# آیا فضای سایبری آمریکا در حال افول است ؟

*حملات سایبری سرخط خبرهای آمریکا در سال ۲۰۲۱ را به خود اختصاص داده، بذرآشوب و وحشت را کاشته و خسارت مالی عظیمی بر دولت ها، تجارت و شهروندان تحمیل می کنند. با بدتر شدن مشکل، سیاست گذاران برای واکنش به این موضوع تلاش می کنند. مشکل راهبرد سایبری ایالات متحده چیست؟ اگر کشور نتواند در مقابل این تهدید بی رحم، دفاع بهتری از خود نشان بدهد، چه چیزی در خطر خواهد بود؟ متن زیر مصاحبه ای است که کیت برانن[1]، معاون سردبیر فارین افرز[2] با دیمیتری آلپروویچ[3]، مدیر ارشد فناوری سابق در شرکت امنیت سایبری کرود استرایک[4]، ژاکلین اشنایدر[5]، پژوهشگر مؤسسه هوور در دانشگاه استانفورد[6] و جوزف نای[7]، استاد دانشکده حکمرانی جان اف. کندی[8] در دانشگاه هاروارد در خصوص راهبردهای سایبری ایالات متحده انجام داده داده است.*[9،10]

**برانن**: ژاکلین، قصد دارم بحث را با شما شروع کنم. شما در مقاله خود به این نکته اشاره داشته اید که چگونه واشنگتن سال ها نسبت به آثار بالقوّه مخرّب واقعی که حملات سایبری می‌توانند به جا بگذارند، هشدار داده است؛ ازجمله هشدار مشهور وزیر دفاع وقت لئون پانه تا[11] درباره احتمال وقوع یک پرل هاربر[12] سایبری. به نظر من این هشدار به روشنی در اذهان همه ثبت شده است. گمان می کنم همه مقالات به این موضوع اشاره کرده‌اند نوعی ارجاع یا اشاره به این موضوع در تمامی مقالات مورد بحث ما وجود دارد. ولی همان گونه که شما هم در نوشته خود بیان کرده‌اید، بسیاری از این هشدارها عملی نشد و در عوض،آنچه روی داد به نوعی دسیسه آمیزتر و مخرّب‌تر بود.

1. Kate Brannen
2. Foreign Affairs
3. Dmitri Alperovitch
4. CrowdStrike
5. Jacquelyn Schneider
6. Hoover Institution at Stanford University
7. Joseph S. Nye, Jr.
8. John F. Kennedy School of Government

9. https://www.foreignaffairs.com/events/2022-01-20/can-united-states-curb-threat-cyberspace
10. https://www.foreignaffairs.com/events/2022-01-20/can-united-states-curb-threat-cyberspace
11. Leon Panetta
12. Pearl Harbor

خواهشمندم آنچه را تهدیدهای حقیقی برخاسته از فضای سایبری شناخته می‌شود، تشریح کنید.

**اشنایدر:** بله، همان‌طور که می‌دانید، این دیدگاه که فضای سایبر چنین تأثیر مستقیم و گسترده ای دارد، واقعاً توجه و تصوّرات را به خود جلب کرده و به نظر من، هدف از طرّاحی آن نیز همین بوده است. مشکل این بود که رویداد بزرگ هرگز رخ نداد و در عوض ما شاهد افزایش چشم‌گیر فعالیت سایبری با دامنه محدود بودیم که در عمل، پیامدهای فوق‌العاده‌ای برای فعالیت اقتصادی و حکمرانی داشته است و به طور کلی فضای سایبری در حال تنزّل دادن اعتمادی است که ما به بازارهای دیجیتال، حکومت در عصر مدرن و حتی همکاری بین المللی داریم. لذا اینکه این پدیده درحال کاستن از اعتماد ما به سیستم‌های دیجیتال مدرن است، درواقع، عامل کلی و تهدید وجودی آن برای جوامع مدرن است.

