فضای مجازی و حکمرانی خوب

گزارش نظری | شماره ۲ | تیر ۱۴۰۱ | گروه مطالعات تحلیل مسائل روز

بسم الله الرحمن الرحیم

مرکز مطالعات راهبردی و آموزش وزارت کشور

جمهوری اسلامی ایران
وزارت کشور

نویسنده: دکتر مه‌سیما سهرابی

تهیه شده در: گروه مطالعات تحلیل مسائل روز

تاریخ انتشار: تیر ۱۴۰۱

گزارش نظری

فضای مجازی و حکمرانی خوب

در این گزارش می‌خوانید

۱ فضای مجازی و حکمرانی وب از جمله مهمترین پیشران‌های شکل دهنده به آینده در حیطه حکمرانی و مدیریت امور عمومی محسوب می‌شود.

۲ برای پرهیز از بی‌نظمی سایبری و به تبع آن ممانعت از شکل گیری و تشدید شکاف در حکمرانی سایبری اتخاذ راهبرد سایبری ملی ضرورت دارد.

۳ فضای مجازی به‌عنوان بستر تحقق حکمرانی خوب و اعمال شاخص‌های آن یکی از راه‌های کسب و افزایش سرمایه اجتماعی نظام سیاسی است.

جمهوری اسلامی ایران
وزارت کشور

مرکز مطالعات راهبردی و آموزش وزارت کشور

چکیده

برای ادارهٔ امور عمومی در «حوزهٔ عمومی» دو الگو وجود دارد: ۱. الگوی نخست، الگوی «حکومت» است که مسئولیت تمام امور را بر عهده دارد. در این الگو، حکومت موظف است تمام «خدمات» را برای مصرف جامعه مدنی یا شهروندان در شکلی «تک بُعدی و یکطرفه» فراهم کند. الگوی دوم، الگوی «حکمرانی» است که در آن مسئولیت ادارهٔ عمومی بین سه نهاد «حکومت، جامعهٔ مدنی و بخش خصوصی» تقسیم می‌شود به گونه‌ای که سه نهاد یاد شده در ارتباطی تعاملی و مستمر با هم قرار دارند. «حوزهٔ عمومی[1]»، عنصر اساسی در هر سازمان سیاسی-اجتماعی است که از مؤلفه‌های مهمی چون «گفتگو»، «آگاهی از افکار عمومی» و «کنش» تشکیل شده است، عرصه‌ای که مردم به مثابهٔ «شهروندان[2]» گرد هم آمده و دیدگاه‌های مستقل خود را به‌منظور تأثیرگذاری بر نهادهای سیاسی-اجتماعی جامعه، مفصل بندی می‌کنند. بنابراین «حکمرانی[3]»، مشابه «دولت» نیست، زیرا تمام نهادهای تأثیرگذار در حوزهٔ عمومی، در دولت و قوهٔ مجریه متمرکز نشده‌اند، بلکه نهادهای تأثیرگذار دیگری هم وجود دارند که خارج از دولت و قوهٔ مجریه در جامعه ایفای نقش می‌کنند، حکمرانی خوب نتیجهٔ تعامل و کارکرد تمام قوای یک کشور و جامعه است. از این رو **موضوع «حکمرانی خوب»، موضوع «چگونگی اعمال اراده» است**، موضوعی است دربارهٔ نحوهٔ «تعامل دولت‌ها با سایر سازمان‌های اجتماعی، مردم نهاد و بخش‌های خصوصی در اتخاذ تصمیمات مرتبط با حوزهٔ عمومی»، فرایندی که از طریق آن جوامع یا سازمان‌ها تصمیمات مهم خود را اتخاذ می‌کنند و به شکل همزمان؛ مشخص می‌کنند چه افراد، گروه‌ها یا سازمان‌هایی در این فرایند درگیر شوند و چگونه وظیفهٔ خود را به انجام برسانند: مجموعه‌ای از توافقات، رویه‌ها، قراردادها و سیاست‌ها که مشخص می‌کنند قدرت در دست چه کسانی باشد، تصمیمات چگونه اتخاذ شوند و وظایف چگونه انجام شوند. همانطور که در فضای واقعی و قلمرو فیزیکی حکومت و عرصه شهروندی، نیروهای چالش‌گر، فرمان‌ها و قواعد و قوانین حکومتی و عمومی را به چالش کشیده و نقض می‌کنند، در فضای مجازی به عنوان «**فضای دوم**» نیز نیروهای چالش‌گر فرمان‌ها، ارزش‌ها، منافع و قوانین حکومتی را نقض کرده و حاکمیت حکومت ها را به چالش می‌کشند. شاخص اصلی نقض حاکمیت حکومت‌ها در فضای مجازی (همانند فضای واقعی)، نیروهای اختلال‌گر داخلی، اپوزیسیون‌های خارجی، نیروهای معاند و «بازیگران در سایه»، کارتل‌های مواد مخدر و قاچاق و...است که به وسیله عاملان آنها در اینترنت و فضای مجازی، کنترل و اعمال حاکمیت حکومت‌ها را در این فضا تضعیف و بی اثر می‌کنند. این در حالی است که در چند سال اخیر با وقوع انقلاب صنعتی چهارم و فراگیری سیستم‌های فیزیکی-سایبری، حاکمیت بر فضای سایبری و حکمرانی سایبری، اصلی‌ترین رویکرد کشورها «مدیریت فضای مجازی» شده است. شواهد نیز نشان

[1] Public Space
[2] Citizens
[3] Governance

می‌دهد که نسبت مستقیمی میان قدرت کشورها و میزان حکمرانی آنها در فضای مجازی وجود دارد. حکمرانی در عصر فضای مجازی را می‌توان از دو منظر تحلیل نمود:

۱. **حکمرانی در فضای مجازی:** این حکمرانی فاوا محور (فناوری اطلاعات و ارتباطات[۴]) است و به تبیین، تنظیم ومدیریت روابط و منافع بازیگران و ذیربطان فضای مجازی می‌پردازد.

۲. **حکمرانی ناشی از فضای مجازی:** حکمرانی ناشی از فضای مجازی به تبع آثار فضای مجازی در زندگی اجتماعی و نیاز روز افزون مردم به فضای مجازی صورت می‌پذیرد.

با تسلط بر فناوری‌های نوظهور، عملاً می‌توان نقش عمده‌ای در ساخت، کنترل و هدایت جریانات اجتماعی در ابعاد مختلف ایفا کرد. قدرت و مشروعیت هر حکومتی از طریق ملاک‌های متعددی مورد شناسایی قرار می‌گیرد که مهمترین آن «حاکمیت» است. حاکمیت در فضای واقعی، قابلیت تحقق و شناسایی آسان‌تری دارد، در حالی که در فضای مجازی، اولاً به جهت غیر ملموس بودن، پویایی و تغییر دائمی فضا و همین طور بی‌مفهوم بودن عنصر زمان و مکان، تحقق حاکمیت به شکل مرسوم آن ممکن نیست، ثانیاً این فضا اقتضائات و ویژگی-های وجودی و ماهیتی دارد که اساساً هرگونه تلاش برای تحقق حاکمیت و به رسمیت شناختن آن را با چالش روبرو کرده است. برای حکمرانی در این فضا، نمی‌توان تنها بر منابع و ابزارهای رصد و اعمال قانون اکتفا کرد، بلکه حضور و مشارکت فعالانه در این فضا خصوصاً از طریق زیرساخت‌های فناورانه باید محقق شود. اما تحقق «حکمرانی خوب» به خودی خود شکل نمی‌گیرد، و علل و عوامل گوناگونی در شکل گیری و تحقق آن نقش دارند. این «الگو» هم محدود به یک بخش، سطح یا گروه و نهاد خاص نیست، بلکه «امری فراگیر» است که تحقق آن به «هماهنگی و آمادگی» تمامی بخش‌ها نیاز دارد: هماهنگی، همکاری و پیوندِ میان سطوح گوناگون جامعه اعم از دولت، نظام سیاسی، مردم، نهادهای میانی همچون احزاب و انجمن‌های مدنی و... اما مسئله اینجاست که با افزایش پیچیدگی‌های بافتاری و جوامع اجتماعی از منظر سیاسی-اجتماعی، فرهنگی و زیست محیطی و ظهور تهدیدهای نوپدید، تحقق «حکمرانی خوب» در شکل سنتی آن مقدور نیست. از این رو، همچنان که قانون تنوع در سایبرنیتیک راس اشبی[۵] (۱۹۵۸ و ۱۹۵۶)[۶] توضیح می‌دهد، برای این که «موجود زنده» از تغییرات شکل گرفته در محیط جان سالم به در ببرد، باید «***راه حل‌هایی بیشتر از تعداد مشکلات موجود در اختیار داشته باشد***». بنابراین با توجه به ظهور تکنولوژی‌ها و پیشرفت‌های موجود در حوزهٔ فناوری-های ارتباطی و اطلاعاتی، بالاخص «فضای مجازی[۷]»، سبب شده تا «فضای مجازی» به دلیل برخورداری از ویژگی‌هایی همچون دسترسی دائم، تعامل دو سویه و چند سویه، فرامکانی و فرازمانی بودن آن، به‌عنوان ابزاری مؤثر و اثربخش در تحقق «حکمرانی خوب» در کشورهای مختلف و شکل گیری «**حکمرانی سایبری**» مورد

---

[4] ICT: در فناوری اطلاعات و ارتباطات، تأکید و محوریت بر روی «بخش ارتباطات» است

[5] Ross Ashby's Law of Requisite Variety in Cybernetics

[6] https://repository.upenn.edu/cgi/viewcontent.cgi?article=1245&context=asc_papers

[7] Virtual Space

توجه قرار گیرد. از این رو ظهور و تحقق «حکمرانی خوب» و در کل «الگوی دولت تسهیل‌گر»، از جمله موضوعات مهم و راهبردی در حوزهٔ ملی و داخلی است که عملیاتی سازی آن در پیوند با «فضای مجازی»، نیازمند تدقیق مفاهیمی چون «**فضای مجازی**»، «**دولت الکترونیک**»، «**امنیت مجازی**» و «**رسانه‌های اجتماعی**» است. این مهم در این پژوهش با تمرکز بر اسناد منتشر شده بین‌المللی و با ببرسی تجبه بریتانیا در حوزهٔ «حکمرانی سایبری» و تحلیل و نقد آن در ارتباط با امکان عملیاتی سازی این مدل در ایران مورد توجه قرار گرفته است.

فهرست

مقدمه

«حکمرانی» در لغت به معنای «اداره و تنظیم امور» است که به رابطهٔ میان «شهروندان و حکومت کنندگان» بر مبنای «***فرایندی پیوسته و همکاری جویانه***» اشاره می‌کند: به تعبیر دقیق‌تر پل زدن بین قدرت، روابط، شفافیت و پاسخگویی بخش‌های مختلف سیاسی-اجتماعی در ایفای نقش خود نسبت به موضوعات مهم و حیاتی جامعه است. اگر در علم سیاست موضوع اصلی «قدرت حکومت» است، در «حکمرانی خوب[8]» موضوع اصلی «**بهتر اداره کردن جامعه با پشتوانهٔ قدرت دولت**» بر مبنای افزایش «ضریب نفوذ فرایندها با مکانیسم‌های اجتماعی است: نفوذ هدایت شده در فرایندهای اجتماعی»، یا به تعبیر دقیق‌تر حاکمیت شبکه‌هایی است که جامعهٔ مدنی را با دولت پیوند می‌دهد، آن هم به منظور خلق «جامعهٔ بهتر» و ارائهٔ «خدمات عمومی بالاتر به شهروندان» در کوتاهترین زمان ممکن به منظور افزایش رضایت، مشارکت، و ارتقای مسئولیت پذیری شهروندان که خود متکی بر «**مدیریت‌های نوین**» است. از این رو تحقق این الگو، نیازمند شناسایی بسترهای مورد نیاز، موانع و تنگناها و فراهم کردن زمینه‌های لازم برای تحقق آن است. بنابراین «حکمرانی خوب»، به چیزی بیشتر از «دولت خوب» نیاز دارد و نیازمند «**فضاسازی برای ورود و اثر بخشی سایر بازیگران**» است و از چهار رکن اصلی تشکیل شده است:

- بخش عمومی و دولت که وظیفهٔ هدایت و راهبری و برقراری حاکمیت قانون را بر عهده دارد
- بخش‌های خصوصی که عهده‌دار ایجاد اشتغال، درآمد، تولید، تجارت هستند و وظیفهٔ کسب و کار را بر دوش دارند
- جامعهٔ مدنی که فراهم کنندهٔ فرصت ابراز وجود مردم و شهروندان است
- سازمان‌های محلی که وظیفهٔ بسیج، سازماندهی و اعمال فرهنگ‌های بومی را بر عهده دارند

بنابراین «حکمرانی خوب»، مفهوم جدیدی که از پیوند بین «سیاست و اداره کردن جامعه»، یعنی ترکیب علوم سیاسی و مدیریت دولتی، به منظور افزایش «کارآمدی نظام» در حوزه‌های مختلف به وجود آمده است. مفهوم «حکمرانی» را می‌توان در سطوح مختلفی چون سطح جهانی، سطح ملی، سطح سازمانی، و جوامع محلی و...مورد استفاده قرار داد. این مسئله با افزایش فرایند «جهانی شدن[9]»، شکل گیری «فضای مجازی» همراه با گذار از وب ۱ (نسل وبِ «داده محور و ایستا»، تک بُعدی و یک طرفه) و ظهور وب ۲ (وب «تعاملی و انسان محور»)، وب ۳ (نسل وب ماشین محور، وبِ معنایی متکی بر هوش مصنوعی و یادگیری ماشینی با قابلیت‌های «واقعیت افزوده» و «واقعیت مجازی»، استفاده از بلاکچین و کریپتوکارنسی‌ها «رمزارزها»، کاربرمحور با تمرکززدایی از شرکت‌های «میانجی، واسطه‌ها و ناظرین»، خروج از قدرت سلسله مراتبی و شکل گیری سطح

[8] Good Governance
[9] Globalization

افقی قدرت فراهم می‌شود) و به زودی ظهور وب ۴[10] بین بازه ۲۰۴۰-۲۰۲۰ (ظهور وبلاگ‌های معنایی مجهز به هوش مصنوعی، جوامع نامتمرکز، فضای بازار هوشمند و ذهن‌های بنگاهی، نسل عامل محور[11]) و قابلیت‌های نوین آنها، «ظهور فناوری‌های نوین اطلاعاتی و ارتباطی(فاوا[12])»، شکل گیری «رسانه‌های اجتماعی[13]» و افزایش سرعت گردش اطلاعات در بین شهروندان و در کل، شکل گیری «دهکدهٔ جهانی[14]» به تعبیر مک لوهان، از اهمیت مضاعفی برخوردار شده است، به گونه‌ای که دولت‌ها دیگر نمی‌توانند در سطح «واکنشگری» نسبت به موضوعات و رخدادهای روز، انتظارات و توقعات شهروندان را برآورده سازند، و به عنوان تنها مجریان و متولیان اِعمال سیاستگذاری‌ها بر مبنای «مونوپولی قدرت» به شکل تک بُعدی عمل کنند.

