سایبری و حقوق جنگ، سرپرست گروه ترجمه: دکتر محمد جواد عربیان، چاپ دوم، انتشارات جهان جام جم، ۱۳۹۵
۳. غلامی، علیرضا؛ خدارحمی، حبیب، کتاب کارکردهای پدافند غیرعامل در رویارویی با تهدیدهای نرم و سخت، چاپ اول، انتشارات جهان جام جم، ۱۳۹۵
٤. عابدینی یزدی، وحید؛ رضایی اصل، سید مجتبی. «پدافند غیرعامل، بررسی تهدیدات سایبری و راهکارهای مقابله با آن»، کنفرانس ملی پدافند غیرعامل و توسعه پایدار، تهران: ۱۲ و ۱۳ مهر ۱۳۹۵
۵. جیستان، ذبیح الله؛ جیستان، حسین. « مفهوم جنگ سایبری و بررسی ابعاد مختلف»، نهمین سمپوزیوم پیشرفت‌های علوم و تکنولوژی، مشهد: ۱۳ آذر ۱۳۹۳
٦. عباسی، مجید؛ مرادی، حسین، «جنگ سایبر از منظر حقوق بین‌الملل بشردوستانه»، فصلنامه علمی-پژوهشی مجلس و راهبرد، شماره ۸۱ بهار ۱۳۹٤

مقدمه

تحلیلگران نظامی، حوزه مجازی را به عنوان یک دامنه جدید در حوزه جنگ به رسمیت شناخته‌اند که اهمیت آن در حال پیشی گرفتن از سایر حوزه‌هاست. امروزه تهدیدها در قالب شبکه‌های رایانه‌ای و مخابراتی رو به افزایش است. بخش‌های کلیدی اقتصاد تمامی کشورها در حال حاضر، از جمله امکانات دولتی و خصوصی، بانکداری و امور مالی، حمل‌ونقل، تولید، پزشکی، آموزش و پرورش و دولت، همگی برای انجام عملیات روزانه وابسته به رایانه هستند. فضای مجازی ابزاری برای قدرت و ثروت است. اگر از آن استفاده نکنیم دیگران از آن استفاده خواهند کرد و آن هم برضد ما. گاهی به دلیل ناشناخته بودن منبع حمله؛ فضای مجازی به مکانی ایده‌آل برای جنگ تبدیل می‌شود.

فناوری اطلاعات در جایگاه مغزافزار فعالیت‌های جهانی، محور عملیات دولت‌ها، رویه‌های کنترل و فرماندهی نظامی، از چنان نقشی برخوردار شده است که برخی استراتژیست‌ها از منسوخ شدن خودکار «جنگ متعارف» در این فضای جدید سخن می‌گویند. جنگ در فضای سایبری را می‌توان حمله‌های اینترنتی طراحی‌شده از سوی گروه‌ها، سازمان‌های مختلف علیه سامانه‌ها و برنامه‌های رایانه‌ای با اهداف به مراتب بزرگتر مانند دستیابی به سود مالی یا آسیب وارد کردن به شهروندان یا دولت به‌وسیله روش‌های مجرمانه مانند کلاهبرداری، جعل، تخریب و اخلال در داده‌ها، سرقت، تضعیف یا غیرفعال کردن زیرساخت‌های نظامی و غیرنظامی تعریف نمود.

جنگ سایبری دارای ویژگی‌های منحصر به‌فردی است که در ثانیه اتفاق می‌افتد، از راه دور و بدون وجود ریسک برای جان سربازان و پرسنل رزمی. جنگ اطلاعات، موج آینده است که همراه با حملات گسترده به بنیان‌های ارتباطاتی امروز (نظامی و غیرنظامی)، شبیخون قرن بیست ویکم را رقم می‌زند.

فضای سایبر یک میدان جنگ دیجیتال است که در آن کشورها و پروکسی‌هایشان، گروه‌های تبهکار سازمان‌یافته، تروریست‌ها، هکرها، و دیگر گروه‌ها در جستجوی راهی برای بهره‌بردن و استیلا بر دیگران از طریق نظارت، جاسوسی، فعالیت‌های مخرب و مجرمانه، استخدام و اغفال نیروها، برنامه‌ریزی و تحریک به حمله سایبری هستند. اگرچه برخی استراتژیست‌ها سایبرتروریسم را تروریسم جدید عصر ما معرفی می‌نمایند اما تاریخچه تروریسم سایبری به اوایل دهه ۱۹۹۰ همزمان با فراگیر شدن شبکه جهانی اطلاعات می‌رسد.

جنگ سایبری

واژه جنگ سایبری برای تشریح نوع جدیدی از جنگ که بر روی سامانه‌های ارتباطی و الکترونیکی دشمن متمرکز می گردد، ابداع شده است. در این جنگ نیازی به اعزام لشکرها یا ناوهای جنگی نبوده و به جای آن از ویروس‌های رایانه‌ای، بمب‌های منطقی و بمب‌های پالس الکترومغناطیسی استفاده می‌شود که قادر است خرابی‌های وسیعی در مدارات الکترونیکی سامانه‌های $C4I$، رادارها، رایانه‌ها، سلاح‌های هوشمند و سامانه‌های مراقبتی به وجود آورد. این نوع از جنگ مقدم بر جنگ واقعی بوده و حتی ممکن است قبل از شروع از وقوع آن جلوگیری کند.

در واقع جنگ سایبری براساس قوانین حاکم بر اطلاعات و از طریق دنیای اطلاعات صورت می‌گیرد. هدف از این نوع جنگ تخریب سیستم‌های اطلاعاتی و ارتباطاتی است. این نبرد حرکتی در جهت تغییر موازنه اطلاعات و دانش به نفع طرف دیگر است. البته مواردی وجود دارد که کار دفاع در مقابل حملات سایبری را دشوار می‌کند. یکی از آن موارد شناسایی هویت و مکان مهاجم است. همچنین شناسایی نیت مهاجم، تشخیص حمله‌های از قبل طراحی شده و بررسی و ارزیابی تلفات بعد از نبرد مجازی از نقاط ضعف دفاعی در مقابل حملات سایبر است. بهترین راهکار قبل از مقابله با حملات سایبری، شناخت موضوع و ابعاد مختلف آن است.

هدف از حمله سایبری، دستیابی به اطلاعات سایر کشورها، ایجاد وقفه در تجارت و یا ایجاد خدشه در زیر ساخت‌ها به نحوی که هزینه‌های اقتصادی را افزایش دهند.

امروزه فضای سایبری بیش از پیش با امنیت کشورها گره خورده است. در بسیاری از کشورها بخش سایبری در درون تشکیلات نظامی فعال شده است و فضای سایبر به طور فزاینده‌ای نظامی شده است. جنگ سایبری به وضوح یک جبهه است که کشورها سعی می‌کنند در آن مزیت نسبی بدست آورند و پیروز میدان باشند اما این جنگ جنبه محرمانه‌ای هم دارد که مخفیانه انجام می‌شود. کشورها هیچگاه اعتباری که به حملات سایبری و هک‌کردن تخصیص می‌دهند را بیان نمی‌کنند. امروزه امنیت و حفاظت از اطلاعات یکی از مهمترین بخش‌هایی است که قدرت دولت‌ها را نشان می‌دهد.

زیرا با افزایش استفاده از اینترنت و تکنولوژی ارتباطات و انقلابی که در جوامع بشری بوجود آمده است، جرایم مختلفی در زمینه‌های مختلف زندگی بشری از جمله

بانکداری، تجارت الکترونیک، کلاهبرداری سایبری، جاسوسی سایبری، جعل، سرقت سایبری سبب تهدید امنیت ملی شده‌اند.

در دهه ۱۹۹۰، جنگ سایبری زیرمجموعه‌ای از جنگ اطلاعات (*IW*) بود. جنگ اطلاعات به اقداماتی اطلاق می‌گردد که به منظور کسب برتری اطلاعاتی میدان نبرد از طریق مخدوش کردن اطلاعات و اختلال در سامانه اطلاعاتی دشمن و محافظت از اطلاعات و سامانه اطلاعاتی خودی اجرا می‌شوند.

مارتین لیبیکی بخش‌های جنگ اطلاعات را بصورت زیر تعریف کرده است:

- جنگ فرماندهی و کنترل (*C۲W*)
- جنگ اطلاعاتی (*IBW*)
- جنگ الکترونیک (*EW*)
- عملیات‌های روانشناختی (*PSYOPS*)
- جنگ هکر
- جنگ اقتصاد اطلاعات (*IEW*)
- جنگ سایبری

یکی از شاخص‌ترین محیط‌های جنگ سایبری به اینترنت و شبکه‌های (نظامی یا غیرنظامی) مرتبط می‌باشد که به نحوی اطلاعات را به اشتراک می‌گذارند. با درنظر گرفتن جنبه نظامی جنگ سایبری می‌توان آنرا جنگی در حوزه اینترنت قلمداد نمود. جنگ سایبری بر این اساس در فضایی به نام فضای سایبری رخ می‌دهد.

