عنوان مقاله: حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری[1]

محمدمهدی قوچانی خراسانی[2] ـ داود حسین‌پور[3]

دریافت: ۱۳۹۶/۵/۲
پذیرش: ۱۳۹۶/۸/۱۴

چکیده:

نظام‌های سیاسی به فراخور فضای اجتماعی، سیاسی و اقتصادی، نوع حاکمیت خود را تغییر می‌دهند؛ یکی از مهم‌ترین دانش‌های بشری، دانش خط‌مشی‌گذاری عمومی است. با توجه به اهمیت این موضوع، در این پژوهش مفهوم حاکمیت و حاکمیت شبکه‌ای و عناصر آن تشریح می‌گردد؛ همچنین، از پر تغییرترین محیط‌های حاکم بر فعالیت‌های امروزی، فضای مجازی و سایبر است؛ امنیت فضای سایبر، پیروِ فضای سایبر، تحت تأثیر تغییرات مستمر است و به‌دلیل این‌که حفظ امنیت در اینَ فضا از مسائل مهم در امنیت ملی کشور محسوب می‌شود و همچنین به علت نبودِ هم‌افزایی نهادهای پژوهشیِ امنیت سایبری در ایران، بهره‌مندی از مدلی برای حاکمیت این فضا به‌منظور استفاده مَتناسب از همهٔ ظرفیت‌ها، راه‌حلی مناسب برای حاکمیت محسوب می‌شود. این پژوهش با هدف دست‌یابی به حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری، به‌دنبال شناسایی عناصر حاکمیت با توجه به شرایط محیطی حاکم بر آن در ایران است. بدین‌منظور، با استفاده از روش نظریهٔ داده‌بنیاد و مصاحبه با خبرگان این حوزه و با ارائهٔ یک مدل، سعی در تبیین آن با گزاره‌های نظری دارد. از مهم‌ترین گزاره‌های موجود می‌توان به ارائهٔ سیاست‌های یکپارچه از طریق ایجاد نقشه راه فناوری و محصولات بومی امنیت سایبر، نهادینه شده دغدغهٔ امنیت در کشور و مدیریت متعهد به بخش خصوصی اشاره نمود.

کلیدواژه‌ها: حاکمیت، حاکمیت شبکه‌ای، نهادهای پژوهشی، امنیت سایبری، نظریهٔ داده‌بنیاد.

۱. این مقاله برگرفته از پایان‌نامه دکتری نویسنده اول است.

۲. دانشجوی دکتری مدیریت دولتی، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی.
ghochany@yahoo.com
۳. دانشیار دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی (نویسنده مسئول).
dhp748@gmail.com

مقدمه

سیر تحول دانش‌های بشری نشان می‌دهد که همراه با تغییر در ماهیت مسائل، بسته‌های دانشی مدیریتی نیز دچار تحولاتی می‌شود. یکی از وظایف پژوهشگران علوم مدیریتی، رصد مشکلات جامعه به‌صورت عینی، به‌منظور حل مسائل دنیای واقع و ارائهٔ راه‌حل‌های مناسب به مدیران و سیاست‌گذاران برای حل آن مسائل است. یکی از مهم‌ترین دانش‌های بشری، دانش حکومت‌داری و خط‌مشی‌گذاری عمومی است؛ بنابراین، با توجه به تغییرات سریع فضای سایبر[1]، برای مدیریت بر این پیچیدگی باید تعاملات پیشِ رو با سازوکاری جدید برنامه‌ریزی شود تا با این سازوکار، هم بتواند بهره‌وری سازمان‌ها و نهادها بالا برود و هم در راستای هدف حاکمیت، پیوندهای میان نهادها به بهترین شکل هدایت و مدیریت شود. همان‌طور که بیان شد، امنیت فضای سایبر، پیروِ فضای سایبر تحت تأثیر تغییرات مستمر است و به دلیل این‌که حفظ امنیت در این فضا از مسائل مهم در امنیت ملی کشور محسوب می‌شود و همچنین به علت پراکندگی، ناهمسویی و نبودِ هم‌افزایی نهادهای امنیت سایبری در ایران، بهره‌مندی از مدلی برای حاکمیت این فضا به معنای استفاده متناسب از همهٔ ظرفیت‌ها، راه‌حلی مناسب برای حاکمیت در این حوزه محسوب می‌شود.

امروزه استفاده از ابزارهای فنّاوری برای تسهیل زندگی بشر در سراسر جهان به‌عنوان راهبردی مهم و پیش‌رو مورد توجه قرار گرفته است. رشد و توسعهٔ فناوری اطلاعات و فنّاوری‌های سازمان باعث شده تا فرصت‌هایی بسیار برای سوءاستفاده از اطلاعات و افراد در سازمان‌ها ایجاد شود. رایانه‌ها، تبلت‌ها، تلفن‌های همراه هوشمند، شبکهٔ جهانی اینترنت و شبکه‌های گسترده اجتماعی، همگی زندگی انسان را تحت تأثیر قرار داده‌اند. این فضای جدید، هم می‌تواند به‌عنوان یک فرصت بزرگ مورد استفاده قرار گیرد و هم می‌تواند تهدیدی جدی برای ادامه حیات باشد. از سال‌های ابتدایی فراگیر شدن رایانه‌های شخصی و پس از آن شبکه اینترنت، موضوع امنیت شبکه‌ها و اطلاعات کاربران و به بیان کلی‌تر امنیت در فضای سایبر، یکی از مباحث مهم بوده است. علاوه بر این، حفظ امنیت سایبری در سطح کلان و حاکمیتی آن در پی تأمین امنیت و منافع ملی است

۱. محیط پیچیده ناشی از تعامل مردم، نرم‌افزار و خدمات در اینترنت با استفاده از دستگاه‌های فناوری و شبکه‌های متصل به آن است که در هر صورت، ماهیت فیزیکی ندارد. سازمان استاندارد بین‌المللی (۲۰۱۱)

و همچنین هدف آن محافظت از زیرساخت‌های حیاتی ملی نظیر ارتباطات، حمل‌ونقل، سوخت، بانکداری و غیره است که طی سنوات اخیر در کشور ما بر بستر فضای سایبری قرار گرفته‌اند. در سال ۲۰۱۰ یک حملهٔ سایبری به سانتریفیوژ[1]های اورانیوم در نطنز توسط بدافزار استاکس‌نت[2] رخ داد که به‌عنوان نخستین حملهٔ سایبری علیه یک کشور محسوب می‌شود. بنابراین، حفظ امنیت فضای سایبر چه در بُعد مجازی (نرم‌افزار و شبکه) و چه حقیقی (سیستم‌های کنترل صنعتی) از اهمیت حیاتی برای حفظ تمامیت اصلی کشور برخوردار است (Langner, 2013). از مهم‌ترین مسائل در حفظ امنیت سایبری کشور، استقلال و خودکفایی در تولیدات محصولات امنیت سایبر است؛ چراکه محصولات وارداتی از جمله نرم‌افزار، سخت‌افزار و محصولات شبکه، شکاف‌های امنیتی نهفته و آشکاری دارند؛ بنابراین، نهادهای پژوهشی امنیت سایبری در کشور برای برآورده‌سازی این امر بسیار پراهمیت هستند. از جمله موارد پراهمیت، خط‌مشی‌گذاری مناسب برای رویارویی موفق با تهدیدات این حوزه در کشور است. استفاده از شبکه به‌معنای استفاده متناسب از همهٔ ظرفیت‌ها، راه‌حلی مناسب برای حاکمیت محسوب می‌شود. در دهه‌های گذشته، واژه‌های شبکه یا شبکه‌سازی در بیش‌تر مباحث مدیریت دولتی و خط‌مشی‌گذاری عمومی متداول شده است. در واقع، علت این امر پیشرفت‌های اجتماعی، سازمانی و فناورانه بوده است. جامعهٔ شبکه‌ای، ساختاری از شبکه‌های سازمانی و اجتماعی دارد که همهٔ فضاهای جامعه را درنظر می‌گیرد. به‌طورکلی، در بسیاری از راهکارهای پیشنهادی برای بازسازی دولت، همگی بر تمرکززدایی دولت و وابستگی با سایر شرکا در جامعه و خصوصی کردن فعالیت‌های دولت تأکید کرده‌اند؛ چراکه شبکه‌ها هماهنگی و کنترل فعالیت‌های دولت را ارتقاء می‌دهند. بر این اساس، شیوهٔ حاکمیت شبکه‌ای نسبت به شیوه‌های رایج با ویژگی‌های عصر فعلی متناسب است. مسأله مهم در حاکمیت شبکه‌ای یا به بیان دیگر حاکمیت از طریق شبکه، چگونگی مفهوم‌سازی، پیکره‌بندی و مدیریت شبکه‌ای از تأمین‌کنندگان[3] عمومی، خصوصی و غیرانتفاعی به‌گونه‌ای است که برای شهروندان یا به بیانی، گیرندگان خدمات ایجاد ارزش نماید (Eggers, 2005). همان‌گونه که بیان شد، از تهدیدات همیشگی و پیش‌روی کشور و به‌عنوان پنجمین صحنهٔ نبرد (در کنار صحنه‌های هوایی، زمینی، دریایی و فضایی) امنیت در فضای سایبر است که به لحاظ تغییرات مستمر در این حوزه و لزوم بومی‌سازی محصولات برای حفظ امنیت ملی کشور نیازمند مدلی برای حاکمیت بر نهادهای پژوهشی در این حوزه است.

در ایران با وجود نهادهای مختلف از جمله دولتی و خصوصی، همسویی میان آن‌ها دیده

1. Centrifuge
2. Stuxnet
3. Providers

نمی‌شود و با وجود صرف بودجهٔ کلان در این حوزه بعد از گذشت حداقل ۱۰ سال همچنان پراکندگی و نبودِ هم‌افزایی در این نهادها مشهود است و به لحاظ پژوهشی، پیشرفتی ناچیز در این حوزه است؛ همان‌طور که در ابتدای بیان مسأله اشاره گردید، بدون حاکمیت شبکه‌ای مدیریت بر این فضا ممکن نیست؛ بنابراین، هدف اصلی این پژوهش ارائهٔ مدل حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری در کشور است. برای رسیدن به این الگو از نظریهٔ داده‌بنیاد استفاده می‌شود. در این پژوهش ابتدا مفاهیم حاکمیت، حاکمیت شبکه‌ای تشریح می‌شود و در ادامه با استفاده از روش تحلیل داده‌بنیاد مدلی در این زمینه ارائه می‌گردد.

