مردم سالاری

حاکمیت حق مردم است

یکشنبه ۵ شهریور ۱۴۰۲ - ۱۰ صفر ۱۴۴۵ - ۲۷ آگوست ۲۰۲۳ - سال بیست و دوم - شماره ۶۰۶۸ - ۱۲ صفحه - ۷۰۰۰ تومان

نیاز اقتصاد ایران به خلاص شدن از تحریم‌ها

صفحه۲

هشدار درباره ریاست‌جمهوری لوپن در فرانسه

صفحه۱۱

سکه و ارز با گزارش توافق غیررسمی ایران و آمریکا ریزشی شد

واکنش مثبت بازار به کاهش تحریم‌ها

صفحه۱۰

شاخص‌های سلامت کاهش یافته است
مرگ زودرس ایرانی‌ها

صفحه ۴

پرستیژ فروریخته آمریکا در خاورمیانه

گاردین در مطلبی به قلم سایمون تیسدال نوشت: نحوه کاهش نفوذ آمریکا در خاورمیانه به نظر می‌رسد مشابه عقب نشینی خفت بار چند دهه قبل بریتانیا از همان منطقه است. گویی کشورهای منطقه که پیشتر از دست یک امپراتوری خودرای و مغرور خلاصی یافته‌اند، اکنون ابرقدرت دیگری را کنار می‌گذارند. رژیم‌های حاکم و رهبران اقتدارگرا به آرامی اما...

صفحه۳

بزرگترین انتقال سال فوتبال ایران

ستاره تیم ملی ایران با عقد قراردادی به مدت یک فصل به عضویت رُم درآمد. به گزارش «ورزش سه»، سردار آزمون که ۴۸ ساعت قبل برای انجام توافق نهایی با باشگاه رم راهی پایتخت ایتالیا شده بود و مذاکرات مثبتی با مدیران این تیم داشت، قراردادش را به طور رسمی امضاء کرد و به جمع شاگردان ژوزه مورینیو پیوست. باشگاه رم رسما از...

صفحه۸

سناریوی کرملین برای این گروه خشن

گروه بین‌الملل- علی ودایع: سقوط هواپیمای رهبران گروه واگنر و مرگ «یوگنی پریگوژین» همچنان سرخط رسانه‌های جهان است. منابع غربی همگی انگشت اتهام را به سمت «ولادیمیر پوتین» رئیس‌جمهوری روسیه نشانه رفته‌اند. کمیته تحقیقات روسیه اعلام کرد که ۲ دستگاه ضبط‌کننده پرواز (جعبه سیاه) مربوط به هواپیمایی که در استان تِوِر این کشور...

صفحه۱۱

سرمقاله

ضعف دیپلماتیک دولت در عرصه سایبری

سجاد عابدی

در جریان تحولات ناشی از عصر فناوری اطلاعات و ارتباطات و تحول در روش‌های ارتکاب جرایم، جرایم سنتی به جرایم نوین مجازی وارد شده است. جرم تروریسم که در دنیای سنتی از قدیم‌الایام به عنوان یک جرم مهم امنیتی مدنظر بوده، این روزها چهره‌ای گسترده به نام مجازی به خود گرفته و با ورود به این دنیای گسترده، صدمات و لطمات وسیعی را مدنظر خود قرار داده است. حال با توجه به اینکه اکثریت ساختارها و زیرساختارهای کشورها مبتنی بر فضای مجازی و تکنولوژی رایانه‌ای شده‌اند و این واقعیت که نه می‌توان از رایانه و این تکنولوژی مفید دست کشید و نه می‌توان تروریست‌های سایبری را نادیده گرفت را نیز پیش‌رو داریم، کشورها باید همواره در پی به‌روزرسانی و تقویت سیستم‌های خود باشند، چراکه همواره تروریست‌های ملی و فراملی به دنبال فرصت و شکافی برای ورود و ضربه زدن به امنیت و بقای دولت‌ها و ملت‌ها هستند.

