Journal of
Improvement Management
Vol. 11 No. 4, Winter 2018 (Serial 38)

A Network Governance Model with Emphasis on Development of Open Innovation Processes at Security Research Institutions

Mohammadmehdi Ghuchani Khorasani[1], Davood Hosseinpour[2]☎, Ibrahim Mahmudzaeh[3], Seyed Mahdi Alvani[4], Seyed Abolhasan Firoozabadi[5]

1- PhD in Public Policy, Faculty of Management and Accounting, Allameh Tabataba'i University, Tehran, Iran.
2- Associate Professor, Faculty of Management and Accounting, Allameh Tabataba'i University, Tehran, Iran.
3- Associate Professor, Faculty of Management and Industrial Engineering, Malek Ashtar University of Technology, Tehran, Iran.
4- Professor, Faculty of Management and Accounting, Qazvin Islamic Azad University, Qazvin, Iran.
5- PhD in Strategic Management, Supreme National Defense University, Tehran, Iran.

Abstract:

Governments change their governance models based on social, political and economic situations. Rapid technological change, increasing innovation cost and drastic competition in new products and services have caused organizations to interact with external environment and stakeholders. Opening boundaries of organization, using open innovation paradigm for internal development and expansion of market to enjoy external innovations are the most significant consequences of this interaction. Cyber security technology is one the most changeable today's technologies, which is a momentous key in national security. Proposing a governance pattern in this case would help the government to deal with problems, such as dispersion and incoordination between organizations. This pattern suggests methods for using all capacities to produce native products. This paper is going to identify governance elements and open innovation development factors, by considering the environmental conditions in Iran, to achieve a network governance pattern for cyber security research organizations. These factors have been recognized by using Grounded theory. For this purpose, 16 semi-structured interviews have been done. Analyzing data in open-coded process by using MAXQDA 10 software has led to produce 16 subcategories in the form of 4 main categories. The model presented in this article is based on Emerging design approach and the results have been explained as theoretical propositions.

Keywords: *Network Governance, Open Innovation, Research Institutions, Cyber Security.*

1. *ghochany@yahoo.com*
2. ☎*Corresponding author: dhp748@gmail.com*
3. *maheb20@gmail.com*
4. *sralvani@gmail.com*

نشریه علمی – پژوهشی بهبود مدیریت
سال یازدهم، شماره ۴، پیاپی ۳۸، زمستان ۱۳۹۶
صفحات ۵۶ - ۳۳

الگوی حکمرانی شبکه‌ای با تأکید بر توسعه فرآیندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری

(تاریخ دریافت: ۹۵/۰۵/۲۵ تاریخ پذیرش: ۱۳۹۶/۱۲/۰۸)

محمدمهدی قوچانی خراسانی[۱]، داود حسین‌پور[۲]*، ابراهیم محمودزاده[۳]، سیدمهدی الوانی[۴]، سید ابوالحسن فیروزآبادی[۵]

چکیده

حکومت‌ها به فراخور فضای اجتماعی، سیاسی و اقتصادی نوع حکمرانی خود را تغییر می‌دهند. تغییر و تحولات سریع در حوزه فناوری، افزایش هزینه‌های نوآوری و رقابت روزافزون در محصولات و خدمات جدید منجر به افزایش نیاز سازمان به تعامل با محیط و ذینفعان خارجی‌شان شده است که از این طریق سبب باز شدن مرزهای سازمان و استفاده از پارادایم نوآوری باز در توسعه روندهای داخلی نوآوری و گسترش بازار برای استفاده خارجی از نوآوری شده است. از پرتغییرترین فناوری‌های روز، فناوری‌های مربوط به فضای سایبری و امنیت آن است؛ حفظ امنیت در این فضا از مسائل مهم در امنیت ملی کشور محسوب می‌شود. به علت پراکندگی، عدم همسویی و عدم هم‌افزایی نهادهای تحقیقاتی امنیت سایبری در ایران، بهره‌مندی از مدلی برای حکمرانی این فضا جهت استفاده متناسب از تمام ظرفیت‌ها برای تولید محصول بومی، راه‌حل مناسبی برای حاکمیت محسوب می‌شود. این مقاله باهدف دستیابی به مدل حکمرانی شبکه‌ای و با تأکید بر توسعه فرآیندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری به دنبال شناسایی عناصر حکمرانی و عوامل توسعه فرآیندهای نوآوری باز با توجه به شرایط محیطی حاکم بر آن در ایران است. این عوامل با استفاده از روش نظریه داده‌بنیاد شناسایی‌شده‌اند. بدین منظور، ۱۶ مصاحبه نیمه ساختاریافته با خبرگان این موضوع صورت گرفته است. تحلیل داده‌ها در فرآیند کدگذاری باز با کمک نرم‌افزار MAXQDA10 منجر به تولید ۱۶ مقوله فرعی در قالب ۴ مقولهٔ اصلی شده است. مدل ارائه‌شده در این مقاله با رویکرد خودظهور به‌دست آمده است و نتایج آن به‌صورت گزاره‌های نظری تبیین می‌شود.

واژگان کلیدی:
حکمرانی شبکه‌ای؛ نوآوری باز؛ نهادهای تحقیقاتی؛ امنیت سایبری.

۱- دکتری مدیریت دولتی (سیاستگذاری عمومی)، دانشگاه علامه طباطبائی(ره): Ghochany@yahoo.com
۲*- دانشیار، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی (ره) (نویسنده مسئول): Dhp748@gmail.com
۳- دانشیار دانشگاه صنعتی مالک اشتر
۴- استاد دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی (ره)
۵- هیأت علمی دانشگاه عالی دفاع ملی

۱- مقدمه

از پرتغییرترین فناوری‌های روز، فناوری‌های مربوط به فضای سایبری و امنیت آن است. رشد و توسعه فناوری اطلاعات و فنّاوری‌های سازمان باعث شده تا فرصت‌های بسیاری برای سوءاستفاده از اطلاعات و افراد در سازمان‌ها ایجاد شود. از سال‌های ابتدایی فراگیر شدن رایانه‌های شخصی و پس‌ازآن شبکه اینترنت موضوع امنیت شبکه‌ها و اطلاعات کاربران و به بیان کلی‌تر، امنیت در فضای سایبر یکی از مباحث مهم هم در سطح شرکت‌ها و هم در سطح حاکمیت بوده است. به علت پراکندگی، عدم همسویی و عدم هم‌افزایی نهادهای تحقیقاتی امنیت سایبری در ایران و حملات و تهدیدات سایبری[۱] اخیر، بهره‌مندی از الگویی برای مدیریت این فضا جهت استفاده متناسب از تمام ظرفیت‌ها برای تولید محصول بومی، راه‌حل مناسبی برای حاکمیت محسوب می‌شود. با توجه به تغییرات سریع فضای سایبری[۲][۱]، برای مدیریت این پیچیدگی باید تعاملات پیش‌رو با سازوکار جدیدی برنامه‌ریزی شود تا با این سازوکار هم بتواند بهره‌وری سازمان‌ها و نهادها بالا برود و هم در راستای هدف حاکمیت، پیوندهای بین نهادها به بهترین شکل هدایت و مدیریت شود. مدل حکمرانی شبکه‌ای با تأکید بر نحوه تعامل دولت و دیگر سازمان‌های اجتماعی با یکدیگر، شیوه هدایت و مدیریت آن‌ها و شیوه گرفتن تصمیمات در محیطی پیچیده، پیشنهاد مناسبی برای همسوسازی این نهادها است؛ بنابراین، شناسایی عناصر مؤثر در مدل حکمرانی شبکه‌ای در نهادهای تحقیقاتی امنیت سایبری موضوعیت پیدا می‌کند. در ایران علی‌رغم وجود نهادهای مختلف، اعم از دولتی و خصوصی، همسویی میان آن‌ها دیده نمی‌شود و علی‌رغم صرف بودجه کلان در این حوزه، بعد از گذشت حداقل ۱۰ سال همچنان پراکندگی و عدم هم‌افزایی در این نهادها مشهود است و به لحاظ تحقیقاتی پیشرفت ناچیزی را در این حوزه شاهد هستیم. پس شناسایی انواع نهادهای تحقیقاتی امنیت سایبری و عوامل زمینه‌ای مؤثر در مدیریت آن‌ها در ایران نیز قابل‌بررسی است. بنابراین، دستیابی به مدلی برای همسوسازی نهادهای تحقیقاتی امنیت سایبری و استفاده از آن در نهادهای حاکمیتی می‌تواند راهکار مناسبی برای مدیریت این فضا پیشنهاد دهد. از مهم‌ترین مسائل در حفظ امنیت سایبری کشور، استقلال و خودکفایی در تولیدات محصولات امنیت سایبر است؛ چراکه محصولات وارداتی –اعم از نرم‌افزار، سخت‌افزار و محصولات شبکه– شکاف‌های امنیتی نهفته و آشکاری دارند. بنابراین با توجه به تغییرات مستمر در این حوزه، کوتاه‌تر شدن چرخه عمر محصولات امنیت سایبری و فناوری‌های به کار گرفته‌شده در آن، تحقیق و توسعه داخلی در این حوزه و تقویت نهادهای تحقیقاتی، از نیازهای مهم و حیاتی کشور محسوب می‌شود. به‌منظور دستیابی به محصولات

---

[۱] حمله بدافزار استاکس نت در سال ۲۰۱۰ به تأسیسات هسته‌ای نطنز.

[۲] محیط پیچیده ناشی از تعامل مردم، نرم‌افزار و خدمات در اینترنت، با استفاده از دستگاه‌های فناوری و شبکه‌های متصل به آن، که درهرصورت ماهیت فیزیکی ندارد (سازمان استاندارد بین‌المللی، ۲۰۱۲)

بومی، استفاده از رویکرد نوآوری باز می‌تواند راهبرد مناسبی در دستیابی به این مهم محسوب شود. توجه به تعریف نوآوری باز که مبتنی بر استفاده هدفمند از جریان رو به داخل و نیز رو به خارج فنی به‌منظور توسعه روندهای داخلی نوآوری و گسترش بازار برای استفاده خارجی از نوآوری است [۳]. بهره‌مندی از این پارادایم موجب تعامل بیشتر میان فعالان این عرصه نظیر بنگاه‌ها، شبکه تأمین‌کنندگان آن‌ها و بازار مشتریان می‌شود. این مقاله به‌منظور دستیابی به محصولات و خدمات امنیت سایبری در کشور، با معرفی پارادایم نوآوری باز، هدایت و هماهنگی نهادهای تحقیقاتی امنیت سایبری را مبتنی بر این پارادایم تبیین می‌کند. در این مقاله، در ابتدا، عناصر حکمرانی شبکه‌ای و عوامل مؤثر بر توسعه فرآیندهای نوآوری باز تشریح می‌شود. سپس، با کمک روش نظریه داده‌بنیاد و مصاحبه‌های اکتشافی نیمه ساختاریافته عناصر این مدل را در نهادهای تحقیقاتی امنیت سایبری ایران شناسایی و با توجه به شرایط محیطی و زمینه‌ای در ایران تبیین می‌شود.

