فصلنامه شناخت پژوهی مطالعات سیاسی
سال ۱، شماره ۲(۲۱)،۶۹-۵۴
تاریخ دریافت: ۱۴۰۳/۰۷/۲۵
تاریخ پذیرش: ۱۴۰۳/۰۹/۰۱

Journal of cognitive research in political studies
Vol.1, No2 (2), 54-69
Reseived Date: 2024/10/16
Accept Date: 2024/11/21

DOI: 10.20241403/CRPS.2410.1013.1.2.3

چرایی آموزش امنیت سایبری در مدارس متوسطه ج.ا.ایران

حبیب‌الله گودرزی دورکی[۱] | آرش سعیدی راد[۲] | محسن فرداودی[۳]

شماره ۲ (۲)
سال ۱
فصل پاییز ۱۴۰۳
مقاله پژوهشی
تاریخ دریافت:
۱۴۰۳/۰۷/۲۵
تاریخ پذیرش:
۱۴۰۳/۰۹/۰۱
صص: ۶۹-۵۴

چکیده

آموزش آنلاین و از راه دور هر چند مزیت‌های خاص خودش را دارد؛ ولی به همان اندازه می‌تواند در برابر حملات سایبری آسیب‌پذیر باشد. با در نظر گرفتن این مسئله، مقاله پیش‌رو با هدف پرداختن به چرایی آموزش امنیت سایبری در مدارس متوسطه جمهوری اسلامی ایران در نظر گرفته شده است. این مقاله بر استراتژی‌های متمرکز است که مؤسسات می‌توانند برای افزایش آگاهی دانش آموزان خود در مورد امنیت سایبری و به‌طور هم‌زمان انگیزه آن‌ها را برای دنبال کردن تخصص امنیت سایبری به‌عنوان شغلی بکار گیرند. از این‌رو نویسندگان تلاش خواهند کرد به چرایی آموزش امنیت سایبری در مدارس متوسطه ج.ا.ایران پاسخ دهند. یافته‌ها نشان می‌دهد که آموزش امنیت سایبری در مدارس متوسطه جمهوری اسلامی ایران مانند سایر کنشگران جهان با چهار چالش عمده «عدم برنامه‌های امنیت سایبری در مدارس»، «فقدان استراتژی و منابع»، «بودجه ناکافی و عدم ارائه آموزش» و «کیفیت پایین برنامه‌های امنیت سایبری» مواجه می‌باشد و تا زمانی که این چالش‌ها پا برجا باشند، نه‌تنها شاهد امنیت سایبری پایداری در کشور نخواهیم بود، بلکه در آینده با کمبود نیرو متخصص سایبری روبرو خواهیم بود که این خود نشان از یک بزنگاه تاریخی وابستگی (استعمار نوین سایبری) در آینده خواهد بود.

کلمات کلیدی: آموزش، امنیت سایبری، مدارس متوسطه، جمهوری اسلامی ایران

[۱] دانش آموخته دکتری، واحد خرم آباد، دانشگاه آزاد اسلامی لرستان، ایران.
[۲] دانش اموخته ارشد مطالعات منطقه‌ای، دانشگاه یزد، یزد، ایران . saiedi1arash@gmail.com
[۳] دانش آموخته ارشد تکنولوژی آموزشی، دانشگاه علامه طباطبائی، تهران، ایران

استناد: گودرزی دورکی، حبیب الله؛ سعیدی راد، آرش و فرداودی، محسن. (۱۴۰۳). چرایی آموزش امنیت سایبری در مدارس متوسطه ج.ا.ایران. شناخت پژوهی مطالعات سیاسی، ۱(۲)، ۶۹-۵۴.

Goudarzi Douraki, H., Saeedi rad, A., fardavoodi, M. (2024). Why cyber security training in J.A. Iranian secondary schools. Cognitive research of political studies, 1(2), 54-69

مقدمه

وظیفه بازیگران جهانی حفاظت از داده‌ها و اطلاعات حریم خصوصی (مردمی و سازمانی) به اشتراک گذاشته شده از طریق سیستم‌های رایانه‌ای است. لذا این دغدغه وجود دارد که آیا آموزش از طریق مدرسه، می‌تواند افرادی را تربیت کند که بتوانند خطرات حملات، جرایم و... سایبری را کاهش دهند یا خیر (Domeij, 2019). چرا که پذیرش آموزش فناوری نوین در مؤسسات دولتی و خصوصی به همان اندازه که راحتی به ارمغان آورده است، شدت خطرات امنیت سایبری را نیز افزایش داده است (Hasib, 2018). خصوصاً با همه‌گیری ویروس کرونا[1] و اجرای برنامه‌های یادگیری از راه دور، چالش‌های امنیت سایبری را نیز چند برابر افزایش داده است (Triplet, 2023: 47). در چند سال گذشته ج.ا.ایران هم از این چالش‌ها یا حملات سایبری دور از دسترس نبوده است و شاهد حملات متعددی بوده که نشان می‌دهد ایران هم مانند کشورهای دیگر با خلاء امنیت سایبری مواجه است. از این‌رو ضروری است که آموزش جهت بر طرف کردن این خلاء از مدارس متوسط ج.ا.ایران شروع شود؛ زیرا جنگ‌های امروزی و آتی علاوه بر فناوری‌های مختلف دفاعی بر مبنای فناوری‌های سایبری در حوزه فناوری اطلاعات و ارتباطات به‌منظور حمله و دفاع همه جانبه طرح‌ریزی و اجرا می‌گردد. به همین منظور مقاله پیش‌رو به این موضوع «چرایی آموزش امنیت سایبری در مدارس متوسطه ج.ا.ایران» اختصاص داده شد که ابتدا با بررسی پیشینه، روش و چارچوب تحقیق به خلاء امنیت سایبری در آموزش متوسطه جهان و ایران پرداخته خواهد شد و در نهایت با تجزیه و تحلیل با نتیجه‌گیری پایان خواهد یافت.