در طول تاریخ، ناامنی، فقر، تبعیض، فساد، تخریب محیط زیست و استفاده نادرست از منابع (اعم از انسانی و طبیعی) و... از جمله دغدغه‌هایی بوده است که همواره جوامع انسانی را تهدید کرده است، اما چگونگی چیرگی بر این موانع و برون رفت از شرایط بحرانی و تهدیدهای ملی در شرایط کنونی، در طیفی از بازیگران و کارگزاران و نظام‌ها و بلوک‌های مختلف در نوسان است، به گونه‌ای که برخی از پژوهشگران تأکید بیش از حد بر «دولت» و «بازیگران دولتی» (مداخلهٔ دولتی) دارند، در حالی که گروهی دیگر، بخش خصوصی و جامعهٔ مدنی را در اولویت قرار داده‌اند. از این رو یکی از مباحث مهم و در عین حال جدید که از دههٔ ۱۹۸۰ به بعد در «ادبیات توسعه»، بالاخص کشورهای در حال توسعه، مورد توجه قرار گرفت، مفهوم «حکمرانی خوب» در راستای استقرار و نهادینه سازی «جامعهٔ مدنی[15]» و چگونگی «**مشارکت**» بخش‌های مختلف به شکل متوازن، هم زمان و متعادل در راستای برون رفت از شرایط بحرانی و مهمتر از آن، استقرار، تحقق و «روندسازی» از «فرایند توسعهٔ پایدار[16]» بوده است: دولت‌ها باید با بسترسازی مناسب، قابلیت مشارکت شهروندان و ذینفعان در «موضوعات عمومی» را فراهم کنند، چرا که «تغییر شرایط» به مدد شکل گیری «جامعهٔ شبکه‌ای[17]» به تعبیر کاستلز، «پاسخگویی جدی‌تر به این شرایط جدید» را می‌طلبد. **در «حکمرانی خوب»، شراکت و ارتباط صحیح و تعاملی بین سه رکن اصلی «دولت»، «جامعهٔ مدنی» و «بخش خصوصی» در انجام فعالیت‌های مختلف وجود دارد** که زمینهٔ تحقق «حکمرانی خوب» را در ابعاد مختلف سیاسی-اجتماعی، اقتصادی، فرهنگی و زیست محیطی فراهم می‌کند. بنابراین «حکمرانی خوب» چیزی بیش از صرفاً مدیریت کارآمد منابع مالی و اقتصادی یا ارائهٔ خدمات عمومی ویژه است، حکمرانی خوب مشتمل بر یک «**راهبرد وسیع**» برای تقویت نهادهای جامعهٔ

[10] Meta Web or Smart Web
[11] Agent-Oriented
[12] ICT
[13] The Social Media
[14] Global Village
[15] Civil Society
[16] The Procedure of Sustainable Development
[17] The Network Society

مدنی است. در این راستا «بانک جهانی[۱۸]» مهمترین «شاخصه‌های حکمرانی خوب[۱۹]» را در شش حوزۀ: ۱. ارائۀ خدمات عمومی کارآمد (اثربخشی حکومتی[۲۰])، ۲. نظام قضایی قابل اعتماد (حکومت قانون[۲۱])، ۳. ریشه کنی فساد[۲۲]، ۴. حق اظهار نظر مردم و پاسخگو بودن دولت[۲۳]، ۵.ثبات سیاسی و ریشه کنی خشونت عریان[۲۴] و ۶. برابری حقوقی[۲۵] تعریف کرده است.

در این راستا این پژوهش در نظر دارد با انتخاب مدل بریتانیا به عنوان یکی از نمونه‌های موفق و پیشگام در حوزۀ حکمرانی سایبری، به بررسی دقیق‌تر این منظومه مفهومی بپردازد بر این اساس گام‌های تدوین این گزارش عبارتند از: ۱. ارائۀ خلاصه ای از مدل مذکور در حوزه و بافتار مربوطه، ۲.ارائۀ یافته های راهبردی (نشانک‌های ضعیف، پیشران‌های کششی و فشاری، شگفتی سازها، روندها و عدم قطعیت‌ها) و در کل ترسیم شِمای کلی از موضوع راهبردی در بافتار هدف و چرایی شکل گیری و «ریخت شناسی[۲۶]» از آن، ۳.ارزیابی انتقادی (شناخت فرصت‌ها و تهدیدها از موضوع مورد نظر از منظر ملی و بین‌المللی)، ۴. جمع بندی از نکات مطرح شده (امکان سنجی عملیاتی سازی یافته‌های راهبردی در سطح ملی و داخلی). چرا که «فضای مجازی» با به کارگیری فناوری‌های جدید ارتباطی و اطلاعاتی، بهبود فرایندهای ارائۀ خدمات در بخش عمومی، تسریع ارائۀ خدمات به شهروندان، پاسخگوتر ساختن دولت و سازمان‌های دولتی در برابر مردم، شفاف سازی اطلاعات، کاهش فاصله بین مردم و دولتمردان، افزایش مشارکت شهروندان و اعضای جامعۀ مدنی در فرایندهای تصمیم گیری دولتی، گسترش عدالت اجتماعی از طریق بسترسازی و خلق فرصت‌های برابر برای افراد و گروه‌های مختلف و دسترسی به اطلاعات، فشردگی زمان و مکان و کاهش هزینه‌های مادی، زمانی و انسانی ناشی از بوروکراسی گسترده و ناموزون و... امکانات گسترده‌ای را برای عینیت یافتن آرمان‌های «حکمرانی خوب » یا به تعبیر دقیقتر، «حکمرانی سایبری» فراهم می‌کند.

---

[18] World Bank
[19] http://info.worldbank.org/governance/WGI/
[20] Government Effectiveness
[21] Rule of Law
[22] Control of Corruption
[23] Voice and Accountability
[24] Political Stability and Absence of Violence/Terrorism
[25] Regulatory Quality
[26] Morphology

مدل بریتانیا

حکمرانی سایبری» از جمله موضوعات مهمی است که مورد توجه دولت بریتانیا (انگلیس، ولز، اسکاتلند و ایرلند شمالی) قرار گرفته است، به گونه‌ای که در سال ۲۰۱۸ دولت بریتانیا پیرامون تحقق شاخص‌هایی چون مسئولیت پذیری، شفافیت و پاسخگویی؛ درخواست تشکیل و شکل گیری کارگروه «کمیتهٔ مجازی[۲۷]» و «امنیت سایبری» به‌منظور شکل دادن به «چارچوب دیدبانی[۲۸]» همبستهٔ آن در ارتباط با پلتفرم‌های رسانه‌های اجتماعی و کاربران آن را ارائه داد[۲۹]. کمیتهٔ مجازی مورد نظر از متخصصان و خبرگان در حوزهٔ فنی، دانشگاهی و مردمی تشکیل شده بود. مهمترین مسئله در کمیتهٔ مجازی مزبور، تلاش برای **هماهنگ و همگام سازی بخش‌های مختلف**[۳۰] درگیر در حوزهٔ حکمرانی سایبری و شمول[۳۱] هر چه بیشتر گروه‌های ذی نفع[۳۲] در مراحل ابتدایی و مقدماتی بود.

اکنون سیاست گذاران و متخصصان «درهٔ سیلیکون[۳۳]»[۳۴] در شرایط پیچیدهٔ بین «آزادی بیان» و «نحوهٔ قانونگذاری» و محدودیت سازی قرار گرفته‌اند، شرایطی که فقط محدود به بریتانیا نیست، بلکه به عنوان یک معضل جهانی مطرح شده و حتی بحث «قانونگذاری جهانی اینترنت[۳۵]» را به‌منظور کاهش جرائم سازمان یافته، مبارزه با خشونت، تروریسم، پورنوگرافی، کلاهبرداری‌های اینترنتی و...مطرح ساخته است[۳۶]. با این وجود اعضای کمیتهٔ مجازی برای عبور از این شرایط؛ تصمیم گرفتند تمرکز خود را بر روی «مجراها و گذرگاه‌های قانونی» قرار دهند که در حیطهٔ کنترل آنها قرار داشت: یعنی شکل دادن به یک چرخهٔ ایجابی از پاسخگویی سازمانی، چگونگی تحقق شفافیت دولتی و سازمانی با اتکا به بخش خصوصی، و در نتیجه تحقق «مسئولیت پذیری دیجیتالی» که خود منجر به شکل گیری حلقه‌ای از سیاست گذاران، پژوهشگران آکادمیک و دانشگاهی و شرکت‌ها و بنگاه‌های خصوصی فعال در این حوزه شد. این حلقه معتقد بود ارتقای مجراها و ترمینال‌های دیجیتالی که در حوزهٔ کنترل دولت قرار دارد در ارتباط با: ۱. افزایش ارتباط و تعامل بین دولت و شهروندان،۲. ارتقای خدمات عمومی آنلاین، ۳. افزایش مشارکت

---

[27] Internet Commission
[28] Duty of Care
[29] https://blogs.lse.ac.uk/medialse/2018/08/23/the-essential-elements-of-the-new-internet-governance-diversity-optimism-and-independence/
[30] Coordination among Government Bodies and involved Institutions
[31] Inclusion
[32] Stakeholders
[33] Silicon Valley
[34] درهٔ سیلیکون، نام رایج و غیر رسمی منطقه ای در ۷۰ کیلومتری جنوب شرقی سانفراسیسکو است که در حومهٔ سنتاکلارا، کالیفرنیا، ایالات متحدهٔ آمریکا قرار گرفته و شهرت آن به دلیل قرار داشتن بسیاری از شرکت های مطرح انفورماتیک جهان در این منطقه است. نمادی از وجود کمپانی های فعال در زمینه فناوری های پیشرفته
[35] Global Internet Regulation
[36] https://www.osce.org/files/f/documents/2/a/13844.pdf

شهروندی،۴.کاهش فساد سیستماتیک سازمانی و دولتی، ۵.ارتقای دسترس پذیر بودن اطلاعات، ۶.کاهش هزینه‌های عمومی،۷.کاهش زمان پاسخگویی به مطالبات و انتظارات شهروندان و ارتقای کیفیت خدمات عمومی و در کل، تحقق شاخص‌های حکمرانی خوب از منظر سایبری مؤثر خواهد بود.

آنچه شکل گیری این حلقه را ضروری ساخت، وجود پلتفرم‌ها و رسانه‌ها و شبکه‌های اجتماعی غیرقابل کنترلی بود که حتی با وجود تلاش بسیار، محدودیت و قانونگذاری در آنها را محدود و سخت ساخته است، (قانون گذاری و نظارت بر رسانه‌ها در بریتانیا بر عهدهٔ سازمان آفکام [۳۷] است، اما در ارتباط با رسانه‌ها و شبکه‌های اجتماعی و دارک وب، این سازمان از محدودیت‌های ساختاری، فنی و انسانی زیادی برخوردار است). بنابراین سیاست گذاران و متخصصان و پژوهشگران دانشگاهی تصمیم گرفتند به جای تمرکز روی یک سیستم «رِپکس[۳۸]: پیچیده و پویا» با رفتارهای غیرقابل پیش بینی، تمرکز و قدرت خود را بر روی بخش‌هایی قرار دهند که بر آنها قدرت و کنترل اعمال نفوذ دارند. به تعبیر دقیق‌تر، افزایش توان و ارتقای پاسخگویی، مسئولیت پذیری و شفافیت دیجیتالی بخش‌های دولتی و سازمان‌های وابستهٔ آنها، مسلماً تأثیرات و پیامدهای مثبتی هم بر روی پلتفرم‌ها و شبکه‌های اجتماعی خارج از کنترل آنها اِعمال می‌کرد و از هرج و مرج و اغتشاشات احتمالی ناشی از بسیج شبکه‌های اجتماعی کاسته می‌شد.

مهمترین بخش در این قسمت و در ارتباط با کارگروه «کمیتهٔ مجازی»، درخواست برای مشارکت کارگزاران، فعالان و ذی نفعان فعال جامعهٔ مدنی[۳۹] در این کارگروه بود تا گزارش نهایی درخواست‌ها، انتظارات و مطالبات جامعهٔ مدنی را هم پوشش داده باشد. گزارش کارگروه مجازی در سه حوزهٔ مهم: ۱. چالش های کلیدی[۴۰]، موانع و تنگناها،۲. مباحث و موضوعات کلیدی مورد انتظار[۴۱]، ۳. بروندادهای نهایی بر مبنای توافقات انجام شده[۴۲] به‌منظور تحقق «حکمرانی سایبری»، همراه با همکاری با «کارگروه حقوقی اینترنت» پیرامون «الزامات قانونی و حقوقی[۴۳]» به‌منظور حفظ الزامات «حق آزادی بیان» همراه با کدگذاری و مفهوم سازی از «محتوای مجازی غیرقانونی و زیان بار» در ارتباط با مواجهه با محتوای خشونت بار، تهدید و ارعاب، تضعیف روحیهٔ اجتماعی و خشونت محتوای تولیدی در فضای مجازی و رسانه‌های اجتماعی نظیر گروه‌های مافیایی و کارتل‌های مواد مخدر، گروه‌های قاچاق اعضای بدن انسان، مبارزه با فحشا و پورنوگرافی و گروه‌های تروریستی[۴۴] و...خاتمه پیدا کرد.

---

[37] https://www.ofcom.org.uk/home
[38] REPLEX: Rapid and Complex
[39] Civil Society Stakeholders
[40] Key Challenges
[41] Areas of Debate
[42] Areas of Agreement
[43] Statutory Requirements
[44] https://blogs.lse.ac.uk/medialse/2018/05/24/a-more-transparent-and-accountable-internet-heres-how/

اما مهمترین دستاور «حقوقی» این جلسه که مورد توافق گروه‌های مختلف قرار گرفت، به‌منظور حفظ منشور حقوق بشر و تعادل دو طرف «دولتی و سازمانی» و «جامعهٔ مدنی»، شکل گیری دادآورهای[۴۵] مختلف وابسته به بخش خصوصی (خارج از پیکره و بدنهٔ دولتی و جامعهٔ مدنی) به‌مثابه ناظر بی‌طرف[۴۶] در پیگیری تخلفات، نقض حقوق و شکایات دو طرف (دولت و جامعهٔ مدنی پیرامون ارتکاب جرائم احتمالی نسبت به یکدیگر) بود.

کمیتهٔ مجازی تأکید داشت که «حکمرانی سایبری» به عنوان شیوه‌ای از «فهم هوشمند در حکمرانی[۴۷]» به‌منظور شناسایی «ناشناخته‌ها» (پدیده‌های سرکوب شده و مغفول مانده در سطح انتظارات و توقعات جامعه)؛ تنها در پرتو تنوع (شمول هر چه بیشتر گروه‌های مختلف سیاسی، اجتماعی، فرهنگی، اقتصادی، مذهبی، نژادی، دینی، سنی و جنسیتی و..) و حفظ و محترم شمردن حریم خصوصی کاربران، فراهم سازی زیرساختارسازی‌های فنی مناسب و استقلال «حکمرانی سایبری» بر مبنای تعادل، موازنه و همکاری بخش‌های مختلف (مدنی، دولتی و خصوصی) (نه وابستگی دولتی و جناحی) محقق می‌شود.

از جمله دیگر موارد مهم مورد بحث در این کمیته، ملزم سازی دولت و ارگان‌های دولتی به ارائهٔ گزارش‌های سه ماهه پیرامون عملکرد خود در ارتباط با «حکمرانی سایبری» و میزان پاسخگویی آنها به مطالبات شهروندان و نیز؛ نحوهٔ تأمین «امنیت سایبری[۴۸]» بود.

