

## نسبت قلمرو حکمرانی با فضای سایبر

علی لکزائی<sup>۱</sup>، کاظم فولادی قلعه<sup>۲</sup>

<sup>۱</sup> دانشجوی کارشناسی ارشد گرایش امنیت سایبری، دانشکده برق و کامپیوتر، دانشگاه تربیت مدرس؛ دستیار پژوهشی آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران  
lakzaei.ali@modares.ac.ir  
<sup>۲</sup> استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛ سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران  
kfouladi@ut.ac.ir

### چکیده

موضوع حکمرانی از مباحثی است که در شرایط کنونی ذهن دانشمندان و سیاستمداران را به شکل توأمان درگیر کرده است. حکمرانی، از آن حیث که هم دانش است و هم کنش، از گستره وسیعی برخوردار بوده و آنچه باعث اهمیت بیشتر آن شده است، نقش و تأثیر آن در پیشرفت و عقب ماندگی کشورها است؛ آنچه امروزه بر پیچیدگی الگوهای حکمرانی افزوده است، افزوده شدن فضای سایبر به عنوان عنصری تعیین کننده در این عرصه می باشد. از این رو تعیین نسبت قلمرو حکمرانی با فضای سایبر از اهمیت مضاعف برخوردار است و اتخاذ هر رویکردی در باب قلمرو حکمرانی مستقیماً بر گستره حکمرانی و سیاست های اتخاذ شده در این زمینه و در نتیجه بر امنیت ملی و بلکه تمامی ساحت های زندگی فردی و اجتماعی هر کشوری اثرگذار است؛ از این رو پرسش اصلی مقاله حاضر نسبت قلمرو حکمرانی با فضای سایبر است. فرضیه مورد بررسی این است که نسبت قلمرو حکمرانی با فضای سایبر سه عرصه را در بر می گیرد. ۱- حکمرانی در فضای سایبر ۲- حکمرانی بر فضای سایبر ۳- حکمرانی با فضای سایبر، مهم ترین دست آورد مقاله این است که غفلت از هر یک از سه عرصه مذکور موجب ناقص دیده شدن نسبت قلمرو حکمرانی با فضای سایبر بوده و به جای فرصت سازی، چالش خیز، تهدیدساز و بحران آفرین خواهد بود.

**کلمات کلیدی:** حکمرانی در فضای سایبر، حکمرانی بر فضای سایبر، حکمرانی با فضای سایبر، قلمرو حکمرانی، سایبرنتیک.

## ۱ مقدمه

تعریف واژه سایبرنتیکس<sup>۱</sup> در لغت نامه آکسفورد به این شرح است: «علم ارتباطات و سیستم های کنترل خودکار در ماشین ها و موجودات زنده». همان طور که واژه فیزیکس<sup>۲</sup> به معنای دانش فیزیک است، واژه

<sup>۱</sup>Cybernetics

<sup>۲</sup>Physics

«سایبرنتیکس» نیز به معنای دانش سایبرنتیک است؛ این واژه به عنوان یک دانش در سال ۱۹۴۸ برای اولین بار توسط نوربرت وینر ریاضیدان و دانشمند آمریکایی مورد استفاده قرار گرفت؛ در لغت‌شناسی نیز واژه سایبرنتیکس به کورنه‌تس<sup>۳</sup> یونانی برمی‌گردد؛ که به معنای «سکان‌دار» است. این واژه با واژه گاورننس<sup>۴</sup> به معنای «عمل یا نحوه کنترل یک ایالت، سازمان و غیره» یک ریشه مشترک دارد. هم‌ریشه بودن واژگان مختلف به معنای ارتباط میان مفهوم آن واژگان است. در زبان پارسی واژه گاورننس به واژه «حکمرانی» ترجمه شده است. در لغت‌نامه آکسفورد واژه «کنترل» در تعریف مفهوم هر دو واژه «سایبرنتیکس» و «گاورننس» به کار برده شده است؛ در نتیجه واژه منسوب به علم حکمرانی و واژه منسوب به علم سایبرنتیک در لغت و مفهوم از یک ریشه هستند و دربردارنده یک مفهوم واحد هستند.

