توسعه سواد سایبری گامی جهت حفاظت سایبری در عرصه پدافند غیرعامل کشور

احمد جان پرور[1]
ریحانه صالح‌آبادی[2]

تاریخ دریافت: ۱۳۹۵/۰۴/۲۰ تاریخ پذیرش: ۱۳۹۵/۶/۱۵

چکیده

با شکل‌گیری و توسعه فضای سایبر زمینه برای ایجاد مسائل و چالش‌هایی برای امنیت، منافع و هویت ملی ناشی از حضور و فعالیت افراد، گروه‌ها و حکومت‌ها به وجود آمده است. بر این مبنا حکومت‌ها برای استفاده از ظرفیت‌های فضای سایبر و از سوی دیگر کاهش آسیب‌ها و تهدیدات ناشی از آن راهبردهای مختلفی نظیر کاهش سرعت و غیره در پیش‌گرفته‌اند که شواهد موجود نشان‌دهنده آن است که این راهبردها به دلایل مختلف نتواسته است مفید واقع شود. ازجمله این تلاش‌ها که مقاله حاضر مبتنی بر آن هدف پیش رفته است توسعه سواد سایبری جهت حفاظت سایبری در عرصه پدافند غیرعامل می‌باشد. سؤال اصلی مقاله حاضر که در پی پاسخ‌دهی به آن است عبارت است از اینکه آیا می‌توان از توسعه سواد سایبری به‌عنوان گامی جهت حفاظت سایبری در عرصه پدافند غیرعامل کشور بهره برد؟ فرضیه تحقیق نیز بدین‌صورت است که به نظر می‌رسد رشد توسعه سواد سایبری در جامعه، بین نیروهای انتظامی، کارکنان و ... می‌تواند درروند حفظ فضای سایبر مهم تلقی گردد. بر این مبنا، مقاله حاضر با روشی توصیفی و تحلیلی و با بهره‌گیری از اطلاعات کتابخانه‌ای و اینترنتی راهبرد توسعه سواد سایبری را به‌عنوان گامی جهت حفاظت سایبری در عرصه پدافند غیرعامل کشور جهت کاهش آسیب‌ها و تهدیدات فضای سایبر مطرح می‌کند. نتایج حاصل از مقاله حاضر نشان‌دهنده آن است که با توجه به اینکه راهبرد مبتنی بر ماهیت بسترسازی و پایه‌ای می‌باشد با افزایش آگاهی در میان افراد، جامعه، کارکنان و کارمندان سازمان‌ها و نهادهای دولت، نیروهای نظامی و انتظامی می‌توان تا حدود زیادی بستر لازم برای کاهش تأثیرات آسیب‌های سایبری در قالب حفاظت سایبری در عرصه پدافند غیرعامل کشور فراهم آورد.

واژگان کلیدی: *سواد سایبری، حفاظت سایبری، پدافند غیرعامل.*

---

۱. استادیار جغرافیای سیاسی دانشگاه فردوسی مشهد (janparvar@um.ac.ir)

۲. کارشناس ارشد جغرافیای سیاسی دانشگاه فردوسی مشهد، نویسنده مسئول (Reyhane.salehabadi@gmail.com)

مقدمه

بهره‌برداری و پیوند روزافزون افراد و حکومت‌ها به فضای سایبر در ابعاد مختلف اقتصادی، علمی، فرهنگی، سرگرمی و ... ضمن به وجود آوردن فرصت‌های فراوان زمینه برای ایجاد مسائل و مشکلات متعددی را فراهم آورده است. ازجمله سرقت اطلاعات محرمانه حساب‌های بانکی، سرقت تصاویر و عکس‌های شخصی و ... همچنین، در کنار این مسائل می‌تواند آسیب‌ها و مشکلات دیگری نظیر سردرگمی و اغتشاش ذهنی، کمرنگ شدن ارتباطات اجتماعی، منزوی شدن و فردیت گرایی، افزایش خشونت، اعتیاد به اینترنت، گوشه‌گیری و عدم توسعه مهارت-های اجتماعی، آسیب‌های جسمی، مسائل چشمی؛ مسائل مچ دست؛ مسائل کمری؛ مسائل دیگر جسمی؛ چاقی؛ توسعه بیماری‌های گردن؛ توسعه بیماری‌های پا؛ آسیب دیدن دستگاه گوارش؛ صدمه به سیستم اسکلتی در اثر نشستن مداوم و غیراستاندارد در جلوی مانیتور و ... را سبب گردد (جان پرور، ۱۳۹۰: ۱۵۹-۱۵۶). در جهان امروز همه‌چیز با سرعت بالایی در حال دگرگونی است و همه حکومت‌ها و کشورها در تکاپوی نوسازی و بهبود خود برای انطباق با این وضعیت جدید هستند. این تغییرات و دگرگونی‌ها به‌صورت‌های مختلف حکومت‌ها را تحت تأثیر قرار داده و آن‌ها را در برخی زمینه‌ها دچار چالش کرده و در برخی زمینه‌های دیگر فرصت‌هایی برای آن‌ها فراهم آورده است. بسیاری از مردم اهمیت و تأثیر فناوری اطلاعات را در زندگی روزمره خود درک کرده‌اند و به دنبال دستیابی به زوایای مختلف آن هستند. درواقع، ورود این فناوری به ابعاد مختلف زندگی تک‌تک افراد امری اجتناب‌ناپذیر است و تمامی افراد دیر یا زود می‌بایست با ابزارهای آن آشنا شوند و کار با آن را آغاز نمایند. در این راستا «مهارت‌های» استفاده از رایانه نقش مهمی خواهند داشت. بدین معنی که کسانی که می‌خواهند از فواید فناوری اطلاعات بهره‌مند گردند، می‌بایست حداقل مهارت‌ها برای ارتباط مؤثر با این وسیله و استفاده از آن را داشته باشند. اگر مهارت‌های کار با رایانه را «مهارت‌های رایانه‌ای» بنامیم، می‌توان گفت مجموعه‌ای از ابتدایی‌ترین و پایه‌ای‌ترین مهارت‌های رایانه‌ای، تشکیل‌دهنده «سواد رایانه‌ای» یک فرد خواهند بود (سلطانی فر، ۱۳۸۷: ۶۲). سواد رایانه‌ای، شناخت اساسی چگونگی کارکرد رایانه و کار با آن است. با ورود به عصر اطلاعات و تشکیل جوامع اطلاعاتی وجود مهارت‌های لازم برای جستجو، استخراج و استفاده از اطلاعات امری ضروری برای شهروندان جامعه محسوب می‌گردد. این‌گونه مهارت‌ها در واژه سواد اطلاعاتی جمع می‌گردد. واژه سواد اطلاعاتی برای اولین بار توسط زورکوسکی در سال ۱۹۷۴ مطرح گردید. واژه‌های دیگری نیز در کنار «سواد اطلاعاتی» همچون «سواد رایانه‌ای»، سواد کتابخانه‌ای، سواد رسانه‌ای، سواد شبکه‌ای (مترادف سواد اینترنتی و سواد هایپر)، سواد دیجیتالی (مترادف سواد

اطلاعات دیجیتالی) نیز مطرح گردیده است (محمدعلیپور و کریمی، ۱۳۸۶: ۵۴۴). برای استفاده از رایانه باید تاحدی از سواد سایبری برخوردار بود زیرا با توسعه اینترنت، شبکه به دنیای «واقعی» متصل شده و واقعیت قوانین حقوقی، اشخاص حقوقی و حقیقی، داخل فضای مجازی شده است؛ تا جای که لغاتی مانند «تجاوز در فضای مجازی[1]»، «جرایم مجازی[2]»، «تروریسم مجازی[3]» بوجود آمد. جنبه‌های مختلفی از مسائل مالی و تجاری مانند قوانین مالیاتی، حقوق مالکیت معنوی، تجارت الکترونیک و غیره حکومت‌ها را واداشته تا نسبت به تنظیم حقوق اینترنت و فضای مجازی چاره‌اندیشی نمایند (Wilske, 2004: 3). در دنیای کنونی، جهان از طریق شبکه اینترنت به‌شدت متداخل شده و فواصل دور، بسیار نزدیک و در جوار یکدیگر قرارگرفته است و حکومت‌ها و ملت‌ها در سطوح مختلف وابسته به این فضای سایبر شده و به‌عنوان قلمرو جدید توانسته است خود را قلمرو جدید مطرح کند. این شبکه جهانی، فرصت‌ها و امکانات زیادی برای افراد، گروه‌ها، حکومت‌ها و ملت‌ها فراهم ساخته است؛ اما نگرانی‌های فزاینده‌ای نیز در حفظ منافع ملی، امنیت ملی، حاکمیت ملی، امنیت شهروندان، جریان‌های سیاسی داخلی کشورها، تأسیسات و تجهیزات حیاتی کشور فراهم آورده است. همچنین آسیب‌پذیری کشور در مقابل حملات جدید دشمن نظیر ویروس‌های الکترونیکی، تهیج افکار عمومی و ... تا حد قابل‌توجهی بالابرده است. در این میان، با افزایش وابستگی به این فضای جدید نیاز به شناخت و یادگیری چگونگی استفاده و ورود به این فضا در قالب سواد سایبری می‌تواند گام مؤثری جهت کاهش مسائل و چالش‌های ناشی از آن و دستیابی به حفاظت سایبری باشد که در مقاله حاضر تلاش شده است جایگاه سواد سایبری در حفاظت سایبر با رویکرد پدافند غیرعامل موردبررسی و تحلیل قرار گیرد.

