بسم الله الرحمن الرحیم

سیاست ملی جمهوری اسلامی ایران در قبال اینترنت ماهواره‌ای، سامانه‌های موقعیت‌یابی و پلتفرم‌های فرامرزی در شرایط مخاصمه

مِتُد
(مرکز توسعه دانش مسئله محوری)

www.Mtod.ir

خلاصه اجرایی

این گزارش سیاستی، سه قلمرو به‌هم‌پیوسته را که در جنگ‌های ترکیبی به «زیرساخت نفوذپذیر» تبدیل شده‌اند، به‌صورت یک بسته یکپارچه سیاست‌گذاری می‌کند: اینترنت ماهواره‌ای (به‌عنوان کانال ارتباطی مقاوم در برابر اختلال زمینی)، سامانه‌های موقعیت‌یابی/ناوبری/زمان GPS/GNSS به‌عنوان ستون فقرات هدایت، لجستیک و خدمات حیاتی)، و پلتفرم‌های دیجیتال فرامرزی (به‌عنوان میدان توزیع روایت، بسیج اجتماعی و عملیات ادراکی). شواهد تجربی جنگ‌های اخیر نشان داده است که این سه، در کنار هم، «چرخه فرماندهی-اقتصاد-افکار عمومی» را هدف می‌گیرند و بنابراین باید با یک معماری سیاستی مشترک مدیریت شوند.

درس کلیدی قابل اتکا از تجربه اوکراین این است که اینترنت ماهواره‌ای تجاری می‌تواند تاب‌آوری ارتباطی ایجاد کند، اما هم‌زمان «نقطه شکست» و «وابستگی راهبردی به تصمیم شرکت» می‌سازد؛ به‌ویژه وقتی هزینه تداوم خدمات، سیاست مالک، و فشارهای سیاسی/امنیتی تغییر کند. گزارش‌های تحلیلی نشان می‌دهد بسته اولیه Starlink برای اوکراین ۵۰۰۰ ترمینال بوده (۳۶۶۷ اهدایی و ۱۳۳۳ خریداری‌شده توسط USAID) و سپس مقیاس به حدود ۲۰هزار دستگاه رسید؛ هم‌زمان، صورت‌حساب‌های پیشنهادی به وزارت دفاع آمریکا از ده‌ها تا صدها میلیون دلار در سال حکایت داشته است.

در حوزه GPS/GNSS، شواهد میدانی نشان می‌دهد «اختلال عمدی» (jam/spoof) دیگر اتفاق حاشیه‌ای نیست؛ گزارش‌ها از افزایش گسترده تداخلات از ۲۰۲۲ به بعد در اروپا و حتی ده‌ها هزار رخداد spoofing در فرودگاه‌های خاورمیانه در سال ۲۰۲۴ حکایت دارند. مهم‌تر اینکه پیامد آن، صرفاً نظامی نیست و هواپیمایی غیرنظامی، حمل‌ونقل و زنجیره تأمین را نیز درگیر می‌کند.

در رکن سوم، اندیشکده‌ها و مراکز سیاستی غربی صراحتاً توضیح داده‌اند که شرکت‌های فناوری و پلتفرم‌ها در جنگ‌ها به «عامل اثرگذار مستقل» تبدیل شده‌اند؛ تصمیم آن‌ها درباره همکاری، محدودسازی، یا تغییر سیاست‌ها می‌تواند سرنوشت تاب‌آوری دیجیتال یک کشور را تغییر دهد.

بر این پایه، سیاست ملی پیشنهادی برای ایران باید بر چهار اصل طراحی شود: حاکمیت دیجیتال (حق تنظیم‌گری و اعمال صلاحیت نسبت به خدمت/داده/الگوریتم در پهنه سرزمینی)، تاب‌آوری چندلایه (جایگزین و افزونگی برای ارتباط و PNT)، مدیریت ریسک سامانه‌ای (به‌جای برخورد تک‌موردی)، و کاهش وابستگی به شرکت‌ها و زیرساخت‌های دشمن با اتکا به ظرفیت داخلی و شرکای غیرمتخاصم.

شواهد و الگوی تهدید

اینترنت ماهواره‌ای به‌عنوان «تاب‌آوری ارتباطی» و «ابزار نفوذ»

گزارش‌های تحلیلی نشان می‌دهد در اوکراین، Starlink به‌عنوان پشتیبان فرماندهی و کنترل ارتباطی عمل کرده و به‌علت ماهیت LEO/pLEO، از منظر «اختلال در سطح مدار» دشوارتر بوده است؛ با این حال، گزارش‌های جدیدتر تأکید می‌کنند که پایانه‌های زمینی در برابر جنگ الکترونیک موضعی آسیب‌پذیرند و محدودیت‌های پهنای باند/تأخیر می‌تواند در عملیات‌های حجیم گلوگاه شود.

هم‌زمان، آسیب راهبردی بزرگ‌تر آن است که سرویس تجاری می‌تواند به «نقطه شکست سیاستی» تبدیل شود: در اسناد رسانه‌ای به نامه‌ها و مذاکرات درباره هزینه‌های سالانه (تا چندصد میلیون دلار در یک دوره) و نیز تغییر مکرر موضع شرکت اشاره شده است. نتیجه سیاستی روشن است: دولت‌ها در جنگ، اگر به سرویس‌های تجاری متخاصم وابسته شوند، «بودجه جنگ» را به «تعهد مالی خارجی» و «ریسک قطع خدمت» گره می‌زنند.

