

Science and Technology in the Iranian -Islamic Model of Progress with a Strategic Hedging Approach

Mohammad Sadegh Khayatian Yazdi¹

Received: 13/08/2021

Zohreh Rahimi Rad²

Accepted: 17/11/2021

Kiarash Fartash³

Ali Saadabad⁴

Abstract

Due to the rapid growth of the field of information and communication technology, this sector has become one of the potentially vulnerable and dangerous platforms, which confirms the growing importance of passive defense in this field. In this regard, the document of the Islamic-Iranian model of progress as a roadmap for the next 50 years of our country, should be able to provide a clear picture of the desired future of Iran in this area as one of its key parts. Therefore, the present study seeks to document the issues related to information technology in this document by cutting the passive defense in order to pave the way for policy makers. The results of this study showed that this document has not been able to address it at all, considering the importance and challenges facing this field, so that only in its policy number 19 it has made a vague reference to this section, which is due to the cyber threats which will seriously endanger the Iranian Islamic civilization and requires a very serious consideration. Finally, according to the analysis, three measures to fill the gaps are proposed.

Keywords

Iranian Islamic Model of Progress; Science & Technology; Hedging; Strategic.

-
1. Assistant Professor, Department of Science and Technology Policy, Shahid Beheshti University, Tehran, Iran (Corresponding Author), Khayatian@sbu.ac.ir
 2. PhD Science and Technology Policy, Mazandaran University, Mazandaran, Iran, zrahimi.rad@gmail.com
 3. Assistant Professor, Department of Science and Technology Policy, Shahid Beheshti University, Tehran, Iran, k_fartash@sbu.ac.ir
 4. PhD Management, Tehran University, Tehran, Iran, a_sadabadi@ut.ac.ir

علم و فناوری در الگوی اسلامی - ایرانی پیشرفت با رویکرد مصون‌سازی راهبردی در منظومه پدافند غیرعامل

محمدصادق خیاطیان یزدی^۱، زهره رحیمی راد^۲، کیارش فرتاش^۳، علی سعدآباد^۴

تاریخ دریافت: ۱۴۰۰/۰۵/۲۲ تاریخ پذیرش: ۱۴۰۰/۰۸/۲۶

چکیده

با توجه به رشد سریع حوزه فناوری اطلاعات و ارتباطات، این بخش به یکی از بسترهای بالقوه آسیب‌پذیر و خطرناک مبدل شده است که این امر بر اهمیت روزافزون توجه به پدافند غیرعامل در این حوزه صحنه می‌گذارد. در این راستا، سند الگوی اسلامی - ایرانی پیشرفت به‌عنوان نقشه راه ۵۰ سال آینده کشورمان، باید بتواند تصویری واضح از آینده مطلوب ایران در این حوزه به‌عنوان یکی از بخش‌های کلیدی خود ارائه دهد. فلذا مطالعه حاضر در پی آن است که با روش اسنادی، موضوعات مرتبط با فناوری اطلاعات مطرح در این سند را با رویکرد مصون‌سازی راهبردی و بُرش پدافند غیرعاملی مورد ارزیابی قرار دهد تا بتواند راهگشای مسیر سیاست‌گذاران قرار گیرد. نتایج پژوهش حاضر نشان داد این سند اصلاً نتوانسته است با توجه به اهمیت و چالش‌های پیش‌روی این حوزه، به آن بپردازد، به‌گونه‌ای که تنها در تدبیر شماره ۱۹ خود اشاره‌ای مبهم به این بخش داشته است. این امر با توجه به تهدیدات سایبری که به جد تمدن اسلامی - ایرانی را به خطر خواهد انداخت، بسیار جای تأمل دارد. در انتها نیز با توجه به تحلیل صورت‌گرفته سه تدبیر برای رفع خلأهای ارائه‌شده، پیشنهاد شده است.

واژگان کلیدی:

الگوی اسلامی - ایرانی پیشرفت؛ علوم و فناوری؛ مصون‌سازی؛ راهبردی؛ پدافند غیرعامل.

۱. استادیار گروه سیاست‌گذاری علم و فناوری، دانشگاه شهید بهشتی، تهران، ایران (نویسنده مسئول)

khayatian@sbu.ac.ir

۲. دانش‌آموخته دکتری تخصصی سیاست‌گذاری علم و فناوری دانشگاه مازندران، مازندران، ایران

zrahimi.rad@gmail.com

k_fartash@sbu.ac.ir

۳. استادیار گروه سیاست‌گذاری علم و فناوری دانشگاه شهید بهشتی، تهران، ایران

a_sadabadi@ut.ac.ir

۴. دانش‌آموخته دکتری مدیریت، دانشگاه تهران، تهران، ایران

مقدمه

کشور ایران از دیرباز هم در منطقه خاورمیانه و هم در کل جهان از یک موقعیت راهبردی برخوردار بوده است، فلذا همیشه مورد تهاجم کشورهای مختلف قرار داشته است. با تغییر رویکردهای بشر به سمت فناوری اطلاعات، سمت و سوی حرکت انسان به سوی فناوری نوین در فضای مجازی تغییر مسیر یافته است و با توجه به رشد سریع و درعین حال نامتوازن ساختار فناوری اطلاعات، این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در جهان بدل شده است؛ به طوری که در ماهیت تهاجمات نیز تغییراتی پارادایمی رخ نموده است و بدین ترتیب ضرورت توجه و پرداخت سریع و درعین حال معقول به منظور مصون‌سازی این بستر از تهدیدات موجود در جهات حفظ امنیت ملی و حریم شخصی شهروندان در فضای جنگ و مخاصمات امروز بین‌المللی را می‌طلبد (وکیلی و همکاران، ۱۳۹۱). امروزه کشورها نمی‌توانند در معادلات امنیتی و راهبردی خود از نقش فضای سایبری و تأثیر آن بر امنیت غافل شوند به طوری که به اعتقاد بسیاری از متخصصین امروزه جنگ سایبری از مهم‌ترین انواع تهدیدات به‌شمار می‌رود. جنگی که پیروزی در آن جز با دفاع هوشیاری و یاری آحاد ملت و متخصصین میسر نخواهد شد (برون، ۱۳۹۸). در اهمیت این فضا همان بس که به فرموده رهبر انقلاب، فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد. از این رو لازم است که کشورها، تدابیری را برای مقابله با این تهدیدات اتخاذ کنند. در پاسخ به این ضرورت، پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات به منظور امنیت، ایمنی و پایداری زیرساخت‌های حیاتی کشور در مقابل تهدیدهای دشمن از این ناحیه شکل گرفته است.

در این راستا الگوی اسلامی - ایرانی پیشرفت به‌عنوان نقشه راه ۵۰ سال آینده کشورمان، باید بتواند تصویری واضح از آینده مطلوب ایران ارائه داده و در ساختار این آینده فضای مجازی دیده شود، به طوری که اجرای این سند آسیب‌پذیری کشور در

مقابل تهدیدات دشمن را کاهش دهد و موجب تقویت مؤلفه‌های قدرت جمهوری اسلامی ایران گردد، خاصه آن‌که امنیت سایبری در ارتباط مستقیم با امنیت ملی کشور است و اگر حملات سایبری کشوری را تهدید کند، در واقع امنیت ملی کشور را تهدید کرده است، فلذا بازدارندگی سایبری؛ لازمه ادامه فعالیت زیرساخت‌های حیاتی در شرایط کنونی است. اما در حال حاضر بحث فناوری اطلاعات و فضای مجازی به‌جز اشاره‌ای مبهم در یک تدبیر جایگاه به‌خصوصی در این الگو ندارد. در حالی‌که هرگونه نقش‌آفرینی مؤثر و مواجهه فعال و هوشمند با این پدیده، در گرو شناخت ابعاد و زوایای تأثیرگذاری این پدیده بر آینده کشور و خصوصاً امنیت آن است و بدون درک و شناخت هرچه کامل‌تر جایگاه و نحوه مواجهه با آن، نتیجه مطلوب حاصل نخواهد شد. با توجه به آن‌که تهدیدات سایبری، یکی از چند حوزه تخصصی مرتبط با پدافند غیرعامل می‌باشد، فلذا مطالعه حاضر در پی آن است که موضوعات مرتبط با فناوری اطلاعات مطرح در این سند را با برش پدافند غیرعاملی مورد ارزیابی قرار داده و سپس تدابیر اصلاحی و پیشنهادی خود را ارائه دهد.

