فصلنامهٔ پدافند غیرعامل و امنیت (پژوهشی)
سال سیزدهم: شمارهٔ ۸ - پاییز ۳
صص: ۸۳ - ۱۱۶
تاریخ دریافت:۱۴۰۳/۱۲/۱۲

*Quarterly of Passive Defense & Security*
*Vol.13, No.48,Autumn 2024*
P-P: 83 - 116
تاریخ پذیرش:۱۴۰۴/۰۷/۰۵

# ارزیابی خطرهای امنیتی-فنی زیرساخت ملی ارتباطات مبتنی بر فیبر نوری در جمهوری اسلامی ایران

مهدی حیدری*[۱]
احمد مصطفایی[۲]

## چکیده

سال‌های متمادی اعتقاد بر این بوده که انتقال اطلاعات از طریق فیبر نوری کاملاً امن و نفوذناپذیر است، اما اکنون و پس از گذشت بیش از ۶۰ سال از کاربست فیبر نوری به‌عنوان یکی از راه‌های برقراری ارتباطات، صاحب‌نظران اعتقاددارند که نشت اطلاعات محرمانه یکی از مسائل مهم در حوزهٔ امنیت شبکه‌های نوری است. با توجه به گسترش شبکه فیبر نوری در کشور، مسئله کلیدی آن است که این شبکه در ج.ا.ایران با چه خطرهای امنیتی مواجه است؟ و شدت این خطرها به چه میزان است؟ هدف این نوشتار شناسایی و تحلیل خطرهای زیرساخت فیبر نوری مخابرات کشور از منظر امنیتی است. برای این منظور از طریق مصاحبه با خبرگان و مطالعات اسنادی، خطرهای امنیتی زیرساخت‌های فیبر نوری کشور شناسایی و سپس با روش تحلیل خطر مورد ارزیابی و تجزیه‌وتحلیل قرار گرفته است. جامعه آماری پژوهش شامل خبرگان حوزه فنّاوری اطلاعات و ارتباطات بوده که از میان آن‌ها تعداد ۱۴ نفر (شاغل در وزارت فنّاوری اطلاعات و ارتباطات، سازمان پدافند غیرعامل و فراجا) به روش هدفمند انتخاب و مورد مصاحبه قرار گرفته است. علاوه بر این برای شناسایی خطرها، بیش از ۳۰ مقاله و ژورنال بین‌المللی و ۲ مقاله داخلی موردمطالعه و بررسی قرار گرفت و ۸۵ مورد از این خطرها از این منابع شناسایی، استخراج و کدگذاری و با استفاده از ماتریس خطر مورد تجزیه‌وتحلیل قرار گرفت. در پایان بر اساس تجزیه‌وتحلیل‌های انجام‌شده،

۱. دانشیار رشته جامعه‌شناسی سیاسی (نویسنده مسئول)mheidar90@gmail.com
۲. دانشجوی دکتری رشته مطالعات امنیتی ایران

مهم‌ترین خطرهای امنیتی زیرساخت فیبر نوری کشور به ترتیب اولویت ذکر گردیده و پیشنهادهایی مطرح شده است.

**واژگان کلیدی: زیرساخت ارتباطات، خطر، خطر امنیتی-فنی، زیرساخت، فیبر نوری.**
**Key words: communication infrastructure, risk, security – technical risk, infrastructure, Fleece fiber**

### ۱- مقدمه

امروزه جهان در گذاری سریع به‌سوی جامعه و اقتصاد جدید اطلاعات محور، پیش می‌رود. به‌هرحال، جنگ‌های آینده و حتی پیشگیری از آن‌ها، مبتنی بر دانش و برتری اطلاعات خواهند بود. ظهور فنّاوری اطلاعات و ارتباطات به چند دهه پیش بازمی‌گردد و از آن زمان تاکنون، با سرعتی بیش از تصور، حوزه‌های مختلف زندگی بشر را تحت تأثیر خود قرار داده است. سامانه‌های دفاعی، طراحی‌های راهبردی و شبکه‌های اطلاعاتی همه و همه سخت تحت تأثیر این دگرگونی قرارگرفته‌اند (محمدی، ۱۳۹۰). در همین راستا فنّاوری اطلاعات و ارتباطات باعث ایجاد تحولات اساسی در جنگ‌ها نیز شده است، به‌طوری‌که بعضاً اندیشمندان دفاعی از آن با تعبیر «انقلاب در امور نظامی» یاد می‌کنند. در این میان، نه‌تنها جنگ‌های کلاسیک دچار تحول شده و پیشرفت‌های گسترده‌ای داشته‌اند، بلکه سبک‌های نوینی از جنگ نیز مانند جنگ سایبری ظهور نموده‌اند (اندیشگاه شریف، ۱۳۸۵).

با توجه به روندهای کنونی فنّاوری نظامی، در راستای ابعاد جنگ‌های آینده، طبقه‌بندی‌های متفاوتی صورت گرفته است و همهٔ آن‌ها تا اندازه‌ای، هم‌پوشانی دارند. آنچه در این میان بسیار بااهمیت است وابستگی بی‌سابقه جنگ‌ها به سامانه‌های اطلاعاتی و ارتباطی است. هرچند این سامانه‌ها، از یک‌سو باعث افزایش توانایی نیروها شده، اما از سوی دیگر منجر به افزایش آسیب‌پذیری نیز شده‌اند. درنتیجه هدف این جنگ، کاربرد مؤثر توانمندی‌های اطلاعاتی و ارتباطی و درعین‌حال تخریب یا ازکارانداختن سرمایه‌های اطلاعاتی دشمن است. ازآنجاکه هدف اصلی در این تحقیق ارزیابی خطرهای امنیتی- فنی زیرساخت ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا

است؛ لذا مؤلفه‌ها و شاخص‌های آن به‌عنوان یکی از ابعاد مهم دفاع موردبررسی قرار گرفته است. نتایج این تحقیق می‌تواند منجر به تبیین اهمیت زیرساخت اصلی ارتباطات در کشور در دفاع و هم‌چنین شناسایی مؤلفه‌ها و شاخص‌های مؤثر بر تأمین خدمات‌دهی این زیرساخت شود. بدیهی است در شرایطی که دشمن از تمام توانمندی‌های فنّاورانه و ظرفیت‌های دانشی خود برای تسلط همه‌جانبه بهره می‌گیرد سیاست‌گذاران، مدیران و کارگزاران کشور نیز به دنبال روشی مطمئن برای مقابله با این هجمه و دفاعی منطقی باشند. لذا این پژوهش می‌کوشد تا با شناسایی خطرهای زیرساخت ملی ارتباطات کشور مبتنی بر فیبر نوری زمینه را برای مقابله با تهدیدات متوجه این زیرساخت فراهم نماید.

**۲- بیان مسئله**

بی‌تردید جنگ‌های نسل بعد برمبنای حجم سنگینی از اطلاعات شکل خواهند گرفت که این اطلاعات از منابع متفاوت جمع‌آوری و برای استفاده بلادرنگ، ارزیابی و تجمیع می‌شوند. در مدیریت جنگ‌های آینده، برتری اطلاعاتی رُکنی تعیین‌کننده بوده و مستلزم بهبود جدی در مدیریت اطلاعات، اطمینان، تبادل و تسهیم دانش برتر است. برتری اطلاعاتی زمانی حاصل می‌شود که یک مزیت رقابتی از توانایی بهره‌برداری از موقعیت اطلاعاتی برتر به وجود آید و رسیدن به برتری اطلاعاتی، به‌عنوان یک منبع راهبردی در هدایت و مدیریت فضای نبرد بیشترین اهمیت را دارد (مانوری، ۲۰۱۱). همین اهمیت سبب شده تا در جنگ‌های اخیر شاهد آن باشیم که سامانه‌های اطلاعاتی و ارتباطی در اولویت هدف‌یابی و انهدام به‌منظور فلج نمودن سامانه فرماندهی و کنترل قرار داشته باشند (نوری و همکاران، ۱۳۹۶).

سرعت تحولات و پیدایش فنّاوری‌های نوین، تنوع خدمات پیشرفته و تقاضای فزاینده برای این خدمات، لزوم استفاده بهینه از منابع مالی و انسانی و گسترش روزافزون بازار رقابت، موجب گردیده تا نگرش به صنعت مخابرات در قیاس با سایر صنایع متفاوت باشد. این نگرش هوشمندانه مبین این واقعیت است که فنّاوری اطلاعات و ارتباطات، نیروی محرکه توسعه در همه ابعاد است و این مهم، ضرورت‌های توسعه را متجلی می‌گرداند. سامانه ارتباطی وظیفهٔ انتقال اطلاعات از یک نقطه به‌نقطهٔ دیگر را بر عهده دارد. در گذشته سامانه‌های ارتباطی آنالوگ بوده‌اند، اما امروزه به‌سوی سامانه‌های دیجیتال

نوین در حال گذار هستند. بعد از اختراع لیزر در سال ۱۹۶۰ میلادی، ایدهٔ به‌کارگیری فیبر نوری برای انتقال اطلاعات شکل گرفت و این موضوع نقطه آغازی برای یک جهش در حوزه فنّاوری اطلاعات و ارتباطات بود.

در میان انواع دارایی‌های زیرساخت ارتباطات کشور، نقش بی‌بدیل فیبر نوری هرروز پررنگ‌تر از گذشته نمایان می‌شود. به دلیل ویژگی‌های ساختاری فیبر نوری طی سال‌های متمادی اعتقاد بر این بوده که انتقال اطلاعات از طریق آن کاملاً امن و نفوذناپذیر است، اما اکنون و پس از گذشت بیش از ۶۰ سال از کاربست فیبر نوری به‌عنوان یکی از راه‌های برقراری ارتباطات، صاحب‌نظران اعتقاددارند که نشت اطلاعات محرمانه یکی از مسائل مهم در حوزهٔ امنیت شبکه‌های نوری است. از سوی دیگر ممکن است با تزریق اطلاعات نادرست به شبکه ارتباطی از طریق زیرساخت فیبر نوری، مشکلاتی پدید آید.

درمجموع چنین قابلیت‌هایی، طیف گسترده‌ای از سوءاستفاده‌ها را شامل می‌شود. از اطلاعات غیرمجاز جاسوسی شرکتی گرفته تا اختلالات تروریستی در زیرساخت‌های مهم ارتباطات. برخلاف حملات فیزیکی آشکار به زیرساخت‌های شبکه، مانند برش کابل نوری، تپ‌های[1] نوری مورداستفاده در شبکه‌های امروزی برای مقاصد اختلال، ماهیت دقیق و ظریفی دارند، لذا به‌راحتی قابل‌تشخیص نیستند و یافتن آن‌ها دشوار است ازطرفی به دلایل مختلف انتشار اخبار مربوط به رخنه در زیرساخت فیبر نوری و شبکه‌های وابسته به‌ندرت رسانه‌ای می‌شود. ازجمله این دلایل می‌توان به مواردی نظیر ملموس نبودن نفوذها، تبعات منفی رسانه‌ای نمودن نقاط ضعف سامانه‌ها برای بهره‌برداران اشاره نمود.

جمهوری اسلامی ایران نیز با فراهم کردن زیرساخت‌های لازم و اجرای بیش از ۷۰۰۰۰ کیلومتر کابل فیبر نوری در کشور، اساس ارتباطات خود را استفاده از فیبر نوری قرار داده است. در حال حاضر اطلاعاتی نظیر سامانه‌های گوناگون ناوبری هوایی و دریایی، مراکز مانیتورینگ و مدیریت (توزیع[2]) برق و گاز سراسری، خودکارسازی‌های ادارات کشور، انتقال دیتا، تصویر و صوت و غیره تنها بخش اندکی از محتوای ارزشمندِ شبکه زیرساخت فیبر نوری است. با اتصال سازمان‌های متعدد به شبکه ملی و عبور تمامی

---

۱. Tap: واژه‌ای به معنای بازکردن، بهره‌برداری کردن، شیر زدن به لوله یا بشکه، مخفیانه به مکالمات تلفنی گوش کردن است. در ادامه نوشتار به دلیل نداشتن معادل فارسی از همین واژه اصلی استفاده می‌شود.
2. Dispatching

اطلاعات آن‌ها از یک زیرساخت واحد[۱]، گنجینه‌ای پدیدار گشته که در معرض تهدیدات گوناگونی قرار دارد.