فضای سایبری عبارت است از فضای غیرملموس بین رایانه‌ها جاییکه داده‌ها یا اطلاعات بصورت لحظه‌ای در مسیر عبور از یک رایانه به رایانه دیگر که درشبکه‌های محلی یا جهانی مبادله می‌شوند. این رایانه‌ها ممکن است برای مقاصدی نظیر ارتباط، هدایت سلاح‌ها، شناسایی و مراقبت یا اموری نظیر حسابداری و بانکداری مورد استفاده قرار گرفته باشند. این فضا همچنین شامل امواج حاصله از ابزارهای مخابراتی، ماکروویو و ارتباطات ماهواره‌ای می‌شود. از آنجا که همه یگان‌های نظامی در همه ارتش‌ها به نوعی به شبکه جهانی ارتباطات متصل هستند لذا همگی، ساکنین فضای سایبری محسوب می‌گردند.

انواع جنگ سایبری

۱- نفوذ سایبری: عبارت است از ایجاد رخنه در یک سامانه با کنترل نرم افزاری به‌نحوی که بتوان آن سامانه را مورد یورش، تهاجم و دستکاری قرار داد. یک روش نفوذ و یورش سایبری وارد کردن مقادیر بزرگی از اطلاعات به درون یک سامانه است که سبب سرریز شدن اطلاعات سیستم و سقوط شبکه مربوطه می‌گردد.

۲- دستکاری سایبری: به دنبال نفوذ سایبری بدست گرفتن کنترل سامانه‌ها از طریق نرم‌افزارهای مرتبط و به کاربردن آن‌ها برای ایجاد خرابی و خسارت در سامانه را دستکاری سایبری می‌نامند. برای مثال استفاده از ابزارهای نرم افزاری برای خاموش کردن سیستم‌ها و مختل کردن شبکه‌ها مصداقی از دستکاری سایبری است.

۳- تاخت سایبری: پس از انجام موفقیت‌آمیز نفوذ سایبری، تخریب نرم‌افزارها و داده‌ها در یک سامانه یا حمله به سامانه به نحوی که کارآیی آن از بین برود را تاخت سایبری می‌نامند. این تاخت همچنین ارسال ویروس‌هایی را شامل می‌شود که از طریق پست الکترونیک اضافه بار زیادی را بر سامانه تحمیل می‌نمایند.

٤- دستبرد سایبری: به دنبال نفوذ سایبری موفق، هرگونه دستکاری یا در اختیار گرفتن اطلاعات یک سامانه که منجر به انتقال، تخریب و یا تغییر اطلاعات آن گردد را دستبرد سایبری گویند. برای مثال سرقت پست الکترونیک و یا بدست آوردن فهرست گذر واژه‌ها از یک سرویس دهنده پست الکترونیک.

۵- عاملان سایبری عمدی: افرادی هستند که به طور عمدی و با قصد و نیت جنگ سایبری را به اجرا می‌گذارند. به این افراد همچنین اپراتورهای سایبری، نیروهای سایبری، رزمندگان سایبری یا عده‌های سایبری نیز اطلاق می‌گردد.

٦- عاملان سایبری غیرعمدی: افرادی که به طور غیر عمدی در سامانه‌ها نفوذ می‌نمایند اما امنیت ملی را به مخاطره انداخته و عموماً از مخاطرات ایجاد شده توسط اعمال خود آگاه نمی‌باشند.

۷- ویروس افکنی: عمل وارد نمودن دستی یا الکترونیکی یک ویروس یا کد ویروس به سامانه‌ها می‌باشد.

ویژگی‌های جنگ سایبری:

برجسته‌ترین ویژگی‌های جنگ در فضای اطلاعاتی به شرح زیر می‌باشند:

۱- سرقت پنهان اطلاعات: اطلاعات دارایی بی‌نظیری است که اگر به طور حرفه‌ای به سرقت رود تنها سارق است که می‌داند که این اطلاعات در دو نقطه وجود دارد. مالباخته چنین سرقتی در بی‌اطلاعی کامل به سر برده و سرنخی از ماجرا در دست نخواهد داشت.

۲- تغییر اطلاعات: یک ویژگی دیگر در جنگ سایبری این است که رزمنده سایبری به جای سرقت اطلاعات ممکن است ترجیح دهد تا اطلاعات را در راستای دستیابی به اهداف خود تغییر دهد. کاربر ممکن است تا مدت‌ها به این موضوع پی نبرد.

۳- تخریب اطلاعات: اگر رزمنده سایبری توانایی تغییر و دستکاری اطلاعات را داشته باشد، مسلماً توانایی تخریب آن‌ها را نیز خواهد داشت. بیشمار اتفاق افتاده است که اطلاعات موجود در یک رایانه به دلیل نواقص سامانه ای به طور تصادفی از بین رفته و با تخریب گردد. این اتفاق ممکن است در اثر ورود یک ویروس رایانه‌ای جدید و یا به واسطه تأثیر پالس‌های الکترومغناطیسی حاصله از دستگاه‌های الکترونیکی و الکتریکی در مجاورت سامانه به وجود آمده باشد.

٤- تخریب تسهیلات اطلاعاتی: سامانه‌های فرمان و کنترل نیروهای مسلح و سامانه‌های سطوح ملی عمیقاً به اطلاعات و پایگاه داده‌های سازمان‌ها وابسته هستند. رزمنده سایبری بر اساس موقعیت، بهترین گزینه را در خصوص تخریب تسهیلات اطلاعاتی ارتش یا کشور هدف و یا از بین بردن کامل توانایی‌های دشمن در پردازش اطلاعات و ارتباط به نحوی که قبل از شلیک اولین گلوله از پا در آمده باشد را انتخاب می‌نماید.

۵- دشواری ارزیابی و اخطار تک: این ویژگی از جنگ سایبری جنبه دیگری از مشکلات اساسی موجود در فضای سایبری را بیان می‌نماید. مشکل اصلی این است که به سختی می‌توان بین یک حمله سایبری و سایر رویدادها نظیر اتفاقات، نقص سامانه، اشباع سامانه و یا حتی نفوذ تصادفی افراد معمولی تفاوتی قائل شد. استنتاج اصلی این ویژگی آنست که یک ملت یا سازمان ممکن است حتی نداند که مورد حمله واقع گردیده و یا اینکه حمله کننده کیست و یا روش حمله چه بوده است.

٦- ورود ارزان: متفاوت از فناوری سلاح‌های سنتی، نفوذ به سامانه‌های اطلاعاتی نیازی به سرمایه‌گذاری کلان اقتصادی و نظارت دولتی ندارد. تنها پیش نیاز رزمنده سایبری، داشتن تبحر و خبرگی در سامانه‌ها و دسترسی به شبکه داده‌ها و اطلاعات مهم هدف است.

۷- نامرئی بودن و عدم شفافیت مرزهای سنتی: با وجود تعداد وسیعی از عوامل مؤثر در فضای جنگ سایبری ازجمله وجود طرف‌های بسیار، سامانه‌های سلاح، وابستگی به فناوری و تجهیزات خارجی و احتیاج به خبرگان نرم‌افزاری؛ تشخیص بین تهدیدات داخلی و خارجی بطور روزافزون دشوارتر می‌شود. قربانی حمله سایبری ممکن است از حمله مطلع نشده و یا حمله کننده را نشناسد، مزیت نامرئی و ناشناس بودن در محیط جنگ سایبری و عدم شفافیت قوانین حاکم بر آن سبب می‌شود که فنون جنگی بالقوه خطرناک به کار گرفته شده و بر خلاف محیط جنگ‌های سنتی حتی نتوان متجاوز را تنبیه نمود.

۸- رویداد انفجاری: یکی از مهمترین ویژگی‌های حمله سایبری اثرات انبوه یک رویداد بر روی یک سازمان یا کشور است. وقتی تنها یک نسخه از یک بمب منطقی در داده‌ها یا رایانه‌های یک سازمان رسوخ نماید می‌تواند سراسر شبکه ارتباطات راه دور یک کشور را مختل نماید. دامنه تخریب یک بمب منطقی ممکن است حتی از این هم فراتر رفته و سایر سامانه‌های آن سازمان یا کشور را تحت تأثیر قرار دهد.

فنون جنگ سایبری:

فنون متعددی در جنگ سایبری وجود دارد که در دو بخش نرم افزار و سخت افزار قابل اجرا هستند.

