

فنی جورجیا و متخصص در حوزه حکمرانی اینترنت که در سال ۲۰۲۰ نوشته شده و از اصلی ترین نظریات مرتبط در این خصوص به شمار می رود.

تنش میان روسیه و اوکراین در شرایطی ادامه می یابد که شاید برای نخستین بار در جهان است که، اینترنت، فضای مجازی و فناوری های ارتباطی در صف خطوط مقدم جنگ قرار می گیرد؛ از تحریم های اپریتلنفرم های رسانه اجتماعی (فیس بوک، تیک تاک، یوتیوب و توئیتر) علیه حساب های کاربری روسی گرفته، تا کمک های زیرساختی اتحادیه اروپا به اوکراین، دسترسی مردم اوکراین به اینترنت ماهواره ای، حملات سایبری متعدد به پایگاه های دولتی هر دو کشور، دستکاری الگوریتم جست و جوی گوگل به درخواست اتحادیه اروپا یا حتی تحریم داخلی نظیر محدودسازی دسترسی کاربران روسی به برخی رسانه های اجتماعی توسط دولت این کشور. دامنه این مداخلات فناوری محور به قدری وسیع و وزن آنها تا اندازه ای سنگین است که می توان به جرت عبارت جنگ مجازی را در کنار سایر ابعاد این پدیده ناگوار و غیرانسانی مثل اقتصاد، تسلیحات، راه های ارتباطی، روابط دیپلماتیک و... مشاهده کرد. در این میان، بار دیگر بحث از معنا و مفهوم حکمرانی (Governance) و حاکمیت (Sovereignty) در دنیای به ظاهر بدون مرز و خط کشی اینترنت، با بالا گرفتن درگیری های فیزیکی بر سر مرز و سرزمین که از قضا به دنیای مجازی نیز کشیده شده، به میان آمده است. در این یادداشت مروری خواهیم داشت بر مقاله ای با عنوان «علیه حاکمیت در فضای مجازی» اثر «میلتون مولر»، استاد برجسته دانشگاه فنی جورجیا و متخصص در حوزه حکمرانی اینترنت که در سال ۲۰۲۰ نوشته شده و از اصلی ترین نظریات مرتبط در این خصوص به شمار می رود.