فرض ما در این مقاله این است که «حاکمیت» و «سایبر» یکی هستند؛ این فرض ما بر دو پایه استوار است، یک پایه آن از منظر علم لغت‌شناسی است که مورد اشاره واقع شد و دیگری موضوع فلسفه «حاکمیت» است. امروزه ساز و کار همه چیز با گردش بلادرنگ و لحظه‌ای اطلاعات ممکن است، از نامه‌نگاری‌های کوچک میان سازمانی گرفته تا سامانه‌های بزرگ بانک‌ها، مراکز داده، تاکسی‌ها و ... که دقیقه‌ای اخلاص در کار آن‌ها می‌تواند منجر به خطرات جبران‌ناپذیر مالی، جانی و حتی به خطر افتادن امنیت ملی شود. همچنین در تمامی سازمان‌ها و سازوکارهای موجود در دولت‌ها، کم‌تر حوزه‌ای وجود دارد که تحت نظر و اشراف کامل بخش فناوری اطلاعات نباشد. به عنوان مثال در سازمان‌ها حتی برای تغییر در کوچک‌ترین ساز و کار اجرایی و اداری ابتدا باید با بخش فناوری اطلاعات هماهنگی لازم به عمل بیاید؛ که آیا چنین تغییری از آن منظر قابل اجراء است یا خیر، اگر که قابل اجرا باشد آنگاه می‌توان آن را در قالب کلی اجرا نمود و اعمال کرد. فضای سایبر فضایی است که اطلاعات در آن به صورت هدفمند به گردش در می‌آید. فضای سایبر برگرفته از دانش سایبرنتیک است و قوانین دانش سایبرنتیک بر آن حاکم است، همان‌طور که در فضای فیزیکی، قوانین دانش فیزیک حاکم است.

## ۱.۱ پیشینه

در زمینه ارتباط حکمرانی و فضای سایبر کتاب‌ها و مقالات متعددی نوشته شده است؛ از جمله کتاب «تحول در عصر فضای مجازی» به کوشش فیروزآبادی [۲]، کتاب «حکمرانی: مقدمه‌ای بسیار کوتاه» [۱۲] نوشته مارک بور، کتاب «فضای سایبر و امنیت سایبر» [۱۱] نوشته کوستوپولوس، کتاب بنیادی «استفاده انسانی از انسان‌ها» [۸] نوشته نوربرت وینر، کتاب «سایبرنتیک: از گذشته تا آینده» [۹] نوشته نوویکو<sup>۷</sup>، مقاله «چالش‌های راهبردی حکمرانی با گسترش فضای سایبر» [۴] به کوشش احسان کیان‌خواه، کتاب «نظریه حکمرانی از منظر اندیشمندان» [۳]، مقاله «شناسایی نقش‌های سیاستی در نظام حکمرانی محتوای فضای مجازی کشور» [۵]، مقاله «تحلیل پیشینه حکمرانی فضای مجازی جمهوری اسلامی ایران» [۶] به کوشش

<sup>3</sup>Kubernētēs

<sup>4</sup>Governance

<sup>5</sup>Governance: a very short introduction

<sup>6</sup>The human use of human beings

<sup>7</sup>Novikov

فیروزآبادی، مقاله «آسیب‌شناسی فضای مجازی» [۷] به کوشش مرضیه رونقی، مقاله «حکمرانی حریم خصوصی» [۱۳] به کوشش دوندا<sup>۸</sup> و آلمیدا<sup>۹</sup>، «حکمرانی در قرن بیست و یکم» [۱۸] نوشته روسناو<sup>۱۰</sup>.

## ۲.۱ مفاهیم

واژه حکمرانی از واژگانی است که علاوه بر استفاده گسترده از آن، تلقی‌های گوناگون و متفاوتی از آن ارائه شده، تا جایی که حکمرانی را به یک لفظ مشترک برای معانی گوناگون بدل ساخته است. این وضعیت تا جایی پیش رفته است که بسیاری از اوقات مفهوم حکمرانی، معادل یکی از مفاهیم اخص آن، یعنی «حکمرانی خوب»<sup>۱۱</sup> انگاشته شده و تمام مؤلفه‌های حکمرانی خوب به مفهوم حکمرانی نیز تسری داده شده است. در یک تعریف ساده و مقدماتی، حکمرانی عبارت است از «فرآیند حکومت کردن» که شامل همه فرآیندهای برنامه‌ریزی، سازماندهی، جهت‌دهی، هدایت و کنترل نیز می‌شود. حکمرانی در محاورات رایج معاصر نیز به این معناست که «چگونه بازیگران - موجودیت‌های چندملیتی، حکومت‌ها، شرکت‌های خصوصی، گروه‌های اجتماعی یا سیاسی، اشخاص حقیقی یا ترکیبی از این موارد - برای تحقق اهدافی که آن بازیگران در آن موافق یا مشترک بوده‌اند، جهت‌دهی شده‌اند.» [۱].

