Journal of Information and Communication Technology

Volume 16, Issue 61-62, Autumn and Winter 2024, pp. 261-281

The Relevance, Importance and Dependence of Critical Infrastructures of The Islamic Republic of Iran from a Cyber-Perspective

Abouzar Solat Rafiee[1], Hossain Gharaee Gharakhani[2*], Fatemeh Saghafi[3] , Mohammad Malekinia [4]

[1] Department of Management and Accounting, South Tehran Branch, Islamic Azad University, Tehran, Iran
[2] Associate Professor, ICT Security faculty, ICT Research Institute (ITRC), Tehran, Iran
[3] Associate Professor, Faculty of Management, University of Tehran, Tehran, Iran
[4] Associate Professor, Department of Management and Accounting, South Tehran Branch, Islamic Azad University, Tehran, Iran

Received: 25 June 2023, Revised: 30 September 2023, Accepted: 18 October 2023
Paper type: Research

Abstract

In recent years, cyber-attacks on the critical infrastructure of countries have increased dramatically. The types of critical infrastructure and their dependencies based on national requirements are different from one country to another. Disruption of the mission or services of a critical infrastructure has a cascading effect on other infrastructures and makes them face serious problems in service delivery. In various studies, approaches Different methods have been adopted to model these dependencies. The important point is not to generalize those models to other countries due to the national requirements of each country. In this research, by forming 11 focus groups consisting of senior and middle managers of each infrastructure field, the network analysis method based on the DEMATEL technique was used, and the most effective and influential critical infrastructure from a cyber-perspective on other critical infrastructures was identified, and the relationship between critical infrastructures and Their prioritization was determined from a cyber-perspective. The results of this research can be useful in the design of the national warning sharing system in order to calculate the national situational awareness in the cyber field and other researches based on the dependence of critical infrastructures.

Keywords: Critical Infrastructure, Critical Infrastructure dependency, DANP.

[*] Corresponding Author's email: gharaee@itrc.ac.ir

دوفصلنامه
فناوری اطلاعات و ارتباطات ایران

سال شانزدهم، شماره‌های ۶۱ و ۶۲، پاییز و زمستان ۱۴۰۳، صفحه ۲۶۱ الی ۲۸۱

ارتباط، اهمیت و وابستگی زیرساخت‌های حیاتی جمهوری اسلامی ایران از منظر سایبری

ابوذر صولت رفیعی[۱]، حسین قرائی گرکانی[۲*]، فاطمه ثقفی[۳]، محمد ملکی نیا[۴]

[۱] دانشجوی دکتری مدیریت فناوری اطلاعات دانشگاه آزاد اسلامی واحد تهران جنوب، تهران، ایران

[۲] دانشیار پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران

[۳] دانشیار دانشکدگان مدیریت دانشگاه تهران، تهران، ایران

[۴] دانشیار دانشکده مدیریت و اقتصاد دانشگاه آزاد اسلامی واحد تهران جنوب، تهران، ایران

تاریخ دریافت: ۱۴۰۲/۰۴/۰۴ تاریخ بازبینی: ۱۴۰۲/۰۷/۰۸ تاریخ پذیرش: ۱۴۰۲/۰۷/۲۶

نوع مقاله: پژوهشی

چکیده

سال‌های اخیر حملات سایبری به زیرساخت‌های حیاتی کشورها به طور چشمگیری افزایش یافته است. انواع زیرساخت حیاتی و وابستگی‌های آنها مبتنی بر مقتضیات ملی، از کشوری به کشور دیگر متفاوت است، اختلال در ماموریت یا خدمات یک زیرساخت حیاتی بصورت آبشاری در دیگر زیرساخت‌ها اثر گذاشته و آنها را با مشکلات جدی در امر خدمات‌رسانی روبرو می‌نماید، در مطالعات مختلف رویکردهای متفاوتی جهت مدلسازی این وابستگی‌ها اتخاذ شده است نکته مهم عدم تعمیم آن مدل‌ها برای دیگر کشورها به واسطه مقتضات ملی هر کشور است. در این پژوهش با تشکیل ۱۱ گروه کانونی متشکل از مدیران عالی و میانی هر حوزه زیرساختی از روش تحلیل شبکه مبتنی بر تکنیک DEMATEL استفاده شد و تاثیرگذارترین و تاثیرپذیرترین زیرساخت حیاتی از منظر سایبری بر دیگر زیرساخت‌های حیاتی شناسائی شد و ارتباط بین زیرساخت‌های حیاتی و اولویت‌بندی آنها از منظر سایبری مشخص شد. نتایج این پژوهش می‌تواند در طراحی سامانه ملی اشتراک‌گذاری هشدار به منظور احصاء آگاهی وضعیتی ملی در حوزه سایبری و دیگر پژوهش‌های متکی بر وابستگی زیرساخت‌های حیاتی مفید واقع شود.

کلیدواژگان: زیرساخت‌های حیاتی، وابستگی زیرساخت‌های حیاتی، DANP.

* رایانامهٔ نویسنده مسؤول: gharaee@itrc.ac.ir

۱- مقدمه

کشورهای مدرن به فضای سایبری، به ویژه، به فناوری اطلاعات، ارتباطات داده، دستگاه‌های تلفن همراه هوشمند و سایر خدمات متصل به سطح جهانی و محاسباتی وابسته هستند. این وابستگی شامل عملیات دولتی، دفاع ملی، زیرساخت‌های حیاتی و رونق اقتصادی است. با این حال، فضای مجازی در معرض اختلالات تصادفی و حملات مخرب از منابع مختلف است [۱]. همچنین ایالات متحده و سایر کشورهای مدرن برای حمایت از جوامع خود به مجموعه وسیعی از زیرساخت‌های حیاتی نیز وابسته هستند. زیرساخت‌ها نیز به روش‌های متعددی به یکدیگر وابسته هستند، اما در کلی‌ترین مفهوم، شبکه‌ای از وابستگی‌های متقابل را تشکیل می‌دهند به طوری که اختلال مداوم در یک زیرساخت می‌تواند عملیات در زیرساخت‌های دیگر را تخریب یا متوقف کند[۲, ۳].

بخش‌های زیرساختی حیاتی شامل تولید و انتقال انرژی، آب و فاضلاب، مراقبت‌های بهداشتی و غذا و کشاورزی و ... است. نه تنها هر یک از این بخش‌ها برای عملکرد مناسب جوامع مدرن حیاتی هستند، بلکه به یکدیگر وابسته هستند و حمله به یکی می‌تواند تأثیر مستقیمی بر دیگران داشته باشد. به عنوان مثال، سیستم مالی به شبکه برق بستگی دارد بانک‌ها نمی‌توانند برای مدت طولانی بدون برق کار کنند [۱]. در صورتی که تولید آب آشامیدنی یا تصفیه فاضلاب در نتیجه تهدیدات مداوم بر سیستم‌های آب و فاضلاب ایالات متحده تحت تأثیر قرار گیرد، شهروندان از آب آشامیدنی سالم و بهداشت محروم خواهند شد. علاوه بر این، بیمارستان‌ها نمی‌توانند کار کنند، شیلنگ‌های آتش نشانی کار نمی‌کنند و مدارس، ادارات و تأسیسات دولتی تحت تأثیر قرار خواهند گرفت. در صورتی که هر بخش زیرساخت حیاتی دیگری مورد هدف قرار گیرد، اثرات دومینوی مشابهی رخ خواهد داد.[1]

همچنین تعداد حملات سایبری‌ای که در سال‌های اخیر متوجه سرویس‌ها و زیرساخت‌های ایرانی شده به میزان قابل توجهی رسیده است. اما نکته‌ای که در این میان قابل توجه است این است که حملاتی که از دو سال قبل تا به امروز انجام شده فقط یک حمله سایبری معمولی نیستند بلکه می‌توان گفت ایران در حوزه امنیت سایبری از مهرماه سال ۹۹ وارد یک جنگ سایبری شده است[2].

مخاطره در زیرساخت‌های حیاتی صرف نظر از منبع انسانی یا طبیعی می‌تواند تأثیر و پیامدهای نگران‌کننده‌ای بر رفاه عمومی داشته باشد که به افراد، مشاغل، دولت و همچنین محیط زیست گسترش می‌یابد. جای تعجب نیست که برخی از نویسندگان پیشنهاد می‌کنند که «شکست این زیرساخت‌ها... یکی از مهم‌ترین آسیب پذیری‌های جامعه مدرن است» [۴].

در جدول ۲ به برخی تعاریف و دیدگاه‌ها در خصوص زیرساخت‌های حیاتی پرداخته شده است.

جدول ۱. برخی حملات سایبری به زیرساخت‌های حیاتی ایالات متحده آمریکا

ردیف	سال	عنوان	حمله از	حمله به	واقعه	آثار	اقدام	زیرساخت های آسیب پذیر/دیده	مرجع
۱	فوریه ۲۰۲۱	تصفیه آب اولدزمار	ارتباطات و فناوری اطلاعات	آب	سیستم های کامپیوتری یک تصفیه خانه آب در اولدزمار، فلوریدا را هک شد	هکر سطح هیدروکسید سدیم کارخانه را به طور موقت به سطح خطرناکی تغییر داد.	این تغییر بلافاصله شناسایی شد و با جداسازی منابع ذخیره آسیب دیده از مسمومیت مردم محلی جلوگیری کرد	آب سلامت محیط زیست	Lyngaas2021
۲	می ۲۰۲۱	خط لوله دولتی	ارتباطات و فناوری	انرژی	حمله باج افزار به بزرگترین خط لوله توزیع سوخت در ایالات متحده	قیمت ها افزایش یافت و عرضه سوخت برای مصرف کنندگان برای چندین هفته مختل شد.	باج به اپراتورهای باج افزار پرداخت شد.	انرژی مالی	Turton2021
۳	ژوئن ۲۰۲۱	شرکت JBS بزرگترین	ارتباطات و فناوری اطلاعات کنترل	غذایی	باج‌افزاری حیرت‌انگیز	کارخانه‌های فرآوری مرغ و گوشت گاو و سازمان های وابسته تعطیل شوند. قطع تغییر عرضه مواد غذایی بازار مصرف به طور موقت	نامعلوم	زنجیره تامین غذائی مالی	Collier2021

[1] https://www.gartner.com/en/articles/why-critical-infrastructure-attacks-are-everyone-s-problem-especially-now

[2] https://cert.ir

جدول ۲. تعاریف و دیدگاه‌ها در خصوص زیرساخت‌های حیاتی

	مرجع	سال	مضامین و دیدگاه زیرساخت حیاتی
۱	Clinton	1996	زیرساخت‌های حیاتی آنقدر حیاتی هستند که ناتوانی یا نابودی آنها تأثیری تضعیف‌کننده بر دفاع یا امنیت اقتصادی ایالات متحده خواهد داشت.[۵]
۲	US Congress	2001	زیرساخت‌های حیاتی شامل : سیستم‌ها و دارایی‌ها، اعم از فیزیکی یا مجازی، آنقدر برای ایالات متحده حیاتی هستند که ناتوانی یا نابودی این گونه سیستم‌ها و دارایی‌ها می‌تواند تأثیر تضعیف‌کننده‌ای بر امنیت، امنیت اقتصادی ملی، سلامت یا ایمنی عمومی ملی یا هر ترکیبی از آنها داشته باشد.
۳	European CounCISl	2004	زیرساخت‌های حیاتی شامل آن دسته از امکانات، شبکه‌ها، خدمات و دارایی‌های فیزیکی و فناوری اطلاعات است که در صورت اختلال یا تخریب، تأثیر جدی بر سلامت، ایمنی، امنیت یا رفاه اقتصادی شهروندان یا عملکرد مؤثر دولت‌ها خواهد داشت[۶].
۴	India (NCISIPC)	2015	زیرساخت‌های حیاتی شامل آن دسته از تأسیسات، سیستم‌ها یا مجموعه‌هایی می‌شود که ناتوانی یا تخریب آنها می‌تواند تأثیر تضعیف‌کننده‌ای بر امنیت ملی، حاکمیت، اقتصاد و رفاه اجتماعی یک کشور داشته باشد[۷].
۵	Israel	2023	زیرساخت حیاتی هر چیزی است که اخلال در آن ثبات را در جامعه تضعیف کند و در نتیجه امنیت ملی را تهدید کند. تأکید می‌شود که زیرساخت سیستمی است که اشیاء مختلف، پیوندهای بین آنها را ترکیب می‌کند و انواع خاصی از فعالیت‌های انسانی را فراهم می‌کند[۸].
۶	Japan The Information Security Policy CounCISl	2009	زیرساخت‌های حیاتی اساس زندگی اجتماعی و فعالیت‌های اقتصادی مردم است که توسط کسب‌وکارهایی شکل می‌گیرد که خدماتی را ارائه می‌دهند که جایگزینی آنها با دیگران بسیار دشوار است، اگر عملکرد آن به حالت تعلیق، زوال یا غیرقابل دسترس شدن باشد، می‌تواند تأثیرات قابل‌توجهی بر زندگی اجتماعی مردم داشته باشد[۹].
۷	Kingdom of Saudi Arabia NISS	2022	زیرساخت حیاتی به عنوان سیستم و دارایی‌ها، اعم از فیزیکی یا مجازی که ناتوانی یا نابودی چنین سیستم‌ها و دارایی‌ها می‌تواند تأثیر تضعیف‌کننده‌ای بر امنیت، امنیت اقتصادی ملی، سلامت یا ایمنی عمومی ملی یا هر ترکیبی از آنها داشته باشد[۱۰].
۸	Gheorghe et al	2006	زیرساخت‌ها حیاتی هستند زیرا خدماتی را ارائه می‌دهند که برای یک یا چند عملکرد یا ویژگی‌های عمومی دولتی یا اجتماعی حیاتی هستند. این امر می‌تواند با بقای شهروندان تا آنجایی که به امنیت جان آنها مربوط می‌شود یا به کیفیت زندگی آنها مرتبط باشد[۱۱].
۹	ITU	2008	زیرساخت حیاتی: سیستم‌ها، خدمات و عملکردهای کلیدی که اختلال یا تخریب آنها می‌تواند تأثیر تضعیف‌کننده‌ای بر سلامت و ایمنی عمومی، تجارت و امنیت ملی یا هر ترکیبی از اینها داشته باشد[۱۲].
۱۰	Australian Critical Infrastructure Resilience Strategy	2010	زیرساخت‌های حیاتی آن دسته از امکانات فیزیکی، زنجیره‌های تامین، فناوری‌های اطلاعات و شبکه‌های ارتباطی هستند که در صورت تخریب، تخریب یا غیرقابل دسترس بودن برای مدت طولانی، به طور قابل‌توجهی بر رفاه اجتماعی یا اقتصادی کشور تأثیر می‌گذارند یا بر توانایی استرالیا برای انجام دفاع ملی تأثیر می‌گذارند. امنیت ملی را تضمین کند[۱۳].
۱۱	Qatar National Cyber Security Strategy	2014	دارایی‌های فیزیکی، سیستم‌ها یا تأسیسات، که در صورت مختل شدن، به خطر افتادن یا تخریب، تأثیر جدی بر سلامت، ایمنی، امنیت یا رفاه اقتصادی قطر یا عملکرد مؤثر دولت قطر خواهد داشت[۱۴].
۱۲	NIST	2015	سیستم و دارایی‌ها، چه فیزیکی و چه مجازی، برای ایالات متحده آنقدر حیاتی هستند که ناتوانی یا نابودی چنین سیستم‌ها و دارایی‌هایی می‌تواند تأثیر تضعیف‌کننده‌ای بر امنیت، امنیت اقتصادی ملی، سلامت یا ایمنی عمومی ملی یا هر ترکیبی از این موارد داشته باشد[۱۵].
۱۳	ISO/IEC TR 27019:	2013	سازمان‌ها و امکاناتی که برای عملکرد جامعه و اقتصاد در کل ضروری است[۱۶].
۱۴	IETF RFC 449 Internet Security Glossary 2		زیرساخت‌های اطلاعاتی حیاتی: آن دسته از سیستم‌هایی که برای یک کشور آنقدر حیاتی هستند که ناتوانی یا تخریب آنها می‌تواند بر امنیت ملی، اقتصاد، یا سلامت و ایمنی عمومی تأثیر منفی بگذارد[۱۷].
۱۵	UK Centre for the Protection of National Infrastructure	2016	آن دسته از امکانات، سیستم‌ها، سایت‌ها و شبکه‌های ضروری برای عملکرد کشور و ارائه خدمات ضروری که زندگی روزمره در بریتانیا به آن بستگی دارد[۱۸].
۱۶	NATO	2013	زیرساخت حیاتی: سیستم‌ها و دارایی‌های فیزیکی یا مجازی تحت صلاحیت یک دولت که به قدری حیاتی هستند که ناتوانی یا تخریب آنها ممکن است امنیت، اقتصاد، سلامت یا ایمنی عمومی یا محیط‌زیست یک دولت را تضعیف کند[۱۹].
۱۷	Canada An Emergency Management Framework for Canada	2022	زیرساخت‌های حیاتی به فرآیندها، سیستم‌ها، امکانات، فناوری‌ها، شبکه‌ها، دارایی‌ها و خدمات ضروری برای سلامت، ایمنی، امنیت یا رفاه اقتصادی کانادایی‌ها و عملکرد موثر دولت اشاره دارد[۲۰].
۱۸	Cuba Glossary of Cyber terms	2018	زیرساخت‌های بحرانی: زیرساخت‌هایی که عملکرد آنها ضروری است و راه‌حل‌های جایگزین را نمی‌پذیرد، به همین دلیل قطع یا تخریب آن تأثیر جدی بر خدمات عمومی اساسی یا ساختارهای دولتی خواهد داشت[۲۱].
۱۹	Germany Germany Federal Ministry of the Interior, FRG	2009	ساختارها و تأسیسات سازمانی و فیزیکی از چنان اهمیت حیاتی برای جامعه و اقتصاد یک ملت برخوردار است که شکست یا تخریب آنها منجر به کمبود مداوم عرضه، اختلال قابل توجه در امنیت و امنیت عمومی یا سایر پیامدهای شگرف می‌شود[۲۲].

