.کترین ملّی «عضو فلج»، استراتژی مقابله با جاسوسی پنج چشم

یکی از مسائل اصلی که در حوزه «سبک زندگی» مورد بررسی قرار می‌گیرد، مسئله ترکیب زندگی بشریّت با تکنولوژی دیجیتالی است. در حالی که نه تنها فقط مردم عادی بلکه حتی متخصصان عرصه فناوری‌اطلاعات، بر این باور اشتباه استوار شده‌اند که: «تکنولوژی برای رفاه بشر ساخته شده و باید قدم به قدم با آن پیش رفت»، این مطلب اثبات گشته که هدف اصلی از اشاعه تکنولوژی سایبری در سراسر جهان، تحقق تبدیل سازمان‌های پنج چشم به «مغز جهان» بوده است. از این رو خطری عظیم در کمین امنیت ملت‌ها است و این در حالی است که راه برگشتی برای آن وجود ندارد و نمی‌توان فضای سایبر را از جوامع باز ستاند.

اما اگر سازمان‌های پنج چشم، سبک زندگی دیجیتالی را جهت تحقّق کنترل جهانی و پیش‌برد اهداف‌شان در سراسر جهان ایجاد نموده‌اند و دیگر نمی‌توان ابزار دیجیتال را از مردم ستاند، باید با آگاهی‌بخشی و ایجاد فرهنگ «بیداری امنیتی – اطلاعاتی» و تزریق آن به متن جامعه، از نا امنی کابران این تکنولوژی جلوگیری نمود.

خواسته فوق محقق نمی‌شود مگر آنکه مبانی آن را تئوریزه کنیم و از نسل جدید و در سنین کودکی، آموزش و آگاهسازی را شروع نماییم و این آموزش‌ها، بطور مستمر ادامه یابد تا شخص به قدرت تشخیص خطرهای دیجیتالی واقف گردد و این روند باید در جامعه به‌عنوان یکی از ضروری‌ترین و حیاتی‌ترین ابعاد آموزشی، همیشه جاری و در حال تکمیل باشد.

اما با توجه به مطلب فوق و آنچه که در مقاله «تحقق قلب جهان و مغز جهان در پیکره زمین» بیان گردید، در این بخش به ارائه دکترین ملّی «عضو فلج» جهت مقابله با این تهدید جدی و روز افزون می‌پردازیم.

همانطور که گفته شد، چون امکان بازگشت جوامع به پیش از گسترش تکنولوژی سایبر وجود ندارد، لذا شرایط فعلی را می‌پذیریم و آن را غیر قابل تغییر فرض می‌کنیم. دلیل این فرض اینست که زندگی مردم سراسر جهان، با تکنولوژی دیجیتالی آمیخته شده و نمی‌توان از آن بازگشت و حتی اگر جمهوری اسلامی ایران را از فضای سایبر دور کنیم، به انزوای بزرگی خواهیم رسید و این موجب توقف بسیاری از پیشرفت‌ها در علوم ملّی است.

پس باید بپذیریم در پیکره زمین، هر چند که نقش بی‌بدیل قلب را داریم اما در برقراری ارتباطات داخلی و فرامرزی، تحت اختیار مغزی هستیم که موسوم به پنج چشم است. حال به‌عنوان عضوی از این بدن که قسمت مغز، اطلاعات و ارتباطات ما را تحت کنترل خود دارد و به‌دنبال ارائه دستور در پاسخ به اعمال و حالات ماست، دکترین ملّی «عضو فلج» را ارائه می‌کنیم.

در بدن یک انسان معلول جسمی – حرکتی، عضو فلج وی را در نظر بگیرید. این عضو از کلیه منابع بدن استفاده می‌کند. از نظر بقاء؛ حیاتی کاملاً طبیعی و مشابه به دیگر اعضای سالم دارد. فعالیّت‌های حیاتی و سلولی در آن جریان دارد اما به‌دلیل قطع سیستم عصبی، اطلاعات خود را به مغز نمی‌دهد و طبیعتاً دستوری از مغز دریافت نمی‌کند. بعبارت دیگر، در نتیجه قطع ارتباط با مغز از دستورات مغز تبعیت نمی‌کند ولی بصورت همزمان، با دیگر اندام‌ها و مکانیسم‌های بیولوژیکی ارتباط سالم دارد و از قلب تغذیه می‌کند.