از منظر تهدید علیه ایران، شواهد رسانه‌ای نشان می‌دهد در برهه‌ای، دولت آمریکا Starlink را به‌عنوان گزینه‌ای برای افزایش دسترسی اینترنت در ایران بررسی کرده است. این گزاره، از منظر سیاست‌گذاری دفاعی ایران، به معنای آن است که اینترنت ماهواره‌ای باید هم‌زمان به‌عنوان «ابزار تاب‌آوری» و «ابزار مداخله خارجی» فهم شود.

GPS/GNSS به‌عنوان زیرساخت مشترک «نظامی-اقتصادی-ایمنی عمومی»

گزارش‌های تحلیلی نشان می‌دهد اختلال (jamming/spoofing GPS) می‌تواند هم تسلیحات هدایت‌شونده و هم خدمات غیرنظامی را دچار اخلال کند؛ گزارش Financial Times از رشد چشمگیر این پدیده از ۲۰۲۲ به بعد سخن می‌گوید و علاوه بر نمونه‌های اروپا، از «تا ۵۰ هزار حمله spoofing روی فرودگاه‌های خاورمیانه در ۲۰۲۴» گزارش می‌دهد.

از منظر پدافند ملی، نکته تعیین‌کننده این است که GPS/GNSS «زیرساخت مشترک» برای: ناوبری هوایی/دریایی، حمل‌ونقل شهری، زمان‌سنجی شبکه‌های مخابراتی و مالی، و هدایت پلتفرم‌های نظامی است. مطالعات سیاستی Belfer Center for Science and International Affairs نیز بر شکنندگی وابستگی شهری/زیرساختی به GPS و ضرورت برنامه‌ریزی تاب‌آوری در سطوح حکمرانی تأکید دارد.

پلتفرم‌های فرامرزی و شرکت‌های فناوری به‌عنوان «بازیگر جنگ»

گزارش‌های Atlantic Council در مورد اوکراین نشان می‌دهد شرکت‌های فناوری در جنگ، صرفاً فروشنده نیستند؛ در مواردی «حمایت حیاتی و غیرقابل جایگزین» ارائه داده‌اند، اما تصمیم آن‌ها تابع ترکیبی از عوامل (هم‌راستایی تجاری، هماهنگی، ریسک تلافی، فشار سیاسی) بوده است. این یعنی در جنگ، سیاست‌گذار باید شرکت‌ها را «کنشگر» و نه «زیرساخت بدیهی» تلقی کند.

افزون بر این، در ساحت امنیت ارتباطات ماهواره‌ای، Center for Strategic and International Studies در سال ۲۰۲۶ هشدار داده است که بخشی از زیرساخت‌های ارتباطی ماهواره‌ای بر «بنیان‌های ناامن» ساخته شده و حتی با تجهیزات ارزان (حدود ۸۰۰ دلار) امکان دریافت داده‌هایی از لینک‌های فاقد رمزنگاری گزارش شده است؛ در همان مطالعه، «۵۰ درصد لینک‌های مشاهده‌شده بدون رمزنگاری» گزارش شده‌اند. نتیجه مستقیم برای ایران این است که اگر در طراحی تاب‌آوری به سمت سرویس‌های ماهواره‌ای (از جمله direct-to-cell) حرکت شود، الزام رمزنگاری end-to-end و الزامات امنیتی تأمین/تدارک باید از ابتدا در معماری تصمیم قرار گیرد.

چارچوب سیاست ملی یکپارچه

هدف کلان و اهداف میانی

هدف کلان: حفظ حاکمیت دیجیتال و افزایش تاب‌آوری کشور در برابر مداخله و اخلال دیجیتال دشمن در شرایط مخاصمه، با کمینه‌سازی هزینه‌های جانبی اجتماعی و اقتصادی.

اهداف میانی:

۱) تنظیم‌گری حاکمیتی خدمت فرامرزی: ایران باید بتواند درباره ارائه خدمت اینترنت ماهواره‌ای/پلتفرمی در قلمرو سرزمینی، قواعد الزام‌آور وضع کند و در صورت عدم‌پذیرش، رژیم کنترل و مقابله تعریف نماید. نمونه‌های مقایسه‌ای نشان می‌دهد Starlink در کشورهای مختلف با «چالش مجوزدهی» مواجه شده و برخی دولت‌ها به‌علت عدم انطباق با رژیم مجوز، استفاده را متوقف/ممنوع کرده‌اند.

۲) تاب‌آوری چندمسیره در ارتباط و PNT: تجربه اوکراین نشان می‌دهد اتکا به یک مسیر (حتی اگر مقاوم‌تر باشد) می‌تواند «نقطه شکست» ایجاد کند. بنابراین تاب‌آوری باید بر ترکیب مسیرهای زمینی، ماهواره‌ای، و گزینه‌های جایگزین بنا شود.

۳) امنیت ارتباطات و اصالت پیام: تهدید در جنگ ترکیبی فقط قطع ارتباط نیست؛ «دستکاری، استراق و جعل» نیز هست. با توجه به هشدارهای امنیتی درباره لینک‌های ماهواره‌ای فاقد رمزنگاری، باید استانداردهای امنیتی اتصال و پیام ابلاغ شود.