مفهوم حاکمیت[1]

حاکمیت موضوعی دربارهٔ شیوهٔ تعامل دولت‌ها و دیگر سازمان‌های اجتماعی با یکدیگر، شیوهٔ ارتباط آن‌ها با شهروندان و شیوهٔ گرفتن تصمیمات در جهانی پیچیده است. حاکمیت فرآیندی است که از آن طریق جوامع یا سازمان‌ها تصمیمات مهم خود را می‌گیرند و مشخص می‌کنند چه کسانی در این فرآیند درگیر شوند و چگونه وظیفهٔ خود را به انجام برسانند. (کاملی و الوانی، ۱۳۹۰). سیستم حاکمیت، چارچوبی است که فرآیند متکی بر آن، بدین معناست که مجموعه‌ای از توافقات، رویه‌ها، قراردادها و سیاست‌ها را مشخص می‌کنند که قدرت در دست چه کسی باشد و تصمیمات چگونه اتخاذ و وظایف چگونه انجام شوند (Folke, Hahn, Olsson & Norberg, 2005).

انواع حاکمیت

همان‌گونه که بیان شد، امروزه حاکمیت به یک فرآیند جدید در اداره حکومت یا شرایط تغییریافته از قانون ابلاغی یا روشی جدید که در آن جامعه اداره می‌شود، اشاره می‌کند (Rhodes, 2007). برحسب این تعریف، نوع‌شناسی‌های مختلفی دربارهٔ حاکمیت ارائه شده است و هریک از نظریه‌پردازان به طبقه‌بندی متفاوتی دست یافته‌اند. اَشکالی مختلف برای حاکمیت بیان شده است؛ حاکمیت مشترک، حاکمیت مدیریت دولتی جدید، حاکمیت خوب، حاکمیت به‌عنوان وابستگی متقابل بین‌المللی، حاکمیت سایبرنتیک اجتماعی، حاکمیت اقتصاد سیاسی جدید و حاکمیت شبکه‌ای (Rhodes, 1996; O'Brien, 2015). همهٔ این مفاهیم دارای این ایدهٔ مشترک هستند و آن حاکمیت بدون نقش فقط دولت است (Rhodes, 1996).

برای دست‌یابی به انواع مدل‌های حاکمیت، با بررسی پیشینهٔ ادبیات دربارهٔ مفهوم حاکمیت، به

1. Governance

نوع‌شناسی به شرح زیر می‌توان دست یافت:

الف. از بُعد سیاست‌گذاری[1]، در این بُعد، حاکمیت به‌عنوان حالتی از ادارهٔ سیاسی تعریف می‌گردد و با ابزارهای اداره متمایز می‌شود. دولت می‌تواند با ابزارهایی نظیر فرماندهی و کنترل، مشوق‌ها و موجودی، اطلاعات، تشویق و تحریک به اهداف اجتماعی خاص خود برسد. در سیاست‌های زیست‌محیطی اتحادیه اروپا، برای مثال ابزارهای سیاست‌گذاری از جمله مقررات سلسله‌مراتب، ابزارهای کنترل بازار، امتیاز کشورهای عضو اکو، نظام‌های مدیریت زیست‌محیطی و موافقت‌های داوطلبانه است (Treib, Bähr & Falkner, 2005).

ب. از بُعد سیاست[2]، تمرکز بر قدرت ارتباط میان فعالان سیاسی است؛ به‌گونه‌ای که رودس (۱۹۹۷) از حاکمیت برای توصیف فرآیند تدوین خط‌مشی در زمان اشتراک قدرت میان عوامل دولتی و خصوصی استفاده نموده است. تدوین خط‌مشی در شبکه‌های درون‌سازمانی با وابستگی متقابل و تبادل منابع صورت می‌گیرد. برخی پژوهشگران بر بُعد سیاست از حاکمیت تأکید می‌کنند و حاکمیت شبکه‌ای را نوع غالبی از حاکمیت می‌دانند که با دولتی‌گرایی[3]، پلورالیسم[4] (ائتلافی) و اتحادیه[5] متمایز است (Treib, Bähr & Falkner, 2005). معیار مهم در تشخیص تمایز انواع حاکمیت روابط میان بخش خصوصی و عمومی در خط‌مشی‌گذاری است.

پ. از بُعد طرز حکومت و اداره[6]، در این بُعد، حاکمیت به‌عنوان نظامی از قوانین است که اقدامات بازیگران را طراحی می‌کند. حالات مختلف در این بُعد از تعریف حاکمیت در دو نوع مخالف بازار و سلسله‌مراتب منعکس می‌گردد. میان این دو نوع می‌توان حالت‌هایی مختلف نظیر انجمن، اتحادیه‌ها و شبکه‌ها را نام برد. در هر صورت، شکل ترکیبی معمولاً باعث ایجاد هماهنگی مؤثر در حاکمیت می‌گردد (Rosenau, 1992).

---

1. Policy
2. Politics
۳. Statism (تمرکز قدرت اقتصادی در دولت مرکزی)
4. Pluralism
5. Corporatism
6. Polity

حاکمیت شبکه‌ای[1]

اصطلاحات «سازمان شبکه‌ای»[2]، «شکل‌های شبکه‌ای سازمان»[3]، «شبکه‌های بین شرکتی»[4]، «شبکه‌های سازمان»[5]، «تخصص انعطاف‌پذیر»[6] و «شبه شرکت‌ها»[7] به‌طور مکرر و تا حدی به‌صورت استعاری مورد استفاده قرار گرفته‌اند تا به هماهنگی میان سازمان‌ها اشاره کنند که با نظام‌های اجتماعی سازمانی یا غیررسمی مشخص می‌شوند. برخلاف ساختارهای بوروکراتیک درون شرکت‌ها و روابط قراردادی رسمی میان آن‌ها این شکل از هماهنگی بین شرکتی را «حاکمیت شبکه‌ای» می‌نامند (Jones, Hesterly & Bor, 1997). ریشه‌های حاکمیت شبکه‌ای را می‌توان در دهه‌های ۱۹۵۰ و ۱۹۶۰ با ظهور پدیدهٔ «سرمایه‌داری دانش»[8] یافت. ظرفیت شبکه‌ای شدن در واقع، مبنای اساسی این ایده را تشکیل می‌دهد (خواجه نائینی، ۱۳۹۳). حاکمیت شبکه‌ای ممکن است دارای مفاهیمی متضاد باشد؛ عبارت شبکه، حمل بر مفهوم می‌شود که آن خودبه‌خود[9]، باز، مسطح و گوناگون[10] است؛ حاکمیت نیز از سوی دیگر به معنای هدایت، هماهنگی و حتی راهبری تعبیر می‌شود. با توجه به گسترش ادبیات بیش‌ترین تفسیر در خصوص ادبیات مدیریت دولتی معاصر بر روش حاکمیت شبکه‌ای، مدیریت شبکه و فراحاکمیت[11] گسترش می‌یابد (Hertting & Vedung, 2012). حاکمیت شبکه‌ای یک «شکل متفاوت از هماهنگی فعالیت اقتصادی» را تشکیل می‌دهد که برخلاف ساختار بازارها و سلسله‌مراتب است (یا با آن رقابت می‌کند) (Jones, Hesterly & Bor, 1997).

در جدول (۱) تعاریفی در مورد حاکمیت شبکه‌ای از دیدگاه پژوهشگران این حوزه ارائه می‌گردد:

1. Network Governance
2. Network Organization
3. Networks Forms of Organization
4. Inter-firm Networks
5. Organization Networks
6. Flexible Specialization
7. Quasi-Firms
8. Knowledge Capitalism
9. Spontaneous
10. Protean
11. Meta-Governance

جدول ۱: عبارات و تعاریف مختلف از حاکمیت شبکه‌ای

مرجع	اصطلاح	تعریف حاکمیت شبکه‌ای
آلتر و هیج[1] ۱۹۹۳	شبکه‌های بین سازمانی	خوشه‌های نامحدود یا محدود از سازمان‌هایی که بنابر تعریف، مجموعه‌های غیر سلسله‌مراتبی از واحدهایی هستند که از نظر قانونی مجزا هستند.
دوبینی و آلدریخ[2] ۱۹۹۱	شبکه‌ها	روابط تبدیل‌شده به الگو میان افراد، گروه‌ها و سازمان‌ها
گرلاخ و لینکولن ۱۹۹۲	سرمایه‌داری متحد	روابط راهبردی و بلندمدت در میان طیف گسترده‌ای از بازارها
گرانووتر[3] ۱۹۹۴، ۱۹۹۵	گروه‌های تجاری[4]	مجموعه‌هایی از شرکت‌ها که به صورت‌های رسمی یا غیررسمی به هم متصل هستند، با یک سطح متوسط از اتصال
کرینر و شولتز[5] ۱۹۹۳	شبکه‌ها	همکاری‌های بین سازمانی غیررسمی
لارسون[6] ۱۹۹۲	شکل‌های سازمانی شبکه	مبادلات بلندمدت تکرارشونده که وابستگی‌های متقابلی ایجاد می‌کند که بر درگیر کردن و شامل کردن تعهدات، انتظارات، اعتبارها و منافع دوجانبه تکیه دارد.
لیبسکایند، الیور، زوکر و بروور[7] ۱۹۹۶	شبکه‌های اجتماعی	جامعیت افرادی که در میان آن‌ها مبادلاتی رخ می‌دهد که فقط توسط معیارهای مشترک رفتار اعتماد برانگیز تأیید می‌شوند.
مایلز و اسنو[8] ۱۹۸۶، ۱۹۹۲	سازمان‌های شبکه‌ای	دسته‌هایی از شرکت‌ها یا واحدهای اختصاصی که با سازوکارهای بازار هماهنگ می‌شوند.
پاول[9] ۱۹۹۰	شکل‌های شبکه‌ای سازمان	الگوهای جانبی یا افقی از مبادله: جریان مستقل منابع؛ خطوط ارتباط دوجانبه

منبع: (Jones, Hesterly & Bor, 1997)

سیر تطور تاریخی در ادارهٔ کشورها نشان می‌دهد که دولت‌ها برای دست‌یابی به اهداف عمومی و ارائهٔ خدمات عمومی به شهروندان با شرکت‌های خصوصی، انجمن‌ها و سازمان‌های غیرانتفاعی همکاری مبتنی بر اعتماد متقابل ایجاد می‌کنند (دانایی‌فرد، ۱۳۹۲). حاکمیت شبکه‌ای نتیجهٔ تعاملاتی است که

1. Alter & Hage
2. Dubini & Aldrich
3. Granovetter

۴. گروه‌های تجاری که با شبکه‌های همکاری متمایز می‌شوند.

5. Gerlach & Lincoln
6. Larson
7. Liebeskind, Oliver, Zucker & Brewer
8. Miles & Snow
9. Powell

در آن شهروندان یا بازیگران آگاه ازجمله سازمان‌های اجتماعی برای انتقال اطلاعات مرتبط با اهداف اجتماعی برای اتخاذ تصمیمات مطلوب به سازمان‌های دولتی کمک می‌کنند (Maturo, 2004).