فعالیت حکومت‌ها به صورت روز افزون در تنظیمات فراملی و بین‌المللی تنیده شده است، امری که ناشی از بین‌المللی شدن تعاملات صنعتی و مالی، ظهور بلوک‌های منطقه‌ای و افزایش نگرانی‌ها درباره مسائل جهانی، مانند تروریسم و محیط زیست، است. «حکمرانی در اینجا به معنای استفاده از روش‌های رسمی و غیررسمی توسط دولت‌ها برای پاسخ به نظم در حال تغییر جهانی است.» [۱۲].

هدف دانش سایبرنتیک به بیان پدر این علم، یعنی نوربرت وینر، بدین شرح است که زبان و تکنیکی را توسعه دهد تا مشکل کنترل و ارتباطات را به‌طور کلی یک بار برای همیشه، نه تنها فقط در ماشین‌ها بلکه در انسان‌ها نیز حل شود [۸]. نوویکو نیز در کتاب خود دانش سایبرنتیک را شاخه‌ای از علم کنترل در کنار فلسفه مدیریت که شاخه دیگر آن است می‌داند؛ که به مطالعه کلی‌ترین قواعد نظری کنترل می‌پردازد: «مبانی علم کنترل شامل قوانین کلی و اصول کنترل کارآمد است که این موارد در حوزه سایبرنتیک قرار می‌گیرد.» [۹].

در این مقاله با بهره‌گیری از تعاریف ارائه شده تعریف ذیل پیشنهاد می‌شود و مقصود ما از حکمرانی در این مقاله، همین تعریف خواهد بود: «حکمرانی به سیستم و فرآیندهایی اطلاق می‌شود که سازمان‌ها، نهادها یا جوامع به‌وسیله آن تصمیم‌گیری می‌کنند، سیاست‌ها را اجرا می‌کنند و امور خود را مدیریت می‌کنند. حکمرانی، دربرگیرنده سازوکارها، ساختارها و اصولی است که اعمال و رفتار افراد، گروه‌ها یا نهادها را برای دستیابی به اهداف و مقاصد مدنظر هدایت و تنظیم می‌کند و در عین حال مسئولیت‌پذیری، شفافیت و پایبندی به قوانین و هنجارهای تعیین‌شده را تضمین می‌کند.»

<sup>8</sup>Doneda

<sup>9</sup>Almeida

<sup>10</sup>Rosenau

<sup>11</sup>Good governance

در این مقاله، فضای سایبر را نیز با این تعریف مورد استفاده قرار خواهیم داد: «فضای سایبر، فضای تغذیه هدفمند اطلاعات است: این فضا یک فضای حقیقی ناملموس است و چهار رکن اساسی دارد که شامل اطلاعات، کنترل، ارتباطات و محاسبات می‌باشد.

## ۲ ارکان فضای سایبر

در فضای سایبر سه رکن اساسی وجود دارند که منجر می‌شوند تا رکن پایه اطلاعات در آن به صورت هدفمند به گردش در آید: ۱- کنترل، ۲- ارتباطات، ۳- محاسبات. در یک محیط برای هدفمندسازی گردش اطلاعات، دو عنصر حیاتی وجود دارد:

۱. کنترل‌کننده‌ای که با انجام محاسبات بر اطلاعات دریافتی از محیط و بازخورد (فیدبک) دریافتی از کنترل‌شونده، اطلاعات (فرمان) را به‌وسیله رکن ارتباطات به کنترل‌شونده منتقل می‌کند.
۲. کنترل‌شونده‌ای که با دریافت اطلاعات (فرمان) از کنترل‌کننده، محاسباتی بر روی داده‌های دریافت شده انجام داده و کنش متناظر را بر محیط انجام می‌دهد.