۴) مدیریت ریسک سامانه‌ای پلتفرم‌ها و الگوریتم‌ها: الگوریتم‌های تقویت/توصیه و سیاست‌های تعدیل‌گری، می‌توانند میدان ادراکی را به زیان امنیت ملی دستکاری کنند؛ در شرایط مخاصمه، سیاست باید «ریسک‌محور» و «شاخص‌پذیر» باشد و به جای برخورد تک‌محتوا، روی شبکه‌های هماهنگ، تبلیغات هدفمند، و الگوهای تقویت تمرکز کند. این منطق با تحلیل‌های درباره تبدیل شرکت‌ها به بازیگر جنگی و نیز جنگ اطلاعاتی پلتفرمی هم‌خوان است.

معماری سیاست

معماری پیشنهادی چهار لایه دارد:

- لایه حقوقی-تنظیم‌گری: رژیم مجوزدهی، الزامات نمایندگی/پاسخ‌گویی، قواعد داده و الگوریتم، و سازوکارهای اعمال قانون.
- لایه عملیاتی-فنی: رصد، آشکارسازی و پاسخ سریع به اتصال ماهواره‌ای غیرمجاز، اخلال GNSS، و موج‌های پلتفرمی؛ همراه با استانداردهای امنیت اتصال.
- لایه تاب‌آوری زیرساختی: افزونگی ارتباطی و PNT برای دولت و خدمات حیاتی؛ تنوع‌بخشی به فناوری و تأمین‌کننده.
- لایه دیپلماسی فناوری و اقتصاد سیاسی: تبدیل موضوعات فوق به «پرونده مذاکره» و «هزینه‌سازی حقوقی/اقتصادی» برای ارائه‌دهندگان متخاصم و حامیان آن‌ها؛ هم‌زمان با همکاری‌های فنی-استانداردی با شرکای غیرمتخاصم. (تجربه‌های تنظیم‌گری و مجوزدهی Starlink در کشورهای مختلف نشان می‌دهد مسیر دیپلماسی/تنظیم‌گری، عملی و قابل پیگیری است.)

بسته اقدامات اجرایی

در این بخش، اقدامات سیاستی به واحدهای اجرایی مشخص، زمان‌مند و قابل سنجش تبدیل می‌شود تا سیاست ملی جمهوری اسلامی ایران در قبال اینترنت ماهواره‌ای، سامانه‌های موقعیت‌یابی و پلتفرم‌های فرامرزی در شرایط مخاصمه، از سطح توصیه کلی به سطح اقدام نهادی و عملیاتی ارتقا یابد. منطق حاکم بر این بسته آن است که سه قلمرو «اینترنت ماهواره‌ای»، «خدمات موقعیت‌یابی و زمان‌سنجی مبتنی بر GPS/GNSS» و «پلتفرم‌های دیجیتال فرامرزی» در وضعیت جنگ و فشار مرکب، نباید به‌صورت منفک و بخشی اداره شوند؛ بلکه باید ذیل یک سیاست ملی واحد، با فرماندهی روشن، ابزار حقوقی مشخص، سازوکار مالی تعریف‌شده، مهلت زمانی صریح و خروجی‌های قابل ارزیابی تنظیم شوند.

اقدام نخست، تصویب مصوبه ملی «حاکمیت دیجیتال در مخاصمه» برای سه قلمرو اینترنت ماهواره‌ای، خدمات موقعیت‌یابی و پلتفرم‌های فرامرزی است. این مصوبه باید به‌عنوان سند بالادستی واحد، وضعیت اضطرار دیجیتال، حدود صلاحیت دستگاه‌ها، قواعد مجوزدهی، الزامات رصد و پاسخ، و تکالیف نهادی همه بازیگران مسئول را به‌صورت یکپارچه تعریف کند. مسئولیت مستقیم این اقدام بر عهده شورای عالی فضای مجازی در سطح سیاست‌گذاری و مرکز ملی فضای مجازی در سطح تدوین، ابلاغ و پیگیری اجرایی قرار می‌گیرد. وزارت ارتباطات و فناوری اطلاعات، سازمان پدافند غیرعامل کشور، ستاد کل نیروهای مسلح، بانک مرکزی، سازمان هواپیمایی کشوری، سازمان بنادر و دریانوردی، سازمان صدا و سیمای جمهوری اسلامی ایران و وزارت امور خارجه باید به‌عنوان نهادهای همکار به این سازوکار متصل شوند. مبنای حقوقی این اقدام، مصوبه شورای

عالی فضای مجازی و دستورالعمل‌های اجرایی ابلاغی به دستگاه‌ها است. از حیث مالی، هزینه سیاست‌گذاری این اقدام محدود است و بار اصلی آن به دبیرخانه و سازوکارهای رصد و گزارش‌دهی مربوط می‌شود؛ ازاین‌رو تأمین اعتبار آن از محل بودجه جاری مرکز ملی فضای مجازی و سهم مشارکت دستگاه‌های عضو امکان‌پذیر است. مهلت اجرای این اقدام نباید از ۳۰ روز برای تصویب و ابلاغ فراتر رود؛ زیرا هرگونه تأخیر موجب استمرار عمل‌کرد جزیره‌ای دستگاه‌ها، تداوم وابستگی بدون فرمان واحد به شرکت‌ها و سرویس‌های خارجی، و کاهش ظرفیت اعمال سیاست در اوج بحران خواهد شد. خروجی‌های قابل سنجش این اقدام عبارت‌اند از تصویب و انتشار مصوبه، ابلاغ سه دستورالعمل تخصصی برای حوزه‌های اینترنت ماهواره‌ای، PNT و پلتفرم‌های فرامرزی، و تشکیل کارگروه‌های تخصصی متناظر.