همان‌گونه که بیان شد، حاکمیت شبکه‌ای در تعاریف مختلفی به‌کار گرفته شده است؛ اما اشتراک همهٔ تعاریف نشان می‌دهد که حاکمیت شبکه‌ای مدلی در اختیار سیاست‌گذاران است که به‌وسیلهٔ آن می‌توانند با مسائل بغرنج[1] روبه‌رو شوند. مسائلی که زمان کمی برای پاسخ‌گویی به آن‌ها وجود دارد، همان‌گونه که بیان شد، هزینهٔ مبادله و شکست بالایی دارند، برای شهروندان (کاربران) حیاتی است و بازیگران از طیف‌های مختلف در حل آن نقش ایفا می‌کنند (Kettl, 2005). حاکمیت شبکه‌ای درواقع یک شکل مطلوب ادارهٔ امور است که با فراهم بودن زمینهٔ مشارکت برقرار می‌شود و به‌عنوان راه‌حلی است که در پی تغییر و بهبود تعاملات سازمان است (Lester & Reckhow, 2012). در این‌جا مفاهیمی نظیر «تسهیم منافع مشترک»، «برقراری و هماهنگی ارتباطات مطلوب»، «تقویت اعتماد»، «تعاملات غیررسمی نهادها»، «مذاکرات تعاملی» از اهمیتی به‌سزا برخوردار است. در این‌جا حاکمیت از طریق شکل‌های تعاملی اداره صورت می‌گیرد که بازیگران زیادی به ایفای نقش می‌پردازند و تعاملات آن‌ها به گونه‌ای افزایش می‌یابد که یک الگوی به‌نسبت پایدار و هماهنگی به‌وجود می‌آورد (خواجه نائینی، ۱۳۹۳). بنابراین، حاکمیت نتیجهٔ هم قوانین رسمی (مثل سیاست‌ها، نرم‌ها، قوانین و...) و هم تعاملات غیررسمی بازیگران در شبکه است که منجر به ارتقای پاسخ‌گویی جمعی به مسائل و مشکلات محیطی می‌گردد (Huitema *et al*., 2009). با توجه به این‌که این پژوهش به دنبال مدل حاکمیت شبکه‌ای است، با بررسی مدل‌های مختلف حاکمیت شبکه‌ای که در ادبیات نظری این موضوع آمده است، به عناصر شکل‌گیری حاکمیت شبکه‌ای در جدول (۲) اشاره می‌شود:

۱. Wicked Problems مسائلی که راه‌حل‌های روتین ندارد.

جدول۲: بررسی تطبیقی عناصر شکل‌گیری حاکمیت شبکه‌ای

پژوهشگر	سال	عناصر مدل حاکمیت شبکه‌ای				
سورنسن[1] و ترفینگ[2]	۲۰۰۹	طراحی شبکه	شکل‌گیری شبکه	مدیریت شبکه	مشارکت در شبکه	
گلداسمیت[3] و ایگرز[4]	۲۰۰۴	تدوین راهبرد شبکه	طراحی و فعال‌سازی شبکه	سرمایه انسانی شبکه	یکپارچه‌سازی شبکه	ارزیابی عملکرد شبکه
بُک تِیکیم[5]	۲۰۰۹	پیکربندی شبکه	هماهنگی شبکه	خودتنظیمی شبکه		
دانایی‌فرد	۲۰۱۴	تدوین راهبرد شبکه	شبکه‌ای کردن شبکه	طراحی شبکه	انتخاب شرکای مناسب	

همان‌طور که ملاحظه گردید، در مرور ادبیات، تلاش شد با توجه به اهداف این پژوهش، مطالعات به نسبت جامعی از انواع و عناصر حاکمیت شبکه‌ای انجام شود. بر اساس مطالعهٔ انجام‌شده و با توجه به جمع‌بندی صورت گرفته، عناصر، تدوین راهبرد شبکه، طراحی و فعال‌سازی شبکه، مدیریت شبکه، مشارکت و یکپارچه‌سازی و ارزیابی عملکرد شبکه، تقریباً پوشش‌دهندهٔ عناصر شکل‌گیری حاکمیت شبکه‌ای است. در کنار آن برای بررسی عوامل زمینه‌ایِ شکل‌گیری این مدل از الگوی PEST[6] (عوامل سیاسی، اقتصادی، اجتماعی و فناورانه) بهره گرفته که در شکل (۱) ارائه شده است.

1. Sorensen
2. Torfing
3. Goldsmith
4. Eggers
5. Bok-Tae Kim
6. PEST Analysis (Political, Economic, Social & Technological)

شکل ۱: چارچوب نظری پژوهش

با توجه به مطالب گفته‌شده، این پژوهش در پی پاسخ به این پرسش اساسی است که:
مدل مناسب حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت فضای سایبر چیست؟
این مدل باید به پرسش زیر هم پاسخ دهد:
۱. عناصر حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت فضای سایبر کدام هستند؟
۲. شرایط زمینه‌ای مؤثر در سیاست‌گذاری نهادهای پژوهشی امنیت‌سایبری کدام هستند؟

روش پژوهش

در این پژوهش از روش کیفی استفاده شده است و از میان راهبردهای مختلف پژوهش کیفی از راهبرد داده‌بنیاد بهره‌مند شده است. چون مرور پژوهش‌های پیشین حکایت از ضعف نظریه‌های موجود در تبیین پدیدهٔ موردنظر دارد، به‌کارگیری نظریهٔ داده‌بنیاد توجیه‌پذیر به‌نظر می‌رسد. سه مرحلهٔ اساسی در این روش که شامل کدگذاری باز، کدگذاری محوری و کدگذاری انتخابی است، در این پژوهش تشریح می‌گردد (دانایی‌فرد و امامی، ۱۳۸۶).

در پژوهش حاضر، به‌منظور ثبت داده‌ها، پس از گرفتنِ مجوزهای لازم، همهٔ مصاحبه‌ها به

شکل صوتی ضبط شد؛ در مرحلهٔ بعد مصاحبه‌ها به‌طور کامل پیاده و در قالب Word فایل‌ها وارد نرم‌افزار MAXQDA10 گردید.

در این پژوهش، انتخاب مصاحبه‌شوندگان به‌صورت هدفمند (نمونه‌گیری جهت‌دار یا نظری) یا به‌صورت گلوله برفی بوده است. در هر مرحله فرآیند جمع‌آوری داده‌ها تا جایی ادامه پیدا می‌کند که به اشباع نظری رسیده شود و مطلب جدیدی به مدل اضافه نگردد. نمونه‌گیری نظری بهترین روش برای توسعهٔ یک نظریه است. در نمونه‌گیری نظری، مصاحبه‌های عمیق با خبرگان تا جایی پیش می‌رود که به حد اشباع نظری می‌رسد. این پژوهش با مصاحبه با ۱۶ نفر[۱] به اشباع و کفایت نظری دست یافته است. مصاحبه‌شوندگان از میان سیاست‌گذاران و مدیران ارشد اجرایی در نهادهای پژوهشی حاکمیتی (نظامی و دولتی) و خصوصی، صاحب‌نظران و اعضای هیأت علمی مؤثر امنیت سایبری در کشور انتخاب شده‌اند.

اعتمادپذیری یافته‌های پژوهش

بیش‌تر روش‌شناسان کیفی به‌جای استفاده از واژه‌های روایی و پایایی که از لحاظ مبانی فلسفی ریشه در روش‌های کمّی دارند، از معیار اعتمادپذیری یا قابلیت اعتماد برای بررسی ارزیابی کیفیت نتایج پژوهش کیفی استفاده می‌کنند (Twining, 2000). گوبا و لینکلن قابلیت اعتماد را شامل چهار معیار قابل قبول بودن، انتقال‌پذیری، قابلیت اطمینان و تأییدپذیری می‌دانند (Lincoln & Guba, 1985). در این پژوهش از راهبردهای جدول (۳) برای تأمین اعتمادپذیری استفاده گردید.

۱. اطلاعات مصاحبه‌شوندگان نزد پژوهشگران محفوظ است.

جدول ۳: روش‌های تأمین اعتمادپذیری در پژوهش حاضر

معیار	زیرمعیارها		راهبرد تأمین	اقدام صورت‌گرفته
قابل‌قبول بودن	روایی ورودی‌های پژوهش	روایی داده‌های ورودی پژوهش	نمونه‌گیری گلوله‌برفی (نیومن، ۲۰۰۰، ۱۹۹)	معرفی مصاحبه‌شوندگان بعدی توسط مصاحبه‌شوندگان پیشین
			نمونه‌گیری بر مبنای اعتبار (اسنو، هاچسون و پراتر، ۱۹۸۱)	انتخاب مصاحبه‌شوندگان بر اساس توصیه متخصصان
	روایی تحلیل‌های انجام‌شده در پژوهش	روایی توصیفی (مکسول، ۱۹۹۲)	بازخور مشارکت‌کننده	ارائه بازخورد توصیفی مصاحبه به مصاحبه‌شونده و دریافت نظرات اصلاحی
		روایی تفسیری (ماکسول، ۱۹۹۲)	استفاده از توصیف‌گرهای با حداقل مداخله	بهره‌گیری از عبارات توصیفی مانند نقل‌قول در تفسیرها
	انتقال‌پذیری		استفاده از روش نمونه‌گیری بر مبنای اعتبار	انتخاب مصاحبه‌شوندگان از بین افراد معتبر مدیران ارشد نظامی و دولتی و خصوصی در پژوهش‌های امنیت سایبری
			وصف تفصیلی همه جزئیات	ارائهٔ یک تصویر مفصل از زمینه‌ای که پژوهش در آن انجام شده
	قابلیت اطمینان		ممیزی قابلیت اطمینان (توینینگ، ۲۰۰۰، ۱۰)	در اختیار گذاشتن داده‌ها، روش‌ها و تصمیمات با هدف بازبینی و موشکافی پژوهش توسط دیگر پژوهشگران
	تأییدپذیری		ارائهٔ جزئیات روش‌ها و داده‌های پژوهش	ارائهٔ گزیدهٔ مصاحبه‌ها و نیز توضیح روند تحلیل داده‌ها تا دست‌یابی به نتایج پژوهش

تجزیه‌وتحلیل و یافته‌های پژوهش

کدگذاری باز

در نظریهٔ داده‌بنیاد، فرآیند تحلیل داده‌ها با کدگذاری باز آغاز می‌شود. کدگذاری باز فرآیندی تحلیلی است که طی آن مفاهیم شناسایی‌شده و ویژگی‌ها و ابعاد مربوط به هر مفهوم کشف می‌شود. در کدگذاری باز رخدادهای مشاهده شده در داده‌ها نام‌گذاری می‌شوند. در این مرحله، دو فعالیت کلیدی شامل مفهوم‌سازی و مقوله‌بندی وجود دارد.

مفهوم‌سازی

شکل‌گیری یک نظریه با مفهوم‌سازی آغاز می‌شود. مفهوم‌سازی به کوشش پژوهشگر برای کاوش عمیق در یک مشاهده، جمله، بند (پاراگراف) یا یک صفحه و برگزیدن یک نام برای هر رویداد یا اتفاق اطلاق می‌شود. پژوهشگر کمک می‌کند تا رخدادها، ایده‌ها یا رویدادهای مشابه را با نامی واحد یا در قالب دسته‌ای واحد گروه‌بندی کند. پدیده‌هایی که برای آن‌ها اسمی انتخاب می‌شود را در اصطلاح مفهوم می‌نامند. مفاهیم زیربنای نظریه به‌حساب می‌آیند.