با توجه به موقعیت ویژه جمهوری اسلامی ایران و دشمنی‌های نظام استکبار جهانی از یک‌سو و وابستگی کشور در صنعت الکترونیک و مخابرات به بیگانگان از سوی دیگر، بدیهی است زیرساخت ارتباطی فیبر نوری به‌عنوان شاهراه اطلاعات کشور مطمع دشمن بوده و همواره به‌عنوان یک هدف جذاب قلمداد گردد؛ بنابراین حفظ امنیت و پایداری در ارائه خدمات شبکهٔ ملی ارتباطات مبتنی بر فیبر نوری موضوعی حیاتی است و کم‌توجهی به این مسئله می‌تواند زمینه را برای بروز تهدیدات جدی علیه امنیت ملی ایران فراهم نماید. با این نگاه و در یک تحلیل کلی، خطرهای امنیتی- فنی شبکهٔ ملی ارتباطات مبتنی بر فیبر نوری کشور در حوزه‌های ذیل قابل‌بررسی و تحلیل است:

- حوزهٔ نیروی انسانی (درون‌سازمانی و برون‌سازمانی): نیروی انسانی متخصص مرتبط با زیرساخت فیبر نوری از دو بعد قابل‌بررسی است؛ نیروهای خارجی که صاحبان فتاوری بوده و در طراحی، ساخت و حتی در نصب سامانه‌های مربوطه نقشی بی‌بدیل دارند. از سوی دیگر نیروهای متخصص داخلی نیز در مدیریت و نگهداری شبکه حضوری فعال دارند. با توجه به اینکه بسیاری از فعالیت‌های زیرساختی در ارتباطات ملی به شرکت‌ها و بخش خصوصی واگذار شده و نظارت بر این شرکت‌ها و افراد شاغل در آن از طرف مراجع نظارتی و امنیتی ضعیف است بنابراین توجه به نیروی انسانی مرتبط با زیرساخت ارتباطی کشور موضوعی مهم و شایسته توجه است.
- حوزهٔ ابنیه (سایت‌ها، اماکن اداری و پشتیبانی): مکان‌هایی که به‌عنوان نقطه اتصال شبکه و محل مدیریت شبکه تعریف‌شده‌اند به دلیل وجود سامانه‌های و حتی سامانه‌های اصلی شبکه همواره می‌تواند محلی برای ایجاد آسیب‌های احتمالی باشد.
- حوزهٔ تجهیزات (نرم‌افزار، تجهیزات پسیو و اکتیو): وابستگی صنعت مخابرات کشور به خارج و برتری دانش بیگانگان باعث شده که نرم‌افزارهای مورداستفاده در شبکه

۱. بخش وسیعی از خدمات سازمان‌های اقتصادی، سیاسی، فرهنگی، صنعتی، دفاعی و حتی امنیتی جمهوری اسلامی ایران در بستر زیرساخت فیبر نوری تبادل می‌شود که منجر به وابستگی امنیت کشور به این زیرساخت شده است.

و حتی تجهیزات مرتبط به آن، بستر مناسبی برای انجام اقدامات ضدامنیتی و یا خرابکاری باشد.

ازآنچه گفته شد می‌توان نتیجه گرفت وضع مطلوب در مدیریت کلان شبکه ارتباطات مبتنی بر فیبر نوری، الگوبرداری از کشورهایی مرجع و مدیریت آن با رویکرد امنیتی در سطح ملی است. در کشوری مانند ایالات‌متحده آمریکا همواره فنّاوری اطلاعات و ارتباطات از موضوعات مهم حاکمیتی بوده و به‌شدت از حوزه‌های سه‌گانه ذکرشده مراقبت و صیانت می‌شود. کشوری مانند جمهوری اسلامی ایران که نشانگاه پیکان عداوت نظام سلطه است می‌تواند هدف ثابت تهاجمات دشمنان باشد. در این میان وابستگی تمامی اجزای حاکمیتی به فنّاوری ارتباطات و اطلاعات به‌صورت عام و زیرساخت ارتباطات فیبر نوری به‌صورت خاص، اهمیت موضوع را صدچندان می‌کند.

با عنایت به مطالب ذکرشده، ضروری است در کنار بیان محاسن زیرساخت فیبر نوری، خطرهای آن نیز مورد ارزیابی و تحلیل قرار گیرد. برای دستیابی به این هدف، این پژوهش قصد دارد به تحلیل خطرهای زیرساخت فیبر نوری مخابرات کشور بپردازد و آن‌ها را از منظر امنیتی واکاوی نماید. در این راستا سؤالات اصلی و فرعی که این پژوهش به دنبال پاسخگویی به آنان است، به شرح زیر است:

**سؤال اصلی**

عوامل مؤثر بر خطرهای امنیتی- فنی زیرساخت فیبر نوری مخابرات کشور کدامند؟

**سؤالات فرعی**

۱) احتمال وقوع هر یک از خطرهای زیرساخت فیبر نوری مخابرات کشور چقدر است؟
۲) شدت پیامد هر یک از خطرهای زیرساخت فیبر نوری مخابرات کشور چقدر است؟
۳) خطرهای شدید، متوسط و خفیف در زیرساخت فیبر نوری مخابرات کشور کدامند؟

## ۳-مرور ادبیات پژوهش

### ۳-۱ تاریخچه

مزیت‌های فیبر نوری و قابلیت منحصربه‌فرد آن در گسترش قابل‌توجه پهنای باند، سرعت‌بالای کم‌نظیر، نرخ خطای کم، ایزولاسیون الکتریکی، ایمنی نسبی در مقابل

تـداخلات و تأثیـرات خارجـی و نیز پایـداری ارتباط باعث شـد تا این زیرسـاخت ارتباطی به‌سـرعت در جهـان گسـترش یابـد. اکنـون زیرسـاخت‌های ارتبـاط مبتنـی بـر فیبـر نوری گذرگاه‌های اصلی اطلاعات بوده و تا سال‌های متمادی یگانه زیرساخت محبوب ارتباطی خواهد بود.

دیگر مزیت مهم فیبر نوری، وجود امنیت بالا در انتقال اطلاعات است. هرچند در ابتدای امر بسیاری بر این باور بودند که به دلیل ساختار فیبر نوری دسترسی به اطلاعات موجود در آن بسیار دشوار خواهد بد، اما گذر زمان واقعیت‌ها نمایان کرد. طبق گزارش‌های منتشرشده در دو دهه اخیر و برخلاف اعتقاد اولیه، به نظر می‌رسـد دسترسـی به اطلاعات فیبر نوری چندان مشکل نبوده و حتی به‌راحتی قابل‌دسترسی باشد. ازآنجایی‌که سامانه‌های انتقال نوری در کـد کردن اطلاعات و ارسـال آن‌ها از اسـتانداردهای بین‌المللـی بهره می‌برند، این موضوع کار شـنود اطلاعات را تسـهیل کرده اسـت. قسمت کوچکی از توان نری نشت شده در فیبرهای نوری، دارای تمامی اطلاعات ارسـالی اسـت که با دسترسـی به آن و با استفاده از سـامانه‌های مـوازی و قراردادهـای اسـتاندارد، تمامی اطلاعات قابل رمزگشـایی و شـنود خواهد بود (صیدی و جباری، ۱۴۰۳).

همـواره قسـمت کمـی از تـوان در فیبـر نوری از هسـته وارد پوسـته می‌شـود و در طـول آن مستهلک‌شـده یا از آن خارج خواهد شـد؛ بنابراین وجود قسـمت کوچکی از توان سیگنال اصلـی بـرای آغـاز عملیـات شـنود کافـی اسـت. در ادامـه بـه برخـی از روش‌هـای نفـوذ در فیبرهای نوری و روش‌های ایجاد انشعاب در شبکه ارتباطی مبتنی بر فیبر نوری، به‌صورت گذرا اشاره خواهد شد (مصطفایی، ۱۳۹۹).

۱) روش هم‌بافتـی: در ایـن روش فیبـر نوری قطع‌شـده و با اسـتفاده از تجهیـزات مربوطه، یـک انشـعاب از آن گرفته می‌شـود. دو زروز مکانیکی و گدازشـی بـرای هم‌بافت کردن فیبرها وجود دارد.

۲) روش خمـش: مبنـای اسـتفاده از ایـن روش تئـوری خمـش، مفهوم ضریب شکسـت و بازتاب کلی در فیبر نوری است. این تئوری امکان نشت نور از هسته و غلاف خم‌شده را بیان می‌کند. خمش نیز به دو صورت ریز خمش و بزرگ خمش دسته‌بندی می‌شود که هرکدام کاربرد خاص خود را دارد.

۳) روش جفتگر: استفاده از جفتگر یا کوپلینگ بین دو فیبر نوری به هم نزدیک شده، دارای کاربردهای گوناگونی است. جفتگرهای گدازشی، اسید کاری شده و صیقل‌کاری شده از روش‌های سه‌گانه موجود هستند.

۴) برش v شکل در سطح فیبر: این برش باعث می‌شود نمایه توانی سیگنال عبوری در غلاف به سطح v شکل برخورد کرده و چون زاویه آن بیش از زاویه حدی، نور در مرز برش بازتابش یافته و از فیبر خارج می‌شود.

۵) پراکندگی رایلی: این اتلاف مربوط به بی‌نظمی ایجادشده در ذوب سیلسکا است. مواد افزایش‌دهنده ضریب شکست در هسته، موجب افزایش این پراکندگی می‌شوند.

۶) پراکندگی برانگیخته: این روش شامل کریستال کردن بخشی از هسته با استفاده از گرما و یا با استفاده از لیزر $CO_2$ است. در این روش می‌توان با تنظیمات دقیق میزان کمی از توان سیگنال داخل فیبر نوری را استخراج کرد تا سیگنال افت زیادی پیدا نکند.

۷) توری‌های پراگ: این روش از پیشرفته‌ترین روش‌های پایش فیبر نوری بوده و به دلیل ویژگی‌های فنی آن به‌راحتی قابل‌شناسایی نیست. در این روش با استفاده از لیزر اگزایمر فرابنفش و تاباندن پرتو آن به داخل فیبر در محدوده‌ای از آن توان پراگ تشکیل می‌شود. با این عملیات بخشی از سیگنال نوری به بیرون از فیبر منتقل‌شده و از آن بهره‌برداری می‌شود.

۸) پاشیدن نور: در این روش از فن پاشیدن نور اضافی به درون فیبر نوری و استنباط اطلاعات اصلی با توجه به اثر متقابل بین دو سیگنال استفاده می‌شود. تزریق سیگنال به درون فیبر نوری می‌تواند کاربردهای دیگری نظیر واردکردن اطلاعات نادرست یا تخریب اطلاعات را داشته باشد (اسلامی و همکاران، ۱۳۹۵).

