اخبار

اعلام آمادگی قطر و پاناما برای میانجیگری میان آمریکا و ونزوئلا

قطر و پاناما در بحبوحه تنش‌های ناشی از استقرار نظامی آمریکا در کارائیب و در نزدیکی آب‌های ونزوئلا، پیشنهاد میانجیگری میان واشنگتن و کاراکاس را مطرح کردند.

به گزارش ایرنا از خبرگزاری افه، «ماجد الانصاری» سخنگوی وزارت امور خارجه قطر اعلام کرد این کشور «منتظر» است تا طرف‌های درگیر یا سایر کشورها از دوحه برای میانجیگری میان آمریکا و ونزوئلا درخواست کمک کنند.

وی در حاشیه مجمع دوحه به خبرنگاران گفت: ما منتظریم کسی از ما درخواست کند.

الانصاری افزود مقام‌های قطری «با همه طرف‌ها در ارتباط هستند» اما در حال حاضر، دوحه «به طور رسمی، هیچ اقدامی انجام نمی‌دهد».

سخنگوی وزارت خارجه قطر یادآوری کرد که در سال‌های اخیر، کشورش مذاکراتی را با ونزوئلا و آمریکا برای دستیابی به توافق تبادل زندانیان انجام داده است؛ وی همچنین تایید کرد که قطر در صورت لزوم «به این روند متعهد است».

«کارلوس اویوس» معاون وزیر امور پاناما نیز در حاشیه مجمع دوحه و در مصاحبه با افه اعلام کرد که «خوسه رائول مولینو» رئیس‌جمهوری پاناما، تمایل خود را برای میزبانی موقت از «افراد خاصی» از دولت ونزوئلا به منظور کمک به «حل اوضاع» در آن کشور ابراز کرده است.

این مقام پانامایی با در نظر گرفتن احتمال اقدام آمریکا علیه ونزوئلا و حظور گسترده واشنگتن در کارائیب، «نگرانی زیاد نسبت به وقوع اتفاقی»، هم در کشور متبوعش و هم در منطقه را ابراز کرد؛ روندی که می‌تواند «همه را بی ثبات کرده و تحت تاثیر قرار دهد».

از ماه اوت گذشته (شهریور)، آمریکا با طرح ادعای مبارزه با قاچاق مواد مخدر، به صورت گسترده نیروهای نظامی خود را در کارائیب و در نزدیکی مرز ونزوئلا مستقر کرده است اما کاراکاس این اقدام را به عنوان «تهدیدی» با هدف تغییر حکومت خود محکوم کرده است.

حمله‌های آمریکا به شناورهای مظنون به حمل مواد مخدر تا کنون بیش از ۸۰ کشته برجای گذاشته است. واشنگتن مدعی است که این حملات با هدف مختل کردن قاچاق غیرقانونی مواد مخدر انجام می‌شود؛ این در حالی است که کاراکاس، هدف واقعی واشنگتن را از این اقدامات برکناری «نیکلاس مادورو» رئیس‌جمهوری این کشور از قدرت و دستیابی به منابع و ذخایر عظیم ونزوئلا می‌داند.

زیرساخت‌های نظامی روسیه زیر حملات سایبری کشورهای اروپایی

روابط روسیه و اروپا زیر سایه جنگ دیجیتال

تحول نوامبر ۲۰۲۵ با نهادینه شدن رویکرد تهاجمی، به نقطه عطفی مهم تبدیل شده است. این فرآیند دیگر پاسخی انفعالی و مقطعی از سوی چند کشور نیست، بلکه به شکلی دائمی و جمعی تحت ساختارهای ناتو و اتحادیه اروپا در آمده است

اتحادملت - گروه بین‌الملل - عاطفه عبدالهی‌نژاد؛ اتحادیه اروپا و ناتو، پس از سال‌ها تمرکز بر رویکردهای دفاعی، به صورت علنی و هماهنگ عملیات‌های سایبری تهاجمی علیه زیرساخت‌های نظامی حیاتی روسیه، از جمله کارخانه پهپادسازی «آلابوگا» در تاتارستان، را آغاز کردند. آنچه این هفته به وقوع پیوست، فراتر از یک تبادل ساده حمله و پاسخ بود و در واقع نشان‌دهنده یک تغییر بنیادین در راهبردهای سایبری غرب است؛ تغییر از «بازدارندگی دفاعی» به «بازدارندگی تهاجمی». این نقطه عطف، به‌نوعی آغازکننده دورانی جدید برای اروپا در عرصه جنگ‌های دیجیتالی و سایبری محسوب می‌شود.

