Presenting an Ontology Model of Cyberspace Sovereignty:
In Order to Provide a Comprehensive Definition

Hatef Rasouli
PostDos Researcher; Faculty of Management and Economics;
Tarbiat Modares University; Tehran, Iran;
Email: hatef.rasouli@modares.ac.ir

Mohammad Hassanzadeh*
Professor; Faculty of Management and Economics;
Department of Information and Knowledge Science;
Tarbiat Modares; Tehran, Iran Email: hasanzadeh@modares.ac.ir

Samaneh Rahimian
PhD Candidate in Information and Knowledge Management;
Faculty of Management and Economics; Tarbiat Modares;
Tehran, Iran Email: s_rahimian@modares.ac.ir

Iranian Journal of Information Processing and Management

Received: 05, Feb. 2023 **Accepted: 12, Jul. 2023**

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Vol. 39 | No. 2 | pp. 425-452
Winter 2024
https://doi.org/10.22034/jipm.2023.706799

Abstract: Cyberspace is a society that has been formed in the context of information and communication technology. This space has no territorial boundaries and is not governed by a single power. The ability of computer networks to go beyond the modern concept of time and space has significant consequences for governance based on state-nation relations. Due to increasing lack of communication control in cyberspace, traditional methods of governance are weakening. Therefore, issues such as the governance model of the cyber space and governance practices, cyber border guarding, monitoring, control, privacy protection, virtual society structure architecture appropriate to the native society are raised. Also, due to increasing need of people for virtual space, cyberspace sovereignty has become an important part of the governance of real national space. Therefore, the existence of cyberspace sovereignty is necessary and important. This research has been done with the aim of providing a comprehensive and complete definition for cyberspace sovereignty by using ontology tools.

This research is a qualitative research according to different definitions and viewpoints in the field of cyberspace governance, while examining the theoretical foundations of cyberspace sovereignty. Through up-to-date and reliable sources and documents (2004-2022) and using theme analysis method, that important components and themes were identified in the field of cyberspace sovereignty. Based on the themes obtained,

* Corresponding Author

the ontology of cyberspace sovereignty was extracted. Finally, a more comprehensive definition of cyberspace sovereignty was provided by organizing entities related to cyberspace sovereignty through the extraction of its ontology.
According to the findings, 17 components related to cyberspace sovereignty have been introduced, which form the entities of the main ontology model of cyberspace sovereignty. Based on the findings, these 17 components are: type of governance, basic principles of governance, legal governance, approaches to cyberspace sovereignty, guiding principles, beneficiaries of cyberspace sovereignty, multi-stakeholder approach to cyberspace sovereignty, governance of digital platforms, cyber space regulation, cyber assets, internet governance, network governance distributed and decentralized, digital economy, thematic areas, digital transformation, digital knowledge and talent, and cyber justice.
The extracted ontology shows the classes and their relationships in the domain of Cyberspace sovereignty basics. Despite the findings of this research and the presentation of ontology based on documents and evidence, a detailed understanding of the domain of cyberspace sovereignty is possible. The extracted ontology has helped in the structural organization of cyberspace sovereignty knowledge and at the same time makes a suitable format for understanding how to use the above knowledge.

Keywords: Anthology, Sovereignty, Cyberspace, Cyberspace Sovereignty

ارائه الگوی هستی‌شناسی حاکمیت فضای سایبر: طرح یک تعریف جامع

هاتف رسولی
دکتری مدیریت فناوری اطلاعات؛ پژوهشگر پسادکتری؛ دانشکده مدیریت و اقتصاد؛ دانشگاه تربیت مدرس؛ تهران، ایران hatef.rasouli@modares.ac.ir

محمد حسن‌زاده
دکتری مدیریت اطلاعات و دانش؛ استاد؛ دانشکده مدیریت و اقتصاد؛ دانشگاه تربیت مدرس؛ تهران، ایران؛ پدیدآور رابط hasanzadeh@modares.ac.ir

سمانه رحیمیان
دانشجوی دکتری مدیریت اطلاعات و دانش؛ دانشکده مدیریت و اقتصاد؛ دانشگاه تربیت مدرس؛ تهران، ایران؛ s_rahimian@modares.ac.ir

پژوهش‌نامهٔ پردازش و مدیریت اطلاعات

دریافت: ۱۴۰۱/۱۱/۱۶ **پذیرش:** ۱۴۰۲/۰۴/۲۱ مقاله برای اصلاح به مدت ۱۷ روز نزد پدیدآوران بوده است.

نشریهٔ علمی | رتبهٔ بین‌المللی
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISTA، ISC، و SCOPUS
jipm.irandoc.ac.ir
دورهٔ ۳۹ | شمارهٔ ۲ | ص‌ص ۴۲۵-۴۵۲
زمستان ۱۴۰۲
https://doi.org/10.22034/jipm.2023.706799

چکیده: فضای سایبر جامعه‌ای است که در بستر فناوری اطلاعات و ارتباطات شکل گرفته است. این فضا دارای مرزهای سرزمینی نیست و در ظاهر توسط قدرت واحدی اداره نمی‌شود. توانایی شبکه‌های رایانه‌ای برای فراتر رفتن از مفهوم مدرن زمان و مکان، عواقب قابل توجهی برای حکومت‌داری بر اساس روابط دولت-ملت دارد. به‌دلیل کمبود فزاینده کنترل ارتباطات در فضای سایبر، روش‌های سنتی حکومت‌کردن در حال سست‌شدن هستند. از این‌رو، مسائلی مانند الگوی حکمرانی فضای سایبر و اعمال حاکمیت، مرزبانی سایبری، نظارت، کنترل، حفظ حریم خصوصی، معماری ساختار جامعه مجازی متناسب با جامعه بومی مطرح می‌گردد. همچنین با توجه به نیاز روزافزون انسان‌ها به فضای مجازی، حاکمیت فضای سایبر به بخش مهمی از حاکمیت فضای واقعی ملی تبدیل گردیده است. بنابراین، وجود حاکمیت در فضای سایبری امری ضروری و حائز اهمیت است. بر این اساس، هدف پژوهش حاضر ارائه تعریفی جامع و کامل از حاکمیت فضای سایبر با استفاده از ابزار هستی‌شناسی است.
در این پژوهش که یک پژوهش کیفی است، با توجه به تعاریف و دیدگاه‌های مختلف در حیطه حاکمیت فضای سایبر، ضمن بررسی مبانی نظری حاکمیت فضای سایبر از طریق منابع و اسناد به‌روز و معتبر (سال‌های ۲۰۰۴-۲۰۲۲) و تحلیل آن‌ها با استفاده از روش تحلیل مضمون، مؤلفه‌ها و مضامین حائز اهمیت در حوزه حاکمیت فضای سایبر شناسایی

گردید. بر اساس مضامین به‌دست آمده، هستی‌شناسی حاکمیت فضای سایبری استخراج شد. سرانجام، با سازماندهی موجودیت‌های مرتبط با حاکمیت فضای سایبر از طریق استخراج هستی‌شناسی آن، تعریفی جامع‌تر از حاکمیت فضای سایبر ارائه گردید.
با توجه به یافته‌ها، ۱۷ مؤلفه مرتبط با حاکمیت فضای سایبر معرفی شده است که موجودیت‌های الگوی اصلی هستی‌شناسی حاکمیت فضای سایبر را تشکیل می‌دهند. بر اساس یافته‌ها، ۱۷ مؤلفه عبارت‌اند از: نوع حاکمیت، اصول اساسی حاکمیت، حاکمیت حقوقی، رویکردهای حاکمیت سایبری، اصول هدایت‌گر، ذی‌نفعان حاکمیت سایبری، رویکرد چندذی‌نفعی حاکمیت سایبری، حاکمیت پلتفرم‌های دیجیتال، تنظیم‌گری فضای مجازی، دارایی‌های سایبری، حاکمیت اینترنت، حاکمیت شبکه‌های توزیع‌شده و غیرمتمرکز، اقتصاد دیجیتال، حوزه‌های موضوعی، تحول دیجیتال، دانش و استعداد دیجیتال، و عدالت سایبری. هستی‌شناسی استخراج‌شده در این پژوهش، کلاس‌ها و روابط آن‌ها را در حوزه مبانی حاکمیت فضای سایبر نشان می‌دهد. با وجود یافته‌های این پژوهش و ارائه هستی‌شناسی مبتنی بر اسناد و شواهد متقن، فهم دقیق قلمرو حاکمیت فضای سایبر امکان‌پذیر شده است. هستی‌شناسی استخراج‌شده به سازماندهی ساختاری دانش حاکمیت فضای سایبر کمک کرده و همزمان قالب مناسبی را در جهت چگونگی استفاده از دانش فوق قابل درک می‌کند.

کلیدواژه‌ها: هستی‌شناسی، حاکمیت، فضای سایبر، حاکمیت فضای سایبر

۱. مقدمه

یکی از بنیادی‌ترین مفاهیم علوم سیاسی، مفهوم حاکمیت است؛ مفهومی که در بطن دولت مدرن جای دارد و با مفاهیم مهم سیاسی مانند قدرت، نظم، مشروعیت و اقتدار مرتبط است. مفهوم حاکمیت در یک طبقه‌بندی به دو بعد داخلی و خارجی تقسیم می‌شود که در بعد داخلی به مفهوم اراده برتر نسبت به تمام اراده‌های جزئی در یک سرزمین و در بعد خارجی به معنای حاکمیتی است که در روابط بین دولت‌ها ظاهر می‌گردد و مستلزم استقلال و نفی هرگونه تبعیت یا وابستگی در برابر دولت‌های خارجی است. دولت مظهر حاکمیت داخلی و خارجی است که قدرت برتر را اعمال می‌کند (عالم ۱۴۰۱، ۲۴۳-۲۶۶). البته قدرت و رفتار دولت‌ها در عصر حاضر نیز به قیدهای مختلفی محدود شده است. برخی قیدها مانند قانون اساسی که قدرت سیاسی را چارچوب‌بندی می‌کند، داخلی و برخی قیدها مانند قواعد و الزامات نظام حقوق بین‌الملل (همچون حقوق بشر، معاهدات و قواعد آمره) خارجی هستند. استقلال در امور خارجی نیز امری نسبی است. در واقع، استقلال تبلور حاکمیت دولت‌ها در ارتباط با کشورهای دیگری است که دربرگیرنده صلاحیت‌های دولت در امور برون‌مرزی و درون‌مرزی می‌شود. یکی از مهم‌ترین اصول بین‌المللی پذیرفته‌شده که در کنوانسیون‌های متعدد و اساسنامه سازمان‌های مختلف بین‌المللی از جمله منشور ملل متحد به آن

اشاره شده، **اصل برابری حاکمیت دولت‌ها**ست. مفاد این اصل بیان می‌کند که کلیه دولت‌ها دارای حق حاکمیت برابرند و این حق باید از سوی سایر دولت‌ها نیز محترم شمرده شود (منشور سازمان ملل ۱۹۴۵[1]). همه دولت‌ها حقوق و وظایف برابر دارند و بدون در نظر داشتن تفاوت‌های اقتصادی، اجتماعی، سیاسی، جمعیتی، جغرافیایی و غیره، تمامی اعضا از حقوق یکسانی در جامعه بین‌المللی برخوردارند (خلیلی‌نژاد ۱۳۹۹). بنابراین، حاکمیت به لحاظ لفظی، «اقتدار اعمال اراده» معنا می‌شود.