۱. روش پژوهش

جهت‌گیری اصلی پژوهش حاضر، کاربردی و هدف آن اکتشافی است که با استراتژی مطالعه موردی و به‌کارگیری روش اسنادی به بررسی سند الگوی اسلامی - ایرانی پیشرفت از منظر توجه به فناوری اطلاعات و ارتباطات پرداخته است. روش اسنادی یکی از مهم‌ترین ابزارهای تحقیق، به‌ویژه در تحقیق موردی محسوب می‌شود. روش اسنادی را تحلیل آن دسته از اسنادی می‌دانند که شامل اطلاعات درباره پدیده‌هایی است که قصد مطالعه آن‌ها را داریم (Bailey, 2008). این روش مستلزم جستجوی توصیفی و تفسیری است و پژوهشگر این است که از فهم مقاصد و انگیزه‌های اسناد و متون یا تحلیل‌های تأویلی یک متن خارج شود و آن را به زبان مکتوب و گفتمان نویسنده، پذیرفته و مورد استناد قرار دهد (صادقی و عرفان منش، ۱۳۹۴). بنابراین در

این روش پژوهشگر تلاش می‌کند تا با استفاده از داده‌های اسنادی به کشف، استخراج، طبقه‌بندی و ارزیابی مطالب مرتبط با موضوع پژوهش خود اقدام کند. شیوه کار در این پژوهش نیز بدین‌صورت بوده که ابتدا سند الگوی اسلامی - ایرانی پیشرفت به‌عنوان یک مورد، مطالعه شد و سپس بخش‌های آرمان‌ها، رسالت، افق و تدابیر که به‌صورت عام یا خاص به موضوع مطالعه یعنی فناوری اطلاعات و ارتباطات مرتبط بودند، مورد بحث و بررسی قرار گرفتند. در ادامه مبتنی بر تحلیل اولیه صورت‌گرفته، سه تدبیر برای تقویت سند الگو از منظر فناوری اطلاعات و ارتباطات پیشنهاد شد. همچنین سعی شد تدابیر پیشنهادی دربردارنده اصول حاکم بر پدافند سایبری کشور مستخرج از سند راهبردی پدافند سایبری کشور باشد و این اصول مبنای عمل قرار گیرند.

۲. نقد و ارزیابی اجمالی سند الگوی پایه در محور فناوری اطلاعات و ارتباطات

همان‌گونه که اعلام شده (میرمعزی، ۱۳۹۷) (حسینی نژاد، ۱۳۹۷) الگوی اسلامی - ایرانی پیشرفت، سند بالادستی همه اسناد برنامه‌ای کشور خواهد بود؛ اسناد برنامه‌ای اعم از چشم‌انداز، سیاست‌های کلی، برنامه‌های کلی پنج‌ساله و سالانه است؛ فلذا این الگو باید جامعیتی داشته باشد که بتوان ذیل آن، برنامه‌های مختلف را منسجم کرد. تاکنون اسناد بالادستی مختلفی در حوزه فناوری اطلاعات و ارتباطات تدوین شده که از جمله آن‌ها می‌توان به سند چشم‌انداز بیست‌ساله، سیاست‌های کلی برنامه ششم توسعه، سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای، راهبردهای کلان ارائه خدمات اطلاع‌رسانی و اینترنت در کشور، برنامه توسعه و کاربری فناوری ارتباطات و اطلاعات ایران (تکفا)، سند راهبردی نظام جامع فناوری اطلاعات کشور، سند راهبردی جامعه اطلاعاتی ایران، سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور (افتا)، سیاست‌های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات، نقشه مهندسی فرهنگی کشور، حکم تشکیل شورای عالی فضای مجازی از سوی مقام معظم رهبری،

و حکم نصب اعضای جدید شورای عالی فضای مجازی از سوی ایشان. پیش از ورود به بحث ذکر این نکته ضروری است که ارزیابی‌های صورت گرفته در این تک‌نگاشت بر مبنای آرمان‌های انقلاب اسلامی، قانون اساسی، اسناد بالادستی که پیشتر ذکر شد و شرایط کنونی و آتی کشورمان در حوزه بین‌الملل و همچنین سیاست‌های کلان اعلامی پدافند غیرعامل و سند راهبردی پدافند سایبری خواهد بود. در این راستا مطابق با هاشمی و همایون (۱۳۹۶) سیاست‌های معطوف به فناوری اطلاعات و فضای مجازی در کل اسناد بالادستی که بر اهمیت این موضوع صحنه خواهد گذاشت را می‌توان در محورهای زیر خلاصه کرد:

- سیاست‌های مربوط به بهره‌گیری از فرصت‌های فضای مجازی و صیانت از تهدیدهای آن؛
- سیاست‌های حمایتی در قبال ظرفیت‌های سخت‌افزاری و نرم‌افزاری کشور؛
- سیاست‌های مربوط به توسعه جامعه شبکه‌ای و ایجاد فرصت‌های برابر و عادلانه در دسترسی به خدمات شبکه برای آحاد مردم؛
- سیاست‌های مربوط به راهبری و مدیریت راهبردی فضای مجازی در سطوح ملی و فراملی؛
- ایجاد نظام جامع اطلاعات و ارتباطات در کشور.

علی‌رغم ملاحظه موارد بالا که نشانگر توجه به حوزه فناوری اطلاعات و ارتباطات در اسناد بالادستی پیشین است، مشاهده می‌شود که سند الگوی اسلامی - ایرانی پیشرفت تنها در تدبیر شماره ۱۹: «پیریزی و گسترش نهضت کسب‌وکار هنرهای نمایشی و کاربردهای فضای مجازی با استفاده از میراث فرهنگی و ادبی ایرانی - اسلامی و قابلیت‌های ملی و محلی مطابق تقاضا و پسند مخاطب منطقه‌ای و جهانی» اشاره‌ای مبهم به این بخش داشته است. این اشاره گذرا و مبهم این سؤال را از پدیدآورندگان سند به وجود می‌آورد که آیا به نظر ایشان فضای سایبری که سبک

زندگی، امنیت، توسعه بازارها و بسیاری بخش‌های دیگر از جامعه بشری حتی بخش‌های صنعتی و اقتصادی در جهان امروز مبتنی بر آن شده است، واقعاً یک فضای غیرواقعی و مجازی است؟ و آیا باورشان این است که میزان اهمیت فضای سایبر در الگوی پیشرفت، به اندازه همین عباراتی که در بند نوزدهم آمده است، کفایت می‌کند؟ (پورسینا، ۱۳۹۷). توجه به این نکته لازم است که گرچه یک سند بالادستی امکان توجه به جزئیات حوزه‌های مختلف را ندارد، اما باید به گونه‌ای تدوین شود که هر حکم آن از جامعیت لازم برخوردار بوده و بتواند اهداف و ابزارهای سیاست‌گذاری را در خود بگنجاند، ولیکن این سند اصلاً نتوانسته است با توجه به اهمیت و چالش‌های پیش‌روی این حوزه، به آن پردازد که این امر با توجه به تهدیدات سایبری که به جد تمدن اسلامی - ایرانی را به خطر خواهد انداخت، نشان از مفروضات و انگاشته‌های نادرست سند دارد. به‌عنوان مثال برخی از تهدیدات سایبری پیش‌روی کشورمان به شرح ذیل هستند:

۱. تشکیل قرارگاه فرماندهی دفاع سایبری توسط آمریکا؛
۲. تشکیل قرارگاه سایبری توسط ناتو برای انجام اقدامات آفندی و دفاعی سایبری علیه برخی کشورها و برگزاری چندین مانور عملیات سایبری تاکنون؛
۳. اشراف دشمن بر فضای اینترنت و سایبری دنیا اعم از شبکه، اطلاعات، مراکز نگهداری داده، تولیدکنندگان اصلی سخت‌افزارها و نرم‌افزارها و خدمات؛
۴. وجود توافقات ضد امنیتی اعلام نشده بین برخی کشورها علیه جمهوری اسلامی ایران در فضای سایبر؛
۵. امکان تعبیه حفره امنیتی مخفی (دروازه پشتی) در تجهیزات فروخته‌شده به ایران توسط سازندگان مربوطه؛
۶. امکان و سابقه حمله سایبری به شبکه‌های کشور؛
۷. ممانعت از فروش برخی از سامانه‌های سایبر، به بهانه تحریم‌های بین‌المللی به ایران؛

۸. رویکرد و استراتژی‌های تهاجمی دشمنان در استفاده از توان سایبری خود برعلیه زیرساخت‌های حیاتی کشور که بر سایبر متکی هستند؛
۹. اعمال حاکمیت دشمن با استفاده از فضای حقوق بین‌الملل سایبر بر شبکه‌های جهانی از قبیل اینترنت، شبکه‌های ماهواره‌ای و...؛
۱۰. فقدان نظام حقوق بین‌المللی در حوزه دفاع سایبری (جلالی فراهانی و میر رفیع، ۱۳۹۸).

