فصلنامه علمی اقتصاد و بانکداری اسلامی، شماره چهل و نهم، زمستان ۱۴۰۳- صفحات ۳۳۶-۳۰۷

# امنیت فضای سایبری و رشد اقتصادی: مطالعه موردی کشورهای اسلامی

## نوع مقاله: پژوهشی

علی مهرگان[۱]
نیلوفر مرادحاصل[۲]

تاریخ دریافت: ۱۴۰۳/۴/۱۷ تاریخ پذیرش: ۱۴۰۳/۷/۲۱

**چکیده**

*هدف از این پژوهش بررسی اثر امنیت فضای سایبری بر رشد اقتصادی در کشورهای اسلامی (شامل ایران) می‌باشد. بطورکلی هرگونه اختلال در امنیت سایبری می‌تواند چالش‌هایی را برای کسب وکارها ایجاد نموده و ثبات و رشد اقتصادی را مختل نماید. می‌توان اینگونه ادعا نمود که در شرایط حملات سایبری اقتصاد با نوعی شکست بازار مواجه می‌گردد. لذا برقراری امنیت سایبری در سطح کلان کشور بعنوان یک خدمت عمومی درنظر گرفته می‌شود. بررسی این موضوع (اثر امنیت فضای سایبری بر رشد اقتصادی) در منتخبی از کشورها در دستور کار مطالعه حاضر قرار دارد. بازه مورد بررسی در این پژوهش دوره ۲۰۲۲-۲۰۱۲ و روش برآورد الگوی اقتصاد سنجی پانل دیتا می‌باشد. نتایج حکایت از آن دارد که افزایش امنیت سایبری اثر معنادار و مثبتی بر رشد اقتصادی کشورهای مورد مطالعه داشته است. هرچند این اثر اندک بوده است. این یافته تلویحاً این توصیه سیاستی را خاطر نشان می‌سازد که همزمان با سرمایه‌گذاری در زیرساخت‌های فناوری اطلاعات و ارتباطات و افزایش ضریب نفوذ این فناوری (بعنوان شرط لازم)، توجه به مقوله امنیت این حوزه (به عنوان شرط کافی) ضروری و اجتناب ناپذیر می‌باشد.*

**کلمات کلیدی:** شاخص جهانی امنیت سایبری، کشورهای اسلامی، رشد اقتصادی، اقتصاد دیجیتال.
**JEL**: O47, H41, F5, C23

۱ دکتری علوم اقتصادی، پژوهشگر، پژوهشگاه ارتباطات و فناوری اطلاعات 110mehregan@gmail.com
۲ استادیار اقتصاد، عضو هیئت علمی پژوهشگاه ارتباطات و فناوری اطلاعات (نویسنده مسئول)
nmoradhasel@itrc.ac.ir

**مقدمه**

از دهه ۱۹۹۰ تاکنون«اقتصاد دیجیتال» به صورت مداوم تکامل یافته است؛ که این موضوع نشان دهنده ماهیت سریع فناوری و استفاده از آن توسط بنگاه‌ها و مصرف‌کنندگان است (بیرفوت[۱] و همکاران، ۲۰۱۸). «اقتصاد دیجیتال» به اقتصادی گفته می‌شود که مبتنی بر فناوری‌های محاسبات دیجیتال است (چوهان[۲]، ۲۰۲۰). به عبارتی اقتصاد دیجیتال، یک اقتصاد مبتنی بر داده‌ها و محاسبات دیجیتال و تلفیق آن با فناوری‌های نوین به منظور اثرگذاری بر تمام فرآیندهای سیاسی، اجتماعی، اقتصادی و... یک زیست بوم است.(مرادحاصل و همکاران،۱۴۰۰) با آشکار شدن اثرات مثبت اقتصاد دیجیتال در ارتقای بهره‌وری، ایجاد اشتغال، رشد اقتصادی، توسعه بازارهای صادراتی و افزایش ارزش کالا و خدمات صادراتی، این موضوع به عنوان یکی از مهم‌ترین برنامه‌ها در هر کشور و حتی موتور پیشران اقتصاد در برخی کشورهای توسعه یافته و اقتصادهای نوظهور مورد توجه دولت‌ها قرار گرفته است (اسعدی، ۱۳۹۸).

امنیت و برقراری یک رابطه تجاری ایمن و سالم در اقصاد دیجیتال بسیار مهم است. اقتصاد دیجیتال، بخاطر دسترسی وسیعتر کاربران، ازمیان رفتن تعاملات حضوری و تهدید امنیت فضای سایبری از طریق بدافزارها[۳]، فیشینگ[۴]، باج‌افزار[۵]، رخنه داده‌ها[۶] و امثال آن با چالش‌های متعدد امنیتی مواجه می‌باشد. کسب‌وکارهای دیجیتال برای انجام عملیات و فعالیت‌های خود به انواع ابزار و تجهیزات دیجیتالی نیاز دارند که این ابزارها می‌توانند هدف حملات سایبری قرار گیرند. این حملات می‌توانند عملیات تجاری را مختل کنند و باعث خرابی، از دست دادن درآمد، آسیب به اعتماد مشتریان، نقض حریم خصوصی، سرقت اطلاعات محرمانه و عواقب قانونی شوند. بنابراین، تأمین امنیت سایبری برای کسب‌وکارهای دیجیتال از اولویت‌های اصلی است که باید به آن توجه کافی شود(لین[۷]،۲۰۲۲).

