تحلیل و بررسی سند الگوی اسلامی ایرانی پیشرفت از منظر فنّاوری اطلاعات و ارتباطات با رویکرد پدافند غیرعامل

علی اصغر سعدآبادی
استادیار گروه سیاست‌گذاری علم و فنّاوری دانشگاه شهید بهشتی. تهران. ایران.
A_sadabadi@sbu.ac.ir

زهره رحیمی راد
دکتری تخصصی سیاست‌گذاری علم و فنّاوری دانشگاه مازندران. بابلسر. ایران.
zrahimi.rad@gmail.com

کیارش فرتاش
استادیار گروه سیاست‌گذاری علم و فنّاوری دانشگاه شهید بهشتی. تهران. ایران.
k_fartash@sbu.ac.ir

محمد صادق خیاطیان یزدی
استادیار گروه سیاست‌گذاری علم و فنّاوری دانشگاه شهید بهشتی. تهران. ایران.
Khayatian@sbu.ac.ir

چکیده

با توجه به رشد سریع حوزهٔ فنّاوری اطلاعات و ارتباطات، این بخش به یکی از بسترهای بالقوهٔ آسیب‌پذیر و خطرناک مبدل شده است که همین امر بر اهمیت روزافزون توجه به پدافند غیرعامل در این حوزه صحه می‌گذارد. در این راستا، سند الگوی اسلامی ایرانی پیشرفت به‌عنوان نقشهٔ راه ۵۰ سال آیندهٔ کشورمان، باید بتواند تصویری واضح از آیندهٔ مطلوب ایران در این حوزه، به‌منزلهٔ یکی از بخش‌های کلیدی خود، ارائه دهد؛ ازاین‌رو، مطالعهٔ حاضر درپی آن است که با روش اسنادی موضوعات مرتبط با فنّاوری اطلاعات مطرح در این سند را با برش

• این مقاله با هماهنگی دبیرخانه دائمی کنگره بین‌المللی علوم انسانی اسلامی در نشریه مطالعات امنیت اقتصادی، شماره اول، پاییز ۱۳۹۹ منتشر شده است.

پدافند غیرعاملی ارزیابی کند تا بتواند راهگشـــای مسیر سیاست‌گذاران قرار گیرد. نتایج پژوهش حاضر نشـــان داد این ســـند، با توجه به اهمیت و چالش‌های پیش روی این حوزه، اصلاً نتوانسته است به آن بپردازد؛ به‌گونه‌ای که تنها در تدبیر شمارهٔ ۱۹ خود اشـــاره‌ای مبهم به این بخش داشته است که این امر با توجه به تهدیدهای سایبری، که به جد تمدن اســـلامی 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.

کلیدواژه‌ها: الگوی اسلامی ایرانی پیشرفت، پدافند غیرعامل، فناوری اطلاعات و ارتباطات.

۱. مقدمه

کشـــور ایران از دیرباز هم در منطقهٔ خاورمیانه و هم در کل جهان از موقعیتی راهبردی بهره‌مند بوده است؛ به همین دلیل، همیشه موردتهاجم کشورهای مختلف قرار داشته است. با تغییر رویکردهای بشر به سمت فنّاوری اطلاعات، سمت و سوی حرکت انسان به‌سوی فنّاوری نوین در فضای مجازی تغییر مسیر یافته است و با توجه به رشد سریع و درعین‌حال نامتوازن ساختار فنّاوری اطلاعات، این بستر به یکی از نقاط بالقوهٔ آسیب‌پذیر و خطرناک در جهان بدل شده است؛ به‌طوری‌که در ماهیت تهاجمات نیز تغییراتی پارادیمی رخ داده اســـت و بدین‌ترتیب، ضرورت توجه و پرداخت ســـریع و درعین‌حال معقول به‌منظور مصون‌سازی این بستر از تهدیدهای موجود در جهت حفظ امنیت ملی و حریم شـــخصی شهروندان در فضای جنگ و مخاصمات امروز بین‌المللی را می‌طلبد (وکیلی و همکاران، ۱۳۹۱، ص۴۱). امروزه کشـــورها نمی‌توانند در معادلات امنیتی و راهبردی خود از نقش فضای سایبری و تأثیر آن بر امنیت غافل شوند؛ به‌طوری‌که به اعتقاد بسیاری از متخصصان، امروزه جنگ ســـایبری از مهم‌ترین انواع تهدیدها به‌شـــمار می‌رود. جنگی که پیـــروزی در آن جز با دفاع هوشیاری و یاری آحاد ملت و متخصصان میسر نخواهد شد (برون، ۱۳۹۸، ص۱). در اهمیت این فضا همان بس که به فرمودهٔ رهبر انقلاب، فضای مجازی به‌اندازهٔ انقلاب اســـلامی اهمیت دارد؛ ازاین‌رو، لازم اســـت کشـــورها تـــدابیری را بـــرای مقابلـــه بـــا ایـــن تهدیدها اتخاذ کنند. در پاسخ به این ضـــرورت، پدافند غیرعامل در حوزهٔ فنّاوری اطلاعات و ارتباطـــات به‌منظور امنیت، ایمنی و پایداری زیرساخت‌های حیاتی کشور در مقابل تهدیدهای دشمن از این ناحیه شکل گرفته است.

در این راستا الگوی اسلامی ایرانی پیشرفت، به‌مثابه نقشهٔ راه ۵۰ سال آیندهٔ کشورمان، باید بتواند تصویری واضـــح از آیندهٔ مطلوب ایران ارائه کند و در ســـاختار این آینده فضای مجازی دیده شـــود؛ به‌طوری‌که اجرای این سند آسیب‌پذیری کشـــور در مقابل تهدیدهای دشمن را کاهش دهد و موجب تقویت مؤلفه‌های قدرت جمهوری اسلامی ایران شود، خاصه آنکه امنیت سایبری در ارتباط مستقیم با امنیت ملی کشور است و اگر حملات سایبری کشوری را تهدید کند درواقع، امنیت ملی کشور را تهدید کرده اســـت؛ ازاین‌رو، بازدارندگی سایبری لازمهٔ ادامهٔ فعالیت زیرساخت‌های حیاتی در شرایط کنونی است. اما درحال‌حاضر، بحث فنّاوری اطلاعات و فضای مجازی، به‌جز اشاره‌ای مبهم در یک تدبیر، جایگاه به‌خصوصی در این الگو ندارد. درحالی‌که هرگونه نقش‌آفرینی مؤثر و مواجههٔ فعال و هوشمند با این پدیده در گرو شناخت ابعاد و زوایای تأثیرگذاری این پدیده بر آیندهٔ کشور و به‌ویژه امنیت آن است و بدون درک و شناخت هرچه کامل‌تر جایگاه و نحوهٔ مواجهه با آن، نتیجهٔ مطلوب حاصل نخواهد شد. با توجه به آنکه تهدیدهای سایبری یکی از چند حوزهٔ تخصصی مرتبط با پدافند غیرعامل است؛ ازاین‌رو، مطالعهٔ حاضر درپی آن اســـت که موضوع‌های مرتبط با فنّاوری اطلاعات مطرح در این سند را با برش پدافند غیرعاملی ارزیابی کند و سپس تدابیر اصلاحی و پیشنهادی خود را ارائه دهد.

۲. روش پژوهش

جهت‌گیری اصلی پژوهش حاضر، کاربردی و هدف آن اکتشـــافی اســـت که با اســـتراتژی مطالعهٔ موردی و به‌کارگیری روش اســـنادی به بررسی سند الگوی اســـلامی ایرانی پیشرفت از منظر توجه به فنّاوری اطلاعات و ارتباطات پرداخته اســـت. روش اسنادی یکی از مهم‌ترین ابزارهای تحقیق، به‌ویژه در تحقیق موردی، محسوب می‌شود. روش اسنادی را تحلیل آن دسته از اسنادی می‌دانند که شـــامل اطلاعات دربارهٔ پدیده‌هایی است که قصد مطالعهٔ آن‌ها را داریم (Bailey, 2008, p.276). این روش مســـتلزم جست‌وجویی توصیفی و تفسیری اســـت و پژوهشگر درپی آن 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 نویســـنده بپذیرد و مورداســـتناد قرار دهد (صادقی و عرفان‌منـــش، ۱۳۹۴)؛ بنابراین، در این روش پژوهشگر تلاش می‌کند تا با اســـتفادهٔ نظام‌مند از داده‌های اسنادی به کشف، استخراج، طبقه‌بندی و ارزیابی مطالب مرتبط با موضوع پژوهش خود اقدام کند.

