Specialized Scientific Quarterly Journal of

Arman Process (APJ)

Investigating the security challenges in cyberspace

N. Mojtabazadeh [*,1]

[1] *Department of Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran*

KEYWORDS:

Security management
Computer crimes
Information security technologies
Encryption

Corresponding author
n.mojtabazadeh@yahool.com

ABSTRACT

From the beginning of human life, security has been one of the main concerns of human beings. Today, with the expansion of the Internet and networked spaces in our country, the need for security to operate in these virtual spaces is felt more than ever. Fear of destroying moral and social foundations, and lack of psychological and cultural security due to the influx of contaminated and destructive information through the Internet and cyberspace is a logical response, because each society has its own information frameworks. It is natural that any kind of information that breaks these boundaries can endanger the health and security of society. Despite the positive aspects of global networks, the misuse of these computer networks by norm-breakers has endangered national security in various countries. Therefore, the use of various methods and solutions to prevent the penetration of malicious data and the selection of healthy information in these networks is increasing. Fortunately, despite the much hype that makes the World Wide Web and cyberspace uncontrollable, the technology needed to control the network and select healthy information is evolving. In this article, we first get acquainted with topics such as cyber security and cybercrime and its types, then deal with various types of information technologies in general and provide examples of it, and finally with the pathology of security space and information We will address the country and review the challenges and solutions to meet these challenges.

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
12	0	0

فصلنامه تخصصی

آرمان پردازش

بررسی چالش های امنیتی در فضای سایبری

نیما مجتبی زاده [1,*]

[1] *گروه مهندسی کامپیوتر، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران*

چکیده

از ابتدای زندگی بشر امنیت یکی از دغدغه های اصلی انسان ها بوده است، امروزه با گسترش اینترنت و فضاهای شبکه ای در کشورمان لزوم امنیت برای فعالیت در این فضاهای مجازی بیش از پیش احساس می شود. طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکند، می تواند سلامت و امنیت جامعه را به خطر اندازد. برخلاف وجود جنبه های مثبت شبکه های جهانی، سوء استفاده از این شبکه های رایانه ای توسط افراد هنجارشکن، امنیت ملی را در کشورهای مختلف با خطر روبرو ساخته است. از این رو به کارگیری روش ها و راه کارهای مختلف برای پیشگیری از نفوذ دادههای مخرب و مضر و گزینش اطلاعات سالم در این شبکه ها رو به افزایش است. خوشبختانه با وجود هیاهوی بسیاری که شبکه جهانی اینترنت و فضاهای سایبر را غیرقابل کنترل معرفی می کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم رو به گسترش و تکامل است. در این مقاله ابتدا با عناوینی چون امنیت در فضای سایبر و جرائم رایانه ای و انواع آن آشنا می شویم، سپس به انواع فناوری های اطلاعات به طور کلی پرداخته و نمونه هایی از آن را ارائه نموده، در نهایت به آسیب شناسی فضای امنیت و اطلاعات در کشور می پردازیم و چالش ها و راهکارهای مقابله با این چالشها را مرور می نماییم.

واژگان کلیدی:
مدیریت امنیت
جرائم رایانه ای
فناوری های امنیت اطلاعات
رمزگذاری

[1] نویسنده مسئول

n.mojtabazadeh@yahool.com

تعداد جداول	تعداد شکل ها	تعداد مراجع
۰	۰	۱۲

مقدمه

مهمترین مزیت و رسالت شبکه های رایانه ای، اشتراک منابع سخت افزاری و نرم افزاری و دست یابی سریع و آسان به اطلاعات است. کنترل دستیابی و نحوه استفاده از منابعی که به اشتراک گذاشته شده اند، از مهم ترین اهداف یک نظام امنیتی در شبکه است. با گسترش شبکه های رایانه ای (خصوصا اینترنت)، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته شده، وارد مرحله جدیدی گردیده است. در این راستا لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند خود، به یک راهبرد خاص پایبند باشد و براساس آن، نظام امنیتی را اجرا نماید. نبود نظام مناسب امنیتی، بعضا پیامدهای منفی و دور از انتظاری را به دنبال دارد. توفیق در ایمن سازی اطلاعات، منوط به حفاظت از اطلاعات و نظام های اطلاعاتی در مقابل حملات است؛ بدین منظور از سرویس های امنیتی متعددی استفاده می گردد. سرویس های انتخابی باید پتانسیل لازم در خصوص ایجاد یک نظام حفاظتی مناسب، تشخیص به موقع حملات، و واکنش سریع را داشته باشند. بنابراین می توان محور راهبردی انتخاب شده را بر سه مؤلفه حفاظت، تشخیص و واکنش استوار نمود. حفاظت مطمئن، تشخیص به موقع و واکنش مناسب، از جمله مواردی هستند که باید همواره در ایجاد یک نظام امنیتی رعایت شود. مقاله حاضر با توجه به این رویکرد به طبقه بندی فناوری های امنیت اطلاعات، براساس دو ویژگی خواهد پرداخت؛ اول مرحله خاصی از زمان که در هنگام تعامل فناوری با اطلاعات، عکس العمل لازم در برابر یک مشکل امنیتی، ممکن است به صورت کنشی یا واکنشی باشد، و دوم سطوح پیادسازی نظام های امنیتی در یک محیط رایانه ای [1, 2].