اقدامات سایبری کشورهای اروپایی که با افشای برنامه‌های مشترک و هماهنگ ناتو و بروکسل برای هدف‌گیری زیرساخت‌هایی مانند مجتمع صنعتی «آلابوگا» همراه بود، صرفاً یک رویداد امنیتی نیست. این حرکتی استراتژیک با بار سیاسی-راهبردی سنگینی است که نشان‌دهنده تغییر رویکرد غرب نسبت به جنگ هیبریدی روسیه است. به نظر می‌رسد صبر اروپا در برابر اقدامات کرملین و استراتژی سنتی بازدارندگی مبتنی بر مدارا به پایان رسیده باشد. رهبرانی همچون دونالد تاسک از لهستان و گیدو کروستتو از ایتالیا به‌صراحت درباره ضرورت برنامه‌ریزی برای حملات سایبری مشترک، عملیات‌های مقابله‌ای ترکیبی، و مانورهای نظامی غیرمنتظره صحبت می‌کنند. این مواضع تازه بر پایه یک درک جمعی استوار است: تحریم‌ها و دیپلماسی سنتی تأثیر لازم برای تغییر رفتار کرملین را نداشته‌اند، درحالی‌که حملات مشابه—مانند اختلالات در سیستم‌های ناوبری و خرابکاری در زیرساخت‌های حیاتی—به بخشی از الگوی ثابت تعامل روسیه با غرب تبدیل شده‌اند.

ریشه این رویکرد تازه به تحولات فوریه ۲۰۲۲ و حمله روسیه به اوکراین بازمی‌گردد. بر اساس اطلاعات ارائه‌شده توسط مؤسسه مطالعات استراتژیک بین‌المللی، این رویداد عامل اصلی افزایش قابل توجه حملات هیبریدی روسیه بوده است. این عملیات‌ها تنها به فضای مجازی محدود نمانده و اثرات آن به دنیای فیزیکی نیز گسترش یافته، امنیت شهروندان اروپایی را مستقیماً تحت تأثیر قرار داده است.

مسئله کلیدی اکنون این است: آیا این تغییر راهبرد اروپا و ناتو به سمت انجام عملیات سایبری تهاجمی می‌تواند مفاهیم سنتی قدرت، حاکمیت در دنیای دیجیتال، و اصول بازدارندگی را در قرن بیست‌ویکم بازتعریف کند؟ یا اینکه این مسیر به افزایش تنش‌ها، تشدید متقابل و دورنمایی نگران‌کننده از بی‌ثباتی بلندمدت منجر خواهد شد؟

هدف قرار دادن مجتمع صنعتی آلابوگا، که طبق برآوردها، حدود ۷۰ درصد از پهپادهای پیشرفته روسیه، از جمله پهپاد انتحاری لانست را تولید می‌کند، نمادی مهم از تغییر رویکرد در جنگ سایبری است. این اقدام نشان‌دهنده جابه‌جایی تمرکز عملیات سایبری اروپا از واکنش به حملات موجود به سوی تضعیف ظرفیت نظامی آینده روسیه است. چنین تغییری جنگ هیبریدی را از سطح اختلال به سطح تخریب ساختاری ارتقا داده و ابعاد مختلفی را برجسته می‌کند:

۱. بعد عملیاتی-اقتصادی: مجتمع آلابوگا، با ظرفیت تخمینی تولید سالانه صد هزار پهپاد، یکی از نقاط کلیدی در زنجیره تأمین نظامی روسیه محسوب می‌شود. یک حمله سایبری که سیستم کنترل صنعتی یا شبکه لجستیکی این مجموعه را مختل کند، می‌تواند به‌طور مستقیم بر میدان نبرد در اوکراین اثر بگذارد و پیوند میان جنگ سایبری و جنگ فیزیکی را تقویت کند.

۲. بعد روانشناختی-بازدارندگی: این حرکت سیگنالی روشن به کرملین ارسال می‌کند که اروپا دیگر صرفاً یک قربانی منفعل نیست؛ بلکه توانایی و اراده ایجاد هزینه‌های نظامی و اقتصادی در داخل خاک روسیه را دارد. این پیام حس مصونیت جغرافیایی روسیه را به چالش کشیده و منطق بازدارندگی را از ترس از پاسخ به ترس از خسارات ملموس منتقل می‌کند.