اقدام دوم، ایجاد سامانه ملی «رصد و پاسخ سریع» برای اتصال‌های ماهواره‌ای، اخلال در GNSS و موج‌های پلتفرمی است. این سامانه باید سه محصول عملیاتی را تولید کند: نخست، نقشه اتصال‌های ماهواره‌ای مشکوک یا غیرمجاز و نقاط تمرکز آنها؛ دوم، نقشه رخدادهای اخلال، پارازیت یا فریب موقعیت‌یابی و هشدارهای ایمنی و عملیاتی مرتبط؛ و سوم، داشبورد موج‌های پلتفرمی شامل شبکه‌های هماهنگ غیرواقعی، الگوهای تقویت محتوا، رخدادهای جعل و دیپ‌فیک، و موج‌های ادراکی سازمان‌یافته. مسئولیت مستقیم این اقدام بر عهده سازمان پدافند غیرعامل کشور است و وزارت ارتباطات، پلیس فتا، سازمان هواپیمایی، سازمان بنادر، بانک مرکزی، صدا و سیما، مرکز ملی فضای مجازی و در بخش‌های طبقه‌بندی‌شده نهادهای اطلاعاتی، به‌عنوان همکاران اصلی آن عمل می‌کنند. اجرای این اقدام نیازمند ابلاغیه شورای عالی فضای مجازی یا شورای عالی امنیت ملی برای تبادل بین‌دستگاهی داده و الزام به گزارش‌دهی رخدادهای ماهواره‌ای، پلتفرمی و موقعیت‌یابی است. بودجه آن باید در سه سرفصل نرم‌افزار و داده، حسگرها و دریافت‌کننده‌های پایش GNSS و اتصال‌های ماهواره‌ای، و نیروی انسانی تحلیل‌گر تعریف شود. شواهد فنی نشان می‌دهد که هزینه حمله و سوءاستفاده از برخی پیوندهای ماهواره‌ای یا اختلال‌های داده‌ای پایین است؛ بنابراین دفاع باید ماهیت مستمر، داده‌محور و واکنش‌پذیر داشته باشد. نسخه حداقلی سامانه باید ظرف ۶۰ روز و نسخه کامل آن ظرف ۶ ماه عملیاتی شود. در صورت تأخیر، تصمیم‌گیری نسبت به رخدادهای ماهواره‌ای، اخلال‌های ناوبری و موج‌های ادراکی، کور و دیرهنگام خواهد ماند. شاخص‌های ارزیابی این اقدام شامل زمان کشف رخداد، زمان پاسخ، تعداد رخدادهای ثبت و طبقه‌بندی‌شده، هشدارهای ابلاغ‌شده به بخش‌های حمل‌ونقل، مالی و خدمات حیاتی، و گزارش‌های ماهانه روندها خواهد بود.

اقدام سوم، طراحی و اجرای رژیم مجوزدهی و اعمال قانون برای اینترنت ماهواره‌ای در پهنه سرزمینی ایران است. این اقدام باید مبتنی بر یک رژیم مجوزدهی دوگانه تنظیم شود: در سطح اول، ارائه‌دهنده خدمت باید دارای مجوز فعالیت، نماینده پاسخ‌گو، تعهدات امنیتی، قواعد رمزنگاری و

الزامات داده‌ای روشن باشد؛ و در سطح دوم، استفاده‌کنندگان حرفه‌ای و پایانه‌های مجاز، به‌ویژه در حوزه‌های امداد، مدیریت بحران و خدمات حیاتی، باید ذیل نظام ثبت سخت‌افزار، ممیزی و نظارت قرار گیرند. مسئولیت مستقیم این اقدام بر عهده وزارت ارتباطات و فناوری اطلاعات، به‌ویژه سازمان تنظیم مقررات و ارتباطات رادیویی، خواهد بود و گمرک، پلیس، سازمان پدافند غیرعامل، دستگاه‌های خدمات حیاتی و وزارت امور خارجه در سطوح مکمل به آن متصل می‌شوند. ابزار حقوقی لازم برای این اقدام، مقرره تنظیم‌گری در چارچوب سیاست‌های شورای عالی فضای مجازی و آیین‌نامه اجرایی وزارت ارتباطات برای ثبت، کنترل، واردات و توزیع پایانه‌ها است. از نظر مالی، بخش تنظیم‌گری کم‌هزینه است، اما بخش اجرایی نیازمند سامانه ثبت، سازوکار بازرسی، ظرفیت ممیزی و پشتیبانی از پایانه‌های مجاز در بخش‌های خدمات حیاتی است. مهلت اجرای این اقدام ۹۰ روز تعیین می‌شود. اگر این اقدام در این بازه عملیاتی نشود، مسیرهای ارتباطی فرامرزی فاقد پاسخ‌گویی حقوقی تثبیت شده و توان حاکمیت برای اعمال مقررات در زمان بحران کاهش می‌یابد. خروجی‌های قابل اندازه‌گیری این اقدام شامل صدور مقرره و راه‌اندازی سامانه ثبت، درصد پایانه‌های مجاز دارای شناسه و ممیزی، و کاهش سهم استفاده غیرمجاز در مناطق اولویت‌دار بر اساس داده‌های سامانه اقدام دوم است.