اهمیت و ضرورت امنیت در فضای مجازی

امنیت مجازی شاید به شکل قابل توجه آن، موضوع حیاتی برای کشورها باشد. چرا که شرط لازم برای تهدیدپذیری از دنیای مجازی، استفاده گسترده و اتصال به شبکه های الکترونیکی اطلاعات است و شرط کافی، دیجیتالی شدن تمامی سیستم ها و زیرساخت های اقتصادی، اجتماعی، سیاسی یک جامعه می باشد. در عین حال نباید فراموش کرد که گسترش ارتباطات و انقلاب تکنولوژیکی، بسیاری از مسائل امنیتی را جهانی ساخته و شمال و جنوب در این زمینه دارای مسائل مشترکی هستند. به نظر می رسد لازم باشد در فضای مجازی این مفاهیم ابتدا مورد باز تعریف قرار گیرند و سپس به گفتمان امنیتی وابسته بدان پرداخته شود. اما در شرایطی که تمامی این مفاهیم خود بر ماهیت دگرگون شونده و متلون اصرار می ورزند و بر مصداق های گوناگونی دلالت دارند این امر به راحتی امکان پذیر نیست [3].

اهداف تحقیق

- بررسی چالش های اساسی حوزه امنیت فضای مجازی؛
- شناخت مراجع و مراکز دخیل و ذی نفوذ در حل مسائل حوزه امنیت در فضای مجازی؛
- بررسی چشم انداز اولیه در صورت ادامه روند موجود؛
- بررسی چشم انداز مطلوب در حوزه امنیت مجازی؛

سؤالات تحقیق

- چالش های اساسی در امنیت فضای مجازی دنیا کدامند؟
- عوامل دخیل در حل این مسائل کدامند؟
- چشم انداز مطلوب و راه حل ها در حوزه امنیت چیست؟

جرائم رایانه ای

فضای سایبر در معنا به مجموعه هایی از ارتباطات درونی انسان ها از طریق رایانه و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود. به امنیت فناوری اطلاعات، وابسته به سیاست دولت ها، امنیت سایبر می گوئیم. این اصطلاح عموما توسط مؤسسه های دولتی و سیاستگذاران ملی در اسناد، قوانین و پروژه‌های تحقیقاتی استفاده میشود و کمابیش مترادف با " امنیت اینترنت" است. هر دو عبارت به جوانب امنیت شبکه و اصول سیاستگذاری شبکه ها مثل تعریف حریم خصوصی، جرائم سایبر، تجارت و ارتباطات جهانی اشاره دارند. جرم رایانه ای بر دو نوع است: در تعریف محدود (مضیق) جرمی که در فضای مجازی سایبر) رخ می دهد جرم رایانه ای است و بر اساس این دیدگاه، اگر رایانه ابزار و وسیله ارتکاب جرم باشد آن جرم را نمی توان در زمره جرائم رایانه ای قلمداد کرد. در تعریف گسترده (موسع) هر فعل یا ترک فعلی که « از طریق» یا «به کمک سیستم های رایانه ای» رخ میدهند جرم رایانه ای قلمداد می شود. روش های گوناگونی برای دسته بندی و بررسی مجرمین رایانه ای وجود دارد. این کار با یک دسته بندی ساده و معمولی تفاوت دارد. روش های گوناگونی برای طبقه بندی مجرمین رایانه ای وجود دارد، ما آنها را به سه دسته شامل نفوذکننده های غیرمجاز، مجرمین و خرابکاران تقسیم می کنیم [1, 4-6].

این دسته بندی ها مقدار زیادی همپوشانی دارد. از منظری دیگر آنها بر پایه انگیزه ها دسته بندی می شوند: انگیزه اصلی نفوذ کننده غیرمجاز، دسترسی به سیستم یا داده هاست. انگیزه اصلی مجرمین، دست یابی و انگیزه اصلی خرابکاران، ایراد خسارت است. هر چند از مرتکبین هر سه گروه به عنوان مجرم نام برده می شود ولی طبقه بندی مجرمین بر دو رفتار اصلی مجرمانه متمرکز می شود: جاسوسی و کلاهبرداری. در عصر حاضر (خودکارسازی و ارتباطات)، تقریبا هیچ سازمانی از جرائم رایانه

ای مصون نیست. این بخش رایج ترین اهداف در جرائم رایانه ای را مورد توجه قرار می دهد • رایانه های نظامی و انتظامی ممکن است بوسیله سازمانهای جاسوسی مورد هدف قرار گیرند [7].

• تاجرها ممکن است به وسیله رقبا مورد هدف قرار گیرند.

• بانک ها و دیگر سازمان های مالی، ممکن است بوسیله جنایتکاران حرفه ای مورد هدف قرار گیرند.

• هر سازمان به ویژه دولت و رایانه های مربوط به شرکت های خدمات رسانی همگانی ممکن است به وسیله تروریست ها مورد هدف حمله قرار گیرند.