مقوله‌بندی

هنگامی‌که داده‌ها باز شد و مفاهیم از درون آن‌ها سر برآورد، پژوهشگر به دنبال مصداق‌هایی می‌گردد که بتواند با کمک آن‌ها، مفاهیم را در قالب مقوله‌هایی دسته‌بندی کند. بنابر دیدگاه اشتراوس و کوربین[1] (۱۹۹۸) برخی مفاهیم را می‌توان در قالب مقوله‌ای که از انتزاع بالاتری نسبت به آن مفاهیم برخوردار است، دسته‌بندی نمود. به کمک مقوله‌ها می‌توان چیزهای در حال رخداد را توصیف کرد. در جدول (۴) شیوهٔ شکل‌گیری یکی از مقوله‌های اصلی قابل مشاهده است:

جدول ۴: نمونه‌ای از شیوهٔ شکل‌گیری مقولهٔ شرایط زمینه‌ای مؤثر در نهادهای پژوهشی امنیت سایبری

مقوله اصلی	مقوله‌های فرعی	کدگذاری باز	گزاره کلامی
شرایط زمینه‌ای مؤثر در سیاست‌گذاری پژوهش‌های امنیت سایبری	شرایط فناورانه	سرعت تغییرات فناوری در امنیت سایبری	فضای امنیتی سایبر و تهدیدات به‌سرعت تغییر می‌یابد. ظرفیت اینترنت افزایش یابد. ظهور اینترنت اشیا
	شرایط مالی و اقتصادی	حمایت از نهادهای پژوهشی	حاکمیت به‌جای توانمندسازی، جهت‌دهی بکند؛ چون توانمندسازی توسط خود مجموعه‌ها باید کار کند؛ البته می‌توان تسهیلاتی داد که به فرآیند توانمندسازی آن‌ها کمک شود.
		اعتبارات در امنیت سایبری	وضعیت بودجه‌ای در امنیت سایبری مناسب نیست؛ در بعضی جاها برحسب نظر مدیر از بودجه‌های دیگری به امنیت سایبری تخصیص می‌یابد؛ اما برای نمونه، در بودجه برنامه ۹۶ جایگاهی ندارد.

1. Strauss & Corbin

در پژوهش حاضر در مرحلهٔ کدگذاری باز از مجموع ۱۶ مصاحبه، ۵۴۷ کد توصیفی استخراج شد که به روش نظام‌مندی که در شرح بالا ذکر شد، مورد تجزیه‌وتحلیل قرار گرفتند و در قالب ۶۰ مضمون توصیفی بدون تکرار نمایان شدند. در جدول (۵) نحوهٔ شکل‌دهی مقوله‌های فرعی و شکل‌دهی آن‌ها به مقوله‌های اصلی نشان داده شده است.

جدول ۵: ساخت مقولات اصلی و مقولات فرعی

ردیف	مقوله‌های اصلی	مقوله‌های فرعی	میزان فراوانی کدهای باز
۱	عناصر حکمرانی شبکه‌ای	سیاست‌های کلان	۱۸۴
		طراحی و فعال‌سازی	۶۹
		مدیریت شبکه	۱۷
		توانمندسازی و مشارکت	۱۳
		ارزیابی عملکرد	۱۷
۲	شرایط زمینه‌ای مؤثر در سیاست‌گذاری نهادهای پژوهشی امنیت سایبری	شرایط فناورانه	۱۷
		شرایط مالی و اقتصادی	۳۴
		شرایط سیاسی و قانونی	۴۰
		شرایط اجتماعی و فرهنگی	۵۳
۳	نهادهای مؤثر در سیاست‌گذاری پژوهش‌های امنیت سایبری	نهادهای بین‌المللی امنیت سایبری	۱۴
		نهادهای سیاست‌گذار	۲۷
		نهادهای پژوهشی حاکمیتی	۱۱۷
		نهادهای پژوهشی خصوصی	۳۶
		نهادهای بهره‌بردار امنیت سایبری	۹

مقولهٔ حاکمیت شبکه‌ای

توضیح‌های مصاحبه‌شوندگان در پاسخ به پرسش‌های مربوط به حاکمیت شبکه‌ای، منجر به شناسایی کدهای باز جدول (۶) شده است؛ گفتنی است که اعداد داخل جدول خروجی نرم‌افزار MAXQDA10 نشان‌دهندهٔ میزان فراوانی کدهای بیان شده از سوی مصاحبه‌شوندگان است.

جدول ۶: کدگذاری باز مربوط به حاکمیت شبکه‌ای

ردیف	کدگذاری اولیه	مقوله‌های فرعی
۱	فرآیند سیاست‌گذاری در امنیت سایبری [۳۴]	
۲	محصولات راهبردی امنیت سایبری [۱۳]	
۳	عدم هماهنگی در کشور در امنیت سایبری [۷]	
۴	هماهنگ‌سازی نهادهای پژوهشی امنیت سایبری [۲۷]	
۵	سیاست‌گذاری امنیت سایبری [۵۹]	
۶	رصد تهدیدات و وضعیت پژوهش‌های سایبری [۱۴]	سیاست‌های کلان [۱۸۴]
۷	به‌وجود آمدن الزام برای پژوهش‌های بومی [۲]	
۸	تدوین راهبرد و اسناد بالادستی [۱۳]	
۹	سیاست‌گذاری آموزش امنیت سایبری در ایران [۶]	
۱۰	سیاست‌گذاری بخشی [۶]	
۱۱	اهمیت اسناد راهبردی [۳]	
۱۲	فرایندهای ایجاد نیاز پژوهشی [۲۵]	
۱۳	فعال‌سازی نهادهای پژوهشی [۱۴]	
۱۴	جهت‌دهی پژوهش‌های امنیت سایبری [۸]	
۱۵	اصلاح فرایندهای حمایتی از پژوهش‌های امنیت سایبری [۱۳]	طراحی و فعال‌سازی [۱۲۹]
۱۶	فرآیند پژوهش و تولید [۴]	
۱۷	ساختارهای نامناسب در حاکمیت [۱]	
۱۸	طراحی شبکه با حفظ منافع همه [۴]	
۱۹	تعهد مدیریتی [۱۵]	مدیریت شبکه [۱۷]
۲۰	ارتباط تعاملی با همه بخش‌ها [۲]	
۲۱	توانمندسازی بخش خصوصی [۱۲]	توانمندسازی و مشارکت [۱۳]
۲۲	توانمندسازی شبکه [۱]	
۲۳	ایجاد فرآیندهای ارزیابی دقیق [۲]	
۲۴	ایجاد فرآیندهای نظارتی دقیق [۱۱]	ارزیابی عملکرد [۱۷]
۲۵	ارزیابی توان نهادهای پژوهشی در مقابل تهدیدات سایبری [۴]	

مقولهٔ شرایط زمینه‌ای مؤثر در سیاست‌گذاری نهادهای پژوهشی امنیت سایبری

توضیح‌های مصاحبه‌شوندگان در پاسخ به پرسش‌های مربوط به شرایط زمینه‌ای مؤثر در سیاست‌گذاری نهادهای پژوهشی امنیت سایبر، منجر به شناسایی کدهای باز جدول (۷) شده است؛

همان‌طور که ملاحظه می‌شود، ۱۴۵ کد باز مربوط به شرایط زمینه‌ای است که از خروجی نرم‌افزار MAXQDA استخراج شده است.

جدول ۷: کدگذاری باز مربوط به شرایط زمینه‌ای مؤثر در سیاست‌گذاری نهادهای پژوهشی امنیت سایبر

ردیف	کدگذاری اولیه	مقوله‌های فرعی
۱	سرعت تغییرات فناوری در امنیت سایبری [۵]	شرایط فناورانه [۱۷]
۲	اهمیت فناوری‌های بومی در امنیت سایبری [۱۱]	
۳	سطح فنّاوری در امنیت سایبری [۱]	
۴	حمایت از نهادهای پژوهشی [۱۴]	شرایط مالی و اقتصادی [۳۴]
۵	اعتبارات در امنیت سایبری [۱۲]	
۶	فعال کردن بازار امنیت سایبری [۵]	
۷	بازار امنیت سایبری [۳]	
۸	امکانات و ظرفیت بالای امنیت سایبری در کشور [۱]	
۹	الزامات نانوشته [۴]	شرایط سیاسی و قانونی [۴۰]
۱۰	الزامات قانونی و رسمی [۲۲]	
۱۱	قاطعیت در حاکمیت [۲]	
۱۲	سیاست‌زدگی در سیاست‌گذاری [۵]	
۱۳	خط‌مشی‌های برخورد با بخش خصوصی [۱]	
۱۴	نظام‌های قراردادی صحیح [۳]	
۱۵	تغییرات مدیریتی در بخش دولتی [۲]	
۱۶	مشروعیت به نهادهای خصوصی [۱]	
۱۷	ایجاد دغدغه و فرهنگ امنیت در کشور [۱۶]	شرایط اجتماعی و فرهنگی [۵۳]
۱۸	فرهنگ پژوهش و تولید [۹]	
۱۹	تغییر فضای اجتماعی [۴]	
۲۰	فضای مجازی و امنیت آن در جامعه شهروندی [۴]	
۲۱	فرهنگ شهروندی در فضای مجازی [۳]	
۲۲	روند رو به رشد استفاده از شبکه‌های اجتماعی [۳]	
۲۳	عوامل فرهنگی مؤثر در امنیت سایبری [۳]	
۲۴	اصلاح فرهنگ بخش دولتی [۵]	
۲۵	مهندسی اجتماعی [۶]	

مقولهٔ نهادهای مؤثر در سیاست‌گذاری پژوهش‌های امنیت سایبر

توضیح‌های مصاحبه‌شوندگان در پاسخ به پرسش‌های مربوط به نهادهای مؤثر در سیاست‌گذاری پژوهش‌های امنیت سایبر، منجر به شناسایی کدهای باز جدول (۸) شده است؛ همان‌طور که ملاحظه می‌شود، ۱۵۷ کد باز مربوط به این نهادها است که از خروجی نرم‌افزار MAXQDA استخراج شده است.

در تقسیم‌بندی نهادهای مؤثر در پژوهش‌های امنیت سایبری، با توجه به مصاحبه‌های صورت گرفته، نهادهای سیاست‌گذار، نهادهای بهره‌بردار، نهادهای پژوهشی حاکمیتی، نهادهای پژوهشی خصوصی و نهادهای بین‌المللی مطرح هستند. دانشگاه‌ها و مراکز پژوهشی هم که به‌عنوان نهادهای غیرانتفاعی در ادبیات بیان شده‌اند، به دلیل این‌که متأثر از سیاست‌های حاکمیت است می‌توان در زمرهٔ نهادهای پژوهشی حاکمیتی و نهادهای سیاست‌گذار تقسیم‌بندی نمود. همان‌طور که بیان شد، منظور از حاکمیت نهادی است که متأثر از سیاست‌های نظام است حال دولتی می‌تواند باشد یا نظامی.