۱ـ پیشینه تحقیق

پس از جستجو در مسیر یافتن پیشینه پژوهشی هم‌راستا با موضوع این مقاله، نویسندگان متوجه شدند که در کشور، کار تحقیقاتی مشابهی انجام نگرفته است و عمده مقالات یا مکتوبات موجود، به‌دنبال ارزیابی بخشی از وجوه فضای سایبری بوده و جنبه‌های استراتژیک و کلان موضوع را ارزیابی ننموده‌اند. در نتیجه مواردی که از ادبیات جهانی که بخش‌های مهمی از زمینه‌های تئوریک این پژوهش را پوشش داده‌اند بررسی خواهد شد:

---

[1] COVID-19

جدول-۱. پیشینه پژوهش

نویسنده/ نویسندگان	عنوان (مقاله/ کتاب)	یافته پژوهش
ساعد الربایی[۱]؛ موسی الکفیری[۲]؛ عزالدین برکا[۳]	تلاش‌ها و پیشنهادات برای بهبود آموزش امنیت سایبری[۴]	جهان با کمبود نیروی کار متخصصان و متخصصان امنیت سایبری واجد شرایط مواجه است. برای حل این معضل چندین برنامه آموزشی امنیت سایبری بوجود آمده است. اما به دلیل ماهیت خاص امنیت سایبری، مؤسسات آموزشی در هنگام طراحی برنامه درسی امنیت سایبری یا مسائل بسیاری مواجه هستند.
یاسر جنگی؛ همت محمدنژاد	تأثیر آموزش مهارت های مدیریت کلاس بر عملکرد و رفتارهای سازمانی با میانجیگری امنیت سایبری معلمان مدارس ابتدایی منطقه ۱۸ شهر تهران	آموزش مهارت‌های مدیریت کلاس و مؤلفه‌های آن بر عملکرد و رفتارهای سازمانی با میانجیگری امنیت سایبری معلمان مدارس ابتدایی منطقه ۱۸ شهر تهران تأثیر دارد. که مؤلفه مدیریت رفتار بیشترین تأثیر را بر رفتارهای سازمانی با توجه به میانجیگری امنیت سایبری سازمانی دارد.
امیر حسین مقدسی لیچاهی؛ حمید همت	ارائه الگوی امنیت در فضای سایبر جمهوری اسلامی ایران با رویکرد آینده‌پژوهانه	به دلیل اثرگذاری و گستردگی زیاد و سهولت و سادگی کاربرد و تنوع ابزارها و روش‌ها، وقوع تهدید سایبری قطعی است و بایستی با فرهنگ سازی، تو سعه زیر ساخت‌ها، رعایت پدافند غیرعامل سایبری، تدابیر فنی و امنیت فیزیکی و تدابیر مدیریتی یک تغییر بنیادین واقعی در فضای سایبر کشور ایجاد گردد.
علی اصغر دهقانی؛ حسین پوراحمدی	ارزیابی و پیشنهادات سیاست‌گذاری فضای سایبر در جمهوری اسلامی ایران	یافته های پژوهش نشان می دهد که استحصال کامل پتانسیل‌های فضای سایبر، نیازمند شکل خاصی از بازیگری است که تاکنون جمهوری اسلامی ایران درآن موفقیت مطلوبی کسب نکرده است.

[۱] Saed Alrabaee

[۲] Mousa Al-Kfairy

[۳] Ezedin Barka

[۴] Efforts and Suggestions for Improving Cybersecurity Education

میبدی؛ مجتبی ناصری		
پرویز فرشاسعید؛ محمود جلالی؛ مهناز گودرزی	ضرورت همکاری دولت‌ها در تقویت امنیت سایبری	به دلیل اینکه تمام جنبه های زندگی بشری به فناوریهای حوزه سایبری وابسته شده و چنین سطح از وابستگی موجب سوء استفاده بعضی از دولتها در ارتکاب حملات سایبری به زیر ساختهای حیاتی دولتها می گردد نیاز است تا جهت تقویت امنیت سایبری همکاریهایی در سطح بین المللی تو سط دولتها صورت گیرد.
سید مهدی برقعی	مروری بر امنیت سایبری؛ درس هایی برای جمهوری اسلامی ایران	در این مقاله به پرسش چگونه حملات سایبری منجر به تهدیدات امنیتی در نظام جمهوری اسلامی ایران خواهد شد، پرداخته شود و در نهایت راهبردهای مناسب برای امنیت روزافزون فضای سایبری جمهوری اسلامی ایران در برابر حملات سایبری ارائه داده است.
علی آرمان	تهدید های مخرب با موضوع امنیت سایبری در بحبوحه همه گیری کووید-۱۹ و روش‌های پیشگیری	چند مورد از روش‌های مقابله با این تهدیدهای سایبری را مورد بررسی قرار داده که در نتیجه باعث خواهند شد که افراد با رعایت یکسری اصول اولیه تا حدود زیادی از قربانی شدن در فضای مجازی در امان باشند.

جنبه جدید بودن مقاله پیش‌رو در این است که این پژوهش به‌طور ویژه به چرایی آموزش امنیت سایبری در مدارس متوسطه ج.ا.ایران پرداخته شده است که مورد مشابه یا پژوهش‌های مبسوطی در این خصوص انجام نگرفته و در معدود تحقیقات انجام گرفته درباره آموزش امنیت سایبری در مدارس، توجه نداشته‌اند.

۲ـ روش و گردآوری تحقیق

نوع پژوهش از نظر هدف کاربردی است و با توجه به این که برای اولین بار انجام می‌شود توسعه‌ای محسوب می‌شود و این تحقیق به روش موردی- زمینه‌ای انجام شده است.