• هر سازمانی ممکن است به وسیله رباینده‌گان مورد هدف قرار گیرد. در پاردای از موارد مهاجمین برای مبارزات هوشمندانه تر این کار را انجام میدهند و در مواردی دیگر آنها افراد ماهری هستند که برای ارضای خود این کار را انجام میدهند.

این بخش به انواع مختلف حملات رایانه ای از دستکاری حسابهای بانکی و استراق سمع مکالمات گرفته تا برنامه ریزی جهت انجام هرگونه خرابکاری بوسیله ویروس ها می پردازد.

فناوری های امنیت اطلاعات

امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخشهای غیر مجاز اشاره دارد. امنیت اطلاعات مجموعه ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری و علم مطالعه روشهای حفاظت از داده ها در رایانه ها و نظام های ارتباطی در برابر دسترسی و تغییرات غیر مجاز است. با توجه به تعاریف ارائه شده، امنیت به مجموعه ای از تدابیر، روش ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیر مجاز در نظام های رایانه ای و ارتباطی اطلاق می شود. «فناوری امنیت اطلاعات» به بهره گیری مناسب از تمام فناوری های امنیتی پیشرفته برای حفاظت از تمام اطلاعات احتمالی روی اینترنت اشاره دارد. طبقه بندی ارائه شده در مقاله حاضر از فناوری های امنیت اطلاعات، در وهله اول براساس دو ویژگی پایه گذاری شده است. براساس مرحله خاصی از زمان بدین معنا که در زمان تعامل فناوری با اطلاعات، عکس العمل لازم در برابر یک مشکل امنیتی میتواند کنشگرایانه (کنشی) یا واکنشی باشد. غرض از «کنشگرایانه»، انجام عملیات پیشگیرانه قبل از وقوع یک مشکل خاص امنیتی است. در چنین مواردی به موضوعاتی اشاره می گردد که ما را در پیشگیری از وقوع یک مشکل کمک خواهد کرد (چه کار باید انجام دهیم تا ...؟). غرض از «واکنشی» انجام عکس العمل لازم پس از وقوع یک مشکل خاص امنیتی است. در چنین مواردی به موضوعاتی اشاره می گردد که ما را در مقابله با یک مشکل پس از وقوع آن، کمک خواهند کرد (اکنون که به چه کار باید انجام بدهیم ؟). بر اساس سطوح پیاده سازی نظام های امنیتی در یک محیط رایانه ای: فناوری امنیت اطلاعات را، خواه از نوع کنشی باشد یا واکنشی، می توان در سه سطح شبکه، میزبان و برنامه کاربردی قابل پیاده سازی می باشند. بدین منظور می توان نظام امنیتی را در سطح شبکه و خدمات ارائه شده آن، در سطح برنامه کاربردی خاص، یا در محیطی که شرایط لازم برای اجرای یک برنامه را فراهم می نماید (سطح میزبان پیاده کرد [4, 8].

آسیب شناسی تأمین امنیت در فضای مجازی

بسیاری از دولت ها و جوامع، خواسته و یا ناخواسته هنوز هم متوجه تغییر عظیمی که در مناسبات جهانی روی داده است نشده، و نپذیرفته اند که پیوستن آنها به جمع جوامع اطلاعاتی پیشرفته، امتیازات بسیاری برای آنها در پی خواهد داشت. علاوه بر این، حتی اگر اکنون درصد وسیعی از تعاملات تجاری، اداری و اجتماعی جهان به شکل الکترونیک انجام شده و سهم آنها از این روند مطلوب و کار آمد، در حد صفر باشد و نیز اگر آمارهای معتبر و قابل استناد جهانی، آخرین رتبه های نفوذ روابط الکترونیک در میان جوامع را به آنها اختصاص دهد، شاید باز هم کار آمدی فناوری اطلاعات را در فعالیتهای کلان مدیریتی خود لحاظ نکنند. متأسفانه، ادامه این روند و اصرار بر این نپذیرفتن، به کاهش محسوس باز دهی و افت قدرت تأثیر گذار این دولت ها و ملتها در جامعه جهانی خواهد انجامید. چراکه تعاملات الکترونیکی و به طور خاص شکل کلان آنها، بی گمان به روندی بی چون و چرا و غیر قابل اجتناب تبدیل خواهد شد. به نظر می رسد که تلاش بسیاری از دولت ها برای کنترل دنیای الکترونیک، وجود مدیریت سنتی در ساختار اداری سیاسی و نیز عدم اعتنای توده مردم به روشهای نوین تعامل با حکومت، از مهمترین دلایل عدم افزایش فعالیت های کلان الکترونیکی باشد. هرچند عملکرد نهادهای دولتی و غیر دولتی، دارای تأثیر متقابل و قابل توجهی بر یکدیگر هستند، اما در میان کلیه نهادها و تشکل هایی که به شکل آنلاین و الکترونیک به فعالیت می پردازند، دولت های الکترونیک از مهمترین و بالاترین جایگاه برخوردار هستند. دلیل این مسأله نیز کاملا واضح است. حجم قابل توجه، وسیع و متنوع تعاملات آنها به شکل درون یا برون سازمانی، تأثیر عمده و گسترده ای را بر کلیه ابعاد و شئون اجتماع خواهد داشت. شاید بتوان گفت بارزترین مزیت استفاده از روشهای نوین در فعالیتهای کلان، افزایش سرعت رسیدگی به مشکلات و حل مسائل کلان کشورها و نیز صرفه جویی در منابع و ظرفیت های موجود است. تجربه انجام موفقیت آمیز بسیاری از فعالیتهای کلان تجاری، اداری، نظارتی و از این دست، به شکل الکترونیکی و آنلاین، توسط برخی از دولت ها، نشان داده که این شیوه مدرن قادر است علاوه بر افزایش بازده و سرمایه های برگشتی، از فرسایش قابل توجه نیرو ومنابع انسانی بکاهد. باید گفت که تلاش و صرف