بنا بر ادعای مسئولین ایالات متحده، جمهوری‌اسلامی ایران کشوری است که اولین و اصلی‌ترین جامعه هدف مراکز اطلاعاتی سایبری غرب است، لذا باید

امکان تبدیل شدن به «عضو فلج» از نظر ارتباطات دیجیتالی مهیا شود. یعنی در فرایند توسعه فضای سایبری کشور، ساختاری طراحی گردد که ارتباطات کشور را از جهان جدا نموده و تنها در درون خودش جریان بخشد. البته این مسئله به معنی قطع ارتباط با پایگاه‌های داده خارج از ایران نیست بلکه دسترسی کنترل شده و غیر مستقیم کلیه عناصر سایبری فرامرزی را در تقابل با فضای سایبری ملّی رقم می‌زند. در چنین حالتی، هم ارتباطات سایبری و هم ارتباط‌های دیگر مانند تعاملات سیاسی، اقتصادی، نظامی، علمی و ... با دیگر کشورها که منجر به حفظ حیات می‌شود، همچنان ادامه دارد و خدشه‌ای به آنها وارد نمی‌شود.

به منظور تحقق راهکار فوق باید سیستمی ارتباطی درون کشور ایجاد گردد که از کلیه ابزارهای جاسوسی اطلاعاتی به‌دور باشد.

سازمان‌های پنج چشم خصوصاً آژانس امنیت ملی آمریکا، شیوه‌های بسیار متنوعی را برای دسترسی به اطلاعات ملی کشورها طراحی و اجرا نموده‌اند که در حالت کلی موارد زیر را شامل می‌شود:

