چارچوب آینده‌نگاری رویارویی پیش‌فعالانه با تهدیدهای سایبری

مؤلفان:

خلیل کولیوند

ابراهیم ایجابی

نیما فرزام‌نیا

انتشارات دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

۱۴۰۳

سرشناسه	:	کولیوند، خلیل، ۱۳۶۰
عنوان و نام پدیدآور	:	چارچوب آینده‌نگاری رویارویی پیش‌فعالانه با تهدیدهای سایبری/ مولفین خلیل کولیوند، ابراهیم ایجابی، نیما فرزام‌نیا.
مشخصات نشر	:	تهران: ارتش جمهوری اسلامی ایران، دانشگاه فرماندهی و ستاد، انتشارات دافوس، ۱۴۰۳.
شابک	:	۹۷۸-۶۲۲-۸۳۳۰-۲۲-۸
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	کتابنامه:ص.۱۴۶-۱۵۲.
موضوع	:	تروریسم رایانه‌ای -- آینده‌نگری Cyberterrorism-- Forecasting فضای مجازی -- تدابیر ایمنی -- آینده‌نگری Cyberspace -- Security measures -- Forecasting شبکه‌های کامپیوتری -- تدابیر ایمنی -- آینده‌نگری Computer networks -- Security measures -- Forecasting جنگ سایبری -- تدابیر ایمنی -- آینده‌نگری Cyberspace operations (Military science) -- Security measures -- Forecasting
شناسه افزوده	:	ایجابی، ابراهیم، ۱۳۵۳
شناسه افزوده	:	فرزام‌نیا، نیما، ۱۳۵۷
اطلاعات رکورد کتابشناسی	:	فیپا

عنوان: چارچوب آینده‌نگاری رویارویی پیش‌فعالانه با تهدیدهای سایبری

مؤلفان: خلیل کولیوند ، ابراهیم ایجابی و نیما فرزام‌نیا

ویراستار: زهرا قلخانباز

طراح جلد: میلاد فرهادی

صفحه‌آرایی: حسین بیگدلی‌شاد

ناشر: دافوس

شمارگان: ۱۰۰۰

تعداد صفحه: ۱۵۲ ص

نوبت چاپ: چاپ اول

تاریخ نشر: ۱۴۰۳

چاپ و صحافی: مدیریت چاپ، انتشارات و فصلنامه دانشگاه فرماندهی و ستاد آجا

قیمت: ۱.۷۰۰.۰۰۰ریال

نشانی: تهران، میدان پاستور، خیابان دانشگاه جنگ، دانشگاه فرماندهی و ستاد، انتشارات دافوس

تلفن: ۶۶۴۱۴۱۹۱ – ۰۲۱، ۶۶۴۷۰۴۸۶-۰۲۱

فهرست

عنوان **شماره صفحه**

مقدمه

در حوزه دفاع سایبری همواره اهدافی نظیر محرمانه بودن، صداقت، در دسترس بودن، غیر قابل انکار بودن و خروج از سیستم دوستانه مدنظر قرار می‌گیرد. در واقع عملیات سایبر تهاجمی و دفاعی عناصر کلیدی از جنگ اطلاعات هستند. این عوامل همواره برای حمایت از طیف کامل امور امنیت ملی در دسترس هستند، در زمان صلح عناصر قدرت ملی برای جلوگیری از بحران و درگیری کار می‌کنند و در زمان بحران، می‌توانند به شکل دادن اوضاع به نفع کشور و کمک به جلوگیری از تشدید بالقوه خرابکاری‌ها کمک کند.

عوامل مورد نظر در هنگام جنگ سایبری به‌عنوان عوامل فزاینده نیروی جنبشی مورد استفاده قرار می‌گیرد و در عملیات نیز می‌توانند به زمان صلح کمک کنند. امروزه جنگ سایبری از جدی‌ترین چالش‌های امنیتی است که از طریق فضای مجازی به دولت‌ها و اشخاص تحمیل می‌شود. تفاوت قائل شدن بین حالت تهاجمی و غیرتهاجمی در فضای مجازی بسیار حائز اهمیت است، زیرا زمانی که جنگ سایبری مطرح است، روابط بین حالات بسیار مهم بوده و طرفین جنگ نیز باید درباره ماهیت دقیق جنگ سایبری مطلع باشند.