از آنجایی که تحقق «حکمرانی سایبری» طیف گسترده‌ای از موضوعات ساختاری، آموزشی، فنی، محتوایی، حقوقی و...را در بر می‌گیرد، لزوم تشکیل کارگروه‌های مختلف در هر حوزه با تأکید بر استفاده از «مدل هوش مصنوعی[۴۹] مبتنی بر وب ۳ و وب ۴» و متخصصان و پیشگامان این حوزه مورد بحث قرار گرفت.

همچنین لزوم ارتقای «سواد رسانه‌ای» و کاهش «شکاف دیجیتال»، به عنوان نحوه‌ای از «خود قانونمندی شهروندی» مورد بحث قرار گرفت. جایی که شهروندان با برخورداری از «سواد رسانه‌ای مناسب» و دیدگاه انتقادی، از قدرت تجزیه و تحلیل پیام‌های ارسالی برخوردار بوده و نیز، با آگاهی از عواقب منفی حقوقی،

---

[۴۵] مقصود از «آمبودزمان» «Ombudsman»، یا «**دادآور**»، با تلفظ اصلی «اُمبودس مان»، واژه ای سوئدی است که در اصل به معنای نماینده است و ریشه در سنت های اسکاندیناوی دارد. آمبودزمان، به فرد یا دفتر غیرجانبداری گفته می شود که وظیفه دارد به عنوان نماینده عموم مردم، موارد نقض حقوق افراد توسط دولت یا نهادها و شرکت های مختلف را بررسی و بازرسی کند. این وظیفه معمولا توسط دولت یا پارلمان به آمبودزمان محول می شود و به وی استقلال عمل زیادی اعطا می شود. هدف از تشکیل دفاتر آمبودزمان، حمایت از افراد در مقابل سوء جریانات اداری است، به عبارتی آمبودزمان یک نوع ضمانت اجرایی «غیرقضایی» برای نظارت بر حسن جران قانون در کشور و دستگاه دولت و حمایت از حقوق و آزادی هاست. ویژگی ان نوع رسیدگی غیرقضایی، عدم تشریفات و افزایش سرعت عمل در رسیدگی به شکایات است. در ایران «سازمان بررسی کل کشور»، به عنوان نهاد آمبودزمان عمل می کند

[46] Indifferent Witness

[47] Intellectual Understanding in Cyber Governance

[48] Cyber Security

[49] Artificial Intelligence

انسانی و اخلاقی ناشی از ارسال و یا مشارکت در جرائم سایبری، میزان مشارکت آنها در این نوع جرائم کاهش پیدا می‌کند. این مسئله اهمیت «آموزش و پرورش سایبری» در مقاطع مختلف تحصیلی و اجتماعی را گوشزد می‌کند.

همزمان با تشکیل «کمیته‌های مجازی»، کمیته‌های دیگری نیز در راستای بررسی و تحلیل محتوایی و فنی حکمرانی سایبری در بریتانیا بر مبنای نظارت سازمان فرهنگ، رسانه و ورزش[۵۰] تشکیل شده است[۵۱] که بر رفع موانع ساختاری و فنی (تکنولوژیکی، افزایش پهنای باند[۵۲] و سرعت اینترنت، جلوگیری و کاهش «حاشیه نشینی الکترونیکی»)، فرهنگ سازی و آموزش به‌منظور ارائهٔ «مدلی یکپارچه[۵۳]» با توجه به مسائل اقتصادی، فرهنگی و زیست محیطی اختصاص داده شد. از منظر اقتصادی، تمرکز این مدل بر چگونگی ارتقای فضای کسب و کارهای مجازی با هدف افزایش «تولید ناخالص ملی[۵۴]»، از منظر اجتماعی توجه به ریشه کن سازی موانع مربوط به «شکاف دیجیتالی» و ارتقای «سواد رسانه‌ای»، و از منظر زیست محیطی؛ تمرکز بر کاهش آلودگی های محیط زیستی ناشی از رفت و آمدهای روزانه و استفاده از وسایل حمل و نقل فردی و عمومی، صرفه جویی در انرژی (در دنیای جدید، قدرت در حوزهٔ انرژی و صرفه جویی در آن و کاهش آلودگی های ناشی از سوخت‌های فسیلی به منظور تحقق شاخص‌های «توسعهٔ پایدار[۵۵]» است) و... بود.

همچنین، دولت بریتانیا به‌منظور ارتقای «حکمرانی سایبری» خود در حوزه‌های مختلف و به روز رسانی اطلاعات موجود در این حوزه در کشورهای دیگر (محتوایی، فنی و تکنولوژیکی، زیرساختاری، ساختاری و...) و شناسایی مزیت‌های رقابتی نسبی و نقاط ضعف کشورهای دیگر (و شرکت‌های فعال در این حوزه‌ها)، اقدام به تشکیل ارگان و کارگروه ویژه و جداگانه‌ای پیرامون مستند سازی و جمع آوری اطلاعات مرتبط با کشورهای دیگر در حوزهٔ حکمرانی سایبری با عنوان «**مرکز امنیت سایبری ملی[۵۶]**» نموده است[۵۷] با این شعار که: «داده، نفتِ جدید است[۵۸]». این مرکز علاوه بر نظارت امنیت سایبری ملی و داخلی، وظیفهٔ پویش و دیدبانی از دیگر مراکز سایبری دنیا را بر عهده دارد. این مسئله، اهمیت فناوری‌های نوظهور در سال‌های

[50] the Department for Culture, Media & Sport
[51] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/257006/UK_Broadband_Impact_Study_-_Impact_Report_-_Nov_2013_-_Final.pdf
[52] UK's broadband infrastructure: Broadband Delivery UK (BDUK)
[53] Integrated Model
[54] GDP: Gross Domestic Production
[55] Sustainable Development
[56] The National Cyber Security Centre (NCSC)
[57] https://royalsociety.org/-/media/policy/projects/data-governance/uk-data-governance-explainer.pdf
[58] Data is the new Oil

آتی و تغییر و استحالهٔ شکل قدرت از حالت فیزیکی و سخت افزاری به «قدرت نرم و الکترونیک» را نشان می‌دهد.

وزارت دفاع سایبری بریتانیا، اقدام به انتشار سند چشم اندازی[۵۹] کرده است که در آن اهداف راهبردی خود را در چهار حوزهٔ کلان تعریف و مشخص نموده است: ۱. بریتانیا در مقابله با جرائم سایبری (اعم از فردی یا سازمان سافتهٔ ملی و بین‌المللی) باید به یکی از امن‌ترین نقاط دنیا تبدیل شود تا امنیت کسب و کارها و حوزهٔ اقتصادی، سیاسی-اجتماعی و فرهنگی و زیست محیطی بریتانیا تأمین شود. در تحقق این چشم انداز، ما نیازمند تشکیل کارگروههای تخصصی، فنی و همکاری بیناسازمانی وزارت دفاع سایبری با مراکز دانشگاهی، پژوهشکده ها، شرکت های مطرح خصوصی در این راستا هستیم تا تهدیدهای سایبری، خصوصا ناشی از تروریسم بین المللی را کاهش دهیم. ۲. بریتانیا باید از «تاب آوری بالای حملات سایبری[۶۰]» برخوردار باشد، این مهم نیازمند شناسایی و آینده پژوهی و آینده نگاری از انواع تهدیدات ممکن و احتمالی و غیر قابل پیش بینی در آینده هستند که می‌توانند موجودیت بریتانیا در حوزه‌های مختلف را دچار چالش کنند، ۳. بریتانیا باید در تأسیس یک محیط امن، با ثبات و پیشرفتهٔ سایبری، از جمله پیشگامان در این حوزه باشد تا بتواند از کسب وکارها و شرکت‌های اقتصادی بزرگ خود در برابر انواع تهدیدات مختلف، و مهمتر از همه محرمانگی اطلاعات طبقه بندی شدهٔ سازمانی محافظت کند، ۴.بریتانیا باید در شکلی مداوم و مستمر به شناسایی تهدیدها و فرصت‌های موجود در حوزهٔ تهدیدات سایبری پرداخته و نیروی انسانی متخصصی را در این حوزه تربیت کند که در آینده بتوانند به‌عنوان متخصصان و محافظان فضای سایبری پیشرفته در رویارویی و خنثی سازی تمامی تهدیدات سایبری آماده باشند، این مسئله نیازمند سرمایه گذاری بر روی منابع و سرمایه‌های انسانی دانشگاهی در شکل **پروژه‌های هدفمند سازمانی** است (بریتانیا برای تحقق چهار هدف فوق، بودجه‌ای در حدود ۶۵۰ میلیون پوند اختصاص داده است). این موضوع در **«سند چشم انداز دفاع سایبری بریتانیا»** ۲۰۳۰-۲۰۲۲[۶۱]، با هدف «تدوین سند راهبردی دفاع سایبری ملی»، «تمرکز بر توانمندسازی زیرساخت‌های دفاعی سایبری سازمانی»، «ایجاد و شناسایی مهارت‌های جدید دفاع سایبری»، «شناسایی تهدیدهای نوظهور سایبری (به دلیل تکامل آنها)»، «ارتقای فرهنگ دفاع سایبری و آموزش دفاع سایبری در عصر جدید به شهروندان در مواجهه با باج افزارها[۶۲]» نیز مطرح شده است.

59 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
60 Cyber Attacks Resilience
61 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf
62 Ransomware

مؤلفه‌های راهبردی

روندها

«**روندها**»، شرایط معمول و حاکم بر وضعیت موجود هستند که با سرعت متوسط شروع می‌شوند اما بعد از مدتی و در صورت بروز شرایط خاصی (درونی و ملی یا بیرونی و خارجی) شتاب می‌گیرند. زمانی که پتانسیلِ «روند» مصرف شود، به سرعت کند یا به رکود مبدل می‌شود. روندهای حاکم بر تحقق «حکمرانی سایبری» در نقطهٔ آغازین خود و با توجه به افزایش ضریب نفوذ کاربری اینترنت و فضای مجازی در زندگی روزانهٔ شهروندان بریتانیا حاکی از شکل گیری مراحل زیر است:

۱. شکل دادن به کارگروه‌های «کمیتهٔ مجازی» در راستای هم افزایی هماهنگ و همگام سازی گروه‌های مختلف و ذینفعان درگیر در حوزه‌های مختلف دولتی، مدنی و خصوصی
۲. تشکیل کارگروه‌های حقوقی به‌منظور تدوین قوانین سایبری جدید
۳. ارتقای مجراها و گذرگاه‌های دیجیتالی تحت کنترل دولت به‌منظور ارتقا و تحقق شاخص‌های حکمرانی سایبری
۴. شکل گیری آمبودزمان‌های مختلف به عنوان ناظران بی‌طرف مبتنی بر بخش خصوصی به‌منظور صیانت از حقوق گروه‌های مختلف شرکت کننده در حکمرانی سایبری
۵. ارتقای زیر ساخت‌های فنی مورد نیاز در همکاری با شرکت‌های برجسته، بخش خصوصی و پژوهشکده‌ها و مراکز دانشگاهی (اشتغال زایی و تربیت نیرو و سرمایهٔ انسانی مورد نیاز در این حوزه به شکل هدفمند)
۶. توجه به ظهور وب ۳ و وب ۴ و استلزامات فنی، حقوقی و پیامدهای اجتماعی-سیاسی، فرهنگی و اقتصادی ناشی از آنها
۷. کاهش شکاف دیجیتالی و حاشیه نشینی الکترونیکی ناشی از آن و ارتقای سطح سواد رسانه‌ای
۸. تأسیس مرکز امنیت سایبری
۹. تدوین سند چشم انداز امنیت سایبری ۲۰۴۰-۲۰۲۲
۱۰. معرفی تهدیدهای نوظهور در حوزهٔ امنیت سایبری
۱۱. افزایش ضریب نفوذ رسانه‌های اجتماعی و فضای مجازی در زندگی روزانهٔ شهروندان بریتانیا
۱۲. شکل گیری و تقویت دولت الکترونیک در راستای پاسخگویی به انتظارات و درخواست‌های شهروندان
۱۳. شکل گیری و افزایش جرائم و تهدیدات سایبری

عدم قطعیت‌ها

عناصری که بر آنها کنترلی نداریم اما به دلیل تأثیرگذاری آنها در شکل عمیق و چند لایه، قابل چشم پوشی نیستند. بر مبنای اسناد «تحقق حکمرانی سایبری» در بریتانیا، عدم قطعیت‌هایی که مورد توجه دولت بریتانیا قرار گرفته‌اند، عبارتند از:

۱. شکل گیری تهدیدات سایبری نوپدید
۲. جرائم سایبری سازمان یافته و حتی تروریستی نوظهور
۳. ظهور فناوری‌های نوین ارتباطی و اطلاعاتی و تغییر شکل قدرت و نوع ارتباطات اجتماعی و ساختارهای سیاسی-اجتماعی، اقتصادی، فرهنگی و زیست محیطی ناشی از ظهور تکنولوژی‌های نوین ارتباطی و اطلاعاتی است.
۴. دستیابی دیگر کشورها (خصوصا آمریکا، چین، روسیه و...) به فناوری‌ها و فناوری‌های نوین ارتباطی و اطلاعاتی و تقویت زیرساخت‌های فنی این کشورها
۵. ورود هند، ژاپن، کره جنوبی به جمع بازیگران کلیدی در حوزهٔ فناوری‌های نوین ارتباطی و اطلاعاتی و بسترسازی فنی و فراهم سازی زیرساخت‌های مناسب در راستای استفادهٔ هر چه بیشتر از فضای مجازی

مهمترین موضوع در ارتباط با «عدم قطعیت‌ها»، تنها شناسایی آنها نیست، بلکه از «عدم قطعیت‌ها» می‌توان در راستای فلج سازی کشورها و گروه‌های رقیب به‌منظور سردرگمی و یا افزایش وابستگی آنها و به نوعی کنترل آنها به نفع خود استفاده کرد. نظیر ظهور بیماری نوپدید «کووید ۱۹» که بعد از ظهور آن، کشورهای با توان بالای تولید واکسن در مواجهه با این ویروس به‌عنوان قطب‌های پیشران پزشکی، توانستند قدرت خود را بر کشورهای دیگر (از جمله ایران و عدم در اختیار گذاشتن به موقع و درست واکسن های مورد نیاز) به منصهٔ ظهور برسانند. ارتقای زیرساخت‌های فنی و تلاش برای دستیابی به فناوری‌های نوپدید ارتباطی و اطلاعاتی در عصر جدید، از جمله «عدم قطعیت‌های بازدارنده‌ای» است که می‌تواند به‌عنوان یک کارت کلیدی در صحنهٔ قدرت بین‌المللی به‌عنوان «قدرت هوشمند سایبری» مورد استفاده (یا در مواقع لزوم و بحرانی، به عنوان اهرم فشار، مورد سوء استفاده) قرار بگیرد.