با این مقدمه، سؤالی که این تحقیق به آن پاسخ می‌دهد آن است که مدل حکمرانی شبکه‌ای در نهادهای تحقیقاتی امنیت‌سایبری، با تأکید بر توسعه فرآیندهای نوآوری باز در کشور، چگونه است؟ برای رسیدن به این مدل از نظریه داده‌بنیاد استفاده می‌شود. در این پژوهش، ابتدا مفاهیم حکمرانی شبکه‌ای و نوآوری باز تشریح می‌شود و در ادامه، با استفاده از روش تحلیل داده‌بنیاد مدلی در این زمینه تبیین خواهد شد.

الف- حکمرانی شبکه‌ای[۱]

حکمرانی موضوعی درباره نحوه تعامل دولت‌ها و دیگر سازمان‌های اجتماعی با یکدیگر، شیوه ارتباط آن‌ها با شهروندان و شیوه گرفتن تصمیمات در جهانی پیچیده است. حکمرانی فرآیندی است که از آن طریق جوامع یا سازمان‌ها تصمیمات مهم خود را می‌گیرند و مشخص می‌کنند که چه کسانی در این فرآیند درگیر شوند و چگونه وظیفه خود را به انجام برسانند [۲]. برحسب این تعریف، نوع‌شناسی‌های مختلفی درباره حکمرانی ارائه‌شده است و هریک از نظریه‌پردازان به طبقه‌بندی متفاوتی دست‌یافته‌اند. اشکال مختلفی برای حکمرانی ذکرشده است: حکمرانی مشترک، حکمرانی مدیریت دولتی جدید، حکمرانی خوب، حکمرانی به‌عنوان وابستگی متقابل بین‌المللی، حکمرانی سایبرنتیک اجتماعی، حکمرانی اقتصاد سیاسی جدید و حکمرانی شبکه‌ای [۳، ۴]. در دهه‌های گذشته، واژه‌های شبکه یا شبکه‌سازی در بیشتر مباحث مدیریت دولتی و خط‌مشی‌گذاری عمومی متداول شده است؛ درواقع، علت این امر پیشرفت‌های اجتماعی، سازمانی و فناورانه بوده است. جامعه شبکه‌ای، ساختاری از شبکه‌های سازمانی و اجتماعی دارد که همه فضاهای جامعه را در نظر می‌گیرد. به‌طورکلی، در بسیاری از راهکارهای پیشنهادی برای بازسازی دولت همگی بر تمرکززدایی دولت و وابستگی با سایر شرکا در جامعه و خصوصی‌کردن فعالیت‌های دولت تأکید شده است؛ چراکه شبکه‌ها هماهنگی و کنترل فعالیت‌های دولت

---

[۱] Network Governance

را ارتقا می‌دهند. بر این اساس، شیوه حکمرانی شبکه‌ای نسبت به شیوه‌های رایج بـا ویژگـی‌هـای عصـر فعلی متناسب‌تر است. ریشه‌های حکمرانی شبکه‌ای را می‌توان در دهه‌های ۱۹۵۰ و ۱۹۶۰ با ظهور پدیده «سرمایه‌داری دانش[۱]» یافت. ظرفیت شبکه‌ای شدن، درواقع، مبنای اساسی این ایده را تشکیل مـی‌دهـد [۵].

در جدول زیر، تعاریفی در مورد حکمرانی شبکه‌ای از دیدگاه محققان این حوزه ارائه می‌شود:

جدول ۱- عبارات و تعاریف مختلف از حکمرانی شبکه‌ای [٦]

نویسنده، سال	اصطلاح	تعریف حکمرانی شبکه‌ای
آلتر و هیج[۲]، ۱۹۹۳	شبکه‌های بین سازمانی	خوشه‌های غیرمحدود یا محدود از سازمان‌هایی است که طبق تعریف، مجموعه‌های غیر سلسله مراتبی از واحدهایی مجزا (از نظر قانونی) هستند.
دوبینی و آلدریخ[۳]، ۱۹۹۱	شبکه‌ها	روابط تبدیل‌شده به الگو بین افراد، گروه‌ها و سازمان‌ها.
گرلاخ و لینکولن، ۱۹۹۲	سرمایه‌داری متحد	روابط راهبردی و بلندمدت در بین طیف گسترده‌ای از بازارها.
گرانووتر[۴]، ۱۹۹۴ و ۱۹۹۵	گروه‌های تجاری[۵]	مجموعه‌هایی از شرکت‌ها که به صورت‌های رسمی یا غیررسمی به هم متصل هستند؛ با سطح متوسطی از اتصال.
کرینر و شولتز[۶] ۱۹۹۳	شبکه‌ها	همکاری‌های بین سازمانی غیررسمی.
لارسون[۷]، ۱۹۹۲	شکل‌های سازمانی شبکه	مبادلات بلندمدت تکرارشونده که وابستگی‌های متقابلی ایجاد می‌کنند. [این وابستگی‌های متقابل] بر ایجاد تعهدات، انتظارات، اعتبارها و منافع دوجانبه تکیه دارند.
لیبسکایند، الیور، زوکر و بروور[۸]، ۱۹۹۶	شبکه‌های اجتماعی	مجموعه[۹] افرادی که در میان آن‌ها مبادلاتی رخ می‌دهد که تنها توسط معیارهای مشترک رفتار قابل‌اعتماد تأیید می‌شوند.
مایلز و اسنو[۱۰]، ۱۹۸۶ و ۱۹۹۲	سازمان‌های شبکه‌ای	دسته‌هایی از شرکت‌ها یا واحدهای اختصاصی که با سازوکارهای بازار هماهنگ می‌شوند.
پاول[۱۱]، ۱۹۹۰	شکل‌های شبکه‌ای سازمان	الگوهای جانبی یا افقی از مبادله، جریان مستقل منابع، خطوط ارتباط دوجانبه.

همان‌گونه که بیان شد حکمرانی شبکه‌ای در معانی تعاریف مختلفی به کار گرفته‌شده است، اما اشـتراک

۱Knowledge Capitalism
۲Alter& Hage
۳Dubini& Aldrich
٤Granovetter

۵گروه‌های تجاری که با شبکه‌های همکاری متمایز می‌شوند.

٦Gerlach & Lincoln
۷Larson
۸Liebeskind, Oliver, Zucker, & Brewer
۹ Collectivity
۱۰Miles & Snow
۱۱Powell

همه تعاریف نشان می‌دهد که حکمرانی شبکه‌ای مدلی در اختیار سیاست‌گذاران است که به‌وسیله آن می‌توانند با مسائل بغرنج[۱] روبرو شوند. مسائل بغرنج مسائلی هستند که زمان کمی برای پاسخگویی به آن‌ها وجود دارد. حکمرانی شبکه‌ای، درواقع، یک شکل مطلوب اداره امور است که با فراهم بودن زمینه مشارکت برقرار می‌شود و به‌عنوان راه‌حلی است که در پی تغییر و بهبود تعاملات سازمان است [۷]. در اینجا، مفاهیمی نظیر «تسهیم منافع مشترک»، «برقراری و هماهنگی ارتباطات مطلوب»، «تقویت اعتماد»، «تعاملات غیررسمی نهادها»، «مذاکرات تعاملی» از اهمیت به‌سزایی برخوردار هستند. بنابراین، حکمرانی هم نتیجه قوانین رسمی (مثل سیاست‌ها، هنجارها، قوانین و...) و هم تعاملات غیررسمی بازیگران در شبکه است که منجر به ارتقای پاسخگویی جمعی به مسائل و مشکلات محیطی می‌شود [۸]. با توجه به اینکه این تحقیق به دنبال ارائه مدل حکمرانی شبکه‌ای است، با بررسی مدل‌های مختلف حکمرانی شبکه‌ای که در مبانی نظری این موضوع آمده است، عناصر شکل‌گیری حکمرانی شبکه‌ای در جدول ۲ مورد اشاره قرار می‌گیرد:

جدول ۲- بررسی تطبیقی عناصر شکل‌گیری حکمرانی شبکه‌ای

عناصر مدل حکمرانی شبکه‌ای					مرجع
طراحی شبکه	شکل‌گیری شبکه	مدیریت شبکه	مشارکت در شبکه		[۹]
تدوین استراتژی شبکه	طراحی و فعال‌سازی شبکه	سرمایه انسانی شبکه	یکپارچه‌سازی شبکه	ارزیابی عملکرد شبکه	[۱۰]
پیکربندی شبکه	هماهنگی شبکه	خودتنظیمی شبکه			[۱۱]
تدوین استراتژی شبکه	شبکه‌ای کردن شبکه	طراحی شبکه	انتخاب شرکای مناسب		[۱۲]

تغییر و تحولات سریع در حوزه فناوری، افزایش هزینه‌های نوآوری و رقابت روزافزون در محصولات و خدمات جدید منجر به افزایش نیاز سازمان به تعامل با محیط و ذی‌نفعان خارجیشان شده که از این طریق سبب باز شدن مرزهای سازمان به‌منظور تبادل ایده‌های نوآورانه شده است [۱۳]. نهادهای تحقیقاتی امنیت سایبری به علت سه عامل ۱- هزینه‌ی بالای تحقیق و توسعه درون بنگاه‌ها، ۲- کوتاه‌تر شدن چرخه عمر کالاها و فناوری‌های به کار گرفته‌شده در آن‌ها و نیاز به کسب رضایت مشتریان و ۳- گردش و تمایل نیروی انسانی متخصص به تغییر محیط کاری برای کسب درآمد و مزایای بیشتر، به مقوله نوآوری اهمیت مؤثرتری داده‌اند [۱۴]. این بدان معنی است که شرکت‌ها و بنگاه‌ها در مقایسه با دهه‌های گذشته به مقدار زیادتری از منابع جهت توسعه و شکوفایی نوآورانه خود نیازمند هستند؛ بنابراین، باید بتوانند با دسترسی بیشتر به منابع علمی و دانش فنی، ایده‌ها و حق امتیازها در فرآیندهای تحقیق و

[۱] Wicked Problems: مسائلی که راه‌حل‌های متداول ندارد.