شـــیوهٔ کار در این پژوهش نیز بدین صورت بوده اســـت که ابتدا ســـند الگوی اســـلامی ایرانی پیشـــرفت، به‌منزلهٔ یک مورد، مطالعه شد و ســـپس بخش‌های آرمان‌ها، رسالت، افق و تدابیر، که

به‌صورت عام یا خاص به موضوع مطالعــه یعنی فنّاوری اطلاعات و ارتباطات مرتبط بودند، مورد بحث و بررســی قرار گرفتند. در ادامه، مبتنی‌بر تحلیل اولیهٔ صورت‌گرفته، ســه تدبیر برای تقویت سند الگو از منظر فنّاوری اطلاعات و ارتباطات پیشنهاد شد. همچنین، سعی شد تدابیر پیشنهادی دربردارندهٔ اصول حاکم بر پدافند ســایبری کشور مستخرج از سند راهبردی پدافند سایبری کشور باشد و این اصول مبنای عمل قرار گیرند.

۳. نقد و ارزیابی اجمالی سند الگوی پایه در محور فنّاوری اطلاعات و ارتباطات

همان‌گونه که اعلام شده است (میرمعزی، ۱۳۹۷؛ حســینی‌نژاد، ۱۳۹۷)، الگوی اسلامی ایرانی پیشرفت سند بالادســتی همهٔ اسناد برنامه‌ای کشور خواهد بود؛ اسناد برنامه‌ای اعم از چشم‌انداز، سیاست‌های کلی، برنامه‌های کلی پنج‌ساله و سالانه است؛ ازاین‌رو، این الگو باید جامعیتی داشته باشــد که بتوان ذیل آن، برنامه‌های مختلف را منســجم کرد. تاکنون اســناد بالادستی مختلفی در حوزهٔ فنّاوری اطلاعات و ارتباطات تدوین شــده است که ازجملهٔ آن‌ها می‌توان به سند چشم‌انداز بیست‌ســاله، سیاســت‌های کلی برنامهٔ ششم توسعه، سیاست‌های کلی شــبکه‌های اطلاع‌رسانی رایانه‌ای، راهبردهای کلان ارائهٔ خدمات اطلاع‌رســانی و اینترنت در کشور، برنامهٔ توسعه و کاربری فنّاوری ارتباطات و اطلاعات ایران (تکفا)، سند راهبردی نظام جامع فنّاوری اطلاعات کشور، سند راهبردی جامعهٔ اطلاعاتی ایران، سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور (افتا)، سیاست‌های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات، نقشهٔ مهندسی فرهنگی کشور، حکم تشکیل شورای عالی فضای مجازی ازسوی مقام معظم رهبری و حکم نصب اعضای جدید شورای عالی فضای مجازی ازسوی ایشان اشاره کرد. پیش از ورود به بحث، ذکر این نکته ضروری اســت که ارزیابی‌های صورت‌گرفته در این تک‌نگاشت برمبنای آرمان‌های انقلاب اسلامی، قانون اساسی، اسناد بالادســتی، که پیش‌تر ذکر شد، و شرایط کنونی و آتی کشورمان در حوزهٔ بین‌الملل و همچنین، سیاســت‌های کلان اعلامی پدافند غیرعامل و ســند راهبردی پدافند سایبری خواهد بود. در این راســتا، مطابق با یافته‌های همایون و هاشمی (۱۳۹۶)، می‌توان سیاست‌های معطوف به فنّاوری اطلاعات و فضای مجازی در کل اســناد بالادســتی را، که بر اهمیت این موضوع صحه خواهد گذاشت، 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؛

- سیاســت‌های مربوط به توســعهٔ جامعهٔ شــبکه‌ای 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 ملاحظهٔ موارد بالا، که نشــانگر توجه به حوزهٔ فنّاوری اطلاعات و ارتباطات در اسناد بالادســتی پیشین است، مشاهده می‌شــود که سند الگوی اسلامی ایرانی پیشــرفت تنها در تدبیر شــمارهٔ ۱۹ (پی‌ریزی و گسترش نهضت کسب و کار هنرهای نمایشی و کاربردهای فضای مجازی با اســتفاده از میراث فرهنگی و ادبی ایرانی اســلامی و قابلیت‌های ملــی و محلی مطابق تقاضا و پســند مخاطب منطقه‌ای و جهانی) اشاره‌ای مبهم به این بخش داشته است. این اشارهٔ گذرا و مبهم این ســؤال را از پدیدآورندگان ســند به‌وجود می‌آورد که به نظر ایشان، آیا فضای سایبری که سبک زندگی، امنیت، توسعهٔ بازارها و بسیاری بخش‌های دیگر از جامعهٔ بشری، حتی بخش‌های صنعتی و اقتصادی، در جهان امروز مبتنی‌بر آن شــده اســت، واقعاً یک فضای غیرواقعی و مجازی است؟ و آیا باورشــان این است که میزان اهمیت فضای سایبر در الگوی پیشرفت، به اندازهٔ همین عباراتی که در بند نوزدهم آمده اســت، کفایت می‌کند؟ (پورسینا، ۱۳۹۷). توجه به این نکته لازم است که گرچه یک سند بالادستی امکان توجه به جزئیات حوزه‌های مختلف را ندارد، باید به‌گونه‌ای تدوین شــود که هر حکم آن جامعیت لازم را داشته باشد و بتواند اهداف و ابزارهای سیاست‌گذاری را در خود بگنجاند، اما این ســند، با توجه به اهمیت و چالش‌های پیش روی این حوزه، اصلاً نتوانســته اســت به این موضوع بپردازد که با توجه به تهدیدهای سایبری، که به جد تمدن اسلامی ایرانی را به خطر خواهد انداخت، این امر نشــان از مفروضات و انگاشته‌های نادرست سند دارد. برای مثال، برخی از تهدیدات سایبری پیش روی کشورمان به شرح زیر است:

۱. تشکیل قرارگاه فرماندهی دفاع سایبری توسط امریکا؛
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 دشــمن بر فضای اینترنت و سایبری دنیا اعم از شبکه، اطلاعات، مراکز نگهداری داده، تولیدکنندگان اصلی سخت‌افزارها و نرم‌افزارها و خدمات؛
۴. وجود توافق‌های ضد امنیتی اعلام‌نشــده بین برخی کشورها علیه جمهوری اسلامی ایران در فضای سایبر؛

۵. امکان تعبیهٔ حفرهٔ امنیتی مخفی (دروازهٔ پشـــتی) در تجهیزات فروخته‌شده به ایران توسط سازندگان مربوط؛
۶. امکان و سابقهٔ حملهٔ سایبری به شبکه‌های کشور؛
۷. ممانعت از فروش برخی از سامانه‌های سایبر به بهانهٔ تحریم‌های بین‌المللی به ایران؛
۸. رویکـــرد و اســـتراتژی‌های تهاجمی دشـــمنان در اســـتفاده از توان ســـایبری خود برعلیه زیرساخت‌های حیاتی کشور که بر سایبر متکی هستند؛
۹. اعمال حاکمیت دشمن با اســـتفاده از فضای حقوق بین‌الملل سایبر بر شبکه‌های جهانی ازقبیل اینترنت، شبکه‌های ماهواره‌ای وغیره؛
۱۰. فقدان نظام حقوق بین‌المللی در حوزهٔ دفاع سایبری (جلالی فراهانی و میررفیع، ۱۳۹۸: ص۲۷۲).

نکتهٔ دیگر اینکه در افق ۱۴۴۴ ســـند الگو به‌گونه‌ای نوید داده شده است که در همهٔ بخش‌های آن تهدید یا خطری وجود نخواهد داشـــت؛ ازاین‌رو، در این ســـند، امنیت، استقلال و قدرت کامل برای دفاع بازدارنده به‌عنوان ســـه ویژگی برجســـتهٔ کشـــور و از مفاهیم کلیدی آن است که البته هر ســـهٔ این مفاهیم پیوند تنگاتنگی با امنیت ســـایبری دارند. بر این اســـاس، باید به این مهم در متن ســـند تأکید شود؛ ازاین‌رو، با توجه به اینکه تدابیر در راســـتای آرمان‌ها و افق و رسالت سند اتخاذ می‌شـــوند، به‌نظر می‌رســـد لحاظ عبارت «برخـــوردار از فنّاوری دفاع بومی برتـــر» در بخش افق ســـند در این راستا راهگشـــا خواهد بود. به‌طور کلی، برخوردار‌بودن از فنّاوری بومی در حوزه‌های زیرساخت‌های اطلاعاتی و شبکه امکان نفوذناپذیری و کاهش آسیب‌پذیری آن‌ها را فراهم می‌آورد، قید «بومی» نیز به این دلیل اســـت که فنّاوری غیربومی و وابســـته درصورت پیشرفته‌بودن هم برای دشـــمن قابل نفوذ خواهد بـــود؛ بنابراین، بازدارندگی ایجاد نخواهد کرد (احدی و شـــاه‌محمدی، ۱۳۹۸، ص۲۴۵). همچنین، گنجاندن عبارت «آمادگی دفاعی» در بخش آرمان‌ها در دســـتیابی به این هدف راهگشاســـت. آمادگی دفاعی به‌منزلهٔ یک اصل کلی در آیهٔ ۶۰ سورهٔ انفال نیز به‌صورت آموزه‌ای دســـتوری به مسلمانان سفارش شده است که شـــامل فراهم‌آوری توان و نیرو است. توان شـــامل هرگونه ابزار و آلات بازدارنده، هجومی یا دفاعی است؛ ازاین‌رو، تنها به سلاح اشاره نشده اســـت. تهیهٔ هر چیزی که قدرت امت و دولت را افزایش می‌دهد، امری ضروری است و با توجه به شرایط مکانی و زمینی 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

کشـــور، چنان اهمیت و ارزشی دارد که آن را نشـــانهٔ ایمان دانسته است و این موضوع با مبانی سند نیز کاملاً منطبق اســـت (احدی و شـــاه‌محمدی، ۱۳۹۸). ازآنجاکه 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 دشـــمن حفظ کند (فرهادی پیرزینل بک و محســـنی دهکلانی، ۱۳۹۸: ص۱).