علاوه بر این مسئله پیچیدگی فضای مجازی، چالش‌های متأثر از برداشت سنتی دولت‌ها از حذف و سرعت تحول رسانه‌های جمعی همواره باید مدنظر قرار گیرد. در حال حاضر این مسئله می‌تواند دلیلی برای به‌کار نگرفتن ابزار جنگی و بهره‌گیری از تکنیک‌ها و روش‌های جدید در رابطه با راهبرد، همواره در خدمت سیاست محسوب شود. هرچند ممکن است در سطح جهان برای جنگ سایبری سیاست‌های متعددی اتخاذ شود.

پیچیدگی سامانه‌ها و شبکه‌های مبتنی بر فناوری اطلاعات، چالش‌های امنیتی و سایبری فراوانی را برای سازمان‌ها به همراه دارد. برای مثال اقدام‌های تهدیدآفرین بازیگران قوی و ضعیف در فضای سایبر اعم از دولت‌ها، گروه‌های سازمان‌یافته، گروهک‌های تروریستی و حتی افراد عادی در قالب اقداماتی مانند جنگ سایبری[1]، جرائم سایبری[2]، تروریسم

1- Cyber War
2- Cyber Crimes

سایبری[1]، جاسوسی سایبری[2] و دیگر انواع آن هر روزه تهدیدهای جدیدی را متوجه زیرساخت‌های سازمان‌ها می‌کند که از اهمیت خاصی برخوردار است و تشخیص این تهدیدهای بالقوه، پیامدها و چالش‌های امنیتی آن‌ها در محیط پیچیده و سرشار از عدم قطعیت آینده، بر حساسیت کار می‌افزاید[3].

بر این اساس، ارتقاء پایداری عملیاتی و مصون‌سازی زیرساخت‌های حیاتی سازمان‌ها در مقابله با تهدیدهای سایبری نمود ویژه‌ای خواهد یافت. ضمن اینکه اصول نوین حاکم بر فضای سایبر، نهادها و ساختارها را ملزم به شناخت این فضا و استفاده بجا از دانش و ابزارهای به‌روز می‌نماید[4]. عدم قطعیت‌های فزاینده و محیط سرشار از پیچیدگی این فضا، امنیت و دفاع از داده‌ها و شبکه‌های اطلاع‌رسانی را فراتر از سطح سناریونویسی می‌برد. یکی از مباحث علمی مرتبط با آینده که بر اساس تعریف آژانس امنیت سایبری اروپا در حوزه تهدیدهای سایبری از جایگاه ویژه‌ای برخوردار است، مبحث آینده‌نگاری است. در حال حاضر فناوری‌های مدرن امنیت رایانه برای محافظت از کاربران و زیرساخت‌های حیاتی از مجرمان سایبری مفید هستند، اما آینده‌نگاری سایبری موضوعی برای جلوتر بودن از مجرمان و تهدیدآفرینان سایبری در فضای سرشار از شگفتی آینده به‌شمار می‌آید[5]. چارچوب آینده‌نگاری رویارویی پیش‌فعالانه با تهدیدهای سایبری، می‌تواند منجر به ارتقاء توانمندی بدنه سایبری سازمان‌ها به‌منظور شناسایی، تجزیه‌وتحلیل و دفاع در برابر یا مقابله با حمله‌های سایبری احتمالی آینده باشد. در واقع استفاده از آینده‌نگاری در حوزه امنیت سایبری می‌تواند به شناخت دقیق‌تر و واضح‌تر کلان روندها، چالش‌ها و تهدیدهای آینده

---

1 - Cyber Terrorism

2 - Cyber Espionage

۳ - آقایی، محسن. معینی، علی. عرب سرخی، ابوذر. محمدیان، ایوب. و زارعی، علی اصغر. (۱۳۹۸). ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی، امنیت ملی، ۹(۳۲)، صص ۲۰۱-۲۳۱.