بیان مسئله

تغییر و تحولات اخیر در قرن بیست و یکم، نشانگر آن است که انسان‌ها، حکومت‌ها و سایر گروه‌ها تا چه اندازه به رسانه‌ها وابسته هستند. در میان رسانه‌ها، اینترنت با توجه به ظرفیت‌ها و پتانسیل‌های بالایی که دارا می‌باشد، از اهمیت و برجستگی ویژه‌ای برخوردار است. اینترنت با ایجاد شبکه‌های و پویند بین آن‌ها در سطح جهان زمینه برای شکل‌گیری و توسعه فضای سایبر را فراهم آورده است و از این طریق نوعی اجتماع و همزیستی بزرگی را که میلیون‌ها رایانه و کاربران آن در سراسر جهان به هم می‌پیوندند، را به وجود آورده است. به‌نحوی‌که

1. Rape in Cyberspace
2. Cyber Crime
3. Cyber Terrorisme

می‌توان گفت امروزه ما در یک جهان سایبری زندگی می‌کنیم وزندگی به فضای سایبر وابسته است. فضای سایبر با توجه به ظرفیت‌ها و پتانسیل‌های بالایی که دارا می‌باشد توانسته در عرصه‌های مختلف به‌عنوان یک فضای تسهیل‌کننده و پیونددهنده قوی در حوزه‌های مختلف نظیر تعامل افراد، دسترسی به منابع علمی و غیره مفید واقع شود. اما در کنار تسهیلات و خدمات مفید فضای سایبر، ظرفیت‌ها و پتانسیل‌های بالای این فضا به‌صورت‌های مختلف می‌تواند مورد سوءاستفاده افراد، گروه‌ها و حتی حکومت‌ها قرارگرفته و زمینه ایجاد مسائل و مشکلات متعددی در سطوح فردی، گروهی، ملی و حتی جهانی را فراهم آورد. دراین‌بین می‌توان به توسعه مسائلی مانند پورنوگرافی، تبلیغات نژادپرستی، تبلیغات ضد مذهبی، امپریالیسم خبری و اطلاعاتی، تقلب و سوءاستفاده‌های مالی و تجاری، پول‌شویی و غیره اشاره کرد. در این میان حکومت‌ها به‌عنوان سازمان‌های رسمی تأمین امنیت شهروندان و امنیت ملی برای اینکه بتوانند در کنار بهره‌برداری از ظرفیت‌ها و پتانسیل‌های بالای فضای سایبر، مسائل و مشکلات آن را تا حد ممکن کاهش دهند راهبردهای مختلف مبتنی بر دیدگاه پدافند غیرعاملی نظیر فیلتر کردن، محدود کردن دسترسی، کاهش سرعت اینترنت و غیره بهره برده‌اند. باوجود مؤثر بودن هر یک از این راهبردها اما همچنان مسائل و مشکلات ناشی از توسعه فضای سایبر در حدی است که ضریب ناامنی چه در سطح شهروندی و چه در سطح ملی بالاست. تحقیق حاضر مبتنی بر دیدگاه پدافند غیرعامل، مدعی است که راهبرد توسعه سواد سایبر به‌عنوان گام اولیه و پایه‌ای در عرصه پدافند غیرعامل کشور می‌تواند گام مؤثری جهت ارتقاء حفاظت سایبری برای کاهش ضریب ناامنی ناشی از وابستگی و پیوند روزافزون افراد، گروه‌ها و حکومت به این فضا سایبر باشد و امنیت و منافع ملی را تأمین نماید.

اهمیت و ضرورت

امروزه تکنولوژی اطلاعات و ارتباطات، صرف‌نظر از موقعیت جغرافیایی در تمام شئون زندگی واردشده است، به‌طوری‌که در دهه‌های اخیر مجازی شدن امور کشور در نظام اداری و اطلاعاتی پذیرفته‌شده است و ایجاد این فضا به‌عنوان مفهومی برای ایجاد یک فضای کارآمد و انعطاف‌پذیر موردتوجه قرارگرفته است. بنابراین سیستم‌های اطلاعاتی و ارتباطی دیجیتال و شبکه پایه به‌عنوان زیربنای مهم فضای مجازی ایفای نقش می‌کنند (هادوی نیا، ۱۳۹۱: ۱۳۲). لیکن این رشد علی‌رغم مزایای خود جنبه‌های منفی هم در برداشته است. بدین مفهوم که امکان رفتارهای ضداجتماعی و مجرمانه را به وجود آورده که پیش از این به‌هیچ‌وجه امکان‌پذیر نبوده است و با روند روبه رشد این جرایم روبه‌رو هستیم (جلالی فراهانی، ۱۳۸۶: ۶۵). زیرا جرایم رایانه‌ای به دلیل ویژگی‌هایی که دارند، نسبت به سایر طرق ارتکاب جرایم مرجح می‌باشند. اول آنکه، شیوه

ارتکاب آن‌ها آسان است، با مبالغ اندک، خسارات هنگفتی می‌توانند وارد نمایند، می‌توان بدون حضور فیزیکی در یک حوزه قضایی معین در آن حوزه مرتکب این‌گونه جرایم شد، دست‌آخر این‌که در اغلب موارد غیرقانونی بودن آن‌ها روشن نمی‌باشد. از سوی دیگر، با پیشرفت تکنولوژی رایانه، راه‌های ارتکاب جرم فنی‌تر و تخصصی‌تر شده و راه‌های مقابله با آن نیز دشوارتر می‌نماید. یکی از ویژگی‌های فناوری اطلاعات به‌ویژه اینترنت امکان ساماندهی و تدارک تهاجم سازمان‌یافته از فواصل دور علیه اهداف از پیش تعیین‌شده می‌باشد و به مهاجمان این امکان را می‌دهد تا علیه اهداف خود اقدام و ایجاد اختلال کنند. این فناوری علاوه بر این‌که موجب آشکار شدن نقاط ضعف موجود در زیرساخت‌های حیاتی می‌شود، با ایجاد ارتباط مخرب مانع از واکنش‌های دفاعی و یا ایجاد تأخیر در آن‌ها می‌گردد (حسن بیگی، ۱۳۸۴: ۳). در نگاهی به سوابق تحرکات دفاعی -امنیتی در سطوح کلان، بر اساس آمار تاکنون ۳۲ کشور در دنیا، ساختار دفاع سایبری خود را تشکیل داده‌اند و ۱۴۰ کشور در حال مطالعه روی توسعه دفاع ملی در کشور خود هستند.در بازه زمانی حاضر حرکت جهت در پیش‌گیری راهبردهایی برای کاهش چالش‌های ناشی از فضای سایبر به‌عنوان قلمرو جدید قدرت‌نمایی و نفش آفرینی بازیگران در سطوح مختلف به‌ویژه برای کشور به یک الزام و ضرورت تبدیل‌شده است. هرچند تاکنون راهبردهای مختلفی در این حوزه در پیش‌گرفته‌شده است اما به نظر می‌رسد، این راهبردها به دلایل مختلف نظیر تحولات و تغییرات بالا که روزآمدی راهبردها را می‌طلبد، گستردگی فضا و بازیگران و غیره در فضای سایبر نتوانسته است کارایی لازم را داشته باشد. بر این مبنا مسائل و مشکلات فضای سایبر با روندی رو به افزایش زمینه ایجاد ناامنی و چالش را برای امنیت در سطوح مختلف به‌ویژه سطح ملی را فراهم آورده است که نیازمند در پیش‌گیری راهبردی پایه‌ای‌تر است تا از این طریق بتوان آسیب‌ها و تهدیدات ناشی از حضور و گسترش فعالیت‌های ملی در فضای سایبر را تا حدی کاهش داد و از منافع ملی و امنیت ملی کشور حفاظت کرد. بر این مبنا، با افزایش اهمیت و جایگاه فضای سایبر پیگیری و تلاش جهت در پیشگیری راهبردی برای کاهش آسیب‌ها و تهدیدات ناشی از آن به یک ضرورت تبدیل‌شده است.

هدف، سؤال و فرضیه

هدف اصلی تبیین نقش و اهمیت توسعه سواد سایبر در افزایش حفاظت سایبر می‌باشد. بر این مبنا سؤالی که تحقیق حاضر در پی پاسخ‌دهی به آن است عبارت است از: آیا می‌توان از توسعه سواد سایبری به‌عنوان گامی جهت حفاظت سایبری در عرصه پدافند غیرعامل کشور بهره برد؟ به‌طورکلی در ارتباط با سؤال اصلی تحقیق، می‌توان این فرضیه را مطرح نمود: با رشد و توسعه

سواد سایبری در میان افراد، جامعه، کارکنان و کارمندان سازمان‌ها و نهادهای دولت، نیروهای نظامی و انتظامی می‌توان تا حدودی بستر لازم را جهت کاهش تأثیرات تهدیدات سایبری در قالب حفاظت سایبری در عرصه پدافند غیرعامل فراهم آورد.

پیشینه

بررسی‌های صورت گرفته از سوی محقق نشان‌دهنده آن است که کارهای انجام‌شده در زمینه فضای سایبر در کشور زیاد می‌باشد اما در زمینه توسعه سواد سایبر کاری با توجه به منابع در دسترس محقق انجام نگرفته است. اما برخی از کارهایی که به نحوی مرتبط با مقاله هستند عبارتند از: مقاله‌ای با عنوان «مدیریت مرزهای فضای سایبر، گام نخست دفاع سایبری» (۱۳۹۰) نوشته محمدقصری و محسن جان‌پرور اولین همایش دفاع سایبری به جایگاه ترسیم و پررنگ کردن مرزهای موجود در فضای سایبر پرداخته‌شده است و مدیریت این مرزها را به‌عنوان گام نخست دفاع در برابر تهاجمات در این فضا در نظر گرفته‌شده است.

در مقاله‌ای با عنوان «گفتمان جنگ مجازی و رسانه‌های گروهی» نوشته مهسا ماه‌پیشانیان (۱۳۸۶) بیان‌شده است که رسانه‌های گروهی می‌توانند شرایط جنگ را از طریق تبدیل و تخفیف مرگ در طی جنگ‌ها، شبیه‌سازی، مسافت سازی، تلویزیون، رایانه و سینما تغییر دهند که اینترنت و تبلیغات در این شرایط بسیار مؤثر است.