اقدام چهارم، تدوین و ابلاغ استاندارد امنیتی الزام‌آور برای ارتباطات ماهواره‌ای دولت و خدمات حیاتی است. هرگونه ارتباط ماهواره‌ای مورد استفاده در دولت، زیرساخت‌های حیاتی و خدمات عمومی، از جمله ارتباطات مستقیم با تلفن همراه، باید مشمول استانداردهای سخت‌گیرانه رمزنگاری، امنیت انتها به انتها، مدیریت کلید و ممیزی دوره‌ای شود. مسئولیت مستقیم تدوین و ممیزی این استاندارد بر عهده سازمان پدافند غیرعامل و مسئولیت الزام فنی دستگاه‌ها بر عهده سازمان فناوری اطلاعات و وزارت ارتباطات است. این اقدام باید بر پایه دستورالعمل فنی ـ الزامی در چارچوب مصوبه شورای عالی فضای مجازی یا شورای عالی امنیت ملی اجرا شود. هزینه‌های اجرای آن عمدتاً شامل تغییرات نرم‌افزاری، توسعه زیرساخت اعتماد، مدیریت کلید، ممیزی امنیتی و اصلاح پیکربندی سرویس‌هاست. این هزینه‌ها در مقایسه با هزینه عدم اقدام، به‌ویژه در شرایطی که برخی پیوندهای ماهواره‌ای یا داده‌ای در صورت فقدان رمزنگاری می‌توانند هدف استراق یا بهره‌برداری غیرمجاز قرار گیرند، بسیار محدودتر است. مهلت این اقدام ۶۰ روز برای تدوین استاندارد و ۱۸۰ روز برای انجام نخستین ممیزی سراسری است. تعلل در اجرای آن، احتمال نشت داده‌های حساس و استراق ارتباطات زیرساختی، خدماتی و حاکمیتی را در زمان بحران افزایش می‌دهد. خروجی‌های قابل سنجش این اقدام عبارت‌اند از درصد پیوندهای ماهواره‌ای حیاتی دارای رمزنگاری و ممیزی، گزارش ممیزی ریسک، و کاهش رخدادهای نشت یا استراق داده.

اقدام پنجم، اجرای برنامه ملی تاب‌آوری PNT برای کاهش وابستگی تک‌منبعی به GPS است. این برنامه باید به‌طور مرحله‌بندی‌شده در پنج حوزه هوانوردی، دریانوردی، شبکه برق و انرژی، مخابرات

و بخش مالی مستقر شود و استفاده از گیرنده‌های چندمنظومه، بهره‌گیری از سامانه‌های پشتیبان نظیر IMU/INS و تدوین رویه‌های عملیاتی برای شرایط GNSS-denied را به حداقل استاندارد بخش‌های حیاتی تبدیل کند. مسئولیت هماهنگی کلان این اقدام بر عهده سازمان پدافند غیرعامل است و سازمان هواپیمایی کشوری، سازمان بنادر و دریانوردی، وزارت نیرو، بانک مرکزی و وزارت ارتباطات مجریان بخشی آن خواهند بود. ابزار اجرایی این اقدام، مقرره ملی «حداقل استاندارد تاب‌آوری PNT» و درج الزامات آن در مجوزهای بهره‌برداری و ایمنی بخش‌های مربوط است. بودجه آن باید بخشی و مأموریت‌محور تعریف شود؛ به‌گونه‌ای که هر بخش از محل ردیف‌های ارتقای ایمنی، تاب‌آوری یا توسعه زیرساخت خود، هزینه‌های لازم را پوشش دهد. مهلت اجرای حداقل‌های این برنامه در هوانوردی و دریانوردی ۶ ماه و برای استقرار میان‌بخشی ۱۲ ماه تعیین می‌شود. عدم اقدام در این بازه، ریسک ایمنی عمومی، اختلال در خدمات حیاتی و آسیب‌پذیری اقتصادی ناشی از اخلال‌های PNT را افزایش خواهد داد. شاخص‌های سنجش موفقیت این برنامه شامل درصد سامانه‌های حیاتی مجهز به multi-constellation و INS fallback، گزارش کاهش رخدادهای از دست رفتن ناوبری، و تعداد تمرین‌های عملیاتی میدانی و رومیزی است.