نکتهٔ دیگر، که لحاظ آن به‌ویژه در فنّاوری‌های نوین همچون فضای مجازی ضروری اســـت، آن اســـت که به منظور دستیابی به پیشـــرفت مدنظر ما در دنیای واقعی، باید ابتدا این دنیای واقعی به‌درســـتی ترسیم شـــود؛ برای مثال، ابتدا ضمن آسیب‌شناسی اســـناد برنامه‌ای از منظر چگونگی تدوین و الگوی پارادایمی آن‌ها تأثیر این برنامه‌ها بر وضعیت فرهنگی، اقتصادی، سیاســـی کشور طی سال‌های هدف واکاوی شـــود و بر این مبنا، سناریوهای محتمل آینده شناسایی و ترسیم شود. ســـپس باید رســـالت ایران جهت نقش‌آفرینی در وضعیت کنونی جهان مشخص شود که البته این امر نیز با بررســـی و تبیین وضعیت در بخش‌هـــای مختلفی چون فرد، خانواده و جامعهٔ ایران و ذیل فعالیت‌های آینده‌پژوهانه میســـر می‌شـــود (مختاریان‌پور، ۱۳۹۵: ص۱۵) که با توجه به اینکه در ســـند الگو توجهی به اهمیت فضای مجازی نشده، مشخص است که این مسیر و آینده‌شناسی در آن نیز لحاظ نشده اســـت. به‌طور کلی، تصویرسازی و الگوسازی جامعهٔ آینده از دغدغه‌های مهم کشورهای پیشـــرو در عرصهٔ جهانی است. این کشورها عموماً به تصویرسازی جامعهٔ آرمانی خود در افق‌های زمانی مشـــخصی اقدام کرده و ســـپس برای تحقق این تصاویر، علاوه‌بر گفتمان‌سازی گســـترده، به تهیهٔ برنامه‌ها و نقشه‌های راه کلان ملی اقدام کرده‌اند، به‌گونه‌ای که همهٔ ارکان مختلف در قالـــب یک نظام منســـجم، منابع خود را بـــرای این تغییر پارادایم و ایفـــای نقش در تمدن نوین آینده بســـیج می‌کنند. در عرصهٔ فضای ســـایبر نیز وضعیت به همین منوال است؛ درواقع، ویژگی مشترک اســـناد کشورهای پیشرفتهٔ دنیا در این حوزه این‌گونه اســـت که یک تصویرسازی واضح از آینده صورت می‌دهند، تصاویر آینده را مبتنی‌بر فضای ســـایبر ترسیم می‌کنند، بین ارکان حکمرانی خود بر تصویر آینده اجماع حاصل می‌کنند و ســـپس راهبری الگوهای پیشرفت حاصل‌شده را در بالاترین سطوح حاکمیت خود پیگیری می‌کنند. به‌طور کلی، کشورهایی که فاقد تصویری از آیندهٔ خود باشند، در آینده منزوی خواهند شد. در این راستا الگوی ایرانی اسلامی پیشرفت نیز باید بتواند تصویـــری واضح از آیندهٔ مطلوب ایران ارائه کند؛ به‌گونه‌ای که در ســـاختار آن فضای مجازی دیده شـــود (کریمی قهرودی، ۱۳۹۸). برخی تصاویر و چشم‌اندازهای آتی کشورهای پیشتاز جهان که

به‌خوبی به این عرصه توجه کرده‌اند، عبارت‌اند از:

- ژاپن: جامعهٔ پنجم (Society 5.0) یا جامعه اَبَرهوشمند؛
- مالزی: مالزی پیشـــرفتهٔ ۲۰۵۰ و جوامع هوشمند (Smart Communities): کشور مالزی در برنامهٔ خود برای ســـال ۲۰۵۰ سه شاخص افزایش شـــادی، خلاقیت و نوآوری و رشد اقتصادی را مبنا قرار داده است که در تحقق همهٔ این‌ها فضای سایبری محور است.
- اتحادیهٔ اروپا به‌ویژه کشور آلمان: جامعهٔ شـــبکه‌محور مشارکتی و انقلاب چهارم صنعتی (Industry 4.0)؛
- امریکا: اینترنت اشـــیای صنعتی (IIoT) و تولید پیشرفته (Advance Manufacturing) و هوشمند؛
- سنگاپور: ملت هوشمند (Smart Nation)؛
- چین: جامعهٔ ســـایبری‌ـفیزیکی‌ـاجتماعی، ساخت چین ۲۰۲۵ (Made in China 2025) و ابرقدرت برتر تولید در ۲۰۴۹): کشور چین سه برنامهٔ ده‌ساله در راستای تحقق آنچه برای سال ۲۰۴۹ ـ که صدمین سالگرد تأســـیس جمهوری خلق چین است ـ مدنظر دارد تدوین کرده است و می‌کوشد با این برنامه جامعه را به یک فضای سایبری‌ـفیزیکی‌ـصنعتی 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 نمی‌شـــود مگر آنکه فنّاوری‌های دیجیتالی امنیت سایبری داشته باشند.

نکتهٔ دیگری که باز هم در این ســـند به آن بی‌توجهی شده این است که فضای مجازی، همچون شمشـــیری دو لبه از یک‌ســـو، نه‌تنها ســـاختارهای فرهنگی، اجتماعی و امنیتی کشورها را با تهدید جدی مواجه کرده اســـت؛ ازسوی دیگر، فرصت‌های ارزشـــمندی را برای معرفی قابلیت‌های آن‌ها میســـر می‌کند؛ ازایـــن‌رو، علاوه‌بر آنکه می‌توان از ظرفیت عالی فضای مجازی در راســـتای تحقق الگو و دفاع از آرمان‌های انقلاب اســـلامی نهایت استفاده را برد و با به‌کارگیری بهینه از فنّاوری‌های اطلاعاتی، که اینترنت از مهم‌ترین مصادیق آن است، زمینهٔ تحقق اهداف فرهنگی نظام و سند الگو را فراهم کرد، این فضا به‌عنوان ابزاری در خدمت تهاجم فرهنگی و جنگ نرم دشـــمن، امنیت ملی کشـــور را موردهدف قرار می‌دهد و این موضوع اهمیت مدیریت فضـــای مجازی را برای پایداری انقلاب اسلامی نشان می‌دهد.

بر این اســاس، بــا توجه به اهمیت حفظ امنیــت ملی به‌مثابه مهم‌ترین مؤلفهٔ ثبات کشــور و تأثیرپذیری مستقیم امنیت ملی از تهدیدات سایبری، اگر کشوری در چشم اندازها و اسناد بالادستی خود به فکر حفظ حریم‌های فضای ســایبری خود نباشد به هیچ عنوان نمی‌توان آن را در معادلات جهانی جزء کشورهای قدرتمند به‌حساب آورد.

۴. ارائهٔ پیشنهادات و تدابیر در محور فنّاوری اطلاعات و ارتباطات

در این بخش با توجه به نقد و ارزیابی صورت‌پذیرفته در بخش قبل، تدابیر پیشنهادی ارائه می‌شود. در این قسمت سعی شده اســت تا تدابیر پیشنهادی منطبق با تعریف مرکز الگو یعنی «تصمیمات و اقدامات اساسی» و با توجه به افق پنجاه‌ســاله باشد. ضمناً تلاش شده است تا تدابیر پیشنهادی دربردارندهٔ اصول حاکم بر پدافند ســایبری کشور مستخرج از سند راهبردی پدافند سایبری کشور باشد و این اصول مبنای عمل قرار گیرند. این اصول نه‌گانه عبارت‌اند 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 تشــریح هر تدبیر، پیشــنهاد مؤلفهٔ پدافندی آن نیز مشخص شده است. سه تدبیر پیشنهادی این تک‌نگاشت به شرح زیر است:

- گسترش بهره‌گیری از فرصت‌ها و صیانت از آسیب‌ها و تهدیدهای فضای مجازی متناسب با هویت دینی، ملی و ارزش‌های جامعه؛
- ایجاد و راه‌اندازی شبکهٔ ملّی اطلاعات به‌منزلهٔ زیرساخت ارتباطی فضای مجازی کشور؛
- بهبود و توســعهٔ دسترســی امن و پایدار همهٔ مردم به امکانات ارتباطی و اطلاع‌رسانی در چهارچوب ضوابط فرهنگی کشور.