برای نمونه طراحی و اجرای حملات تروریستی سایبری، در کنار کودتا، برافروختن و تحمیل جنگ، ترور شخصیت‌های سیاسی، مذهبی، دانشمندان، براندازی فرهنگی، جنگ رسانه‌ای و... یکی از جنایات و اعمال دولت‌ها و افراد تروریست در قبال دولت‌ها و ملت‌ها بوده است که از نمونه‌های بارز رایانه‌ای آن‌ها استفاده از سلاح استاکس نت (Stuxnet) و فلیم (Flame) برای دستیابی به شبکه‌های کامپیوتری زیرساخت‌های حساس کشورها و سعی در برهم زدن امنیت آن‌ها را می‌توان نام برد.

تروریسم سایبری به عنوان گونه‌ای جدید از تروریسم، نشانگر آسیب‌پذیربودن تابعان حقوق بین‌الملل در فضای سایبر است.

اگر تروریست‌ها زیرساخت‌های حیاتی یک دولت مانند حمل و نقل هوایی، سدها، نیروگاه‌های هسته‌ای و تولید برق، سیستم بانکی و مالی را با انواع بدافزارها مورد حمله قرار دهند و از این طریق باعث رعب و وحشت عمومی گردند و با داشتن انگیزه‌های سیاسی یا ایدئولوژیک این اقدامات را در راستای اجبار دولت یا سازمان‌ها انجام دهند، آنگاه تروریسم سایبری محقق می‌گردد.

جامعه جهانی بر سر تعریف جامعی از تروریسم، به توفیقی دست نیافته و حتی سند جامع الزام‌آوری نیز در این موضوع وجود ندارد، اما این شکل از تروریسم به همراه دیگر گونه‌های نوینی چون بیوتروریسم، تروریسم هسته‌ای و اکوتروریسم، ممکن است خسارات زیان‌بارتری نسبت به انواع کلاسیک تروریسم ایجاد کند. تروریسم سایبری تهدیدی علیه صلح و امنیت بین‌المللی است و در عین حال ناقض قواعد حقوق بشر در هر چهار نسل شناخته شده آن نیز به شمار می‌آید. اهمیت پرداختن به نقض حقوق بشر توسط تروریست‌ها در فضای سایبر و نیز در سیاق مبارزه با تروریسم سایبری در مقابله همه‌جانبه با این پدیده باید مطمح نظر قرار گیرد.

الکترونیکی شدن «زیرساخت‌های حیاتی» همان‌گونه که طراحی، نگهداری و استفاده از آن‌ها را آسان‌تر کرده است، اما خطراتی که موجب آن‌ها می‌شود را نیز افزایش داده است. اگر کسی بتواند از سدهای امنیتی این زیرساخت‌ها عبور کند و کدهای امنیتی آن‌ها را هک کند می‌تواند در عرض چند ثانیه بخشی از یک کشور یا حتی بخش‌هایی از جهان را فلج کند. تروریست‌های سایبری هم اغلب روی همین زیرساخت‌های حیاتی متمرکزند.

ماهیت «چندرسانه‌ای» فضای سایبر، به تروریست‌ها امکان بهره‌برداری‌های سوء دیگری را هم داده است. فشار یک دکمه کافی است تا انتشار بدافزارهای مخرب رایانه‌ای در عرض چند ثانیه هزاران سیستم رایانه‌ای و مخابراتی در جهان را آلوده کند. رایج‌ترین روش‌های این نوع تروریسم عبارتند از: هک کردن، شیوع ویروس‌های رایانه‌ای، جاسوسی الکترونیک، دزدی هویت و تخریب یا دستکاری اطلاعات. نرم‌افزارهای مخرب رایانه‌ای که تروریست‌های سایبری برای پیشبرد اهداف خود استفاده می‌کنند، متنوع هستند که از جمله آن‌ها می‌توان به ویروس‌ها، کرم‌ها، تروجان‌ها و اسپم‌ها اشاره کرد.

هک و نفوذ رایانه‌ای و خرابکاری اینترنتی و شبکه‌ای نیز بخشی دیگر از ابزارهای تروریست‌های سایبری به شمار می‌روند. از آنجایی‌که شبکه‌های اینترنتی در دسترس همگان قرار دارد و بسیاری از سایت‌ها و زیرساخت‌های حیاتی کشورها در بستر اینترنت ارائه می‌شود، تروریست‌های سایبری می‌توانند سنگین‌ترین قفل‌های امنیتی را هم با روش‌های خاص خود بشکنند و در عرض چند ثانیه به اهداف خود دست یابند.