۳. بعد استراتژیک: این رویکرد خطرات عمده‌ای به همراه دارد. هدف گرفتن زیرساخت‌های نظامی-صنعتی یک قدرت هسته‌ای در حوزه‌ای خاکستری از حقوق بین‌الملل قرار دارد و ممکن است از سوی روسیه به‌عنوان یک حمله تفسیر شود. پاسخ مسکو احتمالاً نامتقارن و شدید خواهد بود، مانند افزایش حملات به زیرساخت‌های حیاتی غیرنظامی اروپا. بنابراین، موفقیت این استراتژی به توانایی ارزیابی ظرفیت تحمل و واکنش روسیه بستگی دارد.

تشدید حملات هیبریدی روسیه: دکترین «تخریب زیر آستانه»

اقدام اروپا واکنشی به تحول نگران‌کننده در دکترین نظامی روسیه است که در آن جنگ هیبریدی با هدف تخریب تدریجی و سیستماتیک غرب بدون تحریک ماده ۵ ناتو طراحی شده است. از سال ۲۰۲۲ افزایش این نوع حملات قابل مشاهده بوده و جزئیات کیفی این اقدامات حتی نگران‌کننده‌تر هستند:

- چندبعدی بودن: ترکیبی از عملیات سایبری پیچیده، جنگ اطلاعاتی برای ایجاد شکاف، بهره‌برداری از مهاجرت و خرابکاری فیزیکی توسط عوامل نیابتی.

- انکارپذیری: طراحی این عملیات‌ها به گونه‌ای است که امکان انتساب دقیق آن‌ها به دولت روسیه دشوار باشد، امری که واکنش مؤثر دموکراسی‌ها را پیچیده‌تر می‌کند.

- هدف‌گیری تاب‌آوری ملی: هدف نه فقط ایجاد اختلال فنی، بلکه تخریب اعتماد عمومی به نهادهای دولتی و گسترش اختلافات داخلی در ناتو و اتحادیه اروپا است. از خرابکاری در راه‌آهن لهستان گرفته تا اختلال GPS در سوئد، این اقدامات بیشتر آزمایشی برای سنجش تاب‌آوری روانی-اجتماعی جامعه‌های اروپایی هستند

پاسخ تهاجمی اروپا اکنون قواعد بازی را تغییر می‌دهد. با هدف قرار دادن آلابوگا، پیام روشن است: اگر روسیه زیرساخت‌های غیرنظامی اروپا را مورد حمله قرار دهد، اروپا نیز به طور مستقیم ظرفیت‌های کلیدی نظامی-صنعتی روسیه را هدف خواهد گرفت. در این چارچوب، بازی از «رقابت بر سر تاب‌آوری» به سمت «رقابت بر سر تحمیل هزینه نامتقارن» تغییر مسیر داده است.

نقش تثبیت‌شده ناتو و اتحادیه اروپا: از هماهنگی دفاعی به معماری «پاسخ مشترک»

تحول نوامبر ۲۰۲۵ با نهادینه شدن رویکرد تهاجمی، به نقطه عطفی مهم تبدیل شده است. این فرآیند دیگر پاسخی انفعالی و مقطعی از سوی چند کشور نیست، بلکه به شکلی دائمی و جمعی تحت ساختارهای ناتو و اتحادیه اروپا در آمده است.

چارچوب‌سازی سیاسی: یکی از پیچیده‌ترین چالش‌ها برای دموکراسی‌ها در پیشبرد عملیات سایبری تهاجمی، ابعاد سیاسی و حقوقی آن است. مسائلی نظیر مجوز حملات، تناسب اقدامات متقابل و تطابق با حقوق بین‌الملل نیازمند پاسخ روشن هستند. ناتو و اتحادیه اروپا در حال تدوین مجموعه‌ای از چارچوب‌های مشخص هستند تا این اقدامات قانونی، قابل‌اعتماد و مبتنی بر اجماع مشترک باشند.

تقسیم کار تخصصی: این سازمان‌ها بستری برای همگرا کردن مهارت‌ها و ظرفیت‌های پراکنده کشورهای عضو فراهم کرده‌اند. ممکن است کشوری دارای توانمندی قوی نفوذ سایبری باشد، در حالی که دیگری از اطلاعات هدف‌گیری دقیق برخوردار باشد و کشوری دیگر حمایت‌های دیپلماتیک ارائه دهد. «نیروی وظیفه تاب‌آوری» در ناتو و «مرکز ضد هیبرید» اتحادیه اروپا در هلسینکی نقاطی کلیدی برای هماهنگی این توانایی‌ها ذیل یک استراتژی واحد به شمار می‌روند.