### ۲-۳ پیشینه پژوهش

یکی از پژوهش‌هایی که در سال‌های گذشته انجام شد مربوط به سندرا میلر[1] است. وی طی پژوهشی به بررسی امکان نفوذ در شبکه‌های مبتنی بر فیبرهای نوری پرداخت. به اعتقاد وی علی‌رغم شهرت شبکه‌های فیبر نوری در مورد امن‌تر بودن آن‌ها نسبت به شبکه‌های

1. Sandra key miller

مبتنی بر سیم مسی و امواج رادیویی، حقیقت این است که شبکه‌های فیبر نوری ضد هک نیستند و یک مهاجم زرنگ و کاردان می‌تواند با استفاده از نرم‌افزارها و سخت‌افزار که به سهولت قابل تهیه هستند، به‌راحتی در آن‌ها رخنه کند؛ بنابراین زیرساخت فیبر نوری در برابر هک‌های اصولی و فنی آسیب‌پذیر است (میلر، ۲۰۰۳). از سوی دیگر ظرفیت شبکه رشد چشمگیر خواهد داشت (افزایش پهنای باند و سرعت انتقال)، لذا امنیت در این شبکه و دسترسی به ارتباطات امن مطلوب کاربران است. معمولاً ارتباطات امن از طریق به‌کارگیری پروتکل‌های رمزنگاری در لایه‌های بالاتر مثل لایهٔ MAC[1] به دست می‌آید که فریم‌های دیتا را رمز می‌کند اما فریم‌های کنترلی و هدرها بدون حفاظت رها می‌شوند؛ بنابراین روش ذکرشده دارای خطر بوده و امنیت را بر یک بنیاد غیرمطمئن قرار می‌دهد. ازاین‌جهت مطلوب است که یک لایه فیزیکی امن در مقابل تهدیدات احتمالی به وجود آید (ژانگ و لئو، ۲۰۰۳).

از میان اسناد افشاشده توسط ادوارد اسنودن درباره فعالیت‌های جاسوسی آژانس امنیت ملی آمریکا، اطلاعاتی وجود دارد که نشان می‌دهد این تشکیلات قادر است با قرارگرفتن در مسیر فیبرهای نوری به اطلاعات در حال مبادله به‌واسطه آن‌ها رخنه کند. به گفته او بریتانیا تشکیلاتی بزرگ در یکی از کشورهای خاورمیانه دارد تا به‌طور گسترده تلفن‌ها، ایمیل‌ها و دیگر تبادلات اطلاعاتی در منطقه خاورمیانه را مورد شنود قرار دهد. اطلاعات به‌دست‌آمده از این راه در مرکز دولتی ارتباطات بریتانیا بررسی می‌شوند و نتایج آن در اختیار آژانس امنیت ملی آمریکا قرارمی‌گیرد. تشکیلات جاسوسی بریتانیا در یک کشور خاورمیانه‌ای (که نامش فاش نشده) به کابل‌های زیر دریا دسترسی دارد و همه اطلاعاتی که از طریق آن‌ها مبادله می‌شود را در رایانه‌های بزرگ ویژه ذخیره‌سازی می‌کند، سپس اطلاعات ذخیره‌شده در صورت نیاز در موارد مشخص مورد بازیابی قرار می‌گرفتند (روزنامه ایندیپندنت، ۲۳ اوت ۲۰۱۳).

---

۱. به عبارت ساده آدرس مک مثل یک آدرس خانه ثابت است (البته آدرس مک بعضاً قابلیت تغییر را دارد). این خانه درواقع همان رابط شبکه ما است. حال فرض کنید که در یک شهر با محدوده مشخص (شبکه) قرار داریم و یک نفر (از داخل شبکه) می‌خواهم پیغامی (پاکت‌های داده) را برای ما ارسال کند. فرد برای انجام این کار باید آدرس خانه موردنظر را در دست داشته باشد. به‌این‌ترتیب پاکت‌های داده نیز برای انتقال در درون یک شبکه نیاز به آدرس‌های مک کارت‌های شبکه دارند.

اندکی بعد از رسانه‌ای‌شدن اعترافات اسنودن، کیل گان[1] در پژوهش خود موضوع Taping و نفوذ بدون قطع در فیبرهای نوری را مطرح نمود. وی در این پژوهش به این نتیجه رسید که سامانه‌های انتقال فیبر نوری ظرفیت‌های بالایی در مسافت‌های طولانی فراهم می‌کنند. این زیرساخت‌ها از کابل‌های واقع در زیر اقیانوس‌ها تا شبکه‌های دسترسی نوری غیرفعال (پسیو)[2] است. این سامانه‌ها در معرض خطرهای امنیتی مختلفی قرار دارند و در برابر حملات شنود ساده در سطح لایه فیزیکی آسیب‌پذیر هستند. یکی از نکات حائز اهمیت طبق یافته‌های کیل‌گان، عدم شناسایی و کشف حملات صورت گرفته علیه زیرساخت فیبر نوری تا مدت‌زمان‌های طولانی است (گان، ۲۰۱۴).

در همان سال شائو سو و همکارانش[3] حملات زیان‌آور در شبکه‌های نوری، بر اساس هدف آن‌ها را به دو نوع تقسیم کردند. طبق دسته‌بندی آنان یک نوع حمله این است که از رسیدن اطلاعات درست به مقصد درست، جلوگیری شود، مثل حملات تولید پارازیت و ایجاد اختلال[4] و نوع دیگر حمله، استراق سمع اطلاعات است. مثل حملات Taping. کشف نوع دوم حملات همیشه از نوع اول سخت‌تر است، زیرا حملات نوع اول بر نتیجهٔ ارتباطات به‌صورت مستقیم تأثیر می‌گذارند اما حملات نوع دوم حتی به بر کیفیت ارتباطات تأثیر چندانی ندارند. برای دفاع در مقابل حملات شنود نوع دوم، کشف خطای مؤثر در لایهٔ فیزیکی، بهترین دیدگاه و روش است اما تشخیص آن دشوار بوده و زمان و هزینه بسیاری نیز می‌برد؛ بنابراین کاربران نمی‌توانند از وقوع حملات آگاه شوند و باید برای مدت‌زمان طولانی از این نوع حملات ثابت رنج ببرند. این کار حریم شخصی[5] و امنیت اطلاعات کاربران را دچار تهدید جدی می‌کند. در جمع‌بندی این موضوع می‌توان ادعا کرد که در زیرساخت فیبر نوری، سامانه‌ها در معرض خطرهای امنیتی مختلفی قرار دارند و در برابر حملات شنود ساده در سطح لایهٔ فیزیکی آسیب‌پذیر هستند. برای نمونه،

1. Kyle Guan

۲. در علم شبکه تجهیزات به دودسته پسیو و اکتیو تقسیم می‌شوند. اکتیو به تجهیزاتی در شبکه گفته می‌شود که برای فعالیت خود معمولاً نیازمند به نیروی برق می‌باشند و خود نیز در ایجاد، هدایت و تقویت سیگنال‌های داده نقش دارند برای مثال می‌توان به سوئیچ‌ها و روترها اشاره نمود. پسیو به تجهیزاتی در شبکه گفته می‌شود که برای فعالیت خود معمولاً نیازمند به نیروی برق نمی‌باشند و خود نیز در ایجاد، هدایت و تقویت سیگنال‌های داده نقش ندارند برای مثال می‌توان به کابل، هاب و انواع کانکتورها اشاره نمود.

3. Shao Jing Su et al
4. jamming
5. Privacy

کابل‌های فیبر نوری به‌آسانی قابل‌دسترسی هستند و می‌توانند به‌سادگی جهت Tap مورداستفاده قرار گیرند (سو و همکاران، ۲۰۱۴).

در درون کشور نیز علی پورسلامی و همکارانش در مقاله‌ای با عنوان روش‌های شنود سیگنال در فیبر نوری، تشخیص و جلوگیری از آن اشاره نمودند که حملات شنود یکی از مشکلات امنیتی اصلی در شبکه‌های نوری است. به‌علاوه، برای بعضی از اطلاعات ویژه مثل اهداف نظامی یا اخبار اقتصادی و مالی، آسیب وارده از طریق نشت اطلاعات بدون آگاهی (بدون آگاه شدن کاربران) بسیار بیشتر از آسیب ناشی از حملات نوع اول (ممانعت و جلوگیری از ارسال) است. ازآنجاکه سامانه‌های نوری در کدکردن اطلاعات و ارسال آن‌ها از استانداردهای بین‌المللی بهره می‌برند این مسئله نیز کار شنود اطلاعات را ساده‌تر می‌کند. حتی قسمت کوچکی از توان نوری نشت شده نیز دارای تمامی اطلاعات ارسالی بوده و با دسترسی به قسمت کوچکی از توان نوری نشت شده و با استفاده از سامانه‌های موازی و پروتکل‌های استاندارد تمامی اطلاعات قابل رمزگشایی و شنود خواهد بود. روش‌های متعددی برای نفوذ و انشعاب از شبکه فیبر نوری وجود دارد؛ ازجمله می‌توان به: روش‌های هم‌بافتی[1]، خمش، جفتگر[2]، برش V شکل در سطح فیبر، پراکندگی رایلی، پراکندگی برانگیخته، ایجاد فیبر توری پراگ با استفاده از پرتو UV و پاشیدن نور اشاره کرد (پور سلامی و همکاران، ۱۳۹۵).

موضوع تضعیف سیگنال‌های انتقالی درنتیجه رمزنگاری اندکی بعد توسط کووالسکی[3] مطرح شد. طبق این نظریه، فرایند انتقال اطلاعات در فیبر نوری همیشه از تضعیف، پخش‌شدگی و نویز تأثیرپذیر است. تضعیف سیگنال انتقالی یکی از چالش‌هایی است که اثرات و نتیجهٔ روش رمزنگاری ارائه‌شده را تحت تأثیر قرار می‌دهد؛ بنابراین می‌توان نتیجه گرفت که فیبر نوری یک رسانهٔ ارتباطی کامل نیست (کووالسکی، ۲۰۱۷).

در همان سال بن یو و همکارانش[4] موضوع امنیت در لایه‌های شش‌گانه در مدل را مطرح نمودند. شبکه‌های فیبر نوری ستون فقرات اینترنت را تشکیل می‌دهند و یک

1. Splicing
2. Coupling
3. Marcin Kowalski
4. Ben Wu et al

جزء جدایی‌ناپذیر لایه فیزیکی این شبکه‌ها هستند. ازآنجایی‌که لایه فیزیکی، لایه‌ای واقع در انتهای مدل OSI[1] است، کارایی و امنیت لایهٔ فیزیکی و بخصوص شبکه‌های نوری، تأثیری حیاتی بر روی شش لایه بالایی دارد. طبق نتایج پژوهش ایشان امنیت شبکه نوری روی امنیت کل سامانه ارتباطی تأثیر دارد و ساختن یک سامانه امنیتی روی یک زیرساخت فیزیکی که از قبل مورد تهدید بوده ذاتاً دارای خطرهایی است؛ بنابراین مقابله در برابر تهدیدات شبکه فیبر نوری برای امنیت لایهٔ بالایی نیز ضروری است (یو و همکاران، ۲۰۱۷).

این امکان وجود دارد که نه‌تنها یک، بلکه چندین شنود کننده می‌توانند هم‌زمان به یک فیبر نوری دست یابند. این شنودکننده‌ها می‌توانند مستقل از هم بوده و یا اطلاعات به آمده را با یکدیگر به اشتراک بگذارند. در این صورت سیگنال‌های به‌دست‌آمده را می‌توان با یکدیگر ترکیب کرده و به‌صورت هماهنگ پردازش نمایند. کل گان و همکارانش[2] در مقاله خود به این موضوع پرداختند که در حقیقت ممکن است برخی از دستگاه‌های بهره‌بردار نه‌تنها برای استفادهٔ غیرفعال بلکه برای بهره‌برداری فعال نیز فیبرهای نوری را شنود نمایند. در این صورت تزریق سیگنال‌ها به فیبر نوری برای اهداف گوناگون صورت می‌گیرد. از این فن‌ها می‌توان برای وارد نمودن اطلاعات غلط، اختلال در شبکه و مخدوش نمودن جریان اطلاعات استفاده نمود. این حملات برخلاف حملات فیزیکی آشکار به‌راحتی قابل‌تشخیص نیستند و یافتن آن دشوار است (گان و همکاران، ۲۰۱۷).