حاکمیت فضای سایبر محصول جدیدی است که از طریق ایده‌های سنتی حاکمیت، تحت هدایت علم و فناوری توسعه یافته است (Zhao 2022, 101). به بیان دیگر، حاکمیت فضای سایبر گسترش طبیعی و تجلی حاکمیت ملی یک کشور به بستری مبتنی بر فناوری اطلاعات و ارتباطات است. در داخل یک کشور، حاکمیت فضای مجازی به توسعه، نظارت و مدیریت مستقل کشور بر امور اینترنتی خود اشاره دارد. در خارج کشور، حاکمیت فضای مجازی به جلوگیری از نفوذ و حملات خارجی به اینترنت کشور اشاره دارد. بر اساس محتوای «منشور ملل متحد» و «حقوق بین‌الملل»، چهار حق اساسی حاکمیت ملی را می‌توان به‌طور خلاصه بیان کرد: برابری[2]، استقلال[3]، قلمرو و قدرت[4]، و دفاع از خود[5]. همان‌طور که در جدول زیر اشاره شده، این چهار حق، مفاهیم جدیدی را ارائه می‌دهند که به فضای مجازی نیز بسط داده می‌شوند.

جدول ۱. بسط حاکمیت ملی سنتی به فضای مجازی (Ning 2022)

مقوله حاکمیت	معنای سنتی	معنای فضای سایبری
برابری	همه کشورها از صلاحیت‌ها و هویت‌های برابر برای مشارکت در روابط بین‌المللی برخوردارند.	کشورهای مستقل در اتصال به شبکه و عملیات شبکه از وضعیت برابری برخوردارند و از حق مساوی برای صحبت و مشارکت در حاکمیت فضای سایبری بین‌المللی برخوردارند.
استقلال	هر کشوری حق رسیدگی به امور داخلی و خارجی خود به میل خود و بدون هیچ‌گونه کنترل و دخالت خارجی دارد.	شبکه هر کشور می‌تواند به‌طور مستقل عمل کند، خدمات را به‌دلیل تداخل سایر کشورها متوقف نکند و به‌طور مستقل خط‌مشی اینترنت خود را تنظیم کند.
قلمرو و قدرت	قدرت یک دولت برای اعمال صلاحیت قضایی بر همه مردم و اشیا در قلمرو خود است.	حق یک دولت مستقل برای اعمال قدرت بر فضای سایبری در قلمرو خود است.
دفاع از خود	هنگامی که کشوری مورد حمله مسلحانه قرار می‌گیرد، حق مقاومت در برابر حمله به تنهایی یا با سایر کشورها را دارد.	کشورهای مستقل این قدرت را دارند که در صورت هرگونه حمله و تهدید فضای سایبری خارجی اقدامات دفاعی خود را انجام دهند.

1. charter of the united nations and statute of the international court of justice
2. equal
3. independence
4. jurisdiction
5. self-defense

با این حال، فضای سایبر انعکاسی از دنیای واقعی و فضای نامحدود و بی‌نظم است. مخفی بودن و باز بودن اینترنت، انتشار شایعات اینترنتی را تسهیل می‌کند و نظم اجتماعی را به‌طور جدی مختل می‌سازد. در مواجهه با هرج‌ومرج ناشی از بی‌نظمی فضای سایبری، همه کشورها به اتفاق آرا تصمیم گرفتندکه حاکمیت فضای سایبر را تقویت کنند. در فضای سایبری روندی از «احیای حاکمیت ملی» وجود دارد: لیبرالیسم فضای سایبر کاهش یافته و واقع‌گرایی فضای سایبر به‌شدت بازگشته است (Ning 2022, 131). همچنین دو نگرش نسبت به حاکمیت در فضای سایبر مطرح است. طبق نگرش اول، فضای سایبر همچون سرزمینِ قابل تقسیم میان دولت‌هاست و دولت، یگانه مرجعی است که می‌تواند صلاحیت قانون‌گذاری خود را بر فضای سایبر اعمال کند. طبق دیدگاه دوم، فضای سایبر به مثابهٔ میراث مشترک بشریت است که حاکمیت هیچ دولتی به نحو انفرادی و انحصاری بر آن امکان‌پذیر نیست. دیدگاه اول، حاصل پذیرش مفهوم وستفالیایی حاکمیت[1] در فضای سایبر است. حامیان این نگرش بر این باورند که دولت، بهترین نهاد حاکمیتی موجود در فضای سایبر است. در دیدگاه دوم، دو نظریه «متعلق به همه»[2] و «میراث مشترک بشریت»[3] حائز اهمیت است (ضیایی و شکیب‌نژاد ۱۳۹۶، ۲-۴). همچنین، هنگامی که فضای سایبری خارجی بتواند استاندارد خاصی از امنیت جهانی را از طریق روش یا مکانیسم خاصی حفظ کند، قدرت جدیدی برای ترویج «بالکانیزاسیون»[4] فضای سایبری ایجاد می‌شود.

با این حال، مفهوم حاکمیت فضای مجازی در سراسر جهان گسترش یافته و جامعه بین‌المللی در حال تقویت همکاری برای حفاظت از فضای مجازی جهانی است. مقررات روزافزون تأیید می‌کند که حاکمیت فضای سایبری امتداد حاکمیت ملی سنتی است (Ning 2022, 137).

در این راستا هستی‌شناسی حاکمیت فضای سایبری خلاصه و توصیف ماهیت فضای سایبر است که به معنای توصیف عناصر کلی فضای مجازی برای درک همه‌جانبه آن و تعمیم حاکمیت دولت‌ها بر آن خواهد بود. در یک مفهوم کلی، از طریق هستی‌شناسی حاکمیت فضای سایبر به سؤالاتی مانند سؤالات زیر پاسخ داده می‌شود:

فضای سایبری چیست؟ رابطه بین فضای سایبری و حاکمیت سنتی چیست؟ و اگر

1. Westphalian sovereignty 2. Res communis 3. common heritage of mankind

۴. بالکانی شدن یا تجزیه‌شدن، به تقسیم یک منطقه یا حاکمیت چندقومیتی یا ملیتی به حکومت‌های کوچکی گفته می‌شود که از لحاظ قومیتی همگن و یکدست هستند.

وجود داشته باشد و قابل دفاع باشد، چه عناصر کلیدی در حاکمیت فضای سایبری حایز اهمیت هستند (Zhao 2022)؟ بر این اساس، هدف پژوهش فوق ارائه تعریفی جامع و کامل از حاکمیت فضای سایبر با استفاده از ابزار هستی‌شناسی است که فهم دقیق قلمرو حاکمیت فضای سایبر را امکان‌پذیر سازد.

۲. پیشینه پژوهش

هستی‌شناسی یا آنتولوژی اصطلاحی فلسفی است که به آنچه هست با رویکردی حقیقت‌محور می‌پردازد (Berryman 2019). آنچه در فعالیت‌های مرتبط به ساخت هستی‌شناسی‌ها صورت می‌گیرد، زیرمجموعه‌ای از فعالیت‌های حوزه مهندسی دانش است. با ساخت هستی‌شناسی‌ها، معرفی واژگان و مفاهیم، جست‌وجوپذیری مفاهیم و روابط میان آن‌ها و بازیابی دانش به‌وجود می‌آید و امکان به‌اشتراک‌گذاری اطلاعات موضوعی و تخصصی دامنهٔ مورد بررسی فراهم می‌شود (تقی‌زاده، فهیم‌نیا و نقشینه ۱۳۹۸). بنابراین، هستی‌شناسی‌ها **ساختاری برای بیان ویژگی‌های دقیق و مشخص از یک مفهوم** هستند که شامل تعاریف مفاهیم پایهٔ یک دامنهٔ موضوعی و روابط معنایی میان آن‌هاست. بنابراین، از طریق استخراج هستی‌شناسی حاکمیت فضای سایبر می‌توان دانشی جامع از این حوزه ارائه داد. **در جست‌وجوی ادبیات پژوهش مرتبط با هستی‌شناسی حاکمیت فضای سایبر، پژوهشی یافت نشد. بنابراین در ادامه، به پژوهش‌هایی مرتبط در این حیطه اشاره می‌شود.** «سید زارین»، در پژوهشی با عنوان «هستی‌شناسی امنیت سایبری یکپارچه» به هستی‌شناسی امنیت سایبری یکپارچه که تعدادی از هستی‌شناسی‌های امنیت سایبری موجود و همچنین مفاهیم موجود در ابرداده‌های بازپیوندی است، می‌پردازد (SyedZareen et al. 2016). مشابه آنچه در این هستی‌شناسی انجام شده، DBpedia[1] است که به‌عنوان هسته دانش عمومی در ابرداده‌های بازپیوندی عمل می‌کند. در این پژوهش تلاش شده امنیت سایبری یکپارچه به‌عنوان هسته‌ای برای حوزه امنیت سایبری پیش‌بینی شود که با گذشت زمان با مجموعه داده‌های امنیت سایبری اضافی، تکامل یافته و رشد کند. به ادعای نویسندگان، این پژوهش اولین مقاله هستی‌شناسی امنیت سایبری است که برای پشتیبانی از موارد استفاده گسترده‌تر و متنوع‌تر از امنیت فضای سایبر، به هستی‌شناسی‌های جهانی-عمومی نگاشت شده است.