نشانک‌های ضعیف تغییر

یک ناهنجاری در تحول شناخته شده است. مشاهده‌ای است که ما را به نحوی شگفت زده می‌کند. چیزی است که نمی‌توانیم به راحتی با هر روند و یا پدیده شناخته شده‌ای پیوند دهیم. ما تمایل داریم چیزهایی که خارج از دامنهٔ تجربه و تخصص خودمان هست را «نشانک های ضعیف» قلمداد کنیم. اما در واقع نشانک‌های ضعیف، ساخت و سازی کاملاً ذهنی دارند. یعنی، «تغییراتِ در حال ظهوری» هستند که هنوز بُرد، تأثیرگذاری و میدان نیروی آنها در حوزهٔ بردارهای قدرت موجود به شکل قطعی مشخص نشده است. البته نشانک‌های ضعیف نباید با «نشانک‌های قوی»که چیزهای کاملاً شناخته شده هستند، اشتباه گرفته شوند. به‌علاوه، نشانک-های ضعیف، با «روندها»، «پیشران‌ها» و «شگفتی سازها» متفاوتند. نشانک‌های ضعیف، در بسیاری از لایه‌ها وجود دارند، نشانک‌هایی از چیزی که احتمالاً می‌توانند شروع به تأثیر بر چیز دیگری کنند که آن چیز به نوبهٔ خود، اثر قابل توجهی بر بخش‌هایی دیگر خواهد داشت. از این رو نشانک‌های ضعیف ساده‌تر هستند، انواع چیزهای خلاف قاعده هستند که می‌توانند در صورت بسترسازی لازم منجر به «تغییرات بزرگ» در سطح کلان سیستمی شوند. بر مبنای اسناد منتشر شده توسط دولت بریتانیا در حوزهٔ تلاش برای «تحقق حکمرانی سایبری»، آنچه مشخص است، نشانک‌های ضعیف حاکی از تغییرات سریع و ناگهانی با ظهور فناوری‌های نوین ارتباطی و اطلاعاتی و عدم آمادگی لازم دولت در مواجهه با جرائم و تهدیدات سایبری همبستهٔ آنها هستند و گروه «برنده» در این میان، گروهی است که در حالت انفعالی با راهبردهای تدافعی قرار نگیرد، بلکه با ابزارهای پیش دستانه و به شکل فعال و کنشگرانه و استفاده از راهبردهای تهاجمی، بتواند قاعدهٔ زمین بازی را به نفع خود تغییر دهد. این مهم، لزوم سرمایه گذاری بر پژوهشکده‌ها، مراکز دانشگاهی و علمی، شرکت‌های دانش بنیان و بخش خصوصی را به‌منظور فراهم سازی زیرساخت‌های فناورانه و فنی مورد نیاز و تربیت نیروی انسانی متخصص مورد نیاز در این حوزه را گوشزد می‌کند. متأسفانه در حال حاضر برنامه‌های دانشگاهی در ایران در شکلی گسیخته، نامتمرکز و غیر هدفمند و بدون توجه به نیازهای بازار قرار دارند که خود منجر به شکل گیری یک گسست عمیق بین بخش نظری و دانشگاهی با واقعیت‌ها و مسائل روز جامعهٔ ایران شده است. به‌علاوه، بخش‌های دولتی و ارگان‌ها و سازمان‌های دولتی مربوطه هم تلاش نمی‌کنند پروژه‌های مرتبط با زیرساخت-های فنی در ارتباط با تحقق حکمرانی سایبری خود را در شکل برون سپاری به اندیشکده‌ها و مراکز دانشگاهی بر مبنای یک سند چشم انداز هدفمند، مدون و مشخص (سند راهبردی با اهداف مشخص و کاربردی، نه سوگیری‌ها و تخیلات غیر واقع گرایانه) تنظیم کنند. شاید چرایی این امر را باید در عدم همگام سازی و هماهنگی بخش‌های مختلف دولتی، خصوصی، مدنی، عدم استفاده از مراکز دانشگاهی و فراموش کردن رسالت واقعی آن، و نیزتلاش نیروی انسانی ناکارآمد در بخش‌های بوروکراسی عظیم دولت و... جستجو کرد.

شگفتی سازها

ایده نوعی «رویداد ناگهانی و غیر منتظره»، یا به بیان دیگر «ناشناختهٔ شناخته شده[۶۳]» است که تأثیری قوی بر بخش‌های بزرگی از یک جامعه دارد. به‌عنوان مثال، «پیش بینی» اینکه ترور سارایوو رخ خواهد داد و متعاقب آن جنگ جهانی اول شروع خواهد شد، و یا با خودسوزی بوعزیزی در تونس، زنجیره‌ای از انقلاب در کشورهای عربی رخ خواهد داد، هر دو از شگفتی سازهای سیاسی هستند. در ارتباط با اسناد مرتبط با تحقق «حکمرانی سایبری»، آنچه بیش از هر چیز جلب توجه می‌کند، تلاش به‌منظور گردآوری داده‌ها و اطلاعات فنی از کشورهای دیگر و ارزیابی «**میزان توان پاسخگویی آنها به تهدیدات سایبری**»، و مهم‌تر از همه، معماری «**چگونگی تهدید کشورهای دیگر در حوزهٔ امنیت سایبری**» به‌منظور نفوذ و جمع آوری اطلاعات محرمانه و طبقه بندی شدهٔ کشورهای دیگر است. به شکل همزمان، از جمله شگفتی سازهای محتمل می‌توان به این نکته اشاره کرد که بریتانیا تلاش دارد همانند برخی شرکت‌های کامپیوتری که خود اقدام به ساخت ویروس‌های مخرب کرده و سپس آنتی ویروس آن را در بازار تولید و پخش می‌کنند، اقدام به شناسایی تهدیدات و جرائم سایبری نوظهور و چگونگی مواجهه و بازدارندگی آنها نماید (همانند گروه تروریستی داعش که ساخته و پرداخته غرب بود) . مسلماً در مواجهه با جرائم و تهدیدات سایبری نوظهور، برگ برنده با کسی است که از قبل اشراف و آگاهی لازم را برای مواجهه با این تهدیدات و جرائم داشته و به شکل پیش دستانه با آنها روبرو می‌شود. همچنین «لندن» به‌عنوان یکی از شهرهای جهانی مهم[۶۴] و از جمله قطب‌های اقتصادی مطرح دنیا، می‌تواند از این کارت‌های برنده در راستای تضعیف توان دیجیتالی دیگر شهرهای جهانی نظیر پاریس و..استفاده کند و خود را در صدر جدول حفظ امنیت و ارتقای سهام شرکت‌های اقتصادی و محیط کسب و کار دیجیتالی قرار دهد.

پیشران‌ها

«**پیشران**» یا «**نیروی محرک**»، عاملی است که «**تغییر**» را به جلو می‌راند. دو نوع اساسی از پیشران‌ها وجود دارند: **۱.پیشران های کششی** و **۲. پیشران های فشاری**. پیشران‌های کششی به «تقاضای سطح صفر وسیع» برای چیزی اشاره دارد (سلبی: آنچه وجود ندارد و همه خواهان آن هستند)، به‌عنوان مثال «بی‌اعتمادی عمیق عمومی به سیستم‌های سیاسی در کشورهای عربی»، چیزی است که از آن به «پیشران‌های کششی» یاد می‌شود: جاذب و پوشش دهندهٔ سطح وسیعی از خواسته‌ها و انتظارات محقق نشدهٔ مردمی. در حالی که پیشران‌های فشاری عموماً «پیشنهادی» هستند (ایجابی: آنچه به‌عنوان راه حلی برای برون رفت از وضعیتِ

[۶۳] به عنوان مثال، چیزهایی که ما می دانیم اتفاق خواهد افتاد نظیر به اوج رسیدن قیمت نفت، فورانوزوویو، زلزله بزرگ بعدی کالیفرنیا و...هر چند ممکن است دقیقا ندانیم چه زمانی این وقایع رخ خواهند داد، اینها اثر یک شگفتی ساز را دارند

[64] Global Cities

بحرانی موجود با توجه به امکان سنجی از شرایط موجود صورت می‌گیرد). به تعبیر دقیق‌تر «پیشران‌های فشاری»، عبارتند از آنچه از نظر سیاسی، اجتماعی، اقتصادی و فنی از نظر ایجابی برای برون رفت از شرایط بحرانی موجود به‌عنوان راه حل مسئله، «مورد نیاز» هستند. از نظر تحقق شاخص‌های «حکمرانی سایبری» در بریتانیا، از منظر پیشران‌های کششی، نبود هماهنگی و همگام سازی بین بخش‌های مختلف دولتی، خصوصی و مدنی، عدم توازن و سهم بخشی بین این قسمت‌ها، سواد رسانه‌ای پایین، شکاف دیجیتالی در مناطق محروم، عدم فرهنگ سازی سایبری بالاخص در مواجهه با تهدیدات و جرائم سایبری در سطح خرد و کلان، عدم آمادگی لازم برای ظهور فناوری‌های اطلاعاتی و ارتباطی نوین از جمله پیشران‌های کششی هستند که در صورت تداوم وضعیت موجود، می‌توانند تحقق حکمرانی سایبری و کارکرد دولت الکترونیک را با مخاطرات فراوانی رو برو کنند. از منظر پیشران‌های فشاری، تربیت نیرو و سرمایهٔ انسانی مورد نیاز و متخصص در حوزه‌های مختلف بالاخص تهدیدات و جرائم سایبری نوظهور، سرمایه گذاری‌های کلان در بخش شناخت فرصت‌ها و تهدیدهای ناشی از ظهور و بروز فناوری‌های اطلاعاتی و ارتباطی نوین، برگزاری کمیته‌های مجازی و کارگروه‌های تخصصی خصوصاً در حوزهٔ تدوین منشور و سند حقوقی مرتبط با فضای مجازی، شکل دهی به آمبودزمان‌های مختلف متکی بر بخش خصوصی به‌عنوان میانجی بین بخش‌ها و ارگان‌های دولتی و جامعهٔ مدنی، شناسایی گروه‌های خطر (گروه‌های تروریستی ملی و بین‌المللی، مقابله با نفوذ آنها، کارتل‌های مواد مخدر، قاچاق اعضای بدن انسان و...)، شناسایی و خلق فناوری‌ها و زیرساخت‌های فنی مورد نیاز در آینده در راستای اهداف سند چشم انداز سازمان دفاع سایبری، همگام سازی و همگرایی بخش‌های دانشگاهی، خصوصی، شرکت‌های فعال در حوزهٔ فناوری‌های اطلاعاتی و ارتباطی به‌منظور بستر سازی و تحقق شاخص‌های حکمرانی سایبری و در مجموع، تلاش برای شناسایی انتظارات، توقعات و نیازهای گروه‌های مختلف جامعه و پاسخگویی به آنها، انتشار گزارش عملکرد دولت از منظر حکمرانی سایبری به شکل مرتب به‌منظور افزایش شفافیت، پاسخگویی، اثربخشی و حکمرانی قانون و مبارزه با فساد و...همگی از جمله پیشران‌های فشاری هستند که دولت را موظف به سرمایه گذاری‌های کلان در این حوزه به‌منظور تبدیل شدن به یکی از پیشگامان در حوزهٔ استفاده از فناوری‌های نوین ارتباطی و اطلاعاتی با توجه به افزایش ضریب نفوذ اینترنت و شبکه‌های اجتماعی در بریتانیا نموده است.

ارزیابی انتقادی

اساسی‌ترین مفهوم قابل درک از واژهٔ حکمرانی، آن است که دیگر نمی‌توان «دولت» را تنها کنشگر مستقل و دارای قدرت در جامعه (در یک زمان خاص) دانست، بلکه بخش‌های عمومی، خصوصی و جامعهٔ مدنی در پرتو «حکمرانی خوب» به شیوه‌های گوناگون به هم وابسته بوده، مرزبندی بخش‌های سه گانه «دولت، بخش

خصوصی و جامعهٔ مدنی» بر مبنای ملاحظات ناظر بر نقش «مدیریتی» کمرنگ‌تر می‌شود. اما «حکمرانی خوب»، الگویی نیست که در خلأ شکل گیرد، بلکه یکی از زیرساخت‌های مورد نیاز آن تحقق «جامعهٔ مدنی با ساختار مردم سالارانه» است. از این رو حکمرانی خوب با مباحثی همچون: کاهش مداخلهٔ دولت در تصمیمات حوزهٔ عمومی، کوچک سازی بخش عمومی، شفافیت و کارآمدی دیوان دولتی، بازار آزاد، حذف یارانه‌های غیرضروری و...مرتبط شده است. در الگوی «حکمرانی خوب»، مسئلهٔ ابعاد دولت، یعنی **«کوچک سازی» و «چابک سازی»**، نقش محوری داشته و تمرکز این الگو بر «دولت توانمند با ابعاد کوچک»، دوری از بوروکراسی، شفافیت و مقابله با فساد اداری است که در نتیجه، به افزایش حداکثر مشارکت شهروندان منجر می‌شود، چرا که فضایی را برای ورود دیگر بازیگران کلیدی در این حوزه فراهم می‌کند. توانمندسازی دولت علاوه بر کوچک سازی، از طریق شایسته سالاری، تمرکززدایی، همکاری و نظارت نهادهای مدنی و استاندارد سازی نظام‌های آماری منجر می‌شود. ظهور فناوری‌های نوین ارتباطی و اطلاعاتی و «فضای مجازی»، می‌تواند نقش مهمی در تحقق حکمرانی خوب با عنوان «حکمرانی سایبری» داشته باشد. امروزه فناوری‌های جدید اطلاعاتی و ارتباطاتی نقش مهمی در جوامع پیدا کرده‌اند. این فناوری‌ها با افزایش شفافیت در امور نهادی، سازمانی، اداری و... سبب دسترسی به اطلاعات بیشتر و شفاف تر، دستیابی به خدمات بهتر با زمان و هزینهٔ کمتر، تسهیل تعهدات دولت، توسعهٔ جوامع، افزایش بهره وری دولت، بهبود پاسخگویی و افزایش اعتماد به دولت می‌شوند. بنابراین فناوری‌های ارتباطات و اطلاعات در سه جنبه می‌توانند بر تحقق فرایند «حکمرانی خوب سایبری» مؤثر باشند:

۱. **فنی**: یعنی خودکار کردن وظایف جاری حکمرانی و در نتیجه، بهبود کارآمدی فرایندهای حکمرانی و کاهش فرایندهای بوروکراتیک زمان بر. بعلاوه، فضای مجازی و شبکه‌های اجتماعی، امکان تغییر رابطهٔ یک سویه از دولت به مردم را به رابطهٔ متقابل و تعاملی بین مردم و دولت فراهم می‌کنند و می‌توانند موجب استحکام فرایند دموکراتیک و توانمندسازی مردم برای مشارکت در تدوین سیاستگذاری‌های عمومی شوند.
۲. **پشتیبانی:** به معنی اینکه این فناوری‌ها؛ موجب تکمیل فرایندها و تلاش‌ها در جهت بهبود حکمرانی می‌شوند، اینترنت و فضای مجازی سبب افزایش **«شفافیت اطلاعات»** و **«بهبود شرایط تصمیم گیری»** می‌شوند. زیرا شفافیت و آزادی جریان اطلاعات، به شهروندان این توانایی را می‌دهد که در کنار توزیع قدرت و کثرت بازیگران سیاسی، بر نحوهٔ رفتار دولت نیز نظارت کنند. «فضای مجازی» به‌عنوان دستاورد ارتباطات جدید، موجب کاهش فاصلهٔ میان دولت‌ها و مردم شده و دولت‌ها همچون گذشته نمی‌توانند «اطلاعات» را از مردم پنهان کنند و یا آنها را دچار تحریف و دستکاری نمایند، بلکه ناچارند شفافیت بیشتری از خود نشان دهند. نتیجهٔ این امر، افزایش حق پاسخگویی نسبت به مردم، مسئولیت پذیری، شفافیت عملکرد و تصمیمات دولت، ارتقای حقوق شهروندی و...در جامعهٔ اطلاعاتی و ارتباطی

نوین است. «شفافیت»، به‌عنوان یکی از عناصر حکمرانی خوب، از آن رو اهمیت دارد که جلب اعتماد عمومی و افزایش سرمایهٔ اجتماعی بدون آن، امکان پذیر نیست. در واقع، وجود شفافیت شرط لازم برای کسب اعتماد عمومی نسبت به دستگاه حاکم و شیوهٔ ادارهٔ کشور است

۳. **نقش نوآورانه:** یعنی این فناوری‌ها موجب می‌شوند نوآوری‌های جدیدی در خدمات عمومی محقق شود و این امر به نوبهٔ خود منجر به ایجاد سازوکارها و زیرساخت‌های نوین در بهبود نحوهٔ ارائهٔ خدمات به شهروندان می‌شود.

