



بیانیه ستاد کل نیروهای مسلح جمهوری اسلامی ایران

در قبال حقوق بین الملل فضای سایبری

(شماره یک)

مرکز فضای مجازی نیروهای مسلح - مرداد ۱۳۹۹

مقدمه

ستاد کل نیروهای مسلح جمهوری اسلامی ایران در گفتمان امنیت ملی برای بازدارندگی و دفاع سایبری در مواجهه و مقابله با تهدیدات متنوع و متکثر فضای سایبری مأموریت دارد.

تمامی سازمان‌ها و نهادهای ذی ربط در کشور با توجه به واگذاری مأموریت دفاعی به نیروهای مسلح و وفق فرمان مقام معظم رهبری و فرماندهی معزز کل قوا^{مدظله العالی}، می‌بایستی با ستاد کل نیروهای مسلح هماهنگی و هم‌افزایی داشته باشند و از آنجا که فضای سایبری به اذعان متخصصین امر قلمرو جدیدی در حوزه دفاعی و امنیتی است، سند پیش رو به عنوان "**بیانیه ستاد کل نیروهای مسلح جمهوری اسلامی ایران در قبال حقوق بین الملل فضای سایبری**"، مفاهیم، سیاست‌های کلان و چارچوب اقدامات نیروهای مسلح در مقابله با تهدیدات متنوع و متکثر فضای سایبری را تبیین می‌کند.

ماده ۱: کلیات

۱. معتقدیم، حقوق بین الملل قابل اعمال بر فضای سایبری باید توزیع کننده عادلانه منافع و امتیازات یک فضای صلح آمیز سایبری و متضمن «دسترسی» و «حاکمیت منصفانه» برای تمام دولت‌ها باشد.
۲. تاکید می‌نمائیم، هر چند تمامی دولت‌ها باید در برخورد با فضای سایبری مسئولانه عمل کنند، ولی به اقتضای امکانات و فناوری‌های موجود در هر کشوری، دولت‌ها مسئولیت مشترک ولی متفاوت دارند.
۳. براین باوریم، طیف وسیعی از اصول حقوقی بین المللی موجود، شامل اصول برابری حاکمیت دولت‌ها و ممنوعیت توسل به زور و عمل تجاوزکارانه می‌تواند در استفاده از فضای سایبری قابل اجرا باشد.

ماده ۲: سیاست‌های حاکمیتی نیروهای مسلح جمهوری اسلامی ایران

۱. جمهوری اسلامی ایران حوزه‌های حاکمیتی خود را با تمرکز و در انطباق با قابلیت‌های لازم برای حراست از اقتدار راهبردی نظامی، اقتصادی، اجتماعی، فرهنگی و سیاسی ملی توسعه داده است، در این مسیر، توسعه تخصص‌ها و ابزارهای پیشرفته سایبری، برای دفاع فعال و بازدارنده سایبری، از جمله اولویت‌های مهم برای تحقق و حفظ اقتدار راهبردی نظام است.
۲. قواعد حقوق بین الملل معاصر حکایت از وجود قلمرو محصور در مرزهای جغرافیایی دولت‌هایی دارد که حاکمیت یا لاقط صلاحیت خود را درون آن مرزهای جغرافیایی اعمال می‌کنند. به باور نیروهای مسلح جمهوری اسلامی ایران حاکمیت سرزمینی و صلاحیت دولت، بر تمامی اجزای فضای سایبری نیز تسری دارد.
۳. هر گونه استفاده عمدانه از زور سایبری با پیامدهای فیزیکی یا غیر فیزیکی که تهدیدی برای امنیت ملی بوده یا منجر به بی‌ثباتی آن به واسطه بی‌ثباتی سیاسی، اقتصادی، اجتماعی و فرهنگی شود، ناقض حاکمیت دولت است.
۴. عملیات بهره‌برداری سایبری در مواقعی که مستلزم نفوذ غیرمجاز به زیرساخت‌های سایبری (دولتی یا خصوصی) تحت کنترل دولت دیگری باشد، می‌تواند نقض حاکمیت دولت هدف تلقی شود.

۵. حاکمیت دولت‌ها واقعیتی فراحقوقی نیست و باید در کنار و با توجه به سایر اصول بنیادین حقوقی مانند اصل عدم مداخله، اصل حسن نیت، اصل حق تعیین سرنوشت و سایر اصول اساسی تفسیر گردد، باید توجه داشت که اصل حاکمیت دولت‌ها اصلی برابرگرا و مساوات طلب است و حاکمیت هیچ دولتی برتر از حاکمیت دولت دیگر نیست، لذا اقدامات محدودساز، مسدودساز و تحریم‌ها، نقض حاکمیت دولت‌های مستقل تلقی می‌شود، چرا که منجر به نادیده گرفته شدن حاکمیت دولت هدف می‌شود.