1. https://www.dbpedia.org/

«پاستازوک، بورک وسزپولسکی» در پژوهشی با عنوان «هستی‌شناسی امنیت سایبری برای تحلیل دینامیکی سیستم‌های فناوری اطلاعات» به ارائه هستی‌شناسی امنیت سایبر می‌پردازند. این پژوهش دارای هدف سه‌گانه است: در این پژوهش ابتدا، هستی‌شناسی‌های امنیت سایبری موجود بررسی و کاستی‌های آن شناسایی می‌شود. در مرحله بعد، چارچوبی بر اساس هستی‌شناسی امنیت سایبری پویا معرفی و پیشنهاد می‌شود که شکاف‌های موجود را پر کند. سرانجام، یک سیستم نظارتی بر اساس هستی‌شناسی توسعه‌یافته ترسیم می‌شود که مکانیزم‌های داده‌کاوی خودکار را پیاده‌سازی کرده و نتایج حاصل از منابع دانش پویا، مانند Shodan[1] یا Censys[2] را جمع‌آوری می‌کند. سرانجام، نتایج این پژوهش نشان می‌دهد که با در نظر گرفتن این سه هدف، بررسی هستی‌شناختی سیستم‌ها در طول زمان امکان‌پذیر است (Pastuszuk, Burek & Księżopolski 2021).

«فن، تان و لی» در پژوهشی مشابه با عنوان «روش سلسله‌مراتبی ارزیابی وضعیت امنیت سایبری بر اساس هستی‌شناسی و نقشه‌های شناختی فازی» به روش ارزیابی وضعیت امنیت سایبری سلسله‌مراتبی به ترسیم هستی‌شناسی و نقشه‌های شناختی فازی[3] می‌پردازند. آن‌ها در مرحله اول، رویدادهای امنیت سایبری را از راه‌های مختلف جمع‌آوری و یک رویداد عمومی خطر امنیت سایبری را با توجه به توصیف ساختاریافته رویدادها بر اساس هستی‌شناسی ایجاد کردند. آن‌ها در مرحله بعد، ساختار FCM را با توجه به رویدادهای عمومی خطر امنیت سایبری با استفاده از روش ساخت FCM به‌صورت نیمه‌خودکار تولید و سرانجام، وضعیت امنیت سایبری را بر اساس هستی‌شناسی و FCM ارزیابی و کمی‌سازی کردند و آنگاه، سطح وضعیت امنیت سایبری را بر اساس جدول سطح ریسک امنیت سایبری مربوط تعیین نمودند (Fan, Tan & Li 2024).

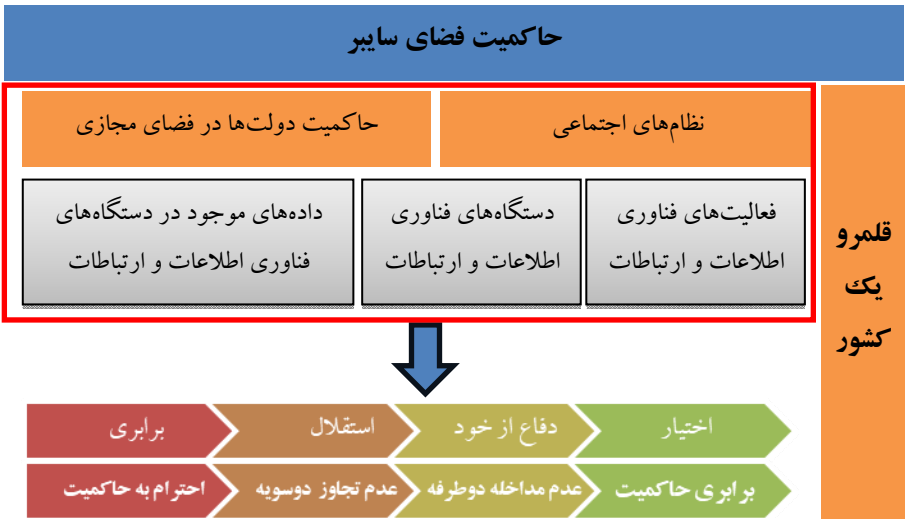
«جانسون» و همکاران نیز در پژوهشی با عنوان «مدل‌سازی معنایی کمپین‌های نفوذ سایبری[4]: مدل هستی‌شناسی و مطالعات موردی» یک مدل هستی‌شناختی جدید از CIC ارائه می‌کنند. در این پژوهش با استفاده از مطالعه موردی، مدلی هستی‌شناسانه با پیوندها و ساختار داده‌های متناسب برای تجزیه‌وتحلیل همزمان هر دو حوزه فیزیکی و سایبری ارائه می‌دهند (Johnson et al. 2021).

1. Shodan Search Engine
2. Censys Search
3. fuzzy cognitive map (FCM)
4. Cyber intrusion campaigns (CIC)

در پژوهش De Rosa et al. (2022) با عنوان «هستی‌شناسی برای حاکمیت امنیت سایبری سیستم‌های ICT» نیز هستی‌شناسی حاکمیت امنیت سایبری برای سیستم‌های فناوری ارتباطات و اطلاعات طراحی شده است. همچنین «مارتین‌ز» در پژوهشی با عنوان «چارچوبی برای توصیف مفهومی هستی‌شناسی‌ها و کاربرد آن در حوزه امنیت سایبری»، به جست‌وجوی آثار قبلی که هستی‌شناسی‌های امنیت سایبری را مورد بررسی قرار داده‌اند، پرداخته است. در این راستا بیست‌وهشت هستی‌شناسی یافت شده و بر اساس آن یک اعتبارسنجی اصطلاحی امنیت سایبری و چارچوبی برای طبقه‌بندی هستی‌شناسی‌ها طراحی و ارائه گردیده است. سرانجام، دو مورد از بهترین شیوه‌ها برای بهبود رویکرد هستی‌شناختی در حوزه امنیت سایبری توسط پژوهشگر ارائه می‌شود (Martins 2022).

بررسی پژوهش‌های فوق حاکی از آن است که در ایران و خارج از ایران پژوهش مستقل و جامعی در خصوص ارائه الگوی هستی‌شناسی حاکمیت فضای سایبر در راستای ارائه یک تعریف جامع از آن انجام نگرفته و پژوهشگران به ارائه چارچوبی برای طبقه‌بندی هستی‌شناسی‌ها و ساخت مدل هستی‌شناختی به موضوعاتی از قبیل امنیت سایبری و امنیت سیستم‌های فناوری اطلاعات پرداخته‌اند. همچنین در مقالاتی مروری و منابع آنلاین از قبیل «ویکی‌پدیا»، سخنرانی‌ها، وبلاگ و منابع اینترنتی قابل دسترس دیگر در «گوگل»، تاریخچه و تعاریف متعددی از حاکمیت فضای سایبر آمده است. آنچه از بررسی این منابع به‌دست می‌آید، تعریف زیر از حاکمیت فضای سایبر است (شکل ۱):

«حاکمیت فضای سایبر تعمیمی طبیعی از حاکمیت دولت‌ها در فضای مجازی است که توسط زیرساخت‌های فناوری اطلاعاتی و ارتباطاتی که در قلمرو سرزمینی یک کشور واقع شده است، میزبانی می‌شود. به‌عبارت دیگر، دولت‌ها صلاحیت و حق مداخله در فعالیت‌های فناوری اطلاعات و ارتباطات (در ارتباط با بازیگران و فرایندهای موجود در فضای مجازی)، دستگاه‌های فناوری اطلاعات و ارتباطات (در رابطه با زیرساخت‌ها)، داده‌های موجود در دستگاه‌های فناوری اطلاعات و ارتباطات (دارایی‌های مجازی) و همچنین نظامات اجتماعی شکل گرفته از تعاملات مبتنی بر شبکه فناوری اطلاعات و ارتباطات (فاوا) (نظام‌های اجتماعی) در حوزه قلمرو سرزمینی کشور خود را دارند (Binxing 2018).



شکل ۱. تعریف حاکمیت فضای سایبر بر اساس مرور پیشینه پژوهش

بر اساس شکل ۱، حاکمیت فضای سایبر از حاکمیت ملی ناشی می‌شود و بسیاری از ویژگی‌های آن از قبیل چهار عنصر اصلی قلمرو، مردم، منابع، و نظام و چهار حق مسلم برابری، استقلال، دفاع از خود، و اختیار و چهار اصل اساسی احترام به حاکمیت، عدم تجاوز دوسو، عدم مداخله دوطرفه در امور داخلی یکدیگر و برابری حاکمیت را دارد (فانگ ۱۳۹۷، ۱۲۲).

همچنین بر اساس بررسی پیشینه پژوهش‌ها مشخص گردید که پژوهشی جامع در حوزه استخراج هستی‌شناسی مرتبط با حاکمیت فضای سایبر انجام نشده و هستی‌شناسی استخراج‌شده در این پژوهش می‌تواند به سازماندهی ساختاری دانش حاکمیت فضای سایبر کمک کند.

۳. روش پژوهش

پژوهش حاضر از نوع پژوهش کیفی است. در مرحله نخست، مرور و بررسی مبانی نظری حوزه مبانی حاکمیت فضای سایبر با هدف استخراج ابعاد، مؤلفه‌ها و زیرمؤلفه‌های مرتبط با حاکمیت فضای سایبر انجام گرفت. با استفاده از ابزار «گوگل ترندز»[1] مشاهده

1. Google Trends

شـد کـه از سـال ۲۰۰۴، بـه ایـن واژه بیشـتر توجـه شـده و در جسـت‌وجوهای اینترنتـی مـورد اسـتفاده قـرار گرفتـه اسـت.

