Supreme National Defense University Quarterly Journal of Strategic Defense Studies
https://sds.sndu.ac.ir E-ISSN: 2980-8286
Vol. 23, No. 3, Issue. 101, Autumn 2025 **Received:** 2024/06/14 **Accepted:** 2024/09/05
Research paper

A Strategic Model for Cyber Protection of the South Pars Gas Complex Infrastructure

Aref Bali Lashek
Associate Professor, Malek-Ashtar University, Tehran, Iran.
Vahid Riazi
Associate Professor, Army Command and Staff University of the Islamic Republic of Iran, Tehran, Iran.
Gholamreza Bahmannia
Professor, University of Guilan, Rasht, Iran.
Amir Ebrahimi Manesh
Ph.D. Student in Strategic Passive Defense Management, Supreme National Defense University and Strategic Research Center, Tehran, Iran (Corresponding Author).
Email: ebrahimimanesh.amir@gmail.com

Abstract
Critical infrastructures form the backbone of a country's growth, development, and overall resilience. Certain infrastructures play a pivotal role in national interests, and any disruption in their operation, even briefly, can cause significant damage to the economy and national security. These infrastructures provide continuous services essential to societal functioning, and damage or operational disruption can interrupt service delivery, potentially leading to public dissatisfaction and unrest. Among the country's energy assets, the South Pars Gas Complex is of strategic importance, supplying natural gas and condensates nationwide. Due to its critical role and high attractiveness, this complex is exposed to a range of threats, including cyber threats. Addressing these threats is essential for ensuring sustainability, continuity of production, and minimizing vulnerability. The main objective of this research is to develop a strategic model for cyber protection of the South Pars Gas Complex infrastructure. The study employed a descriptive mixed-methods approach, combining descriptive-analytical and survey techniques. Dimensions, components, and sub-components of the proposed model were identified and their relationships analyzed using correlation analysis. The resulting model comprises 1 dimension, 3 components, and 34 sub-components, providing a comprehensive framework for cyber protection of the complex.

Keywords: Infrastructure, Infrastructure Protection, Passive Defense, Cyber Threats, Sustainability, Vulnerability.

فصلنامه مطالعات دفاعی استراتژیک

سال بیست و سوم، شماره سوم (پیاپی ۱۰۱)، پاییز ۱۴۰۴، صص. ۳۲۹-۳۴۶
تاریخ دریافت: ۱۴۰۳/۰۳/۲۵ ـ تاریخ پذیرش: ۱۴۰۳/۰۶/۱۵

مقاله پژوهشی

الگوی راهبردی حفاظت سایبری از زیرساخت‌های مجتمع گاز پارس جنوبی

عارف بالی لاشک
دانشیار دانشگاه مالک اشتر، تهران، ایران
وحید ریاضی
دانشیار دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران، تهران، ایران
غلامرضا بهمن‌نیا
استاد دانشگاه گیلان، رشت، ایران
امیر ابراهیمی‌منش
دانشجوی دکتری مدیریت راهبردی پدافند غیرعامل، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران (نویسنده مسئول)
Email: ebrahimimanesh.amir@gmail.com

چکیده

زیرساخت‌های هر کشور، بستر مهم حیات، رشد و پویایی آن به شمار می‌روند، برخی از زیرساخت‌ها نقشی حیاتی در منافع ملی دارند و به‌عنوان یکی از ارکان مهم پیشرفت، بروز اختلال هرچند کوتاه در عملکرد آن‌ها می‌تواند آسیب‌های جدی به اقتصاد و امنیت ملی کشور وارد نماید. زیرساخت‌ها، جریانی به‌هم‌پیوسته از خدمات و پشتیبانی‌ها را برای تأمین نیازهای اساسی جامعه ارائه می‌دهند و بروز آسیب یا اختلال در عملکرد و کارکرد آن‌ها می‌تواند منجر به قطع خدمات زیرساختی به مردم و جامعه گردد و به‌تبع آن نارضایتی و اعتراضات مردم و آحاد جامعه را به همراه داشته باشد. یکی از دارایی‌های ارزشمند قابل حفاظت در حوزه انرژیِ کشور از منظر پدافند غیرعامل، مجتمع گاز پارس جنوبی بوده و این زیرساخت به‌عنوان یکی از زیرساخت‌های بااهمیت بالای کشور نقش بسیار مهمی در تأمین گاز و به‌تبع آن میعانات گازی کشور ایفا می‌کند به همین دلیل با توجه به جذابیت بالایی که این زیرساخت دارد، در کنار انواع تهدیدات دشمن، یکی از تهدیداتی که می‌تواند این مجموعه عظیم و راهبردی را تحت تأثیر قرار دهد، تهدیدات سایبری خواهد بود. براین اساس محقق به دنبال این سؤال است که «الگوی راهبردی حفاظت سایبری از زیرساخت‌های مجتمع گاز پارس جنوبی چیست؟» روش تحقیق با رویکرد آمیخته تشریحی با استفاده از روش‌های توصیفی-تحلیلی و پیمایشی ابعاد، مؤلفه و زیرمؤلفه‌های الگوی مورد نظر را احصا کرده و روابط بین آن‌ها نیز از روش همبستگی سنجیده شده است. در پایان الگوی مورد نظر، ارائه شده است که دارای ۱ بُعد، ۳ مؤلفه و ۳٤ زیر مؤلفه است. طرح مذکور به‌طور خلاصه کل پژوهش را تشریح می‌نماید.

کلیدواژه‌ها: زیرساخت، حفاظت از زیرساخت، پدافند غیرعامل، تهدید، پایداری، آسیب‌پذیری سایبری

مقدمه

با ظهور و رشد فناوری‌های نوین، فضای سایبر یکی از ارکان اساسی اداره جوامع امروزی به شمار رفته و عرضه بخش بزرگی از خدمات عمومی و سهولت و سرعت انجام کار و امکانات گسترده موجود در آن، سایبر را به مهم‌ترین پهنه فعالیت سرمایه‌های ملی تبدیل نموده است (رسولی،۱۳۹۸: ۲). نخستین و مهم‌ترین تهدید فناوری‌پایه، تهدید سایبری است. بر اساس سند راهبردی پدافند سایبری کشور، احتمال هرگونه رویدادی که قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر یا اشتهار دستگاه متولی سرمایه ملی سایبری یا افراد مرتبط، به‌واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام (تخریب)، افشا، تغییر اطلاعات و ایجاد اختلال یا ممانعت از ارائه خدمات را داشته باشد، تهدید سایبری است (سند راهبردی پدافند سایبری کشور،۱۳۹٤:۲). تهاجمات سایبری و تهدیدات خارجی مانند خرابکاری، نفوذ رایانه‌ای، عملیات اطلاعاتی، شنود، جاسوسی، جنگ الکترونیک و مدیریت هوشمند، علیه تأسیسات، زیرساخت‌های حیاتی و حساس کشورها و زیرساخت‌های اداره امور مردم در حوزه‌هایی اعم از: انرژی، برق و پالایشگاه‌ها (نفت، گاز و پتروشیمی)، بسیار محتمل است (هاشمی‌فشارکی و همکاران،۱۳۹۲: ۲). گاز طبیعی یکی از منابع حیاتی انرژی در آینده است. مزایای زیاد آن شامل نشر پایین گازهای گلخانه‌ای و هزینه‌های سرمایه‌ای نسبتاً کم، آن را در رقابت با دیگر بخش‌های منابع انرژی به‌ویژه برای تسهیلات جدید تولید انرژی قرار داده است. پیش‌بینی‌های جهانی در مورد سطح ذخایر گاز طبیعی نیز نشانه روشنی از نقش مهم و فزاینده آن است که نقش مهمی در رشد تجارت آن تا سال ۲۰۳۵ دارد (عسگری، مهدی و همکاران،۱۳۹۲).