تکمیل نوآوری را تسریع ببخشند. با توجه به اینکه منطق تشریح مدل حکمرانی شبکه‌ای، طراحی و پیکره‌بندی، هماهنگی و مدیریت شبکه است و دستیابی به محصولات و فناوری‌های بومی بدون بهره‌مندی از نهادهای دیگر امکان‌پذیر نیست، لذا نیازمند طراحی مدل حکمرانی شبکه‌ای از نهادهای تحقیقاتی امنیت سایبری با تأکید بر عوامل مؤثر بر نوآوری باز در این حوزه و با در نظر گرفتن الزامات مطرح‌شده هستیم. در ادامه، نوآوری باز و عوامل مؤثر بر توسعه فرآیندهای آن تشریح می‌شود.

ب- نوآوری باز[۱]

نوآوری به فرآیند پرورش ایده تا بهره‌برداری و کاربرد عملی آن ، اطلاق می‌شود. نگرش فرآیندی به مقوله نوآوری، شامل بخش‌هایی چون جستجوی ایده‌های نو و فرصت‌های نوآورانه، گزینش آن‌ها، چگونگی تحقق آن‌ها و بهره‌مندی و ارزش‌آفرینی از فرصت‌ها و ایده‌های نوآورانه است [۱۵]. نوآوری باز رویکرد جدیدی است که اگرچه از دهه ۸۰ میلادی مطالعات آغازین آن شکل‌گرفته است، اما مطالعات اولیه به‌قدری ناچیز است که می‌توان از آن چشم‌پوشی کرد. مطالعه در این حوزه با معرفی این مفهوم در سال ۲۰۰۳ میلادی توسط هنری چسبرو به‌سرعت رو به رشد نهاد و از سال ۲۰۰۹ به‌شدت موردتوجه محققان حوزه نوآوری قرار گرفت؛ به‌گونه‌ای که از سال ۲۰۰۳ تا ۲۰۰۹ در این زمینه ۱۸۱ اثر منتشر شده است و این درحالی است که مقالات منتشره بین سال‌های ۲۰۰۹ تا ۲۰۱۴ حدوداً به ۲۰۰۰ اثر معتبر علمی می‌رسد[۲]. رویکرد نوآوری باز، در ابتدا، توسط هنری چسبرو به‌عنوان مجموعه‌ای از فعالیت های توسعه‌ای[۳]مطرح و پارادایمی تعریف شد که در آن شرکت‌ها اگر بخواهند نوآوری خود را افزایش دهند، می‌توانند و بهتر است که ایده‌های خارج سازمان را همچون ایده‌های داخل سازمان به کار گرفته و راه‌های خارجی و داخلی به بازار را بیابند [۱۶].

فرآیندهای نوآوری باز

طبق تعریف نوآوری باز می‌تواند برای افراد مختلف معانی متفاوتی داشته باشد و ازآنجاکه حوزه‌های زیادی تحت‌الشعاع این مفهوم قرار می‌گیرند، برحسب اینکه از چه دریچه‌ای به گشودگی در فرآیندهای یادگیری و نوآوری یک سازمان نگاه شود، تقسیم‌بندی‌های مختلفی از این فرآیندها می‌توان ارائه داد. همان‌گونه که بیان شد این تحقیق به دنبال شناسایی عوامل توسعه فرآیندهای نوآوری باز در نهادهای تحقیقات امنیت سایبری است؛ بنابراین، بامطالعه مدل‌های مختلف توسعه این رویکرد، باید بتوان یک رویکرد مناسب برای توسعه این فرآیندها در نهادهای تحقیقاتی امنیت سایبری احصاء کرد. در جدول ۳ بررسی تطبیقی این مدل‌ها ارائه می‌شود.

---

۱ Open Innovation

۲ جستجو در سایت علمی Science direct.

۳ development activities

جدول ۳- بررسی تطبیقی انواع فرآیندهای نوآوری باز

تمرکز مدل	فرآیندهای نوآوری باز							مرجع
فرآیندهای درونی و بیرونی	فرآیند بیرون به درون	فرآیند درون به بیرون	فرآیند ترکیبی					[۱۶، ۱۷]
کسب نوآوری خارجی	جستجوی فرصت	ارزیابی پتانسیل بازاری و سرمایه‌گذاری	گرفتن شرکای توسعه‌ای بالقوه	ایجاد ارزش از طرق تجاری‌سازی	گسترش نوآوری‌های ارائه‌شده			[۱۸]
بهبود عملکرد نوآورانه	همکاری	جستجو	حفاظت از مالکیت فکری	نوآوری خارجی				[۱۹]
سیاست‌گذاری	شبکه‌سازی	همکاری	کارآفرینی شرکتی	مدیریت مالکیت معنوی	تحقیق و توسعه			[۲۰]
یکپارچگی دانش مدیریتی	تعریف فرآیند نوآوری	تشخیص دانش نوآورانه مرتبط	انتخاب سازوکار یکپارچه‌سازی مناسب	ایجاد سازوکار حکمرانی مناسب	تعادل میان مشوق‌ها و کنترل‌ها			[۲۱]
آماده‌سازی سازمان	آمادگی سازمانی	توانمندی‌های مشارکتی	ظرفیت جذب					[۲۲]
تغییر سازمانی	سازمان‌دهی داخلی	توسعه شبکه‌ها	فرآیندهای ارزیابی	نظام‌های مدیریت دانش	انباشت عظیم از دانش‌پایه	نیروی کار آموزش‌دیده و پویا	دسترسی خوب به اعتبار	[۲۳]
عوامل مؤثر در موفقیت	شبکه‌سازی خارجی	واسطه‌های نوآوری	هوشمندی فناوری	ظرفیت جذب نوآوری	مدل کسب‌وکار	عوامل انسانی		[۲۴]

چارچوب نظری تحقیق

در مرور مبانی نظری، تلاش شد با توجه به اهداف تحقیق، مطالعات نسبتاً جامعی از انواع و عناصر حکمرانی شبکه‌ای و عوامل مؤثر در فرآیندهای نوآوری باز انجام شود. بر اساس مطالعه انجام‌شده و با توجه به جمع‌بندی صورت گرفته، عناصر، تدوین استراتژی شبکه، طراحی و فعال‌سازی شبکه، مدیریت شبکه، مشارکت و یکپارچه‌سازی و ارزیابی عملکرد شبکه، تقریباً پوشش‌دهنده عناصر شکل‌گیری حکمرانی شبکه‌ای است و آمادگی درون‌سازمانی و آمادگی بیرون سازمانی ازجمله عوامل توسعه فرآیندهای نوآوری باز محسوب می‌شود. در کنار آن برای بررسی عوامل زمینه‌ای جهت شکل‌گیری این

مدل از الگوی PEST [۱] (عوامل سیاسی، اقتصادی، اجتماعی و فناورانه) بهره‌مند شده است که در شکل زیر قابل‌مشاهده است.

شکل ۱- چارچوب نظری تحقیق

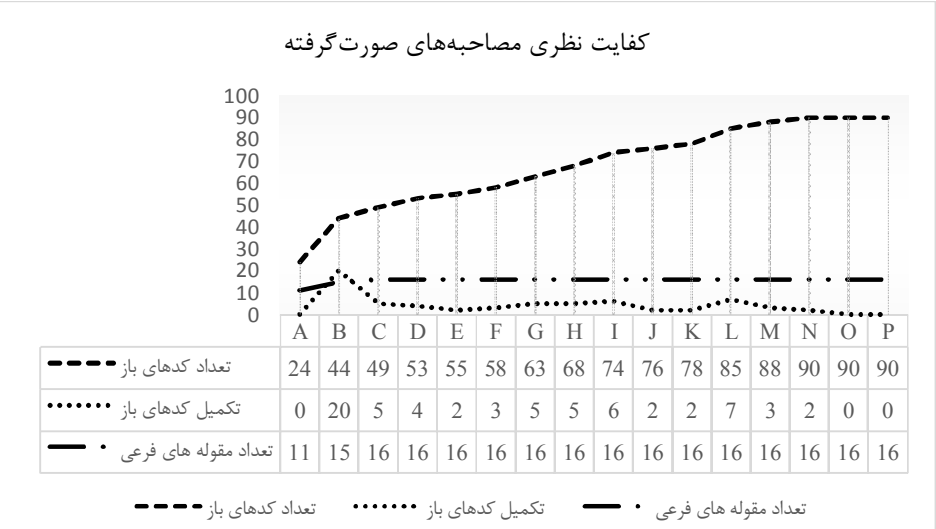
[۱] PEST analysis (political, economic, social and technological)

۲- روش تحقیق

در این پژوهش، با توجه به موضوع و سؤالات تحقیق، از روش کیفی استفاده‌شده است و از بین استراتژی‌های مختلف از نظریه داده‌بنیاد بهره‌مند شده است. سه مرحله اساسی این روش که شامل کدگذاری باز، کدگذاری محوری و کدگذاری انتخابی می‌شود در این پژوهش تشریح می‌شود [۲۵].

به‌منظور ثبت داده‌ها، تمامی مصاحبه‌ها در پژوهش حاضر، پس از اخذ مجوزهای لازم، به شکل صوتی ضبط شد. در مرحله بعد، مصاحبه‌ها به‌طور کامل پیاده و فایل‌ها در قالب Word وارد نرم‌افزار MAXQDA10 شد.

در این پژوهش، انتخاب مصاحبه‌شوندگان به‌صورت هدفمند (نمونه‌گیری جهت‌دار یا نظری) و به‌صورت گلوله برفی بوده است. در هر مرحله، فرآیند جمع‌آوری داده‌ها تا جایی ادامه پیدا می‌کند که به اشباع نظری رسیده و مطلب جدیدی به مدل اضافه نشود. نمونه‌گیری نظری بهترین روش برای توسعه‌ی یک نظریه است. در نمونه‌گیری نظری، مصاحبه‌های عمیق با خبرگان تا جایی پیش می‌رود که به حد اشباع نظری می‌رسد (شکل ۲). در این تحقیق با مصاحبه از ۱۶ نفر[۱]، ترکیبی از متخصصین (اعضاء هیئت‌علمی دانشگاه و محققین) و مدیران ارشد (بخش حاکمیتی و خصوصی) امنیت‌سایبری به اشباع و کفایت نظری دست‌یافته شده است.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
تعداد کدهای باز	24	44	49	53	55	58	63	68	74	76	78	85	88	90	90	90
تکمیل کدهای باز	0	20	5	4	2	3	5	5	6	2	2	7	3	2	0	0
تعداد مقوله های فرعی	11	15	16	16	16	16	16	16	16	16	16	16	16	16	16	16

شکل ۲- نمودار کفایت نظری داده‌ها

[۱] اطلاعات مصاحبه‌شوندگان نزد محققین محفوظ است.