امکان سنجی عملیاتی سازی یافته های راهبردی در سطح ملی

ایران به عنوان کشوری در حال توسعه، طی سالیان متمادی با مسائل و چالش‌های مختلفی روبرو بوده است که سبب شده در مسیر «توسعهٔ واقعی و همه جانبه» حرکت نکند، بلکه برعکس در مسیر توسعهٔ نامتوازن، ناموزون و ناپایدار قرار داشته باشد که نمونه هایی از تحقق «**حکمرانی بد**» در جامعه هست. این مهم را می‌توان از خلال برخی مستندات و بعضی فرایندهای سیاست گذاری عمومی در حوزهٔ برنامه‌های مرتبط با توسعه مشاهده کرد، برنامه‌هایی که برخی از مفاد آنها تاکنون در کوتاه مدت نیز امکان عملیاتی شدن به خود نگرفته‌اند. برای نمونه در زمینه جامعه مدنی، نباید تصور شود میان «حکومت» و «جامعهٔ مدنی» تعارض وجود دارد، بلکه باید تعامل آنها با یکدیگر درست، منطقی و مسالمت آمیز باشد، به گونه‌ای که حکومت بستر و فرصت لازم را برای گسترش و توانمندی جامعهٔ مدنی و سرمایهٔ اجتماعی فراهم کند، از خواست‌ها، انتقادات و انتظارات جامعهٔ مدنی استقبال کرده و نسبت به آنها پاسخگو باشد، زیرا حکومت‌ها تنها در پرتو نقدها و چالش‌ها از ضعف‌های خود آگاه شده و با از میان برداشتن آنها «توانمند» می‌شوند. تنها در این «فضای تعاملی» است که اعتماد، همکاری و دوسویگی درست میان دولت و جامعهٔ مدنی به حکمرانی خوب منتهی می‌شود. نهادهای مدنی با اعتماد آفرینی، به تقویت «سرمایهٔ اجتماعی» کمک می‌کنند، شبکه‌های ارتباطی متشکل از نهادهای مدنی در موضوعات مختلف اجتماعی، سیاسی، فرهنگی می‌توانند با جلب اعتماد شهروندان، خواسته-های مردمی و مطالبات آنها را به شکل سازمان یافته و منسجم مطرح کنند. شکل گیری احزاب سیاسی منبعث از پیکره و بدنهٔ اجتماعی جامعه مبتنی بر رویکرد مردمی هم به تقویت مشارکت، انسجام و همبستگی مدنی برای تحقق جامعهٔ بهتر منجر می‌شود. از سوی دیگر ظهور فناوری‌های اطلاعاتی و ارتباطی، ماهیت، مفهوم و ساختار دولت و عملکرد آن را متحول کرده، به گونه‌ای که دسترسی شهروندان به اطلاعات و ابزار بیان و در نتیجه امکان انتشار نارضایتی‌های عمومی را گسترش داده است، این مسئله به نوبهٔ خود زمینه‌های فعال‌تر شدن نقش جامعهٔ مدنی و در نتیجه کمرنگ‌تر شدن نقش دولت‌ها را فراهم آورده است. اما سئوال در باب نحوه مواجهه و تعامل با جنبش‌های اجتماعی است. دولتی که از سازوکارها و ساختارهای مناسب پاسخگویی، تغییر و اصلاح، شفافیت و...برخوردار نباشد تنها راه مقابله با جنبش ها را در استفاده از تهدید، ارعاب و خشونت

می‌داند. فهم ناصحیح از مطالبات یک جنبش، منجر به سرکوب آن به شکل خشونت‌بار شده و سرکوب یک جنبش نیز حاصلی جز «**زیرزمینی شدن و کنترل ناپذیر شدن جنبش**» ندارد، شرایطی که به طبع آن «جنبشِ زیرزمینی شده» از فناوری‌های اطلاعاتی و ارتباطی (فضای مجازی و رسانه های اجتماعی) در شکل مخرب آن (به منظور بسیج عمومی) استفاده می‌کند (شرایطی که زمینه را برای نفوذ عاملان بیگانه و گروه‌های اپوزیسیون داخلی و خارجی و گروه‌های معاند و دشمنان از منظر پدافند غیرعامل و بهره برداری از شرایط موجود، فراهم می‌کند). این مسئله هم چالش‌ها و هزینه‌های غیرقابل پیش بینی خود (شکاف بین ملت و حکومت) را در دراز مدت به همراه دارد. در این راستا شکل گیری شاخص هایی چون قانون گریزیِ مردم و مسئولان، نافرمانی‌های مدنی، مسئولیت ناپذیری، فساد اداری و بروز ناهنجاری‌هایی همچون اختلاس، عدم مدارای اخلاقی، فرهنگی و اجتماعی، سطح و آستانهٔ تحمل پایین، آسیب در بخش مشارکت، فقدان کارکرد درست و صحیح احزاب سیاسی، تأثیرگذاری اندک فعالیتِ انجمن‌ها و نهادهای مردمی، شکل گیری انحصار در برخی زمینه‌ها و... خود نمونه های بارز و مصادیقی برای حوزهٔ «**حکمرانی بد**» هستند. ضعف وفقدان شاخص‌های حکمرانی خوب موجب ظهور «**دولت شکننده**» می‌شود که با معضلات اجتماعی توسعه نایافتگی پایدار، فقر و درآمد اندک، اعمال تبعیض‌های منفی و برون گذاری برخی گروه‌ها یا اقوام یا مناطق جغرافیایی، مشروعیت پایین و ثبات سیاسی اندک، ناتوانی در اعمال اقتدار و ارائهٔ خدمات باید دست و پنجه نرم کند.

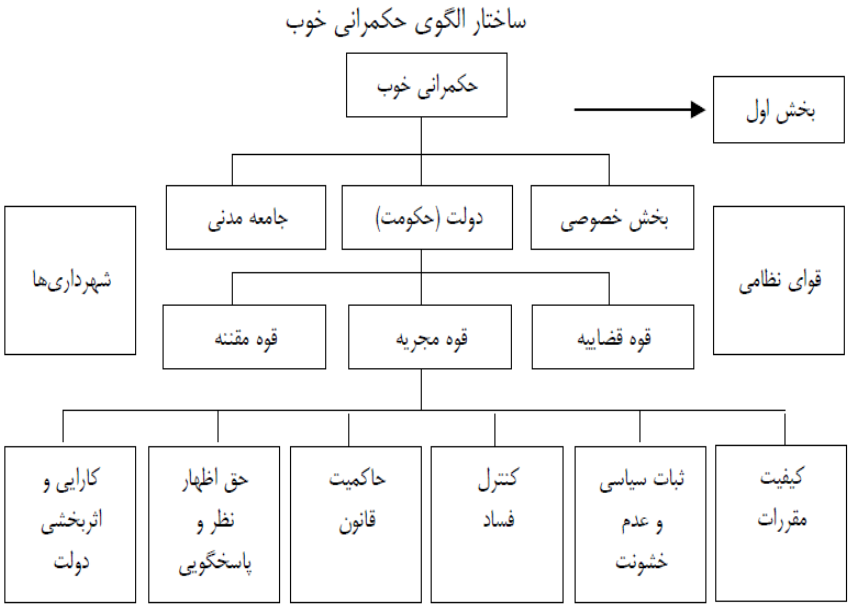
به‌طور کلی می‌توان از گفتمان‌های مختلفی در حوزهٔ «حکمرانی خوب» بر مبنای مناسبات میان دولت و جامعه نام برد و آنها را در چهار حوزهٔ مختلف و کلان دسته بندی کرد:

۱. گفتمان اول (جامعه فعال و دولت منفعل): در این گفتمان، جامعه نیرومند اما دولت کوچک است
۲. گفتمان دوم (جامعه فعال و دولت فعال): در این گفتمان هم جامعه و هم دولت نیرومند هستند
۳. گفتمان سوم (جامعه منفعل و دولت فعال): در این گفتمان، جامعه ضعیف و دولت نیرومند است
۴. گفتمان چهارم (جامعه منفعل و دولت محدود): گفتمانی که در آن هم جامعه و هم دولت به دلایل مختلف (هرج و مرج، جنگ داخلی، مشکلات اقتصادی، و...) ضعیف و کوچک هستند.

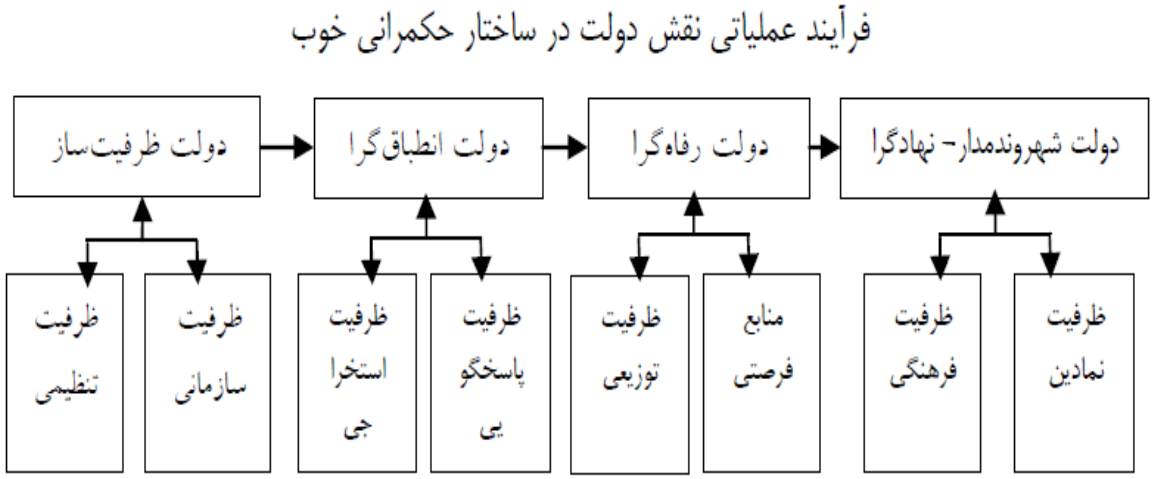
کارآمدی نظام سیاسی، به مجموعهٔ گسترده‌ای از ارزش‌های شهروندی اعم از اعتماد اجتماعی، مشارکت مدنی، شفافیت و پاسخگویی و...نیازمند است، ارزش‌هایی که «شهروندان را به زندگی روزمره و نظام حاکم سیاسی» پیوند داده و پیوندهای سیاسی-اجتماعی و وفاداریشان به نظام سیاسی و اجتماع را تقویت می‌کند. در این راستا مهمترین موانع ساختاری در تحقق حکمرانی خوب در ایران:

۱. سیاست زدگی و سوگیری‌ها (عدم تساهل، مدارا و سعهٔ صدر)

۲. ناکارآمدی در بخش‌هایی از نظام مدیریتی
۳. تفوق نظریه توطئه در برخی نگرش‌های مدیریتی
۴. موانع ساختاری و قانونی
۵. اعمال برخی استانداردهای دوگانه در حوزه اجرا
۶. تورم قانون (وجود تبصره ها و قوانین بیش از حد در حوزه های عمومی و خصوصی) و پارادوکس قانون
۷. شکل گیری الیگارشی‌های اقتصادی-سیاسی، رانت جویی و سوءاستفاده‌های اقتصادی



شکل ۱: ساختار الگوی حکمرانی خوب



شکل ۲: فرایند عملیاتی نقش دولت در ساختار حکمرانی خوب

فضای مجازی در ایران

امروزه «**فضای مجازی**» به همان اندازهٔ «زندگی واقعی افراد»، مهم و قابل تأمل است، جایی که در آن شاهد دنیایی بزرگ هستیم که فرصت‌ها، چالش‌ها، نگرانی‌های امنیتی، محدودیت‌ها و امکانات زیادی را به شکل همزمان برای کاربران خود به ارمغان آورده است. از این رو «فضای مجازی»، «**دنیایی موازی**» با تنوع فوق العاده‌ای از کاربران از هر ملیت، قوم، فرهنگ، نژاد، طبقهٔ اجتماعی، سن و جنس و... مبتنی بر خطوط ارتباطی است که با ویژگی‌هایی چون تمرکززدایی، تکه تکه بودن و مجازی بودن، فرازمانی و فرامکانی بودن، جهانی و بی مرز بودن، تعاملی و دسترسی دائم، سرعت و فراگیری بالا، امکانات متنوعی را با کمترین هزینه (ایاب و ذهاب، و در نتیجه کاهش آلودگی‌های زیست محیطی، سهولت دسترسی و...) برای کاربران خود به ارمغان آورده است. بسیاری از پژوهشگران تحقق «حکمرانی خوب» در بستر فضای مجازی را با عنوان «**حکمرانی سایبری**» مطمح نظر قرار داده‌اند: جایی که فضای مجازی با ویژگی‌های منحصربفرد ابرمتنی، ابرشبکه‌ای، کنش تعاملی، تمرکززدایی از قدرت رسانه‌های، دستیابی به «هویت مجازی» (هویت مخفی) و امکانات تخصصی می‌تواند بستری برای تحقق حکمرانی خوب باشد. **حکمرانی سایبری از چهار لایه** تشکیل شده است: **۱.زیرساخت:** که در حال حاضر تحت سلطهٔ آمریکاست، **۲.لایهٔ منطقی:** شامل بحث IP و DOMAIN می‌شود که این لایه تحت مدیریت شرکت آیکن[۶۵] است. البته آیکن بحث خودتنظیمی را نیز

[65] ICANN: Internet Corporation for Assigned Names

پذیرفته است، به این معنی که کشورهای منطقه‌ای بتوانند در این بخش سیاستگذاری‌های محدودی البته با هماهنگی آیکن داشته باشند، **۳.لایهٔ محتوا:** در لایهٔ محتوا شرکت‌های بزرگی مانند اپل و مایکروسافت و...فعال هستند، **۴.لایه اجتماع:** که خاستگاه اکثر کشورها برای خود ابرازی است، اما متأسفانه کشور ما در این لایه هنوز نتوانسته است به راهبرد مشخص ایجابی برسد. در حال حاضر به نظر می‌رسد قدرت مانور ج.ا.ا در لایهٔ زیرساخت کمتر است، اما در سه لایهٔ دیگر یعنی منطقی، محتوا و اجتماع می‌تواند فرصت خوبی برای اعمال اراده کشور و توسعهٔ حکمرانی سایبری داشته باشد. اما همین ویژگی‌های فضای مجازی، یعنی غیرملموس بودن، پویایی و تغییر دائمی، بی‌مفهوم بودن عنصر زمان و مکان، سبب شده تا تحقق حکمرانی خوب در بستر فضای مجازی همانند «شمشیر داموکلس» از تهدیدها و فرصت‌های همزمان خاص خود برخوردار باشد.از یک سو، در فضای مجازی و شبکه‌های اجتماعی، تعاملات کاربران و امکان ایجاد حلقه‌های دوستی، گروه‌های رأی دهی، **ارتباطات افقی** و غیر سلسله مراتبی فراهم می‌شود. در نتیجه «فضای مجازی» به احیای گفتگوی میان مردم و حاکمان کمک می‌کند و منجر به شکل گیری یک «حوزهٔ تعاملی عمومی» می‌شود که در این حوزه، دولت و شهروندان می‌توانند به‌صورت خصوصی دربارهٔ روش‌ها و اهداف سیاسی-اجتماعی وارد گفتگو شده و موانعی را که موجب جدایی فرد از دولت می‌شود را از میان بر می‌دارد. به علاوه «فضای مجازی» موجب می‌شود دولت‌ها زمینهٔ پاسخگویی و مسئولیت پذیری بیشتری از خود نشان دهند که در نهایت، افزایش اعتماد عمومی به نظام سیاسی و اداری و ارتقای توانمندی و کارایی اثربخشی تصمیمات و عملکرد دولت‌ها را شاهد خواهیم بود. ارتباطات الکترونیک، فرصتی برای تقویت مشارکت سیاسی و «ارتباط افقی میان شهروندان» و تضعیف نظام پدرسالارانه میان دولت-شهروندان شده است. در این میان، رسانه‌های اجتماعی به ابزاری قدرتمند در جوامع مختلف تبدیل شده‌اند که مدیریت جریان اطلاعات، تفکرات، احساسات و هیجانات را بر عهده دارند. هنگامی که فشار رسانه‌های اجتماعی قوی باشد، به دلیل کارکرد «دروازه بانی (افشاگری)، نگهبانی، دیدبانی و گزارش دهی رسانه‌های اجتماعی»، سطح شفافیت بالاتر می‌رود.