جدول ۸: کدگذاری باز مربوط به نهادهای مؤثر در سیاست‌گذاری پژوهش‌های امنیت سایبری

ردیف	کدگذاری اولیه	مقوله‌های فرعی
۱	وضعیت بین‌المللی امنیت سایبری [۶]	نهادهای بین‌المللی امنیت سایبری [۰]
۲	استفاده از نهادهای بین‌المللی در امنیت سایبری [۸]	
۳	نظام‌های مختلف مؤثر در امنیت سایبری [۶]	نهادهای سیاست‌گذار [۰]
۴	نهاد سیاست‌گذار در امنیت سایبری [۱۲]	
۵	نقش وزارت علوم در امنیت سایبری [۹]	
۶	نقش دانشگاه‌ها در امنیت سایبری [۲۸]	
۷	بازیگران پژوهشی در امنیت سایبری [۴۵]	نهادهای پژوهشی حاکمیتی [۰]
۸	نهادهای پژوهشی امنیت سایبری [۲۰]	
۹	نقش نهادهای پژوهشی دولتی [۲۴]	
۱۰	نهادهای خصوصی پژوهشی در امنیت سایبری [۳۶]	نهادهای پژوهشی خصوصی [۰]
۱۱	نهادهای بهره‌بردار امنیت سایبری [۸]	نهادهای بهره‌بردار امنیت سایبری [۰]

کدگذاری محوری: نظریه‌پردازی

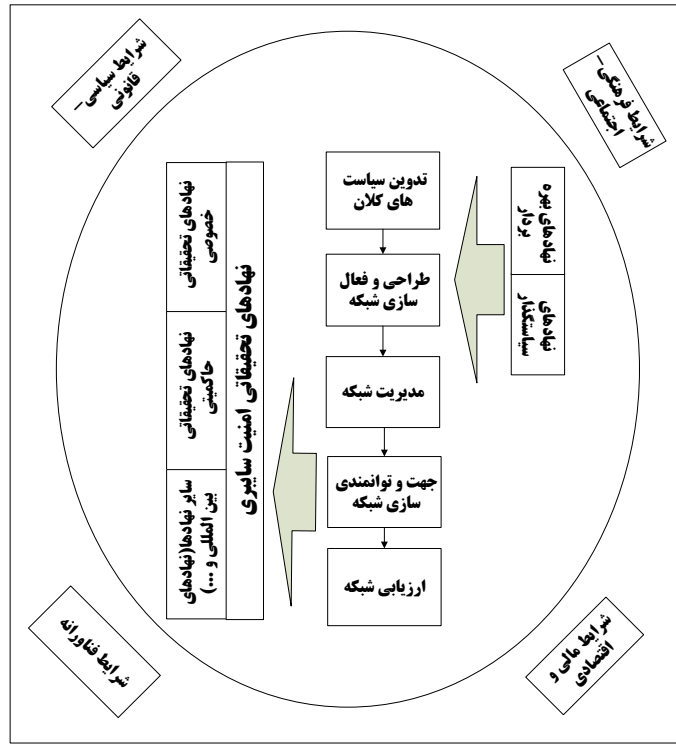
کدگذاری محوری، مرحلهٔ دوم تجزیه‌وتحلیل در نظریهٔ داده‌بنیاد است. هدف از این مرحله، برقراری ارتباط میان مقوله‌های تولیدشده در مرحلهٔ کدگذاری باز است. این پژوهش از رویکرد

خودظهور نظریهٔ داده‌بنیاد مدل گلاسر[1] و کوربین[2] (Glaser & Strauss, 1967) و بر اساس داده‌های جمع‌آوری شده در مصاحبه‌های عمیق میان بازیگران مهم نهادهای پژوهشی امنیت سایبری در کشور استفاده نموده است. در مدل گلاسر بر اهمیت ظهور یک نظریه از دل داده‌ها به‌جای استفاده از طبقه‌بندی معین از پیش تعیین شده نظیر آن‌چه در رویکرد پارادایمی، کدگذاری محوری (شرایط علّی، محتوا، شرایط مداخله‌گر، راهبردها و پیامدها) تأکید می‌کند. بنابراین، همان‌طور که در شکل (۲) مشاهده می‌شود، خروجی کدگذاری محوری، روابط میان طبقه‌ها را بدون مراجعه به یک نمودار یا تصویر نشان می‌دهد. خروجی این رویکرد به‌دنبال مدل حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری است؛ اساس این فرآیند، ارتباط‌دهی در کدگذاری محوری بر بسط و گسترش یکی از مقوله‌ها است که در شکل (۲) ارائه شده است. لازم به توجه است که در رویکرد مورد استفاده در این پژوهش (خودظهور) داده‌ها بر اساس چهار معیار (تناسب، عملی بودن، مناسب بودن و اصلاح‌پذیری) در درون طبقه‌ها قرار گرفته است. بنابراین، از فرآیندهای کدگذاری روش داده‌بنیاد موارد زیر به‌دست می‌آید:

۱. ساخت مقولات اصلی با توجه به مقولات فرعی و ایجاد ارتباط میان آن‌ها؛ در این بخش ابتدا نتایج مربوط به این کارکرد مرحلهٔ کدگذاری محوری ارائه شده است؛ به‌گونه‌ای که ۱۶ مقولهٔ فرعی ظهوریافته در جریان پژوهش در قالب دسته‌های انتزاعی‌تر طبقه‌بندی و ارتباط میان آن‌ها تبیین می‌شود.

۲. ایجاد شبکهٔ ارتباطی میان کل مقوله‌ها در قالب چند طبقه: همهٔ مقوله‌ها (از جمله فرعی و اصلی) در قالب «کدگذاری محوری» دربارهٔ یک مقولهٔ محوری سامان می‌یابند.

1. Glaser
2. Corbin



شکل ۲: حاکمیت شبکه‌ای بر اساس رویکرد خودظهور برای مقوله‌های اصلی

کدگذاری انتخابی: استخراج گزاره‌های نظری

نظریه‌پردازان داده‌بنیاد، نظریه‌ها را در سه قالب ممکن ارائه می‌دهند: ۱. الگوی کدگذاری بصری؛ ۲. مجموعه‌ای از قضایا (یا فرضیه‌ها) و ۳. داستانی به شکل روایی نگاشته می‌شود. در این پژوهش، نظریهٔ پژوهش در قالب گزاره‌های حکمی یا قضایای نظری که طی فرآیند کدگذاری انتخابی به‌دست آمده، بیان می‌شوند. در ادامه با استناد به اظهارات مصاحبه‌شوندگان به تشریح قضایا و نیز زیرقضیه‌های نظری بالا پرداخته می‌شود. این قضایا درواقع چکیده‌ای پرمغز از محتوای مفاهیم کدگذاری شده در پژوهش است و مبین شماری از مهم‌ترین عوامل مؤثر در این مدل حاکمیت است و به کمک این الگو می‌توان مسائل مهم در نهادهای پژوهشی امنیت سایبری در کشور را واکاوی و حل نمود.

قضایای نظری و تشریح آن

قضیه ۱. فعال‌سازی نهادهای پژوهشی امنیت سایبر در کشور نیازمند تدوین سیاست‌های یکپارچه از سوی نهاد حاکمیتی است.

سیاست‌گذاری کلان در امنیت سایبری از جمله مواردی است که در مصاحبه‌های صورت گرفته بیش‌ترین ارجاع را داشته است؛ دو مفهوم «سیاست‌گذاری امنیت سایبری» و «فرآیند سیاست‌گذاری امنیت سایبری» ازجمله مواردی است که در جمع ۹۳ ارجاع به خود اختصاص داده است که نشان‌دهندهٔ اهمیت مفهوم سیاست‌گذاری کلان در حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبر در ایران است. شاید بتوان گفت که توجه به این مفهوم از جمله نقاط کلیدی در حاکمیت نهادهای پژوهشی امنیت سایبر در کشور محسوب می‌شود؛ بنابراین، اهمیت یک نهاد حاکمیتی که بتواند سیاست‌گذاری یکپارچه‌ای برای نهادهای پژوهشی امنیت سایبر در کشور انجام دهد، مشخص می‌گردد. با توجه به ساختار موجود و ایجاد شورای عالی فضای مجازی از طرف مقام معظم رهبری (مد ظله) و پیروِ آن ایجاد مرکز ملی فضای مجازی با توجه به مأموریت ابلاغی می‌تواند پاسخ‌گوی این موضوع مهم باشد. بنابراین، می‌توان گفت بهترین نهادی که در کشور می‌تواند سیاست‌های کلان و یکپارچه برای فعال‌سازی نهادهای پژوهشی در امنیت سایبری وضع نماید، به‌گونه‌ای که نهادهای دیگر هم از آن پیروی کنند، مرکز ملی فضای مجازی است. اما نکاتی مهم برای این نهاد شایان بیان است که در زیرقضیه‌های تدوین‌شده می‌توان به آن اشاره نمود:

زیرقضیه ۱. فعال نمودن شبکه‌های پژوهشی امنیت سایبری در کشور مستلزم نهادینه شدن دغدغهٔ امنیت در کشور و بالارفتن درک و فرهنگ پژوهش در بدنهٔ حاکمیت است.

مهم‌ترین کلیدواژه‌ها در این زیرقضیه، «دغدغهٔ امنیت» و «درک و فرهنگ پژوهش» است. ابتدا در پاسخ به این پرسش که چرا این زیرقضیه به‌عنوان نخستین زیرقضیه در این قسمت مطرح شده است، حکایت از اهمیت این موضوع در سیاست‌گذاری امنیت سایبری و فعال نمودن پژوهش‌های امنیت سایبری در کشور دارد. نکته‌ای مهم که از درون مصاحبهٔ این افراد می‌توان برداشت نمود که به‌گونه‌ای به‌عنوان دردِ دل هم مطرح می‌شد، این است که دغدغه و اهمیت موضوع امنیت سایبری در بدنهٔ کشوری هنوز تبیین نشده است و بیش‌تر مدیران به این موضوع به‌عنوان یک موضوع لوکس نگاه می‌کنند؛ درحالی‌که بی‌توجهی به این موضوع می‌تواند بیش‌ترِ بسترهای حیاتی و حساس کشور را در معرض آسیب‌های جبران‌ناپذیری قرار دهد. این موضوع از جمله مواردی نیست که بنابر ضرب‌المثل «چو فردا شود، فکر فردا کنیم» بتوان به آن عمل نمود.