	مرجع	سال	مضامین و دیدگاه زیرساخت حیاتی
۲۰	Belgium Federale Overheidsdienst Binnenlandse Zaken	2011	یک زیرساخت حیاتی یک تاسیسات، سیستم یا بخشی از آن با منافع فدرال است که برای حفظ عملکردهای حیاتی اجتماعی، سلامت، ایمنی، امنیت، رفاه اقتصادی یا اجتماعی مردم ضروری است و در صورت مختل شدن یا تخریب، تاثیر قابل توجهی خواهد داشت[۲۳].
۲۱	Brazil National Cybersecurity Strategy	2020-2023	زیرساخت‌های حیاتی: شامل بخش‌هایی می‌شود که دارایی‌ها، سیستم‌ها و شبکه‌های آنها، اعم از فیزیکی یا مجازی، آن‌قدر حیاتی تلقی می‌شوند که از کار افتادن یا تخریب آنها تأثیر مخربی بر امنیت، امنیت اقتصادی ملی، سلامت یا ایمنی عمومی ملی یا هر ترکیبی از آنها خواهد داشت[۲۴].
۲۲	RUSSIA NATIONAL SECURITY OF RUSSIA - Information security	(2012)	زیرساخت حیاتی فدراسیون روسیه موضوعی است که نقض (یا خاتمه) عملیات آن منجر به از دست دادن کنترل، تخریب زیرساخت‌ها، تغییرات منفی غیرقابل برگشت (یا شکست) اقتصاد، موضوع فدراسیون روسیه یا اداری-سرزمینی می‌شود و تاثیر قابل توجهی در سلامت و ایمنی افراد ساکن در این مناطق برای دراز مدت دارد[۲۴].
۲۳	Denmark Danish Cyber and Information Security Strategy	(2022-2024)	زیرساخت‌های حیاتی: زیرساخت‌ها، شامل امکانات، سیستم‌ها، فرآیندها، شبکه‌ها، فناوری‌ها، دارایی‌ها و خدمات - لازم برای حفظ یا بازیابی عملکردهای حیاتی اجتماعی[۲۵].
۲۴	European Parliament and of the CounCISl	(2022)	زیرساخت حیاتی به معنای دارایی، تسهیلات، تجهیزات، شبکه یا سیستم، یا بخشی از دارایی، تسهیلات، تجهیزات، شبکه یا سیستم است که برای ارائه یک سرویس ضروری ضروری است[۲۶].

تعریف زیرساخت در این مقاله: به مجموعه‌ای از مراکز و تأسیسات زیربنایی و شریان‌های عمده که خدمات و نیازهای ضروری و اساسی کشور را به مردم و جامعه ارائه می‌کند، اطلاق می‌گردد؛ زیرساخت مشتمل بر فرابخش (حوزه)، بخش، زیربخش، دارایی و اجزاء آن می‌باشد.

ترکیب فهرست بخش زیرساخت حیاتی مبتنی بر موقعیت ملی، از کشوری به کشور دیگر متفاوت است. نمونه‌ای از آنها در جدول ۳ مشاهده می‌شوند. با توجه به اطلاعات قابل مشاهده در این جدول، شش بخش نخست زیرساخت حیاتی، در تمامی کشورها به عنوان زیرساخت حیاتی شناخته می‌شوند. همچنین با توجه به این جدول تعداد زیرساخت‌های موجود در هر کشور نیز مشخص شده است.

با توجه به اطلاعات موجود، و با عنایت به طرح راهبردی حفاظت از زیرساخت‌های کشور ایران مصوب شصت و ششمین جلسه کمیته دائمی (شورای‌عالی) پدافند غیرعامل در تاریخ ۲۹/ ۰۶/ ۱۴۰۱ که به تائید مقام معظّم رهبری و فرماندهی کل قوا (مدظله‌العالی) نیز رسیده است، و بر اساس ماده ۱ بند ۴ آن، حوزه‌های با اهمیت بالا: به هریک از حوزه‌های ۱ـ انرژی، ۲ـ آب، ۳ـ غذا و کشاورزی، ۴ـ حمل و نقل، ۵ ـ بهداشت و سلامت، ۶ ـ دفاعی و امنیتی، ۷ـ صنعت، ۸ ـ رسانه، ۹ـ هسته‌ای، ۱۰ـ فضا، ۱۱ـ جمعیت، ۱۲ـ حاکمیتی، ۱۳ـ خدمات ضروری و فوریتی، ۱۴ـ پولی و مالی، ۱۵ ـ ارتباطات و فناوری اطلاعات، حوزه‌های با اهمیت بالا گفته می‌شود که باتوجه به شاخص‌های زیر، حوزه‌های ؛ ۱ـ انرژی، ۲ـ آب، ۳ـ ارتباطات و فناوری اطلاعات، ۴ـ حمل‌ونقل، ۵ ـ بهداشت و سلامت، ۶ ـ غذا و کشاورزی، ۷ـ دفاعی و امنیتی و ۸ ـ حاکمیتی بعنوان حوزه‌های کلیدی از منظر پدافند غیرعامل دسته‌بندی می‌شوند. آن شاخص‌ها عبارتند از:

- اهمیت کارکرد هر حوزه در تأمین نیازهای حیاتی مردم در شرایط اضطراری
- شدت اثرگذاری بر اقتصاد، امنیت ملی و سلامت مردم
- وابستگی زیرساخت‌های سایر حوزه‌ها به عملکرد آنها
- شدّت پیامد وقوع تهدید مبتنی بر جغرافیا و جمعیت

همچنین زیرساخت حیاتی کشور را از منظر امنیت سایبری می‌توان به پنج بخش زیرساخت انرژی، زیرساخت حمل و نقل، زیرساخت ارتباطات و فناوری اطلاعات، زیرساخت مالی و زیرساخت سلامت تقسیم نمود. زیرساخت انرژی خود به ۷ بخش گاز، پتروشیمی، نفت، برق،آب، کنترل صنعتی و انرژی اتمی مطابق شکل ۱ تقسیم می‌شود.

شکل ۱. زیرساخت‌های حیاتی جمهوری اسلامی ایران از منظر سایبری

جدول ۳. مقایسه برخی زیرساخت حیاتی در چند کشور بطورنمونه

	زیرساخت	استرالیا	اتریش	بنگلادش	بلژیک	کانادا	شیلی	کرواسی	چک	اتحادیه اروپا	آمریکا	فنلاند	انگلستان	اسپانیا	کره	ایران
۱	ارتباطات و فناوری اطلاعات	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
۴	مالی	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
۵	حمل و نقل	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
۶	بهداشت و سلامت	*	*			*	*	*	*	*	*	*	*	*	*	*
۷	انرژی	*	*			*	*	*	*	*	*	*	*	*	*	*
۸	هسته‌ای							*		*	*			*	*	
۹	آب	*	*			*	*	*	*	*	*	*	*	*	*	*
۱۰	پتروشیمی		*													
۱۱	نفت			*	*											
۱۲	گاز			*	*											
۱۳	برق				*	*										
۱۴	غذا (کشاورزی)	*	*			*		*	*	*	*	*	*	*		*
۱۵	پژوهش (تحقیقات)		*							*				*		
۱۶	شبکه اجتماعی		*													
۱۷	رسانه											*				
۱۸	سیستم توزیع		*													
۱۹	امداد و نجات (خدمات اضطراری)		*								*		*			
۲۰	حاکمیتی (نهادهای قانون‌گذار)		*						*							*
۲۱	آثار تاریخی			*				*	*							
۲۲	مراکز تولید					*					*			*		
۲۳	امکانات دولتی					*			*							
۲۴	دفاعی (صنایع دفاعی) (امنیتی)					*	*				*					*
۲۵	خدمات اجتماعی						*	*								
۲۶	علم و آموزش							*								
۲۷	شیمیایی									*	*			*		
۲۸	سد سازی										*					
۲۹	امکانات تجاری										*					
۳۰	محیط زیست										*				*	
۳۱	نگهداری زیرساخت										*					

در این مرحله پنل خبرگی متشکل از متخصصان و مدیران صاحبنظردر حوزه‌های امنیت سایبری و زیرساخت‌های حیاتی با ترکیب جدول ۴ تشکیل گردید و پرسشنامه‌ای متشکل از عناوین زیرساخت‌های حیاتی به منظور تعیین زیرساخت‌های حیاتی کشور از منظر امنیت سایبری در اختیار اعضای پنل قرار گرفت.

جدول ۴. مشخصات اعضای شرکت‌کننده در پنل خبرگی

حوزه و تخصص	تعداد شرکت کنندگان داخل پنل	تحصیلات		جنسیت
امنیت سایبری، مدیریت ارتباطات و فناوری اطلاعات، ارتباطات وفناوری اطلاعات، کامپیوتر، برق و زیرساخت‌های حیاتی و پدافند غیر عامل	۳۶	دکتری	۱۲ نفر	۸ نفر زن
		کارشناسی ارشد	۲۴ نفر	۲۸ نفر مرد

پس از بررسی و تحلیل نتایج ۱۰۰ درصد شرکت کنندگان در پنل زیرساخت ارتباطات و فناوری اطلاعات، زیرساخت مالی (پولی و بانکی)، زیرساخت حمل ونقل، زیرساخت رسانه و زیر ساخت برق را از جز زیرساخت‌های حیاتی از منظر امنیت سایبری (تاثیرگذاری و تاثیرپذیری) انتخاب نمودند همچنین زیرساخت پتروشیمی و زیر ساخت گاز با کسب ۸۸/۸۸ درصد در رتبه بعدی قرار داشتند ۸۳/۳۳ و انرژی هسته‌ای و زیرساخت آب نیز امتیاز ۸۰/۵۵ درصد را به خود اختصاص دادند اما دیگر زیرساخت‌ها عددی بیش از ۵۰ درصد را کسب ننمودند.

با تطبیق نتایج حاصله از نظر خبرگان این پژوهش با اسناد بالادست و دسته‌بندی ارائه شده توسط مرکز ملی فضای مجازی و طرح راهبردی حفاظت از زیرساخت‌های کشور ایران توسط پدافند غیر عامل، نظر خبرگان این پژوه در انتخاب زیرساخت‌ها به جز زیرساخت رسانه در مستندات مذکور تایید شد.

در خصوص زیرساخت رسانه رهبر معظم انقلاب با نگاه کلان و راهبردی خود، در بیانات گوناگونی از سال‌های گذشته به مسئلهٔ «رسانه» و «جنگ رسانه‌ای» پرداخته‌اند و نکات ارزنده و مهمی در ابعاد گوناگون این مفهوم بیان داشته‌اند. از این‌رو با بهره‌گیری از بیانات ایشان فقط در بازه زمانی یک ماه اول سال ۱۴۰۲ به *نقش و اهمیت رسانه در جنگ ترکیبی بی‌سابقه دشمن* علیه امنیت ملی کشور در جدول ۵ اشاره شده است که به لزوم درنظر گرفتن زیرساخت رسانه به عنوان یک زیرساخت حیاتی و مهم تاکید دارد.

همچنین با نگاهی به گزاش مرکز ملی مدیریت امداد و هماهنگی رخدادهای رایانه‌ای در پاییز ۱۳۹۹ الی تابستان ۱۴۰۰ در جدول ۶ تعداد حملات سایبری‌ای که در سال‌های اخیر متوجه سرویس‌ها و زیرساخت‌های ایرانی شده به میزان قابل توجهی رسیده است. اما نکته قابل توجه تعداد حملاتی است که در حوزه زیرساخت رسانه صورت پذیرفته و متوجه سازمان‌های مرتبط با حوزه رسانه شده است.