احتمال این‌که کاربران در شبکه (مبتنی بر فیبر نوری) موردحمله واقع شوند در موقعیت‌های مختلف فیزیکی شبکه متفاوت است زیرا یک شبکه نوری منطقه‌ای وسیع را پوشش می‌دهد و کاربران شبکه با نیازمندی‌های محرمانگی مختلف به‌صورت متغیر توزیع‌شده‌اند؛ بنابراین حملات شنود می‌تواند توسط ماتریس احتمال شنود در هر لینک

---

۱. مدل Open Systems Interconnection ؛که گاه »مدل هفت لایه اُ اِس آی« نیز خوانده می‌شود، توصیفی مفهومی و مجرد از لایه‌هایی است که دو یا چند سیستم مخابراتی یا شبکه کامپیوتری از طریق آن به یکدیگر متصل می‌شوند. مدل OSI سعی بر توضیح چگونگی ارتباط دو سیستم انتقال اطلاعات بر پایه انواع رسانه‌ها در یک شبکه کامپیوتری را دارد. مدل OSI یک معماری شبکه نیست، چون هیچ سرویس یا پروتکلی در آن تعریف نمی‌شود. بلکه یکی از مدل‌های استاندارد و پذیرفته‌شده است که برای طراحی یا توصیف شبکه‌های مخابراتی به کار می‌رود.

2. Kyle Guan at al

توصیف شود و این روش می‌تواند برای حملات شنود مجتمع و یکپارچه استفاده شوند (بیا و همکاران[1]، ۲۰۱۸). در همان سال اگزیاسونگ فو و همکارانش[2] در پژوهشی به این نتیجه رسیدند که در شبکه‌های OFDM-PON[3]، به علت ساختار پخش همگانی[4] از پایانه‌های خطی نوری[5] به واحدهای شبکه نوری[6]، دیتای منتقل‌شده در برابر حملات شنود بیشتر آسیب‌پذیر است که این مسئله باعث تهدیدات جدی برای داده‌های کاربران می‌شود. از سوی دیگر شبکه‌های نوری ارتجاعی[7] می‌توانند در بعضی از سناریوهای مهم مثل ارتباطات نوری بین دیتاسنترها استفاده شوند. این شبکه‌ها به‌عنوان فنّاوری امیدبخش در شبکهٔ انتقالی نوری، در معرض تهدیداتی مثل حملات شنود است. این شبکه‌ها نیز درست مثل شبکه‌های نوری متداول، به خاطر فقدان ایمنی لازم پیشگیری مؤثری در برابر حملات شنود نداشته و ازاین‌رو با مشکلات امنیتی بالقوهٔ بسیاری مواجه هستند (سونگ فو و همکاران، ۲۰۱۸). لوتن کالینز[8] در مقاله خود از جنبه‌ای دیگر به بررسی موضوع پرداخته است. طبق نظر وی امروزه به‌صورت خیلی ساده‌تر و ارزان‌تر از هر زمان دیگر فیبرها مورد بهره‌برداری اطلاعاتی قرار می‌گیرند. در این شرایط یک راهبرد امنیتی پیمانه‌ای[9] و جامع جهت حفاظت مطمئن از دارایی‌های اطلاعاتی مهم شرکت‌ها نیاز است (کالینز، ۲۰۱۸).

بنابراین و طبق مجموع نظرات متخصصین به نظر می‌رسد که نفوذ در شبکه‌های فیبر نوری برخلاف تصور عامه امری بدیهی و میسر بوده که امکان آن با توجه به سطح فنّاوری

---

1. Wei Baia et al
2. Xiaosong Fua at al

۳. OFDM (Orthogonal Frequency Division Multiplexing: به معنای تقسیم فرکانسی چندگانه متعامد از روش‌های مدولاسیون که دارای مزیت‌های بسیاری در انتقال داده‌های دیجیتال است. فن مدولاسیون تقسیم فرکانسی چندگانه متعامد در برخی از جدیدترین سامانه‌های وایرلس پهن باند با نرخ داده بالا مانند WIFI و مخابرات از راه دور سلولی مورداستفاده قرارمی‌گیرد.

۴. Broadcast : آدرس Broadcast یک آدرس شبکه است که در آن تمام دستگاه‌های متصل به یک شبکه ارتباطی چندمنظوره برای دریافت داده‌ها فعال می‌شوند. یک پیام ارسال‌شده به یک آدرس Broadcast توسط همه میزبان‌های متصل به شبکه ممکن است دریافت شود.

5. OLT
6. ONU
7. EON: Elastic Optical Network
8. Lauten Collins
9. modular security strategy

کشورها متفاوت است؛ لذا با این فرض بایستی نگاهی نو به زیرساخت ارتباطی فیبر نوری داشت.

## ادبیات پژوهش

### تحلیل خطر

خطر در استاندارد PMBOK[1] چنین تعریف‌شده که اتفاق یا حادثه‌ای غیرمطمئن که در صورت رخداد می‌تواند بر روی پروژه اثر مثبت یا منفی بگذارد. در صورت بروز خطرهای منفی -که تحت نام تهدید از آنان نیز یاد می‌شود در صورت بروز در طول چرخه حیات پروژه می‌تواند باعث بروز مشکلاتی در روند پروژه شود (شادرخ و همکار، ۱۳۸۷). ازاین‌رو خطر، ترکیب (یا تابعی) از احتمال و پیامدهای ناشی از وقوع یک اتفاق خطرناک مشخص است و تحلیل خطر به فرایند کلی برآورد نمودن میزان خطر و تصمیم‌گیری در خصوص قابل‌تحمل بودن آن می‌گویند. تحلیل خطر به‌طور نظام‌مند تعیین می‌کند چه خطرهایی در محیط کار هستند، احتمال رخ‌دادن خطر چقدر است و چه آسیب و با چه شدتی می‌تواند به وجود آورد (سادات، ۱۳۹۸). مراحل تعیین خطر را می‌توان به سه مرحله تقسیم کرد:

۱) **برنامه‌ریزی مدیریت خطر:** تصمیم‌گیری در مورد چگونگی رویکرد و برنامه‌ریزی برای فعالیت‌های مدیریت خطر در یک پروژه است و خروجی اصلی این فرایند یک برنامه مدیریت خطر است (شوالب، ۱۳۸۷).

۲) **شناسایی خطرها:** اولین قدم در ارزیابی خطر، شناسایی خطر است (گرون، ۲۰۰۶). یک خطر را نمی‌توان مدیریت کرد مگر اینکه ابتدا آن را شناخت. خطرهای یک پروژه هم می‌توانند داخلی و هم خارجی باشند (رهنما و حجازی جوشقانی، ۱۳۹۰). شناسایی خطرها یک گام ضروری برای مدیریت خطر بوده و ممکن است سخت‌ترین مرحله مدیریت خطر نیز باشد (میلز، ۲۰۰۱).

۳) **انجام تجزیه‌وتحلیل کیفی خطر:** فرایند انجام تجزیه‌وتحلیل کیفی خطر مشخصات هر یک از خطرهای منفرد شناسایی‌شده در پروژه را ارزیابی و بررسی کرده و خطرها را بر اساس ویژگی‌های توافق شده رتبه‌بندی می‌کند (بی ام آی، ۱۳۸۸).

1. A Guide to the Project Management Body of Knowledge

۴) **انجام تجزیه‌وتحلیل کمی خطر:** این فرایند تلاشی است برای تعیین میزان خطر موجود در پروژه و محل دقیق آن، به‌گونه‌ای که بتوان به بهترین نحو ممکن، با صرف زمان و تلاشی محدود در حوزه‌های عمده خطر، موفق به کاهش خطر پروژه گردید (مالکهی، ۱۳۹۰).

۵) **برنامه‌ریزی پاسخ به خطر:** چهار راهبرد این مرحله عبارتند از الف) اجتناب از خطر یا حذف یک تهدید خاص که به‌طورمعمول به‌وسیله حذف عمل آن صورت می‌گیرد. ب) پذیرش خطر با قبول پیامدهایی که در اثر وقوع یک خطر رخ می‌دهد. ج) انتقال خطر یا انتقال پیامدهای یک خطر یا مسئولیت مدیریت آن به شخص ثالث. د) کاهش خطر یا کاهش اثر رویداد دارای خطر به‌وسیله کاهش احتمال وقوع آن (شوالب، ۱۳۸۷).

۶) **پایش و کنترل خطر:** اثربخشی مدیریت خطر پروژه به نحوه اجرای برنامه‌های تأییدشده وابسته است. این برنامه‌ها باید به‌درستی اجرا، بررسی و به‌صورت منظم بروز گردند. درصورتی‌که این کار به‌درستی صورت‌پذیرید فعالیت‌های انجام‌شده به نتیجه رسیده و پروژه‌های آتی از تجربیات این پروژه‌ها بهره‌مند خواهند بود (بی ام آی، ۱۳۸۸).

در این پژوهش سه مرحله نخست تحلیل خطر را طبق دسته‌بندی بالا انجام خواهد شد و مراحل بعدی نیازمند پژوهش‌های علمی جداگانه‌ای است که در قالب این نوشتار نمی‌گنجد.

### ۳-روش‌شناسی

این پژوهش به جهت هدف از نوع پژوهش‌های کاربردی است که به روش آمیخته (کیفی و کمی) انجام‌شده است. پژوهش دارای سه مرحله، شامل؛ شناسایی خطر، تحلیل کیفی خطر و رتبه‌بندی خطرهای شناسایی‌شده، است. در مرحله شناسایی خطر با استفاده از روش مصاحبه دقیق و همچنین مطالعات مقالات و پژوهش‌های انجام‌شده (عمدتاً در خارج از کشور) خطرها شناسایی شد. در مرحله دوم به تحلیل کیفی خطرهای شناسایی‌شده پرداخته شده است. در مرحله نهایی به رتبه‌بندی خطرهای شناسایی‌شده در مقیاس شدید، متوسط و خفیف با استفاده از ماتریس خطر پرداخته شده و سپس اولویت خطرها مشخص گردید.

**روش، شیوه و ابزار گردآوری اطلاعات**

در مرحله شناسایی خطرهای زیرساخت فیبر نوری کشور، ۱۴ نفر از خبرگان در وزارت فتاوری اطلاعات و ارتباطات، سازمان پدافند غیرعامل، نیروی انتظامی و غیره به روش هدفمند مورد مصاحبه عمیق قرار گرفتند. همچنین پیشتر بیش از ۳۰ مقاله و ژورنال بین‌المللی و دو مقاله داخلی موردمطالعه و بررسی قرار گرفت و ۸۵ مورد از این خطرها از این منابع شناسایی، استخراج و کدگذاری شدند. در مرحله بعد، داده‌های گردآوری‌شده مورد پیش‌پردازش و پاک‌سازی قرار گرفتند که درنهایت با مشورت با خبرگان خطرهای شناسایی‌شده به ۶۶ خطر تقلیل یافتند. سپس این خطرها به مرحله دوم تحلیل کیفی خطر واردشده و با استفاده از ماتریس خطر مورد تجزیه‌وتحلیل قرار گرفتند.

**ابزار تحلیل اطلاعات (داده‌ها)**

**مقیاس احتمال:** پس از جمع‌آوری اطلاعات مربوط به خطرهای شناسایی‌شده، باید احتمال وقوع هر خطر تعیین شود. احتمال عبارت است از شانس آن‌که یک خطر رخ دهد. در انجام تحلیل کیفی احتمال وقوع هر خطر به‌صورت ذهنی و با استفاده از نظرات کارشناسان تعیین می‌گردد (مالکهی، ۱۳۹۳). در این پژوهش احتمال وقوع خطر مطابق جدول ۱ تعیین شده است.

