# نقش ایالات متحده در توسعه هنجارها و استانداردهای بین‌المللی برای فضای سایبری

محمد ابراهیم یزدانی

کارشناسی ارشد ارتباطات

ماه‌های اخیر، چالش شرکت متا (فیس‌بوک، اینستاگرام و واتس‌اپ) با اتحادیه اروپا درباره مقاومت پیرامون استقرار سرورها در منطقه اروپا، از سرخط‌های اصلی رسانه‌ها در اخبار بوده است. شرکت متا، تهدید به تعطیلی خدمات در اروپا را در دستور کار داشت و مقامات اروپایی از سویی دیگر، از این موضوع استقبال می‌کردند. از یک سو نارضایتی شهروندان اروپایی درباره تعطیلی خدمات متا، منجر به اعتراض نسبت به حاکمیت می‌شد و از طرف دیگر، اهتمام جدی اتحادیه اروپا برای مقابله با این غول فناوری، منجر به کاهش آمار کاربران فعال روزانه و افت ۲۵ درصدی سهام متا در هفته اول ماه فوریه شد. اختلاف اصلی درباره انتقال سرورها و پردازش داده‌ها در ایالات متحده آمریکا بود؛ موضوعی که مخالف و مغایر با مقررات عمومی حفاظت از داده اتحادیه اروپا بود. استدلال متا در بیانیه‌اش این بود که «اگر نتوانیم داده‌ها را بین کشورها و مناطقی که در آن فعالیت می‌کنیم، جابه‌جا کنیم یا اگر در اشتراک‌گذاری داده‌ها در میان محصولات و خدمات خود محدود شویم، این امر می‌تواند بر توانایی ما برای ارائه خدمات تأثیر بگذارد.» بهانه محدودیت و کاهش کیفیت خدمات، دستاویز متا شده بود. این تنها بخشی از نزاع بین حکمرانان و ساختارهای سایبری در عرصه جهانی است. امروزه جهان با حضور ابرقدرت‌ها، با پدیده نفوذ در حکمرانی و هنجارهای بین‌المللی برای فضای سایبر روبه‌رو است. این اعمال قدرت‌ها در عرصه‌های قوانین و قاعده‌های سایبر، بیشتر رخ نمایان می‌کند و عرصه‌های مختلفی را در برمی‌گیرد. اینکه چگونه این دخالت‌ها منجر به تغییر نگاه و همچنین اختلال در حکمرانی سایبری کشورها می‌شود، در یادداشت پیش¬رو بیشتر تشریح می‌گردد.

## امنیت و حکمرانی سایبری

در عصر دیجیتال، امنیت سایبری و ایجاد حکمرانی سایبری، به یکی از مهم‌ترین دغدغه‌های دولت‌ها تبدیل شده است؛ چراکه جهان به شکل فزاینده‌ای برای تقویت اقتصاد و توسعه جوامع و بهبود سطح زندگی بشر، به فضای سایبری نیازمند است. با افزایش رقابت جهانی و استفاده روزافزون از فضای سایبری برای تحقق اهداف ژئوپلیتیکی، نیاز به یک استراتژی جامع و مؤثر در حوزه امنیت سایبری، تبدیل به اصلی حیاتی شده است.

از طرفی، گسترش حملات سایبری با پیامدهای گسترده و جبران‌ناپذیر برای زیرساخت‌های حیاتی، زنجیره تأمین و نظام اقتصادی، به یک مسئله امنیت ملی تبدیل شده است. ایالات متحده آمریکا با درک صحیح از این نیاز، اقدام به تنظیم سند راهبردی امنیت سایبری نموده است. سندی که علاوه بر اشاره به شیوه‌های حکمرانی سایبری در کشور خودش، به ایجاد الزامات و قواعدی در سطح بین‌الملل هم اشاره می‌کند و به‌نوعی هنجارها و استانداردهایی را طرح می‌نماید.

نکته حائز اهمیت در این اسناد بین‌المللی، اهدافی است که عنوان شده است و به حفاظت از منافع و ایجاد امنیت در آمریکا و بهبود توان دفاعی و صنایع نظامی آمریکا اشاره شده است و تحولات تهدیدات سایبری برای این کشور، مورد بررسی قرار گرفته است. تحولات سایبری و وجود این اسناد، با هدف تأمین امنیت سایبری، نشان می‌دهد که امنیت سایبری به‌عنوان یک موضوع حیاتی در سطح جهانی مطرح است و این محوریت سبب می‌شود که کشورهای واضع قوانین، اقدام به ایجاد قواعد و هنجارهایی در سطح بین‌المللی برای فضای سایبری نمایند و دخالت‌هایی را در این عرصه، تسری دهند. این مداخله گاهی با اعمال قدرت و نفوذ سایر توانمندی‌ها به حوزه امنیت سایبری، منجر به تضییع حقوق و حاکمیت سایر کشورها می‌شوند و تهدیدات وجودی علیه امنیت ملی کشورها، پدید خواهد آورد.