نکته دیگر آن‌که، در افق ۱۴۴۴ سند الگو به‌گونه‌ای نوید داده شده، که در همه بخش‌های آن، تهدید یا خطری وجود نخواهد داشت. از این‌رو در این سند، امنیت، استقلال و قدرت کامل برای دفاع بازدارنده به‌عنوان سه ویژگی برجسته کشور و از مفاهیم کلیدی آن است که البته هر سه این مفاهیم پیوند تنگاتنگی با امنیت سایبری دارند. از این‌رو باید این مهم در متن سند مورد تأکید قرار گیرد. فلذا با توجه به آن‌که تدابیر در راستای آرمان‌ها و افق و رسالت سند اتخاذ می‌شوند به‌نظر می‌رسد لحاظ عبارت «برخوردار از فناوری دفاع بومی برتر» در بخش افق سند در این راستا راهگشا خواهد بود. به‌طور کلی برخوردار بودن از فناوری بومی در حوزه‌های زیرساخت‌های اطلاعاتی و شبکه امکان نفوذناپذیری و کاهش آسیب‌پذیری آن‌ها را فراهم می‌آورد، قید «بومی» نیز به این دلیل است که فناوری غیربومی و وابسته در صورت پیشرفته بودن هم برای دشمن قابل نفوذ خواهد بود، لذا بازدارندگی ایجاد نخواهد کرد (احمدی و شاه محمدی، ۱۳۹۷). همچنین گنجاندن عبارت «آمادگی دفاعی» در بخش آرمان‌ها در دستیابی به این هدف راهگشاست. آمادگی دفاعی به‌عنوان یک اصل کلی در آیه ۶۰ سوره انفال نیز به‌صورت آموزه‌ای دستوری به مسلمانان سفارش شده است، که شامل فراهم‌آوری توان و نیرو است. توان شامل هرگونه ابزار و آلات بازدارنده و یا هجومی یا دفاعی است، از این‌رو تنها به سلاح اشاره نشده است. تهیه هر چیزی که قدرت امت و دولت را افزایش می‌دهد، امری ضروری است و با توجه به شرایط مکانی و زمانی

تغییر می‌کند. در دین اسلام همواره به دفاع در مقابل دشمن و حفظ آمادگی در برابر تهاجمات و حملات دشمن تأکید ویژه شده است و افزایش روزافزون توان بازدارندگی یک کشور، از چنان اهمیت و ارزشی برخوردار است که آن را نشانه ایمان دانسته است و این موضوع با مبانی سند نیز کاملاً منطبق است (احمدی و شاه محمدی، ۱۳۹۷). از آن رو که دفاع در برابر دشمن در فضای مجازی تفاوتی با فضای حقیقی ندارد، یک کشور اسلامی باید در فضای سایبری نیز آمادگی کامل خود را در برابر تهاجمات دشمن حفظ کند (پیرزینل بک و محسنی دهکلانی، ۱۳۹۸).

نکته دیگر که لحاظ آن خصوصاً در رابطه با فناوری‌های نوین همچون فضای مجازی ضروری است، آن است که به‌منظور دستیابی به پیشرفت مدنظر ما در دنیای واقعی، بایستی ابتدا این دنیای واقعی خود به درستی ترسیم شود. به‌عنوان مثال ابتدا ضمن آسیب‌شناسی اسناد برنامه‌ای از منظر چگونگی تدوین و الگوی پارادایمی آن‌ها؛ تأثیرات این برنامه‌ها بر وضعیت فرهنگی، اقتصادی، سیاسی کشور طی سال‌های هدف واکاوی شده و بر این مبنا سناریوهای محتمل آینده شناسایی و ترسیم شود. سپس بایستی رسالت ایران جهت نقش‌آفرینی در وضعیت کنونی جهان مشخص شود که البته این امر نیز با بررسی و تبیین وضعیت در بخش‌های مختلفی چون فرد، خانواده و جامعه ایران و ذیل فعالیت‌های آینده‌پژوهانه میسر می‌شود (مختاریان‌پور، ۱۳۹۵). با توجه به آن‌که در سند الگو، توجهی به اهمیت فضای مجازی نشده، مشخص است که این مسیر و آینده‌شناسی در آن نیز لحاظ نشده است. به‌طور کلی تصویرسازی و الگوسازی جامعه آینده از دغدغه‌های مهم کشورهای پیشرو در عرصه جهانی است. این کشورها عموماً اقدام به تصویرسازی جامعه آرمانی خود در افق‌های زمانی مشخصی کرده و سپس برای تحقق این تصاویر، علاوه بر گفتمان‌سازی گسترده، اقدام به تهیه برنامه‌ها و نقشه‌های راه کلان ملی نموده‌اند، به‌گونه‌ای که همه ارکان مختلف در قالب یک نظام منسجم، منابع خود را برای این تغییر پارادایم و ایفای نقش در تمدن نوین

آینده بسیج می‌نمایند. در عرصه فضای سایبر نیز وضعیت به همین منوال است، در واقع ویژگی مشترک اسناد کشورهای پیشرفته دنیا در این حوزه این‌گونه است که یک تصویرسازی واضح از آینده صورت می‌دهند، تصاویر آینده را مبتنی بر فضای سایبر ترسیم نموده، بین ارکان حکمرانی خود بر تصویر آینده اجماع حاصل کرده و سپس راهبری الگوهای پیشرفت حاصله را در بالاترین سطوح حاکمیت خود پیگیری می‌کنند. به‌طور کلی کشورهایی که فاقد تصویری از آینده خود باشند، در آینده منزوی خواهند شد؛ در این راستا، الگوی ایرانی - اسلامی پیشرفت نیز باید بتواند تصویری واضح از آینده مطلوب ایران ارائه کند، به‌گونه‌ای که در ساختار آن فضای مجازی دیده شود (کریمی قهرودی، ۱۳۹۸). برخی تصاویر و چشم‌اندازهای آتی کشورهای پیش‌تاز جهان که به‌خوبی به این عرصه توجه کرده‌اند، عبارتند از:

- ژاپن: جامعه پنجم (Society 5.0) یا جامعه اَبَر هوشمند.
- مالزی: مالزی پیشرفته ۲۰۵۰ و جوامع هوشمند (Smart Communities)، کشور مالزی در برنامه خود برای سال ۲۰۵۰ سه شاخص افزایش شادی، خلاقیت و نوآوری و رشد اقتصادی را مبنای آن قرار داده که در تحقق همه این‌ها فضای سایبری محور است.
- اتحادیه اروپا، به‌ویژه کشور آلمان: جامعه شبکه‌محور مشارکتی و انقلاب چهارم صنعتی (Industry 4.0).
- آمریکا: اینترنت اشیا صنعتی (IIoT) و تولید پیشرفته (Advance Manufacturing) و هوشمند.
- سنگاپور: ملت هوشمند (Smart Nation).
- چین: جامعه سایبری - فیزیکی - اجتماعی، ساخت چین ۲۰۲۵ (Made in China 2025) و ابرقدرت برتر تولید در ۲۰۴۹. کشور چین در برنامه‌ای که برای سال ۲۰۴۹ که صدمین سالگرد تأسیس جمهوری خلق چین است، سه برنامه ۱۰ ساله

برای تحقق آن تدوین کرده است و می‌کوشد با این برنامه جامعه را به یک فضای سایبری - فیزیکی - صنعتی تبدیل کند.

در همین راستا عربستان نیز قصد دارد تا سال ۲۰۲۰ زیرساخت‌های انرژی، آب، برق و قدرت سایبری کشورش را با استقرار شبکه‌های هوشمند و دیجیتال پیشرفته و همچنین تجهیزات تجارت الکترونیک تقویت و مضاعف کند، البته این مهم انجام نمی‌شود مگر آن‌که فناوری‌های دیجیتالی از امنیت سایبری برخوردار باشند.

نکته دیگر آن‌که باز هم در این سند به آن بی‌توجهی شده آن است که فضای مجازی، همچون شمشیری دو لبه، از یک‌سو نه تنها ساختارهای فرهنگی، اجتماعی و امنیتی کشورها را با تهدید جدی مواجه ساخته بلکه از سویی دیگر، فرصت‌های ارزشمندی را برای معرفی قابلیت‌های آن‌ها میسر می‌سازد. فلذا علاوه بر آن‌که می‌توان از ظرفیت عالی فضای مجازی در راستای تحقق الگو و دفاع از آرمان‌های انقلاب اسلامی نهایت استفاده صورت گیرد و با به‌کارگیری بهینه از فناوری‌های اطلاعاتی که اینترنت از مهم‌ترین مصادیق آن است، زمینه تحقق اهداف فرهنگی نظام و سند الگو فراهم آورده شود، این فضا به‌عنوان ابزاری در خدمت تهاجم فرهنگی و جنگ نرم دشمن، امنیت ملی کشور را مورد هدف قرار می‌دهد که این موضوع اهمیت مدیریت فضای مجازی را برای پایداری انقلاب اسلامی نشان می‌دهد.