کنشی که نتیجه‌ی اطلاعات دریافتی توسط کنترل‌شونده است، خود اطلاعات جدیدی را در محیط قرار می‌دهد که کنترل‌کننده بر آن‌ها اشراف پیدا می‌کند و با انجام محاسبات بر روی آن، فرمان بعدی خود را به‌گونه‌ای تعیین می‌کند که کنترل‌شونده به هدف مورد نظر نزدیک‌تر شود. بدین‌گونه چرخه سایبرنتیک متولد می‌شود و اطلاعات به شکلی هدفمند در یک محیط به گردش در می‌آیند. به‌عنوان مثال، در یک اتومبیل، راننده در نقش کنترل‌کننده و پدال‌های گاز و ترمز عامل‌های انتقال پیام یا عامل‌های ارتباطی او هستند. به‌وسیله این عامل‌ها راننده دستور خود را به کنترل‌شونده که اتومبیل است ارسال می‌کند. اتومبیل نیز بر اساس سازوکارهای محاسباتی که در آن تعبیه شده بر محیط کنشی را اجرا می‌کند که می‌تواند افزایش و یا کاهش سرعت باشد؛ راننده نیز با تحلیل بر روی اطلاعاتی که از کنش اتومبیل بر محیط دریافت کرده، قدم بعدی خود را برنامه‌ریزی و اعمال می‌کند.

## ۳ قلمرو حکمرانی

منظور از قلمرو حکمرانی، دایره شمول عرصه‌های حکمرانی است. همان‌طور که در منابع مذکور نیز آمده است، قلمرو حکمرانی و دایره شمول آن، تمامی عرصه‌های زندگی بشر را در بر می‌گیرد. به‌عبارتی، حکمرانی، عهده‌دار ساماندهی عرصه‌های مختلف زندگی سیاسی، اقتصادی، فرهنگی، مدیریتی، اجتماعی و ... جوامع بشری و هر آن چیزی است که به‌نحوی با انسان مرتبط می‌شوند. به‌عنوان مثال محیط زیست، آب، برق، گاز و ...؛ به‌همین دلیل است که ملاحظه می‌کنیم مفهوم حکمرانی برای موضوعات گوناگون به‌کار رفته است؛ از جمله: حکمرانی فرهنگی، حکمرانی اقتصادی، حکمرانی حقوقی، حکمرانی آب، حکمرانی برق، حکمرانی سیاست خارجی و ...

در این مقاله بحث ما محدود به حکمرانی فضای سایبر است. امروزه فضای سایبر به خاطر گستردگی روزافزون، تمام جنبه‌های زندگی ما را در بر می‌گیرد. لذا رویکرد دقیق در نسبت‌سنجی بین قلمرو حکمرانی و فضای سایبر این است که امروزه با توجه به نقش و جایگاهی که فضای سایبر در حاکمیت کشورها پیدا کرده است و اینکه فضای سایبر از یک بحث صرفاً فنی و تکنولوژیک و یا صرفاً ابزاری برای تسهیل امور مختلف و یا ایجاد دولت الکترونیک و حتی نظریه حکمرانی خوب فراتر رفته و تمامی عرصه‌های حاکمیتی زندگی انسان را پوشش می‌دهد.

به طور کلی می‌توان گفت که پنج دیدگاه در رابطه با نسبت سایبر با حاکمیت در جهان مطرح است که در ادامه به آنها اشاره می‌کنیم.

**۱- عدم نسبت میان حاکمیت و سایبر:** در این دیدگاه این ادعا می‌شود که هیچ نسبتی میان سایبر و حاکمیت وجود ندارد. افرادی که این دیدگاه را دارند، به طور کلی، کسانی هستند که اصالت را به «تکنولوژی» می‌دهند. کسی که اصالت را به تکنولوژی می‌دهد، با کسی که از تکنولوژی استفاده می‌کند متفاوت است. چنین شخصی معتقد است که همه چیز در دنیا را باید از نگاه تکنولوژی ملاحظه کرد. این افراد طرح این سؤال که «نسبت میان سایبر و حاکمیت چیست؟» را به طور کلی غلط می‌دانند و استدلال می‌کنند که سایبر یک مقوله تکنولوژیک و فنی است، و حاکمیت یک مفهوم استراتژیک و راهبردی است و برای همین رابطه‌ای ندارند. امروزه طرفداران این دیدگاه نسبت به سالیان گذشته کمتر شده‌اند.