اهمیت حفاظت از زیرساخت‌های مجتمع گاز باعث کمک در ایجاد حلقه‌های اصلی زنجیره تأمین و تولید، ایجاد اشتغال، حفظ و افزایش امنیت،

درآمدزایی و ارزآوری بالا، تأمین‌کننده خوراک اصلی صنایع پائین‌دستی و کمک به همگرایی با سایر شرکت‌های تابعه وزارت نفت و مستقر در پارس جنوبی به‌عنوان موتور محرک اقتصاد کشور است. موارد منبعث از الگوی راهبردی می‌تواند به‌عنوان یک سند بالادستی برای وحدت و یکپارچگی مدیریت باشد.

امروزه با افزایش تراکم و نزدیکی واحدهای صنعتی به همدیگر، عواقب نامطلوب یک حادثه تنها محدود به همان واحد نمی‌شود، بلکه اثرات مخرب آن به واحدهای مجاور یا مناطق مسکونی اطراف نیز می‌تواند گسترش یابد که در صورت عدم تحقق و اجرای این تحقیق، در شرایط اضطراری و بحرانی ممکن است باعث افزایش هزینه، کاهش پایداری ملی در شرایط بحران و کاهش ظرفیت تولید گاز و میعانات گازی گردد.

زیرساخت‌های مورد بررسی در تحقیق حاضر در حوزه فرابخش انرژی، بخش شرکت ملی گاز، زیر بخش مجتمع گاز پارس جنوبی و دارایی پالایشگاه گاز و اجزائی همچون واحدهای عملیاتی، واحدهای پشتیبانی، واحدهای خارج از سایت صنعتی و ... را در برمی‌گیرد. ازآنجایی‌که در ماده ۵ ساختار اجرایی نظام فنی و تخصصی حفاظت از زیرساخت‌های کشور (۱٤۰۲)، به سه سطح راهبردی سیاست‌گذاری، عملیاتی و فنی اشاره شده است؛ این رساله به‌منظور تحدید مسئله خود به سطح ترکیبی عملیاتی و فنی پرداخته است. با توجه به موارد یاد شده در فرایند اقدامات حفاظت از زیرساخت، گام‌هایی متصور است که در این رساله به گام اول (انجام مطالعات) و گام دوم (تجزیه‌وتحلیل و ارائه راهکارها) پرداخته شده است.

۱. پیشینه پژوهش

سعید کافی در رساله خود با عنوان، «تدوین راهبردی پدافند غیرعامل در فضای سایبری زیرساخت‌های حیاتی جمهوری اسلامی ایران» به مواردی اعم از: ارائه

راهبردی پدافند غیرعامل در فضای سایبری زیرساخت‌های حیاتی جمهوری اسلامی ایران، شناسایی قوت‌ها و ضعف‌های زیرساخت‌های حیاتی جمهوری اسلامی ایران در پنج حوزه منابع انسانی، فرایند، فناوری، مکانیسم‌های احراز هویت و سامانه‌های فرماندهی و کنترل با توجه به شاخصه‌های اصلی پدافند غیرعامل و اهداف عالی دفاع سایبری، شناسایی فرصت‌ها و تهدیدات زیرساخت‌های حیاتی جمهوری اسلامی ایران در پنج حوزه منابع انسانی، فرایند، فناوری، مکانیسم‌های احراز هویت و سامانه‌های فرماندهی و کنترل با توجه به شاخصه‌های اصلی پدافند غیرعامل و اهداف عالی دفاع سایبری، احصای شاخص‌های اصلی پدافند غیرعامل و اهداف عالی دفاع سایبری اشاره نموده است (کافی، سعید، ۱۳۹۳).

عباس خیراتی در رساله خود با عنوان: «طرح راهبردی حفاظت از زیرساخت‌های کلیدی کلان‌شهرها در برابر تهدیدات آینده»، عوامل مؤثر در قالب ۱۲ عامل قوت، ۲۵ عامل ضعف، ۹ عامل فرصت و ١٤ عامل تهدید نهایی گردیده و راهبردها نیز در قالب ۸ راهبرد کلان به همراه ٤٧ اقدام اساسی برای تحقق آن‌ها و ۱۱ الزام جهت پیاده‌سازی راهبردها تدوین شده است. اولویت‌بندی راهبردها نشان می‌دهد که راهبرد ارتقای امنیت، تاب‌آوری و پایداری زیرساخت‌های کلیدی شهری از طریق استقرار زیست‌بوم حفاظتی بومی، متمرکز، یکپارچه و هم‌افزا در کلان‌شهرها مبتنی بر تدوین، طراحی، پیاده‌سازی و راهبری طرح‌های عملیاتی پدافندی زیرساختی در قالب اقدامات اساسی مشخص و الزامات پیاده‌سازی آن نقش بسزایی در کاهش آسیب‌پذیری، حفظ آمادگی، مصون‌سازی و امن‌سازی زیرساخت‌های کلیدی کلان‌شهرها در برابر تهدیدات داشته و از اولویت برخوردار است (خیراتی، عباس، ١٤٠١).

رحیم یزدانی چهاربرج در مقاله‌ای با عنوان: «الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران»، ابعاد و

مؤلفه‌های الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی، پس از بررسی مدل‌های بین‌المللی، دستورالعمل‌ها، اصول منتج از تئوری‌ها و کارکردها همراه با بررسی تطبیقی اسناد بالادستی و اسناد راهبردی و ساختار نهادی و طرح‌ها و قوانین حداقل هفت کشور و همچنین از طریق مراجعه به آرای خبرگان در حوزه‌های راهبردی و دفاع و امنیت فضای سایبر، به‌طور منطقی و مفهومی استنباط گردید. پس از تجزیه تحلیل داده‌ها مشخص شد حفاظت از زیرساخت‌های اطلاعاتی حیاتی کشور چهار وجه (عوامل مدیریت امنیت، حکمروایی، حقوقی، عملیات) را دارا است (رحیم یزدانی چهاربرج و همکاران، ۱۳۹۸).

محمود زاده و همکارانش در مقاله‌ای با عنوان: «تدوین راهبردهای امنیت سایبری سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور»، با اشاره به اینکه، زیرساخت‌ها بسترهای مهم حیات، رشد و پویای صنایع و جوامع به شمار می‌آیند و در این میان برخی از زیرساخت‌ها نقشی حیاتی در منافع ملی دارند، نتیجه می‌گیرند که حفاظت از زیرساخت‌ها و تولید محصولات داخلی و بومی‌سازی تدریجی سامانه‌های کنترل صنعتی امری حیاتی بوده و از راهبردهای غیرقابل انکار مقابله با تهدیدات سایبری به شمار می‌رود (محمود زاده و همکاران، ۱۳۹۷).