شکل ۲. روند جست‌وجوی حاکمیت فضای سایبر در موتورهای جست‌وجو (۲۰۰۴-۲۰۲۲)

بـر ایـن اسـاس، مقـالات و اسـناد در پایـگاه اطلاعاتی«گـوگل اسـکولار»[1] در بـازه زمانـی سـال‌های ۲۰۰۴ تـا ۲۰۲۲، کـه در عنـوان خـود حاکمیـت فضـای سـایبر[2] و یـا در کلیدواژه‌هـای خـود حاکمیـت فضـای سـایبر را داشـته‌اند، مـورد بازیابـی قـرار گرفتنـد. نکتـه حائـز اهمیـت در شـکل ۲، ایـن اسـت کـه بیشـترین جسـت‌وجوی حـوزه حاکمیـت فضـای سـایبر در سـال‌های ۲۰۰۴ تـا ۲۰۰۹ بـوده اسـت. تعـداد مقـالات و اسـناد بازیابی‌شـده در ایـن راسـتا ۱۵۶ مقالـه وکتـاب بـوده اسـت. در بررسـی اولیـه به‌دلیـل تکـراری بـودن تعاریـف حاکمیـت فضـای سـایبر در متـون مـورد نظـر، پژوهشـگران از اشـباع نظـری اسـتفاده کردنـد. بـر ایـن اسـاس، مطالعـه متـون تـا زمانـی ادامـه پیـدا کـرد کـه هیـچ داده جدیـدی از داده‌هـای موجـود حاصـل نگردیـد. سـرانجام، کفایـت داده‌هـای گردآوری‌شـده بـا مطالعـه ۴۷ مقالـه و دو کتـاب حاصـل شـد. ابعـاد، مؤلفه‌هـا و زیرمؤلفه‌هایـی کـه بـا مبانـی حاکمیـت فضـای سـایبر مرتبـط بودنـد بـا اسـتفاده از روش تحلیـل مضمـون شناسـایی و اسـتخراج شـدند. بسـیاری از پژوهشـگران معتقدنـد تحلیـل مضمـون فراینـدی اسـت کـه توسـط بسـیاری از روش‌هـای کیفـی اسـتفاده می‌شـود و روشـی مجـزا نیسـت، بلکـه می‌تـوان از آن بـرای کمـک بـه پژوهشـگران در تحلیـل اسـتفاده کـرد (Holloway & Todres 2003; Ryan & Bernard 2000). در مقابـل، برخـی پژوهشـگران ادعـا کرده‌انـد کـه تحلیـل مضمـون بایـد بـه تنهایـی یـک روش در نظـر گرفتـه شـود (Braun & Clarke 2006; King 2004; Leininger 1992; Thorne 2000). بـر ایـن اسـاس، «بـراون و کلارک» تحلیـل مضمـون را روشـی بـرای شـناخت، تجزیه‌وتحلیـل و گـزارش الگوهـای موجـود در داده‌هـای کیفـی می‌داننـد تـا داده‌هـای پراکنـده

1. google scholar
2. cyberspace sovereignty

و متنوع را به داده‌هایی غنی و تفصیلی تبدیل کند (Braun & Clarke 2006). در این پژوهش از روش تحلیل قالب مضامین استفاده شده است. ویژگی اساسی این روش سازماندهی سلسله‌مراتبی مضامین و احصای مضامین سطوح پایین‌تر در قالب خوشه‌ها و ایجاد مضامین سطح بالاتر از آن‌ها است (King 2004, 263). با تعیین روش تحلیل قالب مضمون به‌منظور شناسایی و استخراج مؤلفه‌ها و زیرمؤلفه‌های مبانی حاکمیت فضای سایبر، مراحل کدگذاری دستی و سپس جهت اطمینان از فرایند انجام‌شده، مراحل کدگذاری از طریق نرم‌افزار «مکس‌کیودا ۲۰۲۰»[1] انجام گرفت. تعداد کدهای اولیه ۹۱ کد بوده است. مضامین مرتبط با تعاریف حاکمیت فضای سایبر از بخش‌های کدگذاری‌شده استخراج، پالایش و مورد بازبینی واقع گردید. سرانجام، از ۹۱ کد استخراج‌شده، تعداد ۱۷ کد به‌عنوان مضامین اصلی استخراج گردید.

برای ساخت الگوی هستی‌شناسی حاکمیت فضای سایبر از طریق فرایند دستی، از استراتژی «نوی و مک‌گینس»[2] (۲۰۰۱) به‌نام مهندسی دانش ساده[3] استفاده شد. بر این اساس، مراحل زیر انجام گرفت:

۱. تعیین حوزه و دامنه هستی‌شناسی: طراحی و توسعه یک هستی‌شناسی با تعریف دامنه و محدوده آن شروع می‌شود. پاسخ به سؤالاتی مانند:
   - ◇ حوزه‌ای که هستی‌شناسی باید پوشش دهد، چیست؟
   - ◇ برای چه می‌خواهیم از هستی‌شناسی استفاده کنیم؟
   - ◇ برای چه نوع سؤالاتی می‌بایست اطلاعات موجود در هستی‌شناسی پاسخگو باشد؟
   - ◇ چه‌کسی از هستی‌شناسی استفاده خواهد کرد؟
۲. استفاده مجدد از هستی‌شناسی‌های موجود: بررسی اینکه آیا می‌توان از هستی‌شناسی‌های موجود برای اصلاح و گسترش دامنه و حوزه خاص خود استفاده کرد؟
۳. تعیین اصطلاحات مهم در هستی‌شناسی: نوشتن فهرستی از تمامی اصطلاحاتی که در هستی‌شناسی مفید خواهد بود و پاسخ به سؤالاتی از قبیل:
   - ◇ درباره چه اصطلاحاتی می‌خواهیم صحبت کنیم؟
   - ◇ این اصطلاحات چه ویژگی‌هایی دارند؟
   - ◇ می‌خواهیم در مورد آن اصطلاحات چه بگوییم؟

1. Maxqda 2020 2. Noy & McGuinness 3. A Simple Knowledge-Engineering Methodology

۴. تعیین سلسله‌مراتب بین کلاس‌ها: برای انجام این مرحله از فرایند توسعه بالا به پایین استفاده گردید. بر این اساس، هستی‌شناسی با تعاریف مفاهیم عام آغاز می‌شود و با ایجاد کلاس‌ها و زیرکلاس‌های خاص‌تر فرایند توسعه هستی‌شناسی ادامه می‌یابد؛
۵. توصیف ویژگی‌های کلاس‌ها-چهریزه‌ها: ویژگی‌ها و روابط در نرم‌افزار «پروتژه» با روابط معنایی مضامین مستخرج در این هستی‌شناسی تکمیل گردید. بر این اساس، می‌توان از سه دسته روابطِ رابطه شیء (بیان ارتباط میان نمونه‌ها)، رابطه نوع داده (ایجاد رابطه میان نمونه‌ها و مقادیر نوع داده الگوی RDF, XML) و رابطه تفسیری (افزودن اطلاعات و توضیحات لازم به کلاس‌ها، نمونه‌ها و روابط شیء و نوع داده) (صنعت‌جو و فتحیان ۱۳۹۱) استفاده کرد؛
۶. تعریف چهریزه‌های ویژگی‌ها: در هستی‌شناسی باید برای هر یک از روابط چهریزه‌هایی مانند نوع مقادیر، مقادیر مجاز، تعداد مقادیر و سایر ویژگی‌های مقادیر که چهریزه‌ها می‌توانند دارا باشند، توصیف کرد؛
۷. ایجاد نمونه‌ها: مرحله آخر، ایجاد نمونه‌های منفرد از هر کلاس است. نمونه‌های هر کلاس مستلزم انتخاب همان کلاس، ایجاد یک نمونه مستقل و پرکردن ویژگی‌ها با مقادیر مجاز است.

همچنین در این پژوهش برای ترسیم هستی‌شناسی، از نرم‌افزار «پروتژه» استفاده گردید. در بین نرم‌افزارهای موجود جهت طراحی و ویرایش هستی‌شناسی‌ها، «پروتژه» جایگاه ویژه‌ای دارد. این نرم‌افزار یک ویرایشگر هستی‌شناسی متن باز، رایگان و یک سیستم مدیریت دانش است. همچنین این نرم‌افزار یک رابط کاربری گرافیکی برای تعریف هستی‌شناسی‌ها فراهم می‌کند که شامل طبقه‌بندی‌کننده‌های قیاسی برای تأیید سازگاری مدل‌ها و استنتاج اطلاعات جدید بر اساس تجزیه‌وتحلیل یک هستی‌شناسی است[1].

٤. یافته‌ها

بر اساس یافته‌های پژوهش حاضر، ۱۷ مؤلفه به‌عنوان مضامین سطح اول، ۸۵ مؤلفه به‌عنوان مضامین سطح دوم، و ۳۸ مؤلفه به‌عنوان مضامین سطح سوم در ارتباط با تعریف حاکمیت فضای سایبر شناسایی گردید. جدول ۳، نتایج یافته‌های این بخش را نشان می‌دهد.