در پایان‌نامه‌ای با عنوان «نقش مهارت‌های سواد رسانه‌ای در استفاده‌ی بهینه از فضای سایبر» نوشته یوسف عباسی (۱۳۹۱) به راهنمایی دکتر محمد سلطانی فرد دانشگاه آزاد اسلامی واحد تهران مرکزی، بین مهارت رایانه‌ای برای استفاده از ظرفیت‌های علمی و مهارت در زمینه خرید و پرداخت‌های الکترونیکی و میزان استفاده از فضای سایبر رابطه معناداری وجود ندارد. ولی بین مهارت‌های رایانه‌ای در فضاهای اجتماعی و سرگرمی اینترنت و میزان استفاده از فضای سایبر رابطه معناداری وجود دارد. نتایج بدست آمده نشان داد که میزان مهارت رایانه برای استفاده از ظرفیت‌های علمی و میزان اعتماد و نحوه برخورد با مطالب دریافتی از فضای مجازی در دانشجویان دانشگاه‌های تهران تفاوت معنی‌داری دارند و دانشجویان دانشگاه تهران و علامه طباطبایی توانایی بیشتری برای مقابله با جنگ نرم دارند.

روش پژوهش

این مقاله ازنظر هدف کاربردی بوده و جمع‌آوری داده‌ها و اطلاعات نیز به شیوه کتابخانه‌ای و اسنادی انجام‌گرفته است. روش انجام تحقیق حاضر با توجه به ماهیت نظری آن توصیفی-تحلیلی است. بر این اساس سعی شده است علاوه بر تصویرسازی درست از فضای سایبر و سواد سایبری به تشریح و تبیین چگونگی حفاظت سایبری از کشور بپردازد. ازآنجاکه حفاظت

سایبری از کشور ازجمله کارکردها و اهداف کلی پدافند غیرعامل کشور محسوب می‌شود بر این اساس، سعی شده است که توسعه سواد سایبری با رویکرد حفاظت سایبری در قالب پدافند غیرعامل در نظر گرفته شود.

مفاهیم و مبانی نظری

سواد سایبری[1]: در طی دهه‌های اخیر، پژوهشگران موفق به کشف و معرفی بیش از ۳۴ نوع سواد مفید و مدرن شده‌اند که سواد علمی بامعنای مصطلح در نظام آموزشی ما، تنها یکی از آن‌ها محسوب می‌شود. ازجمله سوادهای مفید و مدرن می‌توان به سواد فرهنگی، سواد اجتماعی، سواد سیاسی، اقتصادی سواد رسانه‌ای، سواد اطلاعاتی، سواد کامپیوتری، سواد محیط کار و سواد خانوادگی و ... به‌ویژه فناوری اشاره کرد که هر یک تعریف، استانداردها و راهکارهای توسعه خویش رادارند (صالحی، ۱۳۸۹: ۴۰). سواد سایبری نوعی سواد سنتی محسوب می‌گردد که توانایی شخص را در انجام اعمال اصلی و پایه‌ای در بردارد و به یک کاربر اینترنت می‌آموزد چگونه از این فضا به‌خوبی بهره ببرد، بدون اینکه خطری او و خانواده‌اش را تهدید کند. سواد رایانه‌ای تداعی‌کننده نوعی مهارت است که متضمن کارایی در تعدادی از کاربردهای رایانه‌ای امروز، مانند واژه‌پردازی و پست الکترونیکی است (معنوی، ۱۳۸۷ :۵۷). این سواد در چهار سطح به‌صورت ذیل طبقه‌بندی می‌شود:

۱- سواد پایه‌ای که همان قدرت خواندن و نوشتن است.

۲- سواد کارکردی که توان عملیاتی یکی از مهارت‌های گوناگون ارتباط است.

۳- سواد فناورانه که قدرت شناسایی نقش تکنولوژی‌های ارتباطی است.

۴- سواد اطلاعاتی که قدرت تشخیص اطلاعات را در برمی‌گیرد.

ملزومات برای سواد کامپیوتری متنوع است اما ممکن است یک فهم پایه از سخت‌افزار سیستم-های رایانه‌ای و آیین‌نامه مهارت‌های ضروری را شامل شود. البته باید توجه داشت که سواد رایانه‌ای یک مفهوم بدون تغییر و ثابت نیست بلکه به‌عنوان ماحصل و نتیجه پیشرفت‌های فناوری رایانه‌ای و به‌تبع آن نرم‌افزاری در جوامع در حال تغییر است. درنهایت سواد رایانه‌ای توانایی استفاده از رایانه و نرم‌افزارهای آن برای انجام وظایف کاربردی است (میرجلیلی، ۱۳۸۵: ۱۰۹-۱۲۲). لوینگستون و تامیم[2] معتقدند نخستین شرط استفاده از اینترنت، داشتن نوعی پختگی و اعتمادبه‌نفس است. استفاده از هر فناوری جدید خواه‌ناخواه برای کاربران

1. Cyber fluency
2. Lingston & tamim

پیش‌شرط‌های عقلی، عاطفی و اخلاقی ایجاد می‌کند که می‌توان با نهادینه کردن آن‌ها، به افزایش آگاهی و خرد امیدوار بود (Livingstone, 2001:369). آلفرد بورک[1] مشکل تعریف سواد رایانه‌ای را این‌گونه بیان می‌کند: سواد رایانه‌ای همانند احساس مادری است که اکثر مردم به آن علاقه‌مند هستند ولی برخلاف آن، این موضوع تعریف روشنی ندارد (Bork, 1993: 76).

حفاظت سایبری: بسیاری از کارشناسان و تحلیل‌گران حوزه امنیت، بر این باورند که پایان یافتن دوران ژئوپلتیکی جنگ سرد نه‌تنها منجر به امن‌تر شدن جهان نشده است، بلکه به وجود آمدن چالش‌های امنیتی غیرنظامی جدیدی همچون تخریب محیط‌زیست، رفاه اقتصادی، سازمان‌های جنایی بین‌المللی و مهاجرت گسترده افراد، امنیت جهانی را با چالش‌های جدی تری نسبت به گذشته مواجه ساخته است (خلیلی، ۱۳۹۱: ۱۷۹). یکی از تهدیدات امنیتی موجود در جهان، مخاطرات موجود در فضای سایبری است که از آن تحت عنوان تهدید سایبری نام‌برده می‌شود. تهدید سایبری یک عامل بالقوه برای نقض امنیت در فضای سایبری است. این تهدید در صورتی وجود خواهد داشت که یک پیشامد، قابلیت، کنش، یا رخداد که می‌تواند در امنیت سایبری رخنه ایجاد نموده، منجر به صدمه شود به وجود بیاید. این بدان معنی است که یک تهدید سایبری، یک خطر بالقوه است که ممکن است منجر به بهره‌برداری از یک آسیب-پذیری امنیتی[2] شود (حسینی، ۱۳۹۲: ۴۵). حمله سایبری، نمونه‌ای از سلاحی جدید است که می‌تواند روش هدایت جنگ مدرن را توسط بازیگران دولتی و غیردولتی دگرگون نماید. سرشت بی‌مانند این تهدید و توانمندی مرتکبان جنگ‌های سایبری در آسیب رساندن، کشتار و تخریب فیزیکی از طریق فضای سایبر، تعریف سنتی توسل به‌زور را متحول ساخته است (قاسمی، ۱۳۹۰ :۱۱۵). همان‌گونه که ابزارها و تکنیک‌های جدید روزانه در دنیای فناوری اطلاعات پدیدار می‌گردند تا اطلاعات را در شبکه جهانی اطلاعات قابل‌دسترس نمایند به همان نسبت آسیب-پذیری ناشی از آن‌ها نیز بیشتر می‌گردد. درنتیجه دفاع سایبری از اهمیت ویژه‌ای برخوردار است تا در خصوص انتقال ایمن و معتبر اطلاعات اطمینان حاصل گردد. امنیت سایبر به‌طور گسترده‌ای با عملکرد انسان ارتباط دارد. در هر دو مورداستفاده از کامپیوتر و ارتباط به‌وسیله کامپیوتر مقررات امنیتی باید رعایت شود. سیستم‌های شناسایی عوامل نفوذ[3]، سیستم‌های شناسایی[4] و جلوگیری از عوامل نفوذ[5] مهم‌ترین فن‌آوری‌هایی هستند که در زمینه حفاظت

1. Alfred boork
2. Security vulnerability
3. Intrusion Detection System
4. Intrusion Prevention
5. Detection System

سایبری وجود دارند. در حقیقت شناسایی عوامل نفوذ فرایند نظارت بر اتفاقاتی است که در یک سیستم کامپیوتری یا یک شبکه رخداده و تحلیل و بررسی علائم اتفاقات محتمل آتی است. شناسایی عوامل نفوذ می‌تواند به‌صورت دستی یا به‌صورت خودکار صورت پذیرد. شناسایی عوامل نفوذ به‌صورت دستی ممکن است از طریق بازرسی فایل‌های ثبت وقایع یا ترافیک شبکه‌ای رخ دهد. بنابراین یک سیستم شناسایی عوامل نفوذ ابزار یا کاربرد نرم‌افزاری است که عملکرد شبکه و سیستم اطلاعات برای اقدامات اشتباه یا نقض قوانین را کنترل می‌نماید و به آن فعالیت مشکوک از طریق اطلاع‌رسانی به مدیر سیستم از راه‌های مختلف پاسخ می‌دهد. سیستم‌های شناسایی عوامل نفوذ می‌توانند بر اساس میزبان یا بر اساس شبکه باشند. سیستم بر اساس میزبان تماس‌ها و وقایع سیستم را کنترل می‌کنند درحالی‌که سیستم‌های بر اساس شبکه جریان بسته‌های کوچک شبکه را کنترل می‌کنند. سیستم‌های مدرن معمولاً تلفیقی از این دو رویکرد هستند. سیستم جلوگیری از عوامل نفوذ ابزار یا کاربرد نرم‌افزاری است که سیستم شناسایی عوامل نفوذ را تکمیل می‌کند و قادر به متوقف نمودن بسیاری از رخدادها پیش از رخداد است.