**۲- حاکمیت به عنوان فراهم‌کننده زیرساخت «سایبر» و نه چیز دیگر:** دیدگاه دوم، حاکمیت را به عنوان فراهم‌کننده زیرساخت و تمهیدکننده امکانات لازم برای سایبر قبول دارد. در واقع، در این دیدگاه شأن حاکمیت تأمین نیاز شهروندان در قبال دریافت حق اشتراک است - نظیر آنچه در زمینه‌ی برق، آب، گاز و موارد مشابه عمل می‌کند - و اساساً نباید به قانون‌گذاری، نظارت، وضع سیاست و ... ورود کند. این دیدگاه نسبت به دیدگاه اول واقعی‌تر است، زیرا برای دستیابی عموم به سایبر، نیازمندی‌های بسیاری وجود دارد، از جمله: تهیه نقشه‌های جغرافیایی از مکان‌های مورد نظر برای بهره‌برداری، کابل‌کشی، دکل‌کشی، زیرساخت‌های مخابراتی و ... و از آنجا که این نیازمندی‌ها استفاده‌ی عمومی دارند، جایگاهی در اندازه‌ی حاکمیت برای راه‌اندازی و پشتیبانی نیاز خواهند داشت. نتیجه‌ی طبیعی این دیدگاه این است که حاکمیت درباره‌ی نحوه‌ی مصرف و بهره‌برداری از سایبر توسط مردم نباید دخالتی داشته باشد، همان‌طور که در خصوص زیرساخت‌هایی چون آب، برق و گاز عمل می‌کند و نهایتاً حجم مصرف را با وضع تعرفه و تعیین هزینه مدیریت می‌کند.

**۳- حاکمیت به عنوان سیاست‌گذار، قانون‌گذار و نظارت‌کننده بر «سایبر»:** در عموم نقاط دنیا مسئله سیاست‌گذاری، قانون‌گذاری، نظارت و مواردی از این قبیل، برای مفهوم سایبر نه تنها به رسمیت شناخته شده بلکه بسیار مورد تأکید و توجه است. در این دیدگاه نقش حاکمیت به عنوان تأمین‌کننده زیرساخت نقض نمی‌شود؛ بلکه علاوه بر آن، به دلیل ویژگی‌های ماهیتی سایبر، برخلاف برق، آب، گاز و ...، حاکمیت باید قانون‌گذاری، سیاست‌گذاری و نظارت را در دستور کار خود قرار دهد. مقوله‌ای که از آن با

نام «حکمرانی فضای سایبر» یا به تعبیری (البته با تسامح) به عنوان «حکمرانی فضای مجازی» یاد می‌کنند، به نوعی از این دیدگاه تازه شروع می‌شود. این دیدگاه بیشتر در شورای عالی فضای مجازی کشورمان رایج است [۲]. این دیدگاه یک نگاه حداقلی و یک نگاه حداکثری دارد. افرادی که این دیدگاه را دارند، در گستره‌ی این طیف قرار می‌گیرند.

**۴- حاکمیت به عنوان بزرگ‌ترین و پیشرفته‌ترین بهره‌بردار «سایبر»:** در بسیاری از کشورهای پیشرفته دنیا، امروزه این دیدگاه در حال تقویت شدن است. این دیدگاه حاکمیت را نه تنها تأمین‌کننده زیرساخت، قانون‌گذار، سیاست‌گذار و ناظر می‌داند؛ بلکه آن را پیشرفته‌ترین و بزرگ‌ترین کاربر سایبر می‌داند. این مورد زمانی رقم می‌خورد که حاکمیت تمام خدماتی را که می‌خواهد به مردم ارائه کند و تمام وظایفی که بر عهده دارد را از طریق فضای سایبر محقق کند: از طریق پلتفرم‌ها، نظارت‌ها از طریق دوربین، از طریق هوش مصنوعی و دیگر مفاهیمی که امروزه در رسانه‌ها به کرات شنیده می‌شوند. تمامی این موارد مربوط به دیدگاه چهارم هستند. برخی افراد عبارت «دولت فوق هوشمند» را برای این دیدگاه به کار می‌برند. این‌ها همه زمانی اتفاق می‌افتد که حاکمیت، خود، بزرگ‌ترین بهره‌بردار و کاربر سایبر می‌شود. امتیاز این مورد آن است که اگر حاکمیت به چنین چیزی دست یابد و خود بزرگ‌ترین بهره‌بردار سایبر شود، آنگاه به دلیل نیازمندی‌های بالای سخت‌افزاری و نرم‌افزاری، اکوسیستم مربوط به پدیده آی‌تی<sup>۱۲</sup> و آی‌سی‌تی<sup>۱۳</sup> فوق‌العاده گسترده می‌شود، چرا که باید پاسخگوی نیازهای حاکمیت باشد. در نتیجه، سرریز تمام این پیشرفت‌ها وارد زندگی مردم نیز می‌شود و شهروندان نیز از این قابلیت‌ها بهره‌مند می‌شوند. در اسناد سازمان ملل این از این دیدگاه با عنوان «حکمرانی خوب» نام برده می‌شود.

