

افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نباشد تن من مباد بدین بوم و بر زنده یک تن مباد
همه سر به سر تن به کشتن دهیم از آن به که کشور به دشمن دهیم

www.afgazad.com

afgazad@gmail.com

Political

سیاسی

فرستنده: مجله هفته

۱۶ می ۲۰۲۰

رسانه چینی:

کاخ سفید، «امپراتور هکرهای جهان»؛ پشت پرده «حادثه کنارک»



به گزارش رادیو بین‌المللی چین، ناوچه کنارک نیروی بحری ارتش ایران اخیراً در یک مانور نظامی به اشتباه هدف اصابت راکت شلیک شده از سوی ناوگان ایران قرار گرفت که این حادثه ۱۹ کشته و ۱۵ مجروح برجای گذاشت. «آیت الله خامنه‌ای» رهبر ایران خواستار رسیدگی به این حادثه شده و «حسن روحانی» رئیس‌جمهور ایران نیز گفته است که دلایل حادثه برای مردم بیان می‌شود.

این در حالی است که برخی رسانه‌ها از وجود یک توطئه وحشتناک در پشت پرده وقوع این حادثه خبر داده و مدعی شده‌اند که این حادثه به دلیل حمله هکرهای امریکایی به شبکه دفاع ملی ایران افتاده است.

روزنامه اسرائیل «جرورالم پست» در تاریخ ۱۱ ماه مه، در گزارشی از احتمال بروز این حادثه به دلیل حمله سایبری امریکا علیه ایران خبر داد و مدعی شد که با توجه به گستردگی شبکه نظامی امریکا در جهان و همچنین در نظر گرفتن وخامت روابط فعلی میان تهران و واشنگتن در سایه تمدید تحریم‌های تسلیحاتی بین‌المللی علیه ایران، دولت امریکا از انگیزه کافی برای انجام چنین حمله‌ای برخوردار بوده است.

از طرف دیگر، در حالی که برخی از رسانه های خبری ایران از حمله سایبری صورت گرفته به بندر شهید رجائی حکایت می کنند، سایر رسانه های خبری این کشور، وقوع چنین حمله ای را تکذیب کرده اند.

آنچه بدیهی به نظر می رسد، این است که در طول سال های اخیر، انجام حملات سایبری، یک روش متعارف از سوی دولت واشنگتن علیه ایران بوده است؛ در تاریخ ۶ اپریل سال ۲۰۱۸ میلادی بود که عملکرد بسیاری از کامپیوترها در ایران مختل و وارد وضعیتی غیر عادی شد و متعاقب آن، پرچم امریکا بر روی مانیتور این کامپیوترها به نمایش در آمد.

در جریان این حمله سایبری علیه ایران، عملکرد ۳۵۰۰ سرور کامپیوتر مختل و اتصال شبکه ای به ۲۰۰ هزار روتر در سراسر جهان مختل و ارتباط اینترنتی نیز قطع شد.

آمارها نشان می دهد ایران در سال ۲۰۱۹ میلادی، بیش از ۳۳ میلیون حمله سایبری را خنثی کرده است. کاخ سفید «امپراتور هکرها»ی جهان امروز به حساب می آید و در دراز مدت، با نقض قوانین بین الملل و اصول روابط بین الملل، حملات سایبری مخفیانه و سازمان یافته و گسترده ای را علیه دولت های خارجی، نهادها و افراد در سراسر جهان عملیاتی کرده و یا اقدام به شنود غیرقانونی کرده است و یک مجرم شناخته شده در این زمینه محسوب می شود و این موضوع برای جامعه جهانی بسیار آشنا است.

چین نیز یکی از قربانیان اصلی حملات سایبری امریکا به حساب می آید. بر اساس جدیدترین تحقیق ها و افشاگری های صورت گرفته توسط شرکت امنیت سایبری چینی موسوم به «۳۶۰»، سازمان هک «APT-C-39» وابسته به سازمان اطلاعات مرکزی امریکا «سیا»، در طول بیش از ۱۰ سال، اقدام به انجام حملات سایبری و نفوذهای کمپیوتری در چین کرده است.

نگاهی به «ویکی لیکس» و افشاگری های «ادوارد سنودن» با کمک تجهیزات رمزگذاری شرکت «کریپتو» سوئیس، این حقیقت را مکرراً به اثبات می رساند که دولت امریکا بزرگ ترین دزد امنیت شبکه ای جهان است.

عادت همیشگی کاخ سفید این است که با این که خودش مجرم است، دیگران را متهم به ارتکاب جرم نشان می دهد؛ دولت واشنگتن همواره مدعی بوده که هدف حمله هکهای ایرانی و چینی قرار گرفته است.

امریکائی ها در جدیدترین مورد ادعائی خود گفته اند که «هکهای چینی در تلاشند تا نتایج توسعه واکسین و داروهای درمان کرونای امریکا را به سرقت ببرند». این در حالیکه چین به عنوان کشوری با بیشترین تجربه در عرصه مقابله با ویروس کرونا، هیچ نیازی به هک و سرقت اطلاعات امریکا ندارد و به عکس باید گفت که طرح چنین اتهاماتی از سوی امریکا یادآور این نکته است که چین باید از دستاوردهای خود در زمینه تولید واکسین و ویروس کرونا محافظت کند و قاطعانه مانع از حملات سایبری و سرقت اطلاعات و دزدی امریکا شود.