در نظریهٔ «پنجره‌های شکسته» در حوزهٔ جامعه شناسی همواره ذکر شده است که اگر یک پنجره از خانه‌ای شکسته شد، عامل شکسته شدن پنجره‌های بعدی این است که کسی مراقب خانه و پنجره‌های آن نبوده است. از منظر آسیب شناسی اجتماعی و «فساد زدایی» در حوزهٔ حکمرانی خوب، اگر رسانه‌های اجتماعی بخواهند در جلوگیری از فرایند «فساد» به‌عنوان یکی از شاخص‌های تحقق حکمرانی خوب موفق باشند، باید نخست به «اطلاعات» دسترسی داشته باشند و دوم، تحت نفوذ گروه‌های فشار نباشند. این مسئله نشان دهندهٔ این مطلب است که «رسانه‌های اجتماعی» به دلیل انتشار شواهد و اطلاعات در زمان مقتضی و مسکوت نگه داشتن هویت افشاگر، یک سکوی مشروع برای فسادزدایی، شفافیت سازی و پاسخگویی دولت‌ها و در کل، به‌عنوان ابزاری قدرتمند برای فشار آوردن به دولت‌ها به منظور حرکت به سمت رفتار و عملکرد مسئولانه

قلمداد می‌شوند. اما از سویی دیگر، پایین بودن «سواد رسانه‌ای[۶۶]» بالاخص در ایران، یکی از مسائل مهم در حوزهٔ پدافند غیرعامل است که سبب شده «فضای مجازی» و «رسانه های اجتماعی» گاه دارای «**کارکردهای ضد امنیتی**» در ایران شوند. «سواد رسانه‌ای» به مجموعه‌ای از مهارت‌های قابل یادگیری اشاره دارد که بر مبنای دیدگاهی انتقادی توانایی دسترسی، تجزیه و تحلیل، تفسیر و «راست آزمایی» محتوای ارائه شده و تولیدی در رسانه‌های اجتماعی را برای مخاطبان خود فراهم می‌کند. سواد رسانه‌ای، سبب می‌شود تا از بروز شایعات و اشاعهٔ اطلاعات نادرست، پراکنده و نامعتبر پرهیز شود. علاوه بر سواد رسانه‌ای، «**امنیت مجازی**[۶۷]» و فراهم سازی زیرساخت‌های متناسب با آن؛ از جمله مقولات مهم دیگر در حوزهٔ فضای مجازی و تحقق حکمرانی خوب محسوب می‌شود. هدف «**امنیت مجازی**»، حفظ سرمایه‌های سازمانی (نرم افزاری، سخت فزاری، اطلاعاتی و ارتباطی و نیروی انسانی) در برابر هرگونه تهدید (دسترسی غیرمجاز به اطلاعات، خطرهای ناشی از محیط و سیستم و خطرهای ایجاد شده از سوی کاربران) است و برای دستیابی به این هدف، به «برنامهٔ منسجمی» نیاز دارد که خود مشتمل بر تأمین امنیت در سه حوزهٔ: **۱.فیزیکی:** حفاظت از دستگاه‌های رایانه‌ای در مقابل خطرات محیطی (صاعقه، سیل، زلزله، بمب گذاری، حملات تروریستی، قطع کابل ارتباط شبکه و..)، سرقت (رایانه‌ها و قطعات آنها)، حفاظت از سخت افزار (دسترسی فیزیکی افراد غیرمجاز، حوادث مانند آتش سوزی و ترکیدگی لوله، دود، دما، پارازیت‌های الکتریکی، نصب تجهیزات استراق سمع و..) انجام تعمیرات قطعات در خارج از سازمان است، **۲. امنیت نیروی انسانی:** بیش از ۸ درصد مشکلات امنیتی پیش آمده ناشی از خطاهای سهوی و عمدی کارکنان بوده است، چرا که «انسان»، خدشه پذیرترین عنصر در حلقه امنیت مجازی است، نیروی انسانی که می‌تواند سبب ساز بروز اختلال در فعالیت‌های نیروی انسانی شود عبارتند از: کار زیاد، نداشتن مهارت لازم و کافی، تداخل مسئولیت‌ها، عدم اطلاع از میزان ارزش مجازی، نداشتن انگیزه، کوتاهی و بی‌مسئولیتی، فراموشکاری. بنابراین، دو مؤلفهٔ «آگاهی کاربران» و «امنیت انسانی» (عوامل تحمیلی بر نیروی انسانی) از جمله مهمترین مسائل در حوزهٔ امنیت انسانی تلقی می‌شود. **۳.امنیت فنی:** بر مکانیسم‌هایی تمرکز دارد که اطلاعات را از انتشار ناخواسته، تحریف و یا تخریب حفظ می‌کند. این بُعد از امنیت معمولاً «محرمانگی» نامیده می‌شود که از دسترسی یا تغییر در داده‌ها، برنامه‌ها و یکپارچگی سیستم توسط کاربران غیرمجاز جلوگیری می‌کند و اطمینان می‌دهد اطلاعات و نرم افزارها دست نخورده و صحیح باقی می‌مانند. با توجه به اهمیت «امنیت فضای مجازی» در سند راهبردی نظام جامع فناوری اطلاعات کشور، راهکارهای «استقرار نظام امنیت فضای الکترونیکی تبادل اطلاعات کشور» عنوان شده در برنامه‌های پنجم و ششم توسعه، موضوع لزوم حفاظت از اطلاعات رایانه‌ای در سیاست‌های کلی توسعه را به شکلی جزئی‌تر تبیین می‌کند. امنیت مجازی در سازمان، به کار گیری یک راهبرد برای دستیابی به وضعیتی است که مدیران

[66] Media Literacy
[67] Cyber Security

مربوطه، توانایی «حفاظت از اطلاعات و ارتباطات سازمانی» را در برابر انواع ریسک‌ها، آسیب‌ها و حوادثی که سازمان را تهدید می‌کند، داشته باشند. این راهبرد باید تکرار داشته باشد و مدیریت شود.

دولت الکترونیک در ایران

امروزه ضریب نفوذ اینترنت در کشور به بیش از ۷۰٪ جامعه رسیده و آمار ایرانیان در استفاده از فضای مجازی و شبکه‌های اجتماعی در دنیا در حال افزایش و از جهاتی، بالاتر از میانگین بین‌المللی قرار گرفته است. مدل دولت الکترونیک، به‌عنوان یکی از ابزارهای قدرتمند تحقق شاخص‌های حکمرانی خوب به‌ویژه شفاف سازی، پاسخگویی، کارایی، اثربخشی، مشارکت جویی و شهروند مداری تعریف می‌شود. **«دولت الکترونیک[۶۸]»**، فرصتی برای تعاملات بهتر میان دولت و مردم از یک سو و سازمان‌ها و بخش‌های خصوصی از سوی دیگر است. دولت الکترونیک به‌معنای اطلاع رسانی و خدمات رسانی به موقع، دقیق و کارآمد در ۲۴ ساعت شبانه روز، هفت روز هفته و ۳۶۵ روز سال از طریق وسایل ارتباطی گوناگون مانند تلفن و اینترنت است. «دولت الکترونیک» عبارت است از تعهد به استفاده از فناوری‌های مناسب برای ارتقای ارتباطات دولت با شهروندان و سازمان‌های وابسته به دولت و به عبارتی، گسترش دموکراسی، ارتقای شأن و منزلت انسان، حمایت از توسعهٔ اقتصادی، توسعهٔ عدالت اجتماعی و بهبود کیفیت ارائهٔ خدمات به مردم، تبادل سریع و آسان داده‌ها و اطلاعات، دسترسی مستقیم و سریع شهروندان به اطلاعات مورد نیاز، صرفه جویی در انرژی، زمان، منابع و هزینه‌ها، افزایش کارایی و بهره وری، آثار مثبت زیست محیطی، بهبود پاسخگویی به شهروندان، افزایش شفافیت فعالیت‌های دولت و در نتیجه کاهش فساد اداری، ساده سازی فرایندهای دولتی و... چرا که سازمان‌های دولتی از طریق کاربست فناوری‌های ارتباطی می‌توانند کارایی، اثربخشی و بهره وری خود را افزایش داده، پاسخگوی شهروندان و در نهایت عاملی برای افزایش سطح مشارکت و شاخص دموکراسی در کشورها باشند. از این رو دولت الکترونیک در راستای شکل گیری «دیجیتال دموکراسی» که در همگرایی با شاخص‌های «حکمرانی خوب» قرار دارد، در ادبیات توسعه از اهمیتی دو چندان برخوردار است. زیرا مهمترین دستاورد «دولت الکترونیک» ایجاد نظامِ اداریِ سالم، کاهش یا حذف ارتباطات مستقیم میان شهروندان و کارکنان، و در نتیجه کاهش تخلفات و فساد اداری و کوچک کردن بدنهٔ دولت است. «دولت الکترونیک» به مثابهٔ یکی از ابزارهای اصلی ایجاد و بسط شفافیت در بخش دولتی، می‌تواند ابزاری مؤثر در امر کاهش «فساد» باشد. از جمله مزایای دولت الکترونیک در حوزهٔ سیاسی، شناخت بهتر اهداف، خط مشی‌ها در سطح دولت، پاسخگویی عمومی بیشتر، ارائهٔ اطلاعات دولتی جامع‌تر و برنامه ریزی و ارائهٔ خدمات یکپارچه است. دولت الکترونیک، باعث شکل گیری دولتی کارآمد و اثربخش در مصرف هزینهٔ عمومی خواهد شد، با دسترسی عامه به اطلاعات و پاسخگویی

[68] E-Government: Electronic Government

بیشتر دولت به شهروندان، فساد کاهش پیدا کرده، رضایت عمومی افزایش خواهد یافت. افزایش شفافیت و تعامل با دولت، به افزایش اعتبارات عمومی دولت میان شهروندان منجر خواهد شد که این خود در بستر اینترنت و فضای مجازی و پیاده سازی «دولت الکترونیک» محقق می‌شود. اما نمی‌توان نادیده انگاشت که در مقابل استقرار دولت الکترونیک، موانع و عوامل بازدارنده‌ای نیز وجود دارند که بدون فراهم سازی بسترهای قانونی، زیرساخت‌های فنی و فرهنگی، استقرار دولت الکترونیک نمی‌تواند مفید و مثمرثمر واقع شود و با شکست مواجه خواهد شد. در واقع، استقرار دولت الکترونیک، خود مستلزم ایجاد زیرساخت‌های فناوری مورد نیاز، پایگاه‌های ارائهٔ خدمات و اطلاعات، **ارتباط و تعامل دوسویهٔ دولت با مردم و مردم با دولت**، آموزش و بستر سازی فرهنگی، رسیدگی به شکایات مردمی و برنامهٔ دورکاری است. این مسئله خود منجر به کاهش عدم شفافیت و سوءاستفاده‌های احتمالی کارکنان و در نتیجه نارضایتی از سازمان‌های مختلف به دلیل انحراف از شیوه‌های قانونی و افزایش نظارت شهروندان می‌شود. همچنین دولت الکترونیک در عصر «جامعهٔ شبکه‌ای»، مدیریت و سلسله مراتب سنتی و قدیمی را تغییر داده، سطوح میانی حذف و فاصلهٔ مدیران عالی با سطوح عملیاتی و تعاملی مردمی کاسته خواهد شد. دولت الکترونیکی می‌تواند پاسخگویی بیشتر، شفافیت و دسترسی به اطلاعات را به همراه داشته باشد. اما متأسفانه کشور ایران در رقابت جهانی استقرار دولت الکترونیک بسیار ناتوان ظاهر شده و در رتبهٔ ۱۰۸ قرار دارد و حتی در میان سیزده کشور آسیای جنوبی و مرکزی نیز جایگاه مناسبی ندارد. مطالعات و پژوهش‌های انجام شده نشان می‌دهند که موانع چهارگانهٔ استقرار دولت الکترونیک در ایران عبارتند از:

۱. موانع مدیریتی
۲. موانع فرهنگی-اجتماعی
۳. موانع اقتصادی-مالی
۴. موانع فنی و زیرساختی

نقش دولت الکترونیک در تحقق «**حکمرانی خوب**» را می‌توان شامل موارد ذیل دانست:

۱. مردم سالاری مبتنی بر مشارکت
۲. انسجام، تعامل و همکاری بیشتر میان سازمانی
۳. هماهنگی، اثر بخشی و کارایی سازمانی
۴. سهولت همکاری و اجرایی شبکه‌ای «دستورکارهای سازمانی» در شکل همزمان و کارآمدتر
۵. شفافیت و امکان دسترسی به فرایندها در سراسر زمان اجرا و تدوین دستورکارها
۶. امکان دسترسی به اطلاعات برای شهروندان
۷. فراهم ساختن امکان مشارکت تمامی اشخاص ذینفع در تصمیم گیری‌ها، زیرا «دولت الکترونیک» حلقه‌ای مرکزی و رابط بین راهبرد، فرایند، سازمان و فناوری است تا به نحوی مؤثر خدمات را به

مشتریان و گروه‌های ذینفع ارائه دهد و بخش دولتی را در حفظ و نگهداری و تقویت حکمرانی خوب یاری کند

۸. کوچک سازی بدنهٔ دولت.