## اعمال قدرت در حکمرانی سایبری

ایالات متحده آمریکا، به‌عنوان یکی از دولت‌های مشارکت‌کننده و تصمیم‌ساز در عرصه حکمرانی سایبری، با تصمیمات و هنجارسازی‌های مختلف، منجر به تغییراتی در استانداردهای بین‌المللی شده است که برخی از آنها شامل موارد زیر می‌شود:

۱. حداقل الزامات امنیت سایبری در تمام صنایع افزایش می‌یابد؛

۲. تکنولوژی، یک زیرساخت حیاتی به‌حساب می‌آید؛

۳. حفاظت از تکنولوژی یک ضرورت امنیت ملی است؛

۴. شرکت‌های خصوصی، عنصر مهمی در امنیت ملی هستند.

به نظر می‌رسد که با گذشت بیش از دو دهه از فراگیری اینترنت، دولت‌ها با گذار از عصر تک‌محوری و خوداتکایی، در عرصه تأمین امنیت سایبری نیز به سمت شکل‌گیری پیمان امنیت دسته‌جمعی و استراتژی‌های مشارکتی حرکت خواهند کرد اما ایالات متحده آمریکا در همین مسیر اتفاق جمعی بر یک‌سری هنجار و قواعد جمعی برای ایجاد امنیت بر عرصه فضای سایبری نیز از مدت‌ها پیش آن را با دخالت

دادن قواعد حوزه‌های دفاعی و صنایع نظامی، دچار تغییراتی کرده است و اکنون به شکل رسمی در فضای سایبری، تدابیر نظامی و امنیتی خودش را به دستور کار آینده جریان سایبری جهانی تبدیل نموده است و با دست یافتن به بنگاه‌های بزرگ و غول‌های بزرگ رسانه و ارتباطات، بقیه کشورها را مجبور به تبعیت نموده است.

بنابراین، در پرتو این تحولات و دخالت‌های ایالات متحده در هنجارهای فضای سایبر، روشن است که امنیت سایبری به‌عنوان یک موضوع حیاتی در سطح جهانی برای کشور اهمیت می‌یابد و بی‌توجهی نسبت به آن، منجر به تغییر در موازنه قدرت و شکل‌گیری تهدیدات وجودی علیه امنیت ملی کشورها خواهد شد.

## دخالت در حکمرانی سایبری

به نظر می‌رسد که با گذشت بیش از دو دهه از فراگیری اینترنت، دولت‌ها با گذار از عصر تک‌محوری و خوداتکایی، در عرصه تأمین امنیت سایبری و قاعده‌گذاری فضای سایبر، به سمت شکل‌گیری پیمان‌های امنیتی دسته‌جمعی و استراتژی‌های مشارکتی حرکت خواهند کرد البته کشورهایی همچون ایالات متحده آمریکا پیش از حضور کشورهای دیگر، در ایجاد ضوابط فضای سایبر، این راه را طی کرده است و به آن راه وارد شده است و اکنون به شکل رسمی، در فضای سایبری، قواعد و اصول خودش که متأثر از قواعد نظامی کشورشان است را به دستور کار آینده خود تبدیل نموده است.

اما مسئله مهم اینجا است که دخالت‌ها در ایجاد استانداردهای بین‌المللی و همچنین ایجاد هنجارها، چگونه می‌تواند توسط کشوری همچون آمریکا رخ دهد؟ یکی از این اعمال هنجارها توسط کشورها، قوانین توسعه و فعالیت پلتفرم‌ها در اروپا است. اهتمام اتحادیه اروپا برای قانون‌گذاری درباره خدمات دیجیتال، به مسئله حراست از داده‌های شخصی شهروندان و مؤلفه‌های امنیت ملی بازمی‌گردد که در تاریخچه قوانین این اتحادیه، در ذیل به آن پرداخته شده است.