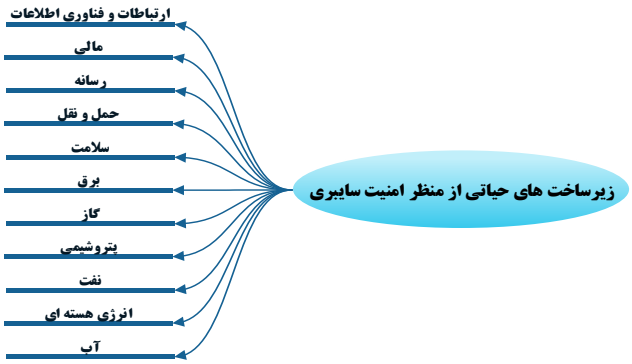
جدول ۵. بیانات رهبر معظم انقلاب در بازه یک ماه (فرودین ماه ۱۴۰۲)در خصوص مبحث رسانه و جنگ رسانه‌ای

ردیف	تاریخ	محل ایراد بیانات	بیانات معظم له
۱	۱۴۰۲/۰۱/۰۱	در اجتماع زائران و مجاوران حرم مطهر رضوی	در مقابل کودتا، در مقابل تحریم، در مقابل فشارهای سیاسی، در مقابل تهاجم رسانه‌ای؛ این تهاجم رسانه‌ای که برای ایران‌هراسی و انقلاب‌هراسی در دنیا راه انداخته‌اند، بی‌سابقه است؛ چنین چیزی هرگز وجود نداشته. در مقابل توطئه‌های امنیّتی کدام ملّت بجز ملّت ایران میتواند یا توانسته در مقابل اینها ایستادگی کند؟
۲	۱۴۰۲/۰۱/۰۱	در اجتماع زائران و مجاوران حرم مطهر رضوی	در جنگ ترکیبی، دشمن از رسانه استفاده میکند، از عامل فرهنگی استفاده میکند، از عامل امنیّتی استفاده میکند، از نفوذ استفاده میکند، از عامل اقتصادی استفاده میکند؛ از همه‌ی این عوامل استفاده میکند برای اینکه ملّت را در محاصره قرار بدهد، برای اینکه ملّت را دچار یأس کند، ملّت را از نیروی خودش غافل کند.
۳	۱۴۰۲/۰۱/۰۱	در اجتماع زائران و مجاوران حرم مطهر رضوی	یک توصیه‌ی مهمّ من به همه‌ی کسانی که توانایی سخن گفتن با مردم را دارند و رسانه در اختیارشان است ــ چه در فضای مجازی، چه در مطبوعات، چه در صدا و سیما ــ امیدآفرینی است. دشمن سعی میکند جوانهای ما را ناامید کند؛ ما باید متقابلاً امیدآفرینی کنیم.
۴	۱۴۰۲/۰۱/۱۵	در دیدار مسئولان نظام	انصافاً گاهی انسان فکرهای بسیار خوب، بسیار نو مشاهده میکند؛ خب اینها امکانات کشور است؛ اینها همه باید در خدمت مهار تورّم و رشد تولید قرار بگیرد. امکانات اجرائی داریم، امکانات تقنینی داریم، امکانات قضائی داریم، امکانات رسانه‌ای داریم، تجربه‌ها و عناصر مجرّب داریم؛ آمریکا با فشار تحریم میخواست مسئله‌ی هسته‌ای را طبق برنامه‌ی خودش به پایان برساند، نتوانست؛ این ضعف آمریکا است. خیلی تلاش کرد هیاهو کرد [از طریق] رسانه، غیر رسانه؛ سیاست، تحریم، غیره [ولی] قادر نشد، نتوانست مسئله‌ی هسته‌ای را طبق برنامه‌ی خودش حل کند.
۵	۱۴۰۲/۰۱/۱۵	در دیدار مسئولان نظام	آخرین مسئله هم مسئله‌ی رسانه است که مهم است. من بارها درباره‌ی رسانه صحبت کرده‌ام، باز هم عرض میکنم. باید سیاه‌نمایی‌های دشمن، تخریبهای دشمن، توطئه‌ها علیه اقتدار کشور که به وسیله‌ی دشمن در فضای مجازی و مانند اینها صورت میگیرد، باید افشا بشود؛ این به عهده‌ی رسانه است. خب، رسانه‌ی ملّی بحمدالله دست افراد مؤمن و پُرانگیزه است؛ تلاش کنند که تلاش دشمن در این باره را خنثی کنند.
۶	۱۴۰۲/۰۱/۱۶	دیدار شاعران و اساتید ادبیات فارسی	حضرت آیت‌الله خامنه‌ای، بخش دیگری از هجوم متنوع بدخواهان به ایران را هجوم رسانه‌ای و استفاده آنها از هزاران رسانه برای ترویج دروغ، شایعه و انحراف دانستند و افزودند: هدف دشمن از این تهاجم، سلب نقاط قوت فکری و معارفی و تضعیف روحیه استقلال و استقامت ملی و وحدت و عمل اسلامی است.
۷	۱۴۰۲/۱/۲۹	در دیدار رمضانی دانشجویان	یک مثال دیگر برای بدبین کردن ما به خود [این است که] رسانه‌های جورواجورِ بدخواه، اصرارشان این است که ثابت کنند ملّت ایران از اعتقادات دینی روگردان شده، از احساسات انقلابی روگردان شده. اصرار دارند؛ این را بارهاوبارها آنها میگویند، یک دنباله‌هایی هم اینجا دارند که اینها هم میگویند؛ در فضای مجازی میگویند.

جدول ۶. گزارش مرکز ملی مدیریت امداد و هماهنگی رخدادهای رایانه‌ای

ردیف	تاریخ	سازمان مورد هدف
۱	۲۲ مهر ۱۳۹۹	سازمان بنادر و کشتیرانی
۲	۲۸ آبان ۱۳۹۹	شرکت ملی گاز ایران
۳	۲۲ فروردین ۱۴۰۰	تجهیزات هسته‌ای نطنز
۴	۱۸ تیر ۱۴۰۰	شرکت راه‌آهن
۵	۱۹ تیر ۱۴۰۰	پورتال وزارت راه
۶	۳۱ مرداد ۱۴۰۰	زندان اوین
۷	۴ آبان ۱۴۰۰	سامانه هوشمند توزیع سوخت
۸	۳۰ آبان ۱۴۰۰	شرکت هواپیمایی ماهان
۹	۷ بهمن ۱۴۰۰	صدا و سیما
۱۰	۱۲ بهمن ۱۴۰۰	سامانه تلویزیون
۱۱	۱۸ بهمن ۱۴۰۰	زندان قزلحصار
۱۲	۲۳ اسفند ۱۴۰۰	وزارت ارشاد
۱۳	۲۰ خرداد ۱۴۰۱	شهرداری تهران
۱۴	۶ تیر ۱۴۰۱	صنایع فولاد
۱۵	۱۲ تیر ۱۴۰۱	سازمان فرهنگ و ارتباطات اسلامی

با توجه به موارد ذکر شده زیرساخت رسانه از اهمیت قابل توجهی در حوزه امنیت سایبری برخوردار بوده و در این پژوهش به زیرساخت‌های تعیین شده توسط اسناد بالادست اضافه می‌گردد. لذا زیرساخت‌های حیاتی کشور از منظر امنیت سایبری مطابق شکل ۲ تعیین می‌گردد.



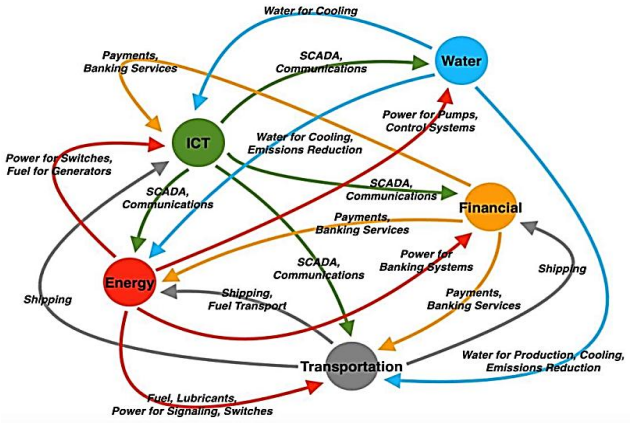
شکل ۲. زیرساخت‌های حیاتی جمهوری اسلامی ایران از منظر امنیت سایبری بر اساس نظر خبرگان در این پژوهش

۲- وابستگی زیرساخت‌های حیاتی (پیشینه پژوهش)

زیرساخت‌های حیاتی ستون فقرات جوامع مدرن هستند زیرا به طور منظم برای اطمینان از وجود و عملکرد فعالیت‌های روزانه مورد استفاده قرار می‌گیرند. با این حال، با توجه به تحولات مداوم در فناوری و جهانی شدن جوامع، شبکه‌های زیرساختی از نظر قابلیت عملیاتی به یکدیگر وابسته‌تر می‌شوند. از این رو، این شبکه‌ها در برابر عوامل استرس‌زای خارجی آسیب پذیرتر می‌شوند زیرا در معرض واکنش‌های زنجیره‌ای ناکارآمدی هستند[۲۷]. همچنین از آنجایی که عملیات تجاری به طور فزاینده‌ای بر فناوری اطلاعات تکیه می‌کنند، زیرساخت‌های مدرن به طور فزاینده‌ای به هم مرتبط شده اند. در نتیجه، خطر این که حتی اختلالات جزئی در یک زیرساخت می‌تواند منجر به یک آبشار فاجعه بار از خرابی در شبکه‌های زیرساخت‌ها شود در حال افزایش است .همچنین توجه دولت‌ها به زیرساخت‌ها و وابستگی‌های متقابل آنها در حال افزایش است. این امر بسیاری از محققان را تحریک می‌کند تا رویکردهای نوآورانه‌ای را برای شناسایی، توصیف و مدل سازی چنین وابستگی‌های متقابل بین زیرساخت‌ها توسعه دهند[۳]. آنها همچنین استدلال می‌کنند که یک زیرساخت را نمی‌توان به عنوان سیستم جدا شده از سایر زیرساخت‌ها در نظر گرفت. ابتدا تعاریف وابستگی و وابستگی متقابل بین زیرساخت‌ها به شرح زیر ارائه می‌شود.

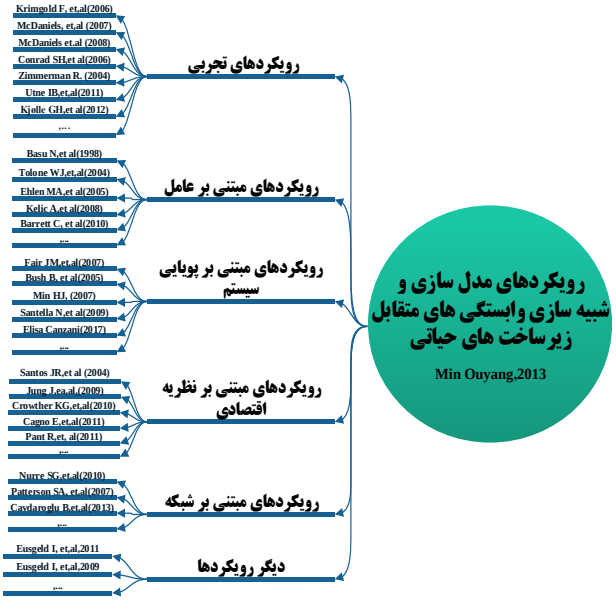
وابستگی یک پیوند یا ارتباط بین دو زیرساخت است که به وسیله آن وضعیت یک زیرساخت بر وضعیت زیرساخت تأثیر می‌گذارد یا به آن متکی است. وابستگی متقابل یک رابطه دوسویه بین دو زیرساخت است که در آن وضعیت هر زیرساخت بر وضعیت دیگری تأثیر می‌گذارد یا به آن وابسته است.

به طور کلی، محققان از وابستگی و وابستگی متقابل برای توصیف مفهوم پیوند مستقیم از یک زیرساخت به زیرساخت بر اساس معیارهای خاص استفاده می‌کنند. رینالدی ایده‌ای از توصیف کیفی وابستگی‌های متقابل مستقیم بر اساس محصولات و خدماتی را ارائه می‌دهد که زیرساخت‌های حیاتی به یکدیگر ارائه می‌کنند[۳].



شکل ۳. نمونه‌ای از توصیف کیفی وابستگی‌های متقابل.[3]

مطالعات دیگر که عمدتاً به مطالعات مفهومی اشاره دارد که پیچیدگی مدل‌سازی وابستگی‌های متقابل زیرساخت‌های حیاتی را نشان می‌دهد، تلاش‌های تحقیقاتی بعدی بر تعیین معیارها و چارچوب‌های ریاضی در میان زیرساخت‌های حیاتی برای تعیین کمیت تأثیرات آبشاری تمرکز می‌کنند[۲۸]. اویانگ بررسی جامع مدل سازی وابستگی متقابل زیرساخت‌های حیاتی را به عنوان یک موضوع نابالغ، اما به سرعت در حال رشد تعریف می‌کند. یک مشکل عمده فقدان داده‌های در دسترس عموم در مورد زیرساخت‌های حیاتی است که محققان را وادار می‌کند تا تحلیل‌های کیفی را برخلاف تحلیل‌های کمی انجام دهند به عنوان مثال اخیراً، درک زیرساخت‌های حیاتی به عنوان «سیستم سیستم‌ها»[۲۹] و «شبکه شبکه‌ها» [30] منجر به بررسی‌های کمی عمیق‌تر وابستگی‌ها در زیرساخت‌های حیاتی و وابستگی‌های متقابل بین آن‌ها می‌شود. با این حال، پیچیدگی مدل‌سازی وابستگی متقابل اغلب بسیاری از مطالعات را محدود می‌کند که تنها یک زیرساخت یا تعداد کمی از آنها را در نظر بگیرند[۳۱]. نان لی در سال ۲۰۲۲ با ارائه چارچوبی از یک رویکرد شبیه‌سازی مبتنی بر معماری سطح بالا برای مدل‌سازی امنیت زیرساخت‌های وابسته به هم با یکپارچه‌سازی دانش موجود، داده‌ها و مدل‌های خاص برای هر حوزه زیرساخت، و شبیه‌سازی انتشار شکست در سیستم‌ها استفاده کرد[۳۲]. همچنین مین اویانگ در سال ۲۰۱۳، رویکردهای مدل‌سازی و شبیه‌سازی در تحقیق و عمل وابستگی‌های متقابل زیرساخت را گروه‌بندی و بررسی می‌کند و آنها را در رویکردهای تجربی، رویکردهای مبتنی بر عامل، رویکردهای مبتنی بر پویایی سیستم، رویکردهای مبتنی بر نظریه اقتصادی، رویکردهای مبتنی بر شبکه، و موارد دیگر تقسیم‌بندی می‌نماید. خلاصه آن در شکل ۴ مشاهده می‌شود.



