

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دولت سیزدهم و حاکمیت سایبرنتیک جمهوری اسلامی



۱۴۰۰/اردیبهشت/۲۵

فهرست

۱مقدمه
۳فضای سایبر: چیستی و چرایی
۴شاخصه‌های کیفی فضای سایبر مطلوب انقلاب اسلامی
۵مدیریت کلان فضای سایبر
۵کنترل جوامع از طریق کنترل فضای سایبر
۷نقش جدی فضای سایبر در دولت سیزدهم
۸الف) فرصت‌ها
۸ب) تهدیدات
۸(۱) حریم شخصی
۹(۲) زیرساخت‌های حساس
۹(۳) باور عمومی جامعه
۱۰پ) آسیب‌ها

مقدمه

قوی شدن کشور جزء هدف‌های ما است... ابعاد قوت ابعاد وسیعی است... امروز قوت در فضای مجازی حیاتی است؛ امروز فضای مجازی حاکم بر زندگی انسان‌ها است در همه‌ی دنیا؛ و قوت در این [زمینه] حیاتی است.^۱

امام خامنه‌ای

بر اساس مطالعات صورت گرفته، فضای سایبر^۲ به‌عنوان مهم‌ترین، راهبردی‌ترین و مؤثرترین حوزه‌ی حاکمیتی در عصر حاضر مطرح است به‌گونه‌ای که راهبردهای کنترل افکار عمومی و شناخت ملت‌های جهان از این طریق، در سال‌های اخیر به اصلی‌ترین گزاره‌ی تسلط و اشراف بر جهان از سوی دولت‌های استکباری تبدیل شده است. در این بین، سایر کشورها تلاش نموده‌اند تا با استقلال مدیریتی فضای سایبری ملی‌شان از فضای سایبر بین‌الملل، ضمن ارتباط با فضای سایبر جهان بتوانند ملت‌هایشان را از تهاجمات نرم، عقیدتی، فرهنگی و سایر آسیب‌های متأثر از فضای سایبر حفظ نمایند.

این در حالی است که جنبه‌های حاکمیتی و راهبردی فضای سایبر در جمهوری اسلامی ایران، آنطور که شایسته بوده و مورد تأکید امام جامعه نیز می‌باشد، شناخته نشده و به این مقوله‌ی بی‌بدیل صرفاً از حیث فتنی نگریسته می‌شود. این خطای راهبردی باعث شده تا کشور با عقب‌ماندگی جدی در کنترل فضای سایبر به‌نفع ارزش‌های ایرانی - اسلامی مواجه شود و تهدیدات و آثار منفی ناشی از آن، تمامی لایه‌های حاکمیت و همچنین ملت شریف ایران را در برگیرد.

بررسی‌های تکمیلی برای مشخص شدن علت خطای مذکور، چنین می‌نمایاند که مسئولان ذی‌ربط در بخش‌های مختلف -بالاخص قوه‌ی مجریه- با مبانی فلسفی و نظری که فضای سایبر بر آنها بنا گشته آشنا نبوده و عمدتاً تحت تأثیر مشاورانی هستند که علی‌رغم دلسوزی و دغدغه‌مندی برای نظام و انقلاب، فاقد بینش عمیق نظری در شناخت، تصمیم‌سازی و طرح‌ریزی صحیح و همه‌جانبه نسبت به فضای سایبر هستند. این در حالی است که شرط اصلی تحول در تمامی مسائل حاکمیتی، تحول نظری و سپس عملی نسبت به فضای سایبر ملی است به‌نحوی که رویکرد آن کاملاً بومی بوده و صرفاً به حوزه‌ی فتنی و تقلید از پروتکل‌ها و استانداردهای بین‌المللی محدود نگردد. از این رو متن حاضر سعی دارد ضمن معرفی

^۱ بیانات در سخنرانی نوروزی؛ ۳ فروردین ۱۳۹۹

^۲ Cyber Space

ماهیت و چیستی فضای سایبر از منظر نقش حاکمیتی آن، به تبیین و توصیف آثار فضای سایبر بر کنترل جوامع، جایگاه بی‌بدیل این فضا در دولت سیزدهم جمهوری اسلامی ایران و همچنین کلیات و رئوس برنامه‌ی عملیاتی برای تحول فضای سایبر به‌نحوی که شاخصه‌های بومی شدن آن لحاظ شود، بپردازد؛ ان شاء الله.