جنگ سرزمین ها در دنیای بدون مرز مجازی؟! |

معادله چندمجهولی حاکمیت بر اینترنت

عمادالدین پاینده | پژوهشگر آزمایشگاه داده و حکمرانی

حکمرانی بر کجا؟

مولر در این مقاله کوشیده است سرنوشت مفهوم حاکمیت سرزمینی را در مواجهه با چالش های فضای مجازی مبتنی بر آی پی ها و زیرساخت های داده محور تشریح کند و حداقل روی کاغذ، دولت ها را از صرفت بازتولید حاکمیت ملی - سرزمینی در عرصه اینترنت، به ویژه در لایه زیرساخت، دسترسی و اتصال منصرف سازد، چه اینکه از نظر او لوازم مدل حکمرانی سنتی با ماهیت نقاط اتصال و پایداری شبکه جهانی سر ناسازگاری دارد. بازخوانی نقطه نظرات این متفکر در پارادایم آمریکایی حکمرانی فضای مجازی که غالباً اصالت را به فعالیت آزاد و بی دردسر شرکت های خصوصی می دهد، این بار در حاشیه وقایع جنگ روسیه و اوکراین و به طور خاص سیاست های اتخاذ شده در همکاری نزدیک میان پلتفرم های بزرگ آمریکایی و سیاست های اتحادیه اروپا، ابعاد چالش برانگیزی از مفهوم حاکمیت مجازی (بخوانید امکان سنجی ملی سازی اینترنت) به نمایش می گذارد. در بحث حکمرانی بر فضای مجازی، برخی کارشناسان باور دارند که حکمرانی در شکل سنتی آن مناسبتی با فضای مجازی ندارد و پیش از اعمال هرگونه حکمرانی در این فضا، لازم است مفاهیم مربوط به حکمرانی و ویژگی های فضای مجازی به عنوان فضایی متمایز به دقت مورد بررسی قرار گیرد. امروزه، فناوری بسیاری از مناسبات؛ از جمله روابط بین المللی را دستخوش تغییر کرده است. با این همه، دولت ها در تلاش هستند تا بر فضای مجازی چیره شوند و سیاق حاکمیت خود را بر شهروندان فضای مجازی خود (Netizens) اعمال کنند. برخی صاحب نظران مدعی هستند که فضای مجازی نیازمند یک مدل حکمرانی دولتی است یا دست کم، دور نیست که فضای مجازی جهانی به فضاهای مجازی منطبق بر مرزهای منطقه ای و ملی تبدیل شود. باری، دولت ها - که بسیاری از آنها مدتی است به دنبال تسلط بر فضای مجازی هستند - اقدام به حکمرانی بر فضای مجازی کرده اند و تمایل دارند به همان شیوه سابق خود - یعنی سازوکار حکمرانی بر مرزهای ملی - عمل کنند. اما سؤالی که در اینجا مطرح می شود این است که آیا این مدل حکمرانی بر فضای مجازی قابلیت از بین بردن محدودیت های جغرافیایی را دارد؟! پاسخی که به این سؤال می توان داد، این است که تلاش ها برای اعمال حاکمیت در فضای مجازی نفع تنها برای این حوزه نامناسب است، بلکه نهادهای حاکمیت فراملی را که با محوریت فعالان بزرگ بخش خصوصی شکل گرفته، تهدید خواهد کرد. همچنین، سؤال دیگری مطرح می شود، مبنی بر اینکه اگر فضای مجازی یک فضای حاکمیتی نیست، پس دقیقاً چیست؟ در پاسخ به این سؤال باید فضای مجازی را به عنوان یک فضای عمومی جهانی برای تعامل در نظر بگیریم که با استفاده مشترک از پروتکل های ارتباط داده محور تعریف می شود. در واقع فضای مجازی بنا بر ماهیت خود نیازمند حکمرانی جهانی است و هر نوع سیاست گذاری در این زمینه باید تا حد امکان جهانی باشد.

فضای مجازی و دعوای ژئوپولیتیک

امروزه فناوری به بخش قابل توجهی از نظام سیاسی در سطح بین المللی و ابزاری برای تعامل بازیگران در مناسبات فراملی تبدیل شده است. همان طور که ظهور یک فناوری صنعتی (حمل و نقل ریلی) باعث تغییرات عمده در سازمان های اقتصادی، سیاسی و نظامی می شود، بر همین اساس افزایش ارتباطات داده ای با قابلیت تعامل جهانی و جامعه ای که به طور فزاینده ای بر اطلاعات متمرکز است، بر نحوه اداره ارتباطات بین المللی و احتمالاً بر شکل دولت ها تأثیر می گذارد. این دامنه اثرگذاری تا جایی است که می توان گفت اثرگذاری «انقلاب مجازی» بر اصول روابط بین المللی، عمیق تر از سایر فناوری های است؛ این امر نه تنها منابعی را که حاکمیت ها می توانند علیه یکدیگر به کار ببرند، تغییر می دهد - همان طور که سایر انقلاب های فناورانه انجام داده اند - بلکه تا حدودی و به طور قابل توجهی از اقتدار دولت در امور امنیتی می کاهد. از آنجایی که فضای مجازی به بازیگران خارج از سیستم دولتی متعارف قدرت می دهد، دولت ها دیگر تنها منبع تأمین کننده و همچنین تهدیدکننده امنیت فضای مجازی نیستند.