در این تحقیق برای جمع‌آوری اطلاعات از روش کتابخانه‌ای و اینترنتی با استفاده از کتابخانه تخصصی و مطالعه اسناد و مدارک موجود و ابزار آن بررسی اسناد، مدارک، آرشیو، کتاب، اینترنت

و استفاده از اطلاعات موجود در وبگاه‌ها می‌باشد (Saeedi rad & farokhi cheshmrh soltani, 2024: 130).

۳ـ مبانی نظری- مفهومی

امنیت سایبری[1] یعنی حفاظت از سیستم‌ها، شبکه‌ها، برنامه‌ها و سامانه‌های نرم افزاری در برابر حملات دیجیتالی. هدف از امنیت سایبری، محافظت از اطلاعات در برابر سرقت و آسیب است. بدون وجود امنیت سایبری، سازمان‌ها نمی‌توانند از خود در برابر نقض‌های داده‌ای و حمله‌های هکرها دفاع کنند. بنابراین شرایط امروز فناوری‌های نوین، امنیت سایبری را در کنار سایر ابعاد امنیت (سیاسی، اقتصادی، اجتماعی، فرهنگی، زیست محیطی و...) جای داده است و به خطرات آن به‌عنوان ابزاری برای نبرد میان کشورها اشاره می‌کند. خطرات این عرصه جدید، موضوعی است که دارای اهمیت زیادی می‌باشد؛ زیرا تمامی بخش‌های مهم کشور به این فناوری وابسته است. با این اوصاف اخلال در امنیت سایبری یعنی اخلال در روند امنیت کشور. به‌علاوه این‌که بازیگران تازه‌ای نیز در این عرصه وارد شده‌اند که هر کدام براساس منافع خود از این فناوری استفاده می‌کنند و امکان گسترش خطرات سایبری نیز به امری رایج تبدیل شده است (National Security Strategy, 2018: 12). از این‌رو کارشناسان تهدیدات سایبری را در دسته‌بندی‌های مختلفی قرار می‌دهند. اما به‌طور کلی شش نوع تهدید در مقابل امنیت سایبری وجود دارد که عبارت‌اند از:

۱ـ جنگ سایبری[2]: بالاترین سطح و پیچیده‌ترین نوع از حمله سایبری به شمار می‌آیند که برضد منافع سایبری کشورها صورت می‌گیرد و عواقب سنگینی را برای کشور هدف دارد (Liu & Li, 2021: 78-81).

۲ـ جرایم سایبری[3]: مجموعه اقداماتی که با انگیزه‌های مجرمانه و به صورت عمدی علیه شهرت یک فرد یا گروه و یا به‌منظور آسیب فیزیکی و روانی، از طریق شبکه‌های ارتباطی مدرن مثل اینترنت به صورت مستقیم یا غیرمستقیم انجام می‌شود (Giantas & Srergiou, 2018: 4).

۳ـ تروریسم سایبری[4]: نوعی از جرایم سایبری بوده که عنصر اصلی آن ترور می‌باشد. حمله یک تروریست سایبری، باعث وحشت و حس ناامنی شدید می‌شود و ویژگی عمده آن اهداف

[1] cybersecurity
[2] Cyber war
[3] Cyber crimes
[4] Cyber terrorism

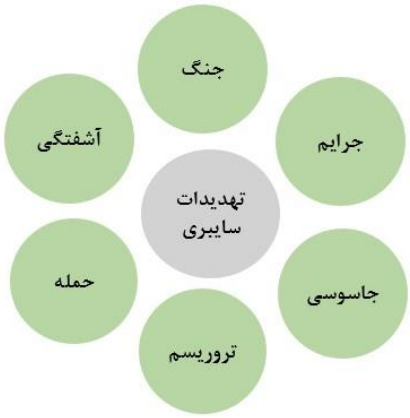
سیاسی عاملان افراط‌گرای آن است (Giantas & Srergiou, 2018: 4-5). در معنای دیگر، استفاده تروریست‌ها از هرگونه فناوری‌های اطلاعاتی را، سایبر تروریسم گویند (Beida & Halawi, 2015: 37).

۴ـ جاسوسی سایبری[1]**:** به اقداماتی گفته می‌شود که با هدف کسب اسرار از افراد، دولت‌ها، دشمنان، شرکت‌ها و رقبا به‌منظور بهره‌برداری‌های سیاسی، اقتصادی و سیاسی و با استفاده از فضای سایبر انجام می‌شود، در تعریف دیگری هم جاسوسی سایبری را به دست آوردن اطلاعات سری بدون اجازه مالک آن معنا می‌کنند. این مالک می‌تواند فرد، دولت، شرکت یا هر بازیگر دیگری باشد (Seddigh, 2016: 80).

۵ـ حمله سایبری: اختلال در صحت یا درستی داده‌هاست که معمولاً از طریق کدهای مخرب و تغییر در منطق برنامه و کمنترل داده‌ها که منجر به خروجی‌های اشتباه می‌شود، انجام می‌گیرد (Rodriguez, 2006: 9-10). این حملات به دلیل جدید بودن، درصد هزینه پایین و فایده بالا، عدم توانایی کشور هدف در مشخص و اثبات نمودن منشأ تهدید و عدم توانایی در تعیین میزان و دامنه خسارات وارد شده در مراحل اولیه شروع حمله، مورد توجه کشورهای متخاصم به‌ویژه در جنگ‌های ترکیبی قرار گرفته است (Taghipoor & Esmaeili, 2019).