هزینه در جهت تحقق و پیشبرد دولت الکترونیک، با توجه به مزایا و بازدهی فراوان آن در کوتاه مدت، خود پیش شرط لازم برای احساس نیاز به ایجاد امنیت در آن است. علاوه بر این، تجربه کشورهای پیشرو در این حوزه، استفاده از گواهی نامه های امنیتی موجود و نیز دسترسی آسان (البته برای کشورهای خارج از محدوده تحریم های جهانی به فناوری های حفاظتی قدرتمند، تضمینی برای قدرت، قوت و استحکام لایه های امنیتی در تعاملات درون و برون سازمانی دولت های الکترونیک، محسوب میشوند. از دیدگاه برخی از کارشناسان، تحقق دولت الکترونیک، مقدم بر بحث امنیت در آن است و کشورها باید تمام سعی خود را برای پرهیز از عواقب وخیم عقب ماندگی از جهان الکترونیک با تعاملات سریع، آسان و ارزان آن، بکار گیرند. در نهایت، می توان فهرستی از موانع بزرگ و کوچک در راه تحقق و تأمین امنیت دولت های الکترونیک را در نظر گرفت. این موانع، که اغلب خواسته یا ناخواسته، به علل مختلف اجتماعی، سیاسی و فرهنگی و در طول زمان ایجاد شدهاند با اعتماد و همکاری نزدیک میان دولت ها و ملتها، ایجاد زیرساخت و بسترهای لازم و نیز توجه بیشتر به جهانی شدن (با حفظ ارزشها و آرمانهای فرهنگی، اجتماعی)، رفته رفته در کوتاه مدت از بین رفته و زمینه تحقق دولتهای الکترونیک یکپارچه و یا مستقل، در سرتاسر جهان، ایجاد خواهد کرد. البته جوامع و توده مردم نیز با عدم اعتماد خود به روشهای نوین، حضور غیر فیزیکی و غیر ملموس برای انجام فعالیتها و پیگیری مسائل، ترجیح دادن روشهای سنتی در تعامل خود با دولت برخلاف وجود ساختارهای لازم برای ارتباط الکترونیک و نیز عدم تمایل به استفاده از نرم افزارهای کامل، رسمی و ثبت شده برای تأمین امنیت لازم در فعالیتهای تجاری، اداری و مالی خود، نشان دادهاند که مانعی بزرگ برای تحقق امنیت دولتهای الکترونیک محسوب می شوند. به هر ترتیب، باید پذیرفت که کشورهای در حال توسعه برای پیشرفت و ارتقاء همه جانبه خود، چاره ای جز ورود به دنیای یکپارچه الکترونیک، نخواهند داشت. هرچند ورود به این دنیا، صرف هزینه ها و منابع خاصی را می طلبد، اما مدت زمان اندک برای بازدهی قابل توجه، صرفه جویی های بسیار در منابع ملی و جهانی، ایجاد اتحاد، همدلی و همکاری نزدیک میان ملتها و دولت ها و نیز عواقب ناخوشایند ناشی از طرد شدن از جامعه جهانی اطلاعات، روز به روز تمایل دولت ها را برای انجام تعاملات و فعالیت های الکترونیکی، افزایش میدهد.

چالش ها و موانع اساسی فراروی امنیت در فضای مجازی و اینترنت

درحال حاضر و در دهه اخیر مهم ترین چالشهای امنیت سایبری در دنیا به شرح زیر می باشند [12-10] :

- **حملات باج افزار**

حملات باجافزاری در چند سال اخیر رایج شدهاند و یکی از برجستهترین چالشهای امنیت سایبری هند در سال ۲۰۲۰ است. طبق گزارش شرکت امنیت سایبری Sophos، حدود ۸۲ درصد از سازمانهای هندی در شش ماه گذشته مورد حمله باجافزار قرار گرفتهاند. حملات باجافزاری شامل هک کردن دادههای کاربر و جلوگیری از دسترسی آنها به آن تا زمانی که مبلغ باج پرداخت شود، میشود. حملات باجافزار برای کاربران فردی حیاتی است، اما بیشتر برای مشاغلی که نمیتوانند به دادهها برای اجرای عملیات روزانه خود دسترسی داشته باشند، بسیار مهم است. با این حال، در بیشتر حملات باجافزار، مهاجمان حتی پس از انجام پرداخت، دادهها را منتشر نمیکنند و در عوض سعی میکنند پول بیشتری را اخاذی کنند.