۴ـ۱. تدبیر پیشنهادی ۱: گسترش بهره‌گیری از فرصت‌ها و صیانت از آسیب‌ها و تهدیدهای فضای مجازی متناسب با هویت دینی، ملی و ارزش‌های جامعه

پیدایـــش فنّاوری‌های ارتباطاتی و اطلاعاتیْ فرصت‌ها و تهدیدهای انقلاب را چنان برجســـته کرده اســـت که استمرار و تکامل انقلاب اسلامی منوط به توجه خاص و جدی و سرمایه‌گذاری نظام در این زمینه اســـت. همان‌گونه که یکی از نکات کلیدی، که رهبر معظم انقلاب همواره به آن اشـــاره می‌کنند، اهمیت بالای فضای ســـایبر است؛ تا جایی که این جمله از ایشان نقل شده است که «اگر امروز رهبر انقلاب نبودم حتماً رئیس فضای مجازی کشـــور می‌شـــدم». در این راستا رهبر معظم انقلاب اینترنت را فرصتی فوق‌العاده توصیف می‌کنند و همواره مخاطب را از تهدیدانگاری صرف به آن برحذر می‌دارند. ایشـــان در سال ۱۳۸۴ در ســـخنانی فرموده‌اند: «امروزه اینترنت و ماهواره و وسایل ارتباطی بسیار متنوعی وجود دارد و حرف، آسان به همه‌جای دنیا می‌رسد. میدان افکار مردم و مؤمنان، عرصهٔ کارزار تفکرات گوناگون اســـت. امروز ما در میدان جنگ و کارزار حقیقی فکری قرار داریم. این کارزار فکری به‌هیچ‌وجه به زیان ما نیست، به سود ماست».

به‌طور کلی، امروزه تمامی ســـرمایه‌ها و زیرساخت‌های ســـایبری و یا متکی بر سایبر به‌وسیلهٔ تهدیدهای تخصصی و از جنس ســـایبر در معرض خطر قرار گرفته‌اند، به‌طوری‌که با آســـیب‌دیدن این ســـرمایه‌ها، مجموعه‌ای از پیامدهای اقتصادی، اجتماعی، سیاســـی، نظامـــی، امنیتی وغیره برای کشـــور به‌بار خواهد آمد؛ ازطرفی، جنگ ســـایبری به‌دلیل نفوذ و گســـترش فضای سایبر، بر ســـایر جنگ‌های جدید مانند جنگ اقتصادی تأثیرگذار اســـت. همچنین، گسترهٔ پدافند غیرعامل به‌دلیل وجود تهدیدهای مختلف در حوزه‌های گوناگون گســـترش یافته است و در این راستا، نیل به اهداف کلان پنج‌گانهٔ پدافند غیرعامل کشـــور مستلزم توجه یکپارچه و همه‌جانبه به همهٔ حوزه‌های کارکردی پدافند غیرعامل است (جلالی فراهانی و میررفیع، ۱۳۹۸: ص۲۶۰). همان‌گونه که رهبر معظم انقلاب فرموده‌اند، این فضا مملو از فرصت و تهدید اســـت. در ادامه به برخی از تهدیدات و فرصت‌ها اشاره خواهد شد.

- **ارتقای ســـرمایهٔ اجتماعی و تقویت قدرت ملی با استفاده از شبکه‌های اجتماعی مجازی:** هرچند سند الگوی پایهٔ اسلامی ایرانی پیشرفت در افق ۱۴۴۴ هجری شمسی، تصویری از جامعهٔ مطلوب و پاســـدار ارزش‌ها، هویت ملی و میراث انقلاب اسلامی ارائه داده است، یکی از ملزومات دســـتیابی به اهداف ترسیم‌شدهٔ این ســـند، داشتن برنامه‌ریزی صحیح و درک کامل و مؤثر از قدرت نرم اســـت. در این میان مشارکت، اعتماد، شبکه‌ها و نهادهای

اجتماعی، وفاداری مردم به حاکمیت و افزایش مشروعیت سیاسی و در یک کلام، افزایش سرمایهٔ اجتماعی نقشی بسیار مهم در قدرت نرم دارد (جهان‌بین و امامی، ۱۳۹۳: ص۴۹). ازسوی دیگر، با دقت در شاخص‌های سرمایهٔ اجتماعی، به‌خوبی می‌توان دریافت که یکی از هدف‌های مهم جنگ نرم، تزلزل در مؤلفه‌های ذکرشده است. به‌گونه‌ای که اگر به اعتماد بین افراد و حکومت خدشـــه وارد شود، شـــالوده‌های آن جامعه سست می‌شود و آن کشور در معرض ناامنی قرار می‌گیرد. بر این اســـاس، لازمهٔ مقابلـــه با جنگ نرم، برخورداری از قدرت نرم اســـت که از ابزارهای اساســـی آن امکان بازتولید سرمایهٔ اجتماعی در لایه‌های مختلف اســـت. در این میان، شبکه‌های اجتماعی بستری مناســـب برای ایجاد مشارکت افراد و اقشار مختلف جامعه فراهم کرده اســـت (قدسی، ۱۳۹۲: ص۱۸۳). به‌طور کلی، مشارکت اجتماعی در کشور بر سه گروه مؤثر است:

۱. ایرانیان داخل مرزهای جغرافیایی؛

۲. ایرانیان خارج از کشور؛

۳. دوستداران و علاقه‌مندان ایران.

- **جنگ نرم در حوزهٔ سایبر:** مقام معظم رهبری دربارهٔ اهمیت جنگ نرم و لزوم ارائهٔ راهکار در این رابطه می‌فرمایند: «اگر دشمن با تولید محتوا (کتاب، فیلم، عکس، سایت‌های اینترنتی وغیره) ســـعی کند اعتقادات مردم را نشانه بگیرد ـ که گرفته است ـ این یک نوع آفند است و البته بســـیار هم خطرناک اســـت و مقولهٔ 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 شـــیوه‌ها اثر نکند و آســـیب‌پذیری به حداقل ممکن برسد؟». به‌طور کلی، جنگ نرم و تهدیدهای ســـایبری یکی از مهم‌ترین چالش‌های پیش روی انقلاب اسلامی است. این مســـئله یکی از مؤثرترین و پیچیده‌ترین تهدیدهایی اســـت که پایداری انقلاب اسلامی را به مخاطره می‌اندازد؛ ازاین‌رو، لازم اســـت بازدارندگی در مقابل آن مورد توجه ســـند الگو قرار گیرد، چراکه غفلت از آن می‌تواند خســـارات جبران‌ناپذیری بر پیکر انقلاب اسلامی وارد کند. در این جنگ، دشمن درصدد است بدون استفاده از حملهٔ نظامی و با استفاده از شـــیوه‌های مختلف، به تسخیر اذهان و افکار عمومی بپردازد و با فروپاشی تدریجی فکری و روانی مردم، زمینه را برای براندازی انقلاب اسلامی فراهم کند (الفی و بشارت، ۱۳۹۸، ص۱). جنگ نرم یکی از مهم‌ترین جلوه‌های تهدیدآفرین امنیت ملی جمهوری اســـلامی

ایران اســـت. در این راستا اسناد رســـمی در گزارش اخیر اندیشکدۀ CSIS[1] نشان می‌دهد که تحلیلگران این اندیشکده در پیشـــنهادی عملیاتی به دولت امریکا می‌گویند: می‌توانید ایران را با قدرت نرم به زانو درآورید. اســـنادی همانند این مـــورد، بیانگر این واقعیت مهم هستند که فعالیت‌های سایبری علیه ایران ازطرف اپوزیسیون‌های مختلف از اتاق‌های فکر امریکایی‌ها و به دســـتور مستقیم آن‌ها صورت می‌پذیرد؛ بنابراین، بسیار ساده‌لوحانه است که اقدام‌های دشـــمنان در عرصۀ جنگ نرم را اقدام‌هایی ســـطحی و فاقد عقبۀ علمی فرض کرد. به یقین، موفقیت در این فضا، مرهون کوشـــش‌های متفکران و حمایت‌های گســـتردۀ نظام ســـلطۀ نوین جهانی در قالب اتاق‌های فکر قدرتمند است؛ ازاین‌رو، برخورد اساسی ازطریق مقابله‌به‌مثل میســـر اســـت و اســـتفاده از روش‌های غیرعلمی و منفعلانه به نتیجه نخواهد رسید (قدسی، ۱۳۹۲: ص۱۵۱).