۶ـ آشفتگی سایبری: آشفتگی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا هدف مورد نظر خود را ناقص کرده، تحت تأثیر قرار داده و یا آن را آزار دهد. اهداف سیاسی و ایدئولوژیکی در پشت این اقدامات وجود دارد و افراد از ابزاری استفاده می‌کنند که غیرقانونی هستند. برخلاف جرایم و جاسوسی سایبری که هدفشان دزدی یا تغییر اطلاعات است، آشفتگی سایبری سعی در مجازات یا تأثیرگذاری بر عقاید و رفتار هدف‌های خود دارد. در واقع قصد اصلی آشفتگی سایبری، آسیب رساندن است (Lord & Sharp, 2011: 18).

[1] Cyber epionage



نمودار-۱. تهدیدات سایبری در خلاء آموزش امنیت سایبری در مدارس

لذا زمانی این چهار تهدید سایبری گریبانگیر امنیت کشوری می‌شود که نیرو انسانی و فناوری مورد نظر نداشته باشد. از این‌رو کشورهای موفق به خنثی شدن این حملات خواهند شد که نیرو انسانی متخصص مورد کافی داشته باشند. اما همه‌گیری ویروس کرونا اثابت کرد که اکثر کشورها حتی توسعه یافته‌ها با کمبود نیرو متخصص در حوزه امنیت سایبری مواجه هستند.

۴ـ خلاء امنیت سایبری در جهان

امنیت سایبری یک حوزه حیاتی و به سرعت در حال رشد است. با این حال، نگرانی‌هایی در مورد در دسترس نبودن متخصصان امنیت سایبری مطرح است (Dunn & Merkle, 2018؛ Filipczuk et al., 2019؛ Hart et al., 2020). مونترویدو و همکاران اظهار داشتند که میزان حملات، جرایم و... سایبری تقاضا را برای متخصصان امنیت سایبری افزایش داده است. به‌طور خاص، مونترویدو[۱] و همکاران در یک نظرسنجی جهانی اشاره دارند که فقط ایالات‌متحده با بیش از ۵۹ درصد خلاء تحلیلگر امنیت سایبری مواجه می‌باشد. شرکت‌هایی بزرگ جهان هم نیز اعلام کردند که با خطر ۸۲ درصدی حمله سایبری روبرو هستند (Mountrouidou et al., 2019). هارت و همکاران، یافته‌های مشابهی که ارتباط قابل توجهی بین حملات سایبری و تعداد متخصصان امنیت سایبری است، ارائه دادند. به‌طور کلی، کمبود متخصصان امنیت سایبری آسیب‌پذیری افراد، شرکت‌ها و مؤسسات یادگیری را در برابر هکرها افزایش داده است (Hart et al., 2020).

---

[۱] Mountrouidou

محققان دیگری هم این نگرانی‌های مطرح شده را تکرار کرده‌اند که کمبود قابل توجهی از متخصصان امنیت سایبری وجود دارد. به‌عنوان مثال، در حالی که مونترویدو و همکاران کمبود ۵۹ درصدی کارکنان امنیت سایبری را گزارش کردند، چودوری[۱] حملات سایبری و افزایش جرایم سایبری در سطح جهانی را به کمبود متخصصان امنیت سایبری نسبت داده است. همچنین گزارش داد که جهان با فقدان بیش از ۳۰ درصد متخصص سایبری روبرو است که بتوانند سیستم‌های دیجیتالی مورد استفاده مردم را آموزش، آزمایش و ایمن کنند (Choudhury, 2022). از این‌رو فقدان متخصصان امنیت سایبری، مشاغل، مؤسسات آموزشی و سازمان‌های دولتی را در معرض جنگ، تروریسم، جرایم و جاسوسی قرار داده است. فقدان بیش از ۳۰ درصد متخصص امنیت سایبری به این معنی است که جهان سیستم‌های امنیت سایبری پیشرفته‌ای را که می‌توانند سیستم‌های فناوری را از دستکاری و کنترل هکرها آزمایش و ایمن کنند، از دست داده است.

برخی از محققان همچنین دلایل کمبود قابل توجه متخصصان امنیت سایبری را مورد بحث قرار داده‌اند. در یکی از این مطالعات، گزارش داده‌اند که فقدان متخصصان واجد شرایط برای راهنمایی دانش‌آموزان خصوصاً دبیرستانی برای پیگیری امنیت سایبری به‌عنوان شغل، عامل مهمی در کمبود است. آن‌ها از متخصصان واجد شرایط امنیت سایبری خواستند تا به‌عنوان مربی و مشاور نسل جوان خصوصاً دانش آموزان را به امنیت سایبری علاقه‌مند کنند تا در کمترین زمان ممکن این خلاء امنیتی را جبران کنند (Armstrong et al., 2018).

۵ـ خلاء امنیت سایبری در مدارس ایران

جمهوری اسلامی ایران مانند سایر کشورها با این چالش بزرگ مواجه هست و از زمان جنگ اول روسیه و اوکراین (۲۰۱۴) و ویروس کرونا (۲۰۱۹) تاکنون (۲۰۲۴) با حملات سنگین سایبری مواجه شده است. اما متاسفانه هنوز تصمیمی برای برنامه‌ریزی پایه‌ای برای آن در نظر نگرفته است. از این‌رو و به نظر می‌رسد که عدم تصمیم‌گیری یا عدم برنامه‌ریزی برای این کار از طریق مدرسه با چالش‌های مواجه می‌باشد که تا آن‌ها را برطرف نکند، نه تنها توان برطرف کردن خلاء امنیت سایبری را نخواهند داشت، بلکه در آینده با کمبود متخصصان در این حوزه روبرو خواهند بود. از این‌رو اگر جمهوری اسلامی ایران در این حوزه برنامه‌ریزی رشته‌ای و شغلی از مقطع متوسطه در پیش بگیرد در آینده میان‌مدت نه تنها خلاء امنیت سایبری خود را برطرف خواهد کرد، بلکه می‌تواند