فضای سایبر: چیستی و چرایی

فضای سایبر که به ظاهر فضای فنی تلقی شده و جنبه‌های حاکمیتی آن مغفول واقع شده است، در اصل فضایی است که ابتناء بر دانش سایبرنتیک^۳ دارد. دانش سایبرنتیک نیز مبتنی بر مراجع و منابع اصلی آن، دانشی نوین است که اصالت آن بر مفهوم آگاهی و اطلاعات است و در طرح‌ریزی حاکمیت، جامعه را از طریق تسلط بر جریان اطلاعات، کنترل می‌نماید. به عبارت دیگر، حاکمیت بر جامعه در عصر سایبرنتیک، به جای آنکه اصالت را به منابع فیزیکی بدهد، منابع اطلاعاتی را از طرق مختلف در اختیار گرفته و با جریان‌سازی در حوزه‌های مختلف، افکار جامعه را نسبت به مسائل مد نظر حاکمیت هدایت و مدیریت می‌نماید. لذا دانش سایبرنتیک را می‌توان باز تعریف نوینی از قدرت نرم دانست.

حال برای تحقق نظریات تدوین شده در این دانش، یک فضای عملیاتی و کاملاً واقعی مورد نیاز است که بتواند حاکمیت اطلاعاتی را بر جامعه ایجاد نموده، توسعه دهد و در نهایت تثبیت نماید که این فضا، فضای سایبر نام دارد. نکته‌ی مهم این است که فضای سایبر در هر عصر بر اساس میزان پیشرفت دانش و تکنولوژی، منطبق با شرایط عصر خود بوده است. به عنوان مثال زمانی به نشریات مکتوب و جراید روزانه، فضای سایبر گفته می‌شد و امروز به پیشرفته‌ترین ابزار و وسایل و زیرساخت‌های ارتباطی نظیر اینترنت اطلاق می‌شود.

در نتیجه تمامی کشورهایی که اهمیت فضای سایبر و نقش بی‌بدیل آن را در تحقق حاکمیت از یک سو و تقابل با تهدیدات راهبردی دشمنان از سویی دیگر درک کرده‌اند، برای بومی‌سازی، استقلال و مدیریت داخلی فضای سایبر ملی‌شان اقدامات متعدد انجام داده‌اند؛ اقداماتی که از عالی‌ترین سطوح نظری تا نازل‌ترین مباحث فنی، پیوسته است. ولی امر مسلمین بارها و بارها بر این مهم تأکید نموده‌اند، از جمله در سخنرانی نوروزی سال ۱۴۰۰ فرمودند:

متأسفانه در فضای مجازی کشور ما هم که آن رعایت‌های لازم با وجود این همه تأکیدی که من کردم صورت نمی‌گیرد و در یک جهاتی واقعاً ول است. همه‌ی کشورهای دنیا روی فضای مجازی خودشان دارند اعمال مدیریت می‌کنند، [در حالی که] ما افتخار می‌کنیم به اینکه ما فضای مجازی را ول کرده‌ایم! این افتخار ندارد. فضای مجازی را بایستی مدیریت کرد!^۴

^۳ Cybernetics

^۴ بیانات در سخنرانی نوروزی؛ ۱ فروردین ۱۴۰۰

لذا تلاش جدی در دولت سیزدهم باید بر این باشد که بومی‌سازی، استقلال و مدیریت داخلی فضای سایبر کشور را به معنی واقعی کلمه و در هر دو حوزه‌ی مبانی نظری و راهکارهای عملی و فنی طرح‌ریزی و اجرا نماید.

شاخصه‌های کیفی فضای سایبر مطلوب انقلاب اسلامی

فضای سایبر مطلوب انقلاب اسلامی، نه آن‌نگاهی است که صرفاً به دنبال مسدودسازی منابع و سرویس‌های مختلف است و صرفاً روش سلبی را برگزیده، نه حاصل این تفکر اشتباه است که اعتقاد دارد هر آنچه در جهان رایج است و پذیرش دارد، در جمهوری اسلامی ایران نیز باید مقبول واقع شود؛ بلکه از تبیین شاخصه‌های کیفی که ابتناء بر نگرش اسلامی - ایرانی دارند به دست آمده است.