اقدام ششم، ایجاد شبکه ملی پایش GNSS و تدوین استاندارد گزارش‌دهی رخداد در سطح کشور است. این شبکه باید از طریق استقرار گیرنده‌ها و حسگرهای پایش در فرودگاه‌ها، بنادر، مراکز صنعتی حساس و کریدورهای حیاتی، امکان تولید نقشه ملی اخلال، پارازیت و فریب موقعیت‌یابی را فراهم کند. مسئولیت مستقیم این اقدام در بخش دریایی بر عهده سازمان بنادر و دریانوردی، در بخش هوانوردی بر عهده سازمان هواپیمایی کشوری و در سطح هماهنگی و استانداردسازی بر عهده سازمان پدافند غیرعامل خواهد بود. مبنای اجرایی آن، دستورالعمل اداری الزام گزارش‌دهی رخداد و تعیین مرجع ملی تجمیع، تحلیل و انتشار هشدارها است. بودجه این اقدام باید صرف نصب حسگرها، راه‌اندازی سامانه داده، ذخیره‌سازی و پردازش اطلاعات و نیروی تحلیلی شود. مرحله پایلوت باید ظرف ۹۰ روز در پنج نقطه اولویت‌دار آغاز و طی ۱۲ ماه به مقیاس ملی توسعه یابد. در صورت تأخیر، الگوی اخلال و فریب GNSS برای کشور ناشناخته باقی خواهد ماند و تصمیم‌گیری نسبت به این حوزه به‌صورت واکنشی و پسینی ادامه خواهد یافت. خروجی‌های قابل ارزیابی این اقدام شامل تعداد نقاط پایش فعال، نقشه ماهانه رخدادها، و هشدارهای صادرشده برای اپراتورها و دستگاه‌های ذی‌ربط است.

اقدام هفتم، تدوین و اعمال بسته حکمرانی پلتفرم‌های فرامرزی در وضعیت مخاصمه است. این بسته باید وظایف اضطراری پلتفرم‌ها و سازوکارهای اعمال قانون را در سه سطح حقوقی، فنی و اجتماعی تعیین کند. در سطح حقوقی، لازم است اخطار رسمی، الزام به تعیین نماینده پاسخ‌گو، قواعد مربوط به داده، تبلیغات هدفمند و تعدیل‌گری محتوای امنیتی تعریف شود. در سطح فنی، باید سازوکار داده‌محور برای شناسایی موج‌های هماهنگ، حساب‌های غیرواقعی و الگوهای تقویت

الگوریتمی برقرار گردد. در سطح اجتماعی نیز باید کانال‌های رسمی و سازوکار راستی‌آزمایی سریع برای کاهش اثرگذاری عملیات ادراکی فعال شوند. مسئولیت مستقیم این اقدام بر عهده مرکز ملی فضای مجازی است و وزارت ارتباطات، پلیس فتا، سازمان صدا و سیما، وزارت فرهنگ و ارشاد اسلامی و وزارت امور خارجه در ابعاد مکمل آن سهیم خواهند بود. اجرای این بسته مستلزم مصوبه شورای عالی فضای مجازی و ابلاغ دستورالعمل‌های اجرایی notice-and-action و پاسخ‌گویی پلتفرم‌ها است. از نظر مالی، بخش مقررات‌گذاری کم‌هزینه است و بار اصلی آن در لایه رصد و تحلیل شبکه‌ای قرار دارد که باید از محل بودجه اقدام دوم پشتیبانی شود. مهلت اجرای این بسته ۶۰ روز است. تأخیر در آن، موجب تثبیت عرف عملیاتی پلتفرم‌ها علیه منافع ملی و کاهش امکان اعمال سیاست در اوج بحران می‌شود. شاخص‌های ارزیابی این اقدام شامل ابلاغ بسته مقرراتی، تعداد اخطارهای رسمی و پاسخ‌های ثبت‌شده، و کاهش موج‌های هماهنگ بر اساس داشبورد اقدام دوم است.

اقدام هشتم، ایجاد زیرساخت اصالت دیجیتال و کانال‌های تأییدشده برای پیام‌های رسمی در بحران است. با توجه به ظرفیت پلتفرم‌های فرامرزی برای تشدید جنگ روایت‌ها، جعل، تحریف و انتشار محتوای دست‌کاری‌شده، همه پیام‌های رسمی مرتبط با بحران باید از طریق زیرساخت امضای دیجیتال، کانال‌های تأییدشده و تیم راستی‌آزمایی ۲۴ ساعته منتشر و پشتیبانی شوند. مسئولیت مستقیم این اقدام بر عهده سازمان صدا و سیمای جمهوری اسلامی ایران به‌عنوان هاب اطلاع‌رسانی عمومی است و پشتیبانی فنی آن باید توسط وزارت ارتباطات و سازمان پدافند غیرعامل انجام شود. مبنای حقوقی این اقدام، مصوبه شورای عالی فضای مجازی درباره استاندارد اصالت پیام و الزام دستگاه‌ها به استفاده از امضای دیجیتال در پیام‌های بحرانی است. بودجه آن شامل هزینه PKI، امضای دیجیتال، ایجاد کانال‌های تأییدشده و تیم راستی‌آزمایی است. نسخه حداقلی این زیرساخت باید ظرف ۳۰ روز و نسخه کامل آن ظرف ۱۲۰ روز مستقر شود. هرگونه تأخیر، هزینه اجتماعی و امنیتی ناشی از جعل و انتشار سریع روایت‌های تحریف‌شده را افزایش خواهد داد. خروجی‌های قابل سنجش این اقدام عبارت‌اند از درصد پیام‌های بحرانی دارای امضای دیجیتال، زمان تشخیص و تکذیب جعل، و کاهش نرخ بازنشر محتوای جعلی پس از پاسخ رسمی.