شکل ۴. انواع رویکردهای مدلسازی وابستگی زیرساخت‌های حیاتی[36]

رویکردهای تجربی وابستگی‌های متقابل زیرساخت‌های حیاتی را با توجه به داده‌های سوانح یا فاجعه تاریخی و تجربه کارشناسان تحلیل می‌کنند. مطالعات با این نوع رویکردها می‌توانند الگوهای شکست مکرر و قابل توجه را شناسایی کنند. در رویکردهای عامل محور به دلیل پیچیدگی ذاتی زیرساخت‌های حیاتی و فرآیندهای تصمیم‌گیری مرتبط، زیرساخت‌های حیاتی‌ها معمولاً به عنوان سیستم‌های تطبیقی پیچیده در نظر گرفته می‌شوند لذا برای تجزیه و تحلیل این سیستم‌ها، یک راه موثر، رویکردهای مبتنی بر عامل است، که روشی از پایین به بالا را اتخاذ می‌کند و فرض می‌کند رفتار یا پدیده پیچیده از بسیاری از تعاملات فردی و نسبتاً ساده عوامل مستقل ظاهر می‌شود. رویکردهای مبتنی بر پویایی سیستم از روشی از بالا به پایین برای مدیریت و تجزیه و تحلیل سیستم‌های انطباقی پیچیده که شامل وابستگی‌های متقابل است استفاده می‌کنند. حلقه‌های بازخورد اتصال و جهت اثرات بین اجزای زیرساخت‌های حیاتی را نشان می‌دهد. وابستگی‌های متقابل کشورهای مستقل مشترک المنافع را می‌توان از طریق مدل‌های وابستگی متقابل اقتصادی تحلیل کرد، دو نوع نظری اقتصادی برای مدل‌سازی وابستگی‌های متقابل زیرساخت‌های حیاتی استفاده می‌شود: ورودی-خروجی و تعادل عمومی قابل محاسبه. رویکردهای مبتنی بر شبکه زیرساخت‌های حیاتی جایی که گره‌ها اجزای مختلف زیرساخت‌های حیاتی را نشان می‌دهند و پیوندها از ارتباطات فیزیکی و رابطه‌ای بین آنها تقلید می‌کنند. بسته به مدل‌سازی جریان ذرات در زیرساخت‌های حیاتی، این بخش را بر توپولوژی و

روش‌های مبتنی بر جریان گروه‌بندی می‌کنند. علاوه بر رویکردهای مذکور، رویکردهای دیگری وجود دارد، مانند روش مدل‌سازی هولوگرافیک سلسله مراتبی، روش مبتنی بر معماری سطح بالا و غیره. او همچنین برای مقایسه رویکردهای مختلف، معیارهای مقایسه کمیت داده‌های ورودی، دسترسی به داده‌های ورودی، انواع وابستگی‌های متقابل، پیچیدگی محاسبات و بلوغ را مد نظر قرار داده و نتیجه در جدول ۹ ارائه شده است

جدول ۷. مقایسه رویکردهای مدلسازی وابستگی زیرساخت‌های حیاتی

مقایسه رویکردها از چند معیار						
نوع رویکرد	**رویکرد فرعی**	**کمیت داده های ورودی**	**قابلیت دسترسی به داده های ورودی**	**انواع وابستگی های متقابل**	**هزینه های محاسباتی**	**بلوغ**
تجربی		متوسط ، زیاد	متوسط	فیزیکی، سایبری، جغرافیایی و منطقی	کم	متوسط
مبتنی بر عامل		زیاد	کم	فیزیکی، سایبری، جغرافیایی و منطقی	زیاد	زیاد
مبتنی بر پویایی سیستم		زیاد	کم	فیزیکی، سایبری و منطقی	کم	زیاد
مبتنی بر نظریه اقتصادی	**ورودی خروجی**	متوسط	زیاد	فیزیکی، سایبری	کم	زیاد
	تعادل عمومی قابل محاسبه	زیاد	متوسط	فیزیکی، سایبری، جغرافیایی و منطقی	متوسط	متوسط
مبتنی بر شبکه	**روش مبتنی بر توپولوژی**	کم، متوسط	متوسط	فیزیکی، سایبری، جغرافیایی و منطقی	کم، متوسط	زیاد
	روش مبتنی بر جریان	زیاد	کم	فیزیکی، سایبری، جغرافیایی و منطقی	زیاد	زیاد

همانگونه که در جدول ۷ مشخص است چهار نوع وابستگی متقابل، در میان سیستم‌های زیرساختی، مشخص شد [۳]

(۱) فیزیکی: زمانی که وابستگی متقابل به دلیل تکیه بر جریان مواد بین دو یا چند سیستم باشد.

(۲) سایبر: زمانی که وابستگی متقابل به دلیل اتکا به انتقال اطلاعات بین دو یا چند سیستم باشد.

(۳) جغرافیایی: زمانی که وابستگی متقابل به دلیل نزدیکی دو یا چند سیستم باشد. و

(۴) منطقی: زمانی که وابستگی متقابل ناشی از عوامل دیگری باشد که در سه دسته فوق قرار نمی‌گیرند.

به طور متناوب، پنج نوع دیگر از وابستگی متقابل زیرساخت ارائه شد [۳۳].

(۱) وابستگی ورودی: زمانی که یک زیرساخت به ورودی از زیرساخت دیگری نیاز دارد.

(۲) وابستگی متقابل: زمانی که حداقل یک فعالیت در یک زیرساخت به فعالیت دیگری از زیرساخت دیگر وابسته است، در حالی که حداقل یک فعالیت در زیرساخت بعدی به فعالیت دیگری از زیرساخت قبلی وابسته است.

(۳) وابستگی مشترک: زمانی که اجزا یا فعالیت‌های فیزیکی بین زیرساخت‌ها به اشتراک گذاشته می‌شود.

(۴) انحصاری/یا وابستگی: زمانی که یک زیرساخت قادر به کار با یک زیرساخت دیگر نباشد. و (۵) وابستگی همزمان: زمانی که اجزای دو یا چند زیرساخت در یک مکان قرار دارند.

می‌توان بین چهار و پنج نوع وابستگی متقابل که در بالا مورد بحث قرار گرفت، روابط برقرار کرد. وابستگی‌های فیزیکی و سایبری که وابستگی سیستم اجزای مادی یا غیر مادی را عنوان می‌کند، می‌تواند ارتباط نزدیکی با وابستگی ورودی و متقابل داشته باشد، در حالی که وابستگی جغرافیایی و همزمان هر دو به نزدیکی مکان‌های اجزای سیستم مرتبط هستند. در نهایت، وابستگی مشترک و انحصاری انواع منطقی وابستگی سیستم هستند[۳۴].

۳- اهمیت و لزوم پژوهش

ادبیات، مطالعات گذشته و مدل‌های ارائه شده در غالب رویکردهای گوناگون اطلاعات و دانش خوبی جهت تحلیل، ایجاد و توسعه یک مدل بومی در اختیار می‌گذارند و از آنجایی که انواع زیرساخت‌های حیاتی مبتنی بر مقتضیات ملی، از کشوری به کشور دیگر متفاوت است، مثلاً ایالات متحده بیشترین تعداد زیرساخت حیاتی را دارد، از طرف دیگر میزان و نوع وابستگی هر زیرساخت به زیرساخت‌های دیگر نیز بر مبنای موقعیت هر کشور متفاوت است به عنوان مثال: در مقایسه نوع و میزان وابستگی در زیرساخت برق، بر اساس گزارش

وضعیت صنعت هسته‌ای جهان در سال ۲۰۲۲[1] (WNISR2022) کشور فرانسه تقریبا دوسوم برق خود را از منابع هسته‌ای تولید می‌کند که این مقدار بیشتر از هر کشور دیگری است، این در حالی است که با بررسی نمودار انرژی در ایران در سال ۲۰۲۲، انرژی هسته‌ای تنها حدود ۱ درصد از تولید برق کشور را به خود اختصاص داده است[2] و گاز طبیعی بیشترین منبع تولید برق در ایران است. این تفاوت باعث تغییر در نوع و میزان وابستگی زیرساخت برق به زیرساخت هسته‌ای یا زیرساخت گاز است. از منظری دیگر نتایج و خروجی‌های این پژوهش می‌تواند به مدیران ارشد حوزه‌های زیرساختی کشور در اتخاذ تصمیمات راهبردی کلان کمک کند، به عنوان مثال مهمترین دلایل خاموشی‌های گسترده در سال ۱۴۰۰ (زیرساخت برق) افت تولید برقابی‌ها در حوزه(زیرساخت آب) به دلیل خالی شدن مخازن سدها عنوان شد، از طرفی در دی ماه سال ۱۴۰۱ شاهد مشکلات حوزه گاز (زیرساخت گاز) درکشور بودیم که منجر به ایجاد نارضایتی و قطع گاز صنایع و مشترکین در برخی استان‌ها شد، لذا با بررسی و تحلیل دقیق جریان انرژی در کشور و تجربیات سال‌های گذشته و بررسی میزان تاثیرپذیری و تاثیرگذاری هر زیرساخت بر زیرساخت دیگر میتوان راهبردهای مناسبی را اتخاذ نمود به عنوان مثال سهم گاز را درتولید برق کاهش داد و سهم تولید برق را از انرژی‌های تجدید پذیر یا انرژی هسته‌ای (زیرساخت هسته-ای) افزایش داد یا نگاه ویژه‌ای به موضوع تولید برقابی با توجه به وضعیت آب در کشور در سال‌های اخیر نمود که به طبع آن اهمیت، نوع و میزان اثر گذاری و اثر پذیری هر زیرساخت تغییر می‌نماید. این موضوع زمانی اهمیت بیشتری دارد که به این مهم توجه نماییم که تعداد حملات سایبری‌ای که در سال‌های اخیر متوجه سرویس‌ها و زیرساخت‌های ایرانی شده به میزان قابل توجهی رسیده است. اما نکته‌ای که در این میان قابل توجه است این است که حملاتی که از دو سال قبل تا به امروز انجام شده فقط یک حمله سایبری معمولی نیستند بلکه می‌توان گفت ایران در حوزه امنیت سایبری از مهرماه سال ۹۹ وارد یک جنگ سایبری شده است. به عنوان نمونه در ۲۸ آبان ۱۳۹۹ حمله به شرکت ملی گاز ایران و ۲۲ فروردین ۱۴۰۰ حمله به تجهیزات هسته‌ای نطنز را میتوان نام برد[3].

همچنین بند ۴ طرح راهبردی حفاظت از زیرساخت‌های حیاتی کشور مصوب ۱۴۰۱/۶/۲۹در (شورای عالی) پدافند غیرعامل کشور، موضوع وابستگی زیرساخت‌های حیاتی به یکدیگر مورد توجه قرار گیرد.

۴- سوالات پژوهش

سوالات این پژوهش به شرح ذیل است:

۱- کدام زیرساخت‌ها از منظر امنیت سایبری تاثیرگذار و کدام یک تاثیرپذیرتر هستند؟

۲ – ارتباط زیرساخت‌های حیاتی در کشور جمهوری اسلامی ایران چگونه است؟

۳– اهمیت و اولویت زیرساخت‌های حیاتی با رویکرد سایبری کدام است؟

ساختار کلی پژوهش جهت پاسخ به سوالات آن در شکل ۵ نشان داده شده است.

شکل ۵. نمودار ساختار کلی پژوهش

به جهت شناسائی ارتباط و وابستگی زیرساخت‌های حیاتی در این پژوهش از رویکرد تجربی استفاده شد، به همین منظور به جهت جامعیت پژوهش از هر زیرساخت حیاتی مدیران و متخصصین مربوط به همان زیرساخت انتخاب و در گروه کانونی دسته‌بندی شدند . گروه کانونی به بحث اکتشافی گروهی اطلاق میشود که به منظور به دست آوردن ادراک در خصوص موضوع‌هایی خاص در فضایی تعریف شده صورت می گیرد. این روش به طور فزایندهای به عنوان یک ابزار پژوهش در علوم اجتماعی و در ابتدا در جامعه‌شناسی مورد استفاده قرار گرفت. گروه‌های کانونی ممکن

[1] World Nuclear Industry Status Report 2022 (WNISR2022)

۲ https://pep.moe.gov.ir

[3] https://cert.ir

است شامل دو نفر، سه نفر، چهار تا شش نفر (گروه بسیار کوچک)، هفت تا ده نفر (گروه کوچک) یا یازده تا بیست نفر (گروه بزرگ) شرکت‌کننده باشد در گروه کانونی، افراد شرکت‌کننده برداشت‌ها، احساسات و تجربه‌های خود را به اشتراک می‌گذارند؛ بنابراین محدوده دیدگاه‌ها درباره موضوعات خاص گسترش می‌یابد و از مشکلات ناشی از تمایلات یکطرفه جلوگیری می‌شود [۳۵].

در گروه کانونی از افراد متخصص و باسابقه مدیریت در هر حوزه بطور مجزا به شرح جدول ۸ استفاده شد. در این گروه‌ها خدمات هر زیرساخت از منظر سایبری به زیرساخت‌های دیگر مورد بحث و بررسی قرار گرفت، سپس نماینده هر گروه کانونی (۱۱ نفر) به منظور پاسخ‌دهی به سوالات و انجام مقایسه‌های زوجی بین زیرساخت‌ها بر اساس خدمات انتخاب گردیدند.

جدول ۸. توصیف خبرگان ۱۱ گروه کانونی پژوهش

	زیرساخت	شرکت کنندگان	تخصص	تحصیلات		تعداد جلسات
۱	ارتباطات و فناوری اطلاعات	۶	مهندسی برق مخابرات، مهندسی فناوری اطلاعات مهندسی کامپیوتر،مدیریت فناوری اطلاعات	دکتری کارشناسی ارشد	۴ نفر ۲ نفر	۳
۲	مالی	۴	اقتصاد، مهندسی سیستم‌های اقتصادی، مدیریت مالی	دکتری کارشناسی ارشد	۱ نفر ۳ نفر	۲
۳	رسانه	۳	رسانه، مدیریت صنعتی، تولید	کارشناسی ارشد	۳ نفر	۲
۴	سلامت	۳	چشم پزشکی فلوشیپ شبکیه، ارتوپدی فوق تخصص جراحی زانو، امنیت شبکه	دکتری کارشناسی ارشد	۲ نفر ۱ نفر	۳
۵	حمل و نقل	۵	شهرسازی گرایش مدیریت شهری،عمران،برنامه ریزی حمل و نقل	دکتری کارشناسی ارشد	۱ نفر ۴ نفر	۱
۶	برق	۳	مندسی برق قدرت،مدیریت دولتی	دکتری کارشناسی ارشد	۲ نفر ۱ نفر	۲
۷	گاز	۳	مهندسی صنایع، مهندسی ایمنی	دکتری کارشناسی ارشد	- ۳نفر	۱
۸	نفت	۶	مهندسی نفت استخراج و مخازن، مهندسی صنایع، مهندسی فناوری اطلاعات	دکتری ارشد	- ۶ نفر	۱
۹	پتروشیمی	۲	مهندسی شیمی،مهندسی صنایع	دکتری کارشناسی ارشد	۱ نفر ۱ نفر	۲
۱۰	آب	۳	مهندسی منابع آب مکانیک هیدرولیک مجاری روباز	دکتری کارشناسی ارشد	- ۳ نفر	۱
۱۱	اتمی(هسته‌ای)	۲	مکانیک، صنایع	دکتری کارشناسی ارشد	۱ نفر ۱ نفر	۱
مجموع شرکت کنندگان				**۴۰ نفر**		

۵- روش شناسی

در یک سیستم دارای وابستگی داخلی، تمام معیارهای سیستم‌ها دو به دو مشابه، مستقیم یا غیرمستقیم هستند. بنابراین، هر رابطه داخلی با یکی از معیارها روی سایر معیارها نیز تأثیر می‌گذارد. از این رو، پیدا کردن اولویت در عمل کار بسیار دشواری است. روش DEMATEL بر مبنای تئوری گراف، ما را قادر می‌سازد تا مسائل را بهتر برنامه ریزی و حل کنیم؛ به نحوی که ممکن است چندین معیار را در گروه علت معلول برای درک بهتر روابط علی، در جهت ترسیم نقشه روابط شبکه‌ای تقسیم کنیم. این روش شناسی ممکن است تائیدکننده روابط متقابل میان متغیر معیارها و محدودکننده روابطی باشد که در یک روند توسعه‌ای و سیستماتیک ضروری هستند محصول نهائی فرآیند DEMATEL ارائه تصویری است که پاسخگو بر اساس آن فعالیتهای خود را سازمان می‌دهد.