اعتمادپذیری یافته‌های پژوهش

اکثر روش شناسان کیفی به‌جای استفاده از واژه‌های روایی و پایایی که ازلحاظ مبانی فلسفی ریشه در پارادایم کمی دارند. از معیار اعتمادپذیری یا قابلیت اعتماد جهت ارجاع ارزیابی کیفیت نتایج پژوهش کیفی استفاده می‌کنند [۲۶]. گوبا و لینکلن قابلیت اعتماد را شامل چهار معیار قابل‌قبول بودن، انتقال‌پذیری، قابلیت اطمینان و تأیید پذیری می‌دانند.در این پژوهش از استراتژی‌های جدول۴ برای تأمین اعتمادپذیری استفاده شد.

جدول٤- روش‌های تأمین اعتمادپذیری [۲۷] در پژوهش حاضر

معیار	زیرمعیارها		استراتژی تأمین	اقدام صورت گرفته
قابل‌قبول بودن	روایی ورودی‌های پژوهش	روایی داده‌های ورودی پژوهش	نمونه‌گیری گلوله برفی	معرفی مصاحبه‌شوندگان بعدی توسط مصاحبه‌شوندگان قبلی
			نمونه‌گیری بر مبنای اعتبار	انتخاب مصاحبه‌شوندگان بر اساس توصیه متخصصان
	روایی تحلیل‌های انجام‌شده در پژوهش	روایی توصیفی	بازخور مشارکت‌کننده	ارائه بازخورد توصیفی مصاحبه به مصاحبه‌شونده و دریافت نظرات اصلاحی
		روایی تفسیری	استفاده از توصیف-گرهایی 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 یعنی مدیران ارشد نظامی، دولتی و خصوصی در تحقیقات امنیت سایبری
			وصف تفصیلی همه جزئیات	ارائه یک تصویر مفصل از زمینه‌ای که پژوهش در آن انجام‌شده
	قابلیت اطمینان		ممیزی قابلیت اطمینان	در اختیار گذاشتن داده‌ها، روش‌ها و تصمیمات باهدف بازبینی و موشکافی تحقیق توسط دیگر پژوهشگران
	تأیید پذیری		ارائه جزئیات روش‌ها و داده‌های پژوهش	ارائه گزیده مصاحبه‌ها و نیز توضیح روند تحلیل داده‌ها تا دستیابی به نتایج تحقیق و تأیید و بازخور مشارکت‌کنندگان

۳- تجزیه‌وتحلیل و یافته‌های پژوهش

۳-۱- کدگذاری باز

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

مفهوم‌سازی

شکل‌گیری یک نظریه با مفهوم‌سازی آغاز شود. مفهوم‌سازی به کوشش محقق برای کاوش عمیق در یک مشاهده، جمله، پاراگراف یا یک صفحه و برگزیدن یک نام برای هر رویداد یا اتفاق اطلاق می‌شود. محقق کمک می‌کند تا وقایع، ایده‌ها یا رویدادهای مشابه را تحت عنوانی واحد یا در قالب دسته‌ای واحد گروه‌بندی کند. پدیده‌هایی را که برای آن‌ها اسمی انتخاب می‌شود، اصطلاحاً، مفهوم می‌نامند. مفاهیم، زیربنای نظریه به‌حساب می‌آیند.

مقوله‌بندی

هنگامی‌که داده‌ها باز شد و مفاهیم از درون آن‌ها سر برآورد، محقق به دنبال مصداق‌هایی می‌گردد که بتواند با کمک آن‌ها، مفاهیم را در قالب مقوله‌هایی دسته‌بندی کند. طبق دیدگاه اشتراوس و کوربین، برخی مفاهیم را می‌توان در قالب مقوله‌ای که از انتزاع بالاتری نسبت به آن مفاهیم برخوردار است، دسته‌بندی نمود [۲۸]. به کمک مقوله‌ها می‌توان چیزهای در حال وقوع را توصیف کرد. در جدول۵، نحوه شکل‌گیری یکی از مقوله‌های اصلی قابل‌مشاهده است:

در پژوهش حاضر، در مرحله کدگذاری باز از مجموع ۱۶ مصاحبه، ۷۸۸ کد توصیفی استخراج شد که به روش نظام‌مندی که در بالا شرح داده شد، مورد تجزیه‌وتحلیل قرار گرفتند و در قالب ۹۰ مضمون توصیفی بدون تکرار نمایان شدند. در جدول۵ نحوه شکل‌دهی مقوله‌های فرعی و شکل‌دهی آن‌ها به مقوله‌های اصلی نشان داده‌شده است.

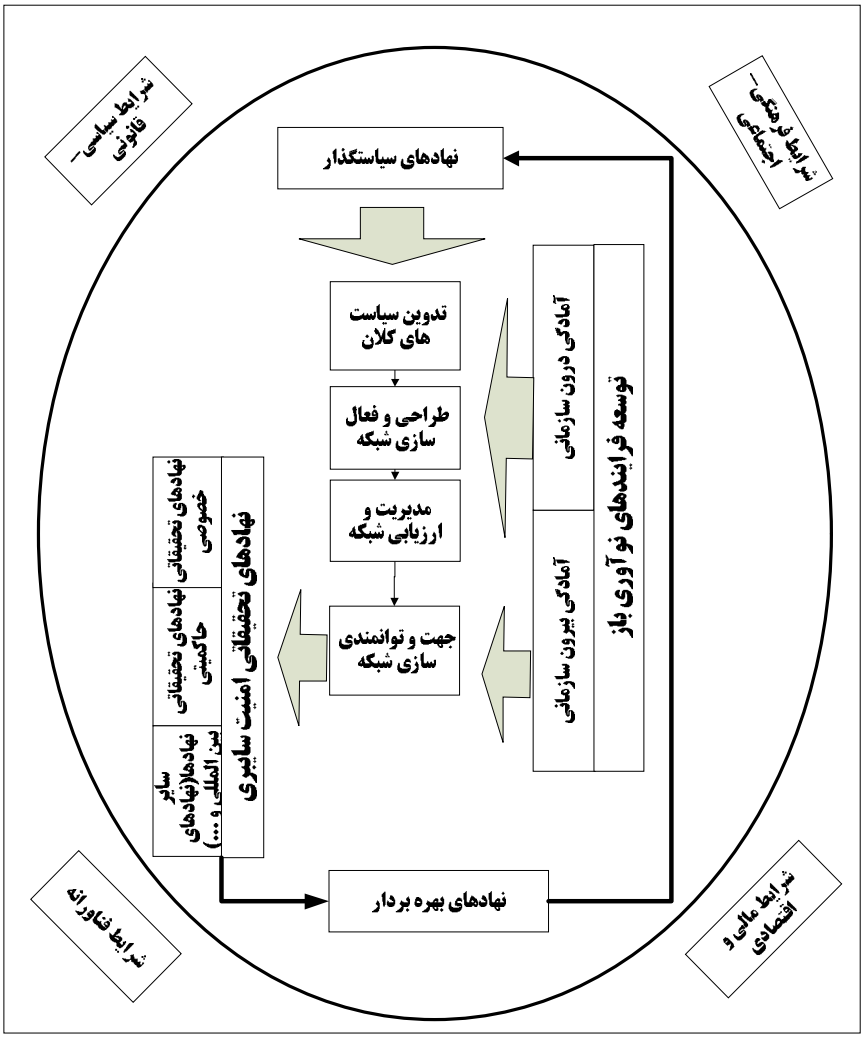
جدول ۵- ساخت مقوله‌های اصلی و مقوله‌های فرعی

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	**عوامل مؤثر در توسعه فرآیندهای نوآوری باز**	آمادگی درون‌سازمانی	۸۹
		آمادگی بیرون سازمانی	۵۲
۳	**شرایط زمینه‌ای مؤثر در سیاست‌گذاری نهادهای تحقیقاتی امنیت سایبری**	شرایط فناورانه	۱۷
		شرایط مالی و اقتصادی	۳۴
		شرایط سیاسی و قانونی	۴۰
		شرایط اجتماعی و فرهنگی	۵۳
۴	**نهادهای مؤثر در سیاست‌گذاری تحقیقات امنیت سایبری**	نهادهای بین‌المللی امنیت سایبری	۱۴
		نهادهای سیاست‌گذار	۲۷
		نهادهای تحقیقاتی حاکمیتی	۱۱۷
		نهادهای تحقیقاتی خصوصی	۳۶
		نهادهای بهره‌بردار امنیت سایبری	۹

۳-۲- کدگذاری محوری: نظریه‌پردازی

کدگذاری محوری، مرحله‌ی دوم تجزیه‌وتحلیل در نظریه داده‌بنیاد است. هدف از این مرحله برقراری ارتباط بین مقوله‌های تولیدشده در مرحله‌ی کدگذاری باز است. این تحقیق از رویکرد خودظهور نظریه داده‌بنیاد (مدل گلاسر وکوربین) و بر اساس داده‌های جمع‌آوری‌شده در مصاحبه‌های عمیق میان بازیگران مهم نهادهای تحقیقاتی امنیت سایبری در کشور استفاده نموده است. در مدل گلاسر بر اهمیت ظهور یک نظریه از دل داده‌ها تاکید می‌شود؛ درحالی که مدل پارادایم کدگذاری محوری (شرایط علی، محتوا، شرایط مداخله‌گر، استراتژی‌ها و پیامدها) بر استفاده از طبقه‌بندی معین از قبل تعیین‌شده تأکید می‌کند. بنابراین، از فرآیندهای کدگذاری روش داده‌بنیاد موارد ذیل حاصل می‌شود:

۱. ساخت مقولات اصلی با توجه به مقولات فرعی و ایجاد ارتباط بین آن‌ها: در این بخش، ابتدا نتایج مربوط به این کارکرد مرحله کدگذاری محوری ارائه‌شده است؛ به‌گونه‌ای که ۱۶ مقوله فرعی ظهور یافته در جریان تحقیق در قالب دسته‌های انتزاعی‌تر طبقه‌بندی و ارتباط میان آن‌ها تبیین می‌شود.
۲. ایجاد شبکه ارتباطی میان کل مقولات در قالب چندطبقه: کلیه مقوله‌ها (اعم از فرعی و اصلی) در قالب «کدگذاری محوری» حول یک مقوله محوری سامان می‌یابند.