«دوروتی دنینگ» استاد علوم رایانه‌ای دانشگاه جرج تاون درباره ماهیت تروریسم سایبری می‌گوید: سایبر تروریسم، بیشتر به معنای حمله یا تهدید علیه رایانه‌ها، شبکه‌های رایانه‌ای و اطلاعات ذخیره شده در آنهاست، هنگامی‌که به منظور ترساندن یا مجبور کردن دولت یا اتباع آن برای پیشبرد اهداف سیاسی یا اجتماعی خاص اعمال می‌شود. یک حمله، برای اینکه به عنوان تروریسم سایبری شناخته شود باید به خشونت علیه اشخاص یا دارایی‌ها منجر شود یا دست‌کم آسیب کافی برای ایجاد ترس را باعث شود. حملاتی که منجر به مرگ یا صدمات بدنی، انفجار، سقوط هواپیما، آلودگی آب یا خسارات متعدد اقتصادی می‌شود را می‌توان به عنوان مصادیق تروریسم نام برد.

امروزه بسیاری از فعالیت‌های تروریستی به شکل حملات هکری و در قالب دزدی اطلاعات صورت می‌گیرد. نخستین‌بار در سال ۱۹۸۲ هکرهای طرفدار دولت پاکستان با نام «باشگاه هکرهای پاکستانی» به کامپیوترهای هند حمله کردند. در سال ۱۹۹۹ هنگام حمله ناتو به کوزوو سایت این سازمان مورد حمله قرار گرفت. در همان زمان، وب سایت ارتش آمریکا و سایت‌های تجاری این کشور به وسیله هکرهای چینی، روسی و صرب مورد حمله قرار گرفت. کشور ما نیز بارها مورد حمله‌های تروریسم سایبری قرار گرفته است. سال ۸۹ کرم جاسوسی استاکس‌نت صنایع مربوط به بخش نفت و نیرو کشورمان را مورد حمله قرار داد.

یکی از جدی‌ترین حملات سایبری حمله‌ای بود که نسبت به تجهیزات نفتی کشورهای خاورمیانه صورت گرفت. این بدافزار که با نام فلیم (شعله آتش) به کشورهای مختلفی ارسال شده بود، پیچیدگی‌های متعددی داشت و علاوه بر جاسوسی، یک ویروس مخرب به شمار می‌رفت. در طول سال‌های فراگیر شدن اینترنت در ایران بارها ویروس‌های مختلف جاسوس و بدافزارهای مخرب زیرساخت‌های کشورمان را مورد حمله قرار داده‌اند. استارس و دوکو نیز دو نمونه دیگر از ویروس‌هایی هستند که اخبار حمله آن‌ها به ایران رسانه‌ای شده است. تروریست‌های سایبری بی‌تردید همین حالا که شما مشغول مطالعه این گزارش هستید در حال طراحی بدافزار یا اجرای برنامه‌های تروریستی خود هستند.

شاید اصلی‌ترین راهکار برای داشتن اینترنتی ایمن، اجرای یک طرح جامع امنیت ملی در حوزه سایبری باشد. طرحی که شبکه ملی اطلاعات هم می‌تواند از اجزای آن باشد. در این طرح می‌بایست به حوزه‌های آموزش عمومی، تقویت سیستم‌های دفاعی و توان مقابله و اجرای عملیات در هر سطح علیه مهاجم مورد توجه قرار گیرد. همچنین نیاز است ملاحظات مربوط به پدافند غیرعامل در همه طرح‌های مربوط به شبکه‌های ارتباطی و الزام دستگاه‌های اجرایی به استفاده از توان داخلی (تا حد امکان) مدنظر باشد. از سوی دیگر به نظر می‌رسد در این زمینه از یک ضعف دیپلماتیک رنج می‌بریم.

یافتن راه‌های پیگیری حقوقی بین‌المللی حملات سایبری به ایران و همچنین تلاش برای سهیم شدن در مدیریت اینترنت جهانی از طریق حضور در مجامع موثر و مرتبط، اقداماتی است که نیازمند یک وزارت امور خارجه توانمند و متعهد است.

رجوع به صفحه ۶