- **حملات IoT**

بر اساس تجزیه و تحلیل اینترنت اشیا، تا سال ۲۰۲۱ حدود ۱۱,۶ میلیارد دستگاه اینترنت اشیا وجود خواهد داشت. نمونههایی از دستگاههای اینترنت اشیا شامل رایانههای رومیزی، لپتاپ، تلفنهای همراه، دستگاههای امنیتی هوشمند و غیره میشود. همانطور که استفاده از دستگاههای اینترنت اشیا با سرعت بیسابقهای در حال افزایش است، چالشهای امنیت سایبری نیز افزایش مییابد. حمله به دستگاه های اینترنت اشیا می تواند منجر به به خطر افتادن داده های حساس کاربر شود. حفاظت از دستگاه های اینترنت اشیا یکی از بزرگترین چالش ها در امنیت سایبری است، زیرا دسترسی به این دستگاه ها می تواند درها را برای سایر حملات مخرب باز کند.

- **حملات ابری**

بسیاری از ما امروزه از خدمات ابری برای نیازهای شخصی و حرفه ای استفاده می کنیم. همچنین، هک کردن پلتفرمهای ابری برای سرقت اطلاعات کاربران یکی از چالشهای امنیت سایبری برای کسبوکارها است. همه ما از هک بدنام iCloud که عکس های خصوصی افراد مشهور را فاش کرد، آگاه هستیم. اگر چنین حمله ای بر روی داده های سازمانی انجام شود، می تواند تهدیدی بزرگ برای سازمان باشد و حتی ممکن است منجر به فروپاشی آن شود.

- **حملات فیشینگ**

فیشینگ نوعی حمله مهندسی اجتماعی است که اغلب برای سرقت اطلاعات کاربر از جمله اعتبار ورود و شماره کارت اعتباری استفاده می شود. برخلاف حملات باج افزار، هکر پس از دسترسی به اطلاعات محرمانه کاربر، آن را مسدود نمی کند. در عوض، آنها از آن برای مزایای خود مانند خرید آنلاین و انتقال غیرقانونی

پول استفاده می کنند. حملات فیشینگ در میان هکرها رایج است زیرا می توانند از داده های کاربر سوء استفاده کنند تا زمانی که کاربر از آن مطلع شود. حملات فیشینگ یکی از چالش‌های اصلی امنیت سایبری در هند باقی می‌ماند، زیرا جمعیت‌شناسی در اینجا با مدیریت داده‌های محرمانه آشنا نیست.

- **حملات بلاک چین و ارزهای دیجیتال**

در حالی که بلاک چین و ارزهای دیجیتال ممکن است برای کاربران عادی اینترنت اهمیت زیادی نداشته باشند، این فناوری‌ها برای کسب‌وکارها معامله بزرگی هستند. بنابراین، حملات به این چارچوب ها چالش های قابل توجهی در امنیت سایبری برای مشاغل ایجاد می کند زیرا می تواند داده های مشتری و عملیات تجاری را به خطر بیندازد. این فناوری ها از مراحل اولیه خود فراتر رفته اند اما هنوز به مرحله ایمن پیشرفته نرسیده اند. بنابراین، چندین حمله مانند DDOS، Sybil و Eclipse بوده اند. سازمان ها باید از چالش های امنیتی همراه با این فناوری ها آگاه باشند و اطمینان حاصل کنند که هیچ شکافی برای تهاجم و بهره برداری متجاوزان باز نمی شود.

- **آسیب پذیری های نرم افزار**

حتی پیشرفته‌ترین نرم‌افزارها دارای آسیب‌پذیری‌هایی هستند که ممکن است چالش‌های مهمی برای امنیت سایبری در سال ۲۰۲۰ ایجاد کند، با توجه به اینکه استفاده از دستگاه‌های دیجیتال در حال حاضر بیش از هر زمان دیگری است. افراد و شرکت‌ها معمولاً نرم‌افزار این دستگاه‌ها را به‌روزرسانی نمی‌کنند، زیرا آن را غیرضروری می‌دانند. با این حال، به روز رسانی نرم افزار دستگاه شما با آخرین نسخه باید در اولویت باشد. یک نسخه نرم افزار قدیمی ممکن است حاوی وصله هایی برای آسیب پذیری های امنیتی باشد که توسط توسعه دهندگان در نسخه جدیدتر برطرف شده است. حمله به نسخه های نرم افزار بدون وصله یکی از چالش های اصلی امنیت سایبری است. این حملات معمولاً بر روی تعداد زیادی از افراد انجام می شود.