**برانن:** به نظر من یکی از نکات مهم توضیحات شما، این است که یاد بگیریم با شکست کنار بیاییم و اینکه به جای تلاش زیاد برای جلوگیری از این حملات، همان‌طور که می دانید تقریباً تلاشی بی‌فایده است تا بر روی ایجاد توانایی برگشت‌پذیری و بهبودپذیری تمرکز کنیم. امکان دارد درباره چگونگی ایجاد حسی از بهبودپذیری هم در سطح فنّی، یعنی در دستگاه‌ها، و نیز اجتماعی همان‌طور که توصیف کردید کاری به مراتب دشوارتر است، صحبت کنید؟

**اشنایدر:** به نظر من برگشت‌پذیری مفهومی بنیادین و فراتر از حوزه سایبری برای ایالات متحده خواهد بود. از این‌رو، در فضای سایبری این مسئله ابعاد بسیار مختلفی دارد. منظور من این است که بهبودپذیری فنّی ناظر به ایجاد انواع مختلفی از شبکه‌ها، گرفتن نسخه پشتیبان، ایجاد روندهای آنالوگ یا توانایی نیروهای نظامی برای انجام عملیات بدون اتصال دیجیتال باشد. من تصوّر می‌کنم که گران‌ترین و دشوارترین بخش بهبودپذیری این است که شما یا خود را در کوتاه‌مدّت کمتر کارآمد می‌کنید یا در آموزش و نیروی انسانی، سرمایه‌گذاری می‌کنید که هزینه بیشتری به همراه دارد. از سوی دیگر، بهبودپذیری جامعه واقعاً دشوار است و گونه‌ای که فضای سایبری بر اطلاعات تأثیر می‌گذارد و چگونگی تعامل ما با یکدیگر بسیار پیچیده است. بخش مشکل قضیه این است که شما چگونه می‌خواهید بهبودپذیری و برگشت‌پذیری جوامع را در مقابل این‌گونه تهدیدها افزایش دهید؟ این مسئله احتمالاً کمتر با حوزه فنّی و بیشتر با چگونگی تعامل انسان‌ها در خارج از فضای دیجیتال مرتبط است.

**برانن:** یک رویّه مشترک در تمامی مقالات، این حس بود که آمریکا تقریباً در درک مشکل دچار خطا شده یا اینکه اشتباهی در راهبرد کنونی و در نوع نگرش به مشکل وجود دارد.

**دیمیتری**، اجازه بدهید تا به مقاله شما مراجعه کنیم که در آن، استدلال می‌کنید چگونه تهدیدهای سایبری اغلب به عنوان یک مشکل امنیت ملّی متمایز قلمداد می‌شوند که بایستی با استفاده از راه‌حلّ‌های سایبری مخصوص رفع شود، با

اینکه آن‌ها نشانه‌های واقعی برای مشکلات ژئوپلیتیک گسترده‌تر هستند. لطفاً از تهدیدهایی که از سوی چین، ایران و روسیه می‌آید و اینکه چگونه این کشورها از حوزه سایبری برای پیش‌برد اهداف ژئوپلیتیک خود استفاده می‌کنند، صحبت کنید؟

**آلپروویچ:** همان‌طور که مدّت‌ها قبل نیز گفته‌ام، بعید می‌دانم که ما یک مشکل سایبری داشته باشیم؛ به نظر من، مشکل ما روسیه، چین، ایران و کره‌شمالی است و پدیده فضا و توان سایبری، مؤلفه‌ای از چشم‌انداز مبارزه

ژئوپلیتیک ما با این چهار دشمن اصلی است. این، بدین معنا نیست که تمامی حملاتی که با آن‌ها مواجه هستیم از این چهار کشور نشئت می‌گیرند، بلکه اکثریت قریب به اتفاق حملات هدایت‌شده توسط ملّت-دولت علیه مؤسسات و بخش خصوصی ما، از سوی نهادهای متعلّق به حکومت در آن دولت‌ها، سازمان‌های نظامی اطلاعاتی آن‌ها، و مجرمانی که در این کشورها غالباً با دریافت عفو اجازه فعالیت یافته‌اند، انجام می‌شود. یقیناً مجرمان بسیار دیگری نیز در سرتاسر جهان هستند، اما عمدتاً ما قادریم تا آن‌ها را یافته و فوراً دستگیر کنیم و بدین ترتیب، مشکل را در سطحی که قابل مدیریت است، حفظ نمائیم. ولی آنچه که از انجام آن عاجزیم مقابله با تهدیداتی است که از این چهار کشور نشئت می‌گیرد، و به همین دلیل است که از نظر تأثیرگذاری، درجه اهمیتشان روزبه‌روز بیشتر افزایش پیدا کرده است.

