مطالبه غرامت حملات تروریستی سایبری آمریکا به زیرساخت‌های سایبری ایران

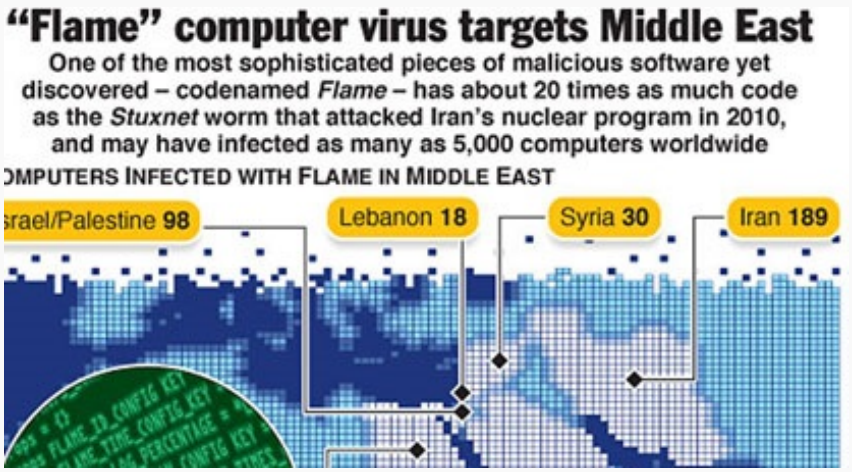
ایالات متحده آمریکا بعنوان کشوری که صراحتاً از سوی بنیانگذار جمهوری‌اسلامی ایران «شیطان بزرگ» و «ام‌الفساد» لقب گرفت، به نیابت از انگلیس روباه صفت، بزرگترین دشمن امروز اسلام و ایران است و در راه ابراز دشمنی و تحقق اهداف خصمانه‌اش از هیچ راهی فروگذار نکرده و نخواهد کرد.

تنها بخشی از اقدامات تروریستی آمریکا بر ضد ج.ا.ایران و امت اسلامی، شامل کودتا، بر افروختن و تحمیل جنگ هشت ساله، ترور شخصیت‌های سیاسی، ترور شخصیت‌های مذهبی، ترور دانشمندان، پشتیبانی از گروه‌های تروریستی مانند سازمان منافقین، براندازی فرهنگی، جنگ رسانه‌ای و دروغ پراکنی و سیاهنمایی، تجهیز مخالفان ایران، ایجاد شورش‌های قومی و اقلیت‌های مذهبی، نفوذ نظامی به درون کشور (عملیات پنجه عقاب که به طبس شناخته می‌شود)، نقشه‌چینی برای براندازی نرم جمهوری‌اسلامی ایران (فتنه ۸۸)، تحریم‌های پیاپی و البته غیر قانونی اقتصادی و سیاسی، مصادره اموال دولتی ایران بصورت غیر قانونی و بسیاری اقدامات دیگر است که بطور واضح در اسناد تاریخی ۳۵ ساله اخیر وجود دارد.

البته اینها تنها جنایات این رژیم منحوس و شیطانی پس از وقوع انقلاب اسلامی است و اگر به دیگر اقدامات این کشور بر ضد ایران پیش از انقلاب بپردازیم، حتی بیان تیتروار آن نیز ار حوصله این بحث خارج است.

اما یکی از جنایات و اعمال دولت تروریست‌پرور آمریکا در قبال ایران، طراحی و اجرای حملات تروریستی سایبری بوده است که در زمان فعلی به شدت در حال اوجگیری و افزایش می‌باشد.

در این راستا دو اقدام معروف دولت آمریکا و متحد صهیونیستش که بر همگان روشن است، با نام سلاح «استاکس‌نت»[1] و سلاح «فلیم»[2] شناخته می‌شود اما اینها تنها بخشی از حملات سایبر تروریسم ایالات متحده آمریکا است.



میزان آلودگی ایران و متحدانش به سلاح فلیم

اجرای عملیات کوانتوم بر ضد تأسیسات اتمی ایران، تلاش برای دستیابی به شبکه‌های کامپیوتری زیرساخت‌های حساس کشور، ارسال تجهیزات سخت‌افزاری جاسوسی در بازار مصرف ایران، تعیین ایران به عنوان اولین و مهمترین هدف حملات آژانس امنیت ملی آمریکا، تعریف پروژه ویژه برای تحت نظر داشتن امام خامنه‌ای بصورت ۲۴ ساعته، تحریم شبکه‌های بین‌المللی صدا و سیمای ج.ا.ایران روی ماهواره‌های جهانی و ... همگی در راستای تروریسم سایبری آمریکا علیه ایران است.