الف) چیپ‌ست‌های سخت‌افزاری

ب) کلیه سیستم‌های عامل

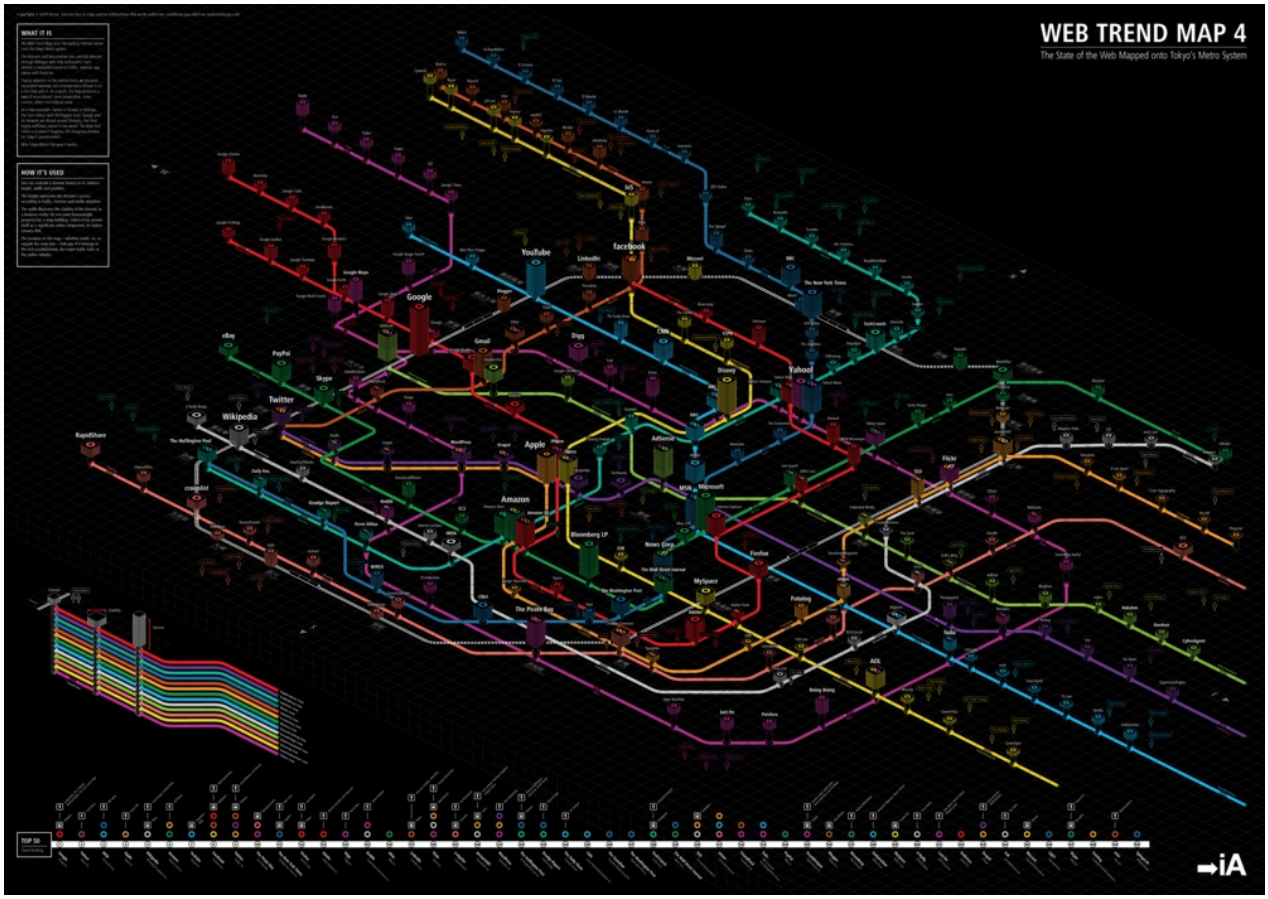
پ) تمامی منابع سایبری شامل منابع اینترنت مانند: موتورهای جستجوی آشکار، موتورهای جستجو پنهان که شما را در تمام مدت اتصال به اینترنت ردیابی می‌کنند، شبکه‌های اجتماعی و فروم‌ها، بدافزارهای جاسوسی مثل تروجان‌ها.

ت) برنامه‌های کاربردی تحت سیستم‌عامل یا تحت وب

ث) پروفایل‌های اطلاعاتی شخصی مانند پروفایل دانشگاهی یا فرم بیمه آنلاین افراد

ج) قابلیت‌های سخت‌افزاری اسمارت فون‌ها، تبلت‌ها و لپ‌تاب‌ها

چ) تمامی پروتکل‌ها و قوانین پیاده شده



پس نیاز است که در یک برنامه منسجم و منظم، کلیه موارد فوق به‌صورت بومی تولید شود تا تمامی راه‌های جاسوسی اطلاعاتی در کشور برای پنج چشم از بین برود.

این مسئله بدین معنی است که در هر زمینه‌ای، باید همه چیز را از صفر و تحت نظر طرح‌ریزی‌های امنیتی شروع نمود و از کلیه ابزار، کد یا اشخاصی که مرتبط با فضای خارج از طرح هستند پرهیز کرد.

به هیچ‌وجه نباید فراموش کرد که کلیه زمان‌ها و هزینه‌های صرف شده، تنها با هدف پاک‌سازی عوامل جاسوس سایبری و خطر دیجیتالی در کشور صورت

می‌پذیرد، نه ارائه همین خطرات به شکلی بومی و با دست خودمان!

لذا خودمان را فریب ندهیم و بدانیم که باید از شیوه‌هایی نظیر دست‌کاری در سیستم‌های عامل و ارائه آنها با ظاهری جدید و امکانات جانبی فارسی، اجتناب نمود؛ در حالی که همچنان از کدهای پایه شرکت تولیدکننده غربی استفاده می‌کنند.