سامانه‌های پیشگیری از عوامل نفوذ در چهار دسته طبقه‌بندی می‌گردند:

پیشگیری از عوامل نفوذ وابسته به شبکه[1]: کل شبکه را برای ترافیک مشکوک از طریق تحلیل فعالیت پروتکل (تبادل داده بین سامانه‌ها) واپایش می‌کند.

سامانه‌های پیشگیری از عوامل نفوذ بی‌سیم: یک شبکه بی‌سیم را برای ترافیک مشکوک از طریق تحلیل پروتکل‌های بی‌سیم شبکه کنترل می‌کند.

تحلیل رفتار شبکه: آمدوشد شبکه را به‌منظور شناسایی تهدیداتی که جریان‌های آمدوشد غیرمعمول تولید می‌کنند بررسی می‌نماید.

پیشگیری از عوامل نفوذ بر اساس میزبان[2] بسته‌ای است که یک میزبان خاص را برای فعالیت مشکوک از طریق تحلیل وقایع رخداده در آن میزبان واپایش می‌نماید (Inyiama,2001: 55).

پدافند غیرعامل: پدافند (دفاع) غیرعامل عبارت است از: به‌کارگیری هرگونه ابزار، شرایط و موقعیت به‌طوری‌که خودبه‌خود و بدون نیاز به عامل انسانی با مراحل مختلف حملات دشمن مقابله شود و از برنامه‌ریزی‌های دفاعی موقعیت‌های مثبت طبیعی، استتار، اختفا، پراکندگی و

1. Network-based interusion prevention
4. Host-based Intrusion Prevention

استحکامات استفاده گردد. به‌عبارتی‌دیگر پدافند غیرعامل به کلیه اقدامات و تدابیری گفته می‌شود که بدون استفاده از سلاح، موجب کاهش آسیب‌پذیری، تلفات، خسارت و افزایش پایداری شود (جلالی فراهانی، ۱۳۹۱: ۵-۴). به‌بیان‌دیگر، پدافند غیرعامل به مجموعه اقداماتی اطلاق می‌گردد که مستلزم به‌کارگیری جنگ‌افزار نبوده و با اجرای آن می‌توان از وارد شدن خسارت مالی به تجهیزات و تأسیسات حیاتی و حساس نظامی و غیرنظامی و تلفات انسانی جلوگیری نمود و یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد (باغ شیخی، ۱۳۸۸: ۹).

نظریات مرتبط به فضای سایبر: فضای مجازی یک فضای جدید است که از لایه‌های متفاوتی تشکیل‌شده است. دیدگاه صاحب‌نظران و اندیشمندان در خصوص پیامدهای استفاده از این فضا و به‌طور خاص اینترنت می‌توان به سه دسته تقسیم نمود: دسته اول که دیدگاه آنان جبرگرایی است، اینترنت را ساختاری عینی، بیرونی و متصلب فرض می‌کنند که ذهنیت افراد در چارچوب آن شکل می‌گیرد و کاربران را در سیطره خود قرار می‌دهد. دیدگاه دسته دوم به اراده‌گرایی معروف است و اینترنت را رشته امکانات محضی در جهت تواناسازی فرد برای گردآوری انبوه اطلاعات و رشد کثرت‌گرایی می‌داند. دسته سوم که دیدگاه آنان به تکنو رئالیسم معروف است، رویکرد بینابینی دارند آن‌ها همچنان که ابعاد هستی شناختی فن‌آوری اینترنت را نادیده می‌گیرند، معتقدند این فناوری تعیین‌کننده نهایی نیست. به‌بیان‌دیگر آن‌ها همچنان که ظرفیت‌ها و توانایی‌های اینترنت را درنظر دارند به آزادی عمل کاربران نیز توجه می‌کنند (قادی، ۱۳۸۶: ۲۵۵). لوینگستن و تامن[1] (۲۰۰۱) معتقدند نخستین شرط استفاده از اینترنت، داشتن نوعی پختگی و اعتمادبه‌نفس است. استفاده از هر نوع فناوری خواه‌ناخواه برای کاربران پیش‌شرط‌های عقلی، عاطفی و اخلاقی ایجاد می‌کند که می‌توان با نهادینه کردن آن‌ها به افزایش آگاهی و خرد امیدوار بود. کرات و پترسون[2]، لاندمک[3]، کسل و همکاران[4] (۱۹۹۸) بیان می‌دارند که بهره‌گیری از فضای مجازی به‌خصوص اینترنت به افسردگی و تنهایی منجر می‌شود. مواجهه نوجوانان و جوانان با سبک‌های گوناگون زندگی، تفکر و ارتباطات در محیط گسترده اینترنت، موجب تشویش زدایی و اضطراب آفرینی در جامعه جوان می‌شود. تامن معتقد است که سواد استفاده از فضای مجازی سبب می‌شود مخاطب خود را ملزوم نماید تا در استفاده از این فضا، جیره مصرف داشته باشد؛ با توجه به ویژگی‌های پیام‌دهنده، برخی پیام‌ها

1. Lingston & taman
2. Krat & peterson
3. Landmak
4. Kesell & et.al

که مطلوب مخاطب است برگزیده شود و به دیگر پیام‌ها توجهی نشود و درنهایت پیام‌های این فضا را نقد نماید (سلطانی فر، ۱۳۸۶: ۵۰).

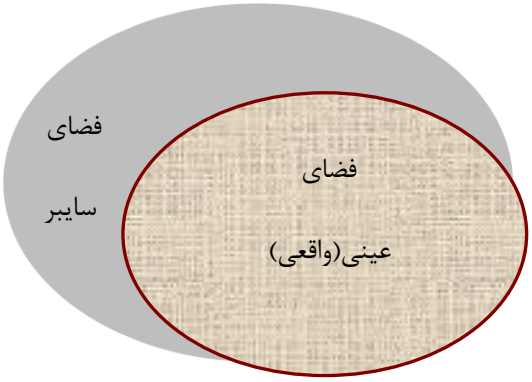
تجزیه‌وتحلیل

۱-فضای سایبر قلمرو جدید: پیشرفت‌ها در زمینه تکنولوژی تحولات زیادی را باعث شده است، که ازجمله آن‌ها شکل‌گیری فضای سایبر[1] است که توانسته است جنبه‌های مختلف زندگی بشری را تحت تأثیر قرار دهد. اگرچه از فضای سایبر تعریف روشنی نشده است، بااین‌وجود می‌توان آن را «فضایی که در آن فعالیت‌های گوناگون در ابعاد داده‌ورزی و اطلاع‌رسانی، ارتباطات و ارائه خدمات، مدیریت و کنترل از طریق سازوکارهای الکترونیکی و مجازی انجام می‌پذیرد» تعریف کرد (کروبی و صدری، ۱۳۸۴: ۵۸). فناوری اطلاعات، عبارت است از فناوری که فرد را در ضبط، ذخیره‌سازی، پردازش، بازیابی، انتقال و دریافت اطلاعات، یاری می‌دهد. فناوری اطلاعات و ارتباطات به یکدیگر وابسته هستند. با در اختیار داشتن فناوری‌های اطلاعاتی و ارتباطی مختلف و پیشرفته، امکان برقراری سریع ارتباط و تبادل سریع اطلاعات بیش‌ازپیش میسر گردیده است (صدوقی، ۱۳۸۲: ۵۵). اصطلاح فضای سایبر را نخستین بار ولیام گیبسون نویسنده کانادایی داستان علمی- تخیلی در کتاب نورومونس به کاربرد. برای وی فضای سایبر فضایی تخیلی بود که از اتصال رایانه‌هایی پدید آمده است که تمامی انسان‌ها، ماشین‌ها و منابع اطلاعاتی در جهان را به هم متصل کرده است (کاوندی کاتب،۱۳۸۹:۶۵). به عقیده «کاستلز[2]» تنها در دهه ۱۹۷۰ بود که فناوری‌های جدید اطلاعاتی در سطحی گسترده انتشار یافتند و توسعه توأمان خود را شتاب بخشیدند و در پارادایمی جدید گردهم آمدند. کاستلز می‌گوید: بی‌گمان می‌توانیم بدون اغراق بگوییم که انقلاب فناوری اطلاعات به‌عنوان یک انقلاب در دهه ۱۹۷۰ متولد شد. به‌ویژه اگر پیدایش و رواج مهندسی ژنتیک به‌طور موازی و تقریباً در همان زمان و مکان را به آن اضافه کنیم (کاستلز، ۱۳۸۱: ۷۱). در این راستا، با پیشرفت و توسعه این فناوری از اوایل دهه ۱۹۸۰ به بعد پدیده رایانه در ساماندهی ارتباطی به کار گرفته شد و در حقیقت پیوندی میان رایانه و مخابرات به وجود آمد که با این پیوند بشر وارد عصر اطلاعات شد که پدیده شبکه حاصل این پیوند بوده است (صدوقی، ۱۳۸۲: ۸۰). این انقلاب تکنولوژیک – علمی معاصر، سیاست جهانی به‌ویژه کشورهای پیشرفته صنعتی، را شدیداً تحت تأثیر قرار داده است. تحولات فوق به‌شدت از اهمیت فاصله و مکان، به‌عنوان عوامل تعیین‌کننده (چه کسی می‌تواند

1. Cyberspace
2. Kastelz

چه اقدامی برای چه کسی بکند) کاسته است. همچنین تعدد فرصت‌ها برای استفاده و یا سوءاستفاده از فضا و محیط آبی، که تحت حاکمیت هیچ کشوری نیست، واقعیت‌های فیزیکی جدیدی را در جهان کنونی ایجاد کرده است (باربر، ۱۳۸۱: ۱۹۳). در این زمینه باید توجه داشت که، فضای سایبر چیزی جدا از فضای واقعی نیست، فضای سایبر، فضایی است که تحت تأثیر فضای واقعی به‌وجود آمده است و به‌صورت متقابل بر آن تأثیر می‌گذارد و از آن تأثیر می‌پذیرد. به‌طورکلی می‌توان گفت فضای سایبر مانند سایه فضای واقعی است که هر اتفاقی و تغییر شکلی که در فضای واقعی رخ دهد، باعث تغییر و دگرگونی در فضای سایبر می‌شود البته با این تفاوت که فضای سایبر مانند یک سایه بدون تأثیر و نقش در فضای واقعی نیست این فضا به‌صورت‌های مختلف و در اشکال مختلف فضای واقعی را تحت تأثیر قرار می‌دهد و باعث شکل-گیری دنیای جدیدی در ارتباط با فضای واقعی شده است که مسائل و مشکلات و راه‌حل‌های مختلفی را به فضای واقعی ارائه می‌کند (جان پرور، ۱۳۸۶: ۵۶). این روابط بین فضای واقعی و فضای سایبر را می‌توان به‌صورت شکل (۱) نشان داد.