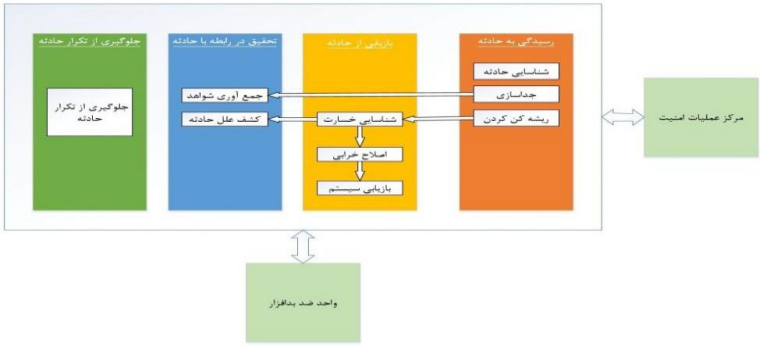
سازمان پدافند غیرعامل و قرارگاه پدافند سایبری در طرحی با عنوان: «طرح پاسخ اضطراری به تهدیدات سایبری در حوزه انرژی»[1]، هدف از ابلاغ سند مذکور را، ارائه چهارچوب و الگوی پاسخ اضطراری به رخدادهای سایبری به‌منظور ارتقای آمادگی برای مقابله با تهدیدات اعم از حمله، نبرد و یا جنگ سایبری برای تداوم کارکردهای ضروری و اساسی حوزه انرژی کشور، کاهش تأثیرات و مدیریت پیامدهای ناشی از این‌گونه رخدادها، معرفی نموده است.

1. Cyber rmergency response plan

قلمروِ این سند، شامل شبکه‌های کنترل صنعتی، سامانه‌های کنترل صنعتی و سامانه‌های فناوری اطلاعات و ارتباطات مربوط به صنایع و زیرساخت‌های حیاتی، حساس و مهم زیرمجموعه وزارت نفت، وزارت نیرو و سازمان انرژی اتمی به‌ویژه برای سامانه‌هایی که با سامانه‌های کنترلی صنایع دیگر ارتباط دارند، است. این سند مهم‌ترین خسارات عمده یا مهم‌ترین پیامدهای عمده رخدادهای سایبری، بـرای سـرمایه‌هـای ملـی سایبری را: ۱. براندازی نظام حاکمیتی یا تهدید فاجعه‌بار امنیت ملی؛ ۲. اختلال گسترده در اداره امور کشور؛ ۳. تخریب یا اختلال گسترده در عملکرد سرمایه‌های ملی سایبری برشمرده است.

در این سند، سطح هشدار سایبری به چهار سطح (سفید، زرد، نارنجی و قرمز) تقسیم‌بندی شده که برای هر یک از آن‌ها با توجه به منشأ تهدید اعم از مجرمین سازمان‌یافته، مزدوران سایبری، هکرها، نویسندگان جاسوس‌افزار و بدافزار و پیامدهای تهدید سایبری نظیر نابودی یا تخریب اطلاعات، دسترسی غیرمجاز به اطلاعات، افشای اطلاعات، دستکاری و ممانعت از سرویس، مطالبی عنوان شده است (قرارگاه پدافند سایبری کشور، ۱۳۹۸).

مرکز امنیت فضای تبادل اطلاعات (افتا) کشور، در طرحی با عنوان: «طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری»، الزامات آن را، کنترل‌های حداقلی به‌منظور کاهش مخاطرات دارای اولویت در زیرساخت‌ها دانسته و هدف از مدیریت حوادث سایبری را، کنترل و به حداقل رساندن خسارت، حفاظت از شواهد، بازیابی سریع و مؤثر سیستم‌ها، جلوگیری از تکرار حوادث مشابه و به دست آوردن دید مناسب نسبت به تهدیدات علیه یک زیرساخت، تعریف نموده است (سازمان پدافند غیرعامل و مرکز امنیت و فضای تبادل اطلاعات کشور، ۱۳۹۸).



نمودار ۱: مؤلفه فرایند در مدیریت حوادث سایبری

(مرکز امنیت فضای تبادل اطلاعات،۱۳۹۸)

۲. مفهوم‌شناسی

پیشرفت فناوری هم فرصت‌آفرین است و هم تهدیدآفرین؛ بنابراین باید با نگاهی هوشمندانه و عاقلانه با این مقوله مواجه شد. هر فناوری، یک برتری و قدرت برای صاحب فناوری ایجاد می‌کند که از این طریق می‌تواند کشور هدف را مورد پایش و کنترل قرار دهد؛ اما برای کشور هدف تهدید محسوب می‌شود. فناوری‌ها معمولاً چهار بُعد اساسی دارند (مطالعات گروهی،۱۳۹٤: ۵۷):

- فن‌افزار (سخت‌افزار): تمام امکانات فیزیکی لازم برای انجام عملیات، مثل ماشین‌آلات، ابزار تولید یا وسایلی که فناوری در آن‌ها جا گرفته است و ... را شامل می‌شود؛
- انسان‌افزار (مغز افزار): مهارت‌ها، تجربیات تولیدی یا فناوری‌های نهفته در انسان‌ها مثل توانایی لازم برای عملیات تولید و مدیریت را در برمی‌گیرد؛
- اطلاع‌افزار (نرم‌افزار): در این حوزه، اطلاعات و دانش فنی نقش محوری ایفا می‌کند؛

- سازمان‌افزار: آن دسته از سازماندهی‌ها و مدیریت تولید و ساختارهایی را در برمی‌گیرد که برای به نتیجه رسیدن فناوری لازم است.

نقش فناوری در حفاظت از زیرساخت: موضوع «فناوری به‌عنوان گلوگاه اصلی حفاظت از زیرساخت» به این معنا است که فناوری مدرن و پیشرفته، نقش اساسی در حفظ و بهینه‌سازی زیرساخت‌ها و تضمین عملکرد مستمر و ایمن آن‌ها دارد. در زیر به تشریح این مفهوم پرداخته می‌شود:

- نظارت و تحلیل داده‌ها: فناوری‌های نوین مانند اینترنت اشیا[1]، حسگرها و تجزیه‌وتحلیل داده‌ها امکان نظارت بر وضعیت زیرساخت‌ها فراهم می‌کنند. این امر کمک می‌کند تا مشکلات پنهان شناسایی و پیش از وقوع بحران حل شوند.
- مدیریت بحران: سیستم‌های فناوری اطلاعات به مدیران امکان می‌دهند تا در مواقع بحران، مانند زلزله یا سیلاب، به‌سرعت واکنش نشان دهند و از طریق شبیه‌سازی و پیش‌بینی شرایط، تصمیمات بهتری اتخاذ کنند.
- خودکارسازی روندها: فناوری‌های خودکارسازی و اتوماسیون در تولید و خدمات به تداوم عملکرد زیرساخت‌ها کمک می‌کنند و احتمال خطاهای انسانی را کاهش می‌دهند.
- پشتیبانی از عملیات ناگهانی: فناوری‌های ارتباطی و اطلاعاتی به سازمان‌ها این امکان را می‌دهند تا در شرایط اضطراری یا غیرمنتظره، به‌سرعت اطلاعات و فرمان‌ها را منتقل کنند.
- توسعه پایدار: فناوری‌های زیست‌محیطی می‌توانند به بهینه‌سازی مصرف انرژی و کاهش ضایعات در زیرساخت‌ها کمک کنند، که در نهایت به پایداری بلندمدت آن‌ها منجر می‌شود.