به لطف خداوند متعال، طی سال‌ها مطالعه‌ی نظری و عملی، شاخصه‌های کیفی فضای سایبر انقلاب اسلامی بر اساس نگاه و گفتمان امام خامنه‌ای تبیین و استحصال شده است که کلیات آن در سه حوزه‌ی

۱. ضرورت‌ها

۲. بایدها و نبایدها (ایجاب و سلب)

۳. کاربردها و روش‌ها

به صورت اینفوگرافی ارائه شده است (پیوست شماره ۱).

بر این اساس فضای سایبر مطلوب انقلاب اسلامی، فضایی است که توانمندی مدیریت کشور را از حیث اطلاعاتی و افکار عمومی دارا است که در این راستا باید از مطالب علمی و متقن و شیوه‌های نوین انتقال فکر استفاده نموده و گزاره‌هایی نظیر حمایت از اقدامات واقعی حاکمیت در جامعه، ابتناء بر طرح‌ریزی راهبردی در سطح کلان، وحدت‌آفرینی، کنترل جریان اطلاعات به نفع ارزش‌های دینی و ملی، ممانعت از قرارگیری مسائل فرعی به جای مسائل اصلی، مؤثر در فرهنگ‌سازی، انتقال‌دهنده‌ی نظرات مردم نسبت به حاکمیت، متصل‌کننده‌ی کمپین‌های ملی و دینی به یکدیگر و نهایتاً حمایت واقعی از کاربران را به صورت جامع و کامل، عملیاتی و محقق کند.^۵

^۵ گزاره‌های مطرح شده تماماً بر اساس صراحت بیانات ولی‌امر مسلمین از سال ۱۳۷۹ تا سال ۱۴۰۰ ه.ش است.

مدیریت کلان فضای سایبر

در حال حاضر مدیریت کلان فضای سایبر، بر عهده‌ی شورای عالی فضای مجازی است که متشکل است از اعضای حقوقی و حقیقی که باید در راستای منویات و دستورات امام جامعه، سیاست‌های فضای سایبر را تدوین و ابلاغ کنند. اما از آنجا که فضای سایبر، سازنده‌ی افکار و اعتقادات جامعه بوده و بر فرد به فرد ملت مؤثر است، کوچک‌ترین اشتباه در جهت‌دهی به آن، تبعات سنگین و بعضاً جبران‌ناپذیری در پی خواهد داشت. از این رو در تمامی کشورهایی که فضای سایبر بومی و ملی خودشان را ایجاد کرده‌اند، کنترل کلان فضای سایبر در اختیار عالی‌ترین سطح حاکمیت قرار گرفته است.

این مهم در بیانات امام خامنه‌ای نیز به صراحت، چنین مطرح شده است:

سیاست‌گذاری [فضای مجازی] کار شخص رهبری است. سیاست‌گذاری در این حوزه فقط کار رهبری است و رئیس‌جمهور مجری است. ما باید با تکیه بر معارف اسلامی و تکیه بر قواعد جمهوری اسلامی، بتوانیم سیاست‌گذاری کنیم.^۶

از قیاس آنچه ولی‌امر مسلمین فرمودند و وضعیت فعلی شورای عالی فضای مجازی چنین بر می‌آید که رئیس‌جمهور به‌عنوان رئیس شورای عالی فضای مجازی، موظف است استعداد کشور را در حوزه‌ی سایبر و در راستای مطالبات امام جامعه هماهنگ نماید تا امر ایشان در خصوص هدایت نرم جامعه زمین نماند؛ نکته‌ی بسیار مهمی که در ایام ریاست رئیس‌جمهور مستقر بر شورای مذکور، به‌شدت مورد غفلت واقع شد.

کنترل جوامع از طریق کنترل فضای سایبر

دانش سایبرنتیک مشخصاً از طریق تحقق سه گام متوالی در افراد، کنترل جامعه به‌صورت نرم را رقم می‌زند که عبارتند از



^۶ بیانات در دیدار با اعضای شورای عالی فضای مجازی؛ ۳ بهمن ۱۳۹۶

بنابر فرایند فوق، هر فرد از طریق ارتباط و دریافت اطلاعات از طریق فضای سایبر و تحلیل و پردازش آنها، ابتدا نسبت به آن اطلاعات باورمند شده، سپس در راستای باورهای ایجاد شده به تصمیم می‌رسد و در نهایت متناسب با تصمیم خویش، اقدام می‌نماید. در نتیجه فضای سایبر توانمندی جهت‌دهی به ذهن و عمل جامعه را دارا است.