- **یادگیری ماشین و حملات هوش مصنوعی**

در حالی که فناوری‌های یادگیری ماشین و هوش مصنوعی برای توسعه گسترده در بخش‌های مختلف بسیار مفید هستند، آسیب‌پذیری‌های خود را نیز دارد. این فناوری‌ها می‌توانند توسط افراد غیرقانونی برای انجام حملات سایبری و ایجاد تهدید برای مشاغل مورد سوء استفاده قرار گیرند. این فناوری ها را می توان برای شناسایی اهداف با ارزش بالا در میان مجموعه داده های بزرگ مورد استفاده قرار داد. یادگیری ماشینی و حملات هوش مصنوعی یکی دیگر از نگرانی های بزرگ در هند است. به دلیل فقدان تخصص امنیت سایبری در کشور ما، رسیدگی به یک حمله پیچیده ممکن است بسیار دشوار باشد.

- **سیاست های BYOD**

اکثر سازمان ها یک خط مشی Bring-Your-Own-Device برای کارمندان خود دارند. وجود چنین سیستم هایی چالش های متعددی را در امنیت سایبری ایجاد می کند. اولاً، اگر دستگاه از نسخه قدیمی یا غیرقانونی نرم افزار استفاده می کند، در حال حاضر یک رسانه عالی برای دسترسی هکرها است. از آنجایی که این روش به دلایل شخصی و حرفه ای استفاده می شود، هکرها می توانند به راحتی به داده های تجاری محرمانه دسترسی پیدا کنند. ثانیاً، این دستگاه‌ها دسترسی به شبکه خصوصی شما را در صورت به خطر انداختن امنیت آنها آسان‌تر می‌کنند. بنابراین، سازمان‌ها باید سیاست‌های BYOD را کنار بگذارند و دستگاه‌های ایمن را در اختیار کارمندان قرار دهند، زیرا چنین سیستم‌هایی دارای چالش‌های عظیم امنیت رایانه و به خطر افتادن کارکرد شبکه ها و سرویس های مرتبط هستند.

- **حملات خودی**

در حالی که بیشتر چالش‌های امنیت سایبری برای مشاغل خارجی هستند، می‌توانند نمونه‌هایی از یک شغل داخلی وجود داشته باشد. کارمندان با نیت مخرب می توانند داده های محرمانه را به رقبا یا افراد دیگر درز کنند یا صادر کنند. این امر می تواند منجر به ضررهای مالی و اعتباری هنگفت برای کسب و کار شود. این چالش های امنیت رایانه را می توان با نظارت بر داده ها و ترافیک شبکه ورودی و خروجی از بین برد. نصب دستگاه‌های فایروال برای مسیریابی داده‌ها از طریق یک سرور متمرکز یا محدود کردن دسترسی به فایل‌ها بر اساس نقش‌های شغلی می‌تواند به به حداقل رساندن خطر حملات خودی کمک کند.

- **سخت افزارهای قدیمی**

خب تعجب نکن همه چالش‌های امنیت سایبری به شکل حملات نرم‌افزاری ظاهر نمی‌شوند. با درک خطر آسیب پذیری نرم افزار توسط توسعه دهندگان نرم افزار، به روز رسانی دوره ای را ارائه می دهند. با این حال، این به روز رسانی های جدید ممکن است با سخت افزار دستگاه سازگار نباشد. این همان چیزی است که منجر به منسوخ شدن سخت افزار می شود، که در آن سخت افزار به اندازه کافی برای اجرای آخرین نسخه های نرم افزار پیشرفته نیست. این باعث می‌شود که چنین دستگاه‌هایی روی نسخه‌های قدیمی‌تر نرم‌افزار قرار بگیرند و آنها را به شدت در معرض حملات سایبری قرار دهد.

لازم به ذکر است، همچنین در جریان سیاستگذاری برای امنیت فضای سایبر و اینترنت در کشور ما چالش ها و موانع جدی وجود دارد. این چالش ها و موانع عبارتند از :

- فقدان راهبرد مشخص در زمینه توسعه الکترونیک
- فقدان متولی مشخص در حفاظت از دادههای موجود در سامانه های نظامی، امنیتی، اقتصادی

- عدم وجود قانون کپی رایت و حفظ حقوق مادی و معنوی افراد در کشور؛
- فقدان سیاست ملی فضای سایبر، اینترنت و مخابراتی
- روشن نبودن سیاست ها در مورد گسترش اینترنت، تلفن همراه و مخابرات دادههاء
- روشن نبودن میزان ظرفیت دولت در پذیرش مشارکت بخش خصوصی در وارد کردن و توزیع اینترنت
- فقدان سیاست روشن گمرکی در مورد مجاز یا ممنوع بودن واردات تجهیزات، دریافت و ارسال ماهواره ای
- افزایش احتمال دستبرد اطلاعات محرمانه کشور و یا خرابکاری توسط بیگانگان
- افزایش جرائم پنهانی در فضای مجازی و حرفه ای شدن مجرمین با افزایش استفاده از شبکه های مجازی در دستگاهها و نهادهای دولتی و خصوصی
- فقدان سیاست مشخص ملی در آموزش و اطلاع رسانی