**جدول ۲: مقیاس احتمال وقوع هر خطر**

| رتبه‌بندی | ۱ | ۲ | ۳ | ۴ | ۵ | ۶ | ۷ | ۸ | ۹ | ۱۰ |
|---|---|---|---|---|---|---|---|---|---|---|
| تفسیر | بسیارکم | | کم | | متوسط | | زیاد | | قطعی | |

**مقیاس شدت پیامد (تأثیر):** پس از جمع‌آوری اطلاعات مربوط به خطرهای شناسایی‌شده و تعیین احتمال وقوع هر خطر، فرض می‌شود که این خطر اتفاق افتاده، سپس شدت پیامد (تأثیر) آن خطر تعیین می‌شود. شدت پیامد یا تأثیر عبارت است از اثری که آن خطر در صورت وقوع بر پروژه خواهد داشت (مالکهی، ۱۳۹۳). برای این منظور از جدول ۲ برای تعیین شدت پیامدهای وقوع هر خطر استفاده شده است. با توجه به فقدان مطالعه در حوزه تعیین شدت پیامدهای وقوع خطرهای زیرساخت فیبر

نوری ج.ا.ا، جدول ۲ توسط محقق، توسعه‌یافته و پایایی و روایی آن توسط خبرگان در نشست تخصصی تأییدشده است.

**محاسبه خطر:** حاصل‌ضرب شدت پیامد (تأثیر) در احتمال وقوع یک خطر

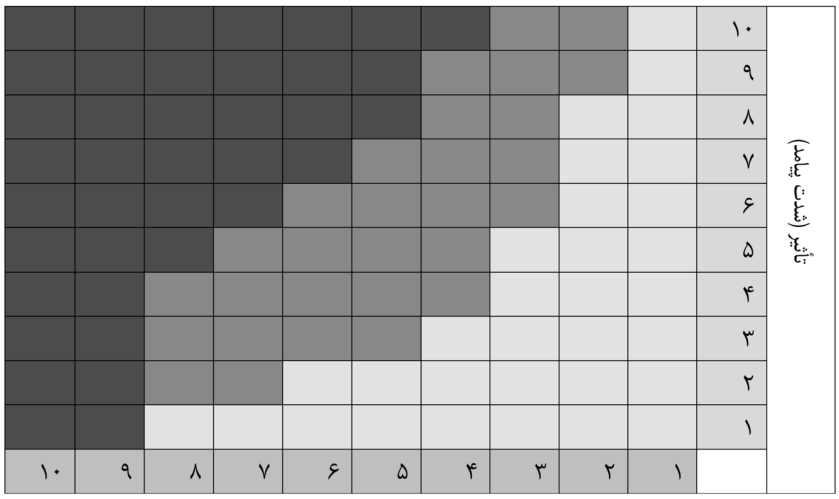
**جدول ۳: مقیاس شدت پیامد (تأثیر) ارزیابی خطرهای امنیتی -فنی زیرساخت ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا**

| رتبه‌بندی | تفسیر<br>بر اساس مؤلفه‌های حوزهٔ امنیت نیروی انسانی/ ابنیه/ تجهیزات (اکتیو، پسیو و نرم‌افزار) |
|---|---|
| ۱ | تأثیری در امنیت ارتباطات و اطلاعات ج.ا.ا ندارد. |
| ۲ | **تأثیر بسیار ناچیز** در امنیت ارتباطات و اطلاعات ج.ا.ا دارد. |
| ۳ | **تأثیر بسیار کم** در امنیت ارتباطات و اطلاعات ج.ا.ا دارد. |
| ۴ | **تأثیر کم** در امنیت ارتباطات و اطلاعات ج.ا.ا دارد. |
| ۵ | **تأثیر متوسط** در امنیت ارتباطات و اطلاعات ج.ا.ا دارد. |
| ۶ | **تأثیر قابل‌توجه** در امنیت ارتباطات و اطلاعات ج.ا.ا دارد. |
| ۷ | **تأثیر زیاد** در امنیت ارتباطات و اطلاعات ج.ا.ا دارد. |
| ۸ | **تأثیر بسیار زیاد** در امنیت ارتباطات و اطلاعات ج.ا.ا دارد. |
| ۹ | **تأثیر بسیار زیاد و تعیین‌کننده** در امنیت ارتباطات و اطلاعات ج.ا.ا دارد. |
| ۱۰ | **تأثیر شگفت‌انگیز** در امنیت ارتباطات و اطلاعات ج.ا.ا دارد. |

### ماتریس خطر (احتمال- تأثیر)

ماتریس خطر، یک ماتریس دوبعدی است که در آن اعداد ۱ تا ۱۰ برای تأثیر و از ۱ تا ۱۰ برای احتمال منظور شده است. خطری که در ناحیه زردرنگ قرارمی‌گیرد، تنها باید مستند و ضبط شود (خطرهای خفیف). خطری که در ناحیه نارنجی قرارمی‌گیرد، باید توسط گروه موردبررسی قرار بگیرد تا مشخص شود که آیا با توجه به دانش تفصیلی گروه در مورد آن پروژه، می‌تواند به مرحله بعد در فرایند مدیریت خطر پیش رود یا خیر (خطر متوسط). خطری که در ناحیه بالا یا قرمزرنگ قرارمی‌گیرد، حتماً به مرحله بعد در فرایند مدیریت خطر پیش خواهد رفت (خطر بالا یا شدید)(مالکهی،۱۳۹۳).

**جدول ۱: ماتریس خطرهای (احتمال- تأثیر)(مالکهی،۱۳۹۳)**




## روش و شیوه تعیین روایی و پایایی

برای تعیین روایی و پایایی سؤالات، یک نشست خبرگی با حضور خبرگان و کارشناسان این حوزه برگزار شد. در این جلسه ضمن وزن‌دهی به‌احتمال و شدت پیامدهای هر خطر، خطرهای مورد بازبینی قرار گرفت.

## ۵-یافته‌های پژوهش

در این بخش، یافته‌های پژوهش در دو بخش ارائه شده است. در بخش اول خطرهای زیرساخت فیبر نوری و سامانه‌های انتقال مربوطه بررسی‌شده و در بخش دوم نتایج رتبه‌بندی خطرهای اطلاعاتی-امنیتی شبکهٔ ملی ارتباطات مبتنی بر فیبر نوری در جمهوری اسلامی ایران ذکرشده است.

**جدول شماره ۴: خطرهای ارزیابی خطرهای امنیتی -فنی زیرساخت ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا در حوزهٔ نیروی انسانی**

| ردیف | عناوین عمومی | احتمال | شدت پیامد | ضریب خطر |
|---|---|---|---|---|
| ۱ | غفلت از تهدیدات امنیتی زیرساخت فیبر نوری به دلیل ناآگاهی و نبود دانش لازم | ۸ | ۷ | ۵۶ |
| ۲ | مشارکت نیروهای بیگانه در طراحی شبکه، تأمین تجهیزات و ارائهٔ خدمات | ۱۰ | ۱۰ | ۱۰۰ |

| ردیف | عناوین عمومی | احتمال | شدت پیامد | ضریب خطر |
|---|---|---|---|---|
| ۳ | بررسی نشدن صلاحیت و سلامت امنیتی نیروی انسانی شرکت‌های طرف قرارداد | ۸ | ۱۰ | ۸۰ |
| ۴ | تخریب، برداشت یا جابجایی غیرقانونی اطلاعات در سامانه‌های انتقال نوری توسط نیروی انسانی متخصص | ۵ | ۱۰ | ۵۰ |
| ۵ | آشکار شدن هویت نیروهای متخصص مؤثر در شبکه زیرساخت با گذر زمان | ۹ | ۶ | ۵۴ |
| ۶ | تمرکز امور در دست عده‌ای اندک به علت وابستگی به تعداد محدودی از نفرات تخصصی | ۱۰ | ۵ | ۵۰ |
| ۷ | کم‌توجهی به رویش نیروهای جدید به علت تلاش برای حفظ وضع موجود | ۹ | ۸ | ۷۲ |
| ۸ | عدم تناسب خدمات ارائه‌شده از سوی نیروهای تخصصی با حقوق دریافتی آنان (فقدان رضایت شغلی) | ۱۰ | ۱۰ | ۱۰۰ |
| ۹ | ضعف مدیران ارشد و تصمیم‌سازان زیرساخت فیبر نوری در شناخت نقاط پر تهدید | ۱ | ۱۰ | ۱۰ |
| ۱۰ | نفوذ در شبکه فیبر نوری در ۲۴ ساعت شبانه‌روز به دلیل فقدان پایش مسیرها | ۱۰ | ۸ | ۸۰ |
| ۱۱ | نفوذ عوامل بیگانه در کادر تخصصی زیرساخت فیبر نوری | ۳ | ۱۰ | ۳۰ |
| ۱۲ | مهاجرت و یا پناهندگی کادر تخصصی زیرساخت فیبر نوری کشور | ۳ | ۸ | ۲۴ |
| ۱۳ | همکاری غیرقانونی نیروهای تخصصی زیرساخت فیبر نوری با عوامل بیگانه | ۴ | ۱۰ | ۴۰ |
| ۱۴ | دسترسی عوامل تخصصی کشورهای بیگانه (قانونی یا غیرقانونی) به زیرساخت فیبر نوری یا سامانه‌های انتقال آن | ۱ | ۸ | ۸ |

**جدول ۵: ماتریس خطرهای (احتمال- تأثیر) شبکهٔ ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا در حوزهٔ نیروی انسانی**

| تأثیر (پیامد) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ۱۰ | ۹ | | ۱۱ | ۱۳ | ۴ | | | ۳ | | ۲ و ۸ |
| ۹ | | | | | | | | | | |
| ۸ | ۱۴ | | ۱۲ | | | ۱ | | | ۷ | ۱۰ |
| ۷ | | | | | | | | | | |
| ۶ | | | | | | | | | ۵ | |
| ۵ | | | | | | | | | | ۶ |
| ۴ | | | | | | | | | | |
| ۳ | | | | | | | | | | |
| ۲ | | | | | | | | | | |
| ۱ | | | | | | | | | | |
| | ۱ | ۲ | ۳ | ۴ | ۵ | ۶ | ۷ | ۸ | ۹ | ۱۰ |

**جدول شماره ۶: خطرهای ارزیابی خطرهای امنیتی -فنی زیرساخت ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا**

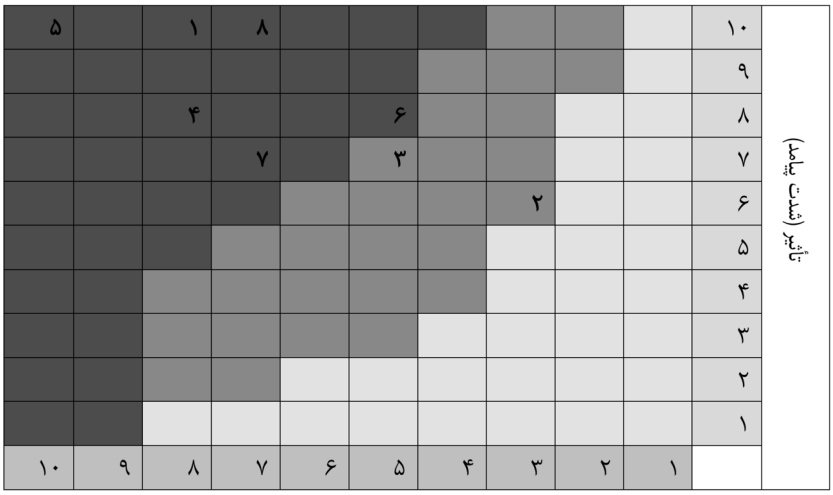
**در حوزهٔ ابنیه (سایت‌ها، اماکن اداری و پشتیبانی)**

| ردیف | عناوین عمومی | احتمال | شدت پیامد | ضریب خطر |
|---|---|---|---|---|
| ۱ | آسیب‌دیدن ابنیه و تجهیزات در اثر حملات دشمن در شرایطی جنگی | ۸ | ۱۰ | ۸۰ |
| ۲ | آسیب‌دیدن ابنیه و تجهیزات در اثر حملات گروهک‌ها | ۳ | ۶ | ۱۸ |
| ۳ | آسیب‌دیدن ابنیه و تجهیزات در اثر اغتشاشات | ۵ | ۷ | ۳۵ |
| ۴ | شناسایی ابنیه و سازه‌های زیرساخت مرتبط به شبکه فیبر نوری به دلیل تیپ بودن آن‌ها | ۸ | ۸ | ۶۴ |
| ۵ | شناسایی ماهیت خریداران با توجه به نوع تجهیزات و سامانه‌های خریداری‌شده | ۱۰ | ۱۰ | ۱۰۰ |
| ۶ | آسیب‌دیدن سامانه‌هایی درون سایت‌ها در اثر بالارفتن دما، آتش‌سوزی داخلی و مختل شدن کارکرد تجهیزات و درنتیجه قطع ارتباط | ۵ | ۸ | ۴۰ |

| ردیف | عناوین عمومی | احتمال | شدت پیامد | ضریب خطر |
|---|---|---|---|---|
| ۷ | دسترسی به برق ورودی سایت‌ها به‌منظور خرابکاری | ۷ | ۷ | ۴۹ |
| ۸ | مختل شدن شبکه به دلیل عدم وجود سایت‌های جایگزین در صورت انهدام سایت‌های اصلی | ۱۰ | ۷ | ۷۰ |