کشمکش‌های اخیر اتحادیه اروپا با شرکت متا، مسئله جدید در عرصه سیاست‌گذاری برای این نهاد نبود و از سال ۱۹۹۵ به آن توجه داشته‌اند. دسامبر ۲۰۲۰ بسته قانونی خدمات دیجیتال شامل قانون بازارهای دیجیتال و خدمات دیجیتال پیشنهاد شد و در ماه فوریه سال ۲۰۲۲، چالش بزرگی بین شرکت متا (فیس‌بوک، اینستاگرام و واتس‌اپ) و اتحادیه اروپا درباره انتقال سرورهای متا به اتحادیه اروپا شکل گرفت؛ تا جایی که تهدید عدم ارائه خدمات توسط متا به شهروندان اروپایی نیز مطرح شد. در نهایت پس از این کشمکش‌ها، اتحادیه اروپا علاوه بر قوانین گذشته، مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR)، بسته قانونی خدمات دیجیتال را در ۵ ژوئیه ۲۰۲۲ به تصویب رساند.

قانون خدمات دیجیتال، بر کنترل قدرت شرکت‌های بزرگ دنیای فناوری از جمله اپل، گوگل و متا تمرکز دارند و به حمایت از مصرف‌کنندگان می‌پردازند. شرکت‌های حوزه فناوری بر اساس ابعاد و اندازه

خود، تعداد کاربران و درآمدی که به دست می‌آورند، به‌عنوان شرکت‌های تأثیرگذار و دربان این حوزه شناخته می‌شوند؛ در نتیجه، در پوشش این قوانین جدید قرار می‌گیرند.

این قانون می‌خواهد نگذارد شرکت‌ها از بزرگی خود سوءاستفاده کنند؛ برای مثال، گوگل از موتور جستجوی خود برای اولویت دادن به پلتفرم فروشگاهی این شرکت استفاده می‌کرد و به فضای رقابت در بازار صدمه می‌زد. این قانون چنین اقداماتی را با جریمه‌های سنگینی روبه¬رو می‌کند.

در چنین شرایطی، کشورهایی همچون آمریکا برخلاف مصالح حکمرانی سایر کشورها و گاهی اوقات با هدف برهم زدن حاکمیت برخی کشورها، اقدام به ایجاد هنجارهایی در فضای سایبر می‌نمایند که سبب برهم ریختگی نظم حکمرانی سایبری جهانی می‌شود. شاید بتوان برخی از این قاعده‌گذاری‌ها را در قالب موارد زیر خلاصه کرد:

ایجاد رانت و ظرفیت جمع‌آوری اطلاعات؛

مدیریتِ توسعه امنِ دستگاه‌های اینترنت اشیا و پلتفرم‌ها؛

ایجاد کمک‌های مالی فدرال و سایر مشوق‌ها برای سرقت اطلاعات؛

ایجاد تغییر در مسئولیت محصولات و خدمات نرم‌افزاریِ ناامن و مصون ساختن آنها از پاسخگویی.

## جمع‌بندی

امروزه شرکت‌های بزرگ فناوری اطلاعات در دنیا که از آنها به غول‌های ارتباطی یا پادشاهان آنلاین تعبیر می‌شود، نقش مهمی در حکمرانی فضای مجازی ایفا می‌کنند. در این باره باید گفت باتوجه‌به کشیده شدن تمامی منازعات حاکمیتی کلاسیک به عرصه سایبری، شرکت‌های بزرگ فناوری، به یکی از طرف‌های اصلی منازعات هم در درون کشورها و هم در بین کشورها در عرصه سایبری تبدیل شده‌اند.

در واقع به دلیل قدرت بازیگری پلتفرم‌ها در عرصه سایبری و قلمروهای انحصاری که آنها در این عرصه برای خود در مقیاس جهانی و منطقه‌ای تعریف کرده‌اند، این پلتفرم‌ها به‌عنوان بازیگر مستقل در هر نوع منازعه‌ای حضور دارند و نقش مهمی در ایجاد توازن یا تغییر موازنه به نفع یا علیه کشورها در روابط بین‌الملل ایفا می‌کنند.

استراتژی جدید امنیت سایبری آمریکا نشان‌دهنده تغییرات قابل‌توجهی در رویکرد ایالات متحده نسبت به فضای سایبری است. یکی از تفاوت‌های قابل‌توجه این استراتژی با اقدامات و استراتژی‌های پیشین آمریکا، تمرکز بر دفاع جمعی و مشارکت با بخش خصوصی و متحدان بین‌المللی است. این استراتژی به دنبال ایجاد یک سپر دفاعی سایبری در اطراف آمریکا و شرکای استراتژیک آن است که بیانگر آغاز عصر شکل‌گیری پیمان‌های سایبری و مشارکت‌های فعال بین‌المللی خواهد بود. شاید بتوان گفت مداخله جدی و مهم بعدی ایالات متحده آمریکا در عرصه حکمرانی سایبری در رویارویی جمعی متحدان با حاکمیت مستقل کشورهای استقلال‌طلب در فضای سایبر است.