امنیت سایبری در اقتصاد دیجیتال نقش مهمی در بهبود کیفیت خدمات دیجیتال دارد. زیرا با ارائه محیطی ایمن و مطمئن برای تعاملات تجاری، افزایش رضایت مشتریان، کاهش ریسک‌ها و خطرات، افزایش اعتماد و وفاداری؛ کیفیت خدمات دیجیتال را بهبود می‌بخشد. امنیت سایبری همچنین با حفاظت از داده‌ها، دارایی‌ها و حریم خصوصی کسب‌وکارها و مشتریان، از نقض حقوق و

---

۱- Barefoot.
۲- Chohan.
۳ Malware
۴ Phishing
۵ Ransomware
۶ Data Breach
۷ Lynn

قوانین مربوط به اقتصاد دیجیتال جلوگیری می‌کند. به طور خلاصه، امنیت سایبری یکی از شرایط ضروری برای موفقیت و پیشرفت کسب‌وکارهای دیجیتال است که باید به آن اهمیت داده شود.

امنیت سایبری اغلب از نظر نقض داده‌ها، جریمه‌های نظارتی و اختلال در تجارت مورد بحث قرار می‌گیرد و مزایای آن به ندرت بررسی می‌شود. امنیت سایبری مؤثر این امکان را برای شرکت‌ها فراهم می‌کند که نوآوری کنند و نوآوری باعث درآمد، سود و رشد می‌شود. دفاع در برابر جرائم سایبری می‌تواند منافع حقیقی برای شرکت‌های کوچک و متوسط داشته باشد. از آنجایی که سازمان‌ها در هر اندازه به سمت افزایش کارایی از طریق فرآیندهای دیجیتالی حرکت می‌کنند، برای رهبران کسب‌وکار مهم است که نحوه تفکر خود در مورد امنیت را دوباره تعریف کنند (لوید[۱]، ۲۰۲۰).

حملات سایبری به شدت افزایش یافته است. بنابراین، سازمان‌های تجاری باید تهدیدات امنیت سایبری و بهترین روش برای کاهش همه جانبه آنها را درک کنند. هدف این حملات معمولاً ارزیابی، تغییر یا از بین بردن اطلاعات حساس است. اخاذی منافع پولی از کاربران؛ یا قطع شدن فرآیندهای عادی کسب‌وکار از جمله موارد حملات سایبری هستند. امنیت سایبری شامل تکنیک‌هایی برای محافظت از رایانه‌ها و شبکه‌ها در برابر دسترسی غیرمجاز و فعالیت‌های مخرب مانند سرقت و تخریب داده‌ها است. هزینه‌های امنیت سایبری و جرائم سایبری در سطح جهانی روند رو به افزایشی را نشان می‌دهند و برخی مطالعات نشان‌دهنده این موضوع هستند که این هزینه توسط عوامل اقتصادی کمتر از حد برآورد می‌شوند (ثقیب سعید[۲]، ۲۰۲۳).

تخمین زده می‌شود که جرایم سایبری در سال ۲۰۲۰ حدود ۱ تریلیون دلار برای اقتصاد جهانی هزینه داشته است که نشان دهنده افزایش بیش از ۵۰ درصدی از سال ۲۰۱۸ است. با افزایش میانگین خسارت بیمه سایبری از ۱۴۵،۰۰۰ دلار در سال ۲۰۱۹ به ۳۵۹،۰۰۰ دلار در سال ۲۰۲۰، روند رو به رشدی نیز در این حوزه مشاهده می شود که این روند ضرورت ایجاد و تدارک منابع اطلاعاتی سایبری کاراتر، پایگاه های داده استاندارد، الزام به گزارش دهی و افزایش آگاهی‌های عمومی و ... را خاطر نشان می‌سازد ( کرمر[۳]، ۲۰۲۲).

بی‌توجهی به امنیت سایبری در اقتصاد دیجیتال پیامدهای بسیاری همچون «نقض داده‌ها و از دست دادن اطلاعات محرمانه»، « کلاهبرداری و سرقت مالی»، «اختلال در عملیات و غیر دسترس نمودن خدمات برای مشتریان»،«آسیب به اعتبار و از دست دادن اعتماد عمومی»، « کاهش اعتماد مشتریان به خدمات و محصولات دیجیتال»، «ایجاد محدودیت در توسعه کسب‌وکارهای نوآورانه» و

---

۱ Lloyd

۲ Saqib Saeed

۳ Cremer

امثال آن دارد که تهدید امنیتی در سطح ملی و خسارات بسیاری به کسب وکارها ایجاد می‌کند. بنابراین، توجه به امنیت سایبری و سرمایه‌گذاری در آن، یک ضرورت راهبردی برای هر اقتصاد دیجیتالی است که می‌تواند منجر به افزایش اعتماد، ثبات و رشد اقتصادی پایدار شود.