شکل ۱: رابطه بین فضای واقعی و فضای سایبر



(حافظ نیا و دیگران، ۱۳۹۲: ۷۶)

۲-عرصه‌های توسعه سواد سایبری(مجازی) با رویکرد پدافند غیرعامل:

توسعه سواد سایبری در بین افراد: ما در حال پای گذاشتن در عصری هستیم که حتی یک فرد به‌تنهایی می‌تواند مخفیانه مرگ میلیون‌ها نفر را رغم بزند و یا برای سالیان سال شهری را غیرقابل‌سکونت سازد. در چنین عصری، یک نقص یا خرابکاری در فضای سایبر می‌تواند جهان را به آشفتگی یا ویرانی بکشاند. مثلاً در بخش اقتصادی، بروز یک نقص فنی می‌تواند حمل‌ونقل هوایی، تولید انرژی و یا سیستم‌های اقتصادی را از پای درآورد. در چنین عصری نه‌فقط یک

فرد معترض، که یک فرد بی‌کفایت ولو غیر مغرض هم می‌تواند به فاجعه‌ای عظیم دامن زند و مخاطرات انسانی گسترده‌ای را سبب شود (ریس، ۱۳۹۲: ۷۱-۷۰). لذا اقدامات متنوعی را می‌توان در راستای پیشگیری از نقض هنجارها به عمل آورد که فرهنگ‌سازی و آموزش –آگاهی(توسعه و بسط سواد سایبری) از اقدامات خاص می‌باشد.پیشگیری اجتماعی جامعه مدار عوامل اجتماعی جرم‌زا در یک جامعه معینی را مورد هدف قرار می‌دهد و اقداماتی که در این راستا به اجرا درمی‌آید باهدف از بین بردن زمینه‌های اجتماعی ایجادکننده انگیزه‌های مجرمانه - خوشبختانه وزارت آموزش‌وپرورش با احیا مقطع ششم ابتدایی گام مثبتی را در این راستا برداشته است و در مقطع ششم ابتدایی درسی را با عنوان«کار و فناوری»با محتوای فناوری اطلاعات و ارتباطات گنجانده است که در نوع خود قابل‌تحسین است و می‌تواند نقش به سزایی در آموزش آگاهی چنین افرادی از تخلفات اجرایم سایبری باشد .است. البته موارد فوق زمانی نتیجه‌بخش خواهد بود که سازوکارهای اجرایی آن‌ها و متولیان امر مشخص شود. در کشور ما بنیان‌های اساسی و راهبردی این نوع پیشگیری در غالب موارد به‌ویژه در ابلاغیه‌های مقام معظم رهبری پایه‌ریزی شده است و نهادهای اجرایی دیگر ازجمله شورای عالی انقلاب فرهنگی،وزارت فرهنگ و ارشاد اسلامی،وزارت ارتباطات و فناوری،وزارت آموزش‌وپرورش و...از طریق طراحی وترسیم شناسایی عوامل خطر گام‌های مثبتی به‌ویژه در حوزه تقنینی برداشته‌اند ولی در نحوه اجرای آن یا ضعیف عمل کرده‌اند و یادر برخی موارد به نظر موازی کاری پیش‌آمده است.ولذا به نظر می‌رسد نهادهای متولی در این راستا چارچوب وظایفشان کاملاً مشخص شود و نهاد مربوطه هم در راستای اهداف و وظایف بالا حرکت کند و از موازی کاری یا انجام ندادن مسئولیت جلوگیری شود.که البته به نظر می‌رسد با تأسیس مرکـز ملی فضای مجـازی به دستور مقام معظم رهبری(مد ظله العالی) که عالی‌ترین نهاد در حوزه فناوری اطلاعات کشور محسوب می‌شود مسائل و مشکلات فضای مجازی و به تبع آن انحرافات سایبری (مجازی) به کمترین اندازه کاهش یابد (پورقهرمانی، ۱۳۹۳: ۶).

توسعه سواد سایبری در سطح جامعه: مدتی است که موضوعی با عنوان آسیب‌های نوپدید به‌ویژه آسیب‌های ناشی از اینترنت، تلفن همراه، ماهواره و بازی‌های رایانه‌ای از سوی مسئولان و کارشناسان ذی‌ربط مطرح‌شده است و بر لزوم برنامه‌ریزی و سیاست‌گذاری در حوزه‌ی پیشگیری از این آسیب‌ها تأکید می‌شود. آسیب‌شناسی را می‌توان شناسایی مجموعه‌ی عوامل و شرایطی دانست که موجب عدم سازگاری فعالیت‌ها و اعمال اجتماعی و روانی فرد با هنجارهای اجتماعی و روانشناسی می‌گردند. آسیب‌های نوپدید در کشور به دلیل توسعه‌ی فناوری‌ها رو به

گسترش هستند و در بسیاری از کشورها با در نظر گرفتن افزایش این فناوری‌ها برای پیشگیری و مقابله با آسیب‌های نوپدید برنامه‌ریزی‌شده است؛ اما در ایران با توجه به‌سرعت گسترش فناوری‌ها و توسعه‌ی اینترنت و فضای مجازی برنامه‌ریزی و راهکار مؤثری برای مقابله با این‌گونه آسیب‌ها تدبیر نشده است و این موجب افزایش دامنه‌ی این‌گونه آسیب‌ها در سراسر کشور شده است. بروز آسیب‌های نوپدید می‌تواند زمین ساز نوع جدیدی از آسیب‌های اجتماعی و روانی باشد. به همین دلیل، برنامه‌ریزی برای شناسایی، پیشگیری و کاهش آسیب-های نوپدید لازم و ضروری می‌نماید. آسیب‌های نوپدید، آسیب‌های مرتبط با فناوری‌های جدید است که آسیب‌های ناشی از استفاده از ماهواره، بازی‌های رایانه‌ای، تلفن همراه و اینترنت می‌توانند در این مجموعه قرار گیرند. در این میان میزان استفاده از اینترنت و شبکه‌های مجازی چنان رو به گسترش است که نسل کنونی را نسل اینترنت یا نسل شبکه نام نهاده‌اند. این نسل متولدین اواسط دهه‌ی ۱۹۹۰ میلادی به بعد هستند. بین استفاده‌ی نسل‌های مختلف از شبکه‌های اجتماعی و همچنین انگیزه‌های آن‌ها از پیوستن به فضای مجازی تفاوت‌های قابل‌توجهی وجود دارد. به‌عنوان‌مثال، نتایج پژوهش‌ها نشان داده است که مادران نسبت به پدران بیشتر از فیس‌بوک استفاده می‌کنند و بیشتر دوستان فیس‌بوکی مادران، اعضای خانواده و خویشاوندان آن‌ها هستند. امروزه کودکان و نوجوانان با دسترسی به فضای مجازی با هجمه‌های از تبلیغات، فیلم‌ها، عکس‌ها، مطالب و شخصیت‌ها آشنا می‌گردند که این وضعیت در کنار آثار مثبت آن، آثار منفی و مخربی نیز به بار آورده است. بنابراین جوامع برای اصلاح و تربیت صحیح نسل آینده خود همواره به دنبال مقابله با این عوامل بوده‌اند. آنچه که به‌عنوان علل گرایش کودکان نوجوانان به محتویات غیراخلاقی قابل‌ذکر است درواقع وضعیت سنی، خواسته‌ها و ارزش‌های مورد تقاضای این قشر، جاذبه‌ی این محتویات و عدم وجود جایگزین مشروع می‌باشد. لذا افراد در سنین پایین به دلیل شرایط خاصی که در آن قرار دارند، بیشتر تحت تأثیر عوامل محیطی قرار می‌گیرند. بنابراین گرفتن تدابیر بازدارنده و پیش‌بینی جایگزین‌های مشروع و پرجاذبه در این زمینه می‌تواند کمک‌کننده باشد. هنوز برخی کاربران ما به این مسئله به‌درستی واقف نبوده و با اعتماد بی‌جا به‌طرف مقابل و بدون توجه به غیرواقعی بودن هویت‌ها در این محیط، به‌سادگی اطلاعات شخصی، خانوادگی و محرمانه خود را در فضای مجازی افشا می‌کنند که این افشای اطلاعات زمینه آسیب‌پذیری فرد را به وجود می‌آورد. بنابراین یکی از مهم‌ترین احتیاط‌هایی که کاربران در محیط اینترنت باید به آن توجه کنند این است که هویت‌های مجازی، هویت غیرقابل‌اعتمادی بوده و افشای اطلاعات محرمانه در این