**جدول ۷: ماتریس خطرهای (احتمال- تأثیر) شبکهٔ ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا**

**در حوزهٔ ابنیه (سایت‌ها، اماکن اداری و پشتیبانی)**




**جدول شماره ۸: خطرهای ارزیابی خطرهای امنیتی -فنی زیرساخت ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا در حوزهٔ نرم‌افزار**

| ردیف | عناوین عمومی | احتمال | شدت پیامد | ضریب خطر |
|---|---|---|---|---|
| ۱ | ضعف در توسعه و افزایش ظرفیت شبکه به دلیل نوع طراحی توپولوژی شبکه | ۲ | ۲ | ۴ |
| ۲ | سوءاستفاده از کرهای (تارهای) خاموش | ۴ | ۶ | ۲۴ |
| ۳ | بهره‌برداری غیرقانونی یا تخریب اطلاعات با توجه به تجمیع اطلاعات ترانزیت شبکه در چندکر (تار) مشخص | ۱۰ | ۱۰ | ۱۰۰ |
| ۴ | پایش نشدن تعدادی از مسیرها توسط مونیتورینگ‌ها به دلیل ضعف امکانات و کمبود نیروی انسانی | ۶ | ۶ | ۳۶ |
| ۵ | نادیده‌گرفتن قطعی‌های کوتاه‌مدت در مونیتورینگ سامانه‌ای | ۸ | ۸ | ۶۴ |

| | | | | |
|---|---|---|---|---|
| ۶ | کاهش اثرات رمزنگاری در اثر تضعیف ایجادشده در سیگنال‌های ارسالی | ۱ | ۴ | ۴ |
| ۷ | کاهش امنیت لایه فیزیکی و درنتیجه تأثیر منفی بر امنیت لایه‌های دیگر شبکه | ۸ | ۹ | ۷۲ |
| ۸ | وابستگی به کشورهای بیگانه و عدم تولید نرم‌افزارهای بومی مدیریت شبکه نوری | ۹ | ۹ | ۸۱ |
| ۹ | نفوذ در فریم‌های کنترلی و هدرها به دلیل نداشتن حفاظت امنیتی لازم | ۶ | ۱۰ | ۶۰ |

**جدول ۹: ماتریس خطرهای (احتمال- تأثیر) شبکهٔ ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا**

**در حوزهٔ نرم‌افزاری شبکه**

| تأثیر (شدت پیامد) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ۱۰ | | | | ۹ | | | | | | ۳ |
| ۹ | | | | | | | | ۷ | ۸ | |
| ۸ | | | | | | | | ۵ | | |
| ۷ | | | | | | | | | | |
| ۶ | | | | ۴ | | | | | | |
| ۵ | | | | | | | | | | |
| ۴ | ۶ | | | ۲ | | | | | | |
| ۳ | | | | | | | | | | |
| ۲ | | ۱ | | | | | | | | |
| ۱ | | | | | | | | | | |
| | ۱ | ۲ | ۳ | ۴ | ۵ | ۶ | ۷ | ۸ | ۹ | ۱۰ |

**جدول شماره ۱۰: خطرهای ارزیابی خطرهای امنیتی -فنی زیرساخت ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا**

**در حوزهٔ تجهیزات اکتیو شبکه**

| ردیف | عناوین عمومی | احتمال | شدت پیامد | ضریب خطر |
|---|---|---|---|---|
| ۱ | جاسازی غیرقانونی قطعات در بردها (مدارات) سامانه‌های انتقال نوری به‌منظور فعالیت‌های جاسوسی | ۸ | ۱۰ | ۸۰ |
| ۲ | برداشت، جابجایی و اختلال در اطلاعات موجود در شبکه بدون به‌جاگذاری آثار و نشانه | ۸ | ۸ | ۶۴ |

| ردیف | عناوین عمومی | احتمال | شدت پیامد | ضریب خطر |
|---|---|---|---|---|
| ۳ | بهره‌برداری غیرقانونی به دلیل بازبودن کانال‌های ارتباطی داده در بین پورت‌های بهره‌برداران و شبکه اصلی (DCC) | ۵ | ۹ | ۴۵ |
| ۴ | بهره‌برداری اطلاعاتی- امنیتی از بلاتکلیفی برخی از لینک‌های ارتباطی | ۳ | ۶ | ۱۸ |
| ۵ | ضعف در پایش وضعیت دمای محیط و سامانه‌های انتقال نوری توسط عوامل انسانی | ۲ | ۶ | ۱۲ |
| ۶ | عدم پایش تمامی کرها (تارهای) شبکه توسط مرکز مونیتورینگ به دلیل ضعف امکانات و کمبود نیروی انسانی | ۶ | ۴ | ۲۴ |
| ۷ | نفوذ سریع، بدون ایجاد حساسیت در شبکه به دلیل نادیده‌گرفتن قطعی‌های کوتاه‌مدت در مونیتورینگ سامانه‌ای | ۷ | ۹ | ۶۳ |
| ۸ | آسیب‌دیدن تجهیزات در مقابل بمب‌های الکترومغناطیس | ۹ | ۱۰ | ۹۰ |

**جدول ۱۱: ماتریس خطرهای (احتمال- تأثیر) شبکهٔ ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا**

**در حوزهٔ تجهیزات اکتیو شبکه**

| تأثیر (شدت پیامد) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ۱۰ | | | | | | | | ۱ | ۸ | |
| ۹ | | | | | | ۳ | | ۷ | | |
| ۸ | | | | | | | | ۲ | | |
| ۷ | | | | | | | | | | |
| ۶ | | | ۵ | ۴ | | | | | | |
| ۵ | | | | | | | | | | |
| ۴ | | | | | ۶ | | | | | |
| ۳ | | | | | | | | | | |
| ۲ | | | | | | | | | | |
| ۱ | | | | | | | | | | |
| | ۱ | ۲ | ۳ | ۴ | ۵ | ۶ | ۷ | ۸ | ۹ | ۱۰ |

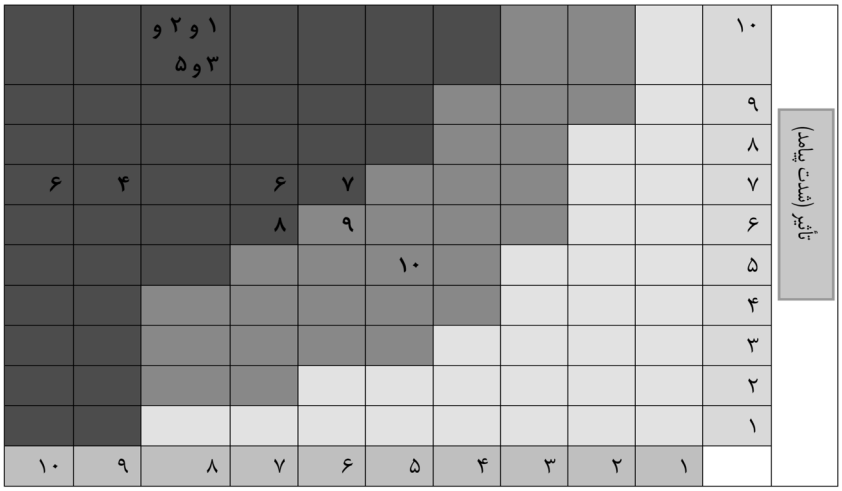
**جدول شماره ۱۲: خطرهای ارزیابی خطرهای امنیتی -فنی زیرساخت ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا**

**در حوزهٔ تجهیزات پسیو شبکه**

| ردیف | عناوین عمومی | احتمال | شدت پیامد | ضریب خطر |
|---|---|---|---|---|
| ۱ | تسهیل در بهره‌برداری اطلاعاتی دشمن با توجه به شنود فیبر نوری در کشورهای جنوب خلیج‌فارس و دریای عمان (استقرار پایگاه، کشتی و زیردریایی) | ۱۰ | ۸ | ۸۰ |
| ۲ | تقرب بدون قطع به فیبرهای نوری به‌منظور تخریب، تزریق و یا برداشت اطلاعات از آن | ۱۰ | ۸ | ۸۰ |
| ۳ | دسترسی غیرقانونی و سهل به فیبر نوری در مسیرهایی که فیبر نوری پایش نمی‌شود، مانند نقاط صعب‌العبور | ۹ | ۷ | ۶۳ |
| ۴ | بهره‌برداری‌های اطلاعاتی- امنیتی از فیبرهای در اماکنی که فیبر شبکه اصلی در داخل حریم شخصی قرار گرفته است | ۱۰ | ۸ | ۸۰ |
| ۵ | دسترسی آسان به بسیاری از مفصل‌های فیبرهای شهری از طریق حوضچه‌های مخابراتی | ۱۰ | ۷ | ۷۰ |
| ۶ | آسیب‌دیدن فیبرهای نوری داخل شهرها به دلیل حفاری‌های کم‌عمق و سطحی | ۷ | ۷ | ۴۹ |
| ۷ | مختل یا قطع شدن بخشی از ارتباطات ملی به دلیل تحریم و ممانعت از واگذاری تجهیزات اکتیو و یا پسیو توسط شرکت‌های خارجی تأمین‌کننده | ۶ | ۷ | ۷۲ |
| ۸ | قطع ارتباطات به دلیل بلایای طبیعی و ازبین‌رفتن بخشی از زیرساخت فیبر نوری | ۷ | ۶ | ۴۲ |
| ۹ | گسترش شبکه فیبر نوری با عدم درنظرگرفتن ملاحظات امنیتی-اطلاعاتی | ۶ | ۶ | ۳۶ |
| ۱۰ | بهره‌برداری اطلاعاتی و امنیتی غیرقانونی از زیرساخت فیبر نوری به دلیل بی‌توجهی و رهاسازی بخشی از مسیرهای فیبر نوری | ۵ | ۵ | ۲۵ |