سخن آخر این بخش آن‌که، با توجه به اهمیت حفظ امنیت ملی به‌عنوان مهم‌ترین مؤلفه ثبات کشور و تأثیرپذیری مستقیم امنیت ملی از تهدیدات سایبری اگر کشوری در چشم‌اندازها و اسناد بالادستی خود به فکر حفظ حریم‌های فضای سایبری خود نباشد، به‌هیچ‌عنوان نمی‌توان کشور مزبور را در معادلات جهانی جزو کشورهای قدرتمند به‌حساب آورد.

۳. ارائه پیشنهادات و تدابیر در محور فناوری اطلاعات و ارتباطات

در این بخش با توجه به نقد و ارزیابی صورت پذیرفته در بخش قبل، تدابیر پیشنهادی ارائه می‌گردد. در این بخش سعی شده تا تدابیر پیشنهادی منطبق با تعریف مرکز الگو که عبارتست از «تصمیمات و اقدامات اساسی» و با توجه به افق ۵۰ ساله، باشد. ضمناً تلاش شده تا تدابیر پیشنهادی دربردارنده اصول حاکم بر پدافند سایبری کشور مستخرج از سند راهبردی پدافند سایبری کشور باشد و این اصول مبنای عمل قرار گیرند. این اصول نُه‌گانه عبارتند از:

- مصون‌سازی و پایداری؛
- وحدت مدیریت؛
- بازدارندگی؛
- حفظ آمادگی؛
- پیش‌بینی در تهدیدشناسی؛
- اقتصادی‌سازی (رعایت صرفه و صلاح)؛
- اشراف اطلاعاتی؛
- دیپلماسی فعال؛
- اقتدار درون‌زا.

همچنین در پایان تشریح هر تدبیر، پیشنهادی مؤلفه پدافندی آن نیز مشخص شده است. سه تدبیر پیشنهادی این تکنگاشت به شرح ذیل است:

- گسترش بهره‌گیری از فرصت‌ها و صیانت از آسیب‌ها و تهدیدات فضای مجازی متناسب با هویت دینی، ملی و ارزش‌های جامعه.
- ایجاد و راه‌اندازی شبکه ملی اطلاعات به‌عنوان زیرساخت ارتباطی فضای مجازی کشور.

▪ بهبود و توسعه دسترسی امن و پایدار همه مردم به امکانات ارتباطی و اطلاع‌رسانی در چارچوب ضوابط فرهنگی کشور.

۳-۱. تدبیر پیشنهادی (۱): گسترش و بهره‌گیری از فرصت‌ها و صیانت از آسیب‌ها و

تهدیدات فضای مجازی متناسب با هویت دینی، ملی و ارزش‌های جامعه

پیدایش فناوری‌های ارتباطی و اطلاعاتی، فرصت‌ها و تهدیدهای انقلاب را چنان برجسته کرده که استمرار و تکامل انقلاب اسلامی منوط به توجه خاص و جدی و سرمایه‌گذاری نظام در این زمینه است. همان‌گونه که یکی از نکات کلیدی که رهبر معظم انقلاب همواره به آن اشاره می‌کنند اهمیت بالای فضای سایبر است تا جایی که این جمله از ایشان نقل شده است که: «اگر امروز رهبر انقلاب نبودم حتماً رئیس فضای مجازی کشور می‌شدم». در این راستا رهبر معظم انقلاب اینترنت را فرصتی فوق‌العاده توصیف می‌کنند و همواره مخاطب را از تهدیدانگاری صرف نسبت به آن برحذر می‌دارند. ایشان در سخنانی در سال ۸۴ می‌فرمایند: «امروزه اینترنت و ماهواره و وسایل ارتباطی بسیار متنوعی وجود دارد و حرف، آسان به همه جای دنیا می‌رسد. میدان افکار مردم و مؤمنان، عرصه کارزار تفکرات گوناگون است. امروز ما در میدان جنگ و کارزار حقیقی فکری قرار داریم. این کارزار فکری به هیچ وجه به زیان ما نیست؛ به سود ماست». ایشان همچنین در مقام تشبیه فرمودند که: «این فضا مثل یک رودخانه پر از آب و خروشان است که می‌آید و دائماً هم بر آب آن افزوده و خروشان‌تر می‌شود. اگر ما برای این رودخانه تدبیر کنیم و برنامه داشته باشیم؛ زه‌کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می‌شود فرصت. اگر ره‌ایش کنیم و برنامه‌ای برای آن نداشته باشیم، می‌شود یک تهدید». ایشان تأکید بسیاری بر اهمیت این فضا و لزوم مدیریت آن داشتند؛ به گونه‌ای که همه ارکان نظام باید نقش خاص خود را با حضوری فعال در این فضا ایفا کنند.^۱

1. <http://farsi.khamenei.ir/others-dialog?id=19272>

به طور کلی امروزه تمامی سرمایه‌ها و زیرساخت‌های سایبری و یا متکی بر سایبر به وسیله تهدیدات تخصصی و از جنس سایبر در معرض خطر قرار گرفته‌اند، به طوری که با آسیب دیدن این سرمایه‌ها، مجموعه‌ای از پیامدهای اقتصادی، اجتماعی، سیاسی، نظامی، امنیتی و ... برای کشور به بار خواهد آمد. از طرفی جنگ سایبری به دلیل نفوذ و گسترش فضای سایبر، بر سایر جنگ‌های جدید مانند جنگ اقتصادی تأثیرگذار است. همچنین گستره پدافند غیرعامل به دلیل وجود تهدیدات مختلف در حوزه‌های گوناگون، گسترش یافته است و در این راستا، نیل به اهداف کلان پنج‌گانه پدافند غیرعامل کشور مستلزم توجه یکپارچه و همه‌جانبه به همه حوزه‌های کارکردی پدافند غیرعامل است (جلالی فراهانی و میر رفیع، ۱۳۹۸). همان‌گونه که رهبر معظم انقلاب فرموده‌اند این فضا مملو از فرصت و تهدید است، در ادامه به برخی از تهدیدات و فرصت‌ها اشاره خواهد شد:

• ارتقای سرمایه اجتماعی و تقویت قدرت ملی با استفاده از شبکه‌های

اجتماعی مجازی: هرچند سند الگوی پایه اسلامی - ایرانی پیشرفت در افق ۱۴۴۴ هجری شمسی، تصویری از جامعه مطلوب و پاسدار ارزش‌ها، هویت ملی و میراث انقلاب اسلامی ارائه داده است، ولی یکی از ملزومات دستیابی به اهداف ترسیم‌شده این سند، دارا بودن برنامه‌ریزی صحیح و درک کامل و مؤثر از قدرت نرم است. در این میان مشارکت، اعتماد، شبکه‌ها و نهادهای اجتماعی، وفاداری مردم به حاکمیت و افزایش مشروعیت سیاسی و در یک کلام افزایش سرمایه اجتماعی نقشی بسیار مهم در قدرت نرم دارد (جهان‌بین و امامی، ۱۳۹۳). از سوی دیگر با دقت در شاخص‌های سرمایه اجتماعی، به خوبی می‌توان دریافت که یکی از هدف‌های مهم جنگ نرم، تزلزل در مؤلفه‌های فوق‌الذکر است. به گونه‌ای که اگر به اعتماد بین افراد و حکومت خدشه وارد شود، شالوده‌های آن جامعه سست شده و آن کشور در معرض ناامنی قرار می‌گیرد. بر این اساس، لازمه مقابله با جنگ نرم، برخورداری از قدرت نرم بوده که از ابزارهای اساسی آن امکان بازتولید سرمایه اجتماعی در لایه‌های مختلف است. در این

میان، شبکه‌های اجتماعی، بستری مناسب برای ایجاد مشارکت افراد و اقشار مختلف جامعه فراهم ساخته است (قدسی، ۱۳۹۲). به‌طور کلی مشارکت اجتماعی در کشور بر سه گروه مؤثر است:

۱) ایرانیان داخل مرزهای جغرافیایی.

۲) ایرانیان خارج از کشور.

۳) دوستان و علاقه‌مندان ایران.