موارد متعددی در ایران اسلامی و همچنین سایر کشورها وجود دارد که یک باور مشخص در خصوص موضوعی مشخص به جامعه تزریق شده به‌گونه‌ای که اقدام بخشی از مردم بر اساس آن تنظیم گردیده است. به‌عنوان مثال دولت مستقر در انتخابات ریاست‌جمهوری سال ۹۶ با استفاده از تجمیع، تحلیل و برآوردگیری اطلاعات کاربران در فضای سایبر - به ویژه در پیام‌رسان تلگرام - سه کار را انجام داد:

۱. مخاطب‌شناسی

۲. ذائقه‌شناسی

۳. روش‌شناسی

در مخاطب‌شناسی، کسانی که رأی قطعی نداشتند - موسوم به قشر خاکستری - را شناسایی کرده و با بررسی ذائقه‌ی آنها، این گروه چند میلیونی را مجدداً به سه زیر دسته تقسیم نمود که شامل دغدغه‌مندان سیاسی، دغدغه‌مندان اقتصادی و دغدغه‌مندان فرهنگی می‌شدند. در نهایت بر اساس روش‌شناسی برای هر زیر دسته، کلیدواژه‌ای خاص طراحی کردند به‌گونه‌ای که استمرار دولت روحانی مورد تأیید ذائقه‌ی آنها قرار بگیرد؛ بدین ترتیب که:

الف) عده‌ای که توجه به مسائل سیاسی داشتند را با **آیت‌الله قتل‌عام و آیت‌الله اعدام**؛

ب) عده‌ای که نگرانی اقتصادی داشتند را با **کلید واژگان دلار پنج‌هزار تومانی و سایه‌ی جنگ**؛

پ) کسانی که در حوزه‌ی فرهنگی به‌دنبال ولنگاری بودند را با **کلیدواژه‌ی دیوارکشی جنسیتی** فریب دادند.

انتشار این کلیدواژه‌ها که یک جنگ شناختی و فریب‌گسترده‌ی افکار عمومی را در برداشت و به رقیب‌هراسی منتج شد را طی ۷۲ ساعت منتهی به انتخابات رقم زدند و مطالب آماده‌ی مرتبط با این کلید واژه‌ها را به‌طور گسترده در فضای سایبر منتشر ساختند تا نهایتاً بتوانند در انتخابات پیروز شوند.

مسئله کنترل فضای سایبر تا آنجا مهم است که در سایر کشورها نظیر آمریکا، زمانی که اصل حاکمیت از طریق فضای سایبر در حال نقض شدن است، حتی اگر ناقض آن رئیس‌جمهور مستقر باشد نیز تمامی حساب‌های وی را در پیام‌رسان‌ها و شبکه‌های اجتماعی مسدود می‌نمایند تا افکار عمومی جامعه تحت تأثیر ناخواسته قرار نگیرد.^۷

این مسئله به‌عنوان جدی‌ترین چالش دولت انقلابی منتخب، مطرح است که اگر فضای سایبر را به‌نفع ارزش‌های انقلاب اسلامی تحت مدیریت جمهوری اسلامی در نیاورد، هر آنچه از اقدامات مثبت نیز صورت دهد اما نهایتاً دشمن با وارونه‌سازی وضعیت و باورمندی مردم از طریق اطلاعات غلط و مهندسی اطلاعات، مانع از بازتاب صحیح زحمات و جهادهای دولت نزد آحاد ملت خواهد شد.

امام جامعه در این خصوص فرموده‌اند:

امروز به‌منی از گزاره‌های درست و نادرست دارد روی سر مراجعین اینترنت ما فرود می‌آید. ما چرا باید اجازه بدهیم آن چیزهایی که برخلاف ارزش‌ها و اصول مسلم‌های ما است، به‌وسیله‌ی کسانی که بدخواه ما هستند در داخل کشور توسعه پیدا کند؟!... قوی‌ترین کشورها، در این زمینه‌ها در [فضای مجازی] خط قرمز دارند؛ راه نمی‌دهند؛ خیلی از بخش‌های فضای مجازی اعزام‌شده‌ی از سوی آمریکا و دستگاه‌های پشت سر و پشت صحنه‌ی این قضیه را راه نمی‌دهند؛ کنترل می‌کنند. ما هم باید کنترل کنیم.^۸