انتساب سریع به‌عنوان ابزار بازدارندگی: از جمله مأموریت‌های کلیدی این نهادها، تسریع فرآیند انتساب حملات سایبری و ارائه عمومی اسناد مرتبط است. چنین اقدامی دو هدف عمده را محقق می‌کند؛ نخست، ارائه مشروعیت لازم برای پاسخ‌های تهاجمی، و دوم، بی‌اثر کردن استراتژی انکار مهاجم. اگر روسیه بداند که هرگونه اقدامش به سرعت و با دقت شناسایی و اعلام خواهد شد، هزینه اقدامات غیرقانونی‌اش در سطح سیاسی و بین‌المللی به طور چشمگیری افزایش خواهد یافت.

پیامدهای ژئوپلیتیک: آغاز دوران جدید «جنگ سرد سایبری» و پایان منطقه خاکستری

این تحولات پیامدهای گسترده‌ای بر روابط بین‌الملل خواهد داشت و مسیر چندین دهه آینده را ترسیم می‌کند:

تثبیت درگیری دائمی زیر آستانه: فضای مبهم میان صلح و جنگ به وضعیتِ معمول جدیدی تبدیل خواهد شد. مناسبات بین قدرت‌های بزرگ بیش از پیش به کشمکش‌های پیوسته در حوزه‌های سایبری، اطلاعاتی و اقتصادی گرایش خواهد یافت.

قطبی‌سازی جهانی و بازتعریف حاکمیت: جو بی‌اعتمادی عمیق روند همکاری‌های جهانی در موضوعاتی همچون کنترل تسلیحات، تغییرات اقلیمی یا امنیت هسته‌ای را تضعیف می‌کند. همزمان، مفهوم سنتی حاکمیت که بر پایه قلمرو فیزیکی بنا شده است، در برابر تهدیدات فرامرزی سایبری ناتوان به نظر می‌رسد. این شرایط نیازمند بازتعریف اصول حاکمیت و حق دفاع مشروع در فضای سایبری خواهد بود.

رقابت تسلیحاتی چندجانبه: پیش‌بینی می‌شود رقابتی پرفشار در حوزه‌هایی نظیر سایبر، هوش مصنوعی، جنگ الکترونیکی و فضا میان قدرت‌ها شکل بگیرد. این رقابت نقش فزاینده‌ای برای بخش خصوصی و شرکت‌های فناوری ایجاد خواهد کرد و آنها را به بازیگران کلیدی در این عرصه تبدیل خواهد نمود.

در سطحی از تحلیل، چرخش اروپا امری اجتناب‌ناپذیر بود. در چارچوب نظام بین‌الملل آنارشیک، روسیه با بهره‌گیری از ابزارهای هیبریدی موفق شده بود موازنه قدرت را به زیان غرب تغییر دهد. همین امر اروپا را وادار کرد تا برای بازگشت به تعادل، قدرت و اراده‌ای مشابه را به نمایش بگذارد. این حرکت، نشانه‌ای از یک ارزیابی سرد و قدرت‌محور است. در سوی دیگر، گفتمان تازه رهبران اروپا در خصوص «عدم ترس از تشدید» به تدریج در حال شکل دادن به هویتی جدید برای این قاره به عنوان یک «قدرت استراتژیک» است، و دیگر تنها به «قدرت مدنی» محدود نمی‌شود. این دگرگونی هویتی، نگاه روسیه به اروپا را به‌عنوان تهدیدی جدی‌تر تقویت کرده و چرخه دشمن‌سازی را بیش از پیش شدت می‌بخشد. نکته قابل توجه این است که هر دو طرف گرفتار یک بازی تکراری با مجموع منفی شده‌اند. ادامه این روند به زیان هر دو طرف خواهد بود، اما ترس از زیان‌های بزرگ‌تر در صورت عقب‌نشینی (و احتمال بهره‌برداری طرف مقابل)، آنان را به ادامه رویارویی سوق می‌دهد. خروج از این «تله تشدید» نیازمند ایجاد سازوکارهای اعتمادسازی و برقراری ارتباطات شفاف جهت جلوگیری از سوءتفاهم‌های خطرناک است.

در نهایت، در جنگ سایه‌های دیجیتال، تخریب دشمن تضمینی برای امنیت خودی نخواهد بود. شکنندگی دنیای امروز که به‌صورت گسترده به هم پیوسته است، نشان می‌دهد که پیامدهای یک درگیری گسترده سایبری، همه را تحت تأثیر قرار خواهد داد. هدف اصلی باید دستیابی به یک «بازدارندگی پایدار مبتنی بر قدرت ملموس و خرد دیپلماتیک» باشد، نه تکیه بر پیروزی در نبردهای بی‌پایان که امنیت جمعی بشر را به خطر می‌اندازد. چالش واقعی رهبران غرب در دهه‌های آتی، مدیریت همین تناقض ظاهری خواهد بود.