[۱] Choudhury

بخش اصلی نیروهای متخصص کشورهای همسایه، همسو و... را پوشش دهد؛ در واقع با داشتن چنین متخصصانی می‌تواند هژمونی منطقه‌ای خود را تثبیت کند. در واقع پیش‌بینی می‌شود که کشوری که این خلاء امنیتی را برطرف کند و متخصصان حرفه‌ای داشته باشد، می‌تواند کشورهای دیگر را با خود همسو کند. در واقع داشتن متخصصان سایبری در آینده همان بازدارندگی را در پی خواهد داشت که بمب هسته‌ای در دهه‌های گذشته داشت. از این‌رو کشوری قدرتمند خواهد شد که در این حوزه سرمایه‌گذاری بلندمدت داشته باشد. در مجموعه اگر جمهوری اسلامی ایران بخواهد این راهبرد کلیدی را در پیش بگیرد باید برای برطرف کردن چهار خلاء که نه تنها ایران، بلکه کل جهان با آن‌ها روبرو است برطرف کند. این چهار خلاء عبارت‌اند از:

۵ـ۱ـ برنامه‌های امنیت سایبری در مدارس

محققان[۱] استدلال کرده‌اند که فقدان متخصصان امنیت سایبری تا حدی به دلیل عدم برنامه‌های آموزشی امنیت سایبری در مدارس است. به عنوان مثال، اسمیت اظهار داشت که تعداد محدود متخصصان و کمبود مهارت در امنیت سایبری، مجموعه دانشی را محدود می‌کند که می‌تواند یک برنامه درسی امنیت سایبری قوی برای دانش آموزان دبیرستانی ایجاد کند (Smith, 2018). آرمسترانگ و همکاران تکرار کردند که دوره‌ها و آموزش‌های امنیت سایبری ارائه شده به دانش آموزان از کیفیت پایینی برخوردار بوده و با مهارت‌های مورد نیاز کارفرمایان در بخش امنیت سایبری مطابقت ندارد (Armstrong et al., 2018). سانزو و همکاران، هم چنین دیدگاهی دارند و اشاره کردند که در حالی که مدارس سعی کرده‌اند دوره‌های امنیت اطلاعات خود را به‌روزرسانی کنند، اما فقدان متخصصان در حوزه امنیت سایبری باعث شده که مدارس با تغییر محیط امنیت سایبری عملاً غیرممکن باشند (Sanzo et al., 2021). الربایی و همکاران فقدان برنامه‌های آموزشی استاندارد در این حوزه و عدم مهارت‌های لازم در مدارس را به عنوان موانع اصلی علاقه دانش آموزان به دنبال کردن تخصص امنیت سایبری می‌داند (Alrabaee et al., 2022).

۵ـ۲ـ فقدان استراتژی و منابع

[۱] اسمیت (۲۰۱۸)، حسیب (۲۰۱۸)، دان و مرکل (۲۰۱۸)، آرمسترانگ و همکاران (۲۰۱۸)، فیلیپچوک و همکاران (۲۰۱۹)، مونترویدو و همکاران (۲۰۱۹)، هارت و همکاران (۲۰۲۰)، چودوری (۲۰۲۲) و... .

فقدان استراتژی و منابع لازم، به هکرها اجازه می‌دهد تا اطلاعات حساس افراد، شرکت‌ها و دانش‌آموزان را از سرورهای مؤسسه سرقت کنند. فیلیپچوک و همکاران شواهدی از افزایش خطرات حملات سایبری به دلیل کمبود متخصصان امنیت سایبری ارائه کردند. آن‌ها دریافتند که هکرها از معدود متخصصان موجود در بخش آموزش برای هدف قرار دادن اطلاعات مدارس و دانش‌آموزان استفاده می‌کنند (Filipczuk et al., 2019). نتایج مشابهی توسط اویدتون[1] گزارش شد. اویدتون دریافت که تغییر به یادگیری از راه دور باعث افزایش حساسیت دانش آموزان به حملات فیشینگ[2] و مهندسی اجتماعی می‌شود. بسیاری از مؤسسات آموزشی در زمان شیوع کووید-۱۹، فاقد متخصصان رایانه بودند تا به معلمان و دانش آموزان، آموزش عملی در مورد فناوری و خطرات حملات سایبری ارائه دهند (Oyedotun, 2020). بنابراین آموزش نقش مهمی در افزایش آگاهی امنیت سایبری ایفا می‌کند؛ چرا که آگاهی از فناوری و امنیت سایبری به یک مهارت مهم در بازار کار تبدیل شده است و نیاز به آموزش اولیه دانش آموزان در مورد امنیت سایبری برای رفع کمبود فعلی متخصصان امنیت سایبری را افزایش داده است (Garba et al., 2020). با این حال، تنها تعداد کمی از مدارس منابع لازم برای مقابله مؤثر با حوادث امنیتی و ایجاد آگاهی در مورد حوادث امنیت سایبری در بین دانش آموزان و مربیان خود را دارند (Coleman & Reeder, 2018).

۵ـ۳ـ بودجه ناکافی و عدم ارائه آموزش

چالش عمده دیگری که در جهان و ایران شاهد آن هستیم، بودجه ناکافی و عدم ارائه آموزش‌های ارزشمند امنیت سایبری در مدارس است. اکثر مدارس در این خصوص هیچ دوره آموزشی برگزار نمی‌کنند و حتی یک واحد درسی در حوزه امنیت سایبری ارائه نمی‌دهند. در حالی که یکی از عمده تهدیدهای آینده افراد، شرکت‌ها، مؤسسات، ادارات دولتی و... در دل همین حوزه به شمار رشد می‌کند.