محیط نادرست است. اهمیت این دانش ازآنجا است که در ابتدا بیشتر کاربران اینترنت جوانان و نوجوانان هستند و آسیب‌پذیری این قشر به لحاظ تأثیرپذیری از سبک زندگی حاکم بر این فضا بالا است (جلالی فراهانی، ۱۳۸۶: ۱۲۵). یکی از استفاده‌های مهم دیگری که در سطح بین‌المللی از فضای مجازی برای آسیب‌رسانی به سایر حکومت‌ها و دولت‌ها صورت می‌گیرد شایعه‌سازی و به راه انداختن جنگ روانی در سطح بین‌المللی برعلیه حکومت و دولت موردنظر از طریق این فضا است. اصطلاح جنگ روانی در سال ۱۹۴۱ از زبان آلمانی وارد امریکا شد. بر طبق تعریف کریستوفر سیمپسون[1] جنگ روانی به معنای کاربرد علمی تبلیغات سیاسی، ترور و فشار دولتی به‌عنوان وسایلی برای تضمین پیروزی ایدئولوژیکی بر یک دشمن است. تا با استفاده از این شایعه‌ها و جنگ روانی کشور و دولت موردنظر را تحت‌فشار قرار داده و اهداف خود را در سطح بین‌الملل برعلیه آن کشور و یا امتیازگیری از آن کشور دنبال کنند. در این شرایط، حکومت‌ها اگر بخواهند جریان اطلاعات را از راه اینترنت کنترل نمایند، ناچار به تحمیل هزینه‌های بالایی خواهند شد و در آخر کار از تلاش‌های خود ثمر چندانی نخواهند گرفت. در ارتباط با این موضوع می‌توان به ۵ مورد که به‌عنوان جنگ سایبری علیه کشور ایران محسوب می‌شود اشاره نمود: جنجال‌سازی، ایجاد و گسترش تنش‌های اجتماع متراکم و گسترده، تضعیف سرمایه‌های اجتماعی، توانمندسازی جنبش‌های مدنی و سیاسی و تحریف یا جعل مفاهیم فرهنگی و تمدنی (نورمحمدی،۱۳۹۰:۱۳۵). درنتیجه، اینترنت از طریق همین ابزارهای ارتباطی، ناراضیان را یک‌صدا کرده تا شنیده شوند و به عموم مردم وسیله‌ای داده است تا سازماندهی شوند. درحالی‌که برخی تحلیل گران نقش اینترنت در انقلاب‌های خاورمیانه و شمال آفریقا را انکار می‌کنند، شبکه‌های اجتماعی همچون توئیتر و فیس‌بوک، نقش به‌سزایی در شکل‌گیری این حوادث داشته‌اند. از سوی دیگر، اینترنت می‌تواند مورد سوءاستفاده دیکتاتورها و تروریست‌ها نیز قرار بگیرد. به‌عبارت‌دیگر، دیکتاتورها و گروه‌های افراطی نیز با استفاده از همین روش، ایدئولوژی خود را گسترش داده و در سرتاسر دنیا عضو می‌گیرند (خلیلی، ۱۳۹۱: ۱۸۴). نای[2] معتقد است باوجود چنین تحولاتی، دولت‌ها همچنان به‌عنوان بازیگر غالب درصحنه جهانی باقی خواهند ماند، اما کنترل آن‌ها بر مسائل مشکل و پیچیده‌تر خواهد شد. بخش وسیعی از جمعیت، هم در داخل کشورها و هم در روابط میان کشورها به قدرتی دسترسی پیدا می‌کنند که از اطلاعات برمی‌آید. از سوی دیگر، فضای سایبری جایگزین فضای

1. Christopher Simpson
2. Nay

جغرافیایی نخواهد شد و حاکمیت دولت را لغو نمی‌کند، اما انتشار قدرت در فضای سایبری اعمال قدرت را پیچیده‌تر خواهد کرد.

توسعه سواد سایبری در سطح مسئولان و کارکنان دولتی: پیدایش رایانه‌ها و فناوری اطلاعات عامل تأثیرگذار بر فعالیت سازمان‌ها در سه دهه اخیر بوده است. فناوری اطلاعات می‌تواند نقش مهمی در ارتقاء کارایی و بهره‌وری سازمان داشته باشد (زارعی، ۴۱:۱۳۹۲). گسترش شبکه‌های جهانی اینترنت در قرن بیست و یکم به‌عنوان مهم‌ترین دستاورد فناوری اطلاعات و ارتباطات بسیاری از مرزهای موجود در ارتباطات میان افراد، دولت‌ها و حکومت‌ها را از میان برداشته و تأثیرات عمیقی بر چگونگی عملکرد و روابط آن‌ها داشته است. این فناوری‌های اطلاعاتی و ارتباطی به دلیل آن‌که به نسبت ارزان است و به میزان گسترده‌ای در دسترس، توانمندی قابل‌ملاحظه‌ای، حتی برای فقیرترین حکومت‌ها و کنشگران منطقه‌ای و جهانی فراهم کرده است که ممکن است برای به چالش کشیدن و آسیب‌رسانی به دیگران استفاده شود. این مسأله درست برخلاف فناوری‌های نظامی مهم عصر صنعتی است. در عصر اطلاعات، سخت‌افزارها و نرم‌افزارها به‌صورت گسترده در دسترس و به‌سادگی قابل‌استفاده است، درحالی‌که سلاح‌های عصر صنعتی مانند سلاح‌های هسته‌ای، موشک‌های قاره‌پیما، ناوهای جنگی هواپیمابر و تانک‌ها این‌گونه نیست. بنابراین، در عصر اطلاعات، حکومت‌ها تنها کنشگران بین‌المللی نیستند که ممکن است توانمندی‌های فنی را توسعه دهند، تا برای آسیب‌رسانی استفاده کنند. هم‌چنین شرکت‌های چندملیتی، سازمان‌های غیردولتی، گروه‌های جنایی و تروریستی و حتی افراد ممکن است دست به عملکرد جنگی بزنند (آلبرتس، ۱۳۸۵: ۴۵). ازجمله این تحولات در عرصه بین‌المللی می‌توان به تغییر در روابط بین حکومت‌ها و دولت‌ها در عرصه منطقه‌ای، بین‌المللی و جهانی را که پیش‌تر توسط دیپلمات‌ها انجام می‌گرفت، اشاره کرد. این تحولات در عرصه فناوری اطلاعات و ارتباطات این نوع روابط بین کشورها و دولت‌ها را به روابطی چندجانبه تبدیل کرده است که در آن بیشترین تلاش دستگاه دیپلماسی و سیاست خارجی برقراری روابط با ملت‌ها آن‌هم از طریق رسانه‌ها و در فضای سایبر حاصل از به‌کارگیری آن‌ها است. به‌طوری‌که کارکنان رسانه‌ها و بازیگران غیردولتی بانفوذ به افشاگری می‌پردازند و باانگیزه جلب افکار عمومی به دخالت در مسائل می‌پردازند. این روندها موجب شده است که گفتگو و مذاکره با مقامات برای سفیران بسیار دشوار شود؛ زیرا آنان باید با بازیگران زیاد و درعین‌حال گوناگونی درگیر شوند. اطلاعات گوناگونی کسب نمایند. آن‌هم در شرایطی که شاهد تبدیل بازیگران فراوان به بازیگرانی محدودتر اما هشیارتر، مانند سازمان‌های غیردولتی هستیم که با برخورداری

از توانایی اتخاذ روش‌های سازمان‌یافته و جمعی، نظم دیپلمات‌ها را در تمام جهان دست‌خوش تحول کرده‌اند. همچنین این انقلاب فناورانه- علمی معاصر، سیاست جهانی به‌ویژه کشورهای پیشرفته صنعتی، را شدیداً تحت تأثیر قرار داده است. تحولات فوق به‌شدت از اهمیت فاصله و مکان، به‌عنوان عوامل تعیین‌کننده (چه کسی می‌تواند چه اقدامی برای چه کسی بکند) کاسته است (باربر، ۱۳۸۱: ۱۹۳). در راستای این تحولات و شکل‌گیری فضای مجازی عرصه جدیدی پیش روی حکومت‌ها و دولت‌ها برای استفاده از آن در سطح بین‌المللی گشوده است و فرصت‌ها و آسیب‌هایی را نیز برای آن‌ها فراهم آورده است. در زمینه فرصت‌های پیش روی حکومت‌ها و دولت‌ها مطالب زیادی نوشته‌شده است اما به آسیب‌های ناشی از فضای مجازی بر حکومت‌ها و دولت‌ها کمتر پرداخته‌شده است.

توسعه سواد سایبری در سطح نیروهای مسلح و انتظامی کشور: در حال حاضر فضای مجازی در فضاهای سنتی شامل قلمرو زمینی، دریایی، هوایی و فضایی نفوذ کرده و با کشمکش‌های این قلمروها درآمیخته است (Porche, 2013: 2). در اواخر سال ۱۹۶۰ وزارت دفاع امریکا طرحی را به نام آرپانت[1] طراحی کرد. در این طرح، بخش‌های موردنظر وزارت دفاع امریکا در سراسر کشور به‌صورت شبکه‌ای به یکدیگر متصل شدند تا در صورت وقوع هرگونه اختلال در اثر بمباران، بقیه قسمت‌ها بتوانند ارتباط میان خود را حفظ کنند و هدایت بخش‌های تابعه نیز دچار اختلال نشود. این موفقیت سبب شد، پروژه آرپانت به‌سرعت در مراکز نظامی و دانشگاه‌ها توسعه‌یافته و به دنبال آن رایانه‌های مستقر در این مراکز به یکدیگر مرتبط شده و زمینه‌ساز ظهور اینترنت در جهان شود (حافظ نیا، ۱۳۹۰ :۵۰). به‌تدریج بااتصال دیگر شرکت‌ها و علاقه‌مندان به این شبکه ارتباطی، اینترنت به یک پدیده خارق‌العاده تبدیل شد به‌گونه‌ای که هم‌اکنون دیگر هیچ نیرویی قادر به جلوگیری از توسعه آن نیست و هرروزه میلیون‌ها نفر انسان به این دنیای مجازی راه می‌یابند (میرزا آقایی، ۱۳۸۲: ۱). شبکه‌های ارتباطات غیرنظامی همانند اینترنت نقش بسیار مهمی در جنگ مجازی و عملیات اطلاعاتی داشته و برای بازبینی، واپایش و جنگ اطلاعاتی مورداستفاده قرار می‌گیرند. به‌یقین چنین مسئله‌ای باعث فرسایش انفکاک ساختاری روابط رسانه‌ای، دیپلماسی عمومی و نظامی شده و با توجه به افزایش پیچیدگی صنایع نظامی و تبلیغات رسانه‌ای شده است. در تعریف عملیات اطلاعاتی می‌توان گفت این عملیات‌ها که جنگ را با واقعیت‌های پیچیده قدرت نرم همراه می‌سازند، به جمع‌آوری، شکل‌بخشی، تجزیه‌وتحلیل و اشاعه بی‌وقفه اطلاعات تا تخریب توانمندی رقیب در این زمینه‌ها می‌پردازد. هدف نهایی واصلی