**۵- این‌همانی سایبر و حاکمیت** به نظر می‌رسد چهار دیدگاه مذکور، برای شکل‌گیری یک حکمرانی و حاکمیت مستقل و قدرتمند در یک کشور، دیدگاه‌های کاملی نیستند. ضعف دیدگاه اول که بدیهی است، اما دیدگاه دوم، سوم و چهارم، همگی یک نقطه ضعف دارند و آن این است که دیدگاه آنها به سایبر یک نگاه ابزاری است و به عنوان یک پدیده ابزاری و وسیله به سایبر نگاه می‌شود، البته یک وسیله پیشرفته و شگفت‌انگیز. اما نگاه همه‌ی آنها در نهایت یک نگاه ابزاری است. اما در نگاه پنجم از نگاه ابزاری فاصله می‌گیریم و می‌گوییم که سایبر در واقع خود حاکمیت است. از این منظر، این‌همانی و نسبت تساوی بین این دو برقرار است. در نتیجه فضای بحث و اقدام از فضای تکنولوژیک و ابزاری به فضای استراتژیک و راهبردی تغییر می‌کند.

با این نگاه توجه به وجوه و لایه‌ها و سطوح حکمرانی سایبری دارای اهمیت است، که در ادامه مقاله به آن می‌پردازیم.

<sup>12</sup>Information technology

<sup>13</sup>Information and communications technology

## ۴ حکمرانی بر / با / در فضای سایبر

### ۱.۴ حکمرانی بر فضای سایبر

«فارغ از استفاده‌ای که دولت‌ها از فضای مجازی برای تقویت حاکمیت خود دارند، یکی از دغدغه‌های مهم آن سامان‌دهی و مدیریت فضای مجازی است. بر این اساس، دولت‌ها فضای مجازی را به‌عنوان یکی از اجزای زندگی مردم تحت حاکمیت در می‌آورند و آن را متناسب با قوانین موجود در کنار سایر اجزا مدیریت می‌نمایند. به عبارت دیگر، حکمرانی بر فضای مجازی<sup>۱۴</sup>، وضعیتی است که حاکمیت ملی بتواند فضای مجازی را به‌منزله بخشی از قلمرو خود، تحت قوه آمرانه خود قرار دهد.» [۲]. در اینجا، حاکم، فضای سایبر را به‌مثابه یک محصول می‌بیند. به‌عنوان پدیده‌ای که وارد قلمرو حاکمیتی می‌شود و حاکمیت مانند تمامی پدیده‌های دیگر، این پدیده را نیز باید تحت حاکمیت خود درآورد. به‌عنوان مثال، محصولی حیاتی همچون آب که نیازمند سازوکار مشخص و قانونی مطابق با اهداف حاکمیتی است، حکومت تلاش می‌کند تا این حوزه را تحت سلطه خود درآورد و بر آن سیطره پیدا کند. به‌عنوان مثالی دیگر، کارخانه‌ای بزرگ در حوزه ماشین‌آلات، این کارخانه را به‌اندازه‌ای بزرگ و قدرتمند تصور کنید که درصد زیادی از حجم بازار ماشین‌آلات کشوری را شامل شود؛ حکومت در اینجا چنین موجودیت عظیمی را به دلایل متعدد تحت سلطه خود در می‌آورد و بر آن قانون‌گذاری می‌کند تا بتواند از خطرات احتمالی جلوگیری کند و با استفاده از آن به سمت اهداف خود قدم بردارد.

### ۲.۴ حکمرانی با فضای سایبر

«در رویکرد حکمرانی با فضای سایبر<sup>۱۵</sup> از فضای مجازی به‌عنوان «ابزار خدمت‌رسانی» و اعمال حاکمیت در فضای حقیقی استفاده می‌کنند. آنچه به‌عنوان دولت الکترونیک طرح می‌شود در این سطح است. تلاش دولت‌ها در استفاده از این فضا برای اعمال حاکمیت کلاسیک و سنتی نیز در همین صورت خلاصه می‌شود. در این صورت، اصول حاکمیت تغییر نکرده و فقط از فناوری‌های اطلاعاتی و ارتباطی با نگاه ابزاری خدمات اتوماسیون ارائه می‌گردد.» [۲]. به‌نوعی در این منبع، روش حکمرانی همان حکمرانی خوب است. حکومت تنها به جهت سهولت بخشیدن به فرآیندها، خدمت‌رسانی و اتوماسیون، نقش فراهم‌کننده زیرساخت را خواهد داشت. در این رویکرد، اصول حاکمیت تغییر نکرده، فضای سایبر با ظهور خود نقش کلیدی در گستره حکمرانی نخواهد داشت، بلکه اهمیت این موضوع محدود شده و فقط دیدگاه «حاکمیت به‌عنوان فراهم‌کننده زیرساخت سایبر و استفاده ابزاری از آن» مورد نظر است.