1. Nternet Of Thing (IOT)

- نوآوری‌های مستمر: با پیشرفت‌هایی در فناوری، دیگر روش‌ها و شیوه‌های قدیمی مدیریت زیرساخت‌ها بهینه می‌شوند و به‌روزرسانی‌ها به سهولت انجام می‌پذیرد.
- امنیت سایبری: با افزایش وابستگی به فناوری، حملات سایبری به زیرساخت‌ها تهدیدی جدی به‌حساب می‌آیند. استفاده از فناوری‌های پیشرفته در امنیت اطلاعات و داده‌های حساس می‌تواند این تهدیدات را مدیریت کند.
- مدیریت ریسک: با استفاده از مدل‌های تحلیلی و شبیه‌سازی، می‌توان ریسک‌های بالقوه را شناسایی و با اتخاذ تدابیر پیشگیرانه از بروز بحران‌های جدی جلوگیری کرد.

در دنیای امروز، زیرساخت‌ها به‌شدت به فناوری وابسته هستند و به همین دلیل، ارتقای فناوری و نوآوری در این حوزه به‌عنوان یک گلوگاه اصلی در حفاظت، مدیریت و تداوم کارکرد زیرساخت‌ها مورد توجه قرار دارد. بهره‌برداری مناسب از فناوری می‌تواند به سازمان‌ها کمک کند تا با چالش‌های موجود در این زمینه مقابله کنند و از آسیب‌ها و خطرات احتمالی جلوگیری نمایند.

الگو: عبارت است از کوشش برای ساده‌تر کردن و آسان‌تر فهماندن واقعیت از طریق تنظیم عناصر و وارد کردن نظمی در آن‌ها؛ مثلاً می‌توان طرح منطقی روابطی را که بین برخی از عناصر یک سیستم وجود دارد، به شکل یک پیکره درآورد (توسلی، ۱۳۸۰: ۱٤۲).

راهبرد: راهبرد، ثمره اندیشه و عمل ذهنی فرماندهان و مبنای اقدامات اجرایی آینده، جهت تحقق اهداف است. راهبرد، مسیر و جهت سازمان برای دستیابی به اهداف است. راهبرد به فرماندهان و مدیران نشان می‌دهد که بهترین راه برای رسیدن به اهداف کدام است (شهلایی، ۱۳۸۸: ۷۳).

الگوی راهبردی: الگوی راهبردی نمونه‌ای ذهنی و انسجام یافته از اجزا و عناصر تشکیل‌دهنده یک پدیده راهبردی و چگونگی روابط اجزا با یکدیگر است (سلمانی به نقل از گروه مطالعاتی چهارم پدافند غیرعامل، ۱۳۹٤: ۱۹).

زیرساخت[1]: عبارت است از مجموعه‌ای از مراکز و تأسیسات زیربنایی و شریان‌های عمده که خدمات و نیازهای ضروری و اساسی کشور را به مردم و جامعه ارائه می‌کند (طرح راهبردی حفاظت از زیرساخت‌های کشور، ۱٤۰۱).

حفاظت از زیرساخت[2]: مجموعه تدابیر و اقدامات پدافند غیرعاملی که توانایی و آمادگی عملیاتی زیرساخت و تداوم کارکرد آن و دستگاه‌های اجرایی مسئول برای پاسخ مؤثر به حوادث ناشی از تهدیدات نظامی، امنیتی، سایبری زیرساختی و تهدیدات از درون دشمن پایه را افزایش می‌دهد به‌طوری‌که فعالیت آن حفظ گردیده و خسارات انسانی و مادی ناشی از آن را به حداقل می‌رساند.

تهدید سایبری[3]: سایبر پیشوندی است برای توصیف یک شخص، یک شیء، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است (جلالی، ۱۳۹۰:۱۱). حمله سایبر، به معنی استفاده از کامپیوترها و فضای تبادل اطلاعات به‌عنوان یک اسلحه یا به‌عنوان ابزاری برای انجام کارهای خشونت‌بار جهت ترساندن، تغییر و یا نابودی یک گروه یا کشور است. اهداف نظامی، خدمات اجتماعی، سامانه‌های نقل‌وانتقال، مخابرات، نیرو، انرژی و هر زیرساخت حیاتی می‌تواند هدف این حملات بوده و امنیت، ایمنی و پایداری آن به خطر افتد (بیطرفان،۱۷۲:۱۳۹۰).

تهدیدات حوزه نرم‌افزار و سایبری: فنون متعددی در جنگ سایبری وجود دارد که در دو بخش نرم‌افزار و سخت‌افزار قابل‌اجرا هستند. هرکدام از بخش‌ها

1. Infrastructure
2. Infrastructure Protection (IP)
3. Cyber Threat

بیانگر نوع خاصی از فضا و جنگ سایبری است. در این رویکرد دایره اثرگذاری و کارکرد نرم‌افزار و سخت‌افزار جنگ‌های سایبری متفاوت است (عبدالله خانی،۱۳۹۱: ۱۳۷ – ۱۶۰).

جدول ۱: تعاریف و مفاهیم اساسی حوزه‌های سایبری از دیدگاه سند راهبردی پدافند سایبری کشور

ردیف	عنوان	تعریف
۱	فضای سایبری	شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده (جاگذاری‌شده)، کنترلگرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات است. این فضا، ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد.
۲	سرمایه ملی سایبری	یک زیرساخت حیاتی (یا حساس) کشور، یک سامانه حیاتی (یا کلیدی) سایبری و یا اطلاعات حیاتی (یا کلیدی) یا افراد متعلق به کشور و برخوردار از شرایط ذیل: - دارای سطح اهمیت حیاتی یا حساس؛ - دارای کارکرد ملی (فرا استانی)؛ - برخوردار از اداره متمرکز (اداره زیرساخت، از مرکز کشور انجام می‌گیرد)؛ - برخوردار از حوزه عملکرد تخصصی؛ - برخوردار از قابلیت تأثیرگذاری بر امنیت ملی، اقتصاد ملی؛ - سلامت و ایمنی عمومی، اطمینان عمومی و باورهای دینی و ملی.
۳	آسیب‌پذیری سایبری	آسیب‌پذیری، به ضعف موجود در داخل یک سرمایه، رویه‌های امنیتی یا کنترل‌های داخلی، یا پیاده‌سازی آن سرمایه ملی سایبری که قابلیت بهره‌برداری یا فعال شدن توسط تهدیدات داخلی و خارجی به‌منظور انجام جنگ سایبری را داشته باشد، اطلاق می‌گردد.