۵-۱- تکنیک دیمتل

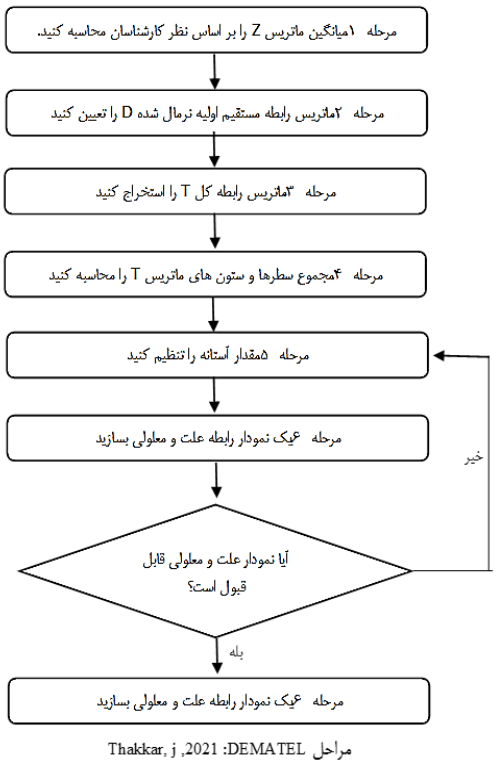
روش ارزیابی تصمیم‌گیری DEMATEL برای اولین بار توسط Fontela و Gabus در سال ۱۹۷۶ مورد استفاده قرار گرفت و توانسته است با در نظر گرفتن قضاوت متخصصان بسیاری از مشکلات پیچیده جهانی را در حوزه‌های علمی، سیاسی و اقتصادی حل کند. موسسه BMI از روش DEMATEL برای اجرای پروژه‌های بزرگ و پیچیده استفاده کرد. روش DEMATEL در ژاپن محبوب‌تر شده است، زیرا یک تکنیک گسترده است که قادر است تمام روابط علت و معلولی در هم تنیده را در هر مدل ساختاری ارزیابی و فرموله کند.

DEMATEL یک روش جامع برای ساخت و تجزیه و تحلیل یک مدل ساختاری است که شامل روابط علی بین عوامل پیچیده است. مراحل اساسی DEMATEL شامل ساخت سلسله مراتب ارزیابی،

انتخاب تیم خبره، محاسبه ماتریس کل رابطه، تعیین درجه تاثیر است و R + C و R - C برای ترسیم نقشه تاثیر رابطه کل محاسبه می‌شود.

مرحله ۱: در پانل گروه‌های کانونی و ابعاد / معیارها تعیین می‌شود. در این مرحله، گروهی از کارشناسان برای جمع آوری نظرات ذهنی انتخاب می‌شوند. بر اساس ادبیات و نظر کارشناسان، چالش‌ها تعیین و بحث می‌شود.

مرحله ۲: ماتریس رابطه مستقیم اولیه ساخته می‌شود. این ماتریس با انجام مقایسه‌های زوجی بین چالش‌ها/معیارها ایجاد می‌شود. برای ارزیابی رابطه بین معیارها از مقیاس زیر استفاده می‌شود.



مراحل DEMATEL :Thakkar, j ,2021

شکل ۶. مراحل گام به گام DEMATEL

$$\frac{1}{n(n-1)}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{\left|g_c^{ij\rho}-g_c^{ij(\rho-1)}\right|}{g_c^{ij\rho}}\times 100\% \qquad (۱)$$

صفر: بدون تاثیر. ۱: تاثیر بسیار کم. ۲: تاثیر کم ۳: تاثیر بالا ۴: تاثیر بسیار بالا.

$i=j$, the x_{ij}^{k} nXn x_{ij}^{k} نشان دهنده میزان تأثیر معیار i بر معیار j است که توسط متخصص k مشاهده می‌شود. اجازه دهید، M متخصص و n معیار وجود داشته باشد. ماتریس متوسط A با فرمول زیر محاسبه می‌شود:

$$a_{ij}=\frac{1}{M}\sum_{k=1}^{M}x_{ij}^{k}$$

قبل از آغاز مرحله بعدبه منظور بررسی اعتبار و پایایی ماتریس میانگین از فرمول ذیل استفاده می‌نماییم. که باید عددی کمتر از ۰/۰۵ باشد.

مرحله ۳: ماتریس مستقیم اولیه نرمال شده D ساخته می‌شود.

$$D=A\times S$$

$$T=(I-D)^{-1} \quad \text{where } S=\min\left(\frac{1}{\max\sum_{i=1}^{n}a_{ij}},\frac{1}{\max\sum_{i=1}^{n}a_{ij}}\right)$$

هر عنصر در ماتریس D بین صفر و ۱ قرار دارد.

$$R_i=\sum_{j=1}^{n}t_{ij}$$
$$C_j=\sum_{i=1}^{n}t_{ij} \qquad (۲)$$

R_i+C_j is called the "Prominence" and R_i-C_j is called the "Relation".

مرحله ۴: ماتریس رابطه کل T ایجاد می‌شود. I ماتریس هویت است.

مرحله ۵: امتیاز (برتری) و رابطه برای هر معیار محاسبه می‌شود.

مرحله ۶: نمودار علت و معلول با نگاشت مجموعه داده ایجاد می‌شود.

$$(R\,i+C\,j:\ R\,i-C\,j) \qquad (۳)$$

۶- تحلیل داده‌ها و یافته‌ها

پس از تشکیل جلسه‌های گروه کانونی خبرگان حوزه زیرساخت‌های حیاتی و با بحث و بررسی پیرامون مبانی نظری و تجربه‌های کاربردی و بر اساس روش DEMATEL با کمک ۱۱ نفر از اعضای کارگروه تاثیر میزان هر زیرساخت بر زیرساخت دیگر بر اساس ماتریس (۱۱*۱۱) جمع آوری شده و میانگین ماتریس Z به شرح جدول ۹ احصاء شد.

در این مرحله جهت بررسی اعتبار و پایایی ماتریس میانگین، ادغام نظرات ۱۰ نفر و ماتریس ادغام نظرات ۹ نفر را بر اساس فرمول ذیل

$$\frac{1}{n(n-1)}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{\left|g_c^{ij\rho}-g_c^{ij(\rho-1)}\right|}{g_c^{ij\rho}}\times 100\% \qquad (۴)$$

عمل شد عدد حاصل برابر با ۰/۰۴۹۴ شد که کمتر از ۰/۰۵ می‌باشد و پایایی ماتریس Z را تایید می‌نماید. در ادامه با محاسبه ماتریس نرمال و کسر ماتریس I (ماتریس واحد) از آن، ماتریس حاصله را معکوس نموده و ماتریس T را از ضرب ماتریس نرمال در ماتریس معکوس بدست می‌آوریم جدول (۱۲) تا (۱۵).

جدول ۹. میانگین ماتریس Z

ماتریس میانگین Z	فاوا	مالی	سلامت	حمل و نقل	برق	آب	نفت	گاز	پتروشیمی	هسته ای	رسانه
فاوا	۰	۳/۸	۳/۱	۳/۴	۳/۱	۲/۷	۲/۶	۲/۸	۳/۵	۱/۶	۳/۸
مالی	۲/۳	۰	۱/۸	۲/۲	۱/۸	۰/۹	۰/۹	۱/۱	۱/۷	۰/۱	۲/۸
سلامت	۰/۴	۱/۱	۰	۲	۰/۴	۰/۶	۰/۳	۰/۳	۰/۳	۰	۰/۹
حمل و نقل	۱/۷	۲/۷	۲	۰	۱/۳	۰/۴	۲/۱	۲/۱	۳	۰/۱	۲
برق	۲/۶	۳/۱	۳	۳/۲	۰	۱/۶	۱/۴	۱/۲	۲/۹	۱/۴	۳/۱
آب	۰/۱	۰/۴	۲/۷	۰/۵	۱/۶	۰	۰/۳	۱/۴	۱/۷	۱/۱	۰/۳
نفت	۰/۳	۱/۴	۰/۳	۲/۹	۲/۱	۰/۲	۰	۱/۵	۳/۷	۰	۰/۸
گاز	۰/۳	۱/۱	۱	۳/۱	۴	۰/۹	۱/۲	۰	۲/۳	۰	۰/۵
پتروشیمی	۱/۹	۲/۷	۱/۴	۲/۶	۱/۴	۰/۳	۱/۶	۰/۹	۰	۰/۷	۰/۸
هسته های	۰	۰/۱	۱/۱	۰	۱/۱	۰	۰	۰/۲	۰	۰	۰
رسانه	۲/۶	۳	۲/۴	۲/۴	۲/۱	۱/۸	۱/۶	۱/۹	۱/۹	۱/۶	۰

جدول ۱۰. ماتریس نرمال

ماتریس‌نرمال	فاوا	مالی	سلامت	حمل‌ونقل	برق	آب	نفت	گاز	پتروشیمی	هسته‌ای	رسانه
فاوا	۰/۰۰۰۰	۰/۱۲۵۰	۰/۱۰۲۰	۰/۱۱۱۸	۰/۱۰۲۰	۰/۰۸۸۸	۰/۰۸۵۵	۰/۰۹۲۱	۰/۱۱۵۱	۰/۰۵۲۶	۰/۱۲۵۰
مالی	۰/۰۷۵۷	۰/۰۰۰۰	۰/۰۵۹۲	۰/۰۷۲۴	۰/۰۵۹۲	۰/۰۲۹۶	۰/۰۲۹۶	۰/۰۳۶۲	۰/۰۵۵۹	۰/۰۰۳۳	۰/۰۹۲۱
سلامت	۰/۰۱۳۲	۰/۰۳۶۲	۰/۰۰۰۰	۰/۰۶۵۸	۰/۰۱۳۲	۰/۰۱۹۷	۰/۰۰۹۹	۰/۰۰۹۹	۰/۰۰۹۹	۰/۰۰۰۰	۰/۰۲۹۶
حمل‌ونقل	۰/۰۵۵۹	۰/۰۸۸۸	۰/۰۶۵۸	۰/۰۰۰۰	۰/۰۴۲۸	۰/۰۱۳۲	۰/۰۶۹۱	۰/۰۶۹۱	۰/۰۹۸۷	۰/۰۰۳۳	۰/۰۶۵۸
برق	۰/۰۸۵۵	۰/۱۰۲۰	۰/۰۹۸۷	۰/۱۰۵۳	۰/۰۰۰۰	۰/۰۵۲۶	۰/۰۴۶۱	۰/۰۳۹۵	۰/۰۹۵۴	۰/۰۴۶۱	۰/۱۰۲۰
آب	۰/۰۰۳۳	۰/۰۱۳۲	۰/۰۸۸۸	۰/۰۱۶۴	۰/۰۵۲۶	۰/۰۰۰۰	۰/۰۰۹۹	۰/۰۴۶۱	۰/۰۵۵۹	۰/۰۳۶۲	۰/۰۰۹۹
نفت	۰/۰۰۹۹	۰/۰۴۶۱	۰/۰۰۹۹	۰/۰۹۵۴	۰/۰۶۹۱	۰/۰۰۶۶	۰/۰۰۰۰	۰/۰۴۹۳	۰/۱۲۱۷	۰/۰۰۰۰	۰/۰۲۶۳
گاز	۰/۰۰۹۹	۰/۰۳۶۲	۰/۰۳۲۹	۰/۱۰۲۰	۰/۱۳۱۶	۰/۰۲۹۶	۰/۰۳۹۵	۰/۰۰۰۰	۰/۰۷۵۷	۰/۰۰۰۰	۰/۰۱۶۴
پتروشیمی	۰/۰۶۲۵	۰/۰۸۸۸	۰/۰۴۶۱	۰/۰۸۵۵	۰/۰۴۶۱	۰/۰۰۹۹	۰/۰۵۲۶	۰/۰۲۹۶	۰/۰۰۰۰	۰/۰۲۳۰	۰/۰۲۶۳
هسته های	۰/۰۰۰۰	۰/۰۰۳۳	۰/۰۳۶۲	۰/۰۰۰۰	۰/۰۳۶۲	۰/۰۰۰۰	۰/۰۰۰۰	۰/۰۰۶۶	۰/۰۰۰۰	۰/۰۰۰۰	۰/۰۰۰۰
رسانه	۰/۰۸۵۵	۰/۰۹۸۷	۰/۰۷۸۹	۰/۰۷۸۹	۰/۰۶۹۱	۰/۰۵۹۲	۰/۰۵۲۶	۰/۰۶۲۵	۰/۰۶۲۵	۰/۰۵۲۶	۰/۰۰۰۰

جدول ۱۱. ماتریس I-N

ماتریس I-N	فاوا	مالی	سلامت	حمل‌ونقل	برق	آب	نفت	گاز	پتروشیمی	هسته‌ای	رسانه
فاوا	۱/۰۰۰۰	-۰/۱۲۵۰	-۰/۱۰۲۰	-۰/۱۱۱۸	-۰/۱۰۲۰	-۰/۰۸۸۸	-۰/۰۸۵۵	-۰/۰۹۲۱	-۰/۱۱۵۱	-۰/۰۵۲۶	-۰/۱۲۵۰
مالی	-۰/۰۷۵۷	۱/۰۰۰۰	-۰/۰۵۹۲	-۰/۰۷۲۴	-۰/۰۵۹۲	-۰/۰۲۹۶	-۰/۰۲۹۶	-۰/۰۳۶۲	-۰/۰۵۵۹	-۰/۰۰۳۳	-۰/۰۹۲۱
سلامت	-۰/۰۱۳۲	-۰/۰۳۶۲	۱/۰۰۰۰	-۰/۰۶۵۸	-۰/۰۱۳۲	-۰/۰۱۹۷	-۰/۰۰۹۹	-۰/۰۰۹۹	-۰/۰۰۹۹	۰/۰۰۰۰	-۰/۰۲۹۶
حمل‌ونقل	-۰/۰۵۵۹	-۰/۰۸۸۸	-۰/۰۶۵۸	۱/۰۰۰۰	-۰/۰۴۲۸	-۰/۰۱۳۲	-۰/۰۶۹۱	-۰/۰۶۹۱	-۰/۰۹۸۷	-۰/۰۰۳۳	-۰/۰۶۵۸
برق	-۰/۰۸۵۵	-۰/۱۰۲۰	-۰/۰۹۸۷	-۰/۱۰۵۳	۱/۰۰۰۰	-۰/۰۵۲۶	-۰/۰۴۶۱	-۰/۰۳۹۵	-۰/۰۹۵۴	-۰/۰۴۶۱	-۰/۱۰۲۰
آب	-۰/۰۰۳۳	-۰/۰۱۳۲	-۰/۰۸۸۸	-۰/۰۱۶۴	-۰/۰۵۲۶	۱/۰۰۰۰	-۰/۰۰۹۹	-۰/۰۴۶۱	-۰/۰۵۵۹	-۰/۰۳۶۲	-۰/۰۰۹۹
نفت	-۰/۰۰۹۹	-۰/۰۴۶۱	-۰/۰۰۹۹	-۰/۰۹۵۴	-۰/۰۶۹۱	-۰/۰۰۶۶	۱/۰۰۰۰	-۰/۰۴۹۳	-۰/۱۲۱۷	۰/۰۰۰۰	-۰/۰۲۶۳
گاز	-۰/۰۰۹۹	-۰/۰۳۶۲	-۰/۰۳۲۹	-۰/۱۰۲۰	-۰/۱۳۱۶	-۰/۰۲۹۶	-۰/۰۳۹۵	۱/۰۰۰۰	-۰/۰۷۵۷	۰/۰۰۰۰	-۰/۰۱۶۴
پتروشیمی	-۰/۰۶۲۵	-۰/۰۸۸۸	-۰/۰۴۶۱	-۰/۰۸۵۵	-۰/۰۴۶۱	-۰/۰۰۹۹	-۰/۰۵۲۶	-۰/۰۲۹۶	۱/۰۰۰۰	-۰/۰۲۳۰	-۰/۰۲۶۳
هسته های	۰/۰۰۰۰	-۰/۰۰۳۳	-۰/۰۳۶۲	۰/۰۰۰۰	-۰/۰۳۶۲	۰/۰۰۰۰	۰/۰۰۰۰	-۰/۰۰۶۶	۰/۰۰۰۰	۱/۰۰۰۰	۰/۰۰۰۰
رسانه	-۰/۰۸۵۵	-۰/۰۹۸۷	-۰/۰۷۸۹	-۰/۰۷۸۹	-۰/۰۶۹۱	-۰/۰۵۹۲	-۰/۰۵۲۶	-۰/۰۶۲۵	-۰/۰۶۲۵	-۰/۰۵۲۶	۱/۰۰۰۰