۴ - بصیری کجانی، محسن. (۱۴۰۰)، طراحی استراتژی دفاعی در برابر حمله‌ها سایبری و فیزیکی-سایبری در سیستم قدرت، رساله دکتری، دانشکده فنی و مهندسی، دانشگاه اصفهان.

5 - Enisa, (2021), Foresight Challenges (A Study to enable foresight on emerging and future cybersecurity challenges), The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary.

این حوزه کمک نموده و ماهیت چند رشته‌ای بودن آن نیز به بررسی دقیق‌تر پیامدهای ناشی از تهدیدهای سایبری بیانجامد.

مأموریت آینده‌نگاری را می‌توان ایجاد تعهد میان ذی‌نفعان داخلی (کلیه کارکنان در اجرای برونداد آینده‌نگاری)، تولید گزینه‌های راهبردی بیشتر، کمک به ژرف‌نگری در پویش محیطی سرشار از عدم قطعیت، نگاه میان‌رشته‌ای با دخالت افراد بیشتر، یادگیری، ایجاد گفتگوی راهبردی، ایجاد چشم‌انداز مشترک، پیوند با برنامه‌ریزی، پرهیز از جهت‌گیری و گرایش به یک پیش‌فرض غالب و کشف آینده‌های بدیل متنوع بر اثر دخالت تصاویر ذهنی ذی‌نفعان مختلف در نظر گرفت[1]. در نظر داشته باشیم که آینده از بر هم کنش چهار مؤلفه‌ی رویدادها[2]، روندها[3]، تصویرها[4] و اقدام‌ها[5] پدید می‌آید و می‌توان چهار هدف تصور حوادث ممکن، ارزیابی احتمالات، یافتن حوادث محتمل و در نهایت تصمیم‌گیری در جهت امور ترجیح داده‌شده را برای آینده‌نگاری نام برد. از مزایای بالقوه کاربرد آینده‌نگاری نیز می‌توان توانایی در شناسایی و تفسیر تغییرات محیطی، ارتقاء فرآیند برنامه‌ریزی راهبردی، رشد قابلیت‌های ابتکاری و اجرای تصمیمات راهبردی برشمرد. با افزایش نرخ تغییرات و دگرگونی‌ها، روش‌های برنامه‌ریزی شده امروز که بر پیش‌بینی آینده استوار است، دیگر جوابگوی نیازها نبوده و سایه سنگین عدم‌قطعیت آینده، وضعیتی را به وجود خواهد آورده که پیش‌بینی آینده غیرممکن می‌گردد[6].

در گزارشی تحت عنوان آینده‌نگاری امنیت سایبری که توسط آژانس امنیت سایبری اتحادیه اروپا در سال ۲۰۲۱ منتشر شده، ویژگی‌های مشترکی برای فضای سایبر و

---

۱ - ایجایی، ابراهیم. درویشی سه تلاتی، فرهاد. مینایی، حسین. فضلی، صفر. و کشاورز، عین‌اله. (۱۳۹۷). طراحی چارچوب آینده‌نگاری راهبردی فناوری‌های دفاعی در حوزه پدافند هوایی به روش مدل‌سازی ساختاری- تفسیری. رساله دکتری، دانشکده علوم اجتماعی، دانشگاه امام خمینی (ره) قزوین.

2- Events
3- Trends
4- Images
5- Actions
6- Yuksel, N., Chifchi, H., & Chakir, S. (2017). New Foresight Generation and Framework of Foresight. In 2nd World Conference on Technology, Innovation and Entrepreneurship (pp. 224-233).

تهدیدهای ناشـــی از آن با آینده‌نگاری عنوان گردیده که می‌توان به میان رشـــته‌ای بودن، پوشـــش قلمرو جغرافیایی گســـترده، توانمندی در مدیریت ریســـک و چالش‌های جاری و آینده سازمان‌ها، تأثیرگـذاری شـگرف در توسعه آینده‌های بدیل، پیچیدگی و عدم اطمینان فراینده محیطی در فضایی مملو از عدم قطعیت‌ها اشاره نمود[1].