• **جنگ نرم در حوزه سایبر:** مقام معظم رهبری در رابطه با اهمیت جنگ نرم و لزوم ارائه راهکار در این رابطه می‌فرماید: «اگر دشمن با تولید محتوا (کتاب، فیلم، عکس، سایت‌های اینترنتی و...) سعی کند اعتقادات مردم را نشانه بگیرد - که گرفته است - این یک نوع آفند است و البته بسیار بسیار خطرناک نیز می‌باشد و مقوله براندازی و تهدید نرم نیز در همین راستا به‌کار گرفته می‌شود، بنابراین ما چه نوع دفاعی باید از خود داشته باشیم که مردم محکم بایستند و این شیوه‌ها اثر نکند و آسیب‌پذیری به حداقل ممکن برسد؟». به‌طور کلی جنگ نرم و تهدیدات سایبری یکی از مهم‌ترین چالش‌های پیش‌روی انقلاب اسلامی است. این مسئله یکی از مؤثرترین و پیچیده‌ترین تهدیداتی است که پایداری انقلاب اسلامی را به مخاطره می‌اندازد. از این‌رو لازم است بازدارندگی در مقابل آن مورد توجه سند الگو قرار گیرد چرا که غفلت از آن می‌تواند خسارات جبران‌ناپذیری بر پیکر انقلاب اسلامی وارد نماید. در این جنگ، دشمن درصدد است بدون استفاده از حمله نظامی و با استفاده از شیوه‌های مختلف به تسخیر اذهان و افکار عمومی پرداخته و با فروپاشی تدریجی نظام فکری و روانی مردم، زمینه را برای براندازی انقلاب اسلامی فراهم نماید (الفی و بشارت، ۱۳۹۸). جنگ نرم یکی از مهم‌ترین جلوه‌های تهدیدآفرین امنیت ملی جمهوری اسلامی ایران است. در

این راستا اسناد رسمی در گزارش اخیر اندیشکده (CSIS)^۱ نشان می‌دهد که تحلیل‌گران این اندیشکده در یک پیشنهاد عملیاتی به دولت آمریکا می‌گویند: «ایران را می‌توانید با قدرت نرم به زانو درآورید». اسنادی همانند این مورد، بیانگر این واقعیت مهم هستند که فعالیت‌های سایبری علیه ایران از طرف اپوزیسیون‌های مختلف از اتاق‌های فکر آمریکایی‌ها و به دستور مستقیم آن‌ها صورت می‌پذیرد. بنابراین بسیار ساده‌لوحانه است که اقدام‌های دشمنان در عرصه جنگ نرم را اقدام‌هایی در سطح و فاقد عقبه علمی فرض کرد. مطمئناً موفقیت در این فضا، مرهون کوشش‌های متفکران و حمایت‌های گسترده نظام سلطه نوین جهانی در قالب اتاق‌های فکر قدرتمند است. از این رو، برخورد اساسی از طریق مقابله به مثل میسر بوده و استفاده از روش‌های غیرعلمی و منفعلانه، به نتیجه نخواهد رسید (قدسی، ۱۳۹۲).

بهره‌برداری از فضای مجازی در جنگ نرم، در جهت کسب منافع بیشتر برای صاحبان قدرت است که این موضوع در گذشته با جنگ رو در رو انجام می‌شد. در این بین رسانه‌های مجازی در حال تبدیل شدن به امپراطوری‌های بزرگ در عصر جدید هستند. اگر تا پیش از این، منطق پیروزی در جنگ‌های سنتی، برخورداری بیشتر از نیروها و ابزارآلات فیزیکی بود، اما بدون شک، پیدایش محیط مجازی، باعث تشکیک اساسی در این منطق شده است. این فضا، قدرتی را به وجود آورده و بسیاری از عرصه‌های تقابل را متفاوت از گذشته ساخته است. شبکه‌های اجتماعی به دلیل قابلیت جذب مخاطبین به یکی از ابزارهای تأثیرگذار جنگ تبدیل شده و سعی می‌کند با استفاده از مؤلفه‌هایی چون تغییر افکار و نگرش‌ها اهداف خود را در کشورها اجرایی نمایند (کاویانی، ۱۳۹۸). در حال حاضر شبکه‌های اجتماعی همچون تلگرام، اینستاگرام، واتساپ، فیس‌بوک و توییتر در میان کاربران ایرانی محبوبیت بیشتری دارند. بر اساس

۱. CSIS به‌عنوان اندیشکده رتبه اول در جهان در میان اندیشکده‌های دفاع و امنیت ملی و رتبه چهارم بهترین اندیشکده‌ها با بیشترین ایده‌ها و پیشنهادهای نوآورانه معرفی شده است.

آمارهای سایت آماری آکسا^۱، در سال ۱۳۹۳ تعداد کاربران ایرانی تلگرام ۲۲ میلیون نفر بوده که در فاصله بین سال‌های ۱۳۹۳ تا ۱۳۹۵ این تعداد به بیش از ۴۵ میلیون کاربر رسید. این آمار علاوه بر این‌که بیانگر استقبال بسیار بالای کاربران ایرانی از شبکه‌های اجتماعی در سال‌های اخیر است، بیانگر آن است که این شبکه‌ها به همان میزان که فرصت‌های ویژه‌ای را در ارتباطات اجتماعی تسهیل می‌سازند، به همان میزان نیز می‌توانند فضایی برای ارتکاب انواع جرائم سایبری باشند. بر اساس گزارش پلیس فتا، در سال ۱۳۹۵ نزدیک به ۶۰ درصد جرائم سایبری در تلگرام شکل گرفته که در این بین، جرائم اخلاقی با ۳۷ درصد بالاترین حجم جرائم را به خود اختصاص داده‌اند.^۲ همچنین این شبکه‌ها بستر انواع آسیب‌های اجتماعی و فرهنگی را از قبیل: تضعیف ارتباطات صمیمی در کانون خانواده، اختلال در امر آموزشی و افت تحصیلی دانش‌آموزان و دانشجویان، اعتیاد اینترنتی، انواع انحرافات و سوءاستفاده‌های جنسی در میان نوجوانان و جوانان و حتی تضعیف هویت دینی و ملی برای مخاطبان و کاربران این شبکه‌ها به دنبال داشته است. امروزه ابزارهای نظارت سنتی دیگر باید جای خود را به شیوه‌ها و ابزارهای جدیدی بدهند که با توانمندسازی مخاطبان در مقابل آثار سوء رسانه‌ها به آن‌ها مصونیت بیشتری ببخشند و مخاطب منفعل را به مخاطب گزینشگر مبدل نمایند به نحوی که خود فرد نیز می‌تواند رژیم مصرف رسانه‌ای خود را تنظیم نماید (اکبرزاده و همکاران، ۱۳۹۷).

• **تهدیدات سایبری:** تهدید امنیت ملی می‌تواند سطح زندگی شهروندان را با خطر افت مواجه کند به طوری که حمله به هر کدام از ساختارهای امنیتی در سطوح مختلف ملی و بین‌المللی، به‌عنوان تهدیدی نوین و ویرانگر علیه امنیت کشور است که می‌تواند موجبات فروپاشی و نابودی زیرساخت‌های حیاتی و بنیانی جامعه شود (داوودی، ۱۳۹۶). در این رابطه رهبر معظم انقلاب نیز می‌فرماید: «تنها راه مقابله با تهدیدها این

1. Alexa

2. <https://www.cyberpolice.ir/category>

است که وضعیت داخلی به‌گونه‌ای ساماندهی شود که دشمن از پیروزی خود مطمئن نباشد و زمینه را برای ماجراجویی فراهم نبیند».

در این راستا تهدیدهای سایبری متنوعی در کشورهای مختلف احصاء و مورد تجزیه و تحلیل قرار گرفته است از جمله: سرقت اطلاعات تجاری و بیمه‌ای و بهداشتی، تهدید سایبری برهم‌زدن اقتصاد کشور و رشکستی شرکت‌های بزرگ، اخبار جعلی به‌منظور عملیات روانی در شبکه اجتماعی، بدافزارهای بانکی در تلفن همراه، اینترنت اشیا در حمل‌ونقل عمومی تجهیزات پزشکی و دوربین‌های مداربسته، استفاده از تروریست، اخاذی سایبری، عدم آشکاری آسیب‌پذیری، الگوریتم مبهم، تهدید کشتی‌ها و زیردریایی‌ها، تهدید در صنایع نفت و گاز، سلاح‌های اتوماتیک، روبات قاتل، حملات به تأسیسات هسته‌ای، حملات به تأسیسات مخابراتی، کنترل جریان نفت، انجام معاملات مالی، نام برد.

کشور ما نیز جزء کشورهایی است که بیشترین حملات تروریستی سایبری را به زیرساخت‌های مالی، هسته‌ای و نظامی خود متحمل می‌شود و هر لحظه ممکن است زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی در سامانه‌های رایانه‌ای کشور که اصطلاحاً به‌عنوان سرمایه ملی سایبری تلقی می‌شوند از طریق تهدید سایبری، تخریب شده یا اطلاعات آن‌ها افشا یا به‌علت دسترسی غیرمجاز مختل شود. به ثمر نشستن هرکدام از این حملات می‌تواند نتایج فاجعه‌باری برای امنیت و سلامت کشور و ملت به‌همراه داشته باشد و لذا بایستی هم امنیت فضای سایبر در کشور را ارتقاء داده و هم بتوانیم با تقویت مکانیزم‌های امنیتی در بعضی موارد حتی مقابله‌به‌مثل نماییم (کورکی‌نژاد، ۱۳۹۴). بنابراین با لحاظ استراتژی بازدارندگی سایبری و برای جلوگیری از خطرات ذکرشده، نظام جامع پدافند کشور باید طوری طراحی و ایجاد شود که از طریق رصد، پایش و مدیریت و کنترل به‌هنگام، تهدید و تهاجم سایبری دشمن را خنثی و از زیرساخت‌های فناوری اطلاعات کشور محافظت نماید (کرم‌روان، ۱۳۹۸).