نکته ای که باید به آن توجه شود، این است که بحث حاکمیت در فضای مجازی صرفاً یک بحث نظری نیست، بلکه بازتابی از مبارزه قدرت بر سر حکمرانی اینترنت در میان قدرت های بزرگ جهان، به ویژه ایالات متحده، چین و روسیه است. بر همین اساس پیوند فضای مجازی با حاکمیت باید در چهار چوب تعارضات ژئوپولیتیکی معاصر ارزیابی شود. بدیهی است که ایالات متحده و متحدانش در ناتو به دنبال حاکمیت در فضای مجازی



تنش میان روسیه و اوکراین در شرایطی ادامه می یابد که شاید برای نخستین بار در جهان است، اینترنت، فضای مجازی و فناوری های ارتباطی در صف خطوط مقدم جنگ قرار می گیرد؛ از تحریم های اپریتلنفرم های رسانه اجتماعی (فیس بوک، تیک تاک، یوتیوب و توئیتر) علیه حساب های کاربری روسی گرفته، تا کمک های زیرساختی اتحادیه اروپا به اوکراین، دسترسی مردم اوکراین به اینترنت ماهواره ای، حملات سایبری متعدد به پایگاه های دولتی هر دو کشور، دستکاری الگوریتم جست و جوی گوگل به درخواست اتحادیه اروپا یا حتی تحریم داخلی نظیر محدودسازی دسترسی کاربران روسی به برخی رسانه های اجتماعی توسط دولت این کشور. دامنه این مداخلات فناوری محور به قدری وسیع و وزن آنها تا اندازه ای سنگین است که می توان به جرت عبارت جنگ مجازی را در کنار سایر ابعاد این پدیده ناگوار و غیرانسانی مثل اقتصاد، تسلیحات، راه های ارتباطی، روابط دیپلماتیک و... مشاهده کرد. در این میان، بار دیگر بحث از معنا و مفهوم حکمرانی (Governance) و حاکمیت (Sovereignty) در دنیای به ظاهر بدون مرز و خط کشی اینترنت، با بالا گرفتن درگیری های فیزیکی بر سر مرز و سرزمین که از قضا به دنیای مجازی نیز کشیده شده، به میان آمده است. در این یادداشت مروری خواهیم داشت بر مقاله ای با عنوان «علیه حاکمیت در فضای مجازی» اثر «میلتون مولر»، استاد برجسته دانشگاه

خودگردان اهمیت دارد، پایداری شبکه و تبادل بی‌وقفه داده از خلال آنهاست که در اکثر قریب‌به‌اتفاق موارد با اقتضانات مرزهایی که برای دولت‌ها دارای اهمیت هستند، هم‌خوانی ندارند. همچنین ایجاد امنیت به دلیل مقیاس گسترده آنها، در سطح سازمانی و غالباً فراملی مطرح می‌شود، نه در سطح سرزمینی. بیشتر تهدیدهای مجازی مربوط به آسیب‌پذیری در کدها، برنامه‌ها و سیستم‌عامل‌ها در سراسر جهان است و مرز خاصی را دربر نمی‌گیرد و حملات ممکن است شامل سرقت مدارک مربوط به سازمان خاصی شود. پکت‌های داده بدون توجه به اینکه از داخل یا خارج از مرزهای یک کشور آمده باشند، می‌توانند تهدیداتی را دربر داشته باشند. همچنین پکت‌هایی که از داخل مرزها می‌آیند، ممکن است توسط عوامل خارج از مرزها تولید شده باشند. پس مسئله این نیست که آیا فضای مجازی یک منطقه عاری از امنیت است یا خیر. بلکه سؤال اصلی این است که چه کسی مرزهای سیستم‌های خودگردان را تعریف و مدیریت می‌کند؟!