الف) نرم افزار: این فنون همه کدها و برنامه‌های نرم افزاری مرتبط را شامل می‌شود که برخی از آن‌ها عبارتند از: ویروس، اسب تروا، کرم و...

ب) سخت افزار: میکروب، نانو ماشین (مورچه آتشین)، اخلال تراشه‌ای، دستگاه‌های الکترومغناطیسی ناپایدار

هنوز زیرساخت‌های کافی برای جلوگیری از حملات سایبری در سیستم‌های رایانه‌ای کشورها تعبیه نشده است. فضای مجازی به یک مکان بالقوه برای جرایمی این چنینی تبدیل شده است. میلیاردها دلار بدون کمترین امنیتی در فضای سایبر روزانه جابه‌جا می‌شوند و بخشی از مهم‌ترین اطلاعات دولتی و شخصی بدون کمترین امنیتی در فضای مجازی وجود دارند که خطر حملات سایبری را افزایش می‌دهند.

وجود نداشتن قوانین بین‌المللی باعث شده که هر کشوری به خود اجازه دهد تا برضد کشور دیگر وارد جنگ مجازی شود. در حال حاضر کشور ایالات متحده در جهان مرکز فرماندهی فضای مجازی را در پنتاگون راه اندازی کرده است که هدف از ایجاد آن حمله به شبکه‌های سایر کشورها و دفاع در مقابل حملات مجازی است. همچنین آژانس امنیت اطلاعات و شبکه اروپا نیز چنین مرکزی است.

انواع تهدیدهای مختلف ناشی از جنگ سایبری

۱- جاسوسی و نقض امنیت ملی؛

جاسوسی سایبری به عملی اشاره دارد که به منظور بدست آوردن اسرار (حساس، اختصاصی و یا اطلاعات طبقه‌بندی شده) از افراد، رقبا، گروه‌ها، دولت‌ها و دشمنان برای استفاده نظامی، سیاسی یا اقتصادی با استفاده از روش‌های بهره‌برداری غیر قانونی در اینترنت، شبکه، نرم‌افزار و یا رایانه صورت می‌گیرد.

۲- خرابکاری؛

فعالیت‌های نظامی که با استفاده از ماهواره و رایانه برای اختلال در تجهیزات دشمن صورت می‌پذیرد، خرابکاری نام دارد. زیرساخت‌های برق، آب، سوخت، ارتباطات، حمل‌ونقل و ... ممکن است در جنگ مجازی در معرض خطر باشند. سایر تهدیدها می‌تواند شامل سرقت اطلاعات کارت‌های اعتباری، اختلال در برنامه قطارها و یا حتی بازار سهام باشد.

۳- شبکه برق.

شبکه‌های انتقال برق به دلیل وابستگی به فضای مجازی و اینترنت از مهم‌ترین هدف‌ها در جنگ مجازی محسوب می‌شوند. در سال ۲۰۰۹م. دولت ایالات متحده بیان داشت که دولت‌های چین و روسیه قصد داشتند تا با نفوذ نرم‌افزاری در شبکه‌های برق این کشور در آن اختلال ایجاد کنند. از سوی دیگر و در نقطه مقابل نیز حملات نظامی به شبکه‌های انتقال برق برای از کار انداختن اینترنت از موارد مورد توجه در جنگ مجازی است.

انگیزه‌های جنگ سایبری:

۱- مقاصد نظامی؛

درست مانند جنگ واقعی در اینجا بر خلاف ٤ رکن دیگر جنگ که پیش‌تر بیان داشتیم، این جنگ در سایه فضای مجازی صورت می‌پذیرد. در اینجا نیازمند یک مرکز فرماندهی جنگ سایبری و سلاح‌هایی مجازی و دفاعی هستیم تا جلوی حمله گرفته شود و قادر به حمله متقابل باشیم.

۲- اهداف غیرنظامی؛

این امر عبارت از اختلال در سرویس دهنده وب، سیستم‌های اطلاعات سازمانی، سیستم‌های سرور، لینک‌های ارتباطی، تجهیزات شبکه و رایانه‌های رومیزی و لپ‌تاپ‌های خانگی و امور تجاری است که گاهاً برای کسب انگیزه‌های تجاری رقابتی و یا مالی صورت می‌پذیرد و گاهی نیز خرابکاری به دلیل صرفاً سرگرمی است.

۳- اهداف شخصی.

باید باور کرد که بیش از ۹۰ درصد حملات سایبری برای اهداف شخصی صورت می‌گیرد. بسیاری از حملات برای جلب توجه رسانه‌ها انجام می‌شود. شرکت (*McAfee*) می‌گوید، روزانه با میلیون‌ها جنبه از این نوع حملات سایبری توسط نرم‌افزارهای امنیتی‌اش روبه‌رو می‌شود.

عوامل کلیدی مقابله با تهدیدات سایبری :

عوامل تأثیرگذار بر مقابله با تهدیدات سایبری به ترتیب:

- فرهنگ‌سازی و افزایش سطح آگاهی کاربران
- بومی‌سازی
- پدافند غیرعامل

- پدافند غیرعامل در حوزه سایبری

از آنجا که هیچگاه نمی‌توان امنیت را صد درصد برقرار نمود لذا حتی با رعایت نمودن کلیه موارد ذکر شده، امکان بروز حوادث غیرمترقبه و تهدیدات پیش‌بینی نشده وجود دارد لذا در اینجا اهمیت پدافند غیرعامل محرز می‌باشد. دفاع غیرعامل در واقع مجموعه تهدیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت گیرد چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب دیده را با کمترین هزینه فراهم آورد.

شناخت محیط فضای سایبری و حوزه آسیب‌پذیر کشور، اولین نکته از پدافند سایبری است. پس از شناخت، قدم بعدی پژوهش، طراحی و برنامه‌ریزی برای هر حوزه خاص است. فضای سایبر به شدت مبتنی بر علم و فناوری و دانش بنیان است. فرماندهان و مدیران این عرصه نیز به همان شدت باید متخصص و مسلح به دانش این فن باشند. دانش این فضا ترکیبی از علوم مختلف مانند رایانه، الکترونیک، ارتباطات، روانشناسی، جامعه‌شناسی و حقوق است همچنین فاکتورهای مهم در این مقوله نیز شامل موارد زیر می‌شود :

- کاربران و نیروی انسانی
- داده‌ها و اطلاعات
- روش‌ها و رویه‌های اجرایی
- نرم‌افزارهای رایانه‌ای
- سخت‌افزارهای رایانه‌ای

- جنگ سایبری از دیدگاه حقوق بین‌الملل:

وقتی جنگ سایبری از دیدگاه حقوق بین‌الملل در نظر گرفته می‌شود، شفاف‌سازی برخی اصطلاحات تخصصی بسیار حائز اهمیت می‌باشد، برخورد مسلحانه یعنی حملات مسلحانه و تهدید یا توسل به زور. حقوق بین الملل بطور عمده از اصطلاح برخورد مسلحانه به جای جنگ یا برخورد استفاده می‌کند.

از منظر جنگ سایبری، یکی از اسباب‌های کلیدی حقوق بین‌الملل، منشور سازمان ملل است که در کنار موارد دیگر، استانداردی را برای توسل به (یا منع توسل به) زور بین کشورها تعیین می‌کند. درحالیکه بطور عمومی ((تهدید یا توسل به زور)) منع گردیده است (ماده(٤)٢)، این منشور موارد استثناء را نیز در نظر گرفته است. به ویژه ماده ٤٢ به سازمان ملل اجازه می‌دهد تا برای حفظ یا اعاده صلح و امنیت بین‌المللی، تحریم‌هایی را اعمال نماید و در ماده ٥١، کشورهایی که درگیر دفاع از خود (جمعی) در برابر یک حمله مسلحانه هستند، مستثنی شده‌اند.

اگر یک عملیات سایبری آفندی یا یک سری از این عملیات به تنهایی بتوانند به آستانه حمله سایبری برسند، سطح مخاطره بطور معناداری برای طرف مهاجم تغییر می‌کند و در صورتیکه عملیات مورد سؤال منطبق با آستانه حمله مسلحانه نباشد، به طور قانونی از زور استفاده خواهد کرد (دفاع از خود تحت ماده ٥١ منشور ملل متحد). درک این مسئله بسیار حائز اهمیت است که هیچ الزامی برای تقارن و تناسب دفاع از خود وجود ندارد. اگر یکی از طرفین، عملیات سایبری را انجام دهد که سطحی از حمله مسلحانه را در پی داشته باشد، آنگاه طرف مقابل می‌تواند با موشک‌های کروز، اقدامات دریایی، عملیات سایبری یا ... مقابله کند. عوامل دیگری نیز وجود دارند که بایستی درنظر گرفته شوند از جمله تناسب پاسخ که لزوماً نوع زور اعمال شده را محدود نمی‌کنند. در حالیکه آستانه (مقیاس و اثرات) همچنان مورد بحث است، واضح است که جامعه حقوق بین‌الملل به طور کلی موافق این نکته است که عملیات سایبری می‌تواند به حمله سایبری ختم شود.