نقش جدی فضای سایبر در دولت سیزدهم

دولت‌های سابق در تلاش بودند تا عنان قدرت اجرایی کشور را از طریق کنترل کامل وزارت‌خانه‌هایی که ماهیت سیاسی و اقتصادی دارند - نظیر وزارت کشور و وزارت اقتصاد - در اختیار بگیرند. اما به‌دلیل تغییر فضای اجتماعی جهان از جمله ایران به‌واسطه‌ی توسعه‌ی فضای سایبر، دولت یازدهم و دوازدهم به‌عنوان دوره‌ی گذار ثقل قدرت از مدیریت سنتی به مدیریت سایبرنتیک مطرح شد که متأسفانه از این فرصت حساس و راهبردی، نه تنها برای تسلط جمهوری اسلامی بر فضای سایبر کشور و گردش جریان اطلاعات استفاده نشد، بلکه از طریق نقض دستورات صریح امام جامعه، توسعه‌ی پیام‌رسان‌های غربی، عدم حمایت از تولید محتوا و نرم‌افزار داخلی و ... تمام تلاش صورت پذیرفت تا فضای سایبر دشمن بر افکار عمومی

^۷ مسدودسازی حساب‌های اجتماعی ترامپ در انتخابات اخیر ریاست‌جمهوری آمریکا

^۸ بیانات در دیدار با اعضای هیئت دولت؛ ۲۲ خرداد ۱۳۹۶

جامعه حاکم گردد. لذا دولت سیزدهم با حجمی از عقب‌ماندگی‌های سایبری مواجه است که اگر در مواجهه با آن، رویکردی فعال و علمی اتخاذ نماید، دچار مشکلات عدیده خواهد شد.

به‌صورت مشخص، فضای کلی جامعه بر اساس فضای سایبر در تناسب با دولت سیزدهم در سه حوزه‌ی فرصت‌ها، تهدیدات و آسیب‌ها قابل تبیین است.

الف) فرصت‌ها

هرچند دولت یازدهم و دوازدهم در حوزه‌ی فضای سایبر، یک فرصت‌سوزی عمیق و گسترده را موجب شده اما به این معنا نیست که امکان جبران ندارد. همراهی آحاد جامعه با دولت انقلابی منتخب از یک سو و افزایش حجم تهدیدات سایبری علیه اخلاق و فرهنگ و حریم خصوص مردم از سوی دیگر موجب شده تا جامعه، برای مدیریت قاطعانه بر این فضا مطالبه داشته باشد.

همچنین برنامه‌های متعدد برای تحقق امر فوق از سوی مراکز علمی و دانشگاهی تهیه و تدوین شده که جهت اجرا در اختیار دولت قرار می‌گیرد و صرفه‌جویی در زمان بابت برنامه‌ریزی این مهم را رقم می‌زند. لذا از اولین اولویت‌های دولت سیزدهم، رسیدگی عملی و عمیق به وضعیت فضای سایبر است به‌گونه‌ای که شاخصه‌های کیفی مد نظر امام جامعه محقق گشته و افکار عمومی جامعه از منابع اطلاعاتی صحیح و واقع‌گرا تغذیه شوند، نه منابعی که مهندسی اطلاعاتی دشمن را به جامعه تزریق می‌کنند.

ب) تهدیدات

به‌طور کل تهدیدات فضای سایبر را در سه حوزه می‌توان بررسی نمود:

۱) حریم شخصی

حدأقل میزان تهدیدات سایبری نسبت به افراد جامعه، نقض حریم خصوصی و سوء استفاده از اطلاعات شخصی آنها است که حتی توسط سازمان‌های اطلاعاتی دشمن نیز دارای سابقه است، چنانکه برای انجام هرگونه عملیات خاص، افراد مستعد را در فضای سایبر یافته و مدتی آنها را رصد می‌کنند تا بتوانند نقاط ضعف را دریافته و ذخیره نمایند. سپس اقدام به

اخاذی عملیاتی می‌کنند که به معنای عدم نشر اطلاعات شخص در مقابل انجام کاری است که مد نظر سازمان‌های مذکور است.

یقیناً اگر فضای سایبر بومی و مستقل، با مدیریت داخلی بنا شود، امکان فعالیت‌های ضد امنیتی، ضد قانونی، ضد اخلاقی و ... تا حد بسیاری کاهش یافته و کشف و رصد معهود موارد باقیمانده نیز بسیار راحت‌تر انجام می‌شود.