رویکرد دو فضایی نیز بر این دیدگاه حاکم است. بدین‌گونه که فضای واقعی و فضای مجازی را به‌مثابه دو فضای جدا در نظر گرفته است. چرا رویکرد دوفضایی به‌جای رویکرد امتدادی به کار گرفته شده است؟ این پدیده زمانی اتفاق می‌افتد که ما واژه Cyberspace را با عنوان «فضای مجازی» ترجمه کنیم و به‌نوعی با به‌کار بردن این واژه در ترجمه، ماهیت واقعیت ناملموس فضای سایبر را از آن گرفته و ماهیت مجازی و غیرواقعی بودن را به آن بدهیم. این کار باعث می‌شود تا ما فضای مجازی را جدا از فضای واقعی بدانیم. از

<sup>14</sup>Governance on Cyberspace

<sup>15</sup>Governance by Cyberspace

این اشتباه شناختی، تعابیر غلطی نظیر «هر چیزی که در فضای واقعی وجود دارد، باید در فضای مجازی نیز وجود داشته باشد» سر بر می‌آورند.

ما در دیدگاه مورد نظرمان در این مقاله «حکمرانی با فضای سایبر» را نتیجه اعمال درست رکن «حکمرانی بر فضای سایبر» می‌دانیم، بدین گونه که اگر حکمرانی بر فضای سایبر به درستی صورت گیرد، می‌توان دست به عمل حکمرانی با فضای سایبر زد. در نتیجه باید سازوکارها، ساختار و اصولی را برای آن تعریف کرد تا بتوان با آن به اهداف مورد نظر حاکمیتی در فضای سایبر دست یافت.

### ۳.۴ حکمرانی در فضای سایبر

«در رویکرد حکمرانی در فضای سایبر<sup>۱۶</sup>، دولت‌ها تحول زندگی بشر در عصر فضای مجازی را به خوبی درک کرده و می‌پذیرند که فضای مجازی «فقط» مولد پاره‌ای از مسائل نیست؛ بلکه کلیت فضای زندگی مردم و افق تمدنی جدیدی را می‌سازد. به همین دلیل دولت‌ها، فراتر از دو حالت قبلی سعی می‌کنند ساختار خود را در راستای اعمال حاکمیت «در» آن عصر متحول کنند.» [۲]. در این دیدگاه فضای سایبر به عنوان یک زیست بوم تصور می‌شود. یک فضای زندگی که تمامی شئون زندگی در آن قرار دارد و حاکمیت نیز جزئی از آن است. لذا هنگامی که حاکمیت می‌خواهد اعمال حاکمیت کند، با در نظر گرفتن این موضوع اقدام می‌کند که خود نیز در آن زیست بوم حضور دارد. البته که این رویکرد پیچیدگی بیشتری از دو رویکرد قبلی دارد و به مراتب نیز اثربخش تر است، هر چند ملاحظات خاص خود را خواهد داشت.

## ۵ نتیجه‌گیری

با توجه به آنچه گفته شد و به ویژه تأکید بر این نکته که فضای سایبر در بردارنده همه قلمروهای حکمرانی است می‌توانیم اکنون بر این نتیجه تأکید کنیم که از میان نسبت‌های چهارگانه منطقی، یعنی نسبت تباین، نسبت عام و خاص من وجه، نسبت عام و خاص مطلق و تساوی، میان قلمرو حکمرانی و فضای سایبر، تساوی وجود دارد، دلایل این امر از آنچه آمد روشن شد. به طور خلاصه، استدلال این بود که چون فضای سایبر در بردارنده همه ساحت‌های امر حاکمیتی است و قلمرو حکمرانی هم در بردارنده تمام ساحت‌های حاکمیتی است، بنابراین بین این دو نسبت تساوی برقرار است. این امر از تأملاتی که در عرصه حکمرانی با فضای سایبر، حکمرانی در فضای سایبر و حکمرانی بر فضای سایبر آمد نیز به نحو دیگری روشن گشت.