جنگ سایبری به عنوان یک قابلیت سایبری

میدان عملیات سایبری یا جنگ سایبری همچنان در حال توسعه بوده و بنابراین در چارچوب فناوری‌ها و نظام‌های جنگی از قبیل نبرد هوایی یا موشک‌های زمین به زمین جای نمی‌گیرد. هرگاه توسعه فناورانه با تاکتیک جدیدی راه خود را به میدان نبرد باز کند، این فرآیند آزمون و تجمیع تجربیات عملی بصورت طبیعی رخ می‌دهد.

قابلیت جنگ سایبری را می‌توان از دو جنبه متفاوت مورد توجه قرار داد. ابتدا جنگ سایبری را می‌توان بعنوان بخشی از عملیات اطلاعاتی در نظر گرفت، جایی که تأکید روی اطلاعات است. این یک رویکرد نرم است جایی که سایبر یکی از راه‌های اثرگذاری بر فرایند تصمیم (توانایی) دشمن می‌باشد. بعنوان مثال تغییر شکل دادن (جایگزینی محتوای سیستم هدف) با استفاده از زیرساخت ارتباطی دشمن برای انتشار اطلاعات (مثلاً ارسال پیام‌های متنی حاوی تبلیغات یا هشدار یک حمله بازدارندگی)، انحطاط یا از کار انداختن سیستم‌های ارتباطی با هدف انسداد اطلاعات و ... .

دومین رویکرد جنگ سایبری، فناوری را هدف قرار می‌دهد به ویژه فناوری اطلاعات که اثربخشی تاکتیک‌ها و تسلیحات سنتی را ارتقاء می‌بخشد. نقش عملیات آفندی سایبری، اداره (تخریب، انحطاط، مسدودسازی و ...) سیستم‌های دشمن است بطوریکه قابلیت جنگی آن‌ها بطور معناداری کاهش پیدا کند.

نتیجه‌گیری:

قابلیت نظامی جنگ سایبری دستخوش یک دوره رشد سریع در خصوص درک قابلیت اجراء و کاربرد هنجارهای مقرر هم بر حسب حقوق بین‌الملل و هم عرف نظامی شده است. کشورها مرزهای سیاست، قانون و فناوری را تجربه کرده تا به موازنه درست دست یابند که این موضوع یادآور بحث درباره جنگ‌های هوایی یک قرن پیش می‌باشد.

عملیات سایبری که در زمینه مخاصمات مسلحانه (بین المللی) صورت گرفته است تحت حقوق بین‌الملل می باشد. شاید مهمتر از همه این باشد که عملیات آفندی سایبری با مقیاس و اثر کافی می‌توانند به سطح حمله مسلحانه ختم شوند که باعث می‌گردد کشور قربانی، در دفاع از خود به زور متوسل شود. با شروع مخاصمه مسلحانه، تمامی عملیات نظامی سایبری بایستی از حقوق مخاصمات مسلحانه تبعیت کنند. لازم به ذکر است عملیات‌های سایبری بایستی منطبق با اصول تناسب، تمایز و ... صورت گیرند.

کشاورزی ارگانیک و غذای سالم

تهیه و تنظیم: پوریا پورپیغمبر (کارشناس امریه اداره کل پدافند غیرعامل)

منابع:
• کشاورزي ارگانيك (آلي) و فواید آن. حسین رزاقیان و محمد میرجلیلي. حوزه ترویج و نظام بهره‌برداري یزد. ۱۳۸۶
• سلامت و ایمنی محصولات کشاورزی ارگانیک. دکتر بهادر حاجی محمدی- دکتر گیلدا اسلامی- دکتر هنگامه زندی. مرکز تحقیقات سلامت و ایمنی غذا، دانشکده بهداشت، دانشگاه علوم پزشکی شهید صدوقی یزد. ۱۳۹۶
• بررسی عوامل مؤثر بر تمایل به پرداخت اضافی مصرف‌کنندگان خیار ارگانیک در شهر ارومیه. محمد خداوردیزاده. تحقیقات اقتصاد کشاورزي
• مروري بر ویژگي ارگانیك‌هاي غذا در صنایع تبدیلي. مریم میرلوحی و زهرا اسفندیاری. تحقیقات نظام سلامت. ۸ (۱ . ۱۳۹۱ ۳۴۹ ۳۵

مقدمه

با افزایش روز افزون جمعیت و نیاز به مواد غذایی بیشتر و همچنین توسعه علم و فناوری، رویکرد بشر به نهاده‌های غیرطبیعی و اغلب شیمیایی برای افزایش تولید محصولات کشاورزی تغییر فراوانی کرده است به گونه‌ای که امروزه کمتر محصولی را می‌توان یافت که به صورت طبیعی به دست مصرف کننده برسد. از سوی دیگر یکی از مشکلاتی که امروزه گریبان جوامع بشری را گرفته، افزایش سرطان، بیماری‌های مزمن، اختلالات کبدی و بیماری‌های تنفسی می‌باشد که در نتیجه ورود سموم دفع آفات نباتی و دیگر آلودگی‌های شیمیایی است که از خاک وارد مواد غذایی و در نهایت بدن انسان می‌شود و باعث بیماری‌های فوق می‌گردد. با بروز انواع و اقسام بیماری‌ها و مشکلات زیست محیطی که ناشی از بکارگیری نهاده‌های شیمیایی در کشاورزی است، ارزش کشاورزی ارگانیک بیش از پیش مشخص شده است.

کشاورزی ارگانیک یا کشاورزی غیر شیمیایی و یا کشاورزی بومی قصد دارد ضمن حفاظت از حاصلخیزی خاک و افزایش تولید محصول، کمترین اتکاء به استفاده از مواد شیمیایی را نیز داشته باشد.

ارگانیک یا آلی در معنای کلمه، ماده‌ای مشتق شده از موجودات زنده است ولی در کشاورزی و صنعت غذا ارگانیک یک روش تولید است که از اولین مراحل زنجیره تولید غذا یعنی آماده‌سازی زمین کشاورزی تا زمانی که غذا به صورت خام یا فرایند شده در بسته بندی به دست مصرف کننده می‌رسد را در بر می‌گیرد. طراحی اساس سیستم‌های تولید ارگانیک، تولید مقدار قابل قبولی از غذای مورد نیاز انسان با کیفیت بالا و با حداقل خسارت ممکن به محیط زیست و حیات وحش بوده است.

کشت ارگانیک قدیمی‌ترین نوع کشاورزی در روی کره زمین است و نگرش علمی و جدید به آن چیزی است که اجداد ما به آن عمل می‌کردند. این نوع کشاورزی براساس مدیریت صحیح خاک و محیط رشد گیاه استوار است در این نوع کشت به گونه‌ای عمل می‌شود که در تغذیه گیاه و درخت تعادل بین عناصر مورد نیاز در خاک به هم نخورد و هنگام رشد نیز نیاز به استفاده از سموم و آفت‌کش‌ها نباشد.

در این سیستم نسبت به منابع برگشت‌پذیر مورد بهره‌برداری از طبیعت درجه اطمینان بالایی وجود دارد و نوعی پایداری در درون آن نهفته است و پایداری نه تنها به معنی حفظ منابع تجدید پذیر مثل خاک، انرژی و کانی‌ها؛ بلکه پایداری زیست محیطی و حتی پایداری اجتماعی نیز در طراحی اصول این سیستم مورد توجه قرار گرفته است. وجود علامت ارگانیک بر بسته‌بندی غذا نشانگر این است که قوانین و استانداردهایی ویژگی در این سیستم‌های این غذا را تعریف نموده، تمام مراحل تولید مورد بازرسی قرار گرفته و مطابقت شرایط آن با قوانین و استانداردها به وسیله شرکت‌های معتبر و مستقلی تأیید شده است.

وضعیت کشت محصولات ارگانیک در جهان

قاره اقیانوسیه، استرالیا، آمریکای لاتین و شمالی، آسیا و کشورهای آفریقایی، بخشی از اراضی خود را به کشت محصولات ارگانیک اختصاص داده‌اند. در آسیا سطح زیر کشت ارگانیک به طور مقایسه‌ای کوچک است و در میان کشورهایی که بیشتر به تولید محصولات اهمیت می‌دهند می‌توان به هند، اکراین، چین و اندونزی اشاره کرد. در این میان کشور ژاپن مهمترین بازار محصولات ارگانیک منطقه آسیا است. در چین ابتدا بازار محصولات ارگانیک خوب نبوده اما به تدریج این بازار طرفداران خود را پیدا کرده است. به نظر می‌رسد در چند سال آینده تحولات عظیمی در این بخش اتفاق بیافتد. طبق اطلاعات فدراسیون بین‌المللی جنبش محصولات ارگانیک چین ۲۳ میلیون هکتار زمین گواهی شده ارگانیک دارد که حدود ۱۰% از کل زمین‌های کشت شده چین است. فروش محصولات ارگانیک در چین بیش از ۵۰% درصد رشد داشته است.