۲) زیرساخت‌های حساس

سطح بالاتر تهدیدات سایبری که جنبه‌ی ملی دارد، تهدیداتی است که به صورت حملات سازمان‌یافته علیه زیرساخت‌های حساس تمدنی اعم از نظامی و غیرنظامی از سوی دشمن انجام می‌شود. بر اساس مطالعات چندین ساله، آثار و تبعات امنیتی و راهبردی ناشی از چنین حملاتی، بعضاً از حملات مستقیم نظامی نیز فراتر می‌رود.

مستندات بسیاری در اختیار است که جبهه‌ی دشمن، آرایش جدی گرفته تا در صورت استقرار دولت انقلابی و بازگشت مواضع داخلی و خارجی دولت به اصول انقلاب، این دست حملات را علیه زیرساخت‌های حساس کشور آغاز نموده و تا آنجا ادامه دهد که تاب‌آوری کشور پایان یابد و دولت انقلابی مجبور به تغییر رفتار شود (پیوست شماره ۲). لذا باید نسبت به تأمین امنیت زیرساخت سایبری کشور، بلافاصله اقدامات جدی صورت پذیرد که اهم نکات برای تحقق این گزاره نیز از قبل استحصال شده و می‌توان به برنامه‌ی مدون جهت اجرا تبدیل نمود.

۳) باور عمومی جامعه

تهدیدات سایبری صرفاً محدود به دو حوزه‌ی فردی و زیرساختی نمی‌شود. سطح اصلی و کلان تهدیدات سایبرنتیک، تغییر باورهای مردم از طریق کنترل جریان اطلاعات است به گونه‌ای که دشمن مد نظر دارد. دلیل اصلی این موضوع، مدیریت فضای سایبر و افکار عمومی، خارج از دایره‌ی حاکمیت است زیرا فعلاً کنترل فضای سایبر کشور در اختیار حاکمیت نیست و عوامل بیگانه بر مدیریت این فضا اثرگذار هستند. تهدید اصلی علیه حاکمیت مردمی ایران، تضعیف عقبه‌ی مردمی نظام اسلامی است که اگر چنین اتفاقی برای حاکمیتی که امنیت‌اش به حضور و پشتیبانی مردم گره خورده رخ دهد، به تبع برای مردم نیز مؤلفه‌های امنیت، معاش و اقتصاد، بنیان‌های اجتماعی، زیرساخت‌های تمدنی کشور و ... نیز تضعیف خواهد شد.

مهم آن است که دشمن در سال‌های اخیر برای تحقق این خواسته، بخش جدی از توان خود را بر کنترل فضای سایبر کشور متمرکز نموده و تحقق آن را از این طریق دنبال می‌نماید.

پ) آسیب‌ها

آسیب‌ها شامل مجموعه‌ی ضعف‌ها و نقصان‌هایی است که درون فضای سایبر کشور از جنبه‌های مختلف واقع شده است و دشمن با کشف و رصد آنها می‌تواند تهدیدات مختلف را طراحی و اجرا نماید. لذا اصلی‌ترین راهکار برای ممانعت از تهدیدات سایبری دشمن، رفع آسیب‌های درونی است.

ساختار فضای سایبر به‌طور دقیق و علمی شامل چهار رکن است که عبارتند از اطلاعات، ارتباطات، محاسبات و کنترل.

«ارکان سایبرنتیک»			
کنترل	محاسبات	ارتباطات	اطلاعات
اشراف و نظارت کامل بر محتوا	پردازش و ذخیره‌سازی محتوا	انتقال محتوا	محتوا

در نتیجه بررسی آسیب‌های فضای سایبر کشور و رفع قطعی و صحیح آنها نیز بر اساس ارکان فوق انجام می‌شود. برای نمونه، نظارت بر جریان اطلاعات در فضای سایبر کشور مرتبط با رکن اطلاعات، ساماندهی وضعیت پیام‌رسان‌های فوری و شبکه‌های اجتماعی مربوط به رکن ارتباطات، ایجاد موتور جستجوی بومی در حوزه‌ی رکن محاسبات و تولید سیستم عامل ملی متعلق به رکن کنترل است.

تأکید علمی بر این است که هرگونه طرح‌ریزی راهبردی و برنامه‌ی عملیاتی برای اصلاح وضعیت فضای سایبر کشور از جمله ایجاد شبکه‌ی ملی اطلاعات به‌عنوان زیرساخت اصلی این فضا، باید در بردارنده‌ی چهار رکن فوق باشد؛ در غیر این صورت نقص علمی طرح‌های پیشنهادی و اسناد بالادستی، مانع از تحقق نتایج مطلوب خواهد شد.