اقداماتی که تا کنون خسارات سنگینی را در ابعاد مختلف به منافع مادی و معنوی میهن عزیزمان وارد نموده و پس از این نیز سنگین‌تر خواهد شد.

حال سؤال اصلی این است که وظیفه ما در برابر تروریست سایبری دولتی آمریکا چیست؟

برای پاسخ به این سؤال باید دو بازه زمانی تعریف گردد:

الف) اقداماتی صورت گرفته در گذشته

ب) عملیات‌های در دست اقدام برای آینده

مسلماً آنچه که در گذشته رخ داده است قابل بازگشت نیست و خسارات آن تنها از طریق جایگزینی و بازسازی قابل جبران خواهد بود. باید از آنچه که رخ داده درس گرفته و هوشیارتر باشیم تا از تکرار آن در آینده جلوگیری به عمل آید اما این دست اقدامات ملی نباید تنها به بُعد اصلاح و جایگزینی محصور شود بلکه مطرح کردن موضوع اقدامات تروریستی در مراکز حقوقی جهانی و ارائه اسناد آن جهت اثبات و نهایتاً درخواست پرداخت غرامت به ج.ا.ایران، بخش اصلی وظایف مسئولین مربوطه در ارتباط با حملات گذشته است.

همچنین برای آینده، جدا از اینکه آمادگی و توان رزمی سایبری افزایش می‌یابد، باید ساز و کاری در نظر گرفت که در صورت وقوع اقدامات تروریستی آتی از طریق آن بتوان بطور سنگین‌تری آمریکا و متحدانش را شرمنده نمود و به عذرخواهی و سپس پرداخت غرامت واداشت.

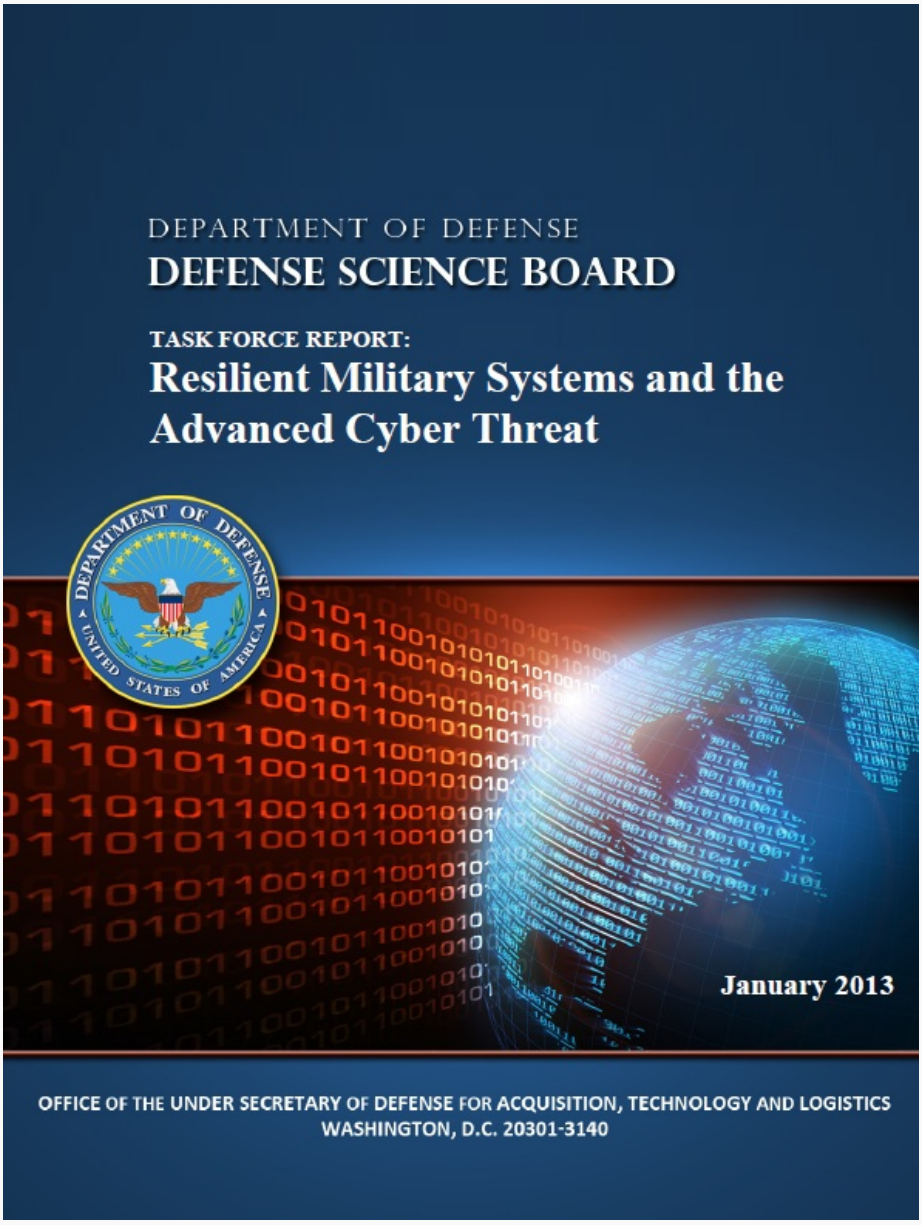
یکی از بهترین شیوه‌های بازدارندگی، اقدام متقابل است که با اصطلاح «**مقابله به مثل**» از آن یاد می‌شود. در حال حاضر توان رزم سایبری ایران به حدی عمیق و بالا است که به راحتی امکان مقابله به مثل با حملات سایبری ایالات متحده، انگلیس، اسرائیل و دیگر متحدان پنج چشم را دارد و دشمن باید از این بابت مطمئن باشد که در صورت وقوع هرگونه حادثه تروریستی برضد فضای سایبری ملی و زیرساخت‌های حساس سایبری ایران، سیستم های امنیتی ایران از اقدام متقابل به هیچ عنوان چشم‌پوشی نخواهند کرد.