• وابستگی به خارج از کشور در حوزه‌های نرم‌افزاری و سخت‌افزاری: یکی از شیوه‌های بازاریابی در حوزه سایبر، سرمایه‌گذاری و بومی‌سازی تجهیزات مرتبط با جهان سایبر است. برای استفاده از تجهیزات سایبری در بخش‌های ویژه حیاتی و حساس کشور همیشه باید با نگاه بدبینانه به این تجهیزات نگریست به دلیل این که این تجهیزات منفذ ورود و اقدامات بعدی هستند و بیشترین آسیب‌های وارد در حوزه سایبری ناشی از استفاده از تجهیزات و فناوری‌های وارداتی بدون توجه به بومی‌سازی متناسب با شرایط کشور است. با رشد تصاعدی فراگیر شدن فناوری اطلاعات در سیستم‌های دولتی و خصوصی و افزایش روزافزون خدمات و سرویس‌های ارائه شده به اقشار مختلف جامعه در بستر فن‌آوری اطلاعات چنانچه به زیرساخت‌های بومی و ابزارهای امنیتی بومی توجه جدی صورت نپذیرد با گذر زمان وابستگی جامعه به خدمات الکترونیک بیشتر و از طرفی وابستگی زیرساخت‌های سرویس‌دهندگان به صاحبان اصلی تکنولوژی این صنعت در خارج از کشور نیز بیشتر خواهد شد. بدون شک با تکیه دادن به ابزارها و تجهیزاتی که ساخته کشورهای بیگانه می‌باشد هیچ‌گاه نمی‌توان امنیت کامل را برقرار نمود زیرا در لایه فیزیکی امنیت وابستگی وجود داشته و در شرایط مختلف از جمله بروزرسانی امکان اختلال و سوءاستفاده وجود خواهد داشت. فلذا باید زیرساخت‌های حوزه سایبر را در زمینه سخت‌افزار و نرم‌افزار با استفاده از ظرفیت‌های بومی تکمیل و تقویت گشته و در حد امکان از استفاده از فناوری‌های غیربومی پرهیز نمایند. گرچه ممکن است، ساخت نمونه بومی در کشور، در همه زمینه‌ها مقرون به صرفه نباشد و ورود یک کالا به داخل، هزینه و زمان کمتری را برای ما به ارمغان بیاورد، اما در درازمدت، قطعاً می‌توان نتایج مثبت و قابل توجهی را در این زمینه به دست آورد. مقامات وزارت دفاع آمریکا نیز با وجود این که این کشور یکی از اصلی‌ترین تولیدکنندگان تجهیزات دیجیتالی به حساب می‌آید، مدتی قبل اعلام کردند در تلاش هستند با همکاری شرکت‌های فناوری و دانشمندان فعال این حوزه،

معماری‌های سخت‌افزاری کاملاً متفاوتی را برای تراشه‌های به‌کاررفته در تجهیزات نظامی طراحی کنند؛ زیرا نمونه‌های فعلی تقریباً حالتی عمومی داشته و دشمنان آن‌ها با مهندسی معکوسشان می‌توانند آسیب‌پذیری یا راه‌کار نفوذ را شناسایی کنند. به‌نظر می‌رسد تجمیع تمام توان و نیروی موجود و سازمان‌دهی و یکپارچه‌سازی دانش در زمینه دفاع سایبری، راهکاری مطمئن برای افزایش بازدارندگی سایبری باشد که در صورت ایجاد چنین ساختاری بر پایه دانش بومی، راهی برای نفوذ بیگانگان باقی نخواهد ماند (پدافند سایبری، ۱۳۹۷).

با این توضیحات که ارائه شد، نتیجه تحقق تدبیر پیشنهادی آن است که کشور به‌جای غافلگیر شدن، همواره در مواجهه با پدیده‌های نوظهور اجتماعی در این حوزه و توسل جستن به اقدام‌های سلبی و منفعلانه و وابستگی به تجهیزات خارجی، به بازیگری فعال، آینده‌پژوه و آینده‌ساز تبدیل می‌گردد. فلذا با توجه به توضیحات ذکر شده، این تدبیر اصول پدافندی مندرج در جدول ذیل را پوشش می‌دهد.

جدول (۲): اصول پدافندی گنجانده شده در تدبیر پیشنهادی (۱)

اصول پدافندی مربوط به فناوری اطلاعات و ارتباطات								
مصون‌سازی و پایداری	وحدت مدیریت	بازدارندگی	حفظ آمادگی	پیش‌بینی در تهدیدشناسی	اقتصادی‌سازی	اشراف اطلاعاتی	دیپلماسی فعال	اقتدار درون‌زا
*	*	*	*	*	*	*	*	*

منبع: یافته‌های تحقیق

۳-۲. تدبیر پیشنهادی (۲): ایجاد و راه‌اندازی شبکه ملی اطلاعات به‌عنوان زیرساخت ارتباطی فضای مجازی کشور

همان‌گونه که در ۱۰ وظیفه و مأموریت شورای عالی فضای مجازی که توسط رهبر معظم انقلاب اعلام گردیده است^۱، تسریع در راه‌اندازی شبکه ملی اطلاعات پس از تصویب طرح آن در شورای عالی و نظارت مستمر و مؤثر مرکز ملی بر مراحل راه‌اندازی و بهره‌برداری از آن به‌عنوان یکی از وظایف این شورا اعلام شد.

1. <https://www.leader.ir/fa/content/13542>

شبکه ملی اطلاعات طبق تعریفی که شورای عالی فضای مجازی در مصوبه جلسه پانزدهم خود در مورخه ۱۳۹۲/۱۰/۳ مشخص کرده است، «به‌عنوان زیرساخت ارتباطی فضای مجازی کشور، شبکه‌ای مبتنی بر قرارداد (پروتکل) اینترنت به‌همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده‌ای است به‌صورتی که درخواست‌های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند به‌هیچ‌وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترنت و خصوصی و امن داخلی در آن فراهم شود». بنابراین شبکه ملی اطلاعات به‌عنوان زیرساخت ارتباطی فضای مجازی کشور یکی از مهم‌ترین پروژه‌های ملی محسوب می‌شود که تحقق آن بنا بر رویکردهای جهانی و ضرورت‌های ملی، مانند ارائه خدمات زیرساختی پیشرفته و مطابق با نیازهای کشور، بهره‌مندی از مزایای اقتصادی، صیانت از فرهنگ ایرانی - اسلامی و حفاظت از اطلاعات و ارتباطات کاربران در برابر تهدیدات امنیتی و حریم خصوصی، الزام شده است.

اهمیت شبکه ملی اطلاعات در حدی است که مقام معظم رهبری نیز بارها بر لزوم ایجاد شبکه ملی اطلاعات تأکید داشته‌اند و کوتاهی در این خصوص را گوشزد کرده‌اند. ایشان در سخنانشان با بیان این‌که «فضای مجازی خیلی مهم است و آنچه از همه مهم‌تر است، مسئله شبکه ملی اطلاعات است»، تأکید کردند: «امروز فضای مجازی مخصوص ما نیست و همه دنیا با فضای مجازی درگیرند و کشورهایی که شبکه ملی اطلاعات درست کرده و فضای مجازی را به نفع خودشان و ارزش‌های مورد نظر خودشان کنترل کرده‌اند، یکی دو تا نیستند. متأسفانه در زمینه شبکه ملی اطلاعات در کشور کوتاهی شده و کاری که باید انجام گیرد، انجام نگرفته است».

به عقیده اکثر صاحب‌نظران نیز، یکی از ضروری‌ترین و مهم‌ترین سرمایه‌گذاری‌های توسعه شبکه‌ها و فناوری اطلاعات در هر کشوری، طراحی و اجرای سامانه‌های به‌طور کامل امن و حفاظت اطلاعات است که به‌عنوان یک سرمایه و اعتبار ملی به‌حساب می‌آید. به‌عنوان مثال با توجه به عدم وجود شبکه ملی اطلاعات و

ارتباطات برای مرتبط شدن مراکز ثقل به یکدیگر، متأسفانه دیده شده است که در مواقعی از بستر اینترنت استفاده می‌شود که این موضوع باعث آغاز تهدیدات سایبری در حوزه شبکه است.