1. https://protege.stanford.edu/

جدول ۲. مضامین مربوط به مؤلفه‌های استخراج‌شده

مضامین سطح اول	مضامین سطح دوم	مضامین سطح سوم
نوع حاکمیت	حاکمیت داخلی (ملی)	برابری
		استقلال
		قلمرو و قدرت
		دفاع از خود
	حاکمیت خارجی (بین‌المللی)	احترام به حاکمیت
		عدم تجاوز دوسویه
		عدم مداخله دوطرفه در امور داخلی یکدیگر
		برابری حاکمیت
		استقلال
		حق اعمال اقتدار
		قدرت
		نظم
		مشروعیت
		اقتدار
اصول اساسی حاکمیت	احترام به حاکمیت	–
	عدم تجاوز دوسویه	–
	عدم مداخله دوطرفه در امور داخلی یکدیگر	–
	برابری حاکمیت	–
	استقلال	–
	حق اعمال اقتدار	–
	قدرت	–
	نظم	–
	مشروعیت	–
	اقتدار	–

مضامین سطح اول	مضامین سطح دوم	مضامین سطح سوم
رویکردهای حاکمیت سایبری	حاکمیت با فضای سایبر	–
	حاکمیت بر فضای سایبر	–
	حاکمیت در فضای سایبر	–
اصول هدایت‌گر حاکمیت سایبری	پاسخگویی	–
	شفافیت	–
	حاکمیت قانون	–
	مشارکت	–
	اثربخشی	–
	کارایی	–
ذی‌نفعان حاکمیت سایبری	دولت	–
	بخش خصوصی	–
	جامعه مدنی	–
	جامعه فنی	–
	جامعه دانشگاهی	–
	کاربران	–
رویکرد چندذی‌نفعی حاکمیت سایبری	همکاری‌های داخلی	روابط میان بخش خصوصی و عمومی
		ائتلاف‌های محلی
	همکاری‌های بین‌المللی	روابط بین دولت‌ها
		ائتلاف‌های بین‌المللی
حاکمیت پلتفرم‌های دیجیتال	حکمرانی بر پلتفرم‌ها	–
	حکمرانی در پلتفرم‌ها	–
	حکمرانی به‌واسطه پلتفرم‌ها	–
تنظیم‌گری فضای مجازی	تنظیم‌گری مبتنی بر کدگذاری	–
	تنظیم‌گری از طریق استانداردها و شبکه فضای مجازی	–
	تنظیم‌گری ترکیبی	–
	تنظیم‌گری چندقطبی و بخشی	–
	تنظیم‌گری پویا	–

مضامین سطح اول	مضامین سطح دوم	مضامین سطح سوم
دارایی‌های سایبری	دارایی‌های فناوری (سخت‌افزار، نرم‌افزار، سیستم‌ها، سرورها، شبکه‌ها)	–
	دارایی‌های اطلاعاتی (داده‌ها و اطلاعات ارزشمند)	–
حاکمیت اینترنت	اینترنت ماهواره‌ای	–
	اینترنت کوانتومی	–
حاکمیت شبکه‌های توزیع‌شده و غیرمتمرکز	رمزارزها	–
	شبکه ملی اطلاعات	–
	فضای رادیویی	–
	شبکه مخابرات و تلگراف	–
	شبکه‌های ماهواره‌ای	–
	اینترنت اشیا	–
	فضای ابری	–
حاکمیت حقوقی	نظام حقوقی ملی	–
	نظام حقوقی بین‌الملل	–
	جرم‌انگاری سایبری	تحریک کودکان به خشونت
		سوءاستفاده جنسی از کودکان و هرزه‌نگاری از آن‌ها
		حملات سایبری
		جعل
		فیشینگ
		جاسوسی سایبری
		تروریسم سایبری
	حوزه قضایی	بازدارندگی
		اختیارات قضایی
		مجازات
		جبران خسارت

مضامین سطح اول	مضامین سطح دوم	مضامین سطح سوم
اقتصاد دیجیتال	تجارت الکترونیک	–
	دولت الکترونیک	–
حوزه‌های موضوعی حاکمیت سایبر	رسانههای اجتماعی	شبکه اجتماعی
		کنترل و هدایت افکار عمومی
		تولید محتوا
	مدیریت هویت دیجیتال	–
	مدیریت بحران سایبری	–
	دیپلماسی سایبری	–
	حاکمیت داده/ اطلاعات	دسترسی آزاد به اطلاعات
		به اشتراک‌گذاری داده بین مرزی
	ظرفیت سایبری	–
	پدافند غیرعامل	–
	پدافند عامل	–
	مدیریت حوادث امنیت اطلاعات	–
	دفاع سایبری	–
	حاکمیت فناوری اطلاعات	–
	شهر هوشمند	–
	کنترل بر زیرساخت‌های سایبری	–
	مدیریت دسترسی دیجیتال	–
	مدیریت ریسک فضای سایبر	–
	امنیت سایبری	–
	حریم خصوصی	کنترل داده‌های شخصی
	محیط زیست	تغییرات اقلیمی
تحول دیجیتال	فناوری‌های تحول‌آفرین	–
	نوآوری فناوری سبز	–
دانش و استعداد دیجیتال	آگاهی و آموزش عمومی	–
	سواد دیجیتال جامعه	شکاف مهارتی

مضامین سطح اول	مضامین سطح دوم	مضامین سطح سوم
عدالت سایبری	هنجارهای اجتماعی	–
	اصول اخلاقی	–
	حفظ حقوق شهروندی	–
	حقوق اساسی بشر	–
	تبعیض جنسیتی و خشونت علیه زنان	–
	قطع کلی اینترنت یا پایین آوردن ظرفیت اینترنت	–
	محافظت از میراث فرهنگی	–
	برابری اجتماعی	–
	حقوق کپی‌رایت	مالکیت فکری

همچنین شکل زیر ابر کلمات استخراج‌شده در تعاریف حاکمیت فضای سایبر از متون مورد مطالعه است که در نرم‌افزار «مکس کیودا ۲۰۲۰» کدگذاری شده است.

شکل ۳. ابر کلمات تعاریف مبانی حاکمیت فضای سایبر

در تصویر فوق درجه وزنی کلمات با اندازه‌ای که در تصویر نمایش داده شده، ارتباطی مستقیم دارد. کلمات و واژگانی که بالاترین فراوانی واژگانی را در بررسی متون داشته‌اند، در تعاریف حاکمیت فضای سایبر استفاده شده‌اند. یافته‌های مرحله نهایی طراحی الگوی

هستی‌شناسانه برای شناسایی روابط بین مضامین و ارائه یک تعریف جامع‌تر از حاکمیت فضای سایبر به‌صورت زیر است:

۱. تعیین حوزه و دامنه هستی‌شناسی: دامنه هستی‌شناسی در پژوهش فوق شامل مضامین، مفاهیم و روابط معنایی مرتبط با تعاریف حاکمیت فضای سایبر در مقالات و اسناد مورد بررسی است؛

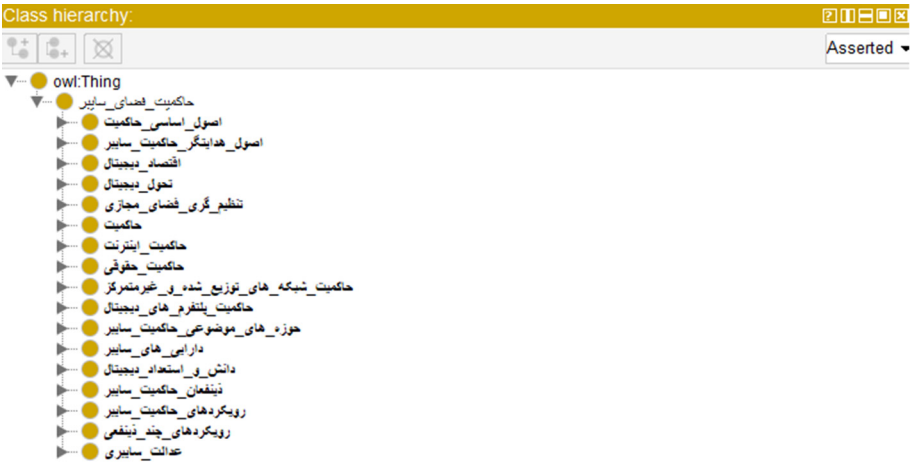
۲. استفاده دوباره از هستی‌شناسی‌های موجود: بر اساس بررسی‌های انجام‌گرفته هستی‌شناسی در حوزه مبانی حاکمیت فضای سایبر یافت نگردید؛

۳. تعیین اصطلاحات مهم در هستی‌شناسی: در این مرحله جفت‌های مفهومی و روابط آن‌ها شناسایی شدند. جدول زیر مثالی از جفت مفهومی را نشان می‌دهد:

جدول ۳. تعیین جفت معنایی بر اساس مفاهیم و رابطه معنایی

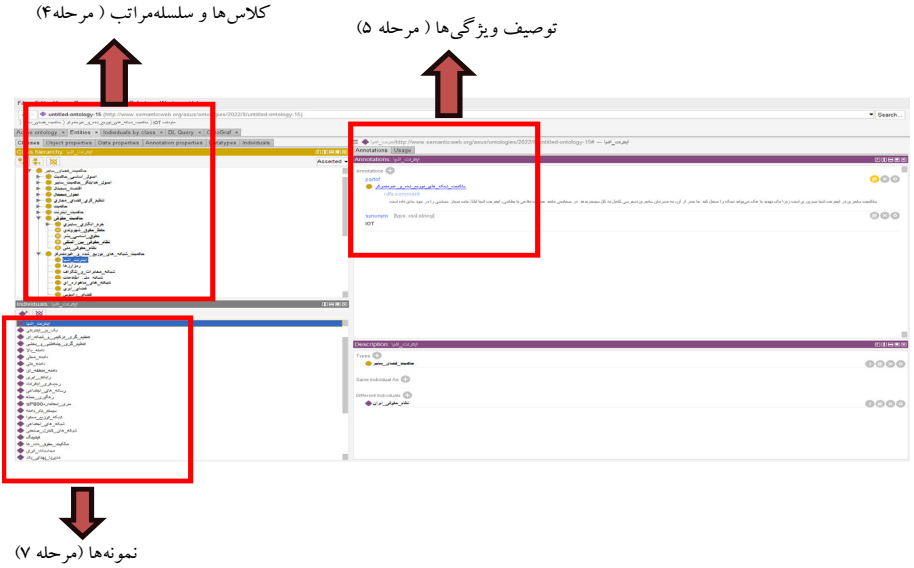
مفهوم یا رابطه مشاهده‌شده در متون	مفهوم یا رابطه برگزیده‌شده
امنیت فضای سایبر	حاکمیت فضای سایبر
مرزبانی فضای سایبر	
کنترل فضای سایبر	

۴. تعیین سلسله‌مراتب بین کلاس‌ها: برای انجام این مرحله از توسعه بالا به پایین استفاده گردید. شکل ۴، تقسیم‌بندی کلاس‌ها را در نرم‌افزار «پروتژه» نشان می‌دهد. بر این اساس، کلاس‌های اصلی عبارت‌اند از: نوع حاکمیت، اصول اساسی حاکمیت، رویکردهای حاکمیت سایبری، اصول هدایت‌گر حاکمیت سایبری، ذی‌نفعان حاکمیت سایبری، رویکرد چندذی‌نفعی حاکمیت سایبری، حاکمیت پلتفرم‌های دیجیتال، تنظیم‌گری فضای مجازی، دارایی‌های سایبری، حاکمیت اینترنت، حاکمیت شبکه‌های توزیع‌شده و غیرمتمرکز، حاکمیت حقوقی، اقتصاد دیجیتال، حوزه‌های موضوعی حاکمیت سایبر، تحول دیجیتال، دانش و استعداد دیجیتال، و عدالت سایبری؛



شکل ٤. تقسیم‌بندی کلاس‌ها

۵. توصیف ویژگی‌های کلاس‌ها- چهریزه‌ها: شکل ۵، بخشی از ویژگی‌های کلاس‌ها و روابط آن‌ها را نشان می‌دهد. به‌عنوان مثال، رابطه «synonym» و رابطه «partof» از نوع رابطه تفسیری[1] در هستی‌شناسی فوق بوده است.