سازمان‌های پنج چشم بعنوان بی بدیل‌ترین تروریست‌های سایبری جهان، این نکته را مد نظر خواهند داشت که: «**امنیت حقی جهانی است و هیچ کشوری حق محروم سازی دیگران را از آن ندارد**».

از طرف دیگر ایالات متحده در پروتکل‌های امنیت سایبر خود بطور صریح ابراز داشته است که: «آمریکا در مقابل اعمال خصمانه در فضای مجازی به عنوان تهدیدی بر علیه منافع کشور پاسخ خواهد داد. **همه کشورها دارای حق ذاتی برای دفاع از خود هستند**، و به اعمال خصمانه ای که از طریق فضای مجازی صورت می گیرد با توجه به تعهدات ما در قبال هم‌پیمانان نظامی خود با اقدامات نظامی به آنها پاسخ خواهیم داد.»

همچنین طی گزارشی که شورای علمی وزارت دفاع ایالات متحده در ژانویه ۲۰۱۳ تهیه نموده با صراحت «امکان استفاده ایالات متحده از تسلیحات هسته‌ای برای مقابله به مثل در برابر حمله سایبری گسترده» لحاظ گردیده است.

با استناد به موارد فوق و پیش‌دستی ایالات متحده در طراحی و اجرای اقدامات تروریستی علیه تأسیسات سایبری ج.ا.ایران، واضح خواهد بود که قانوناً و ذاتاً حق مقابله به مثل و درخواست غرامت را داریم و خواهیم داشت. از این رو در تهیه روندی که در آینده منجر به افزایش ضریب امنیت سایبری ایران شود، مسئله **دعوی حقوقی بین‌الملل** و **مقابله به مثل** بیش از دیگر موارد اهمیت دارد.



گزارش شورای علمی وزارت دفاع آمریکا

پس سران انگلیس، آمریکا و کشورهای عضو پنج چشم این مهم را بدانند که در صورت وقوع هرگونه حمله تروریستی علیه منافع ج.ا.ایران در فضای سایبر، با مقابله به مثلی روبرو خواهند شد که یقیناً برای آنها غیر قابل پیش‌بینی خواهد بود و همواره باید این را مد نظر داشته باشند که «**دشمنان ایران می‌توانند شروع کننده یک جنگ سایبری بر ضد جمهوری‌اسلامی ایران باشند اما نقشی در چگونگی پایان یافتن آن و عواقب پیش‌رو نخواهند داشت.**»

۱- Stuxnet

۲- Flame