بهره‌برداری از فضای مجازی در جنگ نرم، در جهت کســـب منافع بیشـــتر برای صاحبان قدرت است که این موضوع در گذشته با جنگ رودررو انجام می‌شد. در این بین رسانه‌های مجازی درحال تبدیل‌شـــدن به امپراتوری‌های بزرگ در عصر جدید هستند. تا پیش از این، اگر منطق پیروزی در جنگ‌های ســـنتی برخورداری بیشـــتر از نیروها و ابزارآلات فیزیکی بود، بدون شک پیدایش محیط مجازی باعث تشکیک اساسی در این منطق شده است. این فضا قدرتی را به‌وجود آورده و بسیاری از عرصه‌های تقابل را از گذشته متفاوت کرده است. شـــبکه‌های اجتماعی به‌علت قابلیت جذب مخاطبان به یکی از ابزارهای تأثیرگذار جنگ تبدیل شده‌اند و سعی می‌کنند با استفاده از مؤلفه‌هایی چون تغییر افکار و نگرش‌ها اهداف خود را در کشـــورها اجرایی کننـــد (کاویانی، ۱۳۹۸: ص۱). درحال‌حاضر، شـــبکه‌های اجتماعی همچون تلگرام، اینستاگرام، واتساپ، فیس بوک و توییتر در میان کاربران ایرانـــی محبوبیـــت بیشتری دارند. براساس آمارهای ســـایت آماری الکسا،[2] در سال ۱۳۹۳ تعداد کـــاربران ایرانـــی تلگرام ۲۲ میلیون نفر بود که در فاصلۀ بین سال‌های ۱۳۹۳ تا ۱۳۹۵ این تعداد به بیش از ۴۵ میلیون کاربر رسید. این آمار علاوه‌بـــر اینکـــه بیـــانگر اســـتقبال بســـیار

۱.«CSIS» به‌عنوان اندیشـــکدۀ رتبۀ اول در جهان در میان اندیشـــکده‌های دفاع و امنیت ملی و رتبۀ چهارم بهترین اندیشکده‌ها با بیشترین ایده‌ها/ پیشنهادهای نوآورانه معرفی شده است.

2. Alexa

بـــالای کاربران ایرانی از شبکه‌های اجتماعی در ســـال‌های اخیر است، نشان می‌دهد که این شبکه‌ها به همان میزان که فرصت‌های ویژه‌ای را در تسهیل ارتباطات اجتماعی ممکن مـی‌کنند، بـــه همان میزان نیز می‌توانند فضایی برای ارتکاب انواع جرایم سایبری باشند. براساس گزارش پلیس فتا، در ســـال ۱۳۹۵ نزدیک به ۶۰ درصد جرایم سایبری در تلگرام شکل گرفتـــه است کـه در ایـــن بـــین، جـــرایم اخلاقـــی بـــا ۳۷ درصـــد، بـــالاترین حجـــم آمار را بـــه خـــود اختصاص داده‌اند. همچنین، این شبکه‌ها بستر انواع آسیب‌های اجتماعی و فرهنگی ازقبیـــل تضـعیف ارتباط صمیمی در کانون خانواده، اخـتلال در امر آموزشـــی و افت تحصیلی دانش‌آموزان و دانشـــجویان، اعتیاد اینترنتـــی، انواع انحراف و سوءاستفاده‌های جنسی در میان نوجوانان و جوانـــان و حتی تضعیف هویت دینی و ملی برای مخاطبان و کـــاربران ایـــن شبکه‌ها را به دنبال داشته است. امروزه ابزارهای نظارت ســـنتی دیگر باید جای خود را به شـــیوه‌ها و ابزارهای جدیدی دهند که با توانمندســـازی مخاطبان در مقابل آثار ســـوء رســـانه‌ها به آن‌ها مصونیت بیشتری ببخشـــند و مخاطب منفعل را به مخاطب گزینشگر مبدل کنند؛ به‌نحوی‌که خود فرد نیز می‌تواند رژیم مصرف رسانه‌ای خود را تنظیم کند (اکبرزاده و همکاران، ۱۳۹۷).

- **تهدیدهای ســـایبری:** تهدید امنیت ملی می‌تواند ســـطح زندگی شهروندان را با خطر افت مواجه کند؛ به‌طوری‌که حمله به هر کدام از ســـاختارهای امنیتی در ســـطوح مختلف ملی و بین‌المللی، تهدیدی نوین و ویرانگر علیه امنیت کشـــور اســـت کـــه می‌تواند موجبات فروپاشی و نابودی زیرســـاخت‌های حیاتی و بنیانی جامعه شود (داوودی، ۱۳۹۶: ص۱). در این رابطه رهبر معظم انقلاب نیز می‌فرمایند: «تنها راه مقابله با تهدیدها این اســـت که وضعیت داخلی به‌گونه‌ای سامان‌دهی شود که دشمن از پیروزی خود مطمئن نباشد و زمینه را برای ماجراجویی فراهم نبیند».

در این راستا، تهدیدهای ســـایبری متنوعی در کشورهای مختلف احصا و تجزیه و تحلیل شـــده است که از آن میان می‌توان به سرقت اطلاعات تجاری و بیمه‌ای و بهداشتی، تهدید ســـایبری برهم‌زدن اقتصاد کشور، ورشکستی شـــرکت‌های بزرگ، اخبار جعلی به منظور عملیات روانی در شبکهٔ اجتماعی، بدافزارهای بانکی در تلفن همراه، اینترنت اشیا در حمل و نقل عمومی تجهیزات پزشـــکی و دوربین‌های مداربسته، استفاده از تروریست، اخاذی سایبری، عدم آشـــکاری آسیب‌پذیری، الگوریتم مبهم، تهدید کشـــتی‌ها و زیردریایی‌ها،

تهدیـــد در صنایع نفت و گاز، ســـلاح‌های اتوماتیک، ربات قاتل، حملات به تأسیســـات هسته‌ای، حملات به تأسیسات مخابراتی، کنترل جریان نفت، انجام معاملات مالی اشاره کرد.

کشـــور ما نیز جزء کشـــورهایی اســـت که بیشـــترین حملات تروریســـتی ســـایبری را به زیرســـاخت‌های مالی، هسته‌ای و نظامی خود متحمل می‌شـــود و هر لحظه ممکن است زیرســـاخت‌های فنّاوری اطلاعات و شبکه‌های ارتباطی در سامانه‌های رایانه‌ای کشور، که اصطلاحاً به‌عنوان ســـرمایهٔ ملی سایبری تلقی می‌شـــوند، ازطریق تهدید سایبری تخریب شـــود یا اطلاعات آن‌ها افشا یا به‌علت دسترســـی غیرمجاز مختل شود. به‌ثمر نشستن هر کدام از این حملات می‌تواند نتایج فاجعه‌باری برای امنیت و ســـلامت کشـــور و ملت به همراه داشته باشد؛ ازاین‌رو، هم باید امنیت فضای سایبر در کشور را ارتقا دهیم و هم بتوانیم با تقویت مکانیسم‌های امنیتی در بعضی موارد حتی مقابله‌به‌مثل کنیم (کورکی‌نژاد، ۱۳۹۴: ص۹۵)؛ بنابراین، با لحاظ اســـتراتژی بازدارندگی ســـایبری و برای جلوگیری از خطرات ذکرشده، نظام جامع پدافند کشور باید طوری طراحی و ایجاد شود که ازطریق رصد، پایش و مدیریت و کنترل به هنگام، تهدید و تهاجم ســـایبری دشمن را خنثی و از زیرساخت‌های فنّاوری اطلاعات کشور محافظت کند (کرم روان، ۱۳۹۸: ص۱).