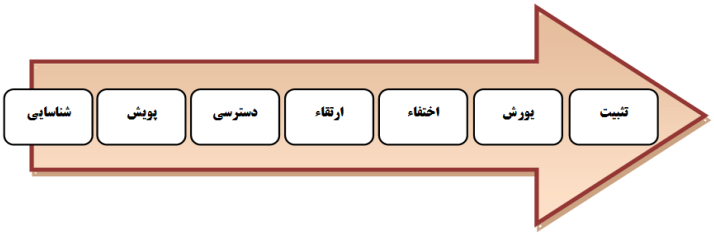
ردیف	عنوان	تعریف
۴	تهدیدات سایبری	هر رویداد یا واقعه باقابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر (پنداره) یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا پرسنل دستگاه به‌واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام (تخریب)، افشا، تغییر اطلاعات و یا ممانعت از ایجاد اختلال در ارائه خدمت.
۵	سطح تهدیدات سایبری	تهدیدات سایبری، قادر به تأثیرگذاری بر سرمایه‌های ملی سایبری، در سطوح فراملی، ملی، دستگاهی، استانی، منطقه حیاتی و حساس و زیرساختی هستند.
۶	احتمال وقوع تهدیدات سایبری	قابل طبقه‌بندی در سطوح: خیلی زیاد (قریب‌الوقوع)، زیاد (محتمل)، کم (غیرمحتمل) و خیلی کم (خیلی غیرمحتمل) هستند.
۷	شدت تهدید سایبری	تهدیدات سایبری علیه سرمایه‌های ملی سایبری، در پنج سطح: خیلی زیاد (فاجعه)، زیاد (بحران)، متوسط (حادثه امنیتی عمده)، کم (حادثه امنیتی) و خیلی کم (رویداد امنیتی) طبقه‌بندی می‌گردند.
۸	تهاجم سایبری	به هرگونه اقدام غیرمجاز سایبری که با هدف نقض سیاست امنیتی یک سرمایه سایبری و ایجاد خرابی یا خسارت، ایجاد اختلال در عملکرد یا از کار اندازی خدمات و یا دستیابی به اطلاعات سرمایه ملی سایبری مذکور انجام گیرد، تهاجم سایبری اطلاق می‌گردد. همچنین استفاده عمدی از یک سلاح سایبری علیه یک سامانه اطلاعاتی، به شکلی که موجب بروز یک حادثه سایبری شود نیز تهاجم سایبری تلقی می‌شود. تهاجم‌های سایبری شاخص عبارت هستند از جرائم سایبری سازمان‌یافته، عملیات شناسایی برای تهاجم سایبری، مبارزه (ستیز- نزاع) سایبری و جنگ سایبری.

ردیف	عنوان	تعریف
۹	سلاح سایبری	سامانه سایبری است که برای وارد نمودن خسارت (تخریب) به ساختار یا عملیات سامانه‌های سایبری دیگر، طراحی و تولید شده باشد. این سامانه‌ها، شامل بمب‌های منطقی، افزارهای بهره‌برداری از آسیب‌پذیری سایبری، انواع بدافزارها و سامانه‌های تولید ترافیک حملات ممانعت از سرویس و ممانعت از سرویس توزیع شده هستند که برای انجام تهاجم‌های سایبری، مورد استفاده قرار می‌گیرند. سلاح‌های سایبری به دو دسته اصلی سلاح‌های رها شده در شبکه و سلاح‌های سایبری برخوردار از کنترل آتش انسانی طبقه‌بندی می‌شوند.
۱۰	جنگ سایبری	بالاترین سطح و پیچیده‌ترین نوع از تهاجم سایبری (عملیات سایبری) است که علیه منافع ملی سایبری کشورها انجام شده و شدیدترین پیامدها را به همراه خواهد داشت. ویژگی‌های این نوع از تهاجم‌های سایبری، برای آنکه دولت‌ها آن‌ها را جنگ علیه منافع ملی خود تلقی نمایند.
۱۱	منشأ جنگ سایبری	نیروی سایبری کشور مهاجم یا گروه‌های سازماندهی‌شده تحت دولت‌های متخاصم، سلاح‌های سایبری تحت کنترل یا رها شده توسط این نیروها
۱۲	پیامدهای جنگ سایبری	- براندازی نظام حاکمیتی یا تهدید فاجعه‌بار امنیت ملی؛ - آغاز هم‌زمان جنگ فیزیکی یا زمینه‌سازی و تسهیل شروع جنگ فیزیکی در آینده نزدیک؛ - تخریب یا صدمه فاجعه‌بار به وجهه کشور در سطح بین‌المللی؛ - تخریب یا صدمه فاجعه‌بار به روابط سیاسی و اقتصادی کشور؛ - تلفات انسانی یا مخاطره گسترده برای سلامت و ایمنی عمومی (از طریق ایجاد آلودگی هسته‌ای، شیمیایی یا بیولوژیک)؛ - هرج‌ومرج و شورش داخلی؛ - اختلال گسترده در اداره امور کشور؛ - تخریب و صدمه گسترده به اطمینان عمومی یا باورهای دینی، ملی و قومی؛ - خسارت شدید به (یا اختلال گسترده در) اقتصاد ملی؛ - تخریب یا اختلال گسترده در عملکرد سرمایه‌های ملی سایبری.

ردیف	عنوان	تعریف
۱۳	سناریوهای جنگ سایبری	سناریو اول: جاسوسی سایبری با حمایت دولت‌ها با هدف جمع‌آوری اطلاعات برای برنامه‌ریزی تهاجم‌های سایبری بعدی. سناریو دوم: یورش سایبری با هدف بسترسازی برای هرج‌ومرج و شورش مردمی. سناریو سوم: یورش سایبری با هدف از کاراندازی تجهیزات و تسهیل تهاجم فیزیکی. سناریو چهارم: یورش (تهاجم) سایبری به‌عنوان مکمل تهاجم فیزیکی. سناریو پنجم: یورش (تهاجم) سایبری با هدف تخریب یا اختلال گسترده به‌عنوان هدف نهایی جنگ سایبری
۱۴	پدافند سایبری	بهره‌گیری از کلیه امکانات غیرمسلحانه سایبری و غیرسایبری کشور، به‌منظور ایجاد بازدارندگی، پیشگیری، ممانعت از انجام، تشخیص به‌موقع، مقابله مؤثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری جمهوری اسلامی ایران، توسط متخاصمین سایبری، اعم از نیروی نظامی (ارتش سایبری) کشورهای متخاصم و گروه‌های تحت حمایت پنهان دولت‌های متخاصم به‌نحوی‌که امکان تهاجم سایبری را از کلیه متخاصمین سلب نماید.
۱۵	زیست‌بوم سایبری	زیست‌بوم به ارتباط متقابل بین موجود زنده و محیط آن اطلاق می‌شود. زیست‌بوم سایبری به شکل‌گیری محیطی بومی، پویا و زنده سایبری اشاره دارد که برای کشور در عرصه‌های مختلف حمایتگر و پشتیبانی‌کننده خواهد بود.
۱۶	موقعیت تدافعی خفیف	سازمان‌هایی که در موقعیت تدافعی خفیف هستند برخی از ویژگی‌های سازمان‌های تدافعی را در مراتب پایین‌تر دارند. ویژگی‌های این سازمان‌ها در حوزه نیروی انسانی، تکنیکی بودن، مأمور و معذور بودن است. افراد متکی به اهداف فردی هستند. در مدیریت و برنامه‌ریزی مبنای کار بودجه‌بندی است. این سازمان‌ها نامنسجم (غیر یکپارچه) و الگوی کنترل در آن‌ها پس کنترل است. این سازمان‌ها در سیطره عوامل محیط هستند و تصمیم‌سازی در آن‌ها مبتنی بر اخبار است.