هیچ قانون یا دستور العملی برای منع رمز گذاری محتوای دادههای مبادله شده وجود ندارد و هیچ قانونی نیز وجود ندارد که سرویس دهندگان را ملزم به کنترل محتوا نماید یا آنان را مسئول محتوای سایت های روی سرویس بداند از طرف دیگر خدمات اینترنت در ایران به سرعت ارزان شده و کافه های اینترنتی به سرعت در حال رشد است و هیچ قانون خاصی برای نحوه تأسیس و نحوه اداره آن وجود ندارد. به نظر می رسد تهدید اصلی و بالفعل کشور در مورد اینترنت، فقدان گفتمان امنیتی در مورد این پدیده است. اینترنت که به طور بالقوه می تواند هم تهدید و هم فرصتی طلایی برای امنیت فرهنگی و سیاسی باشد، به وسیله ای برای فشار سیاسی و اقتصادی تبدیل شده است. برای تحلیل فرایند سیاستگذاری در مورد اینترنت در ایران، پاسخ به سؤالاتی در مورد آزادی بیان، کنترل جریان اطلاعات، قوانین مربوط و نظریه هنجاری حاکم بر رسانه های جدید ضروری است. افراد، سازمان ها و شرکتها امکان دسترسی به سرویس دهندگان اینترنت را از طریق خطوط تلفن دارند. برای دسترسی به اینترنت هیچ گونه مجوز دولتی لازم نیست. دسترسی به اینترنت با پست یا پست الکترونیکی نیاز به هیچ گونه تائیدیه ای ازطرف هیچ سازمان دولتی ندارد. هیچ دستور العمل یا بخشنامه ای وجود ندارد که سرویس دهندگان را موظف کند اطلاعات مربوط به مشترکان، کاربران و محتوای دادههای تبادل شده را به سازمانهای دولتی ارائه دهند. کافه های اینترنتی به سرعت در حال رشد است و هیچ قانون خاصی برای نحودی تأسیس و نحودی اداره وجود ندارد، این کافه ها تابع قانون اماکن عمومی هستند. خدمات اینترنت در ایران به سرعت ارزان شده است و دولت برای دسترسیهای دانشگاهی یارانه قابل ملاحظه ای را پذیرفته است. سیاست گسترش فیبر نوری و افزایش ظرفیت تبادل بین المللی دادهها از سیاست های جاری دولت است. با عنایت به مباحث فوق و باتوجه به این که در صورت انجام سیاستگذاری، برنامه ریزی و نظارت دقیق و کامل در خصوص امنیت فضای سایبر در کشور و تعامل و همکاری مناسب میان تمامی نهادها، سازمان ها و بخش های دولتی و خصوصی در این زمینه می توان چشم انداز مطلوب امنیت فضای مجاز و اینترنت را این گونه ترسیم نمود:

• مسئولیت پذیری دولت در سیاستگذاری علمی، کارشناسانه و همه سو نگر و بهره گیری از تمام توان علمی کشور، جهت تحقق بیشترین منافع و کمترین آسیب ها از صنعت اینترنت در ایران
• جلوگیری از اثرات مخرب ارتباط با پایگاه های ضد اخلاقی و مبتذل با ایجاد و توسعه سایت های مفید و در عین حال جذاب
• جلوگیری از نفوذ اطلاعات آلوده به شبکه های اطلاع رسانی و نیز جلوگیری از صدمات و خسارت های جبران ناپذیر از آلایندههای جسمی بر پیکر جامعه و کشور.

با توجه به مطالب و رویکردهای فوق راه کارها و اقدامات اساسی که می بایست در سیاستگذاری ها و برنامه های آتی کشور در مورد تأمین امنیت فضای مجازی و اینترنت در ایران در نظر گرفته شود به شرح زیر می باشد:

• تدوین و توسعه نظام نظارت و حفاظت امنیتی بر محتوای دادههای مبادله شده با توجه به قانون امنیتی کشور و حفظ حریم عمومی و خصوصی که نقش اساسی در پیشگیری از گسترش فساد، تهدیدات امنیتی، رسوخ جاسوسی و خرابکاری الکترونیک و عملیات روانی خواهد داشت.
• ایمن سازی زیرساختهای حیاتی کشور و منابع ملی در قبال حملات الکترونیکی و ایجاد نظام مدیریت امنیت زیرساختهای حیاتی در دستگاههای مرتبط؛
• توسعه و حمایت از تحقیق و ارتقاء سطح آگاهی دانش و مهارت های مرتبط امنیت فضای مجازی و شبکه های الکترونیکی؛
• توسعه و ارتقاء سطح همکاری های منطقه ای و بین المللی در زمینه امنیت فضای مجازی و شبکه های الکترونیکی شامل مسائل حقوقی، قضایی، انتظامی، کارتهای اعتباری و غیره ؛
• تدوین و اجرای قوانین مورد نیاز و روز آمد در حوزه ارتباطات شبکه ای به خصوص در موضوع حقوق تکثیر و مالکیت آثار فرهنگی و نرم افزارها و اطلاعات الکترونیکی که تأثیر قطعی در تشویق تولیدات و اختراعات بر روی شبکه دارد؛
• سیاستگذاری مناسب در توسعه اینترنت به طوری که توسعه مصرف یا باز تولید محتوای آن محدود نشده، بلکه به گسترش فرهنگ بومی و مقاومت فرهنگی کمک نماید و نیز به خلاقیت گستری مدد رسانده و موجبات خلاقیت زدایی را فراهم آورد؛