- **وابســـتگی به خارج از کشـــور در حوزه‌های نرم‌افزاری و ســـخت‌افزاری:** یکی از شیوه‌های بازدارندگی در حوزهٔ سایبر، ســـرمایه‌گذاری و بومی‌سازی تجهیزات مرتبط با جهان سایبر است. برای استفاده از تجهیزات سایبری در بخش‌های ویژهٔ حیاتی و حساس کشور همیشه بایـــد با نگاه بدبینانه به این تجهیزات نگریســـت؛ زیرا این تجهیـــزات منفذ ورود اقدامات بعدی اســـت و بیشترین آســـیب‌های وارد در حوزهٔ سایبری ناشـــی از استفاده از تجهیزات و فنّاوری‌های وارداتی بدون توجه به بومی‌ســـازی متناســـب با شرایط کشور است. با رشد تصاعدی فراگیرشدن فنّاوری اطلاعات در سیستم‌های دولتی و خصـــوصـــی و افزایش روزافزون خدمات و ســـرویس‌های ارائه‌شـــده به اقشـــار مختلف جامعه در بســـتر فنّاوری اطلاعات، چنانچه به زیرســـاخت‌های بومـــی و ابزارهای امنیتی بومی توجه جدی صـــورت نپذیرد، با گذر زمان وابســـتگی جامعه به خدمات الکترونیک بیشـــتر و ازطرفی، وابســـتگی زیرساخت‌های ســـرویس‌دهندگان به صاحبان اصلی تکنولوژی این صنعت در خارج از کشـــور نیز بیشتر خواهد شد. بدون شـــک با تکیه به ابزارها و تجهیزاتی که ساختهٔ

کشورهای بیگانه اســت، هیچ‌گاه نمی‌توان امنیت کامل را برقرار کرد؛ زیرا در لایهٔ فیزیکی امنیت وابســتگی وجود دارد و در شــرایط مختلف، ازجمله به‌روزرسانی، امکان اختلال و سوءاســتفاده وجود خواهد داشت؛ ازاین‌رو، باید زیرســاخت‌های حوزهٔ سایبر در زمینهٔ ســخت‌افزار و نرم‌افزار با استفاده از ظرفیت‌های بومی تکمیل و تقویت شود و درحدامکان از استفاده از فنّاوری‌های غیربومی پرهیز شود.

اگرچه ممکن اســت ســاخت نمونهٔ بومی در کشــور، در همهٔ زمینه‌ها، مقرون‌به‌صرفه نباشد و ورود یــک کالا به داخل هزینه و زمــان کمتری را برای ما به ارمغان بیــاورد، قطعاً در درازمدت می‌توان نتایج مثبت و مهمی را در این زمینه به‌دست آورد. مقامات وزارت دفاع امریکا نیز، باوجود اینکه این کشــور یکی از اصلی‌ترین تولیدکنندگان تجهیزات دیجیتالی به‌حساب می‌آید، مدتی قبل اعلام کردند که در تلاش هســتند با همکاری شــرکت‌های فنّاوری و دانشــمندان فعال این حوزه، معماری‌های سخت‌افزاری کاملاً متفاوتی را برای تراشه‌های به‌کاررفته در تجهیزات نظامی طراحی کنند؛ زیرا نمونه‌های فعلی تقریباً حالتی عمومی دارد و دشــمنان آن‌ها با مهندســی معکوسشــان می‌توانند آســیب‌پذیری یا راهکار نفوذ را شناسایی کنند. به‌نظر می‌رسد تجمیع تمام توان و نیروی موجود و سازمان‌دهی و یکپارچه‌سازی دانش در زمینهٔ دفاع سایبری، راهکاری مطمئن برای افزایش بازدارندگی ســایبری باشد که درصورت ایجاد چنین ساختاری بر پایهٔ دانش بومی، راهی برای نفوذ بیگانگان باقی نخواهد ماند (پدافند سایبری، ۱۳۹۷).

با توضیحاتی که ارائه شــد، نتیجهٔ تحقق تدبیر پیشــنهادی آن اســت که کشور به‌جای غافلگیرشدن، همواره در مواجهه با پدیده‌های نوظهور اجتماعی در این حوزه و توسل‌جستن به اقدام‌های سلبی و منفعلانه و وابستگی به تجهیزات خارجی، به بازیگری فعال، آینده‌پژوه و آینده‌ساز تبدیل می‌شود؛ ازاین‌رو، با توجه به توضیحات ذکرشده، این تدبیر اصول پدافندی مندرج در جدول زیر را پوشش می‌دهد.

جدول۱. اصول پدافندی گنجانده‌شده در تدبیر پیشنهادی ۱

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

۴ـ۲. تدبیر پیشنهادی ۲: ایجاد و راه‌اندازی شبکهٔ ملی اطلاعات به‌مثابه زیرساخت ارتباطی فضای مجازی کشور

همان‌گونه که رهبر معظم انقلاب در ده وظیفه و مأموریت شورای عالی فضای مجازی بیان کرده‌اند (پایگاه اطلاع رسانی دفتر مقام معظم رهبری،۱۳۹۸)، تسریع در راه‌اندازی شبکهٔ ملی اطلاعات پس از تصویب طرح آن در شورای عالی و نظارت مستمر و مؤثر مرکز ملی بر مراحل راه‌اندازی و بهره‌برداری از آن یکی از وظایف این شورا اعلام شد.

طبق تعریفی که شورای عالی فضای مجازی در مصوبهٔ جلسهٔ پانزدهم خود در ۳/ ۱۰/ ۱۳۹۲ مشخص کرده است، شبکهٔ ملی اطلاعات «به‌عنوان زیرساخت ارتباطی فضای مجازی کشور، شبکه‌ای مبتنی‌بر قرارداد (پروتکل) اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده‌ای است؛ به‌صورتی‌که درخواست‌های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز دادهٔ داخلی نگهداری می‌شوند به‌هیچ‌وجه ازطریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت و خصوصی و امن داخلی در آن فراهم شود»؛ بنابراین، شبکهٔ ملی اطلاعات، به‌منزلهٔ زیرساخت ارتباطی فضای مجازی کشور، یکی از مهم‌ترین پروژه‌های ملی محسوب می‌شود که تحقق آن بنا بر رویکردهای جهانی و ضرورت‌های ملی، مانند ارائهٔ 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 تهدیدهای امنیتی و حریم خصوصی لازم شده است.

اهمیت شبکهٔ ملی اطلاعات در حدی است که مقام معظم رهبری نیز بارها بر لزوم ایجاد شبکهٔ 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، مسئلهٔ شبکهٔ ملی اطلاعات است»، تأکید کردند: «امروز فضای مجازی مخصوص ما نیست و همهٔ دنیا با فضای مجازی درگیرند و کشورهایی که شبکهٔ ملی اطلاعات درست کرده و فضای مجازی را به نفع خودشان و ارزش‌های موردنظر خودشان کنترل کرده‌اند، یکی‌دوتا نیستند. متأسفانه در زمینهٔ شبکهٔ ملی اطلاعات در کشور کوتاهی شده و کاری که باید انجام گیرد، انجام نگرفته است».

به عقیدهٔ اکثر صاحب‌نظران نیز یکی از ضروری‌ترین و مهم‌ترین سرمایه‌گذاری‌های توسعهٔ شبکه‌ها و فنّاوری اطلاعات در هر کشوری، طراحی و اجرای سامانه‌های کاملاً امن و حفاظت اطلاعات است که به‌مثابه یک سرمایه و اعتبار ملی به‌حساب می‌آید. برای مثال، با توجه به نبود شبکهٔ ملی اطلاعات و ارتباطات برای مرتبط‌شدن مراکز ثقل به یکدیگر، متأسفانه دیده شده است

در مواقعی از بستر اینترنت استفاده می‌شـــود که این موضوع باعث آغاز تهدیدهای سایبر در حوزهٔ شبکه است.

علاوه‌بر این‌ها، شبکهٔ ملی اطلاعات به‌عنوان یک طرح کلان و اساسی در حوزهٔ فنّاوری اطلاعات و ارتباطات بستری است که می‌توان بر مبنای آن به پیشبرد سیاست‌های فرهنگی جمهوری اسلامی ایران در این فضا پرداخت؛ چنانچه در اســناد بالادستی مختلف دیگر نیز توجه ویژه بر ایجاد نظام جامع اطلاعات و ارتباطات در کشــور و به‌طور خاص، شــبکهٔ ملی اطلاعات مشــاهده می‌شود. این موضوع علاوه‌بر اینکه جایگاه مهم شــبکهٔ ملی اطلاعات در عرصهٔ سیاســت کشــور را اثبات می‌کند، بیانگر نقش کلیدی این شبکه در فراهم‌ســازی بسترهای لازم جهت پیشبرد سیاست‌های فرهنگی کشــور در این عرصه اســت؛ به بیان دیگر، بدون راه‌اندازی کامل شــبکهٔ ملی اطلاعات نمی‌توان سیاســت‌های مربوط به اســتفاده از فرصت‌های فضای مجازی و صیانت از تهدیدهای آن، سیاســت‌های حمایتی در قبال ظرفیت‌های مردمی داخل کشور، سیاست‌های مربوط به توسعهٔ جامعهٔ شبکه‌ای و ایجاد فرصت‌های برابر و عادلانه در دسترسی به خدمات شبکه را برای آحاد مردم ایجاد کرد (همایون و هاشــمی، ۱۳۹۶: ص۱۱۳). با توجه به توضیحات ذکرشده، این تدبیر اصول پدافندی مندرج در جدول زیر را پوشش می‌دهد.