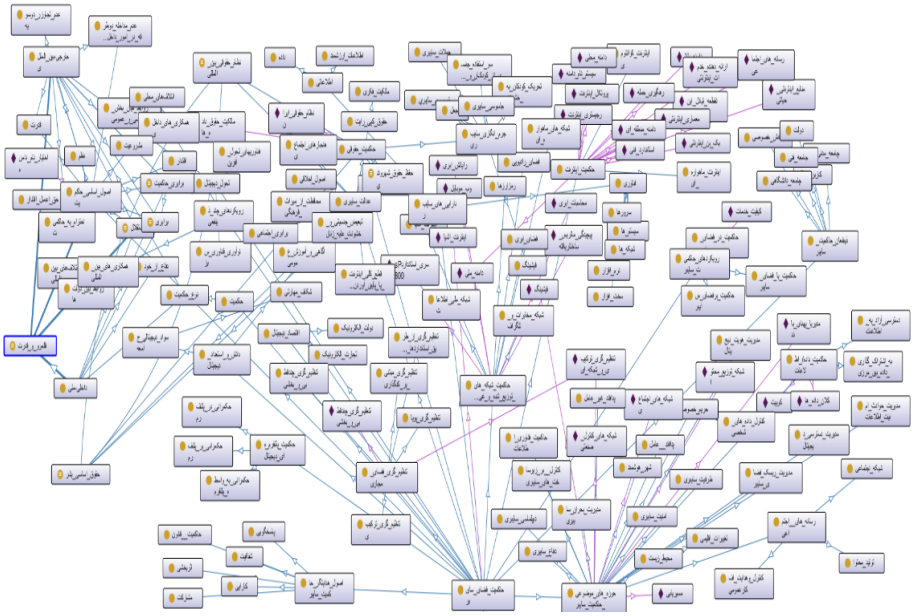
شکل ۵. بخش کلاس‌ها و نمونه‌ها

1. annotation properties

۶. تعریف چهریزه‌های ویژگی‌ها: در این مرحله می‌بایست برای هر یک از روابط هستی‌شناسی، چهریزه‌هایی مانند نوع مقادیر[1]، مقادیر مجاز[2]، تعداد آن‌ها[3] تعریف شود. چهریزه‌ها در هستی‌شناسی برای تعیین دامنه و محدوده[4] روابط بین نمونه‌ها استفاده می‌شود. به‌عنوان مثال، ویژگی "some" می‌تواند با نمونه‌های متفاوت به‌کار رود. بر این اساس، تنظیم‌گری ترکیبی، شبکه‌ای، چندقطبی و چندبخشی؛ بخشی از تنظیم‌گری فضای سایبر هستند. همچنین نوع مقادیر آن‌ها string (مقادیر حرفی) است.

۷. ایجاد نمونه‌ها: مرحله آخر در ساخت هستی‌شناسی پژوهش فوق، ایجاد نمونه‌های مربوط به هر کلاس است. ویژگی‌های توصیف‌کننده نمونه‌ها شامل نام نمونه، مترادف و روابط بین نمونه‌هاست. شکل ۵، نمونه‌های هستی‌شناسی فوق را نشان می‌دهد. در مجموع ۳۵ نمونه در این قسمت وارد شده است.

بر اساس مراحل گفته‌شده، شکل ۶، مفاهیم، نمونه‌ها، کلاس‌ها و روابط آن‌ها را در هستی‌شناسی حاکمیت فضای سایبر نشان می‌دهد. با استخراج مضامین از متون منتخب حاکمیت فضای سایبر، الگوی اصلی هستی‌شناسی حاکمیت فضای سایبر ترسیم گردید. خطوط آبی، روابط معنایی کلاس‌ها و زیر کلاس‌ها و خطوط بنفش روابط معنایی نمونه‌ها را نشان می‌دهد.



شکل ٦. هستی‌شناسی حاکمیت فضای سایبر

1. value type
2. allowed values
3. the number of the values (cardinality)
4. domain and range

۵. بحث و نتیجه‌گیری

در این پژوهش با توجه به تعاریف و دیدگاه‌های مختلف در حیطه حاکمیت فضای سایبر، تلاش گردید ضمن بررسی مبانی نظری حاکمیت فضای سایبر از طریق منابع و اسناد به‌روز و معتبر و تحلیل آن‌ها از طریق روش تحلیل مضمون، مؤلفه‌ها و مضامین حائز اهمیت برای ارائه تعریفی جامع‌تر از حاکمیت فضای سایبر شناسایی شود و با ابزار هستی‌شناسی الگوی این تعریف ترسیم گردد. یافته‌های پژوهش‌های انجام‌شده توسط SyedZareen et al. (2016)؛ Martins (2022)؛ De Rosa et al. (2022)؛ Johnson et al. (2021)؛ Jakub et al. (2021) و Fan, Tan & Li (2021) نشان می‌دهند که ترسیم هستی‌شناسی‌های استخراج‌شده در این پژوهش‌ها به سازماندهی ساختاری دانش فضای سایبر کمک می‌کند. در این پژوهش نیز با سازماندهی موجودیت‌های مرتبط با حاکمیت فضای سایبر از طریق استخراج هستی‌شناسی آن، تعریفی جامع‌تر از حاکمیت فضای سایبر ارائه می‌گردد. در این تعریف هفده مؤلفه به‌عنوان مؤلفه‌های اصلی تعریف حاکمیت فضای سایبر بیان شده است که موجودیت‌های الگوی اصلی هستی‌شناسی حاکمیت فضای سایبر را تشکیل می‌دهند:

۱. نوع حاکمیت- نوع حاکمیت به دو بعد داخلی (اراده برتر نسبت به تمام اراده‌های جزئی در یک سرزمین) و خارجی (روابط بین دولت‌ها) تقسیم می‌شود (خلیلی‌نژاد ۱۳۹۹)؛

۲. اصول اساسی حاکمیت- این اصول شامل این موارد می‌شوند:

پاسخگویی: انتظارات روشنی از ارائه‌دهندگان امنیتی وجود دارد و مقامات مستقل بر برآورده‌شدن این انتظارات نظارت می‌کنند و در صورت عدم تحقق آن‌ها تحریم‌ها را اعمال می‌کنند.

شفافیت: اطلاعات برای کسانی که تحت تأثیر تصمیمات و اجرای آن‌ها قرار گرفته‌اند، آزادانه در دسترس و قابل دسترسی است.

حاکمیت قانون: همه افراد و نهادها، از جمله دولت، تابع قوانینی هستند که به‌طور عمومی شناخته شده، بی‌طرفانه اجرا می‌شوند و با معیارهای بین‌المللی و ملی حقوق بشر مطابقت دارند (DCAF 2019)؛

۳. حاکمیت حقوقی- قدرت برتر فرماندهی یا امکان اعمال اراده‌ای فوق اراده‌های دیگر است؛ بدین معنا که در حوزه اقتدار آن دارای نیرویی است خودجوش که از نیروی دیگری برنمی‌خیزد و قدرت دیگری که بتواند با او برابری کند، وجود ندارد. در

مقابـل اعمـال اراده و اجـرای اقتـدار خـود مانعـی را نمی‌پذیـرد و از هیـچ قـدرت دیگـری تبعیـت نمی‌کنـد (قاضـی ۱۴۰۰)؛

۴. رویکردهای حاکمیت سایبری- این رویکردها به سه بخش تقسیم می‌شود:

حاکمیـت بـا فضـای سـایبر: در ایـن رویکـرد از فضـای مجـازی به‌عنـوان ابـزار خدمت‌رسـانی و اعمـال حاکمیـت در فضـای حقیقی اسـتفاده می‌شـود. آنچـه به‌عنـوان دولـت الکترونیک مطرح می‌شود در این سطح است.

حاکمیـت بـر فضـای سـایبر: بـر ایـن اسـاس، دولت‌هـا فضـای مجـازی را به‌عنـوان یکـی از اجـزای زندگـی مـردم تحت حاکمیـت درمی‌آورند و آن را متناسـب بـا قوانین موجـود در کنار سـایر اجـزا مدیریـت می‌نماینـد. به‌عبارتـی، حاکمیـت بـر فضـای سـایبر وضعیتـی اسـت کـه حاکمیـت ملـی بتوانـد فضـای مجـازی را به‌منزلـه بخشـی از قلمرو خـود، تحت قـوه آمرانه خود قرار دهد.