شکل ۳-مدل حکمرانی شبکه‌ای بر اساس رویکرد خودظهور برای مقوله‌های اصلی

همان‌گونه که در شکل فوق مشاهده می‌شود، از مهم‌ترین مقوله‌های این مدل، تدوین سیاست‌های کلان است که فراوانی معادل ۱۸۴ کد از مجموع ۷۸۴ کد باز مصاحبه‌ها دارد. طبق نکات کلیدی اشاره‌شده در مصاحبه‌ها نهادهای مؤثر در تدوین این سیاست‌ها، مقوله نهادهای سیاست‌گذار تحقیقات امنیت سایبری هستند. این مقوله با مقوله طراحی و فعال‌سازی این شبکه مرتبط است. از سویی دیگر، مقوله آمادگی درون‌سازمانی و بیرون‌سازمانی که در توسعه فرآیندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری مدنظر هستند نیز با طراحی و فعال‌سازی این شبکه‌ها مرتبط هستند؛ از طرف دیگر، شرایط زمینه‌ای که درواقع، شرایط مؤثر در نهادهای تحقیقاتی امنیت سایبری در ایران محسوب می‌شوند نیز با طراحی و فعال‌سازی به‌عنوان یک مقوله فرعی حکمرانی شبکه‌ای مرتبط هستند. طراحی و فعال‌سازی از دو سمت با مقوله‌های دیگر مرتبط است. از سویی با مشارکت و توانمندسازی نهادهای تحقیقاتی خصوصی، حاکمیتی و بین‌المللی و از سوی دیگر، با دو مقوله مدیریت و ارزیابی عملکرد شبکه (که به‌صورت یک مقوله) نمایش داده‌شده است، مرتبط است.تشریح مدل فوق در قالب ارائه قضایای نظری در بخش بعدی تبیین می‌شود.

۳-۳- 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 که به شکل روایی نگاشته می‌شود. ابتدا، نظریه تحقیق در قالب گزاره‌های حکمی یا قضایای نظری طی فرآیند کدگذاری انتخابی به‌دست آمده و بیان می‌شوند. در ادامه با استناد به اظهارات مصاحبه‌شوندگان به تشریح قضایا و نیز زیرقضیه‌های نظری فوق پرداخته می‌شود.

قضایای نظری و تشریح آن

قضیه ۱- فعال‌سازی نهادهای تحقیقاتی امنیت سایبری در کشور نیازمند تدوین سیاست‌های یکپارچه از سوی نهاد حاکمیتی است:

سیاست‌گذاری کلان در امنیت سایبری ازجمله مواردی است که در مصاحبه‌های صورت گرفته بیشترین ارجاع را داشته است. دو مفهوم «سیاست‌گذاری امنیت سایبری» و «فرآیند سیاست‌گذاری امنیت سایبری» ازجمله مواردی هستند که جمعاً ۹۳ ارجاع را به خود اختصاص داده اند و این امر نشان‌دهنده اهمیت مفهوم سیاست‌گذاری کلان در حکمرانی شبکه‌ای در نهادهای تحقیقاتی امنیت سایبری در ایران است. با توجه به ساختار موجود، ایجاد شورای عالی فضای مجازی از طرف مقام معظم رهبری[مدظله] و به‌تبع آن ایجاد مرکز ملی فضای مجازی، با توجه به مأموریت ابلاغی، می‌تواند پاسخگوی این مهم باشد. نکات مهمی جهت تدوین این سیاست‌ها قابل‌ذکر است که در زیرقضیه‌های ذیل می‌توان به آن‌ها اشاره نمود:

زیرقضیه ۱- فعال نمودن شبکه‌های تحقیقاتی امنیت سایبری در کشور مستلزم نهادینه شدن دغدغه امنیت در کشور و بالارفتن درک و فرهنگ تحقیقات در بدنه حاکمیت است:
دغدغه و اهمیت موضوع امنیت سایبری در بدنه کشوری هنوز تبیین نشده است و بیشتر مدیران به این موضوع به‌عنوان یک موضوع غیر ضروری نگاه می‌کنند؛ درحالی‌که بی‌توجهی بیشتر به این موضوع می‌تواند اکثر بسترهای حیاتی حساس کشور را در معرض آسیب‌های جبران‌ناپذیری قرار دهد. نکته پراهمیت دیگری که در این زیرقضیه به چشم می‌خورد «بالارفتن درک و فرهنگ تحقیقات در بدنه حاکمیت» است. مشکل اصلی در این خصوص، نبود دید تحقیقاتی در کشور است. بنابراین، برای رسیدن به محصولات بومی امنیت سایبری، به تغییر دید مدیران در مورد کارهای تحقیقاتی در این حوزه نیاز است؛ به‌گونه‌ای که از نهادهای تحقیقاتی انتظار محصول و سودآوری نداشته باشند و این نیازمند برنامه‌ریزی بلندمدت و تخصیص بودجه‌های مناسب تحقیقاتی است.

زیرقضیه ۲- ایجاد نظام آینده‌پژوهی تحقیقاتی امنیت سایبری به‌منظور دستیابی به نقشه راه فناوری و محصولات بومی (رصد تهدیدات همراه با تغییرات سریع فناوری):
یکی از معضلات در تحقیقات امنیت سایبری، عدم وجود نقشه راه محصول و فناوری مورد وثوق و تأییداست که عدم وجود آن منجر به موازی‌کاری شرکت‌های نوپا در حوزه محصولات شرکت‌های قبلی شده و این حوزه را دچار نابسامانی می‌نماید؛ به‌گونه‌ای که در برخی حوزه‌ها بیش از چند محصول وجود دارد و در بعضی موضوعات محصول و خدمات مناسبی موجود نیست. این نقشه می‌تواند در سه سطح کوتاه‌مدت (سه‌ساله)، میان‌مدت (تا ۷سال) و بلندمدت (۱۵سال) تهیه شود. این نقشه ضمن کمک به سیاست‌گذاران حوزه امنیت سایبری برای درک بهتر آینده، به نهادهای تحقیقاتی دولتی و خصوصی (شرکت‌های فناور و دانش‌بنیان و مراکز توسعه فناوری و...) کمک می‌کند که نقش و جایگاه خود را در آینده مشخص و حرکت خود را به‌سوی آن اهداف برنامه‌ریزی نمایند.

زیرقضیه ۳- تدوین نظام ارزیابی و نظارتی دقیق جهت پایش فعالیت نهادهای تحقیقاتی حاکمیتی و خصوصی:
ازجمله عناصر مهم در حکمرانی که تقریباً در تمام مدل‌های حکمرانی و همچنین خط‌مشی‌گذاری به چشم می‌خورد، ارزیابی عملکرد است که در مبانی نظری موضوع به آن اشاره شد. البته این عنصر در دو بعد موردبحث است؛ ارزیابی عملکرد عناصر شبکه نهادهای تحقیقاتی امنیت سایبری و از بعد نظارت دقیق بر فعالیت‌های نهادهای تحقیقاتی که هر دو نیازمند ایجاد نظامی یکپارچه است. همان‌طور که در زیر قضیه قبل مطرح شد، بهره‌مندی از نهادهای تحقیقاتی غیردولتی در ایجاد صنعت بومی امنیت سایبری از موارد ضروری بوده و بهره‌مندی از نهادهای خصوصی نیازمند ایجاد فرآیندهای نظارتی دقیق است؛ بنابراین، ایجاد نظام ارزیابی و نظارتی دقیق برای فعالیت نهادهای تحقیقاتی امنیت سایبر ضروری

است. در این راستا، ازجمله پیشنهادهایی که مطرح است ایجاد نظام‌مهندسی افتا[۱] در کشور است که می‌توان فعالیت بخش خصوصی را به شکل مناسبی مورد ارزیابی و نظارت قرار داد. بنابراین می‌توان نتیجه گرفت ایجاد نظام ارزیابی نهادهای تحقیقاتی و همچنین نظارتی آن‌ها، ازجمله موارد پراهمیت در فعال‌سازی نهادهای تحقیقاتی امنیت سایبری محسوب می‌شود و نکته مهم این است که در این راستا می‌توان با تدوین مقررات لازم، این نظام را پیاده نمود و با نظارت کلان نهاد حاکمیتی، نقش آن را به بخش خصوصی واگذار نمود که در ضمن چابک‌سازی، این ارزیابی خارج از رانت‌های دولتی صورت گیرد و در صورت تخلف بتوان با متخلفین برخورد لازم را صورت داد.

زیرقضیه ۴- تدوین نظام حمایتی و ایجاد بازار رقابتی امنیت سایبری جهت افزایش مشارکت و شکوفا شدن ظرفیت‌های تحقیقاتی در کشور:

همان‌طور که در مبانی نظری تحقیق هم اشاره شد، استفاده از ظرفیت‌های تحقیقاتی و نهادهای خصوصی در بومی‌سازی محصولات امنیت سایبری در کشور، اهمیت بالایی دارد و کشور نیازمند شکوفا شدن این ظرفیت است. ازجمله فعالیت اخیر سازمان فناوری اطلاعات، ایجاد و فعال‌سازی مراکز آپا در کشور است. به‌غیراز مراکز آپا، بخش خصوصی هم‌ظرفیت مناسبی در کشور در حوزه امنیت‌سایبری دارد. بنابراین، ایجاد نظام حمایتی از بخش‌های غیردولتی در فعال کردن و استفاده از ظرفیت تحقیقاتی امنیت سایبری در کشور مؤثر است. از مهم‌ترین دغدغه‌های بخش غیردولتی حمایت نهادهای حاکمیتی از آن‌ها از دو جنبه است. اول، حمایت از آن‌ها جهت رشد و توسعه و دوم، ایجاد بازار باثبات. ازجمله حمایت‌ها می‌توان به معافیت‌های مالی و مالیاتی، تسهیلات در ضمانت‌های مالی، وارد نکردن هزینه‌های اضافی به آن‌ها، ایجاد نقشه راه امنیت‌سایبری و حمایت از طریق خرید سهام آن‌ها یا عضویت در هیئت‌مدیره بخش‌های خصوصی اشاره نمود.