جدول۲. اصول پدافندی گنجانده‌شده در تدبیر پیشنهادی ۲

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

۴ـ۳. تدبیر پیشنهادی ۳: بهبود و توسعهٔ دسترسی امن و پایدار همهٔ مردم به امکانات ارتباطی و اطلاع‌رسانی در چهارچوب ضوابط فرهنگی کشور

پیدایش فنّاوری‌های ارتباطاتی و اطلاعاتی، فرصت‌ها و تهدیدهای انقلاب را چنان برجســته کرده اســت که استمرار و تکامل انقلاب اسلامی منوط به توجه خاص و جدی و سرمایه‌گذاری نظام در این زمینه اســت و همین مسئله یکی از دلایلی است که حوزهٔ فضای مجازی را در نظر رهبر معظم به اندازهٔ خود انقلاب اسلامی پراهمیت کرده است.

امروزه شاخص‌های گسترش فنّاوری اطلاعات به‌مثابه یکی از شاخص‌های توسعه‌یافتگی محسوب می‌شــود. هر کشوری بتواند ضریب نفوذ این فنّاوری را در میان شــهروندان خود افزایش دهد، از

فواید متعدد آن در حوزه‌های مختلف بهره‌مند می‌شـــود. به موازات اســـتفاده از فنّاوری اطلاعات و ارتباطات در تمامی ابعاد حیات بشـــری، جهان به‌ســـرعت درحال تبدیل به یک جامعهٔ اطلاعاتی اســـت؛ همچنین، فنّاوری اطلاعات به‌منزلهٔ عمده‌ترین محور تحول و توسعهٔ 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 فنّاوری اطلاعات و ارتباطات استفاده می‌کنند.

بنابرایـــن، با توجه به اهمیت پیش‌گفته، حوزهٔ ارتباطات کشـــور به‌مثابه سلســـله اعصاب و نقش تعیین‌کننده‌اش در ادارهٔ امور کشـــور بسیار حساس و حیاتی اســـت و در اولویت‌های تهاجم دشمن قرار خواهد داشت. دشمن برای فلج‌کردن کشور، اولین موج‌های شدید تهاجمی خود را چه به لحاظ ســـخت‌افزاری و یا نرم‌افزاری متوجه این حوزه خواهد کرد. در پاسخ به این ضرورت، پدافند غیرعامل در حوزهٔ فنّاوری اطلاعات و ارتباطات و جنگ سایبر به منظور امنیت، ایمنی و پایداری زیرساخت‌های حیاتی کشور در مقابل تهدیدهای دشـــمن از ناحیهٔ فنّاوری اطلاعات و ارتباطات شکل گرفته است. اما اقدام مناســـب در حوزهٔ پدافندی امنیت فنّاوری اطلاعات و ارتباطات منوط به شـــناخت صحیح آن اســـت. به‌طور کلی، تأمین و حفظ امنیت فنّاوری اطلاعات به محورهای محرمانگی، جامعیت، دســـترس‌پذیری و عدم انکار اشـــاره دارد. محرمانگی به معنا و مفهوم حفاظت داده‌های سیستم‌های رایانه‌ای در برابر دسترســـی‌های غیرمجاز، جامعیت یا یکپارچگـــی به مفهوم تأمین دقت و جامعیت اطلاعات و نرم‌افزارهای رایانه‌ای، دسترسی یا دسترس‌پذیری به مفهوم ضمانت دسترسی به اطلاعات و خدمات حساس در زمان موردنیاز و عدم انکار تبادل اطلاعات است.

در این راســـتا پدافند غیرعامل در حوزهٔ فاوا به معنای توسعهٔ امن زیرساخت‌ها و رعایت اصول پدافند غیرعامل در مراکز فاوا به منظور ارتقای ضریب امنیت، ایمنی و پایداری اســـت. از مهم‌ترین مأموریت‌های پدافند غیرعامل در فاوا می‌توان موارد زیر را نام برد:

- ایجاد و حفظ امنیت زیرساخت‌های حوزهٔ فنّاوری اطلاعات و ارتباطات در برابر مخابرات محتوایی؛
- ایمنی زیرساخت‌های حوزهٔ فنّاوری اطلاعات و ارتباطات در قبال حملات فیزیکی؛
- پایداری زیرساخت‌های حوزهٔ فنّاوری اطلاعات و ارتباطات در مواجهه با تهدیدها و ادامهٔ مأموریت در شرایط بحران؛

- صیانت از زیرساخت‌های حوزهٔ فنّاوری اطلاعات و ارتباطات در مقابل حملات غیرمترقبه، بلایای طبیعی و مواقع اضطراری؛
- ارتقا و توسعهٔ عزم ملی، باور و فرهنگ عمومی و سازمانی درخصوص رعایت اصول پدافند غیرعامل (استتار، اختفا، پوشش، پراکندگی، استحکام بنا، فریب وغیره) در حوزهٔ فنّاوری اطلاعات و ارتباطات کشور؛
- تولید دانش فنی و بومی و بهره‌گیری آگاهانه از فنّاوری مناسب و روزآمد کشور درخصوص دفاع غیرعامل فاوا به‌وسیلهٔ توسعهٔ جهاد علمی؛
- کاهش آسیب‌پذیری زیرساخت‌های کلیدی و مراکز حیاتی، حساس و مهم کشور در حوزهٔ فنّاوری اطلاعات و ارتباطات در برابر تهدیدها و اعمال ملاحظات، سیاست‌ها و ضوابط خاص پدافند غیرعامل در حوزهٔ فنّاوری اطلاعات و ارتباطات در برنامه‌های در دست مطالعهٔ کشور؛
- تدوین معماری کلان پدافند غیرعامل فنّاوری اطلاعات و ارتباطات کشور (وزارت فنّاوری اطلاعات و ارتباطات، ۱۳۹۸).

با توجه به توضیحات ذکرشده، این تدبیر اصول پدافندی مندرج در جدول زیر را پوشش می‌دهد.

جدول ۳. اصول پدافندی گنجانده‌شده در تدبیر پیشنهادی ۳

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

۵. جمع‌بندی

امروزه کشورها نمی‌توانند در معادلات امنیتی و راهبردی خود از نقش فنّاوری اطلاعات و ارتباطات و تأثیر آن بر امنیت خود غافل شوند. ازاین‌رو، 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 همهٔ اسناد برنامه‌ای کشور و همچنین، نقشهٔ راه ۵۰ سال آیندهٔ کشورمان، باید بتواند تصویری واضح از آیندهٔ مطلوب ایران در این بخش ارائه دهد؛ به‌طوری‌که اجرای این سند آسیب‌پذیری کشور در مقابل تهدیدهای دشمن را کاهش دهد و موجب تقویت مؤلفه‌های قدرت جمهوری اسلامی ایران شود. مطالعهٔ حاضر، که با روش اسنادی صورت گرفت، نشان داد که سند الگوی اسلامی ایرانی پیشرفت تنها در تدبیر شمارهٔ ۱۹

یعنی «پی‌ریزی و گســترش نهضت کسب و کار هنرهای نمایشــی و کاربردهای فضای مجازی با اســتفاده از میراث فرهنگی و ادبی ایرانی اسلامی و قابلیت‌های ملی و محلی مطابق تقاضا و پسند مخاطب منطقه‌ای و جهانی» اشــاره‌ای مبهم به این بخش داشته است. در افق سند الگو به‌گونه‌ای نوید داده شــده است که در همهٔ بخش‌های کشور ایران تهدید یا خطری وجود نخواهد داشت. این درحالی است که امنیت، اســتقلال و قدرت کامل برای دفاع بازدارنده به‌عنوان سه ویژگی برجستهٔ کشــور پیوند تنگاتنگی با امنیت سایبری دارند؛ ازاین‌رو، در متن سند باید به این مهم تأکید جدی شود. علاوه‌براین، فنّاوری اطلاعات نه‌تنها این پتانسیل را دارد که ساختارهای فرهنگی، اجتماعی و امنیتی کشورها را با تهدید جدی مواجه کند، بلکه فرصت‌های ارزشمندی را برای بروز قابلیت‌های یک کشور میسر می‌کند؛ ازاین‌رو، علاوه‌بر آنکه می‌توان از ظرفیت عالی فضای مجازی در راستای تحقــق الگو و دفاع از آرمان‌های انقلاب اســلامی نهایت اســتفاده را برد و بــا به‌کارگیری بهینه از فنّاوری‌هــای اطلاعاتی ازجمله اینترنت به‌عنوان مهم‌ترین مصداق آن، می‌توان زمینهٔ تحقق اهداف فرهنگی نظام و ســند الگو را نیز فراهم آورد. در انتها نیز ســه تدبیر به شرح زیر برای رفع خلأهای سند الگو پیشنهاد شد:

- گسترش بهره‌گیری از فرصت‌ها و صیانت از آسیب‌ها و تهدیدهای فضای مجازی متناسب با هویت دینی، ملی و ارزش‌های جامعه؛
- ایجاد و راه‌اندازی شبکهٔ ملی اطلاعات به‌منزلهٔ زیرساخت ارتباطی فضای مجازی کشور؛
- بهبود و توســعهٔ دسترســی امن و پایدار همهٔ مردم به امکانات ارتباطی و اطلاع‌رسانی در چهارچوب ضوابط فرهنگی کشور.