**جدول ۱۳: ماتریس خطرهای (احتمال- تأثیر) شبکهٔ ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا**

**در حوزهٔ تجهیزات پسیو شبکه**




**جدول شماره ۱۴: خطرهای ارزیابی خطرهای امنیتی -فنی زیرساخت ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا**

**در حوزه‌های دیگر**

| ردیف | عناوین عمومی | احتمال | شدت پیامد | ضریب خطر |
|---|---|---|---|---|
| ۱ | بهره‌برداری هدفمند از یک فیبر ویژه که دارای اطلاعات ارزشمند است با توجه به موقعیت مکانی بهره بدار فیبر نوری (نظیر مراکز هسته‌ای و ...) | ۱۰ | ۱۰ | ۱۰۰ |
| ۲ | ضعف سامانه‌های کنترلی و نظارتی به دلیل مجتمع و یکپارچه نشدن توضیح احتمال خطر در شبکه ارتباطی فیبر نوری کشور | ۲ | ۸ | ۱۶ |
| ۳ | آسیب‌دیدن سایت‌ها و ابنیه به علت وجود وابستگی صنعت مخابرات به کشورهای بیگانه (اطلاع از محل نصب سامانه‌ها خریداری‌شده) | ۶ | ۸ | ۴۸ |
| ۴ | آلوده‌شدن تجهیزات و نرم‌افزار به علت وجود وابستگی صنعت مخابرات به کشورهای بیگانه | ۷ | ۱۰ | ۷۰ |
| ۵ | القای امن بودن بستر فیبر نوری توسط کشورهای دارای صنعت و فنّاوری فیبر نوری به‌منظور اشراف اطلاعاتی و بهره‌مندی از منافع اقتصادی | ۱۰ | ۸ | ۸۰ |
| ۶ | آسیب‌دیدن دارایی‌های اطلاعاتی موجود در بستر فیبر نوری به دلیل عدم وجود استراتژی جامع جهت حفاظت مطمئن از دارایی‌های اطلاعاتی منتقل‌شده از طریق فیبر نوری | ۶ | ۶ | ۳۶ |

**جدول ۱۵: ماتریس خطرهای (احتمال- تأثیر) شبکهٔ ملی ارتباطات مبتنی بر فیبر نوری در ج.ا.ا**

**در حوزه‌های دیگر**

| شبکهٔ ملی ارتباطات مبتنی بر فیبر نوری (ج.ا.ا) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ۱۰ | | | | | | | | ۴ | | ۱ |
| ۹ | | | | | | | | | | |
| ۸ | | ۲ | | | | | ۳ | | | ۵ |
| ۷ | | | | | | | | | | |
| ۶ | | | | | | | ۶ | | | |
| ۵ | | | | | | | | | | |
| ۴ | | | | | | | | | | |
| ۳ | | | | | | | | | | |
| ۲ | | | | | | | | | | |
| ۱ | | | | | | | | | | |
| | ۱ | ۲ | ۳ | ۴ | ۵ | ۶ | ۷ | ۸ | ۹ | ۱۰ |

## ۶- نتیجه‌گیری

خطرهای شدید در زیرساخت فیبر نوری مخابرات کشور به ترتیب اولویت شامل موارد زیر است:

**۱) مشارکت نیروهای بیگانه در طراحی شبکه، تأمین تجهیزات و ارائهٔ خدمات:**

با توجه به اینکه کلیت فتّاوری (فتّاوری) مخابرات کشور در انحصار کشورهای بیگانه است -و عملاً بومی‌سازی صنعت مخابرات به‌ویژه در حوزهٔ سامانه‌های نوری در آینده‌ای نزدیک امری دور از ذهن به نظر می‌رسد- لذا اشراف بیگانگان در ساخت تجهیزات، طراحی شبکه و ارائه خدمات جمهوری اسلامی ایران حداکثری بوده و لذا مهم‌ترین خطر این حوزه است.

**۲) عدم تناسب خدمات ارائه‌شده از سوی نیروهای تخصصی با حقوق دریافتی آنان:**

کادر تخصصی شاغل در زیرساخت فیبر نوری کشور از اجرای شبکه فیبر نوری تا مدیریت سامانه‌های انتقال نوری دارای دانش نسبتاً بالا و کاملاً ویژه‌ای هستند. فقدان رضایت شغلی این قشر -به دلایل متعدد مانند رفتارهای نامناسب درون‌سازمانی توسط مدیران

بالادستی و پایین‌بودن دریافتی- می‌تواند ضمن پایین آوردن بازده آنان، زمینه جذب آنان توسط بیگانگان را فراهم کند.

**۳) شناسایی ماهیت خریداران با توجه به نوع تجهیزات و سامانه‌های خریداری‌شده:**

بنا به اظهارات مسئولین مربوطه تقریباً تمامی تجهیزات مرتبط با سامانه‌های انتقال نوری از کشوری مانند چین با نام و نشانی دقیق بهره‌بردار مربوطه بسته‌بندی و ارسال می‌گردند. این بدان معناست که ضمن مشخص‌بودن ماهیت خریداران تجهیزات، حتی آدرس و نشانی بهره‌برداران خُردتر نیز در اختیار شرکت‌های خارجی قرارمی‌گیرد. این مهم زمانی اهمیت بیشتری می‌یابد که بهره‌برداران ویژه‌ای مانند صنایع هسته‌ای، سازمان‌های نظامی، امنیتی و ... نیز در این چرخه قرار گیرند.

**۴) برون‌سپاری مدیریت شبکه ارتباطات کشور به شرکت‌های خصوصی دانش‌بنیان:**

در سال‌های اخیر به‌منظور چابک سازی سازمان مخابرات کشوری و به‌منظور استفاده از ظریف شرکت‌های دانش‌بنیان، برخی از امورات مرتبط با مدیریت زیرساخت ارتباطات کشور به شرکت‌های خصوصی واسپاری شد. دسترسی به سرورهای اصلی و مغز شبکه ارتباطات کشوری قابلیتی است که بایستی تنها در اختیار نهادهای حاکمیتی باشد. اینکه در صنعت مخابرات کشور بخشی از مدیریت شبکه توسط کارشناسان خارجی و بخشی دیگر توسط شرکت‌های خصوصی انجام می‌شود با مفهوم امنیت ملی در تناقضی آشکار است چراکه در این بستر اطلاعات ارزشمند حاکمیتی نظیر داده‌های کلان اقتصادی، سیاسی، امنیتی و خدماتی مبادله می‌شود.

**۵) بهره‌برداری غیرقانونی یا تخریب اطلاعات با توجه به تجمیع اطلاعات ترانزیت شبکه در تارهای مشخص:**

در شبکه فیبر نوری معمولاً بین سامانه‌های انتقال، تارهای محدود و مشخصی برای مدیریت شبکه و انتقال اطلاعات در نظر گرفته می‌شود؛ این امر شرایط را برای بهره‌برداری غیرقانونی و یا تخریب هدفمند اطلاعات تسهیل می‌نماید.

**۶) بهره‌برداری هدفمند از یک فیبر ویژه که دارای اطلاعات ارزشمند است با توجه به موقعیت مکانی بهره‌بردار فیبر نوری (نظیر مراکز هسته‌ای و ...):**

شبکه فیبر نوری برای ارائه خدمات به بهره‌برداران، بایستی به‌صورت سخت‌افزاری مسیرهای فرعی را به مسیرهای اصلی فیبر نوری متصل نماید و این به معنای مشخص شدن مسیر انتقال اطلاعات بهره‌برداران دارای طبقه‌بندی بالا است.

**۷) آسیب‌دیدن تجهیزات در مقابل بمب‌های الکترومغناطیس:**

ماهیت قطعات و مدارات الکترونیکی ازجمله سامانه‌های انتقال، رک‌های تغذیه، تجهیزات درون سایت‌ها و... به شکلی است که در برابر حملات الکترومغناطیس پرقدرت بسیار آسیب‌پذیر هستند.

**۸) بررسی نشدن صلاحیت و سلامت امنیتی نیروی انسانی شرکت‌های طرف قرارداد:**

ساختار روابط و شکل تعاملات با شرکت‌های داخلی و خارجی به‌گونه‌ای است که تقریباً صلاحیت هیچ‌یک از نیروهای طرف قرارداد و ارائه‌دهنده خدمات موردبررسی امنیتی قرار نمی‌گیرد و این مهم باعث تسهیل نفوذ عوامل بیگانه در شبکه زیرساخت فیبر نوری است.

**۹) نفوذ در شبکه فیبر نوری در ۲۴ ساعت شبانه‌روز به دلیل فقدان پایش مسیرها:**

مسیرهای فیبر نوری در کشور به شکلی است که عوامل حراستی (خط‌بان یا پایشگر مسیر) به‌صورت موتوری یا خودرویی به کنترل روزانه می‌پردازند. بدیهی است که اولاً این نظارت‌ها برای یک مکان خاص لحظه‌ای بود و بخشی از روز و کل شب بر روی مسیرهای فیبر نوری هیچ‌گونه نظارت انسانی وجود ندارد. لذا بدیهی است که با توجه به گستردگی شبکه در کل کشور، تقرب به شبکه فیبر نوری چندان دشوار نبوده و حتی در ساعات ذکرشده کوچک‌ترین مانعی، دسترسی به فیبرهای نوری بسیار ساده است.

**۱۰) آسیب‌دیدن ابنیه و تجهیزات در اثر حملات دشمن در شرایطی جنگی:**

در صورت ایجاد شرایط جنگی بسیاری از ابنیه و مراکز مربوط به فیبر نوری به دلیل آشکار بودن موقعیت آنان آسیب‌پذیر خواهند بود.

**۱۱) وابستگی به کشورهای بیگانه و عدم تولید نرم‌افزارهای بومی مدیریت شبکه نوری:**

علاوه به وابستگی صنعت مخابرات در حوزه سخت‌افزار در بُعد نرم‌افزار نیز این وابستگی وجود دارد و این به معنای واگذار نمودن مدیریت پنهان ارتباطات و اطلاعات به بیگانگان است.

**۱۲) جاسازی غیرقانونی قطعات در مدارات (بُردها) سامانه‌های انتقال نوری به‌منظور فعالیت‌های جاسوسی:**

به دلایل ذکرشده فوق امکان جاسازی تجهیزات جاسوسی و یا تخریبی در سخت‌افزارهای وارداتی بدون ایجاد حساسیت وجود دارد.

**۱۳) تسهیل در بهره‌برداری اطلاعاتی دشمن با توجه به شنود فیبر نوری در کشورهای جنوب خلیج‌فارس و دریای عمان (استقرار پایگاه، کشتی و زیردریایی):**

بنا به اطلاعات افشاء شده در دریا و حتی در کشورهای جنوب خلیج‌فارس سایت‌های سیار و ثابت شنود فیبر نوری استقرار داشته که قادر به بهره‌برداری از اطلاعات این فیبرهای بین‌المللی هستند.

**۱۴) تقرب بدون قطع به فیبرهای نوری به‌منظور تخریب، تزریق و یا برداشت اطلاعات از آن:**

پیشرفت فنّاورانه در صنعت فیبر نوری این امکان را برای صاحبان آن فراهم کرده بدون قطع نمودن فیبرهای نوری امکان دسترسی به اطلاعات درون فیبرها را داشته باشند.

**۱۵) بهره‌برداری‌های اطلاعاتی- امنیتی از فیبرهای در اماکنی که فیبر شبکه اصلی در داخل حریم شخصی قرار گرفته است:**

اقتضائات اجرای شبکه فیبر نوری در کشور به شکلی است که در موارد متعدد فیبرها از درون حریم شخصی افراد عبور کرده است، لذا امروزه شاهد آن هستیم که برخی از فیبرها در زیر ساختمان‌ها و ابنیه‌هایی قرارگرفته‌اند که امکان نظارت و دسترسی به آن‌ها برای دولت وجود ندارد.

**۱۶) القای امن بودن بستر فیبر نوری توسط کشورهای دارای صنعت و فنّاوری فیبر نوری به‌منظور اشراف اطلاعاتی و بهره‌مندی از منافع اقتصادی:**

فرضیه امن بودن فیبر نوری باعث شده که بسیاری از بهره‌برداران با تساهل به موضوع زیرساخت فیبر نوری برخورد کرده و اطلاعات ارزشمند سازمان خود را به‌راحتی در این

بستر منتقل نمایند. این امر باعث کسب درآمد هر بیشتر شرکت‌های مجری فیبر نوری شده و در نگاه کلان‌تر امکان اشراف اطلاعاتی بیگانگان را افزایش می‌دهد.