جدول ۱۲. معکوس ماتریس I-N

معکوس I-N ماتریس	فاوا	مالی	سلامت	حمل‌ونقل	برق	آب	نفت	گاز	پتروشیمی	هسته‌ای	رسانه
فاوا	۱/۰۹۰۹	۰/۲۴۶۶	۰/۲۱۴۷	۰/۲۴۹۴	۰/۲۱۰۳	۰/۱۴۴۳	۰/۱۶۲۰	۰/۱۷۳۰	۰/۲۴۰۷	۰/۰۹۱۰	۰/۲۱۸۲
مالی	۰/۱۲۵۶	۱/۰۸۰۹	۰/۱۲۷۸	۰/۱۵۴۴	۰/۱۲۳۲	۰/۰۶۷۵	۰/۰۷۹۳	۰/۰۸۸۰	۰/۱۳۲۶	۰/۰۲۹۷	۰/۱۴۹۵
سلامت	۰/۰۳۵۲	۰/۰۶۶۱	۱/۰۲۸۵	۰/۰۹۵۰	۰/۰۳۹۱	۰/۰۳۳۴	۰/۰۳۰۱	۰/۰۳۱۶	۰/۰۴۲۳	۰/۰۰۹۲	۰/۰۵۳۹
حمل‌ونقل	۰/۱۰۹۶	۰/۱۶۵۹	۰/۱۳۳۰	۱/۰۹۴۳	۰/۱۱۳۹	۰/۰۵۱۲	۰/۱۱۷۶	۰/۱۱۹۰	۰/۱۷۶۲	۰/۰۲۷۷	۰/۱۲۶۷
برق	۰/۱۵۲۹	۰/۲۰۱۶	۰/۱۸۸۶	۰/۲۱۲۹	۱/۰۹۰۴	۰/۰۹۹۹	۰/۱۱۰۸	۰/۱۰۸۵	۰/۱۹۴۲	۰/۰۷۷۱	۰/۱۷۹۳
آب	۰/۰۲۹۳	۰/۰۵۱۲	۰/۱۲۰۰	۰/۰۶۱۱	۰/۰۸۳۳	۱/۰۱۷۱	۰/۰۳۲۷	۰/۰۶۷۱	۰/۰۸۹۷	۰/۰۴۶۷	۰/۰۳۸۸
نفت	۰/۰۵۷۹	۰/۱۱۱۸	۰/۰۶۶۴	۰/۱۶۲۳	۰/۱۲۰۳	۰/۰۳۴۰	۱/۰۴۳۱	۰/۰۸۹۳	۰/۱۸۱۴	۰/۰۱۸۹	۰/۰۷۶۵
گاز	۰/۰۶۱۳	۰/۱۰۷۷	۰/۰۹۵۷	۰/۱۷۳۸	۰/۱۸۰۴	۰/۰۵۹۶	۰/۰۸۳۱	۱/۰۴۵۵	۰/۱۴۵۶	۰/۰۲۱۹	۰/۰۷۴۰
پتروشیمی	۰/۱۰۶۵	۰/۱۵۲۷	۰/۱۰۵۰	۰/۱۵۶۴	۰/۱۰۳۲	۰/۰۴۱۹	۰/۰۹۴۴	۰/۰۷۵۱	۱/۰۷۱۹	۰/۰۴۲۰	۰/۰۸۳۶
هسته های	۰/۰۰۷۶	۰/۰۱۴۰	۰/۰۴۵۱	۰/۰۱۲۸	۰/۰۴۲۵	۰/۰۰۵۴	۰/۰۰۵۹	۰/۰۱۲۲	۰/۰۱۰۰	۱/۰۰۳۴	۰/۰۰۹۴
رسانه	۰/۱۴۳۳	۰/۱۸۵۹	۰/۱۶۱۲	۰/۱۷۸۶	۰/۱۴۸۸	۰/۱۰۱۲	۰/۱۰۹۲	۰/۱۲۲۲	۰/۱۵۵۸	۰/۰۷۹۵	۱/۰۷۶۷

جدول ۱۳. ماتریس T

ارتباطات کل T	فاوا	مالی	سلامت	حمل و نقل	برق	آب	نفت	گاز	پتروشیمی	هسته ای	رسانه
فاوا	۰/۰۹۰۹	۰/۲۴۶۶	۰/۲۱۴۷	۰/۲۴۹۴	۰/۲۱۰۳	۰/۱۴۴۳	۰/۱۶۲۰	۰/۱۷۳۰	۰/۲۴۰۷	۰/۰۹۱۰	۰/۲۱۸۲
مالی	۰/۱۲۵۶	۰/۰۸۰۹	۰/۱۲۷۸	۰/۱۵۴۴	۰/۱۲۳۲	۰/۰۶۷۵	۰/۰۷۹۳	۰/۰۸۸۰	۰/۱۳۲۶	۰/۰۲۹۷	۰/۱۴۹۵
سلامت	۰/۰۳۵۲	۰/۰۶۶۱	۰/۰۲۸۵	۰/۰۹۵۰	۰/۰۳۹۱	۰/۰۳۳۴	۰/۰۳۰۱	۰/۰۳۱۶	۰/۰۴۲۳	۰/۰۰۹۲	۰/۰۵۳۹
حمل و نقل	۰/۱۰۹۶	۰/۱۶۵۹	۰/۱۳۳۰	۰/۰۹۴۳	۰/۱۱۳۹	۰/۰۵۱۲	۰/۱۱۷۶	۰/۱۱۹۰	۰/۱۷۶۲	۰/۰۲۷۷	۰/۱۲۶۷
برق	۰/۱۵۲۹	۰/۲۰۱۶	۰/۱۸۸۶	۰/۲۱۲۹	۰/۰۹۰۴	۰/۰۹۹۹	۰/۱۱۰۸	۰/۱۰۸۵	۰/۱۹۴۲	۰/۰۷۷۱	۰/۱۷۹۳
آب	۰/۰۲۹۳	۰/۰۵۱۲	۰/۱۲۰۰	۰/۰۶۱۱	۰/۰۸۳۳	۰/۰۱۷۱	۰/۰۳۲۷	۰/۰۶۷۱	۰/۰۸۹۷	۰/۰۴۶۷	۰/۰۳۸۸
نفت	۰/۰۵۷۹	۰/۱۱۱۸	۰/۰۶۶۴	۰/۱۶۲۳	۰/۱۲۰۳	۰/۰۳۴۰	۰/۰۴۳۱	۰/۰۸۹۳	۰/۱۸۱۴	۰/۰۱۸۹	۰/۰۷۶۵
گاز	۰/۰۶۱۳	۰/۱۰۷۷	۰/۰۹۵۷	۰/۱۷۳۸	۰/۱۸۰۴	۰/۰۵۹۶	۰/۰۸۳۱	۰/۰۴۵۵	۰/۱۴۵۶	۰/۰۲۱۹	۰/۰۷۴۰
پتروشیمی	۰/۱۰۶۵	۰/۱۵۲۷	۰/۱۰۵۰	۰/۱۵۶۴	۰/۱۰۳۲	۰/۰۴۱۹	۰/۰۹۴۴	۰/۰۷۵۱	۰/۰۷۱۹	۰/۰۴۲۰	۰/۰۸۳۶
هسته های	۰/۰۰۷۶	۰/۰۱۴۰	۰/۰۴۵۱	۰/۰۱۲۸	۰/۰۴۲۵	۰/۰۰۵۴	۰/۰۰۵۹	۰/۰۱۲۲	۰/۰۱۰۰	۰/۰۰۳۴	۰/۰۰۹۴
رسانه	۰/۱۴۳۳	۰/۱۸۵۹	۰/۱۶۱۲	۰/۱۷۸۶	۰/۱۴۸۸	۰/۱۰۱۲	۰/۱۰۹۲	۰/۱۲۲۲	۰/۱۵۵۸	۰/۰۷۹۵	۰/۰۷۶۷

جهت مشخص شدن تاثیرگذارترین زیرساخت، تاثیرپذیرترین زیرساخت، زیرساختی که بیشترین ارتباط با دیگر زیرساخت‌های حیاتی را دارد و همچنین روابط علت و معلولی احتمالی بین آن‌ها با کمک از ماتریس T موارد مذکور را در جدول ۱۴ استخراج می‌نماییم.

جدول ۱۴. تحلیل ماتریس ارتباطات کل

زیرساخت	D	R	D+R	D-R
فاوا	۲/۰۴۱	۰/۹۲۰	۲/۹۶۱	۱/۱۲۱
مالی	۱/۱۵۸	۱/۳۸۴	۲/۵۴۳	-۰/۲۲۶
سلامت	۰/۴۶۴	۱/۲۸۶	۱/۷۵۰	-۰/۸۲۱
حمل و نقل	۱/۲۳۵	۱/۵۵۱	۲/۷۸۶	-۰/۳۱۶
برق	۱/۶۱۶	۱/۲۵۵	۲/۸۷۲	۰/۳۶۱
آب	۰/۶۳۷	۰/۶۵۶	۱/۲۹۲	-۰/۰۱۹
نفت	۰/۹۶۲	۰/۸۹۹	۱/۸۳۰	۰/۰۹۴
گاز	۱/۰۴۹	۰/۹۳۱	۱/۹۸۰	۰/۱۱۷
پتروشیمی	۱/۰۳۳	۱/۴۴۰	۲/۴۷۳	-۰/۴۰۸
هسته‌ای(اتمی)	۰/۱۶۸	۰/۴۴۷	۰/۶۱۵	-۰/۲۷۹
رسانه	۱/۴۶۳	۱/۰۸۷	۲/۵۴۹	۰/۳۷۶

D: مجموع سطرها (بزرگترین عدد بدست آمده نشان‌دهنده تاثیرگذارترین زیرساخت حیاتی).

R: مجموع ستون‌ها (بزرگترین عدد نشان دهنده تاثیرپذیرترین زیرساخت حیاتی).

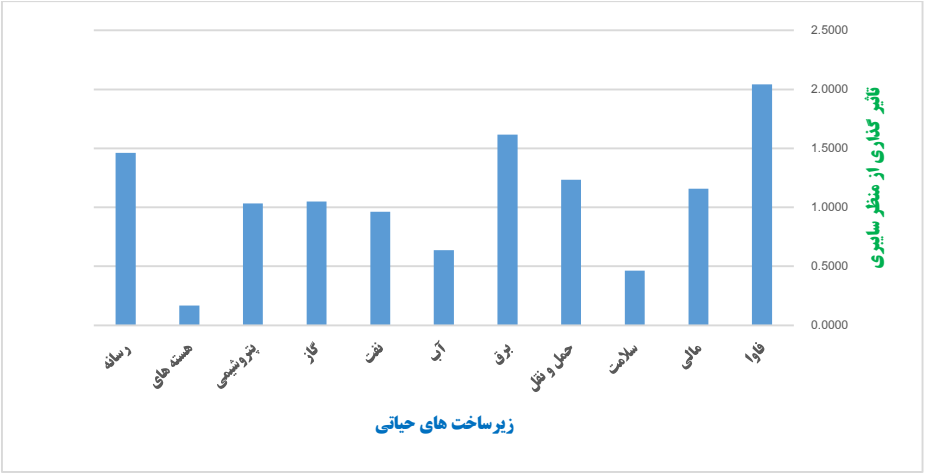
D+R: بزرگترین عدد نشان دهنده زیرساخت حیاتی که بیشترین ارتباط را با دیگر زیرساخت‌های حیاتی دارد.

D-R: اعداد مثبت به عنوان معیارهای (زیرساخت‌های) علت و اعداد مفنی به عنوان معیارهای (زیرساخت‌های) معلول.

بر اساس نتایج حاصله

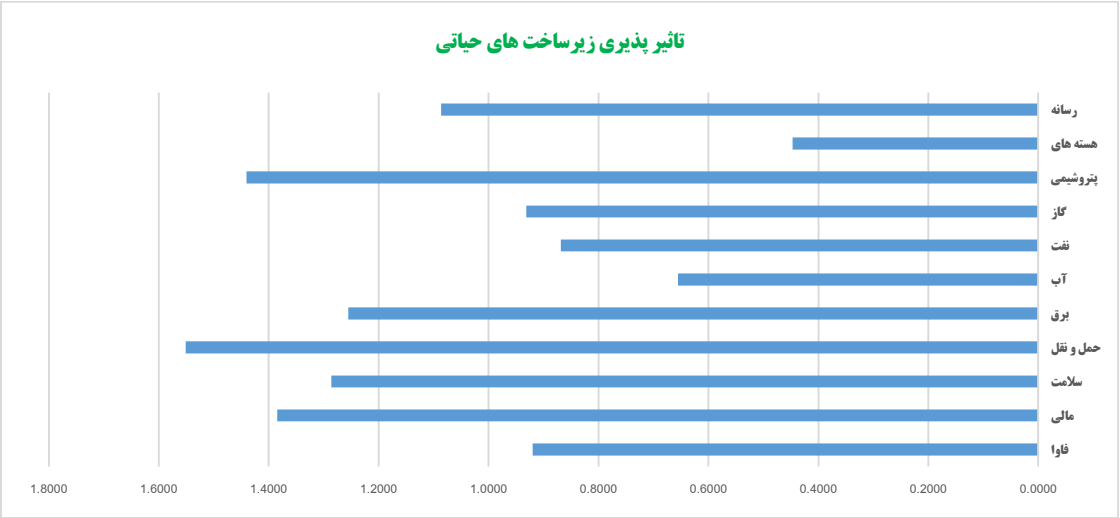
تاثیرگذارترین زیرساخت حیاتی: زیرساخت فناوری اطلاعات و ارتباطات (فاوا) است بعد از آن زیرساخت برق در رتبه دوم زیرساخت رسانه در رتبه سوم زیرساخت حمل و نقل در رتبه چهارم زیرساخت مالی در رتبه پنجم زیرساخت گاز و پتروشیمی به ترتیب رتبه ششم و هفتم و زیرساخت نفت در رتبه هشتم زیرساخت آب در رتبه نهم و زیرساخت سلامت و هسته‌ای در رتبه‌های دهم و یازدهم قرار گرفتند.