ردیف	عنوان	تعریف
۱۷	موقعیت تهاجمی خفیف	سازمان‌هایی که در موقعیت تهاجمی خفیف هستند برخی از ویژگی‌های سازمان‌های تهاجمی را در مراتب پایین‌تر دارند. این سازمان‌ها نتیجه‌گرا هستند. هماهنگی در سطوح تکنیکی، تاکتیکی و عملیاتی وجود دارد. الگوی عمومی مدیریت و برنامه‌ریزی مدیریت استراتژیک است. هم‌راستایی اهداف اعضا، سازمان و جامعه را داریم. مدیریت محیط در این سازمان‌ها مدیریت محیط زمینه‌ای است. این سازمان‌ها درگیر مسائل و مشکلات هستند.

فرایند حمله سایبری: فرایند حمله سایبری معمولاً بر روی یک سامانه یا مجموعه از سامانه‌های هدف متمرکز می‌شود. فرایند همان‌طور که در شکل زیر نشان داده شده است، معمولاً عملیات شناسایی و پویش[1] به‌منظور استخراج اطلاعات لازم از سامانه هدف انجام می‌شود.



شکل ۱: فرایند حمله سایبری

الگوی راهبردی حفاظت از زیرساخت مجتمع گاز پارس جنوبی: عبارت است از مجموعه‌ای از عوامل نظام‌مند مؤثر بر حفاظت از زیرساخت‌های مجتمع گاز پارس جنوبی با رویکرد پدافند غیرعامل که روابط، نسبت‌های آن‌ها، برشماری و تأکید بر تهدیدات بر مبنای اسناد بالادستی و سیاست‌های کلی نظام در امور پدافند غیرعامل و ابلاغی مقام معظم رهبری(مدظله‌العالی) ترسیم می‌کند همچنین با

1. Scanning

در نظر گرفتن عوامل محیطی، دارایی‌ها و آسیب‌پذیری‌های زیرساخت‌های مجتمع گاز پارس جنوبی ابعاد، مؤلفه‌ها، زیرمؤلفه‌های آن‌ها را مشخص می‌سازد.

۳. چهارچوب نظری

در این تحقیق مطالعات تطبیقی و اقدامات انجام شده در حوزه حفاظت از زیرساخت‌های کشورهای آمریکا، استرالیا، سوئیس، قطر و روسیه در حوزه عملیاتی، پشتیبانی و مدیریتی مورد بررسی قرار گرفت و مفاهیم مورد نیاز در تحقیق احصا گردید.

٤. روش‌شناسی

رویکرد این تحقیق آمیخته با استفاده از روش‌های توصیفی-تحلیلی و پیمایشی مؤلفه و زیرمؤلفه‌های الگوی مورد نظر احصا و روابط بین آن‌ها از روش همبستگی سنجیده شده است. همچنین جامعه آماری تحقیق ٤٥ نفر بوده و در این تحقیق از روش‌های گردآوری کتابخانه‌ای (پرسش‌نامه و ترکیبی و ابزار فیش‌برداری و سایت‌های علمی) و میدانی (مصاحبه، پرسش‌نامه و ترکیبی) استفاده شد.

٥. تجزیه‌وتحلیل داده‌ها و یافته‌های تحقیق

تجزیه‌وتحلیل اطلاعات که از مهم‌ترین و اصلی‌ترین قسمت‌های تحقیق است و در آن داده‌های خام با استفاده از نرم‌افزارها و فنون آماری مورد تجزیه‌وتحلیل قرار می‌گیرند و پس از پردازش به شکل اطلاعات در اختیار دیگران گذاشته می‌شود. برای تجزیه‌وتحلیل داده‌های جمع‌آوری شده از آمار توصیفی و استنباطی جهت تشریح و تبیین پاسخ‌های داده شده به سؤالات، استفاده گردیده

است. آزمون‌های مدل اندازه‌گیری انعکاسی مربوط به حفاظت سایبری از زیرساخت‌های مجتمع گاز پارس جنوبی مورد بررسی قرار گرفت، مدل اندازه‌گیری انعکاسی در قالب فرایند تحلیل عاملی تأییدی بر اساس روایی، پایایی و کیفیت‌سنجی مورد آزمون قرار گرفته و در صورت لزوم اصلاحات مورد نظر روی آن اعمال می‌گردد. سپس آزمون همگن بودن مورد بررسی قرار گرفته است. سپس آزمون پایایی مدل شامل آلفای کرونباخ، پایایی ترکیبی، پایایی اشتراکی انجام شد که نتایج مبین تایید پایایی مدل بود و در ادامه آزمون روایی (میانگین واریانس استخراجی) الگو انجام و نتایج تایید گردید.

جدول ۲: آزمون میانگین واریانس استخراجی

	Composite Reliability	Average Variance Extracted (AVE)
الگوی راهبردی حفاظت سایبری از زیرساخت‌های مجتمع گاز پارس جنوبی	0/987	0/536
سایبری	0/920	0/508
زیرساخت‌های خارج از سایت	0/957	0/754
زیرساخت‌های عملیاتی	0/920	0/670
زیرساخت‌های پشتیبانی	0/981	0/656

در ادامه آزمون مدل ساختاری به‌منظور بررسی روابط بین متغیرهای مکنون انجام و برابر جدول ذیل تمامی روابط تأیید شده‌اند.

جدول ۳: آزمون مدل ساختاری

نتیجه	پی ولیو[3]	تی ولیو[2]	ضرایب مسیر[1]	
تأیید	۰/۰۰۰	۱۷۳/۷۰۷	۰/۹۳۶	الگوی راهبردی حفاظت سایبری از زیرساخت‌های مجتمع گاز پارس جنوبی -> سایبری
تأیید	۰/۰۰۰	۵۱/۰۷۶	۰/۷۹۹	سایبری -> زیرساخت‌های خارج از سایت
تأیید	۰/۰۰۰	۱۰۶/۰۳۳	۰/۸۸۲	سایبری -> زیرساخت‌های عملیاتی
تأیید	۰/۰۰۰	۷۳۶/۰۸۲	۰/۹۸۳	سایبری -> زیرساخت‌های پشتیبانی

در نهایت آزمون کلی مدل PLS انجام شد و طی آن آزمون ریشه میانگین‌های مجذورهای خطاهای باقی‌مانده[4] انجام شد که بر اساس این آزمون اگر SRMR کوچک‌تر از ۰/۰۸ باشد بنابراین مدل کلی PLS برازش مناسبی دارد یعنی با مدل مورد نظر در جامعه تطابق دارد.

جدول ٤: آزمون SRMR

	Estimated Model
SRMR	0.062

بر اساس آزمون‌های انجام شده، مؤلفه‌ها و زیرمؤلفه‌های حفاظت از زیرساخت‌های مجتمع گاز پارس جنوبی تأیید گردیدند که در بُعد سایبری شامل ۳ مؤلفه و ۳٤ زیرمؤلفه به شرح زیر هستند و به ترتیب اولویت در جدول زیر ارائه گردیده است.