ایجاد بسترهای بومی و محصولات بومی امنیت سایبری، نیازمند برنامه‌ریزی بلندمدت در کشور است. بنابر نظر، بیش‌تر بسترهای ارائهٔ خدمات در کشور فاقد راه‌حل‌های امنیتی است و از بسترهای غیربومی استفاده می‌شود. فقدان دید مناسب امنیتی در کشور می‌تواند در بلندمدت آسیب‌های جدی برای ایران فراهم کند؛ البته هم‌اکنون هم حملات سایبری مختلفی بر زیرساخت‌های حیاتی کشور وارد شده است که آخرین مورد آن حملهٔ ویروس باج‌افزار موسوم به «واناکرای»[1] است. نکتهٔ مهم دیگری که در این زیرقضیه به چشم می‌خورد، «بالا رفتن درک و فرهنگ پژوهش در بدنهٔ حاکمیت» است. مشکل اصلی در این مورد، نبود دید پژوهشی در کشور است؛ بنابراین، برای رسیدن به محصولات بومی امنیت سایبری، نیاز به تغییر دید مدیران بر کارهای پژوهشی در این حوزه است. نکتهٔ مهم در این نظرها این است که نسبت به امور پژوهشی در کشور باید تغییر فرهنگ در مدیران تصمیم‌گیر در کشور ایجاد شود؛ به‌گونه‌ای که از نهادهای پژوهشی انتظار محصولات و سودآوری نداشته باشند و این نیازمند برنامه‌ریزی بلندمدت و تخصیص بودجه‌های مناسب پژوهشی است که در قضیه‌های بعدی مفصل‌تر توضیح داده می‌شود.

زیرقضیه ۲. ایجاد نظام آینده‌پژوهی پژوهشی امنیت سایبری به‌منظور دست‌یابی به نقشه راه فناوری و محصولات بومی (رصد تهدیدها همراه با تغییرات سریع فناوری).

یکی از معضلات در پژوهش‌های امنیت سایبری، نبودِ نقشهٔ راه محصول و فناوری مورد وثوق و تأیید است که فقدان آن، منجر به موازی‌کاری شرکت‌های نوپا در حوزهٔ محصولات شرکت‌های پیشین شده و این حوزه را دچار نابسامانی می‌نماید؛ به‌گونه‌ای که در برخی حوزه‌ها بیش از چند محصول وجود دارد و در بعضی موضوع‌ها محصول و خدمات مناسبی موجود نیست. نقشهٔ راه محصول و فناوری مورد تأیید و پذیرش که توسط متخصصان تهیه شده باشد و بر اساس روندهای پیشِ رو در حوزه‌های بالادستی امنیت سایبری از جمله توسعهٔ شبکه‌های ارتباطی ملی و بخشی در کشور و همچنین با نگاه به محصولات امنیت سایبری شرکت‌های بزرگ در دنیا و مطالعهٔ روندهای جهانی تهیه شده باشد، سند بالادستی ارزشمندی است که در تنظیم برنامه‌ها و حرکت رو به آینده امنیت سایبر در نهادهای پژوهشی دولتی (دانشگاه و مراکز پژوهشی و...)، خصوصی (شرکت‌های فناور و دانش‌بنیان و...) و نهادهای سیاست‌گذار حاکمیتی می‌تواند کمک کند. بر اساس نظر مصاحبه‌شوندگان برای تدوین این نقشهٔ راه می‌توان از توان نهادهای مختلف استفاده نمود؛ برای نمونه، در حوزهٔ نظامی از نخبگان نظامی که برخی بازنشسته شده‌اند یا با قطب‌بندی دانشگاه‌ها در هر حوزه می‌توان از توان آن‌ها استفاده نمود؛ در این مورد، نهادهای خصوصی پژوهشی به علت

1. WannaCry

ارتباط آسانی که با نهادهای بین‌المللی می‌توانند ایجاد نمایند و همچنین نیروهای پلیس (فتا) که به علت این‌که این نهاد در تحریم‌های بین‌المللی قرار ندارند، گزینه‌هایی مناسب برای تدوین نقشهٔ راه هستند. بنابراین، ایجاد سند نقشهٔ راه ۱۵ ساله امنیت سایبر می‌باید تهیه شود. این نقشه می‌تواند در سه سطح کوتاه‌مدت (سه‌ساله)، میان‌مدت (تا ۷ سال) و بلندمدت (۱۵ سال) تهیه گردد. این نقشه ضمن کمک به سیاست‌گذاران حوزهٔ امنیت سایبری، برای درک بهتر آینده، به نهادهای پژوهشی دولتی و خصوصی (شرکت‌های فناور و دانش‌بنیان و مراکز توسعه فناوری و...) کمک می‌کند تا نقش و جایگاه خود را در آینده مشخص و حرکت خود را به‌سوی اهداف آن برنامه‌ریزی نمایند. این نقشهٔ راه باید با نگاه به تهدیدهای امنیت سایبری و رصد مستمر آن تهیه شود. بنابر نظر برخی مصاحبه‌شوندگان، تهیهٔ این سند باید با هدایت بالاترین نهاد سیاست‌گذار در امنیت سایبری (مرکز ملی فضای مجازی) صورت گیرد و نهادهای دیگر برحسب نیاز خود سیاست‌های مناسبی تدوین نمایند. در دستگاه‌ها باید سیاست‌ها جداگانه تبیین و تشریح شود. ورودی آن‌ها آینده‌پژوهی و خط‌مشی‌های کلان است. در این مورد پیشنهاد می‌شود که این نظام آینده‌پژوهی، برحسب توانمندی از نهادهای مختلف بهره‌مند گردد؛ در این مورد می‌توان دانشگاه‌های کشور را قطب‌بندی نمود و با بهره‌مندی از مراکز آپا[1] هرکدام را در حوزه تخصصی‌شان، یعنی محصول یا خدمات موردنظر فعال نمود و نقشهٔ راه موردنظر را تهیه نمود و با تدوین سند نقشهٔ راه نهادهای پژوهشی مختلف، کشور را قطب‌بندی نمود تا از هر قطب به میزان توانمندی‌شان بتوان بهره‌مند شد.

زیرقضیه ۳. تدوین نظام ارزیابی و نظارتی دقیق برای پایش فعالیت نهادهای پژوهشی حاکمیتی و خصوصی

ازجمله عناصر مهم در حاکمیت که تقریباً در همهٔ مدل‌های حاکمیت و همچنین خط‌مشی‌گذاری به چشم می‌خورد، ارزیابی عملکرد است که در ادبیات موضوع به آن اشاره شد. البته از دو منظر موردبحث است؛ ارزیابی عملکرد عناصر شبکهٔ نهادهای پژوهشی امنیت سایبری و از بُعد نظارت دقیق بر فعالیت‌های نهادهای پژوهشی که هر دو نیازمند ایجاد نظامی یکپارچه است. همان‌طور که در زیرقضیه پیشین مطرح شد، بهره‌مندی از نهادهای پژوهشی غیردولتی در ایجاد صنعت بومی امنیت سایبری از موارد ضروری است. بهره‌مندی از نهادهای خصوصی نیازمند ایجاد فرآیندهای نظارتی دقیق است؛ بنابراین، ایجاد نظام ارزیابی و نظارتی دقیق برای فعالیت نهادهای پژوهشی امنیت سایبر ضروری است؛ در این راستا ازجمله پیشنهادهایی که مطرح است، ایجاد نظام مهندسی

۱. این مراکز بازوی پژوهشی مرکز ماهر وزارت ارتباطات هستند. مرکز ماهر، مرکز رصد تهدیدهای سایبری در کشور است. تاکنون ۳۳ مرکز آپا در کشور در کنار دانشگاه‌های هر استان ایجاد شده است.

افتا[1] در کشور است که می‌توان فعالیت بخش خصوصی را به شکلی مناسب مورد ارزیابی و نظارت قرار داد. هم‌اکنون در کشور سیاست‌های مصوب در سطح حاکمیت (مصوبات شورای عالی فضای مجازی) یا دولت (مصوبات کمیسیون تنظیم مقررات) به حد مناسبی پیگیری نمی‌شود یا این‌که پیگیری اجرای آن نمود چندانی در کشور ندارد. نهادهای مختلفی در کشور وجود دارند که در حوزهٔ سایبری بدون هیچ‌گونه مقرراتی فعالیت می‌کنند که برخی گردش مالی خوبی هم دارند؛ اما نظارتی بر آن‌ها صورت نمی‌گیرد. همان‌طور که بیان شد، با ایجاد فرآیندهای نظارتی دقیق می‌توان از بخش خصوصی در کل چرخهٔ پژوهش امنیت سایبری از ایده تا محصولات از جمله محصولات عمومی و راهبردی بهره‌مند گردید. با ایجاد فرآیندهای نظارتی دقیق بر بخش خصوصی و همراه آن کاهش نقش بخش دولتی در پژوهش‌های امنیت سایبری می‌توان در کوتاه‌مدت شاهد پیشرفتی چشم‌گیر در این حوزه بود. بعضی از مصاحبه‌شوندگان اعتقاد دارند که نظارت و ارزیابی به بخش خصوصی واگذار شود و بخش دولتی فقط قانون‌گذار بوده و حسن اجرای مقررات را رصد نماید؛ به این شکل در صورت تخلف در ارزیابی هم امکان پیگیری تخلف وجود دارد. بنابراین، می‌توان نتیجه گرفت ایجاد نظام ارزیابی نهادهای پژوهشی و همچنین نظارتی آن‌ها ازجمله موارد مهم در فعال‌سازی نهادهای پژوهشی امنیت سایبر محسوب می‌شود و نکتهٔ مهم این است که در این راستا می‌توان با تدوین مقررات لازم، این نظام را پیاده نمود و نقش آن را با نظارت کلان نهاد حاکمیتی به بخش خصوصی واگذار نمود که در ضمنِ چابک‌سازی، این ارزیابی خارج از رانت‌های دولتی صورت گیرد و در صورت تخلف با متخلفان برخورد لازم صورت گیرد.

زیرقضیه ۴. تدوین نظام حمایتی و ایجاد بازار رقابتی امنیت سایبری برای افزایش مشارکت و شکوفا شدن ظرفیت‌های پژوهشی در کشور

همان‌طور که در ادبیات پژوهش هم اشاره شد، استفاده از ظرفیت‌های پژوهشی و نهادهای خصوصی در بومی‌سازی محصولات امنیت سایبری در کشور از اهمیت بالایی برخوردار است که نیازمند شکوفا شدن این ظرفیت در کشور است. ازجمله فعالیت‌های اخیر سازمان فناوری اطلاعات، ایجاد و فعال‌سازی مراکز آپا در کشور است. به‌غیر از مراکز آپا، بخش خصوصی هم ظرفیتی مناسب در کشور در حوزهٔ امنیت سایبری دارد. بنابراین، ایجاد نظام حمایتی از بخش‌های غیردولتی در فعال کردن و استفاده از ظرفیت پژوهشی امنیت سایبر در کشور مؤثر است. از مهم‌ترین دغدغه‌های بخش غیردولتی، حمایت نهادهای حاکمیتی از آن‌ها از دو جنبه است. نخست، حمایت از آن‌ها برای رشد و توسعه و دوم ایجاد بازار باثبات. بنابر گفتهٔ یکی از مصاحبه‌شوندگان، ظرفیت پژوهش‌های

۱. امنیت فضای تبادل اطلاعات

امنیت سایبر در کشور مناسب است؛ اما مدیریت آن نیازمند بازنگری دارد. حاکمیت می‌تواند با جهت‌دهی نهادهای پژوهشی در راستای نیازها و تهدیدات کشور در این حوزه به افزایش مشارکت و شکوفا شدن ظرفیت‌های پژوهشی کمک نماید. این نظام حاکمیتی می‌تواند دربارهٔ محصولات راهبردی مورد نیاز امنیت سایبری در کشور شکل بگیرد. بنابراین، نظام حمایتی می‌تواند با ایجاد بازار امنیت سایبری در حوزه‌های راهبردی کشور شکل بگیرد. نهادهای حاکمیتی علاوه بر ایجاد بازار، به طرق مختلف می‌تواند ظرفیت‌های پژوهشی را در کشور در این حوزه فعال نماید. ازجمله می‌توان به معافیت‌های مالی و مالیاتی، تسهیلات در ضمانت‌های مالی، وارد نکردن هزینه‌های اضافی به آن‌ها، ایجاد نقشهٔ راه امنیت سایبری و حمایت از طریق خرید سهام آن‌ها یا عضویت در هیأت‌مدیره بخش‌های خصوصی اشاره نمود.