جمع‌بندی و ارائه پیشنهادها

پیشنهادهای راهبردی در حوزهٔ ارتقای دولت الکترونیک، افزایش بهره وری فضای مجازی و امنیت فضای مجازی در راستای تحقق «حکمرانی خوب سایبری»:

۱. **داشتن رویکرد کلان مدیریتی:** شناسایی و توجه سازمان‌ها و نهادهای مختلف دولتی نسبت به برقراری سازوکار و ارتقای ارتباط «تعاملی» با مردم، به‌منظور احصای دیدگاه‌های آنها و ارائهٔ گزارش عملکرد و تصمیمات خود در راستای شفافیت بیشتر، تشکیل کمیته‌های مجازی بین بخش‌های مختلف دولتی، مدنی و خصوصی به‌منظور همگام سازی و هماهنگ سازی بین آنها

۲. **تهیه قوانین مدون و ابلاغ به مردم و کارکنان:** آموزش و ارتقای «سواد رسانه‌ای» جامعهٔ ایران توسط دولت، نهادهای آموزشی (مدارس و دانشگاه‌ها) و رسانه‌های گروهی با هدف استفادهٔ بهینه و سودمند از امکانات فضای مجازی و شبکه‌های اجتماعی و مجهز کردن عموم مردم به «دیدگاه اننتقادی رسانه-ای»؛ به جای فیلترینگ و سانسورهای گسترده. تدوین قوانین و حقوق سایبری و شکل دهی به آمبودزمان‌های مختلف متکی بر بخش خصوصی و گروه‌های مدنی

۳. **به روز رسانی تجهیزات نرم افزاری و سخت افزاری بر اساس تحولات امنیتی:** تقویت زیرساخت‌های فنی و فناورانه، ارتباطی و اینترنتی و در کل «عمومی سازی دسترسی به فضای مجازی» به‌منظور کاهش «شکاف دیجیتالی[۶۹]»[۷۰] ناشی از عدم آگاهی از استفاده از فناوری‌های نوین ارتباطی، فقدان دسترسی به فناوری‌های ارتباطی در مناطق محروم، آموزش سواد رسانه‌ای و...به منظور «خوداتکایی» و «درون زایی» در تمامی زیرساخت‌های حیاتی، سخت افزارها و نرم افزارهای پایه و تأسیس سکوهای عمومی مورد نیاز کشور، ارتقای اثربخشی و کارآمدی «دولت الکترونیک» و در نتیجه تحقق حکمرانی خوب سایبری.

---

[69] Digital Divide

[۷۰] «شکاف دیجیتالی» به معنای نابرابری های موجود در استفاده از فناوری های اطلاعاتی و ارتباطاتی و فضای مجازی به دلیل عدم دسترسی به زیرساختارهای مورد نیاز در استفاده از این فناوری ها در مناطق محروم، نداشتن دانش، تخصص و آگاهی کافی، نابرابری های فضایی و کالبدی، امکانات متفاوت شهروندان از لحاظ مالی، تعصبات جنسیتی (به عنوان مثال عدم استفاده و دسترسی زنان و دختران به دلایل مذهبی و...) است. از این رو در عصر حاضر با پدیدهٔ «حاشیه نشینی الکترونیکی» مواجه هستیم، یعنی کسانی که توانایی و هویت شهروندی الکترونیک آنان سلب می شود و با از دست دادن این هویت و امکانات، نه تنها امکانات، رفاه و خدمات و...را از دست می دهند، بلکه مسائل و مشکلاتشان نیز دیده نمی شود

۴. **تعریف چشم انداز، مأموریت‌ها و ارزش‌ها:** توسعه و به کارگیری حکمرانی سایبری در حل معضلات اساسی جامعه و اولویت‌های کلان کشور، در نظر داشتن ظرفیت‌های مختلف فضای مجازی و شبکه-های اجتماعی برای طراحی شبکه‌های بومی اطلاع رسانی و بازخوردگیری تصمیمات و آرای عمومی بر اساس برخورداری از زیرساخت‌های فنی قوی و مناسب (نه شبکه‌های اجتماعی که به سادگی در حوزهٔ «امنیت سایبری» قابل هک بوده و در رقابت با نسخه های بدیل خارجی قادر به ارائهٔ خدمات مناسب نیستند).

۵. **ایجاد تعهد سازمانی و مردمی:** عدم وجود سند راهبردی در حوزهٔ حکمرانی سایبری به‌منظور تدوین چشم اندازها و قوانین در ارتباط با رفع موانع اطلاع رسانی صحیح و مقابله با ابهام اطلاع رسانی خصوصاً به‌منظور مقابله با «شایعه سازی» در فضای مجازی و شبکه‌های اجتماعی، جامعه‌ای که «چشم انداز مطلوب» و هدفمند نداشته باشد و تنها در حالت انفعال و واکنش گرایانه عمل کند محکوم به شکست است.

۶. **برنامه ریزی فعالیت‌های آتی بر مبنای یک محیط تعاملی:** کنشگری هوشمند با به خدمت گرفتن ظرفیت نهادهای فعال در حوزهٔ حکمرانی فضای مجازی، برنامه ریزی مناسب برای استفادهٔ بهتر از امکانات و فرصت‌های فضای مجازی در جامعهٔ مدارس و دانشگاهی در حیطهٔ شناخت علایق و سلایق کاربران فضای مجازی (آینده نگاری از سوگیری‌های فرهنگی و سیاسی-اجتماعی کاربران فضای مجازی در نسل‌های مختلف به‌منظور شناسایی تهدیدها و فرصت‌ها و رخنه‌های سیاسی-اجتماعی و فرهنگی در جنگ‌های روانی و راه‌های مقابله با آنها)

۷. **تخصیص بودجه مناسب به‌منظور آموزش کارکنان، انجام پروژه‌های تحقیقاتی مرتبط**: مدیریت راهبردی سرمایه‌ها و منابع انسانی و نیروهای متخصص در حوزهٔ فناوری‌های ارتباطی و اطلاعاتی، مدیریت صحیح سازمانی در استفاده از نخبگان و نیروهای آموزش دیده در این حوزه (کمبود متخصصین حکمرانی سایبری)، این در حالی است که کشور در شرایط ناشی از کمبود بودجه و کمبود مراکز مطالعاتی و پژوهشی در حوزهٔ حکمرانی سایبری فعال قرار دارد.

۸. **تعیین اهداف امنیتی و ارائهٔ راهکارها و راهبردهای تدافعی-تهاجمی**: طراحی و پیاده سازی چارچوب بومی «معماری امنیت فضای مجازی[۷۱]»، به‌منظور کاهش تهدیدات سایبری و ارتقای سطح حفاظت از اطلاعات رایانه‌ای عمومی و محرمانه و طبقه بندی شده در برابر بدافزارهای جدید (مقابله با تروریسم سایبری)، مقابله با «تهدیدات سایبری و مجازی» یکی از جدی‌ترین چالش‌های امنیتی، اقتصادی، سیاسی-اجتماعی در سطح داخلی و ملی محسوب می‌شوند که با عنایت به «سند راهبردی پدافند مجازی کشور» که در سال ۱۳۹۴ تدوین و منتشر شده، هنوز محقق نشده است. تهدیدات و تهاجمات

[71] Cyber Security of Virtual Space

سایبری را می‌توان در طیف وسیعی از هکتیویسم[۷۲]، جاسوسی سایبری[۷۳]، جرائم سایبری[۷۴]، تروریسم سایبری[۷۵] و جنگ سایبری[۷۶] طبقه بندی نمود. بر اساس گزارش سازمان جهانی استاندارد (۲۰۱۴)، ایران در بین ۱۴ کشور غرب آسیا، از نظر تعداد گواهینامه‌های اخذ شده در سیستم «امنیت مجازی» جایگاه ششم را داراست که این مسئله خود ریشه در فقدان یک نگاه مدیریتی بومی مورد نیاز کشور در قالب حکمرانی خوب و امنیت فضای مجازی دارد. این مسئله در کارگروه «امنیتی» کشور در حوزهٔ «جنگ های نوین مجازی عملیاتی[۷۷] و راهبردی[۷۸]» محسوب می‌شود. چالش «امنیت فضای مجازی» در سازمان‌های بخش دفاع که متولی حفظ امنیت و دفاع از کشور در برابر تهدیدات مختلف هستند، بسیار جدی‌تر و اساسی‌تر است. دستیابی به فناوری های برتر مورد نیاز دفاعی و امنیتی با توجه به شناسایی تهدیدات حال و آینده با تأکید بر نوآوری و پشتیبانی از شرکت‌ها و سرمایه‌های انسانی مستعد در این حوزه به‌منظور خودکفایی کشور در سامانه‌ها، کالاها، خدمات اولویت دار دفاعی و امنیتی توأم با بهسازی تجهیزات موجود و افزایش قابلیت کارایی آنها، ضروری است. تحقق حکمرانی خوب در حوزهٔ «امنیت فضای مجازی» بالاخص در بخش دفاع ج.ا.ا و سازمان‌های مربوطه (ارتش، سپاه پاسداران، وزارت دفاع و نیروی انتظامی) از اهمیت به سزایی برخوردار است. در این زمینه می‌توان به بدافزار «پگاسوس» ساخت شرکت صهیونیستی NSO[۷۹] اشاره کرد که برای جاسوسی نهادهای امنیتی، پلیس، ارتش و...مراکز دفاعی و شناسایی افراد و کارکنان این مراکز و با اهدافی همچون جمع آوری اطلاعات مورد نیاز و در صورت لزوم، ترورهای کور مورد استفاده قرار می‌گیرد. (آلوده سازی تلفن های اندروید و آیفون)

---

[72] Hactivism
[73] Cyber Intelligence
[74] Cyber Crime
[75] Cyber Terrorism
[76] Cyber Warfare

[۷۷] جنگ سایبری عملیاتی، به عملیات سایبر گفته می شود که همزمان و یا قبل از حملهٔ نظامی صورت پذیرفته و حملهٔ نظامی را تقویت و پشتیبانی می کند. به عنوان مثال، ممکن است قبل از حملهٔ نظامی به یک کشور، به وسیلهٔ حملات هکری شبکه های آب، برق، تلفن و یا گاز یک کشور، که همه به وسیلهٔ سامانه های رایانه ای کنترل می شوند از کار بیفتند و سپس حملهٔ نظامی صورت پذیرد

[۷۸] جنگ سایبری راهبردی، به عملیاتی گفته می شود که در جهت وارد آوردن فشار راهبردی به یک کشور انجام شده و هیچ عملیات نظامی را به همراه ندارد، مانند ویروس استاکس نت که برای آسیب رساندن و جلوگیری از برنامه های هسته ای ایران طراحی شده است

[۷۹] یک شرکت فناوری تابع رژیم صهیونیستی است که در اوت ۱۹۹۹ توسط نیو کارمل، امری لاوی و شالو هولیو بنیان گذاشته شد. ستاد این شرکت در هرتزلیا نزدیک تل آویو در سرزمین‌های اشغالی قرار دارد

۹. **کاهش دادن مقاومت در برابر تغییرات:** تطبیق پذیری و انعطاف پذیری بیشتر فضای مجازی برای کاربران[۸۰]، تفویض اختیارات به مقامات محلی[۸۱] جهت حفظ هویت‌های قومی، مذهبی، نژادی کنترل پذیر کردن آنها.

۱۰. **شناسایی و توسعهٔ شایستگی‌ها و مزیت‌های رقابتی نسبی**: تأسیس شرکت‌های بزرگ غیردولتی با رویکرد فراملی و باز کردن میدان نوآوری در حوزهٔ حکمرانی سایبری، بازمهندسی، به روز رسانی و ارتقای زیرساخت‌های فناوری سازمانی همراه با ایجاد سامانهٔ یکپارچهٔ نرم افزاری اطلاعاتی.

۱۱. **تدوین خط مشی و دستورالعمل‌های قانونی و حقوقی:** استاندارد سازی محصولات و سازوکارهای امنیتی حوزهٔ فناوری اطلاعات و فضای مجازی، تدوین قوانین حقوقی متناسب با «تخلفات فضاهای مجازی» به جای اِعمال سیاست های فیلترینگ و سانسور رسانه‌ای. این یعنی زیرساخت، خدمات و محتوا باید سه رگولاتوری متفاوت از هم داشته باشند

۱۲. **شناسایی تهدیدات و آسیب پذیری‌ها و فرصت‌های موجود**: سازمان توسعه و همکاری‌های اقتصادی[82] از اصطلاح «معمای پیچیده[۸۳]» برای توصیف مدیریت فضای مجازی استفاده می‌کند. به این معنا که سیاستگذار در ابتدای توسعهٔ فناوری، هر تغییری که لازم باشد را می‌تواند انجام دهد، اما از تأثیرات آیندهٔ تصمیم خود مطلع نیست و آگاهی چندانی ندارد. اما در انتهای کار، که کمی فضا روشن شد، در می‌یابد که دیگر هر تغییری را که بخواهد نمی‌تواند انجام دهد. از این رو این سازمان پیشنهاد می‌دهد که برای مدیریت فضای مجازی بر اساس فناوری، باید بر اساس «ابرچالش‌ها» و «تجمع داده» تصمیم گرفت. به این معنا که باید در نظر گرفت در حوزه‌های مختلف سیاسی-اجتماعی، اقتصادی، فرهنگی و زیست محیطی با چه چالش‌ها و دغدغه‌هایی روبرو هستیم، لذا بر اساس تجمع داده در همان حوزه، مدل حکمرانی خوب بومی را تنظیم و عملیاتی سازی کنیم. این یعنی تدوین راهبردها، استانداردها، چارچوب‌ها، متدولوژی‌ها و ابزارهای مورد نیاز در حوزهٔ ارتقای فناوری‌های نوین ارتباطی به گونه‌ای که دیگر مصرف کننده و وارد کنندهٔ منفعل فناوری‌های نوین ارتباطی نباشیم، و به شکل همزمان تلاش برای شکل گیری «شهر الکترونیک[۸۴]»[۸۵] و «شهروند الکترونیک[۸۶]» در راستای هم افزایی کارایی و خدمات «دولت الکترونیک»، این در حالی است که در حال حاضر در ارتباط با

---

[80] User-Friendly
[81] Local Authorities
[82] Organization for Economic Cooperation and Development
[83] Collingrage
[84] Cyber City

[۸۵] شهر در حیات مدنی از سه رکن اصلی شهروند، کالبد شهری و مدیریت شهری تشکیل شده است. مراد از شهر الکترونیک، تغییرات فضایی و کالبدی شهری در راستای افزایش ضریب نفوذ فضای مجازی و استفاده از ظرفیت ها و پتانسیل های آن درراستای ارتقای بهره وری و مدیریت شهری است، چرا که شهروند و مدیریت شهری ماهیتی فاعلی دارند، در حالی که کالبد شهر ماهیتی انفعالی دارد و به نوع طراحی و معماری آن وابسته است