در عصـر کنونی با پیشـرفت‌های سـریع و تحولات پرشـتاب آینده در حوزه سـایبر و فناوری، فضای نامطمئن و سرشار از فرصت و تهدید پیش روی سازمان‌ها قرار گرفته است. در حوزه امنیت ســـایبری برنامه‌های راهبردی متنوعی می‌توان تنظیم نمود که یکی از این برنامه‌های کلان که در سطح سازمان‌ها می‌تواند توان مجموعه را برای پیش‌بینی، مدیریت و مقابله با تهدیدها و حمله‌های سایبری افزایش دهد، پیامدهای مخرب ناشی از بروز تهدیدها را کاهش داده و بازسازی حوزه‌های آسیب دیده را با کمترین هزینـــه ممکن، میسر سازد، آینده‌نگاری است[2].

لذا تلفیق آینده‌نگاری و امنیت سایبری مستلزم اجرای یک فرایند آینده‌پژوهانه است که در حال حاضـر در بدنه بیشـتر سـازمان‌ها موجود نیسـت، هر چند که در حال حاضـر با اعمال اقدامات امنیتی ســـایبری توان ســـایبری ارگان‌ها با بهره‌گیری از پروتکل‌ها، رویه‌ها و دسـتورالعمل‌های موجود در مواجه با تهدیدهای سـایبری در شـرایط نسـبتاً قابل قبولی قرار دارد، اما با توسعه و تحولات روزافزون فناوری‌ها در بخش سایبر و کاربردهای متنوع آن و احتمال وقوع کلان روندهای ناشناخته در این بخش می‌تواند با شگفتی‌سازهایی همراه شود. لذا نگارنده در نظر دارد با بررســـی مدل‌های مختلف آینده‌نگاری که از مدل هورتون (۱۹۹۵) تا آخرین مدل آینده‌نگاری به نام مدل پریســـکوپ آینده‌نگاری[3] (۲۰۲۱) که در حوزه فناوری مورد اســـتفاده قرار گرفته[4]، به یک چارچوب مطلوب و جامع در حوزه

1- Enisa, (2021), Foresight Challenges (A Study to enable foresight on emerging and future cybersecurity challenges), The European Union Agency for Cybersecurity, https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary.

2 - Ministry of Transport and Infrastructure. (2019). National Cyber Security Strategy171 2016-2019. Ankara. Retrieved from http://www.ubak.gov.tr/.

3 - Foresight Periscope Model

4 - Weber, V. & Toriser, V. C. L. (2021). Strategic Foresight and the EU Cyber Threat Landscape in 2025: a Workshop Report. (DGAP Report, 23). Berlin: Forschungsinstitut der

رویارویی پیش‌فعالانه با تهدیدهای سایبری دست یابد. با توجه به بررسی‌های اولیه، چارچوب موردنظر در سه بخش پیش‌آینده‌نگاری، آینده‌نگاری و پساآینده‌نگاری ترسیم و با بهره‌گیری از توان بالقوه آینده‌پژوهی و آینده‌نگاری که قابل استفاده در حوزه امنیت سایبری است، ضمن شناسایی اجزاء و روابط میان آن، چارچوب نهایی ترسیم و به‌عنوان مبحثی نو و بی‌سابقه در بسط و ترویج می‌یابد.

اهمیت تدوین این کتاب در این است که با توجه به تحولات شگرف و رشد سریع فناوری اطلاعات و ارتباطات، نقش آینده‌پژوهی و آینده‌نگاری در این حوزه اهمیت ویژه‌ای پیدا می‌کند. بررسی‌های پژوهشی در حوزه آینده‌نگاری فناوری نشان می‌دهد که این فرارشته در سالیان اخیر با رشد روزافزون در امور پژوهشی توسط پژوهشگران روبرو بوده، اما به دلیل نوپا بودن آینده‌نگاری در بخش فضای سایبر، پژوهش‌های محدودی در این حوزه به انجام رسیده است.