سند امنیت سایبری آمریکا، پاسخی به تهدیدات پیچیده و در حال تحول سایبری است. ایالات متحده در طول سال‌های اخیر با آن روبه¬رو است و به

شکل مستمر نیز بیشتر و پیچیده‌تر می‌شود. حملات سایبری نیابتی به زیرساخت‌های حیاتی، سازمان‌های دولتی و مشاغل آمریکا، به‌شدت افزایش‌یافته است و نگرانی‌های فزاینده‌ای در مورد سطح آسیب‌پذیری این کشور در برابر تهدیدات سایبری به وجود آورده است. رسالت استراتژی امنیت سایبری، مقابله با این چالش‌ها و گرفتن رویکرد پیشگیرانه بر اساس اصل دفاع فعال است و این یعنی استانداردهای بین‌المللی هم دستخوش تغییراتی می‌شوند.

همان‌طور که در این گزارش مشخص شد، یکی از راه‌های اصلی این استراتژی برای دستیابی به این هدف، تأکید بر اهمیت مشارکت در دفاع سایبری است. این استراتژی تأکید می‌کند که هیچ نهاد واحدی در بخش خصوصی و دولتی نمی‌تواند به‌تنهایی بر چالش‌های امنیت سایبری ایالات متحده غلبه کند. در عوض، رویکردی هماهنگ را ارائه می‌دهد که تمامی ذی‌نفعان از جمله متحدان بین‌المللی را در رویارویی با تهدیدات درگیر می‌کند.

سطح مشارکت تعریف‌شده برای بخش خصوصی در این استراتژی قابل توجه است. بخش خصوصی، بسیاری از زیرساخت‌های حیاتی آمریکا از جمله شبکه‌های تأمین برق، سیستم‌های مالی و شبکه‌های حمل‌ونقل را در اختیار دارد و آن را اداره می‌کند.

سند امنیت ملی آمریکا با ایجاد مکانیسم‌های حمایتی مختلف، بخش خصوصی را تشویق به مشارکت فعالانه در رویارویی با تهدیدات سایبری می‌کند؛ بنابراین در ساحت حکمرانی بین‌المللی، ما با تغییرات پروتکل‌های پلتفرم‌ها در رویارویی با کشورهایی همچون ایران خواهیم بود؛ به‌گونه‌ای که در نزاع بین قدرت‌ها منجر به ایجاد محدودیت‌ها و تغییرات در ساحت دسترسی و خدمات برای این کشورها می‌شود، امری که کاملاً خلاف عدالت سایبری و حکمرانی سلامت‌محور فضای سایبر است.

قدرت اطلاعاتی، یک تقویت‌کنندهٔ نیرو است که در استراتژی امنیت ملی آمریکا نقش حیاتی به عهده دارد. به‌عنوان یک عنصر قدرت هوشمند، در حوزهٔ محیط اطلاعاتی عمل می‌کند تا از حوزه‌های قدرت دیپلماتیک، نظامی و اقتصادی حمایت کند. مؤلفهٔ نوظهور و وسیع محیط اطلاعاتی، فضای سایبری است. فضای سایبری به سه C تقسیم می‌شود: اتصال، محتوا و شناخت.

استراتژی اطلاعاتی آمریکا باید کاستی‌های قدرت اطلاعاتی را از راه این سه C اندازه‌گیری و ارزیابی کند و به آنها بپردازد. قدرت اطلاعاتی یک کشور را می‌توان با استفاده از پرداختن به فاکتورهای کیفی و کمّی این سه C اندازه‌گیری و ارزیابی کرد؛ بنابراین در پایان باید گفت ایالات متحده آمریکا، با تنظیم سیاست‌های امنیت سایبر که از آن رونمایی کرده است و همچنین تنظیم‌گری‌های بین‌المللی، در تلاش است تا احاطه خود را در سه محور اتصال، محتوا و شناخت باقی نگه دارد و بتواند از راه آن، شیوه‌های استعماری و سلطه‌طلبانه خود را بر کشورهای دیگر ادامه دهد و تسری ببخشد.