1. Original Sample
2. T Statistics (|O/STDEV|)
3. P Values
4. SRMR

جدول ۵: مؤلفه‌ها و زیرمؤلفه‌های حفاظت از زیرساخت‌های مجتمع گاز پارس جنوبی

بُعد سایبری			
ردیف	مؤلفه پشتیبانی	مؤلفه عملیاتی	مؤلفه خارج از سایت
۱	واحد نیروگاه برق (واحد ۱۲۰)	واحد تثبیت میعانات گازی (واحد ۱۰۳)	واحد آبگیر (واحد ۱۲۵)
۲	پست‌های برق (یک تا ده)	واحد صادرات گاز (واحد ۱۰۶)	اتاق کنترل مرکزی (CCR)
۳	پست‌های ابزار دقیق (صفر تا هفت)	واحد نم‌زدایی از گاز (واحد ۱۰۴)	ساختمان مخابرات و شبکه (TER)
۴	واحد Sour water Stripper(واحد ۱۰۹)	واحد احیاء گلایکول (واحد ۱۰۲)	واحد ذخیره‌سازی میعانات گازی (واحد ۱۴۳)
۵	واحد آب‌شیرین‌کن (واحد ۱۲۶)	واحد سیلابه گیر (واحد ۱۰۰)	کریدورهای مرتبط با خوراک ورودی پالایشگاه
۶	واحد مخازن دفنی (واحد ۱۴۱)	واحد سرمایش پروپان (واحد ۱۰۷)	واحد مشعل (واحد ۱۴۰)
۷	واحد تولید هوا (۱۲۳)	واحد مرکاپتان‌زدایی (واحد ۱۱۴)	ساختمان مانیتورینگ
۸	واحد ذخیره‌سازی مواد شیمیایی (واحد ۱۴۶)	واحد شیرین سازی گاز (واحد ۱۰۱)	
۹	واحد تولید نیتروژن (واحد ۱۲۴)	واحد تنظیم نقطه شبنم گاز (واحد ۱۰۵)	

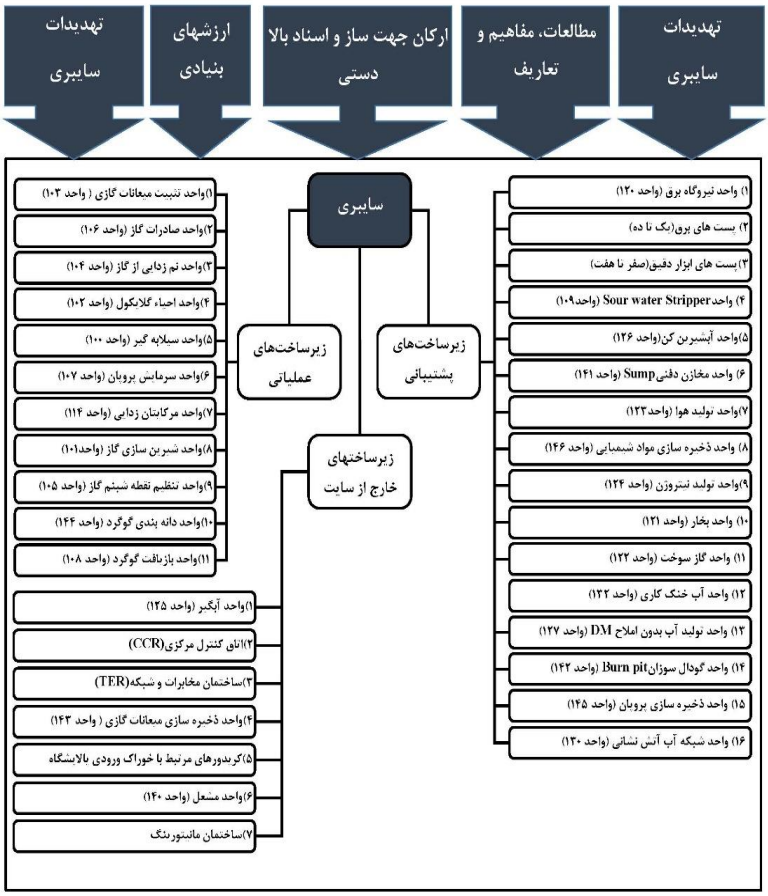
۱۰	واحد بخار (واحد ۱۲۱)	واحد دانه‌بندی گوگرد (واحد ۱۴۴)	
۱۱	واحد گاز سوخت (واحد ۱۲۲)	واحد بازیافت گوگرد (واحد ۱۰۸)	
۱۲	واحد آب‌خنک کاری (واحد ۱۳۲)		
۱۳	واحد تولید آب بدون املاح DM(واحد ۱۲۷)		
۱۴	واحد گودال سوزان Burn pit(واحد ۱۴۲)		
۱۵	واحد ذخیره‌سازی پروپان (واحد ۱۴۵)		
۱۶	واحد شبکه آب آتش‌نشانی (واحد ۱۳۰)		

نتیجه‌گیری و پیشنهاد

با عنایت به روند رشد روزافزون تهدیدات دشمن علیه کشور و میهن عزیز و اسلامی ما و بررسی تجربیات جنگ‌های اخیر و محتمل بودن تهدیدات متنوع علیه سرمایه‌های ملی و با امعان نظر نسبت به راهبرد دشمن در انهدام مراکز ثقل، پُرواضح است که یکی از اهداف مهم در حملات و جنگ‌های آینده، انهدام و یا اخلال در عملکرد و فرایند تولید و ذخیره‌سازی گاز و میعانات گازی در پالایشگاه‌های گاز خواهد بود. با توجه به نقش راهبردی که پالایشگاه‌های گاز به‌ویژه مجتمع گاز پارس جنوبی با ۱۳ پالایشگاه، نقش تولید بالغ بر ۷۵ درصد

گاز مورد نیاز کشور را بر عهده دارد؛ بنابراین حفاظت، صیانت و مصون‌سازی زیرساخت‌های مجتمع گاز از طریق اعمال الزامات و ملاحظات فنی و مهندسی و زیر بنایی با رویکرد سایبری و پیاده‌سازی الزامات و ملاحظات مرتبط با این حوزه سبب ناکامی دشمن در نیل به اهداف خصمانه او خواهد شد.

این تحقیق به دنبال ارائه الگوی راهبردی حفاظت سایبری از زیرساخت‌های مجتمع گاز پارس جنوبی بوده است. بدین منظور در این راستا تحقیق حاضر از طریق پاسخ‌گویی به سؤالات چندگانه زیر تلاش نمود تا ضمن تولید ادبیات جدیدی از مبحث پدافند غیرعامل در قالب حفاظت از زیرساخت‌های مجتمع گاز پارس جنوبی در برابر تهدیدات سایبری، علاوه بر ایجاد هم‌افزایی، هماهنگی و درک مشترکی از موضوع حفاظت از زیرساخت‌ها ایجاد نماید. ابعاد، مؤلفه‌ها و زیرمؤلفه‌های الگوی راهبردی حفاظت سایبری از زیرساخت‌های مجتمع گاز پارس جنوبی پس از بررسی تحقیقات، مدل‌ها، برنامه‌ها و دستورالعمل‌های بین‌المللی و با بررسی تطبیقی اسناد بالادستی، اسناد راهبردی و اقدامات انجام شده در کشورهای آمریکا، استرالیا، سوئیس، قطر، روسیه در حوزه حفاظت از زیرساخت و همچنین مراجعه به آرای نخبگان و صاحب‌نظران در حوزه پژوهش به‌طور منطقی و مفهومی استنباط و در نهایت الگوی راهبردی حفاظت از زیرساخت‌های مجتمع گاز پارس جنوبی استخراج گردید.