این رتبه‌بندی در نمودار شکل ۷ به نمایش در آمده است.



شکل ۷. نمودار رتبه‌بندی زیرساخت‌های حیاتی از نظر تاثیرگذاری

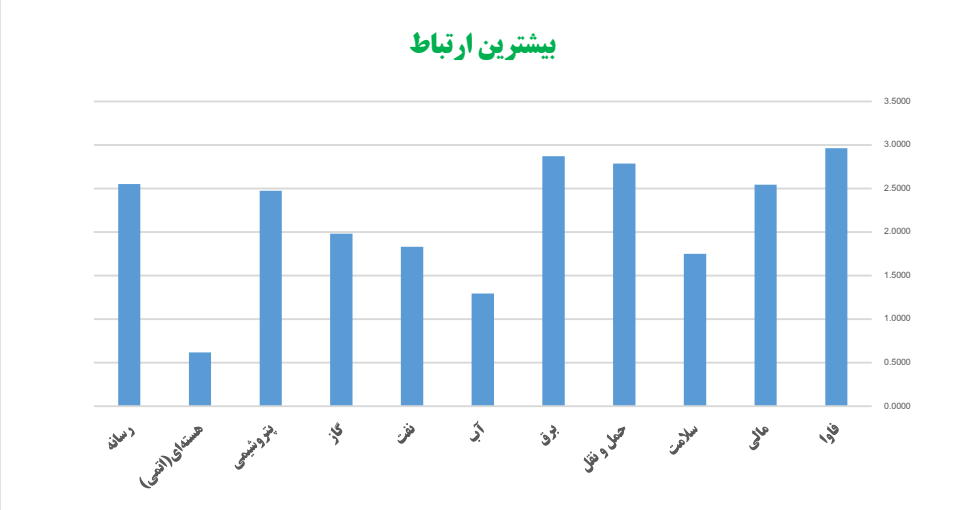
تاثیرپذیرترین زیرساخت حیاتی: زیرساخت حمل و نقل است و بعد از آن زیرساخت پتروشیمی در رتبه دوم و زیرساخت مالی و سلامت به ترتیب در رتبه‌های سوم و چهارم و زیرساخت‌های برق و رسانه و گاز نیز به ترتیب در رتبه‌های پنجم تا هفتم زیرساخت فاوا در رتبه هشتم و زیرساخت نفت و آب و هسته‌ای نیز در رتبه‌های نهم تا یازدهم قرار گرفتند این رتبه‌بندی نیز در نمودار شکل ۸ به نمایش در آمده است.



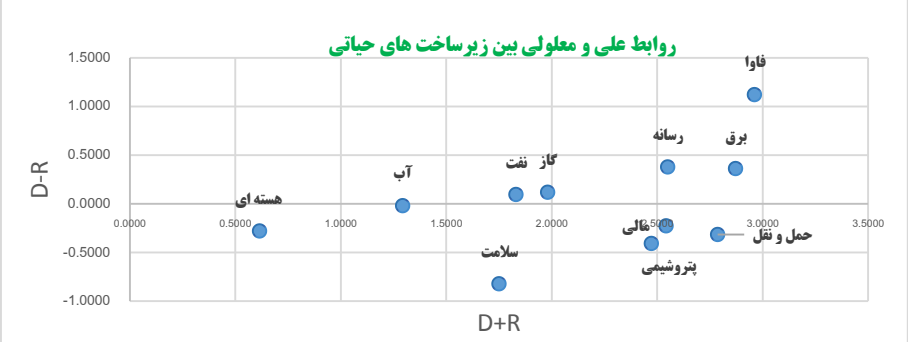
شکل ۸. رتبه‌بندی زیرساخت‌های حیاتی از نظر تاثیرپذیری

نتیجه دیگری که از جدول ۱۴ قابل استنباط است شناخت زیرساخت‌های حیاتی است که دارای بیشترین ارتباط با دیگر زیرساخت‌ها هستند در این تحلیل نیز زیرساخت فاوا از منظر سایبری بیشترین ارتباط را با دیگر زیرساخت‌های حیاتی دارا بود همچنین زیرساخت برق و حمل و نقل بعد از زیرساخت فاوا بیشترین ارتباط را دارا بودند این رتبه‌بندی از ستون سوم جدول ۱۴ احصا شده است و در نمودار شکل ۹ این رتبه‌بندی به نمایش درآمده است

همچنین همانگونه که در نمودار اسکتر ذیل مشخص است زیرساخت فاوا، برق رسانه گاز، نفت و آب علت و زیرساخت‌های حمل و نقل، مالی، پتروشیمی، هسته‌ای و سلامت معلول هستند



شکل ۹. نمودار رتبه‌بندی زیرساخت‌های حیاتی از نظر دارا بودن بیشترین ارتباط با دیگر زیرساخت‌ها



شکل ۱۰. نمودار اسکتر

در ادامه تحلیل داده‌ها، جهت مشخص نمودن روابط بین زیرساخت‌های حیاتی ابتدا با محاسبه میانگین داده‌های ماتریس T عدد آستانه را بدست آورده و ماتریس ارتباط را ایجاد می‌نماییم بدین صورت که در ماتریس ارتباط هر عددی در ماتریس T را که از عدد آستانه کمتر بود ۰ (صفر) منظور نموده به معنی عدم ارتباط است و هر عددی که بیش از عدد آستانه بود نشان دهنده وجود ارتباط بین معیارها (زیرساخت‌های حیاتی) است و خود عدد را به شرح ماتریس جدول ۱۵ منظور می‌نماییم.

جدول ۱۵. ماتریس ارتباط

ماتریس ارتباط	فاوا	مالی	سلامت	حمل و نقل	برق	آب	نفت	گاز	پتروشیمی	هسته ای	رسانه
فاوا	۰	۰/۲۴۶۶	۰/۲۱۴۷	۰/۲۴۹۴	۰/۲۱۰۳	۰/۱۴۴۳	۰/۱۶۲۰	۰/۱۷۳۰	۰/۲۴۰۷	۰	۰/۲۱۸۲
مالی	۰/۱۲۵۶	۰	۰/۱۲۷۸	۰/۱۵۴۴	۰/۱۲۳۲	۰	۰	۰	۰/۱۳۲۶	۰	۰/۱۴۹۵
سلامت	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
حمل و نقل	۰/۱۰۹۶	۰/۱۶۵۹	۰/۱۳۳۰	۰	۰/۱۱۳۹	۰	۰/۱۱۷۶	۰/۱۱۹۰	۰/۱۷۶۲	۰	۰/۱۲۶۷
برق	۰/۱۵۲۹	۰/۲۰۱۶	۰/۱۸۸۶	۰/۲۱۲۹	۰	۰/۰۹۹۹	۰/۱۱۰۸	۰/۱۰۸۵	۰/۱۹۴۲	۰	۰/۱۷۹۳
آب	۰	۰	۰/۱۲۰۰	۰	۰	۰	۰	۰	۰	۰	۰
نفت	۰	۰/۱۱۱۸	۰	۰/۱۶۲۳	۰/۱۲۰۳	۰	۰	۰	۰/۱۸۱۴	۰	۰
گاز	۰	۰/۱۰۷۷	۰	۰/۱۷۳۸	۰/۱۸۰۴	۰	۰	۰	۰/۱۴۵۶	۰	۰
پتروشیمی	۰/۱۰۶۵	۰/۱۵۲۷	۰/۱۰۵۰	۰/۱۵۶۴	۰/۱۰۳۲	۰	۰	۰	۰	۰	۰
هسته های	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
رسانه	۰/۱۴۳۳	۰/۱۸۵۹	۰/۱۶۱۲	۰/۱۷۸۶	۰/۱۴۸۸	۰/۱۰۱۲	۰/۱۰۹۲	۰/۱۲۲۲	۰/۱۵۵۸	۰	۰

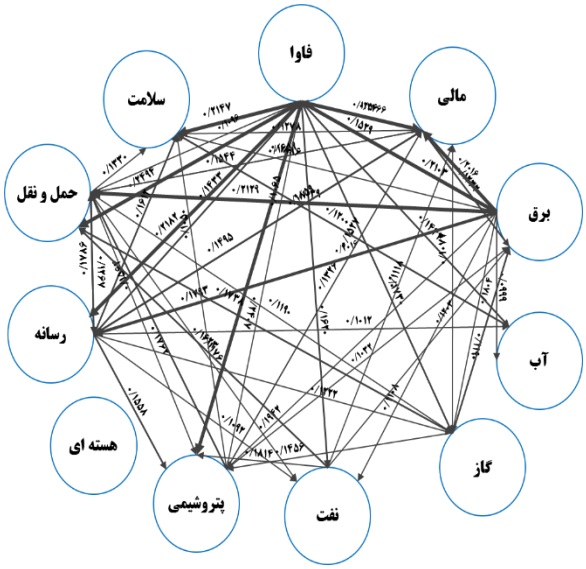
ارتباط بین زیرساخت‌های حیاتی و تحلیل نتایج ماتریس ارتباط برای هر یک از زیرساخت‌های حیاتی و مجموع ارتباط آن‌ها در شکل ۱۱ ارائه شده است. به منظور نمایش بهتر و تحلیل این ارتباطات و وابستگی بین زیرساخت‌ها ارتباط هر زیرساخت به طور مجزا در اشکال ۱۲ الی ۲۰ ارائه شده است.

همانگونه که در شکل ۱۲ ارتباطات زیرساخت فاوا نمایش داده شده است وابستگی زیرساخت‌های سلامت، حمل و نقل، پتروشیمی، رسانه، برق، مالی به زیرساخت فاوا بیشتر است و زیرساخت نفت، گاز و آب وابستگی کمتری دارند به همین ترتیب در شکل ۱۳ ارتباطات زیرساخت رسانه و وابستگی دیگر زیرساخت‌ها به آن به نمایش در آمده است. در شکل ۱۴ ارتباطات زیرساخت برق نمایش داده شده است وابستگی زیرساخت‌های دیگر به آن به روشنی نمایش داده شده است ضمنا این زیرساخت با زیرساخت هسته‌ای ارتباطی ندارد . درشکل ۱۵ نیز ارتباطات زیرساخت حمل و نقل و وابستگی دیگر زیرساخت‌ها به آن به نمایش در آمده است، این زیرساخت ارتباطی با زیرساخت آب و هسته‌ای ندارد و به مفهوم دیگر زیرساخت آب و هسته‌ای به آن وابسته نیستند.

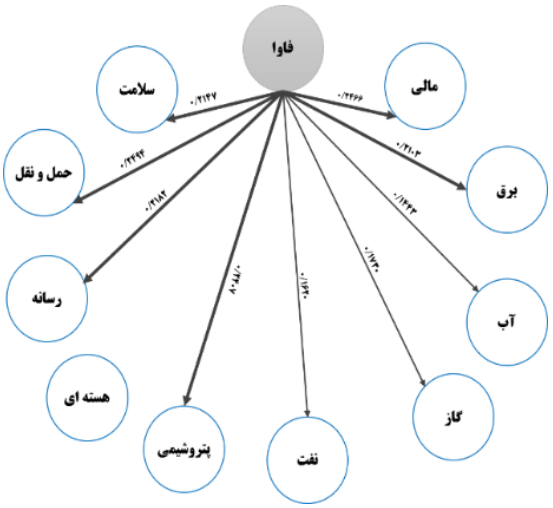
در شکل ۱۶ ارتباطات زیرساخت مالی نمایش داده شده است وابستگی زیرساخت‌های دیگر به آن به روشنی نمایش داده شده است ضمنا این زیرساخت با زیرساخت‌های آب، گاز، نفت و هسته‌ای ارتباطی ندارد. در شکل ۱۷ نیز ارتباطات زیرساخت پتروشیمی و وابستگی دیگر زیرساخت‌ها به آن به نمایش در آمده است، این زیرساخت بیشترین ارتباط را با زیرساخت حمل و نقل داشته و ارتباطی با زیرساخت آب، گاز نفت و هسته‌ای ندارد و به مفهوم دیگر زیرساخت‌های اشاره شده وابسته به آن نیستند.

در شکل ۱۸ ارتباطات زیرساخت گاز نمایش داده شده است زیرساخت برق و حمل و نقل به ترتیب بیشترین وابستگی را به زیرساخت گاز دارند. در شکل ۱۹ نیز ارتباطات زیرساخت نفت و وابستگی دیگر زیرساخت‌ها به آن به نمایش در آمده است، زیرساخت پتروشیمی بیشترین وابستگی را به آن دارد.

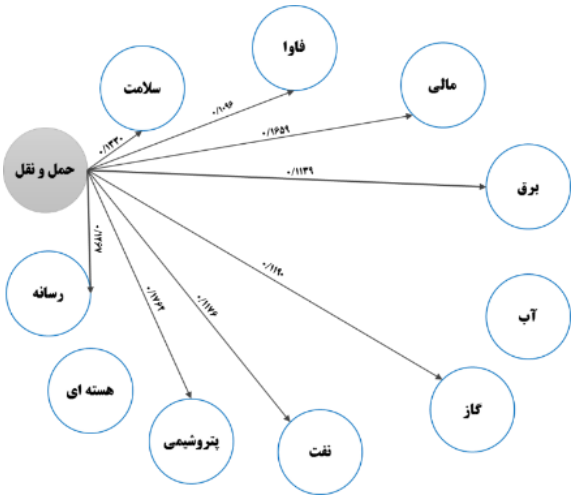
در شکل ۲۰ ارتباطات زیرساخت آب نمایش داده شده است زیرساخت سلامت تنها زیرساختی است که به آن وابستگی را نشان می‌دهد.