شرایط حکمرانی سنتی

دولت‌ها مدعی هستند که بهترین شکل نظارت و پایش فضای مجازی متعلق به آنهاست، در حالی که برای ایجاد یک حاکمیت نسبی مبتنی بر سرزمین در فضای مجازی، باید به صورت گسترده سازمان‌دهی مجددی در فناوری، استانداردها، بازارها، سازمان‌ها و مؤسسات دنیای دیجیتال انجام گیرد. با توجه به مطالبی که گفته شد، حکمرانی بر فضای مجازی در شکل سنتی خود و آنچه دولت‌ها آن را به عنوان مدل مطلوب در پی گرفته‌اند، متضمن این موارد خواهد بود:

- ۱- از بین بردن تمام ۶۰ هزار سیستم خودگردان و کاهش آن به حدود ۲۰۰ سیستم خودگردان و همچنین اجرای مقررات بسیار دقیق در هر یک از آنها.
- ۲- شناسایی هر یک از سیستم‌های خودگردان و اختصاص آنها به نهادهای قضایی. همچنین آدرس‌های آی‌پی دیگر نباید توسط سازمان‌های غیرانتفاعی فراملی مانند ICANN، RIPE-NCC یا ثبت‌های جهانی مانند com اداره شوند.
- ۳- نظارت دقیق بر روند ارائه خدمات اینترنتی و هر یک از ده‌ها هزار ارائه‌دهنده خدمات مبتنی بر وب که باید جداگانه با هر دولت ملی درباره دسترسی به بازار مذاکره کنند.
- ۴- ایجاد سازوکاری به منظور شناسایی و تأیید صلاحیت برای هرگونه جابه‌جایی و استقرار داده؛ چراکه از این طریق می‌توان الزامات بومی سازی داده‌ها را به طور کامل اجرا کرد.
- ۵- تمام دستگاه‌هایی که مورد استفاده کاربران نهایی قرار می‌گیرند، باید دارای مجوز باشند، در غیر این صورت غیرقانونی تلقی می‌شوند.

حرف آخر

از نظر کارشناسان، مفهوم حاکمیت دولت-ملت همچنان از نفوذ قدرتمند و گسترده‌ای برخوردار است. ولی به دنبال گسست و شکاف گسترده بین فضای مجازی جهانی شده و ابزارهای سنتی اعمال حکمرانی دولت‌ها، امروزه شاهد تلاش‌های برخی صاحب‌نظران و سیاست‌گذاران برای اشتهی برقرار کردن میان حاکمیت ملی و اینترنت هستیم. در چنین شرایطی، باید استراتژی‌ای انتخاب کرد که مبتنی بر حکمرانی جهانی باشد، به صورتی که تنوع ترجیحات ملی را هر چه بیشتر با نیاز به درک مشترک جهانی در مورد حکمرانی بر فضای مجازی به نفع پایداری و توسعه شبکه جهانی تطبیق دهد. در نهایت، هیچ تضمینی وجود ندارد که به رسمیت شناختن دامنه‌ها و سیستم‌های خودگردان شبکه به عنوان یک هم‌دار (Commons) در سطح جهانی، به یکباره با عصای جادویی خود، مشکلات حوزه امنیت، جرائم مجازی و نهایتاً نزاع بر سر حاکمیت اینترنت را حل می‌کند، ولی با این حال به نظر می‌رسد این اتفاق از خطرات آشکار تحمیل انگاره‌های حاکمیت سنتی مبتنی بر مرز و الگوهای سرزمینی بر اینترنت جلوگیری کند و دست‌کم چهار چوب بهتری برای حل مشکلات حاکمیت فراملی فراهم آورد.