در قاره آفریقا ۳۸% محصولات ارگانیک توسط اوگاندا

تولید می‌شود و بیش از ۵۰ هزار مزرعه گواهی شده ارگانیک دارد. امروز اوگاندا بیشترین سود را از صادرات محصولات ارگانیک در قاره آفریقا می‌برد و بدلیل داشتن قیمت بالاتر برای محصول ارگانیک کشاورزان سود بیشتری را بدست می‌آورند لذا می‌توان در کشور عزیزمان ایران با برنامه‌ریزی و مدیریت صحیح از امکانات و پتانسیل خدادادی کشاورزی ارگانیک را که همانا کشاورزی آبا و اجدادی و سنتی خودمان است ترویج نماییم.

وضعیت کشت محصولات ارگانیک ایران

طبق اطلاعات کمیته محصولات ارگانیک، کل سطح کشت محصولاتی که در کشور ایران بدون استفاده از سموم و کودهای شیمیایی تولید شده‌اند حدود ۲۳۹ هزار و ٤٦٢ هکتار که شامل ۱۲۵ هزار و ۸۰۲ هکتار محصولات باغی و ۱۱۳ هزار و ٦٥٩ هکتار محصولات زراعی است و به طور کلی میزان سطح زیرکشت محصولات زراعی و باغی که تولید آن‌ها بدون استفاده از کود و سم انجام می‌گیرد به ترتیب ۱% و ۷/۲% از کل سطوح زیرکشت محصولات زراعی و باغی کشور را تشکیل می‌دهد.

ویژگی‌های کشاورزی ارگانیک

• مهمترین ویژگی‌های کشاورزی ارگانیک به دلیل الگو برداری آن از طبیعت می‌توان به صورت زیر برشمرد: حفظ حاصلخیزی خاک در دراز مدت از طریق نگهداری مقدار مواد آلی آن در حد مطلوب.
• بهبود فعالیت موجودات مفید زنده خاک
• استفاده از روش‌هایی چون تناوب زراعی، بکارگیری دشمنان طبیعی، ارقام مقاوم و زودرس برای مقابله با آفات، بیماری‌ها و علف‌های هرز به جای مصرف سموم های شیمیایی
• استفاده از کودهای آلی به جای کودهای شیمیایی

گیاهان تولید شده به روش ارگانیک سالم‌تر بوده و بعنوان غذاهای خوشمزه‌تر برای تغذیه انسان و حیوانات می‌توانند بکار رود. این محصولات خطر ابتلا به بیماری ها بویژه انواع سرطان‌ها را کم می‌کند، خاک را سالم نگه می‌دارد و به حفظ سلامت جوامع روستایی کمک می‌کند.

فواید کشاورزی ارگانیک

کشاورزی ارگانیک باعث بهبود محیط زیست، حفظ خاک و حذف کودهای شیمیایی می‌گردد. در کشاورزی ارگانیک علاوه بر اینکه باعث بهبود سلامت انسان‌ها می‌گردد باعث بهبود جمعیت جانوری و گیاهی خاک نیز می‌گردد. در روش های کشت ارگانیک نهاده‌های خارجی بسیار کم مورد استفاده قرار می‌گیرد. آلودگی‌های کشاورزی از قبیل آلودگی آب‌های زیرزمینی و خاک با کودهای شیمیایی، آفت‌کش و علف‌کش‌ها به مشکل بزرگی برای دنیا تبدیل شده و باعث انواع سرطان‌ها و بیماری‌ها گردیده است. در کشاورزی ارگانیک به دلیل عدم استفاده از آفت کش‌ها و علف‌کش‌ها این سموم از زنجیره غذاهای ارگانیک حذف می‌گردند. روش‌های ارگانیک تنها بر پایه احترام به طبیعت و مسالمت با محیط زیست و استفاده پایدار از آن بنا نهاده شده است.

راهکارهای تولید محصول سالم ارگانیک

برای زارعینی که از روش‌های معمول تولید استفاده می نمایند تولید محصول ارگانیک در یک سال به سادگی امکان پذیر نمی‌باشد و چندین سال باید از زراعت آن بگذرد تا کشاورزان یاد بگیرند که چگونه حاصلخیزی خاک را حفظ و یا با آفات و بیماری‌ها مبارزه کنند. ابتدا جلوگیری از زیان مالی امکان پذیر نمی‌باشد ولی می‌توان آن را به حداقل رساند. زارع باید اکوسیستم محیطی که در آن زراعت می‌کند به خوبی بشناسد و روش‌های جدید کشت و مدیریت خاک را که دارای اهمیت زیادی می‌باشد بیاموزد.

بدون شک عدم استفاده از کود شیمیایی، علف‌کش و سم منجر به کاهش راندمان تولید می‌گردد. مقدار کاهش عملکرد به میزان قابل توجهی بستگی به سطح حاصلخیزی خاک، جمعیت علف‌های هرز و شیوع آفات و بیماری‌ها دارد. در یک زراعت به روش معمول اگر خاک از نظر مواد آلی غنی باشد به تقویت‌کننده دیگری به غیر از ازت نیاز نیست در این حال چنانچه زراعت قبلی حبوبات بوده کاهش راندمان به حداقل خواهد رسید. از نقطه نظر بیماری‌ها و آفات اگر چه میزان کاهش تولید به میزان زیادی بستگی به شدت آلودگی دارد. اما مبارزه به روش غیرشیمیایی به طوری که مورد تأیید کارشناسان فنی باشد می‌تواند از شدت آلودگی و کاهش راندمان بکاهد.

ویژگی‌های تغذیه‌ای

در این بخش ویژگی‌های تغذیه‌ای محصولات ارگانیک از نظر ارزش غذایی، نتایج مطالعات بیولوژیک در مورد خواص سودمند آن‌ها و خواص حسی مورد بررسی قرار می‌گیرند.

ارزش غذایی

دامنه اختلافات در نتایج بدست آمده از مطالعات و مقایسه ارزش غذایی مواد ارگانیک با مواد غذایی رایج بسیار زیاد بوده است؛ به طوری که تأثیر سیستم کاشت بر مواد مغذی ناچیز است و یا به شدت تحت تأثیر سایر عوامل مؤثر بر ترکیبات گیاه در محیط آزمایش قرار می‌گیرد. ژنتیک، شرایط آب و هوایی، زمان برداشت، شرایط منطقه‌ای و نوع خاک مواردی هستند که به شدت در میزان ترکیبات مغذی اثر گذار می‌باشند و در مقایسه‌ها باعث ایجاد خطا می‌شوند. با این حال، در مواردی توافق نظر بیشتری وجود دارد، که از آن جمله می‌توان به کمیت و کیفیت پروتئینی و میزان نیترات اشاره کرد.

ادعا شده است که محصولات ارگانیک دارای پروتئین خام کمتر ولی با ارزش تغذیه‌ای بیشتر از نظر نسبت اسیدهای آمینه ضروری به غیرضروری هستند و در شرایط یکسان، نیترات کمتری در آن‌ها تجمع پیدا می‌کند. علت هر دو به ساختمان خاک و نوع کود مورد استفاده در این سیستم باز می‌گردد؛ چرا که ازت در کود آلی به صورت پیوند شده در ترکیب آلی وجود دارد و در طی مراحل رشد گیاه به آرامی فرایند معدنی شدن را طی می‌کند و به شکل نیترات در گیاه جذب می‌شود؛ در حالی که کودهای شیمیایی مقدار بالایی ازت قابل دسترس و محلول برای گیاه فراهم می‌کنند و بنابراین شرایط مناسبی برای تجمع نیترات و پروتئین در گیاه فراهم می‌شود. علاوه بر این، ترکیبات ناشی از فرایند اکسیداسیون در کود آلی خود اثر موقتی در جلوگیری از نیتریفیکاسیون دارند.

مسأله دیگری که به تازگی مورد توجه قرار گرفته است، احتمال بالاتر بودن مواد زیست فعال مانند ویتامین‌های آنتی اکسیدان و ترکیبات فنولیک در محصولات ارگانیک می‌باشد. در این رابطه برخی از مطالعات از بالاتر بودن ترکیبات فنولیک و آنتی اکسیدان‌های طبیعی در آب گوجه‌فرنگی و فرآورده‌های آن مثل سس گوجه ارگانیک نسبت به نمونه تجاری آن‌ها بررسی کرده‌اند.