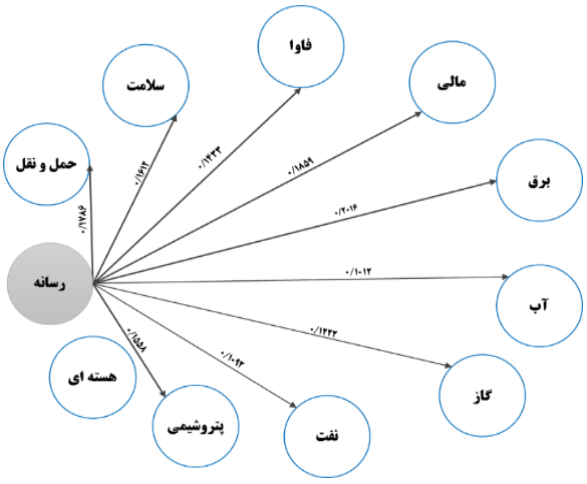
شکل ۱۱. ارتباط بین زیرساخت‌های حیاتی



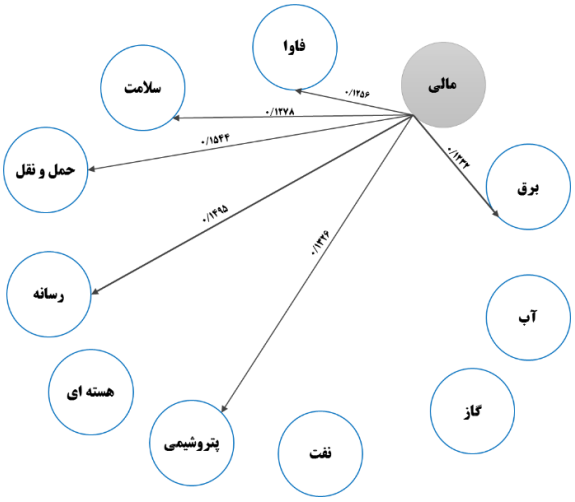
شکل ۱۲. ارتباطات و وابستگی زیر ساخت فاوا



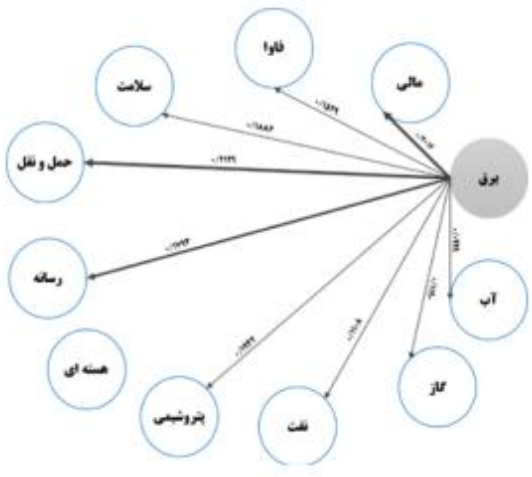
شکل ۱۵. ارتباطات و وابستگی زیرساخت حمل و نقل



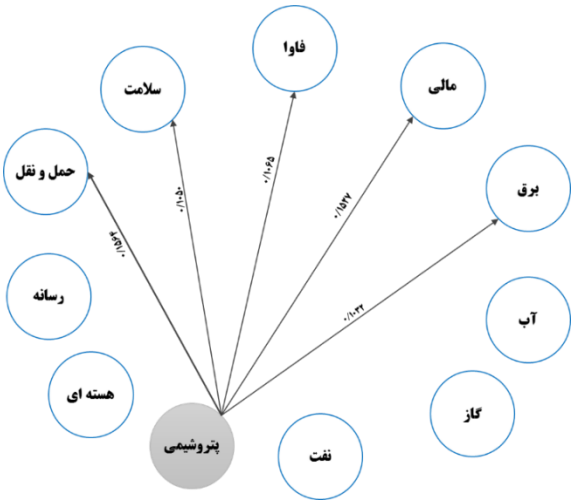
شکل ۱۳. ارتباطات و وابستگی زیرساخت رسانه



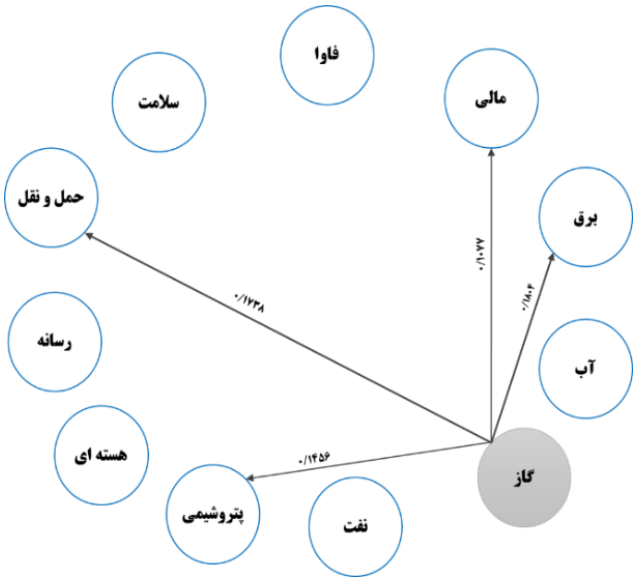
شکل ۱۶. ارتباطات و وابستگی زیرساخت مالی



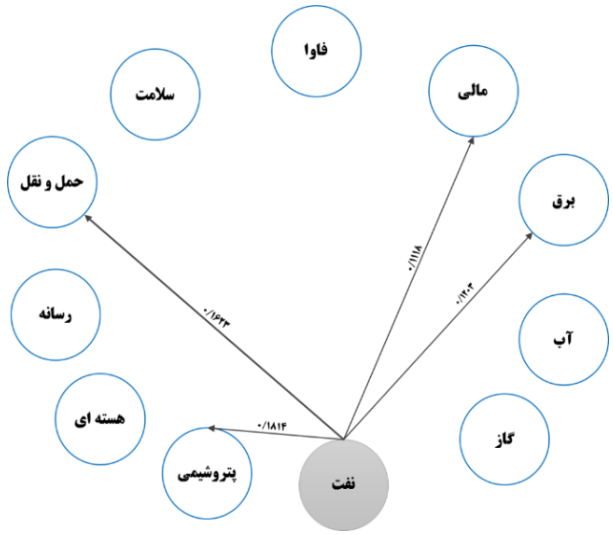
شکل ۱۴. ارتباطات و وابستگی زیرساخت برق



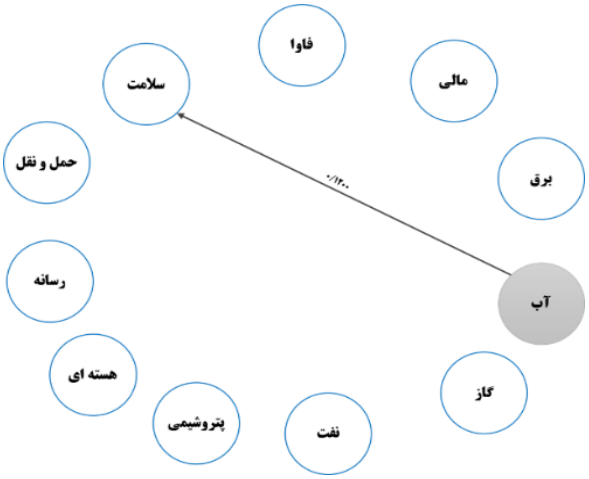
شکل ۱۷. ارتباطات و وابستگی زیرساخت پتروشیمی



شکل ۱۸. ارتباطات و وابستگی زیرساخت گاز



شکل ۱۹. ارتباطات و وابستگی زیرساخت نفت



شکل ۲۰. ارتباطات و وابستگی زیرساخت آب

۷- نتیجه‌گیری و پیشنهاد

در خصوص شناسائی زیرساخت‌های حیاتی بعد از مطالعات تطبیقی با دیگر کشورها زیرساخت‌ها از منظر امنیت سایبری با تشکیل پنل خبرگی احصاء شد با تطابق خروجی‌های پنل با اسناد بالادست و سیاست‌های کلی نظام مشخص شد زیرساخت رسانه می‌بایست به عنوان یک زیرساخت حیاتی از منظر امنیت سایبری مورد توجه ویژه قرار گیرد همچنین خروجی جلسات کانونی و تحلیل نتایج پژوهش نشان می‌دهد که زیرساخت رسانه به عنوان سومین زیرساخت بعد از زیرساخت‌های فاوا و برق جزو تاثیرگذارترین زیرساخت‌ها به شمار می‌آید و همچنین در تاثیرپذیری رتبه ششم را در بین یازده زیرساخت معرفی شده داراست و از نظر ارتباط با دیگر زیرساخت‌های حیاتی در رتبه چهارم قرار دارد این موارد خود تایید و تبیین‌کننده دغدغه مقام معظم رهبری مدظله‌العالی در خصوص رسانه و جنگ رسانه‌ای در فضای مجازی است.

همچنین بر مبنای یافته‌ها زیرساخت فناوری اطلاعات و ارتباطات (فاوا) به عنوان تاثیرگذارترین زیرساخت حیاتی از منظر سایبری بر دیگر زیرساخت‌های حیاتی شناخته شد، زیرساخت برق در حوزه انرژی بعد از آن جز تاثیرگذارترین زیرساخت‌ها قرار دارد همچنین تاثیرپذیرترین زیرساخت حیاتی حمل و نقل معرفی شد و بعد از آن زیرساخت پتروشیمی در رتبه دوم قرار گرفت.

در این پژوهش کلیه ارتباط و وابستگی‌های بین زیرساخت‌های حیاتی احصاء شد و زیرساخت هسته‌ای و سلامت هیچ ارتباطی با دیگر زیرساخت‌های حیاتی از منظر امنیت سایبری نداشتند.

نتایج و خروجی‌های این پژوهش می‌تواند مدیران ارشد حوزه‌های زیرساختی کشور را در اتخاذ تصمیمات راهبردی کلان یاری نماید.

پیشنهاد می‌گردد زیرساخت رسانه جزو زیرساخت‌های حیاتی از منظر امنیت سایبری لحاظ گردد همچنین خروجی و نتایج این پژوهش می‌تواند در طراحی، ایجاد و راه‌اندازی سامانه ملی اشتراک‌گذاری هشدار به منظور احصاء آگاهی وضعیتی ملی در حوزه سایبری و دیگر تحقیقات متکی بر وابستگی زیرساخت‌های حیاتی که در طرح مصوب راهبردی حفاظت از زیرساخت‌های کشور ایران نیز به صراحت به آن اشاره شده است، مفید واقع شود. اما از آن‌جایی‌که تهدیدات و حملات سایبری بر روی دارایی‌های زیرساخت‌های حیاتی صورت می‌گیرد، شناخت، دسته‌بندی و اولویت‌بندی دارائی‌های زیرساخت‌های حیاتی، نگاشت این دارائی‌ها بر خدمات علاوه بر شناخت خدمات و ماموریت‌های زیرساخت‌های حیاتی ضرورت پیدا می‌کند این مهم می‌تواند منجر به شناسائی بهتر

و دقیق‌تر ارتباط بین زیرساخت‌های حیاتی گردد لذا پیشنهاد می‌گردد الگویی تدوین شود تا بوسیله آن زیرساخت‌های حیاتی بتوانند دارائی‌های خود را شناسائی نموده و نگاشتی بین دارائی‌ها و خدماتی که ارائه می‌نمایند حاصل گردد این نکته نیز حائز اهمیت است که اطلاعات دارائی‌های زیرساخت‌های حیاتی جزء اسناد طبقه‌بندی شده کشورها می‌باشد و محدودیتی به جهت پژوهش از این روش فراهم می‌نماید.

مراجع

[1] Ziring, N. NATIONAL CYBER RESILIENCE AND ROLES FOR PUBLIC AND PRIVATE SECTOR STAKEHOLDERS. in International Conference on Critical Infrastructure Protection. 2022. Springer.

[2] Cyber Security and Infrastructure Security Agency, Critical Infrastructure Sectors, Arlington, Virginia (*www.dhs.gov/CISsa/criti* cal-infrastructure-sectors). 2020.

[3] Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE control systems magazine, 2001. **21**(6): p. 11-25.

[4] Thissen, W. and P. Herder, Synthesis of Approaches and Insights: Conclusions and Research Agenda. Critical Infrastructures State of the Art in Research and Application, 2003: p. 283-300.

[5] Clinton, W.J., Executive order 13010-critical infrastructure protection. Federal register, 1996. **61**(138): p. 37347-37350.

[6] CounCIl, E., Communication from the commission to the counCILs and the European Parliament: Critical infrastructure protection in the fight against terrorism. 2004: p. 1–11.

[7] India : workshop presentation by the NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE (NCISIPC), . 2015.

[8] Israel, *https://ironscales.com/blog-how-machine-learning-can-stop-phishing-attacks-critical-infrastructure/(2023*). 2023.

[9] Japan, The Information Security Policy CounCISl, The Second Action Plan on Information Security Measures for Critical Infrastructures, Japan (2009). 2009.

[10] Arabia, K.o.S., Developing National Information Security Strategy for the Kingdom of Saudi Arabia NISS draft 7. 2022.

[11] Gheorghe, A., et al., Critical infrastructures at risk. Securing the European electric power system, 2006.

[12] ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts, ITU-D Secretariat, Geneva. 2008.

[13] Australian :Critical Infrastructure Resilience Strategy. 2010.

[14] QATAR National Cyber Security Strategy. May 2014.

[15] NIST Glossary/ NIST SP 800-30 / CNSSI 4009-2015. 2015.

[16] ISO/IEC TR 27019:2013 Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems speCISfic to the energy utility industry. 2013.

[17] IETF RFC449 Internet Security Glossary 2: *https://tools.ietf.org/html/rfc4949*.

[18] UK.: Centre for the Protection of National Infrastructure (CPNI)

[19] NATO: Tallinn Manual on the International Law Applicable to Cyber Warfare. 2013.

[20] Canada: An Emergency Management Framework for Canada (Second Edition).

[21] Cuba : Glossary of Cyber terms/Glosario de términos, Centro de Seguridad del CISberespaCISo.

[22] FRG, G., National strategy for critical infrastructure protection. 2009: p. 1-18.

[23] Brussels, B., Commission of the European Communities. Retrieved from *http://eur-lex*.

[24] National Cybersecurity Strategy - Towards A Secure Cyberspace 2020-2023. 2020.

[25] Danish Cyber and Information Security Strategy (2022-2024).

[26] European Parliament and of the CounCISl 2022.

[27] Karakoc, D.B., K. Barker, and A.D. González, Analyzing the tradeoff between vulnerability and recoverability investments for interdependent infrastructure networks. Socio-Economic Planning Sciences, 2023. **87**: p. 101508.

[28] Zimmerman, R. Decision-making and the vulnerability of interdependent critical infrastructure. in 2004 IEEE International Conference on Systems, Man and Cybernetics (IEEE Cat. No. 04CH37583). 2004. IEEE.

[29] Eusgeld, I., C. Nan, and S. Dietz, "System-of-systems" approach for interdependent critical infrastructures. Reliability Engineering & System Safety, 2011. **96**(6): p. 679-686.

[30] GAO, U., Critical infrastructure protection: Challenges and efforts to secure control systems. US GAO, 2004.

[31] Eusgeld, I. and C. Nan. Creating a simulation environment for critical infrastructure interdependencies study. in 2009 IEEE International Conference on Industrial Engineering and Engineering Management. 2009. IEEE.

[32] Wang, F., J.J. Magoua, and N. Li, Modeling cascading failure of interdependent critical infrastructure systems using HLA-based co-simulation. Automation in Construction, 2022. **133**: p. 104008.

[33] Lee II, E.E., J.E. Mitchell, and W.A. Wallace, Restoration of services in interdependent infrastructure systems: A network flows approach. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2007. **37**(6): p. 1303-1317.

[34] Haggag, M., et al., Resilient cities critical infrastructure interdependence: a meta-research. Sustainable and resilient infrastructure, 2022. **7**(4): p. 291-312.

[35] Fisher, E., What practitioners consider to be the skills and behaviours of an effective people project manager. International journal of project management, 2011. **29**(8): p. 994-1002.

[36] Min Ouyang Review on modeling and simulation of interdependent critical infrastructure systems, Reliability Engineering & System Safety Volume 121,2014, Pages 43-60, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2013.06.040.