1. Arpanet

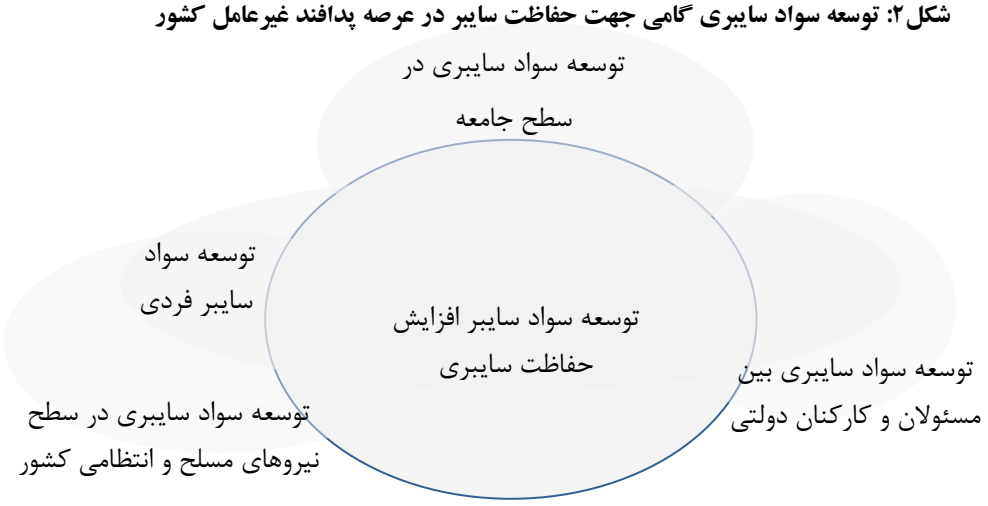
آن‌ها نیز کسب سلطه در قلمرو اطلاعات است (Armistead, 2004: 19). البته کسب برتری در عملیات اطلاعاتی دربرگیرنده اهدافی همچون دست‌یابی به موفقیت‌ها و برتری نظامی در عرصه زمین، هوا، فضا، دریا و عملیات‌های ویژه نیز می‌شود. در فریب نظامی از طریق ارائه اطلاعات، تصاویر یا گزاره‌های نادرست، دشمن به سمت تصمیم‌گیری اشتباه سوق داده می‌شود. فریب نظامی عبارت از مجموعه فعالیت‌هایی است که باهدف گمراه‌سازی طراحان و تصمیم‌گیرندگان امور نظامی دشمن در زمینه قابلیت‌های نظامی نیروهای خودی و درنتیجه سوق دادن دشمن به اتخاذ یا عدم اتخاذ تدابیری معین صورت می‌گیرد که به موفقیت عملیات نظامی نیروهای خودی کمک می‌کند. برای نمونه، در دوره عملیات حمله به عراق، نیروی دریایی امریکا از سیستم تله هوایی باهدف منحرف کردن تمرکز خطوط هوایی عراق از هواپیمای مهاجم اصلی استفاده برد. در ایران توسعه‌ی روزافزون زیرساخت‌های فنّاوری اطّلاعت و ارتباطات در کشور و افزایش کاربران و استفاده‌کنندگان از اینترنت و سایر فنّاوری‌های اطّلاعاتی، ارتباطی و مخابراتی نظیر خطوط تلفن‌های ثابت و همراه، شبکه‌های دیتای کشوری و محلّی، ارتباطات ماهواره‌ای ازجمله‌ی دلایلی است که لزوم ایجاد و توسعه‌ی سازوکاری برای برقراری امنیت در فضای تولید و تبادل اطّلاعات جمهوری اسلامی ایران را توجیه می‌کند. همچنین توسعه‌ی خدمات الکترونیک در کشور نظیر دولت الکترونیک، بانکداری الکترونیک، تجارت الکترونیک، آموزش الکترونیک و سایر خدمات ازاین‌دست، نیز لزوم ایجاد پلیسی تخصّصی در مجموعه‌ی نیروی انتظامی جمهوری اسلامی ایران را برای تأمین امنیت و مقابله با جرایمی که در این فضا به وقوع می‌پیوندند را آشکار می‌کند. از سوی دیگر، رشد قارچ‌گونه‌ی جرایم در حوزه‌ی فضای تولید و تبادل اطّلاعات کشور (فتا) مثل کلاهبرداری‌های اینترنتی، جعل داده‌ها و عناوین، سرقت اطّلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، هرزه‌نگاری و جرایم اخلاقی و برخی جرایم سازمان‌یافته‌ی اقتصادی، اجتماعی و فرهنگی ایجاب می‌کند که پلیس تخصّصی که توان پی‌جویی و رسیدگی به جرایم سطح بالای فنّاورانه داشته باشد، به وجود آید. از سوی دیگر با توجّه به تصویب قانون جرایم رایانه‌ای در مجلس شورای اسلامی و لزوم تعیین ضابط قضایی برای این قانون و نیز مصوّبات کمیسیون تکفای دولت جمهوری اسلامی ایران مبنی بر تشکیل پلیس فضای تولید و تبادل اطّلاعات، این پلیس در بهمن‌ماه سال ۱۳۸۹ به دستور فرماندهی نیروی انتظامی جمهوری اسلامی ایران، تشکیل گردید.

نتیجه‌گیری و پیشنهادها

در گستره روابط انسانی، فضای مجازی، به نسبت نوپاست و از دیدگاه روان‌شناختی با نگاهی موشکافانه به رویدادها، درمی‌یابیم که این فضا تا چه اندازه ممکن است بر زندگی ما اثر گذارد. فضای مجازی زندگی انسان را متحول می‌کند و بر فرهنگ وی تأثیرگذار است. این فضا قطعاً منجر به ارائه روش‌های سریع و کارا در مورد همه وقایع سنن، آداب‌ورسوم جهان می‌گردد، آموزش کلاسیک را متحول کرده و از این طریق دانش عمومی جامعه تغییر نموده و درنهایت یکی از مؤلفه‌های فرهنگ متحول می‌شود. دراین‌بین می‌توان از آسیب‌های فضای مجازی در فضای نامتعادل اجتماعی یاد نمود. در ابعاد امنیتی–اطلاعاتی گزینه‌های فراوانی وجود دارد ازجمله کاهش اقتدار سامانه امنیتی و اطلاعاتی، جاسوسی، آموزش مخرب و ... در بعد اجتماعی مواردی ازجمله ارتباطات نامتعارف میان جوانان، جرائم رایانه‌ای، گسست میان نسلی، بی‌هویت-سازی، تهدید بنیان‌های خانواده، شکل‌گیری خرده فرهنگ‌های مختلف و انتشارات مطالبات قومی و منطقه‌ای و افرایش تحریک‌پذیری قومیت‌ها یاد نمود. در ابعاد سیاسی مواردی مانند ایجاد گروه‌های سیاسی مجازی، اختلال درروند کنترل جریان اطلاع‌رسانی سیاسی، ایجاد گروه-های فشار و ذی‌نفع مجازی، کارکردهای مشروعیتی، دموکراسی دیجیتالی و مکانیسم‌های شایعه‌سازی و بی‌اعتبار سازی مرزها بیان نمود. با توجه به موارد ذکرشده، می‌توان بیان نمود، آگاهی و سواد سایبری در جامعه نقش به‌سزایی ایفا می‌کند. سواد سایبری در کشور در سطوح مختلف جامعه، مسئولان و کارکنان دولتی و به‌ویژه در میان نیروهای مسلح و انتظامی یکی از نیازهای اساسی با توجه به تحولات و وابستگی روزافزون به فضای سایبر می‌باشد که متأسفانه مورد غفلت واقع‌شده است. با توجه به وابستگی روزافزون حکومت‌ها، دولت‌ها و ملت‌ها به فضای سایبر برای استفاده از امکانات و ظرفیت‌های این فضا و ورود کارها، خدمات، وابستگی تأسیسات نظامی و غیرنظامی و حیاتی کشور به این فضای جدید توسعه سواد سایبر (مجازی) در سطوح مختلف یکی از الزامات کشورها برای کاهش آسیب‌پذیری کشور در عصر اطلاعات است که این مهم خود بر یکی از جنبه‌های رو به رشد پدافند غیرعامل یعنی حفاظت سایبر (مجازی) از کشور دلالت می‌کند. زیرا شخصی که دارای سواد سایبری است، علاوه بر سواد سنتی توانایی گردآوری نظام‌مند اطلاعات و ارزیابی آن را دارد. یک باسواد سایبری از قابلیت‌های نرم‌افزار و رایانه آگاه است؛ شبکه‌های اطلاعاتی را می‌شناسد؛ قادر به فهم، درک و تجزیه‌وتحلیل است. داشتن سواد سایبری شخص را خلاق می‌کند و باعث رشد تفکر انتقادی می‌شود. زمینه آموختن و کسب دانش به‌صورت مداوم را ایجاد می‌کند تا شخص به‌عنوان یادگیرنده مستقل به گردآوردی، ارزیابی و تولید دانش بپردازد. بر این اساس می‌توان گفت توسعه سواد سایبر در

کشور در سطوح مختلف آن زمینه کاهش آسیب‌پذیری کشور چه در عرصه جنگ‌های نظامی و چه در عرصه جنگ‌های جدید نظیر جنگ الکترونیکی فراهم می‌آورد و کشورها برای اینکه بتوانند در عصر جدید امنیت خود را فراهم آورند و آسیب‌پذیری خود را کاهش دهند نیازمند آن هستند که سواد سایبری کشور خود را تا حد قابل‌توجهی بالا ببرند. عرصه‌های مختلف توسعه سواد سایبری که به‌صورت‌های مختلف حفاظت سایبری کشور را با رویکرد پدافند غیرعامل بالا می‌برد در شکل (۲) نشان داده‌شده است.