قضیه ۲– توسعه فعالیت‌های تحقیقاتی بومی امنیت سایبری در کشور نیازمند آماده‌سازی درونی و بیرونی نهادهای تحقیقاتی امنیت سایبری است.

همان‌گونه که اشاره شد، از مهم‌ترین مسائل در حفظ امنیت‌سایبری کشور، استقلال و خودکفایی در تولیدات محصولات امنیت سایبری است؛ چون محصولات وارداتی، اعم از نرم‌افزار، سخت‌افزار و محصولات شبکه، شکاف‌های امنیتی نهفته و آشکاری دارند. بنابراین، توسعه فعالیت‌های تحقیقاتی بومی امنیت سایبری در کشور نیازمند توسعه نهادهای تحقیقاتی است. افزایش هزینه‌های نوآوری و رقابت روزافزون در محصولات و خدمات جدید منجر به افزایش نیاز سازمان‌ها به تعامل با محیط و ذی‌نفعان خارجیشان شده و از این طریق مرزهای سازمان به‌منظور تبادل ایده‌های نوآورانه باز شده است؛ ازاین‌رو

[۱] امنیت فضای تبادل اطلاعات.

برای توسعه نوآوری در نهادهای تحقیقاتی، این نهادها هم نیازمند آماده نمودن شرایط داخلی و هم خارجی خود در کسب نوآوری هستند. با مصاحبه‌های صورت گرفته در این زمینه، عوامل درونی و بیرونی توسعه نوآوری در نهادهای تحقیقاتی امنیت سایبری در قالب قضایای زیر تبیین می‌شود:

زیرقضیه ۱- فعال کردن نهادهای تحقیقات امنیت سایبری در کشور نیازمند سیاست‌گذاری بخشی نهادها در بهره‌مندی از منابع انسانی نخبه و توانمند است:

در کنار سیاست‌گذاری کلان در حوزه امنیت سایبری در کشور، هر بخش و هر نهاد نیازمند سیاست‌گذاری بخشی ذیل سیاست‌های کلان حاکمیتی است. این سیاست‌های بخشی، درواقع، برخاسته از همان قوانین و مقررات کلی وضع‌شده در حوزه امنیت‌سایبری کشور است که برحسب نیاز راهبردی، عملیاتی یا فنی آن نهاد بازنویسی و بومی شده‌اند. برای نمونه، بهره‌مندی از نخبگان امنیت سایبری در کشور، یک اصل در بهره‌مندی از ظرفیت امنیت سایبری کشور است اما اینکه نهادهای مختلف هرکدام چگونه از این منابع انسانی بهره‌مند شوند، نیازمند سیاست‌گذاری بخشی مختص خود است؛ مثلاً وزارت علوم می‌تواند با تدوین دستورالعمل‌های لازم از ظرفیت آموزشی و پژوهشی در این حوزه بهره‌مند شود. هم‌اکنون فرآیندهای تحقیقاتی مناسبی برای بهره‌مندی از این ظرفیت در دانشگاه‌ها موجود نیست؛ ازجمله سیاست‌های بخشی در خصوص نخبگان نظامی شاغل می‌توان به ایجاد فرآیندهای بهره‌مندی از این نخبگان مانند فعالیت در انجمن‌های علمی و... و در خصوص مدیران نخبه بازنشسته می‌توان به تسهیلاتی در خصوصی ایجاد شرکت‌هایی در حوزه امنیت سایبری در سطوح راهبردی، عملیاتی و فنی اشاره نمود. نکته قابل‌توجه در این زیر قضیه این است که این باید متمرکز بر ایجاد ظرفیت باشد. برای نمونه، با تقویت مراکز آپا در کشور با توجه به قطب‌بندی که تشریح شد، می‌توان کل ظرفیت امنیت سایبری در کشور را فعال نمود.

زیرقضیه ۲- توسعه فعالیت‌های تحقیقاتی امنیت سایبری نیازمند شبکه‌سازی، شناخت صحیح نیازهای تحقیقاتی، اصلاح فرآیندهای تحقیقاتی با تأکید بر ایجاد اعتماد میان نهادهای مختلف است.

همان‌طور که ذکر شد، توسعه فعالیت‌های تحقیقاتی بومی امنیت سایبری در کشور نیازمند توسعه نهادهای تحقیقاتی است. شبکه‌سازی نهادهای تحقیقاتی امنیت سایبری در کشور بر اساس مصاحبه‌های صورت گرفته مشروط به مشارکت کل نهادها در سطوح راهبردی، عملیاتی و فنی امنیت سایبری است. این شبکه‌سازی بر اساس قطب‌بندی است که نهاد سیاست‌گذار می‌تواند برای مجموعه شرکت‌های تحقیقاتی در حوزه امنیت سایبری ایجاد نماید. این شرکت‌ها بر اساس توانمندی خود در این قطب‌ها فعالیت می‌کنند.

از موارد دیگر می‌توان به شناخت صحیح نیاز تحقیقاتی از نهادهای بهره‌بردار و کارفرما در این حوزه اشاره نمود. گاهی نهادهای بهره‌بردار با عدم شناخت صحیح نیاز تحقیقاتی باعث تحمیل هزینه‌های اضافه به

بخش خصوصی شده یا با تعریف ناصحیح از نهادهای دانشگاهی استفاده صحیحی نمی‌شود. از موارد دیگر، اصلاح فرآیندهای تحقیقاتی در حوزه امنیت سایبری کشور است که شامل ارائه صلاحیت‌های تولید محصولات امنیتی به شرکت‌های تحقیقاتی است که بتوانند با اخذ این صلاحیت‌ها به تحقیق و تولید اقدام نمایند. با ارائه تعریف صحیحی از تحقیق می‌توان فرآیندهای حمایتی صحیحی نیز از آن داشت. این حمایت باعث ایجاد بازار باثبات و مطمئن از آن‌ها شده و باعث ایجاد اعتماد بین بخش خصوصی و دولتی می‌شود.

زیرقضیه ۳- توسعه فعالیت‌های تحقیقاتی امنیت سایبری مبتنی بر نوآوری باز نیازمند استفاده از تمام ظرفیت‌های داخل و خارج ایران با ایجاد شرایط رقابتی برابر و حفظ حقوق مالکیت معنوی آن‌ها است.
همان‌طور که در مرور بر مبانی نظری اشاره شد، با افزایش نیاز سازمان‌ها به تعامل با محیط و ذی‌نفعان خارجی به‌منظور تبادل ایده‌های نوآورانه، باید هم شرایط داخلی و هم شرایط خارجی در کسب نوآوری آماده شوند. در مصاحبه‌های صورت گرفته، عوامل متعددی به‌عنوان عوامل داخلی و بیرونی اشاره شدند؛ ازجمله این عوامل، ایجاد شرایط رقابتی برابر و حفظ حقوق مالکیت معنوی آن‌هاست. حمایت از حقوق مالکیت فکری جهت حفظ حقوق معنوی ایده پردازان و مخترعان جهت توسعه نوآوری می‌تواند کمک مؤثری در تولید نوآوری ایفا نماید.
همان‌گونه که اشاره شد، به‌جای ایجاد نهادهای مختلف دولتی در این حوزه که موجب افزایش سربار دولت می‌شود، می‌توان از ظرفیت‌های موجود در بخش خصوصی و مردم استفاده نمود. متأسفانه دولتمردان در واگذاری این حوزه به بخش خصوصی انحصاری عمل نموده و حتی شرکت‌های خانوادگی ایجاد می‌نمایند. با توجه به توانمندی بخش خصوصی، به اعتراف بسیاری از مدیران ارشد حاکمیتی، تقویت این نهادها باید در اولویت امر قرار گیرد. به نقل از مصاحبه‌شوندگان، شرکت‌های دانش‌بنیان، نخبگان خارج از کشور، هکرها، شرکت‌های خصوصی فعال، مدیران بازنشسته حوزه امنیت سایبری و مراکز آپا در سطح کشور، همه ظرفیت‌هایی هستند که می‌توان با استفاده از ایجاد شرایط رقابتی و حفظ حقوق مالکیت معنوی از آن‌ها بهره‌مند شد. بنابراین، پیشنهاد می‌شود برای حفظ و تأمین حقوق مالکیت معنوی که یکی از عناصر توسعه دانش و نوآوری در نهادهای تحقیقاتی محسوب می‌شود، نظام‌نامه‌ای در نهادهای سیاست‌گذار همراه با الزامات قانونی قوی تهیه و اجرای شود.

زیر قضیه ۴- ایجاد ظرفیت تحقیقاتی امنیت سایبری مستلزم شناخت و آموزش مبانی امنیت سایبری، شبکه‌های مجازی و فناوری‌های مهندسی اجتماعی در جوامع سازمانی و غیرسازمانی کشور است.
از مباحث مهمی که در مصاحبه‌های صورت گرفته اشاره شد، استفاده از ظرفیت تحقیقاتی امنیت سایبری در کشور است. البته بعضی از مصاحبه‌شوندگان بر این باور بودند که ظرفیت بالایی در کشور موجود است. نکته‌ای که باید به آن توجه نمود، ضعف فرهنگ امنیت در کشور در لایه‌های مختلف از راهبردی

و عملیاتی گرفته تا سطح روشی و حتی شهروندان است. ممکن است اخبار پراکنده‌ای از سرقت اطلاعات در محیط مجازی به‌صورت یک حمله سایبری، ویروس یا هک صفحات خصوصی شنیده شود، اما اهمیت این موضوع هنوز در لایه‌های مختلف دولت و مردم در ایران محرز نشده است که این مساله مستلزم ایجاد برنامه‌های آموزشی مناسب در کشور است. با احراز اهمیت امنیت سایبری در کشور و اهمیت بومی بودن محصولات امنیت سایبری توجه به تحقیقات و ایجاد ظرفیت‌های تحقیقاتی نیز خودبه‌خود موردتوجه قرار می‌گیرد. بنابراین، تهیه برنامه‌های آموزشی امنیت سایبری در کشور در سیاست‌گذاری‌های کلان کشور باید موردتوجه قرار گیرد.

قضیه ۳- مدیریت نهادهای تحقیقاتی امنیت فضای سایبری در کشور نیازمند پشتوانه الزامات قانونی قوی است.