• تدوین و طراحی نظام تولید و سازماندهی الکترونیک اطلاعات علمی، اداری و مالی براساس استانداردهای قابل تبادل در شبکه ها پیش از توسعه روز افزون اینترنت؛
• تدوین و تصویب و اجرای سریعتر قانون کپی رایت در کشور؛
• ایجاد همکاری و هماهنگی قوی بین تمامی دستگاهها و نهادهای دولتی و نظامی کشوری و لشگری) جهت ایجاد امنیت فضای مجازی و جلوگیری از دوباره کاری ها و موازی کاریها ؛

نتیجه گیری:

به نظر می رسد در حال حاضر تهدید اصلی کشور در مورد فضای مجازی، فقدان گفتمان امنیتی در مورد این پدیده است. فقدان دانش جامع نگر در مورد صورت مسأله و عدم وجود مطالعات سیاستگذاری مقایسه ای در کشور، حاکمیت روش آزمون خطا و اعمال سلایق فردی و سازمانی را به دنبال داشته است. مسئولیت پذیری دولت در سیاستگذاری علمی، کارشناسانه و همه سونگر و بهره گیری از توان علمی کشور، شرط اصلی تحقق بیشترین منافع و کمترین آسیب ها از فضای مجازی در ایران است. برای جلوگیری از اثرات مخرب ارتباط با پایگادهای ضد اخلاقی باید به سمتی حرکت کنیم که سایت های مفید، جذابیت پیدا کند. یعنی ابتدا در حد توان باید در زمینه ی سایت های مفید و در عین حال جذاب سرمایه گذاری کنیم. از طرف دیگر هم باید موارد منفی را سد کنیم، یعنی از نفوذ سایت های مخرب، به این سو جلوگیری کنیم. برای محافظت از دستگاه‌ها و داده‌های خود در برابر تهدیدات سایبری، می‌توانید اقدامات ساده‌ای مانند استفاده از جدیدترین سخت‌افزار و نرم‌افزار را برای نیازهای دیجیتال خود اتخاذ کنید. همچنین باید اقدامات پیشرفته ای مانند نصب فایروال برای افزودن یک لایه امنیتی اضافی انجام دهید. امیدواریم این مقاله با تشریح چالش های عمده امنیت سایبری، شما را از تهدیدها آگاه کرده باشد و امیدواریم اقدامات اصلاحی را در سطح فردی و سازمانی برای محافظت در برابر چنین مسائل امنیتی انجام دهید.

منابع

[1] Cornish, P., Hughes, R., & Livingstone, D. (2009). Cyberspace and the national security of the United Kingdom Chatham House Report. http://www.chathamhouse.org.uk/files/13679_r0309cyberspace.pdf.

[2] Dunn Cavelty, M. (2010). Cyber-threats. In M. Dunn Cavelty & V. Mauer (Eds.), The Routledge handbook of security studies. London/New York: Routledge.

[3] Dunn Cavelty, M., & Rolofs, O. (2011). From cyberwar to cybersecurity: Proportionality of fear and countermeasures. Munich Security Conference, Munich, 3–4 Feb 2011. Paper available at http://www.securityconference.de/Article-Details.94.0.html?&no_cache=1&L=1&tx_ttnews[tt_news]=560&tx_ttnews[backPid]=92&cHash=55e618dc7b.

[4] Hughes, R. (2010). A treaty for cyberspace. International Affairs, 86(2), 523–541.

[5] IBM. (2010). Meeting the cybersecurity challenge: Empowering Stakeholders and. Ensuring Coordination. IBM U.S. Federal. White Paper. http://www-304.ibm.com/easyaccess3/fileserve?contentid=192188.

[6] Reveron, D.S.: Cyberspace and National Security: Threats, Opportunities, and Power in A Virtual World. Georgetown University Press, Washington D.C. (2012)

[7] Al-khateeb, S., Hussain, M.N., Agarwal, N.: Social cyber forensics approach to study twitter's and blogs' influence on propaganda campaigns. In: Lee, D., Lin, Y.-R., Osgood, N., Thomson, R. (eds.) SBP-BRiMS 2017. LNCS, vol. 10354, pp. 108–113. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60240-0_13

[8] Wei, W., Joseph, K., Liu, H., Carley, K.M.: Exploring characteristics of suspended users and network stability on Twitter. Soc. Netw. Anal. Min. 6(1), 51 (2016)

[9] Dhs.gov. (2015). Cybersecurity | Homeland Security. Retrieved from http://www.dhs.gov/topic/cybersecurity. Accessed December 24, 2015.

[10] Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security, 4(2), 49–60.

[11] Lewis, J. (2009). The "Korean" cyber attacks and their implications for cyber conflict | Center for Strategic and International Studies, Csis.org. Retrieved from http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict. Accessed December 26, 2015.

[12] Rollins, J., & Wilson, C. (2007). Terrorist capabilities for cyberattack: Overview and policy. Washington, DC: Congressional Research Service.