برای مثال در یک مطالعه بازار بنیاد با بررسی تعداد قابل توجهی از انواع سس گوجه‌فرنگی عرضه شده در بازار مشخص شد که سس گوجه ارگانیک به طور قابل توجهی نسبت به انواع تجارتی عرضه شده در رستوران‌ها، فروشگاه‌های زنجیره‌ای و شرکت‌های بزرگ تجارتی خاصیت ضد اکسایشی بیشتری نشان می‌دهد. نکته قابل توجه در این مطالعه بالاتر بودن این قابلیت در بخش آب دوست عصاره سس می‌باشد که نشان دهنده بیشتر بودن غلظت آنتی اکسیدان‌های محلول در آب مثل ترکیبات فلاونوئیدی است. در حالی که در این مطالعه انتظار می‌رفت که مقدار لیکوپن و خواص آنتی اکسیدانی وابسته به آن در نمونه ارگانیک بیشتر باشد.

ایمنی غذایی

مزیت روشن و واضح محصولات ارگانیک، کمتر بودن باقیمانده سموم، مواد دارویی و هورمون‌ها در آن‌ها می‌باشد. البته هیچ‌گاه عاری بودن کامل مواد ارگانیک از سموم کشاورزی توسط شرکت های صادرکننده مجوز تضمین نمی‌شود؛ چرا که همواره مقداری از سموم پایدار در طبیعت مانند انواع سموم آلی کلره و سموم آلی فسفاته از طریق محیط وارد گیاه می‌شوند.

مسأله دیگری که شاید بتوان آن را تهدیدی جدی برای امنیت غذایی محصولات ارگانیک به حساب آورد، وجود باقیمانده‌های سموم قارچی بر روی محصولات ارگانیک است. ممنوعیت استفاده از قارچ‌کش‌ها احتمال حضور این سموم را افزایش می‌دهد. علاوه بر این، خسارت ایجاد شده توسط حشرات و جوندگان باعث تسهیل ورود این سموم به بافت داخلی محصولات کشاورزی می شود. مطالعات در این زمینه، بالاتر بودن سمومی چون داکسی نیوالنول در غلات ارگانیک، پاتولین در آب سیب و آب سیب پاستوریزه ارگانیک و آفلاتوکسین در مغزها و کره بادام زمینی ارگانیک را گزارش کرده‌اند.

سایر فواید

– در کشاورزی ارگانیک آب توسط مواد شیمیایی آلوده کننده مانند کودهای مصنوعی آلوده نمی‌گردد.
– در کشاورزی ارگانیک فرسایش خاک تا ۵۰ درصد کاهش می‌یابد و حاصلخیزی خاک حفظ می‌گردد.
– در کشاورزی ارگانیک به علت عدم استفاده از سموم آفت‌کش و علف‌کش تنوع زیستی ۵۷ درصد بیشتر است.
– کشاورزان در معرض سموم و مواد آلوده کننده کمتری قرار می‌گیرند.

فواید مصرف مواد غذایی ارگانیک

تولیدکنندگان محصولات ارگانیک از استانداردها و دستورالعمل‌های بسیار سخت گیرانه تبعیت می‌کنند به همین دلیل احتمال آلوده شدن این گونه محصولات به هرگونه مواد شیمیایی و سمی منتفی می‌باشد. لذا:

- ارزش غذایی بالاتری دارند، میزان ویتامین C، کلسیم، منیزیم، آهن و فسفر در مواد غذایی ارگانیک بیشتر است.
- مواد غذایی ارگانیک از تجمع و تشکیل مواد مضر بیماری‌زا در بدن جلوگیری می‌کند.
- محصولات ارگانیک فراوری شده سالم‌تر بوده و فاقد افزودنی‌های غذایی می‌باشند.
- خوشمزه و خوش‌طعم‌تر هستند.

پیامدهای کشاورزی غیر ارگانیک ومصرف محصولات آن

در کشاورزی غیر ارگانیک بیش از ۳۰۰ ترکیب شیمیایی خطرناک و مصنوعی نظیر آفت‌کش‌ها، علف‌کش‌ها و کودهای شیمیایی به منظور کنترل آفات و حشرات و حاصلخیزی خاک استفاده می‌گردد که بقایای این مواد پس از ورود به بدن می‌تواند موجب مشکلات عدیده ای گردد. از آن جمله بروز نقص‌های مادرزادی، تولد نوزاد با وزن کم، سقط جنین، بلوغ زودرس و یا دیر رس، تغییر در رفتار جنسی، کاهش تعداد اسپرم مردان، کاهش باروری، ضعف عضلانی، کاهش حافظه، آسیب به سیستم عصبی و مغز، کاهش کارآیی سیستم ایمنی بدن و سرطانزایی. یافته‌ها حاکی از آن است که ۶۰ درصد سموم دفع آفات، ۹۰ درصد قارچ‌کش‌ها و ۳۰ درصد حشره‌کش‌ها سرطانزا می‌باشند. (استفاده بی‌رویه از کودهای شیمیایی و آفت‌کش‌ها موجب می‌شود تا آفات نسبت به سموم مقاوم گردیده و آفت‌های جدید ظاهر گردند) آزمایش‌ها حاکی از آن است که از میان مواد غذایی که به روش سنتی عرضه می‌گردد سیب، هلو، گلابی، سیب زمینی، زردآلو، اسفناج، توت فرنگی، شلیل، انگور، کرفس، تمشک و گیلاس بیشترین و کیوی، انبه، موز، پیاز، آناناس، گل کلم، ذرت، نخود فرنگی، هندوانه، آلو و بادمجان کمترین آلودگی را به باقیمانده آفت‌کش ها دارند.

مطالعات بیولوژیکی در مورد محصولات ارگانیک

به طور کلی نتایج مطالعات بیولوژیکی در مقایسه با مطالعه ارزش غذایی از طریق اندازه‌گیری مواد مغذی در محصولات ارگانیک نتایج بهتر و روشن‌تری داشته است و در میان محققین توافق نظر بیشتری در این زمینه وجود دارد. از جمله اثرات مثبت مصرف مواد ارگانیک مثل افزایش در تشکیل تخمک در جنس ماده، جنین در خرگوش و افزایش تحرک اسپرم گاو نر بوده است.

در حیوانات آزمایشگاهی تازه متولد شده، کاهش مرگ و میر پیش از تولد و دوران نوزادی گزارش شده است و علاوه بر این افزایش سلامتی و کارایی به خصوص افزایش تولید بیشتر در گاوهای ارگانیک را می‌توان مشاهده نمود. رشد و وزن‌گیری بهتر در حیوانات جوان و در طی دوره نقاهت بیماری و یا در زمانی که به اختلالات عصبی دچار بوده‌اند و یا در پرندگانی که از نظر تغذیه‌ای در وضعیت بدی قرار داشتند، نیز از جمله اثرات مثبت مصرف مواد ارگانیک گزارش شده است.

برخی از مطالعات بیولوژیک انسانی شاخص‌های حفاظتی مثل قابلیت آنتی اکسیدانی خون یا پایداری سلول‌های خونی را در برابر عوامل آسیب رساننده به نوکلئوتیدها بررسی کرده‌اند. در این زمینه یک مطالعه انسانی را می‌توان مثال زد که در آن بررسی مقایسه‌ای مصرف سیب ارگانیک با سیب تهیه شده در سیستم متداول کاشت تأثیر قابل توجهی بر شاخص ضد اکسیدانی در افراد نشان نداد. البته باید در نظر داشت مطالعه اخیر تفاوت قابل توجهی از نظر میزان کل ترکیبات فنولیک یا میزان هر یک از گروه‌های شاخص این ترکیبات بین دو گروه سیب تولید شده در دو سیستم ارگانیک و تجاری مشاهده نشده بود. نکته قابل توجه در مطالعه اخیر، افزایش اثر حفاظتی بر نوکلئوتیدها در هر دو گروه مصرف‌کننده پس از دوره آزمایش و مصرف سیب در افراد مورد مطالعه بود.