علاوه بر این‌ها شبکه ملی اطلاعات به‌عنوان یک طرح کلان و اساسی در حوزه فناوری اطلاعات و ارتباطات بستری است که می‌توان بر مبنای آن به پیشبرد سیاست‌های فرهنگی جمهوری اسلامی ایران در این فضا پرداخت، چنانچه در اسناد بالادستی مختلف دیگر نیز توجه ویژه بر ایجاد نظام جامع اطلاعات و ارتباطات در کشور و به‌طور خاص شبکه ملی اطلاعات نیز مشاهده می‌شود. این موضوع علاوه بر این‌که جایگاه مهم شبکه ملی اطلاعات در عرصه سیاست کشور را اثبات می‌کند، بیانگر نقش کلیدی این شبکه در فراهم‌سازی بسترهای لازم جهت پیشبرد سیاست‌های فرهنگی کشور در این عرصه است. به بیان دیگر، بدون راه‌اندازی کامل شبکه ملی اطلاعات نمی‌توان سیاست‌های مربوط به استفاده از فرصت‌های فضای مجازی و صیانت از تهدیدهای آن، سیاست‌های حمایتی در قبال ظرفیت‌های مردمی داخل کشور، سیاست‌های مربوط به توسعه جامعه شبکه‌ای و ایجاد فرصت‌های برابر و عادلانه در دسترسی به خدمات شبکه را برای آحاد مردم ایجاد کرد (همایون و هاشمی، ۱۳۹۶).

بنابراین با توجه به توضیحات ذکرشده، این تدبیر اصول پدافندی مندرج در جدول (۲) را پوشش می‌دهد.

جدول (۲): اصول پدافندی گنجانده‌شده در تدبیر پیشنهادی (۲)

اصول پدافندی مربوط به فناوری اطلاعات و ارتباطات								
مصون‌سازی و پایداری	وحدت مدیریت	بازدارندگی	حفظ آمادگی	پیش‌بینی در تهدیدشناسی	اقتصادی‌سازی	اشراف اطلاعاتی	دیپلماسی فعال	اقتدار درون‌زا
*	*	*	*	*	*	*	*	*

منبع: یافته‌های تحقیق

۳-۳. تدبیر پیشنهادی (۳): بهبود و توسعه دسترسی امن و پایدار همه مردم به امکانات ارتباطی و اطلاع‌رسانی در چارچوب ضوابط فرهنگی کشور

پیدایش فناوری‌های ارتباطی و اطلاعاتی، فرصت‌ها و تهدیدهای انقلاب را چنان برجسته کرده که استمرار و تکامل انقلاب اسلامی منوط به توجه خاص و جدی و سرمایه‌گذاری نظام در این زمینه است. این یکی از جهاتی است که حوزه فضای مجازی را در نظر رهبری معظم به اندازه خود انقلاب اسلامی پراهمیت کرده است.^۱

امروزه شاخص‌های گسترش فناوری اطلاعات به‌عنوان یکی از شاخص‌های توسعه‌یافتگی محسوب می‌گردد. هر کشوری بتواند ضریب نفوذ این فناوری را در میان شهروندان خود افزایش دهد، از فواید متعدد آن در حوزه‌های مختلف بهره‌مند می‌شود. به موازات استفاده از فناوری اطلاعات و ارتباطات در تمامی ابعاد حیات بشری، جهان به سرعت در حال تبدیل شدن به یک جامعه اطلاعاتی است؛ همچنین فناوری اطلاعات به‌عنوان عمده‌ترین محور تحول و توسعه جهان امروزی مطرح شده و دستاوردهای ناشی از آن به‌گونه‌های مختلف در زندگی مردم تأثیرگذار بوده است (فراهانی و همکاران، ۱۳۹۱). امروزه امکان دستیابی به اینترنت و استفاده از منابع اطلاعاتی در تمامی جوامع بشری روندی تصاعدی را طی می‌کند و جوامع مختلف با توجه به زیرساخت‌های متعدد ایجادشده از مزایای فناوری اطلاعات و ارتباطات، استفاده می‌نمایند.

بنابراین با توجه به اهمیت پیش‌گفته، حوزه ارتباطات کشور به‌مثابه سلسله اعصاب بوده و نقش تعیین‌کننده‌اش در اداره امور کشور بسیار حساس و حیاتی است و در اولویت‌های تهاجم دشمن قرار خواهد داشت. دشمن برای فلج نمودن کشور، اولین موج‌های شدید تهاجمی خود را چه به‌لحاظ سخت‌افزاری و یا نرم‌افزاری متوجه این حوزه خواهد نمود. در پاسخ به این ضرورت، پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات و جنگ سایبری، به‌منظور امنیت، ایمنی و پایداری زیرساخت‌های حیاتی کشور در مقابل تهدیدهای دشمن از ناحیه فناوری اطلاعات و ارتباطات شکل گرفته است.

1. <http://farsi.khamenei.ir/others-dialog?id=19272>

اما اقدام مناسب در حوزه پدافندی امنیت فناوری اطلاعات و ارتباطات منوط به شناخت صحیح آن است. به طور کلی تأمین و حفظ امنیت فناوری اطلاعات به محورهای محرمانگی، جامعیت، دسترس پذیری و عدم انکار اشاره دارد. محرمانگی به معنا و مفهوم حفاظت داده‌های سیستم‌های رایانه‌ای در برابر دسترسی‌های غیرمجاز، جامعیت یا یکپارچگی به مفهوم تأمین دقت و جامعیت اطلاعات و نرم‌افزارهای رایانه‌ای، دسترسی یا دسترس پذیری، به مفهوم ضمانت دسترسی به اطلاعات و خدمات حساس در زمان مورد نیاز و عدم انکار تبادل اطلاعات است (پورمراد، ۱۳۹۳).

مهم‌ترین مأموریت‌های پدافند غیرعامل در فناوری اطلاعات به شرح ذیل است:

- ایجاد و حفظ امنیت زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات در برابر مخایرات محتوایی.
- ایمنی زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات در قبال حملات فیزیکی.
- پایداری زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات در مواجهه با تهدیدات و ادامه مأموریت در شرایط بحران.
- صیانت از زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات در مقابل حملات غیرمترقبه، بلایای طبیعی و مواقع اضطراری.
- ارتقاء و توسعه عزم ملی، باور و فرهنگ عمومی و سازمانی در خصوص رعایت اصول پدافند غیرعامل (استتار، اختفا، پوشش، پراکندگی، استحکام بنا، فریب و ...) در حوزه فناوری اطلاعات و ارتباطات کشور.
- تولید دانش فنی و بومی و بهره‌گیری آگاهانه از فناوری مناسب و روزآمد کشور در خصوص دفاع غیرعامل فاوا به وسیله توسعه جهاد علمی.
- کاهش آسیب‌پذیری زیرساخت‌های کلیدی و مراکز حیاتی، حساس و مهم کشور در حوزه فناوری اطلاعات و ارتباطات در برابر تهدیدات و اعمال ملاحظاتی،

سیاست‌ها و ضوابط خاص پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات در برنامه‌های در دست مطالعه کشور.

▪ تدوین معماری کلان پدافند غیرعامل فناوری اطلاعات و ارتباطات کشور^۱.

بنابراین با توجه به توضیحات ذکر شده، این تدبیر اصول پدافندی مندرج در جدول (۳) را پوشش می‌دهد.

جدول (۳): اصول پدافندی گنجانده شده در تدبیر پیشنهادی (۳)

اصول پدافندی مربوط به فناوری اطلاعات و ارتباطات								
مضمون‌سازی و پایداری	وحدت مدیریت	بازدارندگی	حفظ آمادگی	پیش‌بینی در تهدیدشناسی	اقتصادی‌سازی	اشراف اطلاعاتی	دیپلماسی فعال	اقتدار درون‌زا
*	*	*	*	*	*	*	*	*

منبع: یافته‌های تحقیق

جمع‌بندی و نتیجه‌گیری

امروزه کشورها نمی‌توانند در معادلات امنیتی و راهبردی خود از نقش فناوری اطلاعات و ارتباطات و تأثیر آن بر امنیت خود غافل شوند، فلذا با توجه به این نقش کلیدی و حساس، رعایت ملاحظات پدافند غیرعاملی در اسناد بالادستی این حوزه بیش از پیش ضرورت دارد. بنابراین الگوی اسلامی - ایرانی پیشرفت به‌عنوان سند بالادستی همه اسناد برنامه‌ای کشور و همچنین نقشه راه ۵۰ سال آینده کشورمان، باید بتواند تصویری واضح از آینده مطلوب ایران در این بخش ارائه دهد، به‌طوری که اجرای این سند آسیب‌پذیری کشور در مقابل تهدیدات دشمن را کاهش دهد و موجب تقویت مؤلفه‌های قدرت جمهوری اسلامی ایران گردد. مطالعه حاضر که با روش اسنادی صورت گرفت، نشان داد که سند الگوی اسلامی - ایرانی پیشرفت تنها در تدبیر شماره ۱۹: «پی‌ریزی و گسترش نهضت کسب‌وکار هنرهای نمایشی و کاربردهای فضای مجازی با استفاده از میراث فرهنگی و ادبی ایرانی - اسلامی و قابلیت‌های ملی و محلی مطابق تقاضا و پسند مخاطب منطقه‌ای و جهانی» اشاره‌ای مبهم به این بخش داشته