عدم توجه به گسترش تهدیدهای نوظهور و فناورانه از طرف بازیگران مختلف حوزه سایبر و بهره‌گیری از این فضا برای انجام حمله‌های سایبری، می‌تواند منجر به غافل‌گیری راهبردی شود که با وجود اطلاعات باارزش و حیاتی در بدنه سازمان‌ها و بعضاً امکان دستیابی، خرابکاری، افشاء و سرقت این اطلاعات اهمیت برقراری امنیت سایبری جهت مقابله با این‌گونه تهدیدها را در قالب چارچوب آینده‌نگاری بیش از پیش نمایان می‌کند[1]. بنابراین کتاب حاضر در راستای توسعه فرایندهای آینده‌نگاری و به‌منظور اتخاذ تصمیم‌های راهبردی متناسب با شرایط مملو از پیچیدگی و عدم قطعیت آینده مهم جلوه می‌کند.

- نیازمندی‌ها و ویژگی‌های مورد نیاز سازمان‌ها را به‌منظور شناسایی تهدیدهای سایبری در افق زمانی میان‌مدت (دو تا پنج ساله) تبیین می‌نماید؛

Deutschen Gesellschaft für Auswärtige Politik e.V. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-77209-3.

۱- حقی، مجید. (۱۳۹۸). ارائه مدل مدیریت راهبردی امنیت فضای سایبر بر اساس کلان‌داده‌های فضای سایبر. امنیت ملی، ۹(۳۴)، صص ۲۷۷-۳۰۹.

- بخشی از نگرانی‌ها در حوزه امنیت سایبری را در قلمرو زمانی مدنظر پژوهش برطرف می‌کند؛
- از علوم نوین و روش‌های نوظهور آینده‌پژوهی در سازمان‌ها به‌منظور ارتقاء امنیت سایبری با توجه به کلان روندهای مؤثر بر این حوزه بهره‌برداری می‌کند؛
- می‌تواند تا حدود زیادی موجب افزایش کارایی و اثربخشی مجموعه‌های کاری و اداری مستقر در سازمان‌ها گردد؛
- به راهکاری عملی جهت رویارویی پیش‌فعالانه با توجه به تهدیدهای ناشی از وقوع کلان‌روندهای حوزه سایبر دست خواهد یافت.

ضرورت انجام آن را نیز می‌توان این‌گونه عنوان نمود که تجهیزات محور بودن سازمان‌ها در بخش سامانه‌ها و سخت‌افزارهای به‌کارگرفته شده و در آینده‌ای نه‌چندان دور در بخش نیروی انسانی با به‌کارگیری تجهیزات هوشمند که مبتنی بر فضای سایبر خواهد بود و همچنین وقوع تحولات شگرف و انقلاب‌آفرینی مانند رایانش ابری[1]، اینترنت اشیاء[2]، انقلاب صنعتی چهارم[3]، متاورس[4] و موضوعاتی از این دست که مبتنی بر زمان آینده هستند، ضرورت مطالعات آینده‌پژوهانه در حوزه سایبر را تبیین می‌نماید. بنابر آنچه مطرح شد ضرورت انجام کتاب حاضر را در موارد زیر می‌توان جستجو نمود:

- مغفول ماندن شناسایی مسیرهای نفوذ نفوذگران مخرب در سامانه‌های مبتنی بر سایبر به دلیل عدم شناسایی دقیق و به‌موقع تهدیدهای این حوزه؛
- عدم مواجه پیش‌فعالانه با بروز رخدادهای احتمالی آینده حوزه فضای سایبر در صورت وقوع شگفتی‌سازهای مربوط به بخش فناوری اطلاعات و ارتباطات؛
- ضرورت ارتقاء ساختاری و تجهیزاتی سازمان‌ها متناسب با پیشرفت فناوری‌های فضای سایبر به‌منظور مقابله با تهدیدهای ناشناخته، نوظهور و روزافزون ناشی از بازیگران مختلف در این حوزه.

---

1 - Cloud Computing
2 - Internet of Things
3 - The Fourth Industrial Revolution
4 - Metaverse