شکل۲: توسعه سواد سایبری گامی جهت حفاظت سایبر در عرصه پدافند غیرعامل کشور



(یافته ها و مطالعات پژوهش)

در جمع‌بندی کلی این مباحث باید گفت توسعه سواد سایبر، می‌تواند نقش مهمی در حفاظت جامعه و ... داشته باشد. می‌توان با اجرای پیشنهادهای زیر تا حدودی از شدت آسیب‌ها و تهدیدات فضای مجازی که ناشی از عدم توسعه سواد سایبری (مجازی) است کاست و ضمن جلوگیری از تبدیل‌شدن آن‌ها به بحران در سطح جامعه توانایی‌های جامعه را برای مقابله با آن‌ها بالابرده تا امنیت اجتماعی در کشور تأمین شود و زمینه رشد و تعالی کشور فراهم آید.

- شناساندن آسیب‌های ناشی از فضای سایبر به افراد، خانواده‌ها و جامعه.
- فعال نمودن انجمن‌های اولیا و مربیان درزمینه آگاهی بخشی درباره آسیب‌های نوپدید فضای مجازی.
- پخش برنامه‌های آموزشی سواد سایبری در شبکه‌های مختلف صداوسیما.
- تدوین و انتشار جزوات و کتاب‌های ویژه برای استفاده مناسب و نقادانه از اطلاعات در سطح جامعه، مدارس و دانشگاه‌ها.

منابع

۱. آلبرتس دیوید، پاپ دانیل. (۱۳۸۵). ***الزامات امنیتی ملی در عصر اطاعات***. پژوهشکده مطالعات راهبردی.

۲. باربر، جیمز، اسمیت، مایکل .(۱۳۸۱). ***ماهیت سیاست‌گذاری خارجی در دنیای وابستگی متقابل کشورها***. ترجمه حسین سیف‌زاده، تهران: انتشارات قومس.

۳. باغ شیخی، احمد. (۱۳۸۸). ***دانستنی‌های عمومی پدافند غیرعامل***. چاپ دوم. تهران: انتشارات معاونت تربیت و آموزش سازمان بسیج مستضعفین.

۴. پور قهرمانی، بابک، صابرنژاد، علی. (۱۳۹۳). نقش آموزش و آگاهی در پیشگیری از انحرافات سایبری، ***اولین کنفرانس فضای سایبر و تحولات فرهنگی*** تبریز ۳۰بهمن ماه ۱۳۹۳.

۵. جان پرور، محسن، حیدری موصلو، طهمورث. (۱۳۹۰). آسیب شناسی فضای سایبر بر امنیت اجتماعی. ***فصلنامه نظم و امنیت انتظامی***. سال چهارم. شماره سوم.

۶. جلالی فراهانی، امیرحسین. (۱۳۸۶). مزیت‌ها و محدودیت‌های فضای سایبر در حوزه‌های آزادی بیان. آزادی اطلاعات و حریم خصوصی، ***حقوقی دادگستری***. تابستان ۱۳۸۶. شماره ۵.

۷. جلالی فراهانی، غلامرضا. (۱۳۹۱). ***مقدمه‌ای بر مبانی نظری پدافند غیرعامل با رویکرد تهدیدات جدید***. تهران. انتشارات دانشگاه امام حسین (ع).

۸. حافظ نیا، محمدرضا. (۱۳۹۰). ***جغرافیای سیاسی فضای مجازی***، انتشارات سمت.

۹. حافظ نیا، محمدرضا و جان پرور، محسن. (۱۳۹۲). ***مرزها و جهانی‌شدن (با نگاهی کوتاه به مرزهای ایران)***. تهران. انتشارات پژوهشکده مطالعات راهبردی.

۱۰. حسن بیگی، ابراهیم. (۱۳۸۴). ***حقوق و امنیت در فضای سایبر***. تهران. موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.

۱۱. حسینی، پرویز، ظریف منش، حسین. (۱۳۹۲). مطالعه تطبیقی ساختار دفاع سایبری کشورها. ***فصلنامه پژوهش‌های حفاظتی-امنیتی***، دانشگاه امام حسین. سال دوم. شماره۵.

۱۲. خلیلی‌پور رکن‌آبادی، علی، نورعلی وند، یاسر. (۱۳۹۱). تهدیدات سایبری و تأثیرات آن بر امنیت ملی. ***فصلنامه مطالعات راهبردی***. سال۱۵. شماره۲. تابستان ۱۳۹۱. شماره مسلسل ۵۶.

۱۳. زارعی، جواد، آرمات، فیروزه، عبدالخانی، رباب. (۱۳۹۲). بررسی میزان آشنایی کارکنان بخش مدارک پزشکی بیمارستان‌های دانشگاهی اهواز با رایانه و مفاهیم پایه فناوری اطلاعات در سال ۱۳۹۰. ***فصلنامه علمی پژوهشی ماب و تزکیه***. بهار ۱۳۹۲ . دوره ۲۲. شماره ۱.

۱۴. سلطانی فر، محمد. (۱۳۸۷). تحلیل وضعیت سواد اینترنتی دانش آموزان سال سوم دبیرستان شهر تهران ۱۳۸۵-۱۳۸۶ درمقایسه با مربیان و والدین آن‌ها، ***فصلنامه نوآوری‌های آموزشی***. شماره۲۷. سال هفتم. پاییز۱۳۸۷.

۱۵. صالحی، محمد، حاجی‌زاده، محمد. (۱۳۸۹). بررسی سواد عمومی کامپیوتری کارکنان دانشگاه‌های آزاد اسلامی استان مازندران. ***فصلنامه فن‌آوری اطلاعات و ارتباطات در علوم تربیتی***. سال اول شماره اول پاییز۱۳۸۹.
۱۶. صدوقی، مرادعلی. (۱۳۸۲). ***تکنولوژی اطلاعات و حاکمیت ملی***. چاپ دوم. تهران: انتشارات وزارت خارجه.
۱۷. قادی، مجتبی. (۱۳۸۶). بررسی رابطه استفاده از اینترنت و هویت دینی کاربران. ***فصلنامه رسانه***. شماره۶۹.
۱۸. قاسمی، علی، چهار بخش، ویکتور بارین. (۱۳۹۱). حملات سایبری و حقوق بین الملل. ***مجله حقوقی دادگستری***. شماره۷۸.
۱۹. قصری، محمد، جان پرور، محسن، حیدری موصلو، طهمورث. (۱۳۸۹). مدیریت مرزهای فضای سایبر، گام نخست دفاع سایبری. ***مجموعه مقالات نخستین همایش ملی دفاع سایبری***.
۲۰. کاستلز، مانوئل. (۱۳۸۱). ***عصر اطلاعات (اقتصاد، جامعه و فرهنگ)***، مترجمان احمد علیقلیان. افشین خاکباز. انتشارات طرح نو.
۲۱. کاوندی کاتب، ابوالفضل، میرزایی، میثم. (۱۳۸۹). جهانی شدن اسلام و فضای سایبر. ***فصلنامه ادیان و عرفان اندیشه تقریب***. تابستان ۱۳۸۹. شماره ۲.
۲۲. کروبی، محمدتقی و صدری، محمدرضا. (۱۳۸۴). ابعاد حقوقی محیط سایبر در پرتو توسعه ملی. ***مجموعه سخنرانی‌ها و مقالات اولین همایش حقوق فن‌آوری اطلاعات و ارتباطات کشور***. تهران. انتشارات بقعه.
۲۳. محمدعلیپور، نسرین و کریمی، منصوره. (۱۳۸۶). بررسی تطبیقی پیرامون مطالعات مربوط به آموزش الکترونیکی. ا***ولین کنفرانس بین‌المللی شهر الکترونیک***.
۲۴. معنوی، فیروزه. (۱۳۸۳). ***سواد رایانه‌ای؛ ضرورت یا هیاهو***. اطلاع‌رسانی و کتابداری. بهار ۱۳۸۳. شماره۳.
۲۵. منطقی، مرتضی. (۱۳۸۷). ***تلفن همراه راهنمای والدین در استفاده فرزندان از فن‌آوری-های ارتباطی جدی***. چاپ دوم. تهران: انتشارات عابد.
۲۶. اطلاع‌رسانی و کتابداری. ***فصلنامه مطالعات ملی کتابداری و سازماندهی اطلاعات***. بهار ۱۳۸۵ - شماره ۶.
۲۷. میرزا آقایی، حمید. (۱۳۸۲). نگاهی به جهان امروز و آشنایی با دنیای اینترنت. ***روزنامه اعتماد***. ۱۵ بهمن۱۳۸۲.
۲۸. نورمحمدی، مرتضی. (۱۳۹۰). جنگ نرم فضای سایبر و امنیت جمهوری اسلامی ایران. ***فصلنامه علمی پژوهشی علوم اجتماعی راهبرد فرهنگ***. شماره۱۶.

۲۹. هادوی نیا، عباس، محترم قلانی، رحیم. (۱۳۹۱). جایگاه اعتماد اطلاعاتی در سپهر خط مشی دفاعی کشور (ارائه چارچوب پژوهشی برای مطالعه راهبرد دفاع در عمق برای مقابله با تهدیدات رایانه‌ای). ***مجله سیاست دفاعی***. سال بیستم. شماره۷۹. تابستان.

30. *http://hamshahrionline.ir/news*-4411 *.asp*
31. Armistead, Edwin l. (2004). ***Information operations: warfare and the hard reality of soft powerT Potomac books inc***
32. Bork,howard. (1993). ***Education as marketplace***. In computer in education. Cresskill. N,j: Hampton pr
33. Livingstone, Sonia; Thumim, N.(2001). ***'Assessing the media literacy of UK adults***: a ... Edited by Livingstone, S.; Bovill, M. Lawrence Erlbaum Associates
34. Porche & Others. (2013). ***Redefining Information Warfare Boundaries for an Army in a Wireless World***. RAND: USA.
35. Wilske (2004). ***International law jurisdiction***. Available:file:/a:/wilske.html.