شکل ۲: الگوی راهبردی حفاظت سایبری از زیرساخت‌های مجتمع گاز پارس جنوبی

پیشنهادها

❖ پیشنهادهای تحقیقاتی

۱. با توجه به اینکه تهدیدات حوزه حفاظت از زیرساخت‌ها پویا بوده و دائماً در حال تغییر هستند؛ لازم است به‌طور مستمر این تهدیدات مورد رصد و پایش قرارگرفته و بر اساس تهدیدات جدید، راهکارهای متناسب به‌منظور مقابله با آن تهدیدات مورد بازنگری قرار گیرند.

۲. با توجه به گسترش و محدوده وسیع حوزه حفاظت سایبری از زیرساخت‌های مرتبط با انرژی و به‌ویژه در سطح وزارت نفت، در تحقیقات آتی به بخش‌های دیگر وزارت نفت به‌صورت محدودتر و مشخص‌تر و تخصصی‌تر در حوزه حفاظت از زیرساخت‌ها پرداخته شود. مانند طراحی الگوی راهبردی حفاظت از زیرساخت‌های شرکت نفت و گاز پارس، طراحی الگوی راهبردی حفاظت از زیرساخت‌های شرکت پخش و پالایش نفت و ... .

۳. دانشگاه‌های معین پدافند غیرعامل در کشور به‌منظور دستیابی به نتایج بهتر و مؤثرتر در ارتقای دانش فنی حوزه حفاظت از زیرساخت، از این تحقیق در قالب محتوای آموزشی برای تدریس در دوره‌های تحصیلات تکمیلی رشته پدافند غیرعامل استفاده نمایند.

٤. دانشگاه عالی دفاع ملی رساله‌ای در خصوص آمایش زیرساخت‌های کشور با رویکرد حفاظت سایبری از زیرساخت‌ها در برابر تهدیدات در دستور کار قرار دهد.

❖ پیشنهادهای اجرایی

۱. تمرکز بر ارتقای قابلیت‌های شرکت‌های مشاور، مجری و ناظر و دانشگاه‌ها و بهره‌گیری از این ظرفیت‌ها و تخصصی نمودن

گواهینامه‌های صلاحیت حرفه‌ای مشاور ذیصلاح در حوزه حفاظت از زیرساخت‌ها از سوی سازمان پدافند غیرعامل کشور.

۲. معاونت پژوهش و فناوری وزارت نفت این تحقیق را با مقداری اصلاحات به‌عنوان یک سند لازم‌الاجرا جهت تهیه و تدوین طرح حفاظت از زیرساخت‌های حوزه وزارت نفت مورد استفاده قرار دهد.

❖ پیشنهادات آموزشی

۱. برگزاری دوره‌های آموزشی عرضی و طولی به‌منظور تربیت نیروهای ماهر و کارآزموده.

۲. انجام مانورها و رزمایش‌های آمادگی به‌منظور کسب مهارت، هماهنگی و سازماندهی در مقابله با تهدیدات.

۳. تولید محتوا و ادبیات علمی حوزه حفاظت از زیرساخت‌ها با به‌کارگیری ظرفیت‌های دانشگاهی و پژوهشگاه‌ها.

فهرست منابع

- بی‌نام (۱۳۹٤)، ***سند راهبردی پدافند سایبری کشور***، تهران، سازمان پدافند غیرعامل کشور
- بی‌نام (۱٤۰۱)، ***طرح راهبردی حفاظت از زیرساخت‌های کشور***، تهران، سازمان پدافند غیرعامل کشور
- بی‌نام (۱٤۰۲)، ***نظام فنی و تخصصی حفاظت از زیرساخت‌های کشور***، تهران، سازمان پدافند غیرعامل
- تقی‌پور، رضا؛ لشکریان، حمیدرضا؛ چهاربرج یزدانی، رحیم (۱۳۹۸)، ***الگوی راهبردی حفاظت از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران***، تهران، فصلنامه علمی امنیت ملی، شماره ۳٤
- توسلی، غلام عباس (۱۳۸۰)، ***نظریه‌های جامعه‌شناسی***، تهران: انتشارات سمت.
- جلالی‌فراهانی، غلامرضا (۱۳۹۹)، جزوه آموزشی حفاظت از زیرساخت‌های حیاتی در برابر تهدیدات ترکیبی و هیبریدی، دانشگاه عالی دفاع ملّی.
- خیراتی، عباس (۱٤۰۱)، ***طرح راهبردی حفاظت از زیرساخت‌های کلیدی کلان‌شهرها در برابر تهدیدات آینده***، دانشگاه عالی دفاع ملی.
- شهلایی، ناصر (۱۳۸۷)، ***تئوری‌های استراتژیک پدافند غیرعامل***، تهران، دافوس آجا.
- رسولی، عباس (۱۳۹۸)، ***مفهوم حملات سایبری و راهکارهای مقابله با آن***، تهران: دومین کنفرانس ملی پدافند سایبر.
- سازمان پدافند غیرعامل و مرکز امنیت و فضای تبادل اطلاعات کشور (۱۳۹۸)، طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری.
- عبدالله‌خانی، علی (۱۳۸۵)، ***حفاظت از زیرساخت‌های حیاتی اطلاعاتی***، فصلنامه سیاست دفاعی، سال چهاردهم
- عسگری، مهدی؛ طوسی، اعظم (۱۳۹۳)، ***نگاهی بر نقش گاز طبیعی در آینده انرژی جهان***، تهران: شانا.
- کافی، سعید (۱۳۹۳)، ***تدوین راهبردهای پدافند غیرعامل در فضای سایبری زیرساخت‌های حیاتی جمهوری اسلامی ایران***، تهران: دانشگاه عالی دفاع ملی.

- قرارگاه پدافند سایبری کشور (۱۳۹۸)، طرح پاسخ اضطراری به تهدیدات سایبری در حوزه انرژی.
- مجمع تشخیص مصلحت نظام (مصوب ۱۳۸۶)، ***سیاست‌های کلی نظام در امور پدافند غیرعامل***، ابلاغی امام خامنه‌ای(مدظله‌العالی)
- محمود زاده، ابراهیم؛ حسنی‌اصل، حمیدرضا؛ قوچانی، محمدمهدی؛ نیک‌نفس، علی (۱۳۹۷)، ***تدوین راهبردهای امنیت سایبری سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور***، تهران، فصلنامه علمی پژوهشی مطالعات بین‌رشته‌ای دانش راهبردی.
- مطالعات گروهی دوره چهارم مدیریت راهبردی پدافند غیرعامل (۱۳۹٤)، ***ارائه الگوی راهبردی دفاع دانش‌بنیان برای مقابله با تهدیدات آینده***. تهران: دانشگاه عالی دفاع ملی.
- هاشمی فشارکی، سیدجواد؛ شهردار، شهاب‌الدین (۱۳۹۲)، ***تبیین تهدیدات سایبری در پالایشگاه‌ها از منظر دفاع غیرعامل، تهران***، کنفرانس تبیین تهدیدات سایبری در پالایشگاه ها از منظر دفاع غیرعامل، ششمین کنگره انجمن ژئوپلیتیک ایران پدافند غیرعامل.