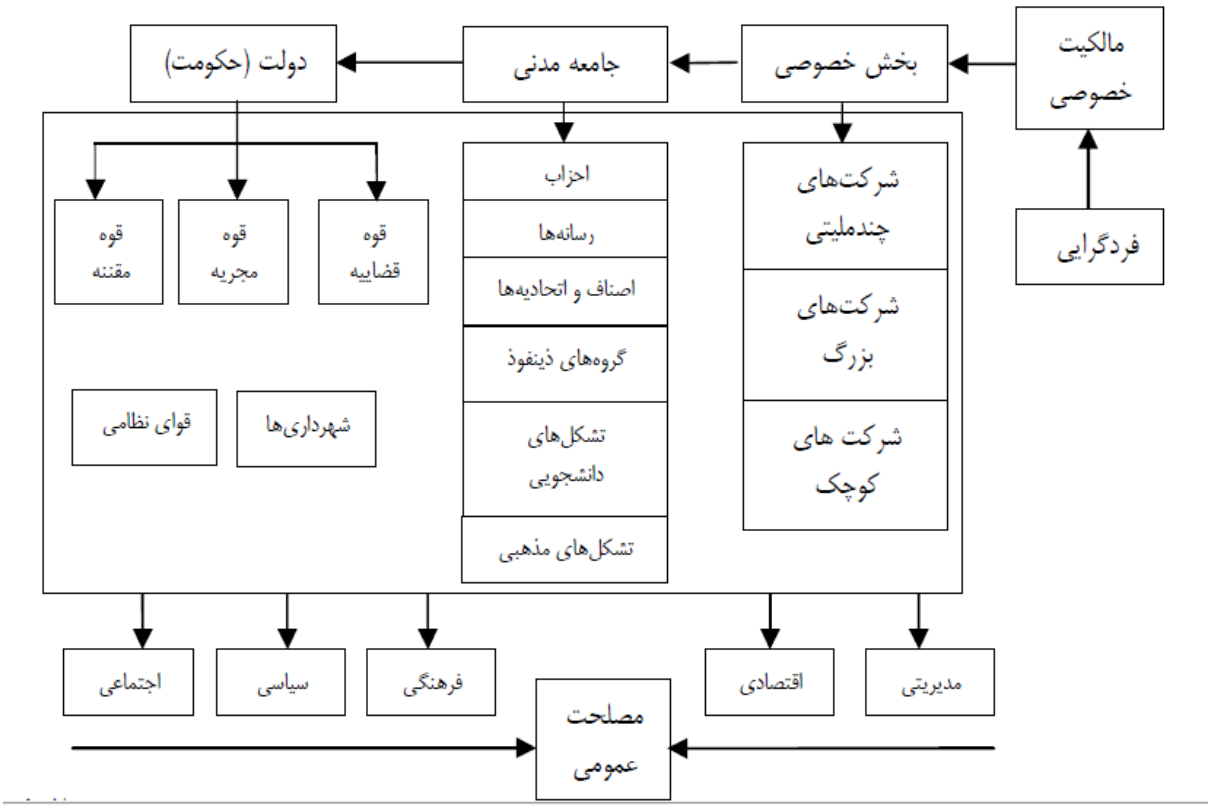
[۸۶] شهروند الکترونیک کسی است که از امکانات مالی و حداقل دانش، تخصص و سواد رسانه ای لازم در برقراری ارتباط با فضای مجازی برخوردار است

حکمرانی خوب سایبری، کشور از فقدان «**راهبرد سایبری**» رنج می‌برد و تنها بر رویکردهای منفعلانه، سلبی و محدودیت زا متمرکز شده‌ایم.

شکل ۳: محورهای حکمرانی سایبری

اما مسئله این جاست که «**بی‌نظمی فضای سایبری**» در نهایت منجر به «**شکاف حکمرانی سایبری**» می‌شود، به این معنا که شرایطی شکل می‌گیرد که ارزش‌های دولت با ارزش‌های سایر بازیگران در تناقض آشکار قرار می‌گیرد و منجر به امنیتی شدن فضا می‌شود. آشفتگی نهادی در سامانه سیاستگذاری مربوط به حکمرانی سایبری، تعدد و موازی کاری در بین نهادهای مسئول سیاست گذاری، اجرایی، نهادهای میانجی و مؤسسات آموزشی، پژوهشی و فناوری، نگاه خطی و سبک راهبری دستوری حاکمیت در سیاستگذاری مرتبط با فضای مجازی و کم رنگ بودن نقش مردم، نهادهای مردمی و بخش خصوصی در فرایند سیاستگذاری، عدم نظام یافتگی فرایند سیاستگذاری و نامشخص بودن تفکیک وظایف میان برخی نهادهای موجود و ضعف در همکاری‌های بین‌المللی در زمینهٔ سیاستگذاری سایبری و فضای مجازی و عدم استفاده از تجارب دیگر کشورها در این زمینه، از جمله چالش‌های بحث برانگیز در حوزهٔ تحقق «حکمرانی سایبری» در ایران شده است.

مدل جامعه همکار در الگوی حکمرانی خوب



شکل ۴: مدل جامعه همکار در الگوی حکمرانی خوب

یادداشت‌ها و منابع

ابراهیم پور، حبیب و الیکی، فهیمه. (۱۳۹۵). بررسی نقش حکمرانی خوب در کارآمدی دولت‌ها. کنفرانس بین‌المللی نخبگان مدیریت (ص. ۱۸-۱). تهران: دانشگاه شهید بهشتی.

الوانی، سید مهدی و علیزاده ثانی، محسن. (۱۳۸۶). تحلیلی بر کیفیت حکمرانی خوب در ایران. مطالعات مدیریت (بهبود و تحول) , ۱۸ (۵۳), ۱-۲۴.

امام جمعه زاده، سید جواد.؛ شهرام نیا، امیر مسعود و صفریان گرمه خوانی، روح الله. (۱۳۹۵). الگوی حکمرانی خوب؛ جامعه همکار و دولت کارآمد در مدیریت توسعه. *فصلنامه تخصصی علوم سیاسی , ۱۲* (۳۶), ۷-۴۰.

آرائی، وحید و نجف پور، شعبان. (۱۳۹۹). بررسی نقش رسانه در سیاستگذاری مبارزه با فساد مبتنی بر رویکرد نظام ملی درستکاری. فصلنامه علمی نظارت و بازرسی ناجا , ۱۴ (۵۳), ۵۸-۳۹.

باطنی، ابراهیم و یزدان شناس، مهدی. (۱۳۸۵). نگاهی به فرایند شکل گیری دولت الکترونیک و چالش‌های فراروی آن. *فقه و حقوق , ۳*, ۹۴-۵۹.

بشیری، سعید؛ ابطحی، سید مصطفی. و مرشدی زاد، علی. (۱۳۹۹). نقش فضای مجازی بر وضعیت شفافیت در ایران (بررسی دیدگاه دانشجویان دانشگاه آزاد اسلامی واحد علوم و تحقیقات). *فرهنگ در دانشگاه اسلامی , سال دهم* (شماره اول), ۱۲۷-۱۵۶.

بل، دیوید. (۱۳۹۰). *نظریه پردازان فرهنگ سایبری (رایا فرهنگ): مانوئل کاستلز و دانا هاروی*. (م. شفیعیان, مترجم) تهران: دانشگاه امام صادق.

بیابانی، غلامحسین و ذوقی، بهنام. (۱۳۹۷). رسانه ها ابزاری برای ترویج شفافیت و مقابله با فساد سیاسی و مالی. *رسانه , ۲۹* (۳), ۸۵-۱۰۴.

پولاک، فِرد. (۱۳۹۸). *تصویر آینده*. (ح. قاسمی, & ع. کرامت زاده, مترجم) تهران: پژوهشکده اندیشه دفاعی، گروه پژوهشی آینده نگاری علوم و فناوری های دفاعی.

جاسبی، جواد و نفری، ندا. (۱۳۸۸). طراحی الگوی حکمرانی خوب بر پایه نظریه سیستم های باز. *فصلنامه علوم مدیریت ایران , ۴* (۱۶), ۸۵-۱۱۷.

جمشیدی، محمد حسین و نقدی، فرزانه. (۱۳۹۸). تأثیر انقلاب فناوری نوین ارتباطی و اطلاعاتی بر دگرگونی و تحول مقوله «دولت». *فصلنامه سیاست* , ۴۹ (۳), ۶۰۷-۶۲۶.

حشمت زاده، محمد باقر.؛ حاجی یوسفی، امیر محمد و طالبی، محمد علی. (۱۳۹۶). بررسی موانع تحقق حکمرانی خوب در فرهنگ سیاسی ایران. *جستارهای سیاسی معاصر، پژوهشگاه علوم انسانی و مطالعات فرهنگی* , ۸ (۱), ۱-۲۴.

دوله، فاطمه.؛ سیف اللهی، سیف الله. و زنجانی، حبیب الله. (۱۳۹۸). مطالعه زمینه ها و موانع شکل گیری حکمرانی خوب در ایران معاصر. *فصلنامه علمی-پژوهشی علوم اجتماعی دانشگاه آزاد اسلامی واحد شوشتر* , *سال سیزدهم* (شماره دوم، پیاپی ۴۵), ۱۲۳-۱۵۴.

رضایی، مهدی و بابازاده مقدم، حامد. (۱۳۹۳). اصول تدوین قوانین و مقررات برای اینترنت با تأکید بر مصوبات یونسکو و شورای اروپا. *فصلنامه پژوهش حقوق عمومی* , *۱۵* (۴۲), ۴۳-۸۲.

سهیلی مقدم، سید مهدی. (۱۳۹۹). واکاوی حاکمیت دولت بر فضای مجازی؛ مطالعه موردی عربستان در مواجهه با معارضان. *دو فصلنامه علمی مطالعات بیداری اسلامی* , ۹ (۱), ۲۸۱-۳۰۹.

شیخیانی، حمزه و همکاران. (۱۳۹۹). نقدی بر پروژه ایران ۲۰۴۰ دانشگاه استنفورد (حکمرانی و توسعه در ایران). *دومین همایش ملی حکمرانی اسلامی* (ص. ۱۵-۱). تهران: مدرسه حکمرانی شهید بهشتی.

شیرودی، محمد سجاد و همکاران. (۱۴۰۰). دولت مجازی در جمهوری اسلامی ایران و ارتقای مشروعیت و کارآمدی سیاسی. *فصلنامه علمی پژوهش های انقلاب اسلامی* , *۱۰* (۳), ۳۵-۵۳.

فرزام نیا، نیما و عبدی، بهنام. (۱۴۰۰). ارائه الگوی حکمرانی خوب امنیت فضای مجازی. *دومین همایش حکمرانی اسلامی* (ص. ۲۵-۱). تهران: مدرسه حکمرانی شهید بهشتی.

قاسمی خیرآبادی، عبدالله و همکاران. (۱۳۹۹). ارائه الگوی حکمرانی آموزشهای مهارتی در سطح فروملی با رویکرد نظری داده بنیاد. *فصلنامه علمی - پژوهشی کارافن* , *۱۷* (۳), ۲۹-۴۰.

قاسمی، ابوالفضل و همکاران. (۱۴۰۰). تحلیل مضامین حکمرانی خوب شهری در برنامه های توسعهٔ جمهوری اسلامی ایران. *پژوهش های راهبردی مسائل اجتماعی ایران* , *۱۰* (۳۴), ۱۱۷-۱۴۱.

قهرمان، میثم و عباس زاده مرزبالی، مجید. (۱۳۹۲). اینترنت و رادیکال دموکراسی: درآمدی بر شکل گیری رادیکال دموکراسی مجازی. *پژوهش سیاست نظری* , *۱۳*, ۲۹-۵۲.

کاستلز، مانوئل. (۱۴۰۰). *شبکه های خشم و امید: جنبش های اجتماعی در عصر اینترنت*. (م. قلی پور, مترجم) تهران: مرکز.

کاستلز، مانوئل. (۱۳۹۸). *قدرت ارتباطات*. (ح. بصیریان جهرمی, مترجم) تهران: انتشارات علمی و فرهنگی.

کیان خواه، احسان. (۱۳۹۸). چالش های راهبردی حکمرانی با گسترش فضای سایبر. *امنیت ملی , ۹* (۳۴), ۱۷۴-۱۵۳.

گل محمد زاده، محمد علی.؛ اسمعیل زاده، علیرضا و احدی، پرویز. (۱۳۹۹). پیامدهای سیاسی شکافهای اجتماعی و مساله حکمرانی خوب در ایران پس از دهه ۱۳۴۰. پژوهش های روابط بین الملل , ۱۰ (۳۶), ۲۰۰-۱۶۷.

لشگری، احسان. (۱۳۹۵). تبیین اهمیت استراتژیک حوزۀ جغرافیایی مدیریت و کنترل فضای مجازی. فصلنامه ژئوپلیتیک , ۱۲ (۲), ۱۰۵-۱۲۳.

محمدی، حافظ. (۱۳۹۹). چالش‌های حکمرانی فضای مجازی و ارائه راهکارها برای جمهوری اسلامی ایران. دومین همایش حکمرانی اسلامی (ص. ۱۳-۱). تهران: مدرسه حکمرانی شهید بهشتی.

مرکز بررسی های استراتژیک ریاست جمهوری . (۱۳۹۹, آبان ۱۹). www.css.ir. بازیابی در تیر ۱۴۰۱، از https://www.css.ir/Media/PDF/1399/08/19/637405180336871417.pdf

مرکز بررسی های استراتژیک. (۱۳۹۹, مهر ۲۳). مرکز بررسی های استراتژیک ریاست جمهوری. بازیابی در تیر ۱۴۰۱، از http://www.css.ir/Media/PDF/1399/07/23/637382645215385963.pdf

معینی فر، مریم و عطار، عباس. (۱۳۹۴). بررسی موانع فضایی و کالبدی اجرای شهرداری الکترونیک از نظر شهروندان و کارکنان شهرداری تهران. مدیریت شهر , ۲۲ (۹), ۵۳-۶۲.

نظریان، اصغر و شوهانی، نادر. (۱۳۹۰). توانمند سازی نظام مدیریت شهری بر اساس الگوی شهر شهروند مدار در ایلام. چشم انداز جغرافیایی , ۶ (۱۶), ۱۳۴-۱۵۱.

DCMS. (2013). https://assets.publishing.service.gov.uk. Retrieved 2022, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/257006/UK_Broadband_Impact_Study_-_Impact_Report_-_Nov_2013_-_Final.pdf

https://assets.publishing.service.gov.uk. (2016). Retrieved 2022, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

https://assets.publishing.service.gov.uk. (2022). Retrieved 2022, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf

https://blogs.lse.ac.uk. (2018). Retrieved 2022, from https://blogs.lse.ac.uk/medialse/2018/08/23/the-essential-elements-of-the-new-internet-governance-diversity-optimism-and-independence/

https://blogs.lse.ac.uk. (2018). Retrieved 2022, from https://blogs.lse.ac.uk/medialse/2018/05/24/a-more-transparent-and-accountable-internet-heres-how/

Kleinsteuber, Hans J. (n.d). Self-regulation, Co-regulation, State Regulation. The Organization for Security and Co-operation in Europe , 1-63, Can be Retrieved from : https://www.osce.org/files/f/documents/2/a/13844.pdf.

The Royal Society. (2020). https://royalsociety.org. Retrieved 2022, from https://royalsociety.org/-/media/policy/projects/data-governance/uk-data-governance-explainer.pdf

گزارش نظری

فضای مجازی و حکمرانی خوب

تاریخ انتشار: تیر ۱۴۰۱

شناسه یکتا:IDG-THR-۱۶۰

جمهوری اسلامی ایران
وزارت کشور

مرکز مطالعات راهبردی و آموزش وزارت کشور