قضیه ۲. مدیریت نهادهای پژوهشی امنیت فضای سایبری در کشور نیازمند پشتوانه الزامات قانونی قوی است.

ایجاد قوانین و مقررات لازم در امنیت فضای مجازی ازجمله مواردی مهم است که حتی نهادی فراتر از مجلس شورای اسلامی بر آن ایجاد شده است. شورای عالی فضای مجازی، نهادی است فرا وزارتی در جمهوری اسلامی که مصوبات آن حکم قانون را دارد و برای همهٔ نهادهای کشوری و لشگری در کشور لازم‌الاجراست. این نهاد حاکمیتی با اختیاراتی که دارد می‌تواند با وضع سیاست‌های کلان و به دنبال آن مقررات اجرایی، خط‌مشی‌های لازم را در کشور در این حوزه ایجاد نماید. اما نکتهٔ مهم، اجرای این مقررات است. در بند نخست، مأموریت‌های این مرکز به‌صراحت به برآورده‌سازی اهداف و سیاست‌های این مرکز و نظارت بر حُسن اجرای مصوبات شورای عالی فضای مجازی اشاره می‌نماید.

موارد مهم در این مورد که در مصاحبه‌های صورت گرفته به آن دست‌یافته شده است، در زیرقضیه‌های زیر اشاره می‌گردد.

زیرقضیه ۱. مدیریت دغدغه‌مند و متعهد به امنیت بومی سایبری همراه با قاطعیت در اجرا و به دور از سیاست‌زدگی از الزامات حفظ امنیت سایبری در کشور است.

به‌منظور دست‌یابی به قضیه دوم که تأکید بر مدیریتی در امنیت فضای مجازی در کشور اشاره می‌کند که مصوبات قانونی شورای عالی فضای مجازی را به‌خوبی اجرا نماید. در این مورد، بنابر مصاحبه‌های صورت‌گرفته، به مدیریت دغدغه‌مند و متعهد به امنیت سایبری در کشور نیاز است.

در این میان، اهمیت قاطعیت مدیران در ایجاد این امنیت و پیگیری اجرای مصوبات لازم‌الاجرای امنیت در کشور نیز مورد اشاره است و البته به دور از سیاست‌زدگی؛ گاهی مشاهده

شده است که با وجود مصوبات قانونی و دستور بر اجرای آن‌ها، همچنان تغییرات در سطوح و بدنهٔ دولت این مصوبات نادیده گرفته شده است؛ این سیاست‌زدگی از مهم‌ترین آسیب‌های وارد شده به نهادهای پژوهشی بخش خصوصی است و باعث بی‌اعتمادی این بخش به دولت و سرمایه‌گذاری آن‌ها در این مورد می‌گردد.

زیرقضیه ۲. ایجاد نظام‌های قراردادی صحیح میان نهادهای پژوهشی (حاکمیتی و خصوصی) با حفظ حقوق مالکیت معنوی، بسترساز استفادهٔ بیشینه از توانمندی‌های شبکه‌های پژوهشی امنیت سایبر است.

همان‌گونه که اشاره شد از عناصر حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری در کشور «طراحی و فعال‌سازی» و «مشارکت و توانمندسازی» این نهادهاست. ازجمله عوامل فعال شدن این شبکه‌ها، حفظ حقوق مالکیت معنوی آن‌هاست؛ اما ایجاد بستر حفظ این حقوق با ایجاد نظام‌های قراردادی رسمی میان اعضای این شبکه‌ها امکان دارد. از مهم‌ترین زیرساخت‌های لازم برای گسترش ظرفیت‌های شبکه‌های فناوری، زیرساخت‌های مالی و معاملاتی در تعامل با شبکهٔ همکاران و گلوگاه‌های موجود در این زمینه است (انصاری، ۱۳۸۷). روشن بودن این قوانین باعث ایجاد و توسعهٔ اعتماد متقابل میان شبکه‌ها، گسترش همکاری و ارتباطات متقابل، ارتقای قابلیت و خواست طرفین برای تسهیم منافع و ریسک‌های همکاری و درنهایت، توسعهٔ تعهد متقابل میان آن‌ها می‌شود. با این اوصاف، ارتقای قابلیت‌های قانونی و حقوقی از طریق قوانین مالی و معاملاتی از گام‌های مهم در ایجاد بستر استفاده از نهادهای پژوهشی امنیت سایبری محسوب می‌شود. درواقع، زیرساخت قانونی در زمینهٔ مالی و معاملاتی سازگار و تسهیل‌کنندهٔ جریان همکاری با شبکه است (فرتوک‌زاده و دیگران، ۱۳۹۱).

زیرقضیه ۳. مدیریت متعهد به بخش خصوصی و نخبگان برای اطمینان‌بخشی به آن‌ها و دغدغه‌های آن‌ها باشد؛ به‌گونه‌ای که به دور از سیاست‌زدگی و برخوردهای سلیقه‌ای با بخش خصوصی باشد.

با توجه به مصاحبه‌های صورت گرفته، مهم‌ترین بخش برای توسعهٔ پژوهش در امنیت فضای سایبر، بخش خصوصی است. با توجه به تجربه‌های چندین ساله در حوزهٔ پژوهش، این نتیجه حاصل شده که فرآیند پژوهش در نهادهای دولتی به دلیل بوروکراسی در زمان‌های طولانی صورت گرفته است؛ اما نهادهای خصوصی که هزینه ـ فایده و حل مسأله برای آن‌ها اهمیتی بیشتر دارد، در این زمینه چابک‌تر عمل می‌نمایند. بنابراین، ایجاد اطمینان به آن‌ها در حفظ دستاوردهای پژوهشی‌شان و ایجاد بازار ثابت و با اطمینان می‌تواند در شکوفایی این نهادها یا افراد

مهم واقع شود. بنابراین، در کشور باید بخش خصوصی را باور نمود و به آن‌ها متعهد بود. متأسفانه همان‌گونه که اشاره شد، در بخش حاکمیتی احترامی به حقوق بخش خصوصی گذاشته نمی‌شود و معمولاً اعتراض‌های آن‌ها در این مورد به‌جایی نمی‌رسد. اما واقعیت این است که تا بخش خصوصی قوی نشود، توسعه و جهشی در پژوهش‌های امنیت سایبر صورت نمی‌گیرد؛ بنابراین، پیشنهاد می‌شود که فرآیندهایی برای ایجاد این فرهنگ در بخش حاکمیتی ایجاد گردد. اهمیت بخش خصوصی منحصر به شرکت‌های خصوصی نیست؛ بلکه نهادهای دانشگاهی، پژوهشگاه‌ها و همچنین نخبگان این حوزه را شامل می‌شود؛ بعضی از این نخبگان در خارج از کشور هستند که ظرفیت مناسبی برای جهش در پژوهش‌های امنیت سایبر در کشور می‌توانند ایجاد نمایند.

از راهکارهای پیشنهاد شده در این مورد، مشارکت اعضای مؤثر نهادهای حاکمیتی در هیأت‌های مدیرهٔ بخش‌های خصوصی است و با این سازوکار، بخش خصوصی از اعتماد بخش حاکمیتی برخوردار می‌شود و هم می‌تواند بازار ثابت و مطمئنی را برای سرمایه‌گذاری پژوهشی داشته باشد. ایجاد سازوکارهای قوی برای رصد فرآیندهای پژوهشی در این نهادها می‌تواند افراد مؤثر، به‌خصوص در بخش دولتی را از ایجاد رانت‌های اطلاعاتی یا سیاست‌گذاری‌های سلیقه‌ای دور نگه دارد.

نتیجه‌گیری

همان‌گونه که در مقدمه بیان شد، همراه با تغییر در ماهیت مسائل، بسته‌های دانشی مدیریتی نیز دچار تحولاتی می‌شود. از مهم‌ترین این دانش‌ها، دانش حاکمیت و خط‌مشی‌گذاری عمومی است. با توجه به روند رو به افزایش ارتباطات افقی در جامعه، کشورها را به‌سوی جوامع شبکه‌ای با شاخص‌های وابستگی متقابل سوق داده است. حاکمیت، موضوعی دربارهٔ شیوهٔ تعامل دولت‌ها و دیگر نهادهاست. مورد مطالعه در این پژوهش، نهادهای پژوهشی امنیت سایبری بود که به دلیل ناهمسویی و نبودِ هم‌افزایی این نهادها در کشور و از سوی دیگر اهمیت حفظ امنیت بومی سایبری در زیرساخت‌های حیاتی کشور، حاکمیت مناسب این نهادها از اهمیتی به‌سزا در حفظ امنیت ملی کشور برخوردار است. در این مقاله، حاکمیت شبکه‌ای به‌عنوان مدلی در اختیار سیاست‌گذاران که به‌وسیلهٔ آن می‌توانند با مسائل بغرنج سیاست‌گذاری پژوهش‌های امنیت سایبری روبه‌رو شوند، پیشنهاد شد. ابتدا عناصر حاکمیت تشریح گردید و با کمک روش نظریه داده‌بنیاد و مصاحبه‌های اکتشافی نیمه ساختاریافته توانست عناصر این مدل را در نهادهای پژوهشی امنیت سایبر ایران شناسایی و با توجه به شرایط محیطی و زمینه‌ای در ایران تبیین نماید. همان‌گونه که در بخش‌های