1. www.ipfn.ir

است. در افق سند الگو به گونه‌ای نوید داده شده، که در همه بخش‌های کشور ایران، تهدید یا خطری وجود نخواهد داشت. این در حالی است که امنیت، استقلال و قدرت کامل برای دفاع بازدارنده به‌عنوان سه ویژگی برجسته کشور پیوند تنگاتنگی با امنیت سایبری دارند. از این رو باید این مهم در متن سند مورد تأکید جدی قرار گیرد. علاوه بر این فناوری اطلاعات نه تنها این پتانسیل را دارد که ساختارهای فرهنگی، اجتماعی و امنیتی کشورها را با تهدید جدی مواجه سازد، بلکه فرصت‌های ارزشمندی را برای بروز قابلیت‌های یک کشور میسر می‌سازد. فلذا علاوه بر آن که می‌توان از ظرفیت عالی فضای مجازی در راستای تحقق الگو و دفاع از آرمان‌های انقلاب اسلامی نهایت استفاده صورت گیرد و با به‌کارگیری بهینه از فناوری‌های اطلاعاتی از جمله اینترنت به‌عنوان مهم‌ترین مصداق آن، می‌توان زمینه تحقق اهداف فرهنگی نظام و سند الگو را نیز فراهم آورد.

در انتها نیز سه تدبیر به شرح ذیل برای رفع خلأهای سند الگو پیشنهاد شد:

- گسترش بهره‌گیری از فرصت‌ها و صیانت از آسیب‌ها و تهدیدات فضای مجازی متناسب با هویت دینی، ملی و ارزش‌های جامعه.
- ایجاد و راه‌اندازی شبکه ملی اطلاعات به‌عنوان زیرساخت ارتباطی فضای مجازی کشور.
- بهبود و توسعه دسترسی امن و پایدار همه مردم به امکانات ارتباطی و اطلاع‌رسانی در چارچوب ضوابط فرهنگی کشور.

کتابنامه

- احدی، محمد و شاه‌محمدی، محمد (۱۳۹۷)، «طرح راهبردی دفاع سایبری جمهوری اسلامی ایران در حوزه بازدارندگی»، *مطالعات بین‌رشته‌ای دانش راهبردی*، ۸ (۳۱)، ۲۲۵-۲۵۲.
- اکبرزاده، علیرضا (۱۳۹۷)، «رویکرد مخاطب‌محور در مواجهه با شبکه‌های اجتماعی مجازی»، *رسانه و فرهنگ*، ۱۶، ۱-۱۹.

- برون، مهرداد (۱۳۹۸)، امنیت و دفاع سایبری، دومین کنفرانس ملی پدافند سایبری، مراغه: دانشگاه آزاد اسلامی واحد مراغه.
- پدافند سایبری (۱۳۹۷). تقویت زیرساخت‌های بومی - سایبری، تقویت سپر دفاعی کشور، بازیابی از قرارگاه پدافند سایبری کشور: <https://www.papsa.ir>
- پورسینا، بهروز (۱۳۹۷)، چند پرسش اساسی از پدیدآورندگان سند الگوی پیشرفت. بازیابی از روزنامه مردم‌سالاری: <http://newspaper.mardomsalari.ir/4719/page/1/47000>
- پورمراد، مجید (۱۳۹۳)، حفاظت فناوری اطلاعات و ارتباطات، تهران: کوثر.
- جلالی فراهانی، غلامرضا؛ و میر رفیع، علی (۱۳۹۸)، «ارائه راهبردهای پدافند غیرعامل کشور در برابر تهدیدات سایبری»، مطالعات دفاعی استراتژیک، ۱۷ (۷۵)، ۴۵-۶۲.
- جهان‌بین، فرزاد و امامی، اعظم (۱۳۹۳)، «سرمایه اجتماعی حلقه ارتباطی قدرت نرم، امنیت نرم، تهدید نرم»، مطالعات قدرت نرم، ۱۰ (۴)، ۴۹-۷۴.
- حسینی نژاد، سیداکبر (۱۳۹۷)، نقد، نظر و بررسی سند الگوی اسلامی ایرانی پیشرفت در جمع نمایندگان طلاب و فضلا، بازیابی شده در تاریخ (۱۵، ۹، ۱۳۹۷)، مجمع نمایندگان طلاب و فضایی حوزه علمیه قم، <http://mntqom.com/?p=5975>.
- داودی، فاطمه (۱۳۹۶)، «تأثیر تهدیدات مرتبط با جرائم سایبری بر امنیت ملی»، کنفرانس ملی پژوهش‌های نوین در مدیریت، اقتصاد و علوم انسانی، کازرون: دانشگاه آزاد اسلامی واحد کازرون.
- صادقی فسایی، سهیلا و عرفان‌منش، ایمان (۱۳۹۴)، «مبانی روش‌شناختی پژوهش اسنادی در علوم اجتماعی؛ مورد مطالعه: تأثیرات مدرن‌شدن بر خانواده ایرانی»، راهبرد فرهنگ، (۲۹) ۸، ۹۱-۶۱.
- فراهانی، احمد (۱۳۹۱)، «اثرات گسترش فناوری اطلاعات در توسعه روستایی (مورد: روستاهای استان خراسان جنوبی)»، اقتصاد فضا و توسعه روستایی، ۱ (۲)، ۷۹-۹۴.
- فرهادی پیرزینل بک، دانیال و محسنی دهکلانی، محمد (۱۳۹۸)، «اهمیت دفاع سایبری در اسلام»، دومین کنفرانس ملی پدافند سایبری، مراغه: دانشگاه آزاد اسلامی واحد مراغه.
- الفی، محمدرضا و بشارت، علی (۱۳۹۸)، «پایداری انقلاب اسلامی در مقابله با جنگ نرم و تهدیدات سایبری»، دومین کنفرانس ملی پدافند سایبری، مراغه: دانشگاه آزاد اسلامی واحد مراغه.

- قدسی، امیر (۱۳۹۲)، «تأثیر فضای مجازی بر امنیت ملی جمهوری اسلامی ایران و ارائه راهبرد (با تأکید بر ایفای نقش سرمایه اجتماعی)»، *راهبرد دفاعی*، ۱۱ (۴۴)، ۱۴۹-۱۸۶.
- کاویانی، ارشاد (۱۳۹۸)، «بررسی نقش شبکه‌های اجتماعی در جنگ نرم»، *دومین کنفرانس ملی پدافند سایبری*، مراغه: دانشگاه آزاد اسلامی واحد مراغه.
- کرم‌روان، فرمان (۱۳۹۸)، «تحلیل حقوقی سند راهبردی پدافند سایبری کشور»، *دومین کنفرانس ملی پدافند سایبری*، مراغه: دانشگاه آزاد اسلامی واحد مراغه.
- کریمی قهرودی، محمدرضا (۱۳۹۸). لزوم ورود مباحث فضای مجازی به ساختار الگوی ایرانی - اسلامی پیشرفت. بازیابی از ایکننا <http://iqna.ir/fa/news/3829745>
- کورکی نژاد، مجید (۱۳۹۴)، *تروریسم سایبری و راهکارهای افزایش امنیت سایبر در ایران با تأکید بر عملکرد ایالات متحده آمریکا*، پایان‌نامه کارشناسی ارشد دانشگاه تهران.
- مختاریان‌پور، مجید (۱۳۹۵)، «مدل فرایندی طراحی الگوی اسلامی ایرانی پیشرفت»، *الگوی پیشرفت اسلامی ایرانی*، ۴ (۸)، ۹-۳۰.
- میرمعزی، سید حسین (۱۳۹۷)، *سند الگوی اسلامی ایرانی پیشرفت*، ضربه کاری به دشمن بود، بازیابی شده در تاریخ (۲۰، ۹، ۱۳۹۷)، خبرگزاری حوزه، <http://www.hawzahnews.com/news/472162>.
- همایون، محمدساجد و هاشمی، محمدهادی (۱۳۹۶)، «جایگاه شبکه ملی اطلاعات در سپهر سیاست فرهنگی جمهوری اسلامی ایران»، *مطالعات راهبردی سیاست‌گذاری عمومی*، ۲۳.
- وکیلی، جهانگیر؛ کیانی، پدram و فرهنگ، رضا (۱۳۹۱)، *پدافند غیرعامل*، اصفهان: ذوب آهن اصفهان.
- Bailey, K. (2008), *Methods of social research*. Simon and Schuster.