ایجاد قوانین و مقررات لازم در امنیت فضای مجازی ازجمله موارد پراهمیتی است که حتی نهادی فراتر از مجلس شورای اسلامی برای آن ایجادشده است. شورای عالی فضای مجازی، نهادی است فرا وزارتی در جمهوری اسلامی که مصوبات آن حکم قانون را دارد و احکام آن برای تمام نهادهای کشوری و لشگری لازم‌الاجراست. این نهاد حاکمیتی با اختیاراتی که دارد می‌تواند با وضع سیاست‌های کلان و به دنبال آن مقررات اجرایی، خط‌مشی‌های لازم کشور در این حوزه را ایجاد نماید؛ اما نکته مهم اجرای این مقررات است. بند اول مأموریت‌های این مرکز به‌صراحت به تحقق اهداف و سیاست‌های این مرکز و نظارت بر حسن اجرای مصوبات شورای عالی فضای مجازی اشاره می‌نماید.

موارد مهم در این خصوص که از مصاحبه‌های صورت گرفته به‌دست آمده، در زیرقضیه‌های زیر مورداشاره قرار می‌گیرد.

زیرقضیه ۱- مدیریت دغدغه‌مند و متعهد به امنیت بومی سایبری همراه با قاطعیت در اجرا و به‌دوراز سیاست‌زدگی درمورد الزامات حفظ امنیت سایبری در کشور موردنیاز است.

به‌منظور دستیابی به قضیه سوم، تأکید بر مدیریتی در امنیت فضای مجازی کشور شده است که مصوبات قانونی شورای عالی فضای مجازی را به‌خوبی اجرا نماید. در این خصوص طبق مصاحبه‌های صورت گرفته مدیریتی دغدغه‌مند و متعهد به امنیت سایبری در کشور نیازمند است.

در این میان، اهمیت قاطعیت مدیران در ایجاد این امنیت و پیگیری اجرای مصوبات لازم‌الاجرای امنیت در کشور نیز مورداشاره است؛ البته به‌دوراز سیاست زدگی. بعضاً مشاهده شده است، علی‌رغم وجود مصوبات قانونی و دستور بر اجرای آن‌ها، باز هم با تغییرات در سطوح و بدنه دولت این مصوبات نادیده گرفته‌شده است. این سیاست زدگی از مهم‌ترین آسیب‌های واردشده به نهادهای تحقیقاتی بخش خصوصی است و باعث بی‌اعتمادی این بخش به دولت و سرمایه‌گذاری آن‌ها در این خصوصی می‌شود.

زیرقضیه ۲- ایجاد نظام‌های قراردادی صحیح میان نهادهای تحقیقاتی (حاکمیتی و خصوصی) با حفظ حقوق مالکیت معنوی، بسترساز استفاده حداکثری از توانمندی‌های شبکه‌های تحقیقاتی امنیت سایبری است.

همان‌گونه که اشاره شد، از عناصر حکمرانی شبکه‌ای در نهادهای تحقیقاتی امنیت سایبری در کشور «طراحی و فعال‌سازی» و «مشارکت و توانمندسازی» این نهادها است. 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 [۲۹]. روشن بودن این قوانین باعث ایجاد و توسعه اعتماد متقابل میان شبکه‌ها، گسترش همکاری و ارتباطات متقابل، ارتقای قابلیت و خواست طرفین برای تسهیم منافع و ریسک‌های همکاری و درنهایت، توسعه 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 تحقیقاتی امنیت سایبری محسوب می‌شود. درواقع، زیرساخت‌های قانونی درزمینه مالی و معاملاتی، تسهیل‌کننده جریان همکاری با شبکه است [۳۰].

زیرقضیه ۳- مدیریت، متعهد به بخش خصوصی و نخبگان جهت اطمینان بخشی به آن‌ها و دغدغه‌های آن‌ها باشد؛ به‌گونه‌ای که تعاملات به‌دوراز سیاست‌زدگی و برخوردهای سلیقه‌ای با بخش خصوصی باشد.

با توجه به مصاحبه‌های صورت گرفته مهم‌ترین بخش برای توسعه تحقیقات در امنیت فضای سایبر، بخش خصوصی است.

از راهکارهای پیشنهادشده در این خصوص مشارکت اعضای مؤثر نهادهای حاکمیتی در هیئت‌های مدیره بخش‌های خصوصی است و با این سازوکار، بخش خصوصی هم از اعتمادبخشی حاکمیتی برخوردار می‌شود و هم می‌تواند بازار ثابت و مطمئنی را برای سرمایه‌گذاری تحقیقاتی داشته باشد. ایجاد سازوکارهای قوی برای رصد فرآیندهای تحقیقاتی در این نهادها می‌تواند افراد مؤثر مخصوصاً در بخش دولتی را از ایجاد رانت‌های اطلاعاتی یا سیاست‌گذاری‌های سلیقه‌ای دور نگهدارد. در این تحقیق، قضایای مذکور با راهبردهای مختلف تأمین‌شده است که یکی از اصلی‌ترین آن‌ها، راهبرد بازخورد مشارکت‌کننده بوده است. طی آن، تفسیر گفته‌های مشارکت‌کنندگان و نتایج حاصل از تحلیل آن‌ها به بعضی از مشارکت‌کنندگان و بازیگران کلیدی عرضه شد و مواردی که نتیجه‌ی ادراک نادرست بودند، تعیین و اصلاح شد. از مهم‌ترین نتایج این مقاله می‌توان به قضایای نظری اشاره نمود که حاصل کدگذاری انتخابی روش داده‌بنیاد است. با توجه به نبود نظریه در موضوع این تحقیق، نتایج مذکور حاصل بررسی و تحلیل مجدد توسط مشارکت‌کنندگان کلیدی بوده است؛ به‌گونه‌ای که در تبیین آن‌ها از آموخته‌های تجربی آن‌ها نیز بهره‌برداری شده است.

٤- نتیجه‌گیری و پیشنهاد

همان‌طور که در مقدمه بیان شد، روند رو به افزایش ارتباطات افقی در جوامع، کشورها را به‌سوی جوامع شبکه‌ای با شاخصه‌های وابستگی متقابل سوق داده است. حکمرانی، موضوعی درباره نحوه تعامل دولت‌ها و دیگر نهادهاست. موردمطالعه در این تحقیق، نهادهای تحقیقاتی امنیت سایبری بود که به دلیل عدم همسویی و هم‌افزایی این نهادها در کشور و از سوی دیگر، اهمیت حفظ امنیت بومی سایبری در زیرساخت‌های حیاتی کشور، حاکمیت مناسب این نهادها به‌منظور دستیابی به محصولات و خدمات امنیت سایبری در کشور از اهمیت به‌سزایی در حفظ امنیت ملی کشور برخورداراست. این مقاله با معرفی پارادایم نوآوری باز، هدایت و هماهنگی نهادهای تحقیقاتی امنیت سایبری را مبتنی بر این پارادایم تبیین می‌کند. در ابتدا، عناصر حکمرانی و عوامل مؤثر بر توسعه فرآیندهای نوآوری باز تشریح شد و با کمک روش نظریه داده‌بنیاد و مصاحبه‌های اکتشافی نیمه ساختاریافته عناصر این مدل در نهادهای تحقیقاتی امنیت سایبری ایران شناسایی و با توجه به شرایط محیطی و زمینه‌ای در ایران تبیین شد. همان‌طور که در بخش‌های قبلی تشریح شد، از عناصر اصلی حکمرانی شبکه‌ای در ایران می‌توان به سیاست‌گذاری کلان، طراحی و فعال‌سازی شبکه، مدیریت، جهت‌دهی و توانمندسازی و ارزیابی شبکه اشاره نمود و عوامل توسعه فرآیندهای نوآوری باز نیز در قالب آمادگی درون سازمان و آمادگی بیرون‌سازمانی بیان شدند. از مهم‌ترین نتایج این مقاله می‌توان به قضایای نظری اشاره نمود که حاصل کدگذاری انتخابی روش داده‌بنیاد است. با توجه به نتایج به‌دست‌آمده در این پژوهش، نهادهای مختلف و متنوعی در کشور در حوزه امنیت فضای سایبری فعالیت می‌کنند که کشور نیازمند فعال‌سازی ظرفیت این نهادها از طریق تدوین سیاست‌های یکپارچه از سوی شورای عالی فضای مجازی است. از مهم‌ترین سیاست‌هایی که این شورا باید دنبال آن باشد، نهادینه شدن دغدغه و اهمیت امنیت سایبری و درک و توسعه فرهنگ تحقیقاتی در بدنه حاکمیت کشور است. البته در بین نهادهای حاکمیتی، فرهنگ‌سازی آن در نهادهای دولتی از اهمیت بالاتری برخوردار است. ازجمله سیاست‌های دیگر، تدوین نقشه راه امنیت سایبری با تصویب شورای عالی فضای مجازی است تا بتوان از ظرفیت‌های نهادهای تحقیقاتی، اعم از حاکمیتی یا خصوصی، به بهترین شکل استفاده نمود. تدوین نظام‌های ارزیابی و نظارتی دقیق در کنار بهره‌مندی از نهادهای تحقیقاتی و همچنین ایجاد نظام‌های حمایتی و بازار رقابتی می‌تواند ازجمله سیاست‌هایی باشد که در مشارکت بخش خصوصی در کشور مؤثر واقع شود. سیاست‌گذاری یکپارچه در این حوزه نیازمند آمادگی درون‌سازمانی و بیرون سازمانی از قبیل تدوین سیاست‌های بخشی در بهره‌مندی از نخبگان توانمند، شبکه‌سازی مناسب میان نهادهای تحقیقاتی، شناخت صحیح نیازها و فرآیندهای تحقیقاتی، استفاده از تمام ظرفیت‌های داخل و خارج با ایجاد شرایط رقابتی و آموزش مبانی امنیت سایبری است. ازجمله نتایج دیگر این تحقیق توجه به الزامات قانونی به‌عنوان رکن حکمرانی مؤثر در نهادهای تحقیقاتی امنیت سایبری است. تدوین نظام‌های قراردادی صحیح میان نهادهای تحقیقاتی (حاکمیتی و

خصوصی) با حفظ حقوق مالکیت معنوی، بسترساز استفادهٔ حداکثری از توانمندی‌های شبکه‌های تحقیقاتی امنیت سایبری است و در کنار آن، تربیت مدیرانی توانمند با قاطعیت در اجراست که خود را متعهد به بخش خصوصی دانسته و به‌دوراز سیاست زدگی و برخوردهای سلیقه‌ای بتوانند از این ظرفیت در تولید محصول بومی امنیت سایبری در کشور بهره‌مند شوند.