در چهار چوب قوانین بین‌المللی هستند. این رویکرد ریشه‌های ابزاری دارد؛ با استناد به قانون درگیری‌های مسلحانه، آنها می‌خواهند سازوکارهای مناسبی برای پاسخ یا بازدارندگی حملات مجازی از سوی کشورهای متخاصم اما ضعیف‌تر بیابند. از سوی دیگر، ادعاهای حاکمیتی رقیب آمریکا-روسیه و چین-شکل بسیار متفاوتی دارد، اگرچه هر دو گروه، حاکمیت بر اینترنت را فعالانه دنبال می‌کنند. چین و روسیه با مشروعیت بخشی به پاسخ نظامی به حملات مجازی، سیاست‌های امنیت مجازی را نظامی می‌کنند. بنابراین جدی‌ترین تلاش‌ها برای اعمال حکمرانی سرزمینی و بازتولید قدرت سیاسی-نظامی در فضای اینترنت را می‌توان در این سه کشور ملاحظه کرد، هر چند در رویکرد قانون‌مدارانه و مبتنی بر منافع عمومی اتحادیه اروپا نیز رگه‌هایی از ارجحیت بازارهای ملی و مقاومت در برابر تداوم سلطه ایالات متحده (وضع موجود) احساس می‌شود. در یک تقسیم‌بندی کلی، دو گروه در زمینه حاکمیت بر فضای مجازی وجود دارد؛ کشورهایی که اقدامات تنبیهی، از جمله اعمال تحریم‌ها و حتی اقدام نظامی در برابر حملات مجازی را به رسمیت می‌شناسند و در مقابل، کشورهایی که اعمال این قوانین و اصول حقوقی را تأیید نمی‌کنند و معتقدند مردم کشورها ایشان آزادند تا در فضای مجازی و از طریق آن برای دستیابی به اهداف سیاسی خود بدون هیچ محدودیتی اقدام کنند. به صورت ساده‌ای می‌توان چین و روسیه را در گروه اول و ایالات متحده و بسیاری از کشورهای اروپایی را در گروه دوم قرار داد.

قلمرو و حاکمیت در فضای مجازی

حامیان حکمرانی بر فضای مجازی ادعای خود را بر اساس دوگانه کاذبی قرار می‌دهند. آنها معتقدند که باید مرزهای دولتی و حوزه قضایی را بر فضای مجازی تحمیل کرد؛ چراکه در غیر این صورت مرزی وجود نخواهد داشت و چنین وضعیتی به بی‌نظمی منجر خواهد شد. اما این استدلال مبتنی بر یک فرض نادرست است؛ چراکه مرزها در فضای مجازی وجود دارند، فقط با اصول دولت‌ها هم‌خوانی ندارند. اینترنت در ابتدای شکل‌گیری (به دنبال پروژه تحقیقاتی دارپا در وزارت دفاع ایالات متحده) قرار نبود که یک فضای مجازی همگن و بدون مرز را شکل دهد؛ در نتیجه به صورت شبکه‌ای از شبکه‌ها طراحی شد. سیستم‌های خودمختار شبکه اصطلاحی فنی مربوط به شبکه‌های انفرادی است که برای ایجاد اینترنتی که امروزه تجربه می‌کنیم، با یکدیگر پیوند می‌خورند. به نظر می‌رسد واحد تعریف حاکمیت در فضای اینترنت این سیستم‌های خودگردان شبکه هستند که در حال حاضر اکثراً به صورت خصوصی اداره می‌شوند و به لحاظ وضعیت جغرافیایی استقرار نیز فراملی (و به ندرت ملی) هستند؛ توگویی واحدهای اصلی سرزمینی در دنیای اینترنت، این سیستم‌های خودگردان هستند که ابتکار عمل کامل را در فرایندهای حیاتی مسیریابی (Routing)، اختصاص آدرس‌ها (IP)، اتصال به دیگر شبکه‌ها (BGP) و پروتکل‌های درگاه‌های مرزی (Gateway) در اختیار دارند. نمونه‌ای از این سیستم خودگردان بزرگ و فراملی شرکت آمازون است که با ثبت ۱۶۵۰۹ سیستم منفرد، دارای ۲۶ میلیون آدرس آی‌پی و بیش از ۳۱۷ نقطه همتایابی (Peering) است که در ۳۰ کشور جهان توزیع شده است. در مقابل و به عنوان یک نمونه کاملاً متفاوت، می‌توان به ناحیه کالج ایالتی سیاتل در آمریکا اشاره کرد که با برخورداری از ۱۲۵۴۴ آدرس آی‌پی صرفاً در یک نقطه همتایابی انجام می‌دهد که آن هم به دانشگاه واشنگتن در قلمرو سرزمینی ایالات متحده تعلق دارد. در حقیقت، آنچه برای تداوم و توسعه این سیستم‌های