نتیجه‌گیری

مصرف هزاران تن انواع سموم و مواد شیمیایی در حوزه‌های کشاورزی، سلامت جامعه تهدید می‌شود. ضرورت پرداختن به شرایط مخاطره‌آمیز و ترویج و تولید محصولات ارگانیک در کشور بیشتر احساس می‌شود. اگر چه استفاده از این نام در جوامع مصرف کننده برای خریداران، محصولی با کیفیت بالاتر را تداعی می‌کند و از جهاتی نیز ممکن است ارزش غذایی و امنیت غذایی بالاتری نسبت به مواد رایج داشته باشد ولی قوانین و استانداردهای اصلی که تولید این محصولات بر اساس آن‌ها صورت می‌گیرد به شدت استفاده از جملاتی مانند غذای برتر یا سالم‌تر را در تبلیغات ارگانیک منع کرده‌اند. مطرح شدن و موفقیت چنین سیستم‌هایی در جوامع پیشرفته که با بکارگیری علم و تکنولوژی غنی به حداکثر تولید دست یافته‌اند، نشان دهنده اهمیتی است که انسان امروزی برای سلامتی و امنیت خود و محیط زیست اطرافش قایل است؛ به طوری که با نوعی بازگشت به روش های سنتی، درصدد است با هزینه بیشتر و بازده کمتر در تولید غذای سالم تری بدست آورد.

صرف نظر از این که این سیستم‌ها تا چه اندازه در رسیدن به اهداف خود در راستای کشاورزی پایدار موفق هستند، اهمیت و حمایت دولت از آن‌ها قابل توجه است و نشان‌دهنده نگرانی دولت از کاربرد بی رویه مواد شیمیایی مصنوعی در فرآورده‌های کشاورزی و عواقب احتمالی آن می‌باشد. به طور قطع در کشور ما بکارگیری سیستمی مانند ارگانیک در وضعیت فعلی امکان پذیر نیست؛ چرا که در کشاورزی همچنان افزایش تولید در درجه اول اهمیت قرار دارد، ولی افزایش سطح آگاهی کشاورزان، مصرف‌کنندگان و دقت و نظارت سازمان‌های مسئول با بکارگیری تدابیر قانونی و جدی، می‌تواند زمینه‌ای برای اجرای سیستم‌های حد واسطی مانند کشاورزی پایدار در کشور ما باشد.

آسیب‌پذیری

آسیب‌پذیری بحرانی *SigRed* در ویندوز سرور

آسیب‌پذیری بحرانی کرم گونه در محصول مایکروسافت ویندوز سرور کشف شده که این آسیب‌پذیری در مجموعه بروزرسانی‌های ماه جولای رفع شده و دارای درجه حساسیت بالا ۱۰ *CVSS* می‌باشد. این آسیب‌پذیری مربوط به *Windows DNS Server* و یک سرویس سیستم نام دامنه در سیستم‌عامل ویندوز است. آسیب‌پذیری با نام *SigRed* نیز معرفی شده است که بدلیل قابلیت کرم گونه آن، یک عامل مخرب می‌تواند درون شبکه سازمان، بدون تعامل کاربر، خود را گسترش دهد.

یک مهاجم با سوءاستفاده از این آسیب‌پذیری می‌تواند دستورهای *DNS* مخرب ایجاد کرده و کد دلخواه اجرا کند که در نهایت منجر به نفوذ به کل زیرساخت مورد هدف می‌شود. این آسیب‌پذیری تمامی نسخه‌های ۲۰۰۳ تا ۲۰۱۹ ویندوز سرور را تحت تأثیر قرار می‌دهد.

آسیب‌پذیری بدلیل نحوه تجزیه یک درخواست *DNS* ورودی و درخواست‌های ارسالی در *Windows DNS Server* بوجود آمده است. به طور خاص، ارسال یک پاسخ *DNS* با یک رکورد *SIG* بیش از ٦٤ کیلوبایت می‌تواند منجر به سرریز بافر پشته کنترل شده شود. در صورتی که یک مهاجم یک درخواست *DNS* مخرب را فعال کند، باعث ایجاد سرریز بافر مبتنی بر پشته می‌شود که می‌تواند هکر را قادر به تحت کنترل درآوردن سرور و انجام اقداماتی چون دستکاری ایمیل‌ها و ترافیک کاربران، از دسترس خارج کردن سرور، استخراج اطلاعات احراز هویت کاربران و غیره شود.

از آنجایی که این سرویس در سطح دسترسی بالایی اجرا می‌شود، در صورت نفوذ به آن مهاجم می‌تواند سطح دسترسی *Domain Administrator* را بدست آورد. در سناریوهای حمله محدودی این آسیب‌پذیری را می‌توان از طریق جلسات مرورگر و با دسترسی از راه دور مورد سوءاستفاده قرار داد. آسیب‌پذیری‌های کرم گونه دارای قابلیت گسترش از طریق یک بدافزار بین سیستم‌های آسیب‌پذیر و بدون تعامل کاربران هستند. *Windows DNS Server* یک ویژگی شبکه اصلی است و احتمال بهره‌برداری مهاجمین از این آسیب‌پذیری بسیار بالا است.

پایان پشتیبانی از *Adobe Flash Player* تا پایان سال میلادی

شرکت *Adobe* قصد دارد تا پایان سال میلادی جاری از کاربران بخواهد تا *Flash Player* را از رایانه‌های خود حذف کنند. نرم‌افزار *Flash Player* در تاریخ ۳۱ دسامبر ۲۰۲۰ از رده خارج خواهد شد و پشتیبانی آن متوقف می‌شود.

شرکت *Adobe* در یک صفحه مربوط به اطلاع‌رسانی در خصوص پایان عمر (*EOL*) نرم‌افزار *Flash Player* اعلام کرد که پس از تاریخ برنامه‌ریزی شده برای توقف پشتیبانی این نرم‌افزار، هیچ بروزرسانی جدیدی برای آن منتشر نخواهد و تمامی لینک‌های آن از وب‌سایت این شرکت حذف خواهد شد.

Adobe همچنین اعلام کرد که محتواهای مبتنی بر *Flash* پس از تاریخ پایان عمر آن مسدود خواهند شد. این موضوع نشان می‌دهد که این شرکت قصد دارد به طور کامل از استفاده کاربران از آن در سال آینده جلوگیری کند.

این اقدامات *Adobe* به این دلیل است که *Flash Player* همواره مورد هدف هکرها و توسعه‌دهندگان بدافزار قرار گرفته است. هنگامی که *Flash Player* به تاریخ پایان عمر خود در پایان سال میلادی برسد، *Adobe* به روزرسانی‌های جدید امنیتی را برای آن ارائه نخواهد کرد، بنابراین کاربران *Flash* در معرض آسیب‌پذیری‌ها و حملات جدید قرار خواهند گرفت.

تاریخ پایان عمر *Flash Player* اولین بار در جولای ۲۰۱۷ اطلاع‌رسانی شد که بسیاری از توسعه‌دهندگان پس از آن کدهای خود را به *HTML۵* و تکنولوژی‌های مبتنی بر جاوااسکریپت منتقل کردند. درصد استفاده کنندگان *Flash* هم اکنون بسیار پایین است. در حال حاضر تنها ۲,٦ درصد از وب‌سایت‌های کنونی از کدهای *Flash* استفاده می‌کنند، درصورتی که در اوایل سال ۲۰۱۱ سهم بازار آن ۲۸.۵ درصد بوده است.

مهمترین به‌روزرسانی‌های ماه جاری شرکت‌های تولید کننده سخت افـزار و نرم افـزار

شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی می منتشر کرد. این اصلاحیه‌ها در مجموع، ۱۲۳ آسیب‌پذیری را در سیستم عامل *Windows* و برخی دیگر از سرویس‌ها و نرم‌افزارهای مایکروسافت ترمیم می‌کنند.

درجه حساسیت ۱۸ مورد از آسیب‌پذیری‌های ترمیم شده حیاتی و ۱۰۵ مورد از آن‌ها مهم اعلام شده است. تعداد آسیب‌پذیری ترمیم شده توسط مجموعه اصلاحیه‌های این ماه پس از ماه ژوئن ۲۰۲۰ که در جریان آن ۱۲۹ ضعف امنیتی در محصولات مایکروسافت ترمیم شدند بی‌سابقه است.

از نکات قابل توجه در خصوص مجموعه اصلاحیه‌های این ماه، ترمیم یک آسیب‌پذیری روز- صفر در بخش سرویس‌دهنده *DNS* سیستم عامل *Windows* است. این آسیب‌پذیری که بر اساس استاندارد *CVSS* به آن بالاترین شدت حساسیت (۱۰ از ۱۰) تخصیص داده شده از باگی در نحوه پیاده‌سازی نقش سرویس‌دهنده *DNS* در تمامی نسخ *Windows Server* – از ۲۰۰۳ تا ۲۰۱۹ – ناشی می‌شود. بهره‌جویی از آسیب‌پذیری مذکور، مهاجم را قادر به اجرای کد به‌صورت از راه دور می‌کند. نظر به نقش کلیدی سرویس‌دهندگان *DNS* در سطح شبکه و در اکثر مواقع ارتباط تمامی ایستگاه‌های کاری با آن‌ها، بکارگیری این آسیب‌پذیری جدی در بدافزارهای از نوع کرم محتمل دانسته شده است.