لذا در حال حاضر (۲۰۲۴)، وظیفه مدارس متوسطه، دانشگاه‌ها، مؤسسات و... این است که در روش‌های آموزشی دانش آموزان و دانشجویان در زمینه امنیت سایبری تجدید نظر کنند.

۵ـ۴ـ کیفیت برنامه‌های امنیت سایبری

---

[1] Oyedotun

[2] Phishing: نوعی حمله سایبری است که به اشکال مختلف، حساب‌های کاربری و پسوردهای آن‌ها را مورد تهدید قرار می‌دهد (jangi & mohammadnejad, 2023: 166).

کمبود متخصصان امنیت سایبری خطرات حملات سایبری را افزایش داده و منجر به برنامه‌های امنیت سایبری بی‌کیفیت شده و دانش‌آموزان را از دنبال کردن حرفه‌ای در امنیت سایبری تقریباً دور کرده است. برای رسیدگی به نتایج منفی متخصصان امنیت سایبری، محققان برخی از استراتژی‌های مورد استفاده برای جذب و ایجاد انگیزه در دانش آموزان برای انتخاب و علاقه امنیت سایبری به‌عنوان شغل مورد بررسی و گزارش قرار داده‌اند. یکی از استراتژی هایی که محققان از آن حمایت کرده‌اند، افزایش آگاهی از امنیت سایبری در میان دانش آموزان است. با شیوع ویروس کرونا و تعلیق یادگیری حضوری، مربیان فرصتی برای افزایش آگاهی دانش آموزان در مورد امنیت سایبری به‌عنوان یک انتخاب شغلی پیدا کردند. خطرات هک شدن یا دریافت ایمیل‌های مشکوک و لینک‌های وب سایت، آسیب‌پذیری دانش آموزان از راه دور را در برابر هکرهایی که اطلاعات خصوصی آن‌ها را سرقت می‌کنند، افزایش داده است (Sanzo et al., 2021). کاسپری[1] و وارنر[2]، گزارش داده‌اند که مسیرهای حرفه‌ای که شامل آموزش مقدماتی امنیت سایبری، آموزش تخصصی و کاربرد عملی مهارت‌های امنیت سایبری است، دانش‌آموزان را برای تخصص در امنیت سایبری انگیزه می‌دهد (Caspary & Warner, 2016).

۶ـ استراتژی‌هایی ارتقاء امنیت سایبری در مدارس

ظهور اینترنت به انسان این امکان را داد که از دو قلمرو زندگی واقعی و دنیای مجازی استفاده کند، اما تأثیرات منفی هم مانند تهدیدات سایبری مانند جرایم، حمله، آشفتگی، جنگ و... به همراه دارد؛ بنابراین کنترل زودهنگام چنین مسائلی ضروری است تا تأثیر عمده‌ای برجا نگذارد. لذا آموزش امنیت سایبری بسیار ضروری است؛ زیرا موارد مانند جرایم سایبری، جنگ سایبری و... می‌تواند در هر جایی بدون توجه به افراد، سازمان‌ها و مکان‌ها رخ دهد. بنابراین لازم است دانش‌آموزان را در چنین فرآیند یادگیری مشارکت داد که استعداد آن‌ها را در این حوزه شناسایی کرد. البته باید در نظر داشت که سیستم آموزشی امنیت سایبری در مدارس به گونه‌ای باشد که توسعه تفکر انتقادی، تعاملی و سایر مهارت‌های منطقی درک را در زمینه ایمنی و امنیت در هنگام یادگیری و آموزش افزایش دهد (Sareen & Jasaiwal, 2021: 189). مدارس می‌توانند دوره‌های ارتباطات و فناوری اطلاعات را ارائه دهند، می‌توانند آگاهی از امنیت سایبری را در برنامه درسی

[1] Caspary
[2] Warner

خود بگنجانند تا اطمینان حاصل شود که هر دانش آموز فرصتی برای یادگیری تأثیرات و اهمیت امنیت سایبری دارد.

علاوه بر این، مسائل ایمنی مربوط به امنیت سایبری را می‌توان از طریق دوره‌ها و موضوعات دیگر آموزش داد. به عنوان مثال، می‌توان به دانش آموزان تکالیفی برای نوشتن مقاله در مورد آگاهی از امنیت سایبری داد. مهم‌تر از آن، دانش آموزان در سایر فعالیت‌های آموزشی مانند مناظره‌ها می‌توانند در مورد جنبه‌های مختلف امنیت سایبری بحث کنند. همچنین، مسابقات سخنرانی می‌تواند سازماندهی شود که موضوع اصلی آن امنیت سایبری باشد. این می‌تواند به آموزش دانش آموزان در زمینه امنیت سایبری کمک کند (Rademaker, 2016: 97) تا نسل‌های آینده درک کنند که چگونه از خود در برابر تهدیدات سایبری محافظت کنند.

ارائه دانش حیاتی برای ارتقاء و درک دانش آموزان و معلمان از امنیت سایبری برای حرکت به سمت جامعه‌ای محافظت شده از هرگونه تهدید سایبری بسیار مهم است. مهم‌تر از آن، یک منطقه محافظت شده از تهدیدات سایبری می‌تواند به جلوگیری از تکامل تهدیدات امنیت سایبری کمک کند. با توجه به پیشرفت تکنولوژی، مسائل جدید و نوظهور هر روز به وجود می‌آیند و بنابراین، راه حلی که دیروز استفاده می‌شود، ممکن است امروز بی‌اثر باشد؛ بنابراین، برنامه‌های امنیت سایبری باید مرتباً ارتقاء یابند تا اطمینان حاصل شود که به‌روز هستند و تنها از طریق آموزش از مدرسه تا دانشگاه می‌توانند با مشکلات جدید و نوظهور مقابله کنند (Negi & Sunita, 2019).