از موشک تا ماوس

پیونگ‌یانگ میدان نبرد با آمریکا را عوض کرد

وزارت دادگستری آمریکا اعلام کرد که هکرهای وابسته به کره شمالی توانسته‌اند هویت ۸۰ شهروند آمریکایی را جعل و در مصاحبه‌های شغلی بیش از ۱۰۰ شرکت این کشور شرکت کنند، اقدامی که تاکنون دستکم سه میلیون دلار خسارت مالی به همراه داشته و نشان‌دهنده ضعف سیستم احراز هویت و آسیب‌پذیری سایبری ایالات متحده است.

به گزارش ایرنا از پایگاه خبری- تحلیلی «نشنال اینترست»، امسال وزارت دادگستری ایالات متحده، اعلام کرد که افرادی وابسته به کره شمالی توانسته اند هویت ۸۰ آمریکایی را جعل کنند و در مصاحبه‌های شغلی دورکاری بیش از ۱۰۰ شرکت در این کشور شرکت کنند. این نفوذ هدایت شده از سوی کره شمالی شرکت‌های آمریکایی را متحمل دستکم ۳ میلیون دلار ضرر کرد. و گمان می‌رود این تنها آغاز ماجرا باشد.

پیشتر کره شمالی به عنوان تهدیدی نظامی برای ایالات متحده شناخته می‌شد که نمونه آن آزمایش موشک قاره‌پیماست که می‌تواند خاک آمریکا را هدف قرار دهد. با این حال چالشی که واشنگتن اکنون از سمت آسیای شرقی با آن روبروست شکلی متفاوت دارد. توانمندی‌های جنگ سایبری کره‌شمالی اکنون به یک ابزار قدرت ملی تبدیل شده‌اند؛ این توانایی ها ترکیبی از جاسوسی، امور مالی و دورزدن تحریم‌هاست که آن‌ها را نه در قالب حملات مقطعی و گاه‌به‌گاه بلکه به عنوان یک کارزار مداوم به کار می‌گیرند.

کارکنان کره‌شمالی به کارفرمایان این را القا می کردند که داخل خاک ایالات متحده هستند؛ در حالی که بسیاری از آن‌ها در واقع در کره‌شمالی یا چین مستقر بودند. درآمدی که از این راه به دست می‌آمد، به حساب‌هایی منتقل می‌شد که تحت کنترل کره شمالی بود. این حساب‌ها به کره‌شمالی امکان می‌دهند تحریم‌های آمریکا را دور بزنند و برنامه‌های تسلیحاتی پیونگ یانگ را تامین مالی کند.

نفوذ پیچیده کره شمالی حکایت از آسیب‌پذیری سیستم احراز هویت آمریکا دارد. سیستمی که قرار است برای اشتغال قانونی در آمریکا، کارکنان را در بالاترین سطح امنیتی احراز هویت کند، در عمل نشان داده که آزمون‌های امنیتی‌اش در برابر این جاسوس‌ها بی‌اعتبار و ناکارآمد است.

نفوذ اخیر کره شمالی تنها بخشی از فهرست حملات سایبری است که تاکنون ایالات متحده متحمل شده است. چین حملات مداوم دارد و هرج و مرج، سلاح روسی است و از هردو کره شمالی است که سود می‌برد. این‌ها همه حکایت‌گر پیچیده‌تر شدن فزاینده فناوری هوش مصنوعی است و رقبای آمریکا همواره از آن بهره می برند.

طبق گزارش این نشریه در طول تعطیلی ۴۳ روزه دولت آمریکا، نهادهای فدرال و کارمندانشان ۵۵ میلیون حمله سایبری را تجربه کردند و رقبای واشنگتن از تعطیلی به عنوان فرصتی برای بهره‌برداری از نقاط ضعف در آمادگی نیروی سایبری استفاده کردند.

این پایگاه خبری در ادامه در بررسی آسیب شناسی سایبری اذعان می‌کند که ایالات متحده ابزار کافی برای امنیت سایبری را داراست ولی در اجرا و استفاده از آن دقت کافی ندارد و رقبا سریع تر از روند معمول در این کشور فناوری‌های خود را به روز می‌کنند. همچنین این حملات در پهنه سایبری را به «جنگ سرد جدید» تشبیه می کند که واشنگتن در آن علاوه بر استفاده از تسلیحات متعارف باید کدهای کامپیوتری را برای دفاع از خود بکارگیرد.