## مراجع

- [۱] قلی پور، حسین (۱۴۰۰). حکمرانی علم: دانشمندان چگونه راهبری می‌شوند؟ انتشارات سروش.
- [۲] فیروزآبادی، ابوالحسن (۱۳۹۹). تحول در عصر فضای مجازی. انتشارات پژوهشگاه فضای مجازی.
- [۳] خان محمدی، هادی و خداپرست، عباس (۱۴۰۱). نظریه حکمرانی از منظر اندیشمندان. انتشارات سازمان جهاد دانشگاهی تهران.

<sup>16</sup>Governance in Cyberspace



- [۴] کیان خواه، احسان (۱۳۹۸). چالش‌های راهبردی حکمرانی با گسترش فضای سایبر. انتشارات امنیت ملی.
- [۵] خدمتگزار، حمیدرضا و نامداریان، لیلا (۱۴۰۲). شناسایی نقش‌های سیاستی در نظام حکمرانی محتوای فضای مجازی کشور. مجموعه مقالات نهمین کنفرانس بین‌المللی وب‌پژوهی.
- [۶] فیروزآبادی، ابوالحسن، آزادی احمدآبادی، جواد (۱۳۹۹). تحلیل پیشینه حکمرانی فضای مجازی جمهوری اسلامی ایران. نشریه دانش سیاسی. شماره ۲.
- [۷] رونقی، مرضیه (۱۳۹۶). آسیب‌شناسی فضای مجازی. کنفرانس پژوهش‌های نوین ایران و جهان در روان‌شناسی و علوم تربیتی حقوق و علوم اجتماعی.
- [8] Wiener, N. (1954). The human use of human beings: Cybernetics and society.
- [9] Novikov, D. N. (2016). Cybernetics: From past to future. Springer. <https://link.springer.com/book/10.1007/978-3-319-27397-6>
- [10] Lerner, A. Ya. (1972). Fundamentals of Cybernetics. Plenum Publishing Corporation.
- [11] Kostopoulos, G. K. (2017). Cyberspace and Cybersecurity. (2nd ed.). CRC Press.
- [12] Bevir, M. (2012). Governance: a very short introduction. Oxford University Press.
- [13] Doneda, D., & Almeida, V. A. F. (2015). Privacy governance in Cyberspace. IEEE, 19(3).
- [14] Liaropoulos, A.N. (2017). Cyberspace Governance and State Sovereignty. In: Bitros, G., Kyriazis, N. (eds) Democracy and an Open-Economy World Order. Springer, Cham. [https://doi.org/10.1007/978-3-319-52168-8\\_2](https://doi.org/10.1007/978-3-319-52168-8_2)
- [15] Bajaj, K. (2014). Cyberspace: Post Snowden. Strategic Analysis, 38, 582–587.
- [16] Betz, D., & Stevens, T. (2011). Cyberspace and the state. Toward a strategy for cyber-power (Adelphi Paper 424). Oxon: IISS, Routledge.
- [17] Choucri, N. (2012). Cyberpolitics in international relations. Cambridge, MA: The MIT Press.
- [18] Rosenau, J. (1995). Governance in the twenty-first century. Global Governance, 1, 13–43.
- [19] Jayawardane, S.; Larik, J.E.; Jackson, E. (2015). Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance. <http://www.thehagueinstituteofglobaljustice.org/wp-content/uploads/2015/12/PB17-Cyber-Governance.pdf>
- [20] Chertoff, M., & Simon, T. (2015). The impact of the dark web on Internet Governance and Cyber Security (Global Commission on Internet Governance: Paper Series No. 6). The Centre for International Governance. Retrieved February 20, 2016, from [https://www.cigionline.org/sites/default/files/gcig\\_paper\\_no6.pdf](https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf)
- [21] Cornish, P. (2015). Governing cyberspace through constructive ambiguity. Survival, 57, 153–176.
- [22] Deibert, R. (2013). Bounding cyber power: Escalation and restraint in global cyberspace (Internet Governance Papers: Paper No. 6). The Centre for International Governance Innovation. Retrieved February 20, 2016, from [https://www.cigionline.org/sites/default/files/no6\\_2.pdf](https://www.cigionline.org/sites/default/files/no6_2.pdf)