لذا وقتی به هرکدام از این چهار کشور می‌نگرید، آن‌ها از حوزه سایبری به اشکال مختلفی استفاده می‌کنند تا اهداف راهبردی خود را محقق سازند. چین بسیار متمرکز برادامه توسعه قدرت اقتصادی خود و استفاده از پدیده فضای سایبری برای سرقت مالکیت معنوی مرتبط با سیستم‌های امنیت ملّی، دفاع و سایر برنامه‌ها است. این کشور بیش از بیست سال است که در این حوزه فعالیت دارد و تقریباً هم موفق بوده و مالکیت معنوی را -که احتمالاً تریلیون‌ها دلار ارزش دارد- به سرقت برده است. پس اگر تأمّلی نموده و به ماوراء عملیات‌های سایبری که آن‌ها

انجام می‌دهند، نگاهی بیندازید، آنچه بسیار روشن خواهد شد، این است که آن‌ها با استفاده از خارج‌ساختن ما از میدان رقابت و با سرقت مالکیت معنوی که به شکلی بی‌سابقه در حال وقوع است، اساساً یک جنگ تجاری علیه ما به راه انداخته‌اند.

ماجرا در مورد روسیه، بسیار دشوار است. روس‌ها بسیار در استفاده از زور برای تحقق اهداف یا تلاش برای تحقق آن‌ها تبحر دارند. بسیاری از حملاتی که از سوی روس‌ها مشاهده می‌کنیم، از نظر دولت روسیه، مشتمل بر ایجاد اختلال و عملیات‌های اقدامات فعال بوده و پویش‌ها و جنبش‌ها را تحت تأثیر قرار می‌دهند؛ مانند حمله به انتخابات آمریکا در سال ۲۰۱۶، انتخابات فرانسه در سال ۲۰۱۷ و انتخابات اوکراین. اضافه کنید به این حملات مختل‌کننده، آن‌هایی که روس‌ها در طول هشت سال گذشته ضد اوکراین انجام داده‌اند و نیز آن‌هایی که احتمالاً در آینده نزدیک در صورت حمله نظامی به این کشور، از سوی روسیه انجام خواهد شد. همچنین، روسیه چشم خود را به روی این واقعیت که تعداد کثیری از مجرمان سایبری در داخل مرزهایش، همچون باج‌افزارها، مشغول فعالیت هستند، بسته است. از گذشته تاکنون، این کشور هیچ اقدامی در مقابله با این مجرمان صورت نداده است، به جز مورد هفته گذشته که چهارده عضو باند باج‌افزاری رویل[1] که گفته شده مسئول حمله به شرکت جی‌بی‌اس[2] و کاسیا[3] در تابستان گذشته بودند، بازداشت شدند. به نظر من، انجام این اقدامات واقعاً از دولت روسیه بی‌سابقه است و آن‌ها اعلام کردند که این کار در پاسخ به درخواست آمریکا، انجام شده است. به نظر من شما نمی‌توانید از مبارزه ژئوپلیتیک وسیع‌تری که ما با روسیه داریم، این واقعیت را جدا کنید که آن‌ها اکنون تلاش دارند تا در این دیپلماسی، باج‌افزار مشارکت داشته باشند، با ارسال این پیام به دولت بایدن[4] که شما می‌توانید روی کمک‌مان برای مقابله با چنین مجرمانی که از گذشته اقدامی در رابطه با آن‌ها انجام نداده‌ایم، حساب کنید ولی نباید به واسطه اقداماتی که ضد اوکراین انجام می‌دهیم، دست به تحریم ما بزنید. این بررسی مختصر بازیگران اصلی است که ما در فضای سایبری با آن‌ها مواجه هستیم.

**برانن**: پروفسور نای؛ می‌خواهم از شما سؤال مشابهی را در مورد نگاه به فضای سایبری به عنوان موضوعی متمایز از مجموعه گسترده‌تر مشکلات امنیت ملّی، بپرسم. تردیدهای فراوانی وجود دارد نسبت به اینکه هر قانونی می‌تواند در فضای سایبری پیاده شود و اینکه این فضای غرب وحشی است. به نظر شما چرا چنین تردیدهایی وجود دارد و مردم چه سوءبرداشت‌هایی درباره ضوابط و قوانینی دارند که علاوه بر سلاح هسته‌ای و سایر مسائل، بر فضای سایبری نیز قابل انطباق هستند؟

**نای**: متشکرم کیت. اجازه بدهید ابتدا عرض کنم که من، کاملاً با سخنان ژاکلین و دیمیتری موافق هستم. شما نمی‌توانید فضای سایبری را از کل روابط جدا کنید؛ این فضا ابزاری است که کشورها از آن استفاده می‌کنند. یک ابزار متفاوت از این نظر که "صدا و

1. REVil
2. JBS
3. Kaseya
4. Biden

انفجار مهیبی" را ایجاد نکرده و به مراتب سریع‌تر است و در این قضیه، اقیانوس‌ها نمی‌توانند از ما محافظت کنند و گاهی دشوار است که منشأ آن را بیابیم، اما با این حال، همچنان ابزاری برای رقابت میان قدرت‌ها محسوب می‌شوند.