از آنجایی که در کشور ایران برنامه خاصی در مدارس جهت آموزش امنیت سایبری در نظر گرفته نشده است و به احتمال زیاد آموزش و پرورش به این زودی‌ها جهت بر طرف کردن این خلا وارد نمی‌شود، تنها راه جبران این خلا از خودگذشتی و فداکاری هدفمند معلمان در این مسیر است و مؤثرترین راه برای ارتقای درک و فهم این حوزه در بین دانش‌آموزان، یادگیری فعال و مستمر است؛ چرا که از طریق یادگیری فعال، دانش‌آموزان می‌توانند نسبت به تهدیدات امنیت سایبری مانند آزار و اذیت سایبری آگاهی پیدا کنند و به جلوگیری از چنین حوادث امنیت سایبری کمک کنند و افرادی این حوزه به عنوان رشته و تخصص خود انتخاب کنند.

نتیجه‌گیری

تجزیه و تحلیل مطالعات در این بررسی سیستماتیک کمبود قابل توجهی از متخصصان امنیت سایبری را نشان می دهد. کمبود متخصصان امنیت سایبری بر جمعیت و کیفیت مربیان در دسترس

دانش‌آموزانی که به دنبال حرفه‌ای شدن در امنیت سایبری هستند تأثیر منفی می‌گذارد و بر کیفیت آموزش دریافتی این دانش‌آموزان تأثیر می‌گذارد. فقدان مربیگری، آموزش ضعیف و نداشتن مهارت‌های لازم در امنیت سایبری مورد نیاز برای ایمن کردن شغل در بخش امنیت اطلاعات، بسیاری از دانشجویان را از انتخاب امنیت سایبری به عنوان شغل منصرف کرده است. با در نظر گرفتن این دغدغه، آموزش امنیت سایبری در مدارس نه تنها یک گزینه بلکه یک ضرورت است. به همین منظور هدف این مقاله چرایی آموزش امنیت سایبری در مدارس متوسطه ج.ا.ایران در نظر گرفته شده بود. این مقاله بر استراتژی‌های متمرکز بود که مؤسسات می‌توانند برای افزایش آگاهی دانش آموزان خود در مورد امنیت سایبری و به‌طور هم‌زمان انگیزه آن‌ها را برای دنبال کردن تخصص امنیت سایبری به‌عنوان شغلی بکار گیرند.

یافته‌ها نشان داد که آموزش امنیت سایبری در مدارس متوسطه جمهوری اسلامی ایران مانند سایر بازیگران جهان با چهار چالش عمده «عدم برنامه‌های امنیت سایبری در مدارس»، «فقدان استراتژی و منابع»، «بودجه ناکافی و عدم ارائه آموزش» و «کیفیت پایین برنامه‌های امنیت سایبری» مواجه می‌باشد و تا زمانی که این چالش‌ها پا برجا باشند، نه تنها شاهد امنیت سایبری پایداری در کشور نخواهیم بود، بلکه در آینده با کمبود نیرو متخصص سایبری روبرو خواهیم بود که این خود نشان از یک بزنگاه تاریخی وابستگی (استعمار نوین سایبری) در آینده خواهد بود.

در مجموع، بر اساس یافته‌های پژوهش حاضر نتیجه می‌گیریم آموزش امنیت سایبری از طریق مدارس متوسطه نه تنها می‌تواند خلا این حوزه در آینده را پر کند، بلکه می‌توان در بُعد ملی و منطقه‌ای مانع ظهور استعمار نوین سایبری شود. لذا با توجه به یافته‌های فوق پیشنهادهای در شش قالب ذیل ارائه می‌گردد:

جدول-۲. پیشنهادات

قالب پیشنهاد	روش برگزاری
دوره	✓برگزاری دوره‌های آموزشی- مهارتی در حوزه امنیت سایبری برای کلیه دانش آموزان و حتی معلمان جهت بهبود و توسعه حوزه سایبری؛ ✓معرفی دوره‌ها و مفاهیم امنیت سایبری در برنامه‌های درسی به‌طور مؤثر تعداد دانش آموزانی را که مایل به انتخاب شغل در امنیت سایبری هستند افزایش می‌دهد؛

کارگاه	✓کارگاه آموزشی ضمن خدمت به‌منظور آگاهی معلمان و دانش آموزان با حوزه امنیت سایبری؛
سمینار	✓علاوه بر دوره‌های مقدماتی، سمینارهایی را برای گسترش دانش دانشجویان در مورد امنیت سایبری طراحی کنند. با این حال، درگیر کردن این دانش آموزان در سمینارهای آگاهی از امنیت سایبری، دانش آن‌ها را افزایش می‌دهد و حتی انگیزه آن‌ها را برای تبدیل شدن به متخصصان امنیت سایبری ایجاد می‌کند.
بازی	✓طراحان و توسعه دهندگان بازی‌های پیشرفته‌ای را توسعه دهند که علاوه بر افزایش دانش آن‌ها، توانایی پاسخگویی به حملات سایبری را داشته باشند و به راحتی مورد حمله سایبری قرار نگیرند؛
اردو	✓تشویق دانش‌آموزان به شرکت در اردوهای تابستانی مرتبط با امنیت سایبری و آگاهی امنیت سایبری ملی، دانش آن‌ها را در مورد تهدیدات سایبری و ابزار احتمالی حملات بهبود می‌بخشد؛
همکاری	✓همکاری بین آموزش و پرورش و سازمان‌ها تضمین می‌کند که دانش آموزان و دانشجویانی که دوره‌های امنیت سایبری را می‌گذرانند می‌توانند از طریق دوره‌های کارآموزی به آموزش‌های عملی از این سازمان‌ها دسترسی داشته باشند. در دسترس بودن فرصت‌های کارآموزی در سازمان‌های شرکتی که دانش آموزان و دانشجویان را در معرض چالش‌های امنیت سایبری واقعی و خطرات مرتبط با اطلاعات مهم در دست هکرها قرار می‌دهد، انگیزه دانش آموزان و دانشجویان را برای حرفه‌ای شدن در امنیت سایبری افزایش می‌دهد.
گرایش تخصصی	✓در حال حاضر (۲۰۲۴) جهان با کمبود ۳۰ درصد متخصص در حوزه امنیت سایبری مواجه است و در آینده این خلا چند برابر خواهد شد. از این‌رو کشوری که برنامه‌ای برای تربیت نیرو متخصص در این حوزه نداشته باشد در آینده با چالش‌های شدید در حوزه سایبری مواجه خواهد شد. لذا پیشنهاد می‌شود که چنین رشته‌ای از متوسطه دوم در نظر گرفته شود و برای سایر رشته‌ها هم واحدی مجزا در نظر گرفته شود.