اقدام نهم، اجرای برنامه تنوع‌بخشی راهبردی و کاهش وابستگی به زیرساخت‌های دشمن است. این برنامه باید در سه محور ارتباط، PNT و پلتفرم اجرا شود. در محور ارتباط، لازم است مسیرهای پشتیبان و سرویس‌های داخلی یا مبتنی بر همکاری با شرکای غیرمتخاصم توسعه یابد. در محور PNT، استفاده از چند منظومه و راهکارهای جایگزین یا پشتیبان تقویت شود. در محور پلتفرم نیز باید ظرفیت‌های بومی و شبکه‌های توزیع محتوا و پیام‌رسانی توسعه پیدا کند تا تداوم خدمات در شرایط بحران تضمین شود. مسئولیت مستقیم این اقدام در محور توسعه فناوری بر عهده معاونت علمی، فناوری و اقتصاد دانش‌بنیان ریاست جمهوری و در محور زیرساخت و خدمات بر

عهده وزارت ارتباطات است. مبنای اجرایی آن باید از طریق تصویب سند برنامه و تعیین پروژه‌های اولویت‌دار در شورای عالی فضای مجازی و ایجاد سازوکار تأمین مالی پروژه‌محور، از جمله صندوق‌های پروژه یا منابع ترکیبی دولتی و شبه‌دولتی، فراهم شود. این اقدام پرهزینه‌ترین جزء بسته است و باید بر مبنای پروژه‌های مشخص، دارای زمان‌بندی و شاخص عملکرد طراحی شود. افق زمانی آن بسته به پروژه‌ها از ۶ تا ۲۴ ماه متغیر خواهد بود. تأخیر در آن، وابستگی ساختاری به زیرساخت‌های دشمن را در بحران بعدی تثبیت می‌کند و نقاط تک‌شکست را حفظ خواهد کرد. خروجی‌های قابل سنجش این برنامه شامل سهم خدمات حیاتی دارای مسیر پشتیبان، کاهش نقاط single point of failure، و رشد ظرفیت داخلی در شاخص‌های کیفیت و تداوم خدمت است.

این بسته اجرایی زمانی مؤثر خواهد بود که سه اصل در اجرای آن رعایت شود: نخست، فرمان واحد و سیاست یکپارچه برای هر سه قلمرو؛ دوم، ترجمه سریع مصوبات به سامانه، استاندارد، پروتکل و ممیزی؛ و سوم، سنجش‌پذیری مستمر همه اقدامات بر پایه شاخص‌های عملیاتی، نه صرفاً پیشرفت‌های شکلی و اداری. بر این مبنا، موفقیت سیاست ملی جمهوری اسلامی ایران در قبال اینترنت ماهواره‌ای، خدمات موقعیت‌یابی و پلتفرم‌های دیجیتال فرامرزی در شرایط مخاصمه، در گرو آن است که این حوزه‌ها از وضعیت واکنشی و بخشی خارج و به یک معماری حکمرانی زمان‌مند، الزام‌آور و قابل ارزیابی تبدیل شوند.

مدل بودجه و تأمین مالی

این گزارش از عددسازی غیرمستند درباره بودجه ملی اجتناب می‌کند و به‌جای آن، «مدل بودجه‌ریزی مبتنی بر واحد هزینه» پیشنهاد می‌دهد تا دستگاه‌های اجرایی بتوانند با داده‌های واقعی خود آن را دقیق کنند.

برای اینترنت ماهواره‌ای، داده‌های مستند درباره اوکراین نشان می‌دهد: (الف) هزینه پایانه‌ها برای مدل‌های جنگی/ارسالی حدود ۵۰۰ ,۱ تا ۵۰۰ ,۲ دلار گزارش شده است؛ (ب) برای سرویس پیشرفته، هزینه ماهانه تا ۵۰۰ ,۴ دلار در برخی برآوردها مطرح شده است؛ (ج) هزینه‌های سالانه در سناریوهای تامین خدمت می‌تواند به ده‌ها/صدها میلیون دلار برسد. بنابراین هرگونه «استفاده مجاز دولت/خدمات حیاتی» باید با مدل مالی روشن (تعداد پایانه × قیمت پایانه + تعداد پایانه × حق خدمت ماهانه × ماه) و ستون‌های ریسک (قطع خدمت، تغییر سیاست شرکت، افزایش قیمت) همراه باشد.

برای GNSS و پایش اخلال، مقیاس رخدادها می‌تواند بسیار بزرگ باشد (ده‌ها هزار رخداد در یک منطقه/سال) و پیامد آن فراتر از نظامی است؛ لذا بودجه این بخش باید به‌عنوان «بودجه ایمنی و تداوم خدمات عمومی» دیده شود و در ردیف‌های بخش‌محور (هواپیمایی، دریانوردی، مخابرات، مالی) تجمیع گردد.

برای امنیت ارتباطات ماهواره‌ای، بخشی از لینک‌ها ممکن است فاقد رمزنگاری باشد و با تجهیزات کم‌هزینه قابل دریافت شود. نتیجه مالی آن این است که «اقدام پیشگیرانه» (رمزنگاری، ممیزی، استاندارد تامین) به‌مراتب کم‌هزینه‌تر از «نشت داده در بحران» است؛ بنابراین باید در ساختار بودجه امنیت اطلاعات دستگاه‌های حیاتی تثبیت شود.