حال سؤال این است که آیا می‌توان برخی از ابزارها را محدود ساخت و قیودی را برای آن‌ها وضع کرد؟ ما تلاش کردیم تا این کار را با امضاء توافق‌نامه‌ها و پیمان کنترل تسلیحات و مانند آن انجام دهیم. بعید می‌دانم که بتوان چنین کاری نسبت به امور سایبری نیز انجام داد، چرا که نمی‌توانید بگویید آیا این دسته از کُدها یک سلاح هستند یا خیر؛ زیرا بستگی به قصد کاربر دارد. از سوی دیگر، شما می‌توانید به دنبال شباهت‌ها باشید و بگویید که گاهی منفعت یک حکومت اقتضاء می‌کند برخی از ضوابط و محدودیت‌ها را بپذیرد و ما نمونه‌هایی از این مسئله را در تاریخ دیده‌ایم که من در مقاله خود، تلاش دارم آن‌ها را تبیین کنم. با وجود این، نسبت به موضوع فضای سایبری، من معتقدم که اگر به نمونه‌ها دقّت کنید، چندین مورد: یک مورد در طول جنگ سرد[1] رخ داد، زمانی که ما قطعاً روابط سردتر و تفاوت‌های ایدئولوژیک با اتحاد جماهیر شوروی داشتیم، همچنین، دستورالعمل‌های مشخصی برای نوع رفتار با جاسوس طرف مقابل ایجاد کرده بودیم. ما آن‌ها را نمی‌کُشتیم، بلکه آن‌ها مبادله می‌شدند. آن‌ها به قوانین مسکو[2] مشهور بودند. این دستورالعمل‌ها در هیچ توافق‌نامه‌ای تبیین نشده بودند، بلکه اقتضای احتیاط و این واقعیت بودند که هر دولت می‌دانست، اگر این قانون را نقض کند، هزینه‌اش از نفعش بیشتر است، یا مثال دیگر سال ۱۹۷۲ است زمانی که آمریکا و شوروی مدام با نزدیک‌شدن به کشتی‌های طرف مقابل، تلاش داشتند تا اطلاعات کسب کنند، و در نهایت ما دریافتیم که دیر یا زود، یکی از این اقدامات ممکن است از کنترل خارج شود. از این‌رو، ما موافقت‌نامه حوادث دریایی[3] را امضا کردیم که براساس آن، تمامی اقداماتمان مشمول محدودیت‌های مشخصی گردید.

بنابراین، گاهی حکومت‌ها درمی‌یابند که به دلایل مختلف، منفعتشان در این است که برخی محدودیت‌ها -که دست و پای حاکمیتشان را می‌بندد- اعمال کنند. یک دلیل همکاری است؛ دلیل دیگر، جانب احتیاط است که به آن اشاره کردم و دلیل سوم نیز عبارت است از برخی تابوها که وقتی نقض می‌شوند، بسیار برای شهرت و وجهه یا قدرت نرم شما هزینه‌ساز هستند. همچنین، دلیل دیگر که گمان نمی‌کنم چندان برای روسیه، چین یا قطعاً کره‌شمالی مهم باشد، تحوّل و تکامل تغییرات در افکار عمومی داخل کشور است، به این معنا که بعد از مدّتی برخی مسائل، دیگر قابل‌قبول نیستند. بنابراین، این‌ها حداقل چهار دلیل اصلی برای این هستند که کشورها خود را محدود می‌کنند و اگر آن‌ها اتفاقاً در حوزه‌های دیگر از برده‌داری گرفته تا سلاح‌های بیولوژیک و بمب هسته‌ای مشاهده شوند، هیچ دلیلی وجود ندارد که در حوزه سایبری رخ ندهند. البته ما نباید هیچ تصور باطلی درباره یک پیمان کنترل تسلیحاتی سایبری بزرگ داشته باشیم.

**پایان بخش اول**

1. Cold War
2. Moscow
3. Incidents at Sea Agreement