با توجه به نتایج به‌دست‌آمده از این تحقیق، پیشنهادهایی ارائه خواهد شد که در حاکمیت باید به آن‌ها توجه شود. در خصوص قضیه اول می‌توان به ترسیم نقشه جامع علمی کشور در افق ۱۴۰۴ و ۱۴۱۴ در حوزه امنیت سایبری، ترسیم نقشه راه محصولات و فناوری‌های راهبردی امنیت سایبری (در افق سه‌ساله، هفت‌ساله و ۱۵ ساله)، لحاظ نمودن امنیت سایبری در پروژه‌های ملی، طراحی نظام یکپارچه پایش فعالیت تحقیقاتی در حوزه امنیت سایبری با تأکید بر استفاده از بخش خصوصی و طراحی سازوکارهایی درخصوص تسهیلات مالی، تخصیص سهم امنیت در پروژه‌های ملی، تخصیص یارانه تولید و سرمایه‌گذاری بر تحقیقات پایه اشاره نمود. در خصوص قضیه دوم نیز می‌توان ایجاد سازمان نظام‌مهندسی افتا، 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. نهایتاً، در خصوص قضیه سوم می‌توان به تربیت مدیران توانمند و مؤثر همراه با ارزیابی آن‌ها در پایبندی به الزامات اجرایی مصوب تأکید نمود.

۵- محدودیت‌های تحقیق

ازجمله محدودیت‌های این تحقیق (نظیر سایر تحقیقات کیفی) جمع‌آوری اطلاعات، مصاحبه‌های اکتشافی با مدیران و سوگیری محقق در ارائه اطلاعات است که در این تحقیق با توجه به روایی و پایایی ارائه‌شده درروش تحقیق، سعی شده است که محدودیت‌های مذکور درنتیجه تحقیق تأثیری نداشته باشد. البته همانند اغلب مطالعات مبتنی بر نظریه داده‌بنیاد، یافته‌های تحقیق با اتکا به دیدگاه‌ها و تجربیات افراد نسبتاً محدودی حاصل‌شده است که با در نظر گرفتن طیف گسترده‌ای از خبرگان از نهادهای مختلف امنیت سایبری کشور، سعی بر غلبه بر این محدودیت شده است. ازجمله محدودیت‌های دیگر می‌توان به راهبردی بودن موضوع این تحقیق اشاره نمود. برخی از مدیرانِ تحقیقاتی با ادبیات سیاست‌گذاری و خط‌مشی‌گذاری عمومی آشنا نبوده و مدیران سیاست‌گذار در این حوزه با ادبیات تولید محصولات بومی امنیت سایبری آشنا نبودند که با انتخاب افرادی که در این دو حوزه تجربه داشتند، سعی شده این محدودیت برطرف شود.

منابع : **References:**

[1] ISO, "Information technology Security techniques Guidelines for cybersecurity," International Organization for Standardization (ISO/IEC 27032), Switzerland, 2012.

[۲] محمدجواد. کاملی و سیدمهدی. الوانی، شبکه‌ها خط‌مشی‌گذاری عمومی، تهران: انتشارات دانشگاه علوم انتظامی، ۱۳۹۰.

[3] M. G. O'Brien, "EPISTEMOLOGY AND NETWORKED GOVERNANCE: AN ACTOR-NETWORK APPROACH TO NETWORK GOVERNANCE," Florida Atlantic University, Boca Raton, FL, 2015.

[4] R. Rhodes, "The New Governance: Governing without Government," Political Studies, vol. XLIV, pp. 652--667, 1996.

[۵] علی. خواجه نائینی، «درآمدی بر مفهوم حکمرانی شبکه‌ای»، فصل‌نامه رهیافت‌های سیاسی و بین‌المللی، ج. ۳۹، ص. ۱۲۹–۱۵۵، ۱۳۹۳.

[6] C. Jones, W. S. Hesterly and S. P. Bor, "A General Theory of Network Governance: Exchange Conditions and Social Mechanisms," The Academy of Management Review, vol. 22, no. 4, pp. 911-945, 1997.

[7] T. W. Lester and S. Reckhow, "Network governance and regional equity: Shared agendas or problematic partners?," Planning Theory, vol. 12, pp. 115-138, 2012.

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

[9] E. Sorensen and J. Torfing, "Making Governance Networks Effective and Democratic Through Metagovernance," Public Administration, vol. 87, pp. 234-258, 2009.

[10] S. Goldsmith and W. D. Eggers, "Governing by network: the new shape of the public sector," in Challenges of the Network Model, Columbia, Maryland, 2004, p. 51.

[11] B.-T. KIM, "A Three Order Network Governance Framework and Public Network Development," FLORIDA STATE UNIVERSITY, FLORIDA, 2009.

[۱۲] حسن. دانایی‌فرد، «مدیریت دولت شبکه‌ای در ایران: خرد نظری–عملی و استلزامات»، پژوهش‌های مدیریت در ایران، ج. ۲، شماره ۱۷، ص. ۶۹–۱۰۴، ۱۳۹۲.

[13] T. Felin and T. Zenger, "Closed or open innovation? Problem solving and the governance choice," Research Policy, 2013.

[14] M. G. Jacobides and S. Billinger, "Designing the boundaries of the firm: From 'make, buy, or ally' to the dynamic benefits of vertical architecture," Organization Science, vol. 17(2), pp. 249-261, 2006.

[15] J. Tidd and J. Bessant, Managing Innovation: Integrating Technological, Market and Organizational change, 4th ed., 2009.

[16] H. Chesbrough, Open Innovation: The new imperative for creating and profiting from technology, Harvard Business School Press, 2003.

[17] O. Gassmann and E. Enkel, "Towards a Theory of Open Innovation: Three Core Process Archetypes," in R&D Management Conference (RADMA), Lisabon, Portugal, 2004.

[18] T. Fetterhoff and D. Voelkel, "Managing Open Innovation In Biotechnology," Research–Technology Management, vol. 3, pp. 49(3), 14–18, 2006.

[19] S. J. Herstad, C. Bloch, B. Ebersberger and E. v. d. Velde, "Open innovation and globalisation: Theory, evidence and implications," Vision EraNet project report, 2008.

[20] J. P. de Jong, W. Vanhaverbeke, T. Kalvet and H. Chesbrough, "Policies for Open Innovation: Theory, Framework and cases`," Vision EraNet, 2008.

[21] M. w. Wallin and G. V. Krogh, "Organizing for Open Innovation: Focus on the Integration of Knowledge," Organizational Dynamics, vol. 39, no. 2, p. 145–154, 2010.

[22] J. Hafkesbrink and M. Schroll, "Organizational Competences for Open Innovation in Small and Medium Sized Enterprises of the Digital Economy," in Competences Management for Open Innovation. Tools and IT- support to unlock the innovation potential beyond company boundaries, Lohmar, 2010, pp. 21-52.

[23] D. Chiaroni, V. Chiesa and F. Frat, "The Open Innovation Journey: How firms dynamically

implement the emerging innovation management paradigm," Technovation, vol. 31, pp. 34-43, 2011.

[۲۴] مصطفی. صفدری، منوچهر. منطقی و غلامرضا. توکلی، «نوآوری باز؛ نگاهی جامع بر مفاهیم، رویکردها، روندها و عوامل کلیدی موفقیت»، رشد فناوری، ج. ۴۰، ص ۱۰-۱۷، ۱۳۹۳.

[۲۵] حسن .دانایی‌فرد، سید.مجتبی. امامی، «استراتژی‌های پژوهش کیفی :تأملی بر نظریه‌پردازی داده بنیاد»، اندیشه مدیریت، ش. ۲، صص. ۶۹-۹۷، ۱۳۸۶.

[26] J. twining, "a Naturalistic Journey into the Collaboratory: in Search-Hrast," Texas woman's university, Texas, 2000.

[۲۷] حسن دانایی‌فرد، «استراتژی‌های نظریه‌پردازی»، تهران، سمت، ۱۳۸۹.

[28] A. Strauss and J. M. Corbin, Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, SAGE Publications, 1998.

[۲۹] باقر. انصاری، «تدوین قراردادهای نمونه و اطلاع‌رسانی درباره شیوه استفاده آن‌ها»، سازوکارهای حقوقی حمایت از تولید علم، تهران، سمت، ۱۳۸۷.

[۳۰] حمیدرضا .فرتوک زاده، محمدرضا. دره شیری محمد. محبی، «بررسی گلوگاه‌های قوانین مالی و معاملاتی صنایع دفاعی در تعامل با شبکه همکاران»، مدیریت بهبود، ش. ۱۳، صص. ۶۴-۸۴، ۱۳۹۱.

[31] R. Langner, "To Kill a Centrifuge A Technical Analysis of What Stuxnet's Creators Tried to Achieve," The Langner Group, Arlington, Hamburg, Munich, 2013.

[32] W. D. Eggers, "The changing nature of government: network governance," 2005.

[33] C. Folke, T. Hahn, P. Olsson and J. Norberg, "Adaptive governance of social-ecological systems," Annual Review of Environment and Resources, vol. 30, pp. 441-473, 2005.

[34] R. Rhodes, "Understanding Governance: Ten Years On," Organization Studies, vol. 28, pp. 1243-1264, 2007.

[35] O. Treib, H. Bähr and G. Falkner, "Modes of Governance: A Note Towards Conceptual Clarification," EUROPÄISCHE GOVERNANCE PAPERS, vol. 17, pp. 1-22, 2005.

[36] J. N. Rosenau, "Governance, order, and change in world politics," in Governance without Government: Order and Change in World Politics, Cambridge, Cambridge University Press, 1992, pp. 1-29.

[37] N. Hertting and E. Vedung, "Purposes and criteria in network governance evaluation: How far does standard evaluation vocabulary takes us?," Evaluation, pp. 27-46, 2012.

[38] A. Maturo, "Network Governance as a Response to Risk Society Dilemmas: A Proposal from the Sociology of Health," Topoi, vol. 23, pp. 195-202, 2004.

[39] D. F. Kettl, "The Next Government of the United States: Challenges for Performance in the 21st Century," IBM Center for the Business of Government, Washington, 2005.

[40] B. G. Glaser and A. L. Strauss, The Discovery of Grounded Theory Strategies for Qualitative Research, New Brunswick: aldine transaction, 1967.