و سـرانجام، حاکمیـت در فضـای سـایبر: در ایـن رویکـرد دولت‌هـا تحـول زندگـی بشـر را در عصـر فضـای سـایبر به‌خوبـی درک کـرده و می‌پذیرنـد کـه فضـای سـایبر فقـط مولـد پـاره‌ای از مسائل نیست، بلکه کلیت فضای زندگی مردم را می‌سازد (چمنی ۱۴۰۰)؛

۵. اصـول هدایت‌گـر حاکمیـت سـایبری- به‌کارگیـری اصـول هدایت‌گـر حاکمیـت فضـای سـایبر صحیـح بـرای حاکمیـت فضـای سـایبر، تأمیـن امنیـت، مدیریـت و نظـارت در فضـای سـایبر لازم و ضـروری اسـت. از ایـن اصـول می‌تـوان پاسـخگویی، شـفافیت، حاکمیـت قانـون، مشـارکت، اثربخشـی و کارایـی را نـام بـرد (DCAF 2019)؛

۶. ذی‌نفعـان حاکمیـت سـایبری- مطابـق بیانیـه NETmundial که در ۲۴ آوریـل ۲۰۱۴ در برزیل بـه تصویـب رسـید، حاکمیـت فضـای سـایبر می‌بایسـت بـر اسـاس فرایندهـای دموکراتیـک، چندجانبـه، تضمیـن مشـارکت معنـادار و پاسـخگوی همـه ذی‌نفعـان در ایـن حـوزه از جملـه دولـت، بخـش خصوصـی، جامعـه مدنـی، جامعـه فنـی، جامعـه دانشـگاهی و کاربـران باشـد؛

۷. رویکـرد چندذی‌نفعـی حاکمیـت سـایبری- بـر اسـاس ایـن رویکـرد، راهبـری اینترنـت، توسـعه و اسـتفاده دولت‌هـا، بخـش خصوصـی و جامعـه مدنـی از اصـول، هنجارهـا، قوانیـن، روندهـای تصمیم‌گیـری و برنامه‌هـای مشـترک بـرای شـکل دادن بـه نحـوه تکامـل و اسـتفاده از اینترنـت اسـت. بـر ایـن اسـاس، حاکمیـت فضـای سـایبر، شـامل موضوعـات سیاسـت عمومـی و تکنیکـی بـوده و بایـد تمامـی ذینفعـان و سـازمان‌های دولتـی و بین‌المللـی مرتبـط در آن مشـارکت کننـد (Klyton 2018)؛

۸. حاکمیت پلتفرم‌های دیجیتال- بر این اساس، سه رویکرد را می‌توان تعریف نمود:
حاکمیت بر پلتفرم‌ها: حاکمیت بر پلتفرم به معنای سیاست‌هایی است که برای مشخص‌کردن مسئولیت‌ها یا عدم مسئولیت‌های پلتفرم‌ها در برابر محتواها و فعالیت‌های کاربرانشان ظاهر شده است (Gillespie 2018).
حاکمیت در پلتفرم‌ها: این نوع حاکمیت شامل اصول و قواعد گوناگون اخلاقی، حقوقی و فرهنگی و نیز ابزارهای فنی است که توسط خود پلتفرم‌ها با هدف قاعده‌مندسازی محتوای نابهنجار را شامل می‌شود (Zwart 2018).
حاکمیت به‌واسطه پلتفرم‌ها: این نوع حاکمیت به معنای تخصیص و کاربرد ابزارهای نوین پلتفرم‌ها توسط دولت‌ها و حکومت‌ها به‌منظور ارائه خدمات گوناگون به شهروندان و ایجاد ارتباط با آن‌هاست (Helberger, Pierson and Poell 2018)؛
۹. تنظیم‌گری فضای مجازی- در فضای مجازی کدها همه‌چیز را تنظیم می‌کنند. اینترنت به‌عنوان نمود کاملی از فضای مجازی نیز از کدها تشکیل شده است. معماری سیستم در فضای مجازی نوعی تنظیم‌گری است که معمار سیستم، تنظیم‌گر آن است (Folsom 2007). حاکمیت فضای سایبر می‌تواند بر قواعد تدوین تنظیم‌گری با اِعمال ابزارهای مختلف، بسته به میزان خاص بودن آن‌ها نظارت کند؛
۱۰. دارایی‌های سایبری- این دارایی‌ها شامل دارایی‌های اطلاعاتی (داده‌ها و اطلاعات ارزشمند) و دارایی‌های فناوری امن (سخت‌افزار، نرم‌افزار، سیستم‌ها، سرورها، شبکه‌ها) است که وظیفه جمع‌آوری، پردازش، ذخیره و به اشتراک‌گذاری اطلاعات و داده را دارند (Keck 2022)؛
۱۱. حاکمیت اینترنت- حاکمیت اینترنت عبارت است از اصول، هنجارها، قواعد، آئین‌های تصمیم‌گیری مشترک و برنامه‌هایی که منجر به شکل‌گیری، تحول و استفاده از اینترنت می‌گردد (Report of the Working Group on the Internet Governance 2005)؛
۱۲. حاکمیت شبکه‌های توزیع‌شده و غیرمتمرکز- فضای ابری، اینترنت اشیا، شبکه‌های ماهواره‌ای، شبکه‌های مخابرات و تلگراف، فضای رادیویی، شبکه ملی اطلاعات، رمزارزها از جمله این شبکه‌ها هستند که در حاکمیت فضای سایبر می‌بایست لحاظ شوند؛
۱۳. اقتصاد دیجیتال- اقتصاد دیجیتال شامل دولت الکترونیک و تجارت الکترونیک است. پلتفرم‌های دولت الکترونیک و تجارت الکترونیک شامل فرایندهایی از قبیل تراکنش‌های الکترونیک (اینترنتی)، پرداخت الکترونیک و پول الکترونیک است که

می‌بایست در برابر تهدیدات سایبری محافظت شوند (E-commerce cyber security: an introduction for online merchants 2020). این محافظت از طریق حاکمیت فضای سایبری اعمال می‌شود؛

۱۴. حوزه‌های موضوعی حاکمیت سایبر- در تعریف جامع از حاکمیت فضای سایبر می‌بایست حوزه‌های موضوعی مرتبط به آن نیز در نظر گرفته شود. از جمله این حوزه‌ها می‌توان موارد زیر را نام برد: محیط زیست و شرایط اقلیمی، حریم خصوصی، رسانه‌های اجتماعی، حاکمیت داده/ اطلاعات؛

۱۵. تحول دیجیتال- برای موفقیت تحول دیجیتال، حاکمیت سایبری باید به‌عنوان یک محرک مهم در نظر گرفته شود. کسب‌وکارهای دیجیتال باید امنیت را در هسته سیستم‌ها و فرایندهای خود تعبیه کنند (Security for Digital Transformation 2021). بر این اساس، مفاهیم تحول دیجیتال می‌باید در تعریف حاکمیت فضای سایبر در نظر گرفته شود؛

۱۶. دانش و استعداد دیجیتال- آگاهی، آموزش و سواد دیجیتالی در سطح عموم جامعه و نیز در سطوح تخصصی می‌بایست در تعریف و اعمال حاکمیت فضای سایبر در نظر گرفته شود؛

۱۷. عدالت سایبری- حاکمیت فضای سایبری مربوط به فضای اینترنتی است و تمرکز اصلی بر روی روش اداره این فضا گذارده می‌شود. روشی که با توجه به اینکه تمامی کشورهایی که در آن وجود دارند باید به‌گونه‌ای در اداره آن سهیم باشند تا بتوان عدالت را در آن برقرار کرد. بنابراین، عدالت سایبری از جمله مؤلفه‌های مهم حاکمیت فضای سایبر است.

استفاده از ابزار هستی‌شناسی و ارائه الگوی هستی‌شناسانه حاکمیت فضای سایبر (شکل ۶) موجبات تعریفی جامع از حاکمیت فضای سایبر را فراهم آورده است. در این تعریف ۱۷ مؤلفه (کلاس‌های هستی‌شناسی) گنجانده شده است. همچنین برخی از مؤلفه‌های اصلی در تعریف حاکمیت فضای سایبر دارای زیرمؤلفه‌هایی (زیرکلاس‌های هستی‌شناسی) هستند که باید برای رسیدن به یک تعریف جامع در حاکمیت فضای سایبر مورد توجه قرار گیرند. بر اساس الگوی هستی‌شناسی حاکمیت فضای سایبر، تعریف نگارندگان از حاکمیت فضای سایبر عبارت است از: «**حاکمیت فضای سایبر، اجماع حاکمیت ملی و بین‌المللی دولت‌هاست که بر اساس اصول حاکمیت حقوقی و سایبری**

همراه با عدالت سایبری به نظارت و حکمرانی پلتفرم‌های دیجیتال، اینترنت، شبکه‌های توزیع‌شده و غیرمتمرکز، تنظیم‌گری فضای سایبر، اقتصاد دیجیتال، تحول دیجیتال و سایر حوزه‌های موضوعی مرتبط از طریق زیرساخت‌های فناورانه مرتبط، با آگاهی و آموزش‌دادن دانش و استعداد دیجیتال در جامعه، در قلمرو حاکمیتی یک کشور انجام می‌شود که می‌بایست تمامی ذی‌نفعان و سازمان‌های دولتی و بین‌المللی مرتبط در آن مشارکت داشته باشند» (شکل ۷).

شکل ۷، نشان‌دهنده مؤلفه‌ها و زیرمؤلفه‌ها (کلاس‌ها و زیرکلاس‌ها)ی به‌دست‌آمده از یافته‌های پژوهش است که در تعریفی جامع از حاکمیت فضای سایبر حایز اهمیت هستند. با توجه به تعاریف بی‌شمار از حاکمیت فضای سایبر در متون مختلف (شکل ۱)، می‌توان اذعان داشت که تعریف بیان‌شده دربردارنده اصلی‌ترین نکات در زمینه حاکمیت فضای سایبر است که می‌تواند دیدگاه روشن‌تر و جامع‌تری به محققان و کاربران در این حوزه ارائه دهد.

در راستای نتایج این پژوهش، پیشنهادهای کاربردی و پژوهشی زیر ارائه می‌گردد:

- پیشنهاد کاربردی: جمهوری اسلامی ایران برای اعمال حاکمیت و حفظ استقلال خود در فضای سایبر یک سند راهبردی در فضای مجازی (۱۴۰۱) و تنها یک کارگروه تعیین مصادیق مجرمانه داشته که ترکیب آن مناسب با کارکردهای آن نیست و در یک کلام در اعمال حاکمیت بر فضای سایبر در ایران دچار مشکل هستیم (جعفری ۱۳۹۸، ۲۳)، بنابراین الگوی آنتولوژی و تعریف جامع ارائه‌شده در این پژوهش می‌تواند در اعمال سیاست‌گذاری‌های حاکمیت فضای سایبر در کشور نقش مهمی ایفا کند؛
- پیشنهاد پژوهشی: تعریف ارائه‌شده از حاکمیت فضای سایبر بر اساس بررسی متون مرتبط بوده است. پیشنهاد می‌شود برای بسط تعریف فوق در پژوهش‌های آتی از دیدگاه خبرگان این حوزه نیز استفاده شود؛
- پیشنهاد پژوهشی: تعریف ارائه‌شده در این پژوهش یک تعریف مطلق از حاکمیت فضای سایبر نیست. بنابراین، پیشنهاد می‌شود از روش‌های دیگر از جمله تحلیل حوزه بهره‌گیری شده و مبانی حاکمیت فضای سایبر مورد بررسی قرار گیرد.