پیش تشریح شد، از عناصر اصلی حاکمیت شبکه‌ای در ایران می‌توان به سیاست‌گذاری کلان، طراحی و فعال‌سازی شبکه، مدیریت، جهت‌دهی و توانمندسازی و ارزیابی شبکه اشاره نمود. از میان عناصر بیان‌شده، عنصر سیاست‌گذاری، جهت‌دهی و توانمندسازی شبکه، فقط حاصل مصاحبه‌های حاصل از نظریه داده‌بنیاد شکل گرفته است و عناصر دیگر نظیر طراحی و فعال‌سازی شبکه، مدیریت و ارزیابی شبکه از نظریه‌های موجود استفاده شده است. البته تعریف و برداشت از کل عناصر بیان‌شدهٔ حاصل از ادبیات و نظریه‌های پیشین، با برداشت آن در حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری در ایران متفاوت است که در ادامه تشریح می‌گردد؛ در واقع می‌توان گفت این پژوهش توانسته است به غنی‌سازی ادبیات حاکمیت شبکه‌ای بیفزاید. در این پژوهش معیارهای بیان شده با راهبردهای مختلف تأمین شده است که یکی از اصلی‌ترین آن‌ها، راهبرد بازخورد مشارکت‌کننده بوده است که طی آن، تفسیر گفته‌های مشارکت‌کنندگان و نتایج حاصل از تحلیل آن‌ها به بعضی از مشارکت کنندگان و بازیگران کلیدی عرضه شد و مواردی که نتیجهٔ ادراک نادرست بودند، تعیین و اصلاح گردید. از مهم‌ترین نتایج این پژوهش می‌توان به قضایای نظری اشاره نمود که حاصل کدگذاری انتخابی روش داده‌بنیاد است. با توجه به نبود نظریه در موضوع این پژوهش، نتایج زیر حاصل بررسی و تحلیل دوباره توسط مشارکت‌کنندگان کلیدی بوده است؛ به‌گونه‌ای که در تبیین آن‌ها از آموخته‌های تجربی آن‌ها نیز بهره‌مند شده است. با توجه به نتایج به‌دست آمده در این پژوهش، نهادهای مختلف و متنوعی در کشور در حوزهٔ امنیت فضای سایبر فعالیت می‌کنند که نیازمند فعال نمودن ظرفیت این نهادها در کشور از طریق تدوین سیاست‌های یکپارچه از سوی شورای عالی فضای مجازی است. با توجه به مشاهدهٔ صورت‌گرفتهٔ حاصل، مصاحبهٔ مستقیم و همچنین پژوهشگرانی که خود از فعالان حوزهٔ امنیت سایبری در کشور هستند، از مهم‌ترین سیاست‌هایی که این شورا باید به‌دنبال آن باشد، نهادینه شدن دغدغه و اهمیت امنیت سایبری و درک و فرهنگ پژوهشی در بدنهٔ حاکمیت کشور است. البته، در میان نهادهای حاکمیتی، فرهنگ‌سازی آن در نهادهای دولتی از اهمیتی بالاتر برخوردار است که هم‌اکنون فقدان آن به‌ویژه در نهادهای دولتی برجسته است. ازجملهٔ سیاست‌های دیگر، تدوین نقشه راه امنیت سایبری با تصویب شورای عالی فضای مجازی است که هم‌اکنون فقدان آن باعث سردرگمی و عدم استفاده از ظرفیت‌های نهادهای پژوهشی اعم از حاکمیتی یا خصوصی شده است. تدوین نظام‌های ارزیابی و نظارتی دقیق در کنار بهره‌مندی از نهادهای پژوهشی و همچنین ایجاد نظام‌های حمایتی و بازار رقابتی می‌تواند ازجمله سیاست‌هایی باشد که در مشارکت بخش خصوصی در کشور مؤثر واقع شود؛ چرا که با توجه به ادبیات و تجزیه‌وتحلیل صورت‌گرفته

از مهم‌ترین موارد در تقویت پژوهش‌های امنیت سایبری تقویت نهادهای پژوهشی خصوصی است. از جمله نتایج دیگر این پژوهش، توجه به الزامات قانونی به‌عنوان رکن حاکمیت مؤثر در نهادهای پژوهشی امنیت سایبری است. تدوین نظام‌های قراردادی صحیح میان نهادهای پژوهشی (حاکمیتی و خصوصی) با حفظ حقوق مالکیت معنوی، بسترساز استفادهٔ بیشینه از توانمندی‌های شبکه‌های پژوهشی امنیت سایبر است و در کنار آن تربیت مدیرانی توانمند با قاطعیت اجرایی که خود را متعهد به بخش خصوصی دانسته و به دور از سیاست‌زدگی و برخوردهای سلیقه‌ای بتوانند از این ظرفیت در تولید محصول بومی امنیت سایبری در کشور بهره‌مند شوند.

پیشنهادها

در این بخش، با توجه به نتایج به‌دست‌آمده در این پژوهش، پیشنهادهایی که برای انجام پژوهش‌های بعدی و در حوزهٔ سیاست‌گذاری باید به آن توجه گردد، ارائه می‌گردد. در مورد قضیهٔ نخست می‌توان به ترسیم نقشهٔ جامع علمی کشور در افق ۱۴۰۴ و ۱۴۱۴ در حوزهٔ امنیت سایبری، ترسیم نقشهٔ راه محصولات و فناوری‌های راهبردی امنیت سایبری (در افق سه‌سال، هفت‌سال و پانزده سال)، لحاظ نمودن امنیت سایبری در پروژه‌های ملی، طراحی نظام یکپارچهٔ پایش فعالیت پژوهشی امنیت سایبری با تأکید بر استفاده از بخش خصوصی و طراحی سازوکارهایی برای تسهیلات مالی، تخصیص سهم امنیت در پروژه‌های ملی، تخصیص یارانهٔ تولید و سرمایه‌گذاری بر پژوهش‌های پایه اشاره نمود. در مورد قضیهٔ دوم می‌توان ایجاد سازمان نظام مهندسی افتا[1]، اصلاح شرح وظایف سازمان تنظیم مقررات رادیویی در وزارت ارتباطات با تمرکز بر امنیت سایبری و تدوین دستورالعمل‌های حفظ حقوق مالکیت معنوی در سطح ملی و بخشی اشاره نمود.

منابع

الف) فارسی

انصاری، باقر (۱۳۸۷). *در سازوکارهای حقوقی حمایت از تولید علم*. تهران سمت.

خواجه نائینی، علی (۱۳۹۳). درآمدی بر مفهوم حاکمیت شبکه‌ای. *رهیافت‌های سیاسی و بین‌المللی*، شمارهٔ ۳۹، صص ۱۵۵-۱۲۹.

دانایی‌فرد، حسن (۱۳۹۲). مدیریت دولت شبکه‌ای در ایران: خرد نظری ـ ملی و استلزامات. *پژوهش‌های مدیریت در ایران*، دوره ۲، شماره ۱۷، صص ۱۰۴-۶۹.

دانایی‌فرد، حسن؛ الوانی، سیدمهدی و آذر، عادل (۱۳۸۸). *روش‌شناسی پژوهش کمی در مدیریت: رویکردی*

۱. امنیت فضای تبادل اطلاعات

جامع. تهران، صفار ـ اشراقی.
دانایی‌فرد، حسن و امامی، سیدمجتبی (۱۳۸۶). استراتژی‌های پژوهش کیفی: تاملی بر نظریه‌پردازی داده‌بنیاد. *اندیشه مدیریت*، دوره ۱، شماره ۲، صص ۹۷-۶۹.
فرتوک‌زاده، حمیدرضا؛ دره‌شیری، محمدرضا و محبی، محمد (۱۳۹۱). بررسی گلوگاه‌های قوانین مالی و معاملاتی صنایع دفاعی در تعامل با شبکهٔ همکاران. *مدیریت بهبود*، شمارهٔ ۱۳، صص ۸۴-۶۴.
کاملی، محمدجواد و الوانی، سیدمهدی (۱۳۹۰). *شبکه‌ها و خط‌مشی‌گذاری عمومی*. تهران، انتشارات دانشگاه علوم انتظامی.

ب) انگلیسی

Eggers, W. D. (2008). *Collaborative Governance: A New Era of Public Policy in Australia? The Changing Nature of Government*: Network Governance. ANUE Press.

Folke, C.; Hahn, T.; Olsson, P. & Norberg, J. (2005). Adaptive Governance of Social-Ecological Systems. *Annual Review of Environment and Resources*, 30, pp. 441-473.

Glaser, B. & Strauss, A. (1967). *The Discovery of Grounded Theory Strategies for Qualitative Research*. New Brunswick: Aldine Transaction.

Goldsmith, S. & Eggers, W. (2004). *Governing by Network: The New Shape of the Public Sector*. In Challenges of the Network Model (p. 51). Columbia, Maryland.

Hertting, N. & Vedung, E. (2012). Purposes and Criteria in Network Governance Evaluation: How Far Does Standard Evaluation Vocabulary Takes Us? *Evaluation*, 18(1), pp. 27-46.

Huitema, D.; Mostert, E.; Egas, W.; Moellenkamp, S.; Pahl-Wostl, C. & Yalcin, R. (2009). Adaptive Water Governance: Assessing the Institutional Prescriptions of Adaptive (Co-) Management from a Governance Perspective and Defining a Research Agenda. *Ecology and Society*, 14(1), p. 26.

Jones, C.; Hesterly, W. & Bor, S. (1997). A General Theory of Network Governance: Exchange Conditions and Social Mechanisms. *The Academy of Management Review*, 22(4), pp. 911-945.

Kettl, D. (2005). *The Next Government of the United States: Challenges for Performance in the 21st Century*. Washington: IBM Center for the Business of Government.

Kim, B. T. (2009). A Three Order Network Governance Framework and Public Network Development. Florida: Florida State University. *Access of http://purl.flvc.org/fsu/fd/FSU_migr_etd-3068.*

Langner, R. (2013). *To Kill a Centrifuge*: *A Technical Analysis of What Stuxnet's Creators: Tried to Achieve*. Arlington, Hamburg, Munich: The Langner Group.
Lester, T. & Reckhow, S. (2012). Network Governance and Regional Equity: Shared Agendas or Problematic Partners? *Planning Theory*, 12, pp. 115-138.
Lincoln, Y. S. & Guba, E. G. (1985). *Naturalistic Inquiry*. Beverly Hills: Sage.
Maturo, A. (2004). Network Governance as a Response to Risk Society Dilemmas: A Proposal from the Sociology of Health. Topoi, 23(2), pp. 195-202.
O'Brien, M. (2015). *Epistemology and Networked Governance: An Actor-Network Approach to Network Governance*. Boca Raton, FL: Florida Atlantic University.
Rhodes, R. (1996). The New Governance: Governing without Government. *Political Studies, XLIV*, pp. 652-667.
Rhodes, R. (2007). Understanding Governance: Ten Years On. *Organization Studies*, 28(8), pp. 1243-1264.
Rosenau, J. (1992). *Governance without Government: Order and Change in World Politics*. Cambridge: Cambridge University Press.
Sorensen, E. & Torfing, J. (2009). Making Governance Networks Effective and Democratic through Metagovernance. *Public Administration*, 87(2), pp. 234-258.
Strauss, A. & Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications.
Treib, O.; Bähr, H. & Falkner, G. (2005). Modes of Governance: A Note Towards Conceptual Clarification. *Europaische Governance Papers*, pp. 1-22.
Twining, j. (2000). *A Naturalistic Journey into the Collaboratory: In Search-Hrast*. Texas: Texas Womans University.