همچنین سه آسیب‌پذیری «حیاتی» در *Edge* و *VBScript Engine* مهاجم را قادر به اجرای کد از راه دور می‌کند. هدایت کاربر به یک صفحه اینترنتی حاوی کد مخرب از جمله سناریوهای احتمالی در بهره‌جویی از این آسیب‌پذیری است. در صورت موفقیت مهاجم در سوءاستفاده از آسیب‌پذیری مذکور امکان اجرای کد به‌صورت از راه دور بر روی دستگاه قربانی با سطح دسترسی کاربر جاری فراهم می‌شود.

در ماه آوریل یک محقق امنیتی سه آسیب‌پذیری جدی در فرایند موسوم به *Deserialization* محصول *WebSphere Application Server* را شناسایی و وجود آن‌ها را به *IBM* گزارش کرد.

دو مورد از آن‌ها با شناسه‌های *CVE*-۲۰۲۰-٤٤٤٨ و *CVE*-۲۰۲۰-٤٤٥٠ آسیب‌پذیری‌هایی از نوع «اجرای کد به‌صورت از راه دور» هستند که به آن‌ها درجه حساسیت «حیاتی» تخصیص داده شده است. مورد سوم با شناسه *CVE*-۲۰۲۰-٤٤٤٩ درجه حساسیت «بالا» نیز ضعفی از نوع «افشای اطلاعات» گزارش شده است.

در پی نقص بحرانی موجود در فایروال *PAN-OS* که به واسطه آن مهاجمان قادرند فرآیند احراز هویت را در این فایروال دور بزنند، شرکت *Palo Alto* اقدام به رفع این آسیب‌پذیری کرده است. هنگامی که احراز هویت *SAML* فعال و قابلیت *'Validate Identity Provider Certificate'* غیرفعال باشد، تأیید هویت نادرست در *PAN-OS SAML*، مهاجم را قادر می‌سازد تا به منابع شبکه دسترسی پیدا کند.

گفتنی است که برای اکسپلویت این آسیب‌پذیری، مهاجم باید به سرور آسیب‌پذیر دسترسی داشته باشد. کمپانی مربوطه اعلام کرده است که در صورت عدم استفاده از *SAML* در فرآیند احراز هویت و نیز غیر فعال بودن قابلیت *Validate Identity Provider Certificate* در *SAML Identity Provider Server Profile*، این آسیب‌پذیری اکسپلویت نخواهد شد.

معرفی کتاب حوزه پدافند عمومی

کتاب کلیات در دفاع غیرعامل، حاصل تلاش سید محمد میرسمیعی است، جهت تجمیع مباحث مختلف مرتبط با پدافند غیرعامل که در یک مجموعه جامع با نام مجموعه کتاب‌های شعله‌های سپید گردآوری شده است.

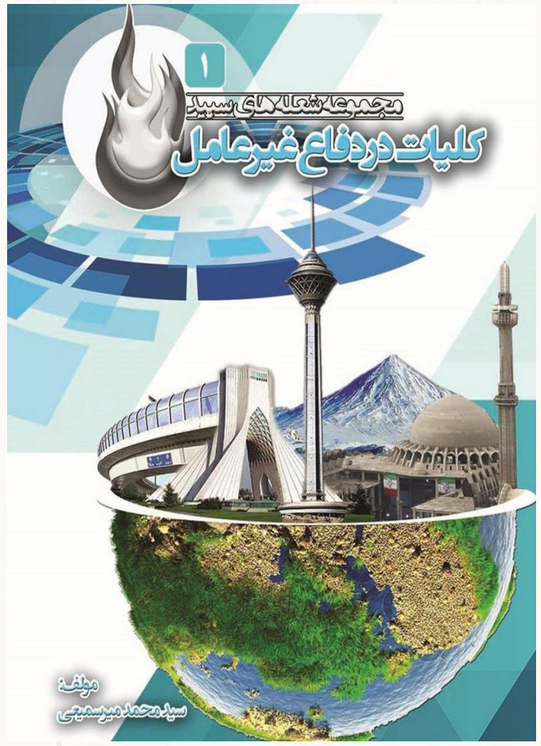
با توجه به اقدامات اخیر در جنگ‌ها و پیشرفت‌های فنّاوری، توجه به مسئله پدافند غیرعامل حائز اهمیّت بوده و لازم است به منظور دستیابی به اهداف و اصول پدافند غیرعامل، فرهنگ پدافند غیرعامل در تمام سطوح و بخش‌های مختلف توسعه یابد تا با بهره‌گیری از آن، نیروی انسانی، تأسیسات و تجهیزات حساس و حیاتی در زمان تهدیدات گسترده دشمن حفظ گردد.

در طول تاریخ چند هزار ساله بشری انسان و جوامع انسانی همواره در تهدید جنگ و خشونت‌های حاصل از آن بوده به طوری که در قرن بیستم بیش از ۲۲۰ جنگ به وقوع پیوسته که بیش از ۲۰۰ میلیون تلفات انسانی در بر داشته است و تنها در طی ٦۹ سال یعنی طی سال‌های ۱۹٤۵-۲۰۱٤ در روی کره زمین چند هفته بدون جنگ بوده است.

مطالعات و بررسی‌های تاریخی از جنگ‌های گذشته که در کتاب آمده است، نشان می‌دهد که کشورهایی که طعم خرابی و خسارات ناشی از جنگ را چشیده‌اند برای حفظ سرمایه‌های ملی و منابع حیاتی خود توجه خاص و ویژه‌ای به پدافند غیرعامل نموده و در راهبرد دفاعی خود جایگاه والایی برای آن قائل شده‌اند.

توجه به پدافند غیرعامل در مقابله با تهدیدات و تقلیل خسارات ناشی از حملات کشورهای مهاجم، امری بسیار مهمّ و ضروری است و باید جهت جلوگیری از آسیب‌پذیری‌های اقتصای، سیاسی، فرهنگی و اجتماعی و امنیت مراکز حیاتی و مهم کشور از قبیل پالاشگاه‌ها، نیروگاه‌ها و ... به پدافند غیرعامل روی آورد.

اندیشه تهیه و تدوین یک مجموعه جامع در زمینه دفاع غیرعامل با نام شعله‌های سپید که برگرفته از فرمایشات فرماندهی معظم کل قوا امام خامنه‌ای عزیز (پدافند غیر عامل باید همچون شعله بلند شود) است، که همواره در راستای ارتقاء دانش دفاعی فرماندهان، مدیران، رؤسا، اساتید و دانشجویان است. زیرا مؤلف معتقد است که گام اوّلیه، اصلی و زیربنایی که نقش محوری و تعیین کننده در شروع و استمرار و تسهیل اقدامات بعدی خواهد داشت، آموزش، ایجاد فرهنگ، شناخت و باور در فرماندهان، مدیران و مسئولان سطوح عالی و میانی و مخاطبان ذیربط سازمان‌های نظامی و غیرنظامی کشور است.



جلد اول این مجموعه با نام کتاب کلیات در دفاع غیرعامل و با ٦ فصل در حوزه کلیات در دفاع غیرعامل است. هدف حفاظت مراکز حیاتی و حساس و سرمایه‌های ملّی و استقلال کشور در برابر تهدیدات بالقوه و بالفعل موجود است تا دشمنان را مأیوس نماییم.

طرح‌های کسر خدمت سربازی

به اطلاع می‌رساند که سازمان پدافند غیرعامل کشور (مرکز مطالعات پدافند غیرعامل کشور و مرکز مطالعات فنی و مهندسی پایداری ملی کشور) برای دانش‌آموختگان و فارغ‌التحصیلان مقاطع کارشناسی ارشد و دکتری طرح‌هایی برای کسر خدمت سربازی و نخبگی (جایگزین خدمت سربازی) در نظر گرفته است. علاقمندان می‌توانند علاوه بر مراجعه به وب‌سایت‌های مربوطه با مراجعه به اداره کل پدافند غیرعامل استانداری آذربایجان شرقی از روند ثبت‌نام مطلع شوند.

وب سایت مرکز مطالعات فنی و مهندسی پایداری ملی کشور: http://www.mafpa.ir

وب سایت مرکز مطالعات پدافند غیرعامل کشور: http://www.pdrc.ir

سایت های مرتبط با پدافند غیرعامل

وب سایت پایداری ملی
http://www.paydarymelli.ir

مرکز مطالعات پدافند غیرعامل
http://www.pdrc.ir

استانداری آذربایجان شرقی - پدافند غیرعامل
http://www.ostan-as.gov.ir/Page/٤٢/

پلیس فتا
http://www.cyberpolice.ir

مرکز مطالعات فنی و مهندسی پایداری ملی
http://www.mafpa.ir