تعارض منافع

بنا بر اظهار نویسندگان، مقاله پیش‌رو فاقد هر گونه تعارض منافع بوده است.

Translated References to English

Alrabaee, S., Al-Kfairy, M., Barka, E. (2022). Efforts and suggestions for improving cybersecurity education. *2022 IEEE Global Engineering Education Conference (EDUCON)*, 1161-1168.

Armstrong, M.E., Jones, K.S., Namin, A.S., Newton, D.C. (2018). The knowledge, skills, and abilities used by penetration testers: Results of interviews with cybersecurity professionals in vulnerability assessment and management. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 62(1), 709–713.

Beida, D., Halawi, L. (2015). Cyberspace : Avenue For Terrorism. *Issues In Information Systems*, 16(3), pp 33-42.

Caspary, K., Warner, M. (2016). What it takes to create linked learning: A report on lessons learned from evaluating the approach in practice. *SRI International*.

Choudhury, M.D. (2022). Shortage of cybersecurity professionals a key worry for firms in '22. Mint. https://www.livemint.com/technology/shortage-of-cybersecurity-professionals-a-key-worry-for-firms-in-22-11642015098080.html

Coleman, C.D., Reeder, E. (2018). Three reasons for improving cybersecurity instruction and practice in schools. In E. *Langran & J. Borup (Eds.), Proceedings of Society for Information Technology & Teacher Education International Conference*, pp. 1020-1025, Association for the Advancement of Computing in Education.

Dunn, M. H., Merkle, L. D. (2018). Assessing the impact of a national cybersecurity competition on students' career interests. Proceedings of the 49th ACM Technical Symposium on Computer Science Education, pp. 62-67.

Filipczuk, D., Mason, C., Snow, S. (2019). Using a game to explore notions of responsibility for cyber security in organisations. Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, 1-6.

Garba, A., Maheyzah, B.S., Siti, H., Ibrahim, B.D. (2020). Cyber security awareness among university students: A case study. *Science Proceedings Series*, 2(1), 82–86.

Giantas, D., Stergiou, D. (2018). From Terrorism to Cyber-terrorism: The Case of ISIS. Greece. University of Peloponnese. Hellenic Institute of Strategic Studies.

Hart, S., Margheri, A., Paci, F., Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. Computers & Security, 95, 101827.

Horowitz, B.M., Scott Lucero, D. (2016). System-Aware Cyber Security: A Systems Engineering Approach for Enhancing Cyber Security. *Insight*, 19, 39-42.

jangi, y., mohammadnejad, h. (2023). The effect of classroom management skills training on organizational performance and behaviors with the mediation of cyber security of elementary school teachers in district 18 of Tehran. *Information and Communication Technology in Educational* Sciences, 14(1), 161-187.

Liu, Q., Li, Y. (2021). A comprehensive review study of cyber attacks and cyber security: Emerging trends and recent developments. Elsevier Ltd .Energy reports.

Lord, K.m., Sharp, T. (2011). America's Cyber future Security and Prosperity in the Information Age. *Center for a New American Security*, Volume I.

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., Yuen, T. T. (2019). Securing the human. *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, 157–176.

National security Archive. (2018). Presidential orders. Availabel at: https://nsarchive.gwu.edu/news/cyber-vault/2018-11-07/presidential-orders

Negi, S., Sunita, M. (2019). Effectiveness of Cyber Bullying Sensitization Program (CBSP) to Reduce Cyber Bullying Behavior among Middle School Children. International Journal of Cyber Research and Education, 1, Article No. 5.

ner, J., Wu, H. (2021). Designing a K-16 cybersecurity collaborative: Cipher. *IEEE Security & Privacy*, 19(2), 56–59.

Oyedotun, T.D. (2020). Sudden change of pedagogy in education driven by COVID-19: Perspectives and evaluation from a developing country. *Research in Globalization*, 2, 100029.

Rademaker, M. (2016). Assessing Cyber Security 2015. *Information & Security: An International Journal*, 34, 93-104.

Rodriguez, C.A. (2006). "Cyber terrorism", Inter-American Defense College as a prerequisite for the Diploma approved Starr, Stuart H. (2009). Towards an Evolving

Sareen, A., Jasaiwal, Sh. (2021). Need of cyber security education in modern times. *International Journal of Multidisciplinary Trends*, 3(2): 188-191.

Seddigh, M.I. (2016). Cyber Revolution and Evolution in Espionage. *Strategic Studies Quarterly*, 19(71), 71-92.

Smith, G. (2018). The intelligent solution: Automation, the skills shortage and cyber-security. *Computer Fraud & Security*, 1(8), 6–9.

Taghipoor, R., Esmaeili, A. (2019). Designing a conceptual model of the cyber defense model of the Islamic Republic of Iran. *National Security*, 8(30), 181-202.