کتابنامه

۱. احدی، محمد؛ شاه‌محمدی، محمد. ۱۳۹۸. «**طرح راهبردی دفاع سایبری جمهوری اسلامی ایران در حوزهٔ بازدارندگی**». مطالعات بین‌رشــته‌ای دانش راهبردی. دورهٔ ۸. شــمارهٔ ۳۱. صص ۲۵۲ـ۲۲۵.

۲. اکبرزاده، علیرضا؛ معمار، ثریا؛کوثری، مسعود؛ همتی، رضا. ۱۳۹۷. «**رویکرد مخاطب‌محور در مواجهه با شبکه‌های اجتماعی مجازی**». نشریهٔ رسانه و فرهنگ. شمارهٔ ۱۶. صص ۱۹ـ۱.

۳. الفی، محمدرضا؛ بشــارت، علــی. ۱۳۹۸. «**پایداری انقلاب اســلامی در مقابله با جنگ نرم و تهدیدات سایبری**». دومین کنفرانس ملی پدافند سایبری. مراغه: دانشگاه آزاد اسلامی واحد مراغه.

۴. برون، مهرداد. ۱۳۹۸. «**امنیت و دفاع سایبری**». دومین کنفرانس ملی پدافند سایبری. مراغه: دانشگاه آزاد اسلامی واحد مراغه.
۵. پایگاه اطلاع رسانی دفتر مقام معظم رهبری. ۱۳۹۸. «**۱۰ وظیفه و مأموریت شورای عالی فضای مجازی در دوره جدید / تسریع در راه‌اندازی شبکه ملی اطلاعات**». بازیابی شده در تاریخ۱۳۹۸/۷/۲۵ از https://www.leader.ir/fa/content/13542.
۶. پدافند سایبری. ۱۳۹۷. «**تقویت زیرساخت‌های بومی‌سایبری، تقویت سپر دفاعی کشور**». بازیابی از قرارگاه پدافند سایبری کشور https://www.papsa.ir.
۷. پورسینا، بهروز. ۱۳۹۷. «**چند پرسش اساسی از پدیدآورندگان سند الگوی پیشرفت**». بازیابی شده در تاریخ۱۳۹۸/۷/۲۵ از روزنامهٔ مردم‌سالاری: http://newspaper.mardomsalari.ir/4719/page/1/47000.
۸. جلالی فراهانی، غلامرضا؛ میررفیع، علی. ۱۳۹۸. «**ارائهٔ راهبردهای پدافند غیرعامل کشور در برابر تهدیدات سایبری**». فصلنامهٔ مطالعات دفاعی استراتژیک. دورهٔ ۱۷. شمارهٔ ۷۵.
۹. جهان‌بین، فرزاد؛ امامی، اعظم. ۱۳۹۳. «**سرمایهٔ اجتماعی حلقهٔ ارتباطی قدرت نرم، امنیت نرم، تهدید نرم**». دوفصلنامه علمی پژوهشی مطالعات قدرت نرم. دورهٔ ۴. شمارهٔ ۱۰. صص ۴۹_۷۴.
۱۰. حسینی‌نژاد، سید اکبر. ۱۳۹۷. «**نقد، نظر و بررسی سند الگوی اسلامی ایرانی پیشرفت در جمع نمایندگان طلاب و فضلا**». بازیابی‌شده در تاریخ ۱۵/ ۹/ ۱۳۹۷. مجمع نمایندگان طلاب و فضلای حوزهٔ علمیهٔ قم: http://mntqom.com/?p=5975.
۱۱. داودی، فاطمه. ۱۳۹۶. **تأثیر تهدیدات مرتبط با جرایم سایبری بر امنیت ملی، کنفرانس ملی پژوهش‌های نوین در مدیریت، اقتصاد و علوم انسانی**. کازرون: دانشگاه آزاد اسلامی واحد کازرون.
۱۲. صادقی فسایی، سهیلا؛ عرفان‌منش، ایمان. ۱۳۹۴. «**مبانی روش‌شناختی پژوهش اسنادی در علوم اجتماعی؛ مورد مطالعه: تأثیرات مدرن‌شدن بر خانوادهٔ ایرانی**». فصلنامهٔ علمی‌پژوهشی راهبرد فرهنگ. دورهٔ ۸. شمارهٔ ۲۹. صص ۹۱-۶۱.
۱۳. فراهانی؛ احمد، فال سلیمان؛ محمود، حجی پور؛ محمد، حق دوست؛ ناهید، فلزی ؛ مرتضی. ۱۳۹۱. «**اثرات گسترش فنّاوری اطلاعات در توسعهٔ روستایی (مورد: روستاهای استان خراسان جنوبی)**». اقتصاد فضا و توسعهٔ روستایی. سال اول. شمارهٔ ۲. صص ۹۴_۷۹.
۱۴. فرهادی پیرزینل بک، دانیال؛ محسنی دهکلانی، محمد. ۱۳۹۸. «**اهمیت دفاع سایبری در**

اسلام». دومین کنفرانس ملی پدافند سایبری. مراغه: دانشگاه آزاد اسلامی واحد مراغه.
۱۵. قدسی، امیر. ۱۳۹۲. «**تأثیر فضای مجازی بر امنیت ملی ج. ا. ایران و ارائهٔ راهبرد (با تأکید بر ایفای نقش سرمایهٔ اجتماعی)**». راهبرد دفاعی. دورهٔ ۱۱. شمارهٔ ۴۴. صص ۱۸۶ـ۱۴۹.
۱۶. کاویانی، ارشاد. ۱۳۹۸. «**بررسی نقش شبکه‌های اجتماعی در جنگ نرم**». دومین کنفرانس ملی پدافند سایبری. مراغه: دانشگاه آزاد اسلامی واحد مراغه.
۱۷. کرم روان، فرمان. ۱۳۹۸. «**تحلیل حقوقی سند راهبردی پدافند سایبری کشور**». دومین کنفرانس ملی پدافند سایبری. مراغه: دانشگاه آزاد اسلامی واحد مراغه.
۱۸. کریمی قهرودی، محمدرضا. ۱۳۹۸. «**لزوم ورود مباحث فضای مجازی به ساختار الگوی ایرانی اسلامی پیشرفت**». بازیابی شده در تاریخ ۱۳۹۸/۷/۲۵ از ایکنا http://iqna.ir/fa/news/3829745.
۱۹. کورکی‌نژاد، مجید. ۱۳۹۴. «**تروریسم سایبری و راهکارهای افزایش امنیت سایبر در ایران با تأکید بر عملکرد ایالات متحدهٔ امریکا**». پایان‌نامهٔ کارشناسی ارشد حقوق بین‌الملل. تهران: دانشگاه تهران.
۲۰. مختاریان‌پور، مجید. ۱۳۹۵. «**مدل فرایندی طراحی الگوی اسلامی ایرانی پیشرفت**». دوفصلنامهٔ علمی‌پژوهشی الگوی پیشرفت اسلامی ایرانی. دورهٔ ۴. شمارهٔ ۸. صص ۳۰ـ۹.
۲۱. میرمعزی، سید حسین. ۱۳۹۷. «**سند الگوی اسلامی ایرانی پیشرفت، ضربهٔ کاری به دشمن بود**». بازیابی‌شده در تاریخ ۲۰/ ۹/ ۱۳۹۷. خبرگزاری حوزه: http://www.hawzahnews.com/news/472162.
۲۲. وزارت فنّاوری اطلاعات و ارتباطات. ۱۳۹۸. « **پدافند غیرعامل در حوزهٔ فناوری اطلاعات و ارتباطات** ». بازیابی شده در تاریخ ۱۳۹۸/۷/۲۵ از https://kurdestan.ict.gov.ir.
۲۳. وکیلی، جهانگیر؛ کیانی، پدرام؛ فرهت، رضا. ۱۳۹۱. **پدافند غیرعامل**. اصفهان: ذوب آهن اصفهان.
۲۴. همایون، محمد ساجد؛ هاشمی، محمد هادی. ۱۳۹۶. «**جایگاه شبکهٔ ملی اطلاعات در سپهر سیاست فرهنگی جمهوری اسلامی ایران**». فصلنامهٔ مطالعات راهبردی سیاست‌گذاری عمومی. شمارهٔ ۲۳.
25. Bailey, K. 2008. **Methods of social research**. New York: The Free Press.