مخاطرات و مدیریت ریسک

۱) ریسک سیاسی-اجتماعی: سیاست‌های سلبی بی‌هدف در پلتفرم‌ها می‌تواند هزینه اجتماعی ایجاد کند؛ بنابراین بسته پیشنهادی بر «ریسک سامانه‌ای» (شبکه هماهنگ، جعل، تبلیغات هدفمند) و «کانال‌های رسمی و اصالت پیام» تمرکز دارد تا مداخله، هدفمند و سنجش‌پذیر بماند.

۲) ریسک فنی: در GNSS و ماهواره، ابزارهای اخلال/فریب می‌تواند به خدمات غیرنظامی آسیب بزند؛ بنابراین برنامه تاب‌آوری باید همراه با دستورالعمل‌های ایمنی و تمرین عملیاتی باشد.

۳) ریسک حقوقی-بین‌المللی: در برخی تحلیل‌های سیاستی (از منظر چین)، اشاره شده که چارچوب‌های بین‌المللی مخابرات/فضا می‌تواند در «کنترل پوشش» محدودیت ایجاد کند و در نتیجه، تمرکز عملی سیاست باید بر «بخش زمینی و پایانه‌ها» و «رژیم مجوزدهی/اعمال قانون» باشد.

۴) ریسک وابستگی به شرکت: تجربه اوکراین نشان می‌دهد وابستگی به سرویس تجاری می‌تواند با تغییر سیاست، هزینه و تداوم خدمت دچار نوسان شود؛ لذا «تنوع‌سازی و قرارداد پایدار» ضرورت امنیت ملی است.

شاخص‌های کلیدی ارزیابی

شاخص تاب‌آوری ارتباطی: درصد خدمات حیاتی دارای مسیر پشتیبان (زمینی/ماهواره‌ای) + زمان بازیابی ارتباط در تمرین‌ها.

شاخص تاب‌آوری PNT: درصد سامانه‌های حیاتی مجهز به multi-constellation + INS fallback + نرخ رخدادهای GNSS-denied.

شاخص امنیت پیام: درصد پیام‌های بحرانی دارای سازوکار اصالت + زمان پاسخ به جعل.

شاخص حکمرانی پلتفرم: تعداد موج‌های هماهنگ شناسایی‌شده و مهار شده + زمان کشف/پاسخ.

شاخص حاکمیت تنظیم‌گری: درصد پایانه‌های ماهواره‌ای مجاز ثبت‌شده + میزان انطباق دستگاه‌ها با استاندارد رمزنگاری.

منابع

A parallel terrain: Public-private defense of the Ukrainian information environment - Atlantic Council - https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-/terrain-public-private-defense-of-the-ukrainian-information-environment

-44cb37b6/How Russia is jamming GPS around Europe - https://www.ft.com/content 98b951f464af-8c96-402f-2d82

Building the digital front line: Understanding big tech decision-making in Ukraine - Atlantic Council - https://www.atlanticcouncil.org/in-depth-research-reports/report/building-the-digital-/front-line

Digital sovereignty: Europe's declaration of independence? - Atlantic Council - https:// www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-europes-/declaration-of-independence

The coming compute war in Ukraine - Atlantic Council - https://www.atlanticcouncil.org/ /content-series/the-big-story/the-coming-compute-war-in-ukraine

Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, politics//13/10/2022/asks Pentagon to pick up the tab | CNN Politics - https://amp.cnn.com/cnn elon-musk-spacex-starlink-ukraine

CNN Exclusive: After Ukraine, Biden administration turns to Musk's satellite internet for Iran politics/white-house-musk-starlink-iran-/21/10/2022/| CNN Politics - https://amp.cnn.com/cnn protests-ukraine

The Satellite Encryption Gap: Why Everyday Citizens' Communications Are at Risk - https://www. csis.org/analysis/satellite-encryption-gap-why-everyday-citizens-communications-are-risk

The City-Sized Hole in U.S. GPS Planning | The Belfer Center for Science and International Affairs - https://www.belfercenter.org/publication/city-sized-hole-us-gps-planning

Digital Democracy in a Divided Global Landscape | Carnegie Endowment for International digital-democracy-in-/05/2025/Peace - https://carnegieendowment.org/russia-eurasia/research a-divided-global-landscape

Wartime content moderation and the Russian invasion of Ukraine - Atlantic Council - /https://www.atlanticcouncil.org/event/wartime-content-moderation

Starlink Militarization: Challenges and Responses to Space Intelligence and Information Security - Interpret: China - https://interpret.csis.org/translations/starlink-militarization- /challenges-and-responses-to-space-intelligence-and-information-security

مِتُد

مرکز توسعه دانش مسئله محوری

Mtod_ir

۰۲۱۹۱۰۹۳۴۲۴

۰۹۰۱۲۱۵۳۹۵۷

تهران، میدان ولیعصر، بلوار کشاورز، خیابان شوریده

تقاطع خیابان شوریده و پرویز، ساختمان سبحان، پلاک ۵، واحد ۳