**۱۷) کم‌توجهی به رویش نیروهای جدید به علت تلاش برای حفظ وضع موجود:**

گردش نخبگان علمی در زیرساخت فیبر نوری کشور نیازمند توجهی جدی است. به دلیل ماهیت دولتی زیرساخت فیبر نوری کشور و محدودیت در مشوق‌های لازم برای جذب نخبگان در این حوزه، تلاش مدیران حداکثر برای حفظ وضع موجود خواهد بود.

**۱۸) مختل شدن شبکه به دلیل عدم وجود سایت‌های جایگزین در صورت انهدام سایت‌های اصلی:**

طراحی شبکه زیرساخت فیبر نوری به شکلی است که اصول فنی-تخصصی و حتی پدافند غیرعامل مورد کم‌توجهی واقع شده است و درنتیجه سایت‌های جایگزین برای شبکه در مواقع بحران در نظر گرفته نشده است. لذا در صورت انهدام یک سایت، شبکه در آن مسیر کارایی خود را از دست خواهد داد.

**۱۹) کاهش امنیت لایه فیزیکی و درنتیجه تأثیر منفی بر امنیت لایه‌های دیگر شبکه:**

به دلیل ماهیت شبکه‌های ارتباطی بدیهی است با کاهش امنیت در یک‌لایه، امنیت در لایه‌های دیگر دچار اختلال گردد.

**۲۰) دسترسی آسان به بسیاری از مفصل‌های فیبرهای شهری از طریق حوضچه‌های مخابراتی:**

در شرایطی که درپوش‌های فلزی حوضچه‌های مخابراتی به‌راحتی هرروزه مورد دستبرد قرار می‌گیرند، امکان دسترسی به مفصل‌های موجود در آن نیز به‌سادگی فراهم است. لذا اقدامات خرابکارانه به‌عنوان بدیهی‌ترین تهدید در کنار سایر آسیب‌ها و تهدیدات از این نقاط، متصور است.

**۲۱) انجام عملیات کابل گذاری ترینچری با عمق بسیار کم:**

به دلیل هزینه کم و سرعت بالا در سنوات اخیر کابل گذاری‌ها با برش زمین و دفن کردن کابل در عمق‌های ناایمن ۳۰ الی ۴۰ سانتیمتری در سطح شهرها و حتی در مسیرهای بین‌شهری انجام می‌شود. این روند از اشتباهات راهبردی در سیاست‌گذاری راهبردی در شبکه ارتباطات کشوری است و نیازمند بررسی جدی خواهد بود.

**۲۲) مختل یا قطع شدن بخشی از ارتباطات ملی به دلیل تحریم و ممانعت از واگذاری تجهیزات اکتیو و یا پسیو توسط شرکت‌های خارجی تأمین‌کننده:**

وجود وابستگی شدید کشور به بیگانگان در حوزه زیرساخت فیبر نوری به‌ویژه در سامانه‌های انتقال، باعث شده که این شبکه از پویایی لازم برخوردار نباشد و همواره حیات آن وابسته به خارج از کشور باشد. در این شرایط است که تحریم می‌تواند بخشی از ارتباطات ملی را مخل یا قطع کند.

**پیشنهادهای کاربردی**

در سال‌های آتی، با ارتقای دانش سازمان‌ها در حوزهٔ فنّاوری اطلاعات و ارتباطات در کشور، ممکن است برخی از وزارتخانه‌ها یا سازمان‌های بزرگ علاوه بر بهره‌مندی از زیرساخت ملی فیبر نوری به دنبال استفادهٔ حداکثری از قابلیت‌های فیبر نوری و سامانه‌های انتقال نوری به‌صورت کاملاً اختصاصی باشند. داشتن شبکه‌ای مستقل و غیروابسته به وزارت ارتباطات و فنّاوری اطلاعات احتمالاً یکی از برنامه‌های بلندمدت برخی از این سازمان‌ها باشد. به نظر می‌رسد ایجاد شبکه ارتباطی مستقل برای یک سازمان به گستردگی یک وزارتخانه پرچالش و بحث‌برانگیز باشد و ممکن است به‌سرعت به یک مسئله امنیتی تبدیل شود.

این شبکه به‌عنوان امانت‌داری مطمئن می‌خواهد تمامی اطلاعات و ارتباطات سازمانی را منتقل و مدیریت نماید و این مهم ضمن آنکه حادثه‌ای بزرگ، رخدادی بی‌نظر و جهش در فنّاوری خواهد بود، ضرورت‌های اجتناب‌ناپذیری خواهد داشت که لازم است به آن‌ها توجه ویژه شود. در گذر زمان برخی از اهداف طراحان شبکه مذکور نظیر؛ رسوب دانش، نیرو و تجهیزات، به‌صورت نسبی محقق خواهد شد. این مولود می‌تواند سازمان‌های بهره‌بردار را به‌سوی یک جامعه اطلاعاتی یکپارچه رهنمون کند و به دنبال خود رشد سریع سامانه‌ها و سرویس‌های فنّاوری اطلاعات را به دنبال داشته باشد اما در کنار آن خطرهای شدیدی را نیز به دنبال خواهد داشت که به‌مراتب از خطرهای امنیتی- فنی زیرساخت ملی ارتباطات مبتنی بر فیبر نوری کشور شدیدتر خواهند بود.

بنابراین به نظر می‌رسد گسترهٔ موضوع امنیت در سه حوزهٔ نیروی انسانی، تجهیزات (سخت‌افزار و نرم‌افزار) و اماکن، نیازمند بررسی دقیق علمی است. تأمین امنیتِ گنجینهٔ

ارزشمند اطلاعاتی بدون‌شک یکی از ضروریات بوده و نیاز است با احصاء و ارزیابی عوامل محیطی (فرصت‌ها و تهدیدها) و همچنین عوامل درونی سازمان (قوت‌ها و ضعف‌ها) نسبت به تدوین راهبرد در این حوزه اقدام نمود و اقدامات متناسب را سریع‌تر عملیاتی نمود؛ بنابراین ضروری است اصول مهم ذیل را مدنظر داشت:

- رعایت اصول پدافند غیرعامل در ساخت ابنیه و سایت‌های تخصصی و اداری
- بومی‌سازی تجهیزات تخصصی موردنیاز و نرم‌افزارهای مربوطه
- پیشگیری از دستیابی غیرقانونی و نفوذ عوامل بیگانه به زیرساخت ارتباطی
- لزوم توجه به نیروی انسانی متخصص و متعهد و ...

## منابع:

### الف) منابع فارسی:


- اندیشگاه شریف، (۱۳۸۵)، «**الزامات جنگ‌های نوین در فضای سایبر (مجازی)**»، وزارت دفاع و پشتیبانی نیروهای مسلح، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، مرکز آینده‌پژوهی علوم و فنّاوری دفاعی، (شرکت اندیشه پردازان شریف).
- م محمدی، (۱۳۹۰)، «**فاوا: جنگ آینده، ماهنامه اطلاعات راهبردی**»، سال نهم، شماره ۳۷ -
- م مهدی نژاد، م خراشادی زاده، م فخری و الف احمدی حاجی‌آبادی، (۱۳۹۸)، «**نقش فنّاوری اطلاعات و ارتباطات در دفاع دانش‌بنیان**»، فصلنامه مطالعات دفاعی استراتژیک سال هفدهم، شماره۷۵، بهار ۱۳۹۸، مقاله پنجم، از صفحه ۱۲۴-۱۰۷
- ع پور سلامی، م یدیسار، ن منتظری و پ ستاری، «**روش‌های شنود سیگنال در فیبر نوری، تشخیص و جلوگیری از آن**»، بیست و چهارمین کنفرانس مهندسی برق ایران، دانشگاه صنعتی شیراز، ۱۳۹۵
- ف کریمی، م یدیسار، م بلوری زاده و ع احمدی، «**سرقت اطلاعات از فیبر نوری**»، بیستمین کنفرانس اپتیک و فوتونیک ایران، دانشگاه صنعتی شیراز،۱۳۹۲
- ش شادرخ و ق کمکی، ق. (۱۳۸۷). «مط**العه موردی PMBOK.مدیریت خطر بر اساس استاندارد**»، چهارمین کنفرانس بین‌المللی مدیریت پروژه. تهران.
- ک شوالب. (۱۳۷۸). مدیریت پروژه با رویکرد پروژه‌های فنّاوری اطلاعات، ترجمه محمود گلابچی. تهران: انتشارات دانشگاه تهران.
- ر مالکهی. (۱۳۹۰). مدیریت خطر پروژه، ترجمه و تألیف حسین عوض خواه، امیرحسین محبی. تهران: کیان رایانه سبز.
- بی ام آی. (۱۳۸۸). استاندارد ملی مدیریت خطر، ترجمه صادق روزبی، خدیجه جدا، تهران: پندار پارس.
- ج صیدی، ع پور اسلامی. (۱۴۰۳). «شناسایی روش‌های استخراج محتوا از فیبر نوری»، تهران: دانشگاه امام حسین (ع)
- الف مصطفایی. (۱۳۹۹). «درآمدی بر امنیت در بستر فیبر نور»، تهران: دانشگاه امان حسین (ع)
- ب) منابع انگلیسی:
- Bartczak Summer (2002) Identifying Barriers to Knowledge Management In The
- United States Military, Americas Conference on Information Systems (AMCIS).
- Gervone, H. (2006). Management digital libraries: the view from 30000 feet (Project iskManagement). OCLC Systems & Services: International digital library perspectives, 256-262.
- Manuri ismail, Abdullah raja. (2011), Perceptions of knowledge creation,
- knowledge management processes, technology and applications in military
- organisations, Malaysian Journal of Library & Information Science, Vol. 16, no. 1.

- X.W. Zou, P., Zhang, G., & Wang, J. (2007).Understanding the key risks in construction projects in China. International Journal of Project Management, 601-614.
- ShaojingSu, JingZhou, ZhipingHuang,YimengZhang, ZhenZuo, “Asecure transmissions cheme on link level for optical fiber communication systems”, (2014)
- Wei Baia, Hui Yanga, AoYua, Hongyun Xiaob, Linkuan Hea, Lei Fengc, Jie Zhang, «Eavesdropping-aware routing and spectrum allocation based on multi-flowvirtual concatenation for confidential information service in elastic opticalnetworks”, (2018)
- Kyle Guan, Junho Cho, Peter J. Winzer, «Physical layer security in fiber-optic MIMO-SDM systems: An overview”, (2017)
- Lauren Collins, Computer and Information Security HandbookOptical, Network Security,Chapter 19, (2013)
- Sandra Kay MillerIssue, Optical Illusion http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1228170,00.htmlby, )Nov 2006(
- Sandra Kay Miller, http://informationsecurity.techtarget.com/magItem, (2006)
- Kyle Guan, Junho Cho, Peter J. Winzer, Physical layer security in fiber-optic MIMO-SDM systems, Optics Communications, (2014)
- Lauren Collins, Optical Network Security, Chapter 19, (2018)
- Wei Baia, Hui Yanga, Ao Yua, Hongyun Xiaob, Linkuan Hea, Lei Fengc, Jie Zhanga, virtual concatenation for confidential information service in elastic optical networks, Optical Fiber Technology, (2018)
- Marcin Kowalski, Marek Zyczkowski, Encryption method based on pseudo random spatial light modulation for single-fibre data transmission, Optics Communications, (2017)
- Ben Wu, Bhavin J. Shastri, and Paul R. Prucnal,, Secure Communication in Fiber-Optic Networks, Chapter 11, (2018)
- Xiaosong Fua, Meihua Bia,b, Xuefang Zhoua, Guowei Yanga, Qiliang Lia, Zhao Zhouc,Xuelin Yangb, A chaotic modified-DFT encryption scheme for physical layer security and PAPR reduction in OFDM-PON, Optical Fiber Technology(2018),
- Bo Liu, LijiaZhang, XiangjunXin, JianjunYu,Physical layersecurityin CO-OFDM transmission systemusing chaotic scrambling, Optics Communications (2013),