ماده ۳: مداخله در امور داخلی از منظر نیروهای مسلح جمهوری اسلامی ایران

۱. تردیدی نیست که اصل عدم مداخله یک اصل مستقل حقوق عرفی است و اعمالی با هدف تغییر رژیم سیاسی دولت‌ها مانند مداخله قهرآمیز سیاسی، نقض آشکار این اصل است. مواردی مانند دستکاری سایبری انتخابات یا مهندسی افکار عمومی در آستانه انتخابات را می‌توان از مصادیق آشکار مداخله تلقی کرد. همچنین مداخله شامل وضعیت‌هایی است که در آن مداخله غیرسایبری در فعالیت‌های سایبری مربوط به امور داخلی و خارجی دولت دیگر صورت می‌گیرد. عملیات سایبری که وب سایت‌ها را به منظور دامن زدن به نزاع و تنش‌های داخلی در یک دولت از کار می‌اندازند یا به منظور تأثیر گذاری بر نتیجه انتخابات در دولت دیگر پیام‌هایی را به صورت گسترده در بستر سایبری به رأی دهندگان ارسال می‌کنند را نیز می‌توان نمونه‌ای از مداخله ممنوعه تلقی کرد.
۲. مداخله مسلحانه و تمامی اشکال دیگر مداخله یا اقدام به تهدید علیه شخصیت دولت یا علیه عناصر سیاسی، اقتصادی، اجتماعی و فرهنگی آن با توسل به ابزار سایبری و غیرسایبری غیرقانونی است و هیچ دولتی نمی‌تواند دولت دیگری را با توسل به ابزار سایبری یا غیر آن به استفاده یا تشویق به استفاده از اقدامات اقتصادی، سیاسی یا هرگونه اقدام دیگری به منظور تحصیل تبعیت آن در اعمال حقوق حاکمیتی‌اش یا تضمین کسب امتیازاتی از آن، از هر نوع، وادار نماید.
۳. تمامی اشکال آشکار، ظریف و تکنیک‌های بسیار پیچیده اجبار، براندازی و هتک حرمت (اعم از سایبری و غیرسایبری) با هدف اخلال در نظم سیاسی، اجتماعی یا اقتصادی سایر دولت‌ها یا بی‌ثبات سازی حکومت‌هایی که در صدد آزادسازی نظام اقتصادی و سیاسی و فرهنگی خود از کنترل یا دست اندازی خارجی هستند، غیر قانونی است.
۴. دولت‌ها حق ذاتی بر توسعه کامل سیستم اطلاعات و رسانه‌های جمعی، بدون مداخله، و استفاده از رسانه‌های اطلاعاتی، به منظور پیشبرد منافع و آرمان‌های سیاسی، اجتماعی، اقتصادی و فرهنگی خود دارند. اقداماتی که منجر به ممانعت، قطع و یا محدود شدن عملکرد سیگنال‌ها و ابزار انتقال اطلاعات و سیستم‌های تأمین کننده کنترل و اعمال حاکمیت دولت می‌شود غیر قانونی است.
۵. برنامه‌های ظرفیت‌سازی در حوزه سایبر باید بر اساس برنامه‌ها و نیازهای ملی دولت‌ها و در انطباق با وضعیت اقتصادی، اجتماعی و فرهنگی آنها طراحی و اجرا شود و خود وسیله‌ای برای مداخله در امور داخلی آنها نباشد.

ماده ۴: توسل به زور و حمله سایبری از منظر نیروهای مسلح جمهوری اسلامی ایران

۱. به باور نیروهای مسلح جمهوری اسلامی ایران تردیدی نیست که آن دسته از عملیات سایبری که منتج به ایراد خسارات مادی به اموال یا صدمه به افراد در گستره و شدت لازم می‌شود یا به طور منطقی احتمال زیادی دارد که چنین آثاری را به بار آورد، توسل به زور محسوب می‌شود. اگر این نوع از عملیات زیرساخت‌های حیاتی ملی، شامل زیرساخت‌های دفاعی را متأثر سازند، طبیعتاً ناقض قاعده توسل به زور تلقی خواهند شد، اعم از این که در مالکیت حکومت یا بخش خصوصی باشند.
۲. به باور نیروهای مسلح جمهوری اسلامی ایران چنانچه شدت عملیات سایبری به زیرساخت‌های حیاتی کشور به آستانه حمله مسلحانه متعارف ارتقاء یابد، حق دفاع مشروع برای نیروهای مسلح جمهوری اسلامی ایران محفوظ است.

جمع بندی

نیروهای مسلح جمهوری اسلامی ایران به سان دکترین قابل اعمال خود در فضای فیزیکی، در فضای سایبری نیز آغازگر هیچ منازعه‌ای نیستند و خط مشی تبیین شده در این سند را به عنوان چارچوب اقدام خود در مواجهه و مقابله با تهدیدات متنوع و متکثر فضای سایبری قلمداد می‌کنند.

بدیهی است نیروهای مسلح جمهوری اسلامی ایران در صورت نقض هر یک از خط مشی‌ها و سیاست‌های تبیین شده، از سوی دولت، گروه یا فردی که تحت حمایت، هدایت یا کنترل دولتی باشد، این حق را برای خود قائل هستند که تهدیدات را در هر سطحی با قدرت و پشیمان کننده پاسخ دهند.