شکل ۷. تعریف حاکمیت فضای سایبر

فهرست منابع

تقی‌زاده نائینی، جواد، فاطمه فهیم‌نیا و نادر نقشینه. ۱۳۹۸. استخراج آنتولوژی هویت دیجیتال مبتنی بر تحلیل حوزه. *پژوهشنامه پردازش و مدیریت اطلاعات* ۴ (۳۴):۱۶۶۹-۱۷۰۰ .

جعفری، افشین. ۱۳۹۸. حاکمیت بر فضای سایبر از منظر حقوق بین‌الملل و نظام حقوقی جمهوری اسلامی ایران. *رهیافت انقلاب اسلامی* ۱۳ (۴۹): ۱۰۹-۱۳۲.

چمنی، ساسان. ۱۴۰۰. تحول در حکمرانی، متأثر از توسعه فضای مجازی. سومین همایش ملی و اولین همایش بین‌المللی حکمرانی متعالی. https://governanceschool.ir/file/download/download/1655292830-1200.pdf?language=fa (دسترسی در ۱۴۰۱/۱۱/۲۳)

خلیلی‌نژاد، سجاد. ۱۳۹۹. مفهوم‌شناسی حاکمیت سایبری. مرکز رشد دانشگاه امام صادق.https://rushd.ir/?p=6940 (دسترسی در ۱۴۰۱/۱۰/۱۲)

صنعت‌جو، اعظم و اکرم فتحیان. ۱۳۹۱. روش‌شناسی طراحی، ساخت و پیاده‌سازی هستی شناسی: رویکردها، زبان‌ها و ابزارها (مطالعه موردی طراحی هستی‌شناسی Asfaont در حوزه کتابداری و اطلاع‌رسانی). *فصلنامه کتابداری و اطلاع‌رسانی* ۱۵ (۵۷): ۱۱۳-۱۴۲.

ضیایی، یاسر، و احسان شکیب‌نژاد. ۱۳۹۶. قانون‌گذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران. *مجله حقوقی بین‌المللی* ۵۷ (۳۴): ۲۲۷-۲۴۹.

عالم، عبدالرحمن. ۱۴۰۱. *بنیادهای علم سیاست*. تهران: نشر نی.

قاضی، ابوالفضل. ۱۴۰۰. *حقوق اساسی و نهادهای سیاسی*. تهران: میزان.

References

Berryman, D. 2019. Ontology, Epistemology, Methodology, and Methods: Information for Librarian Researchers. *Medical Reference Services Quarterly* 38 (3): 271-279.

Binxing, F. 2018. Cyberspace Sovereignty: Reflections on Building Community of Common Future in Cyberspace. Springer pub. https://link.springer.com/book/10.1007/978-981-13-0320-3 https://treaties.un.org/doc/publication/ctc/uncharter.pdf (accessed Feb. 27, 2023)

Braun, V., & V Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3 (2): 77-101.

Charter of the united nations and statute of the international court of justice. san francisco: the united nations. 1945. https://treaties.un.org/doc/publication/ctc/uncharter.pdf (accessed Feb. 7, 2023)

DCAF. 2019. Guide to Good Governance in Cybersecurity. Le Centre pour la gouvernance du secteur de la sécurité: Genève. https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurityhttps://www.dcafch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021.pdf_Governance_ENG_Jan2021.pdf (accessed Feb. 20, 2023)

De Rosa, F., N. Maunero, L. Nicoletti, P. Prinetto, & M. Trussoni. 2022. Ontology for Cybersecurity Governance of ICT. Italian Conference on Cybersecurity https://ceur-ws.org/Vol-3260/paper4.pdf (accessed Mar. 12, 2023)

E-commerce cyber security: An introduction for online merchants. 2020. https://www.getcybersafe.gc.ca/en/blogs/e-commerce-cyber-security-introduction-online-merchants (accessed Mar. 13, 2023)

Fan, Z., C. Tan & X. Li. 2021. A hierarchical method for assessing cyber security situation based on

ontology and fuzzy cognitive maps. *International Journal of Information and Computer Security* 14 (3/4). https://www.inderscience.com/info/inarticle.php?artid=114704 (accessed Mar. 13, 2023)

Folsom, T. C .2007. Defining cyberspace (finding real virtue in the place of virtual reality). *Rutgers Computer & Technology Law Journal* 45 (9): 75.

Gillespie, T. 2018. Regulation of and by Platforms. J. Burgess (edit,(The Sage handbook of Social Media. Los Angeles & London: Sage.

Helberger, N., J. Pierson,& T. Poell. 2018. Governing online platforms: From contested to cooperative responsibility. *The Information Society* 43 (1):1-14.

Holloway, I., & L. Todres. 2003. The status of method: Flexibility, consistency and coherence. *Qualitative Research* 3: 345–357.

Johnson, N., B. Turnbull, T. Maher, & M. Reisslein. 2021. Semantically Modeling Cyber Influence Campaigns (CICs): *Ontology Model and Case Studies. IEEE 9*: 9365-9382.

Keck, M. 2022. The role of cybersecurity and data security in the digital economy. https://static1.squarespace.com/static/5f2d7a54b7f75718fa4d2eef/t/62082f066a25c62651a9ae40/1644703527175/EN-UNCDF-Brief-CyberSecurity-2022.pdf (accessed Mar. 18, 2023)

King, N. 2004. Using templates in the thematic analysis of text. In: Cassels, C. and Symon, G, Eds., *Essential Guide to Qualitative Methods in Organizational Research*. London: Sage. 256-270.

Klyton, A. 2018. The multistakeholder model of Internet governance, ICANN, and business stakeholders - practices of hegemonic power. https://gala.gre.ac.uk/id/eprint/20316/1/van%20Klyton%20%252c%20Arrieta-Paredes%20and%20Soomaree%20%282018%29.pdf (accessed Apr. 2, 2023)

Leininger, M. 1992. Current issues, problems, and trends to advance qualitative paradigmatic research methods for the future. *Qualitative Health Research* 2: 392–415.

Martins, B. S. 2022. A framework for conceptual characterization of ontologies and its application in the cybersecurity domain. S. software and Systems Modeling 21. https://www.semanticscholar.org/paper/A-framework-for-conceptual-characterization-of-and-Martins-Gil/8ddcb6afdc35aba52504fadc3ca1a20b117b348d (accessed Apr. 2, 2023)

Ning, H. 2022. *A Brief History of Cyberspace*. Oxon: CRC Press.

Noy, N. F. & D. L McGuinness. 2001. Ontology Development 101: A Guide to Creating Your First Ontology. Stanford: Stanford Knowledge Systems Laboratory Technical Report and Stanford Medical Informatics Technical Report.

Pastuszuk, J., P. Burek, & B. Księżopolski. 2021. Cybersecurity Ontology for Dynamic Analysis of IT Systems, Procedia Computer Science, Volume 192, Pages 1011-1020, https://doi.org/10.1016/j.procs.2021.08.104.

Report of the Working Group on the Internet Governance. 2005. www.wgig.org/docs/WGIGREPORT.pdf (accessed Apr. 13, 2023)

Ryan G., & H. Bernard. 2000. Data management and analysis methods. In Denzin N., Lincoln Y. (Eds.), Handbook of qualitative research (2nd ed.: 769–802). Thousand Oaks, CA: Sage.

Security for Digital Transformation. 2021. www.fujitsu.com/be/imagesgig5/cyber-security-for-digital-tranformation_eBook_2021-01.pdf (accessed Mar. 15, 2023)

SyedZareen, Z., A. Padia, T. Finin, & A. Joshi. 2016. UCO: A Unified Cybersecurity Ontology. Conference: AAAI Workshop on Artificial Intelligence for Cyber Security. https://www.researchgate.net/publication/287195565_UCO_A_Unified_Cybersecurity_Ontology (accessed Mar. 6, 2023)

Thorne S. 2000. Data analysis in qualitative research. *Evidence Based Nursing* 3: 68–70.

Zhao, H. 2022. *Cyberspace & Sovereignty*. China: Harbin Institute of Technology.

Zwart, M. 2018. Keeping the neighbourhood safe: How does social media moderation control what we see (and think*)? Alternative Law Journal* 43 (4): 283-288.

هاتف رسولی

متولد سال ۱۳۶۳، دارای مدرک تحصیلی دکتری در رشته مدیریت فناوری اطلاعات از دانشگاه آزاد اسلامی است. ایشان هم‌اکنون پژوهشگر پسادکتری و مدیرعامل شرکت دانش‌بنیان برهان در حوزه مشاوره فضای سایبر است.

مدیریت هویت دیجیتال، حاکمیت سایبری و معماری دیجیتال از جمله علایق پژوهشی وی است.

محمد حسن‌زاده

دارای مدرک تحصیلی دکتری در رشته علم اطلاعات و دانش‌شناسی از دانشگاه فردوسی مشهد است. ایشان هم‌اکنون استاد دانشگاه تربیت مدرس و رئیس پژوهشگاه علوم و فناوری اطلاعات ایران است.

مدیریت دانش، نظام‌های دانش‌محور، علم‌سنجی و ارزیابی علم و فناوری از جمله علایق پژوهشی وی است.

سمانه رحیمیان

متولد سال۱۳۶۴، دارای مدرک کارشناسی ارشد علم اطلاعات و دانش‌شناسی از دانشگاه تهران است. ایشان هم‌اکنون دانشجوی دکتری مدیریت اطلاعات و دانش در دانشگاه تربیت مدرس است.

مدیریت اطلاعات، مدیریت دانش، فلسفه علم، سازماندهی دانش و هستی‌شناسی‌ها از جمله علایق پژوهشی وی است.