به همین دلیل می‌توان انتظار داشت که در شرایط حملات سایبری اقتصاد با نوعی شکست بازار مواجه گردد که اثرات جانبی منفی آن توسط بازار تأمین نشده و برای نزدیک‌تر شدن به حالت بهینه نیاز به مداخله دولت احساس می‌شود. در ادبیات نظری برقراری امنیت سایبری در سطح کلان کشور بعنوان یک خدمت عمومی درنظر گرفته می‌شود. در این راستا در ایران در برنامه هفتم توسعه کشور به عنوان سند بالادستی، در ماده ۱۰۷ به صراحت در مورد امنیت فضای سایبری و در ماده ۶۶ در مورد سهم اقتصاد رقومی (دیجیتال) تأکید و توصیه شده است.

تحلیل اقتصادی سرمایه‌گذاری در فناوری‌های امنیتی، با دیگر سرمایه‌گذاری‌های مورد بررسی در اقتصاد تفاوت دارد. در این‌گونه سرمایه‌گذاری‌ها نمی‌توان به صورت مستقیم سودی برای سرمایه‌گذاری در نظر گرفت، بلکه می‌توان اثرات مثبت سرمایه‌گذاری در فناوری‌های امنیتی را در فضای فعالیت‌های اقتصادی مشاهده نمود. در ادبیات سرمایه‌گذاری هرچه ریسک و عدم اطمینان بالاتر باشد، فرار سرمایه و کاهش رشد و گسترش کسادی نیز بیشتر خواهد شد. در واقع اهمیت سرمایه‌گذاری در امنیت هنگامی مشخص خواهد شد که در اثر نبود آن، سرمایه‌گذاری و فضای اقتصادی ضربه بخورد.

یکی از راه‌های بررسی اثرگذاری سرمایه‌گذاری در امنیت اقتصادی بر روی فضای اقتصاد، محاسبه اثرات آن بر روی یکی از مهم‌ترین متغیرهای اقتصادی یعنی تولید ناخالص داخلی است. عوامل مختلفی بر روی تولید اقتصاد اثرگذارند، در این مطالعه پاسخ به این پرسش دنبال می‌شود که با توجه به مدل رشد نئوکلاسیک سولو[۱] (۱۹۵۶)، اثرات سرمایه‌گذاری در فناوری‌های امنیت سایبری به چه صورت خود را در روند رشد اقتصادی نمایان می‌کنند. به همین منظور کشورهای منتخب اسلامی (از جمله کشور ایران) مورد بررسی قرارگرفته‌اند.

در ساختار این پژوهش در ادامه ابتدا ادبیات موضوع شامل مبانی نظری پژوهش و مطالعات تجربی بررسی شده، سپس روش‌شناسی انجام پژوهش ذکر می‌شود، پس از آن نتایج مدل تشریح شده آورده می‌شود و در نهایت جمع‌بندی نتایج پژوهش ارائه می‌شود.

## ادبیات موضوع

### مبانی نظری

۱ Solow

ادبیات رشد اقتصادی نوین با مدل معرفی شده توسط رابرت سولو (۱۹۵۶) آغاز شد. این مدل پایه‌گذار نظریه مدرن رشد اقتصادی است. آنچه تکامل سال‌های طولانی مدل سولو به ادبیات اقتصادی اضافه کرده است بیان می‌دارد که برای رسیدن به رشد اقتصادی باید موانع کسب‌وکار ناشی از مداخله دولت و هزینه‌های مبادله برای فعالیت‌های اقتصادی بر اثر مداخله دولت افزوده نشود و حقوق مالکیت محترم شمرده شود و با حصول امنیت برای کسب‌وکارها، بنگاه‌های ریز و درشت به صورت خودجوش و با تلاش خود برای کاهش هزینه و بهبود کیفیت محصول و معرفی محصولات جدید، اسباب رشد دانش و فنّاوری و به‌کارگیری آن برای خلق ثروت و رشد اقتصادی و رفاه را فراهم سازند.

بر اساس مدل رشد سولو[۱]، رشد اقتصادی تابعی از نیروی کاری، سرمایه و بهره‌وری است که بر این اساس تابع تولید به صورت زیر نوشته می‌شود:

(۱)

$$Q_t = A(\mathrm{t}).\mathrm{f}(\mathrm{K}_t, \mathrm{N}_t)$$

در معادله (۱) $Q_t$ تولید در زمان t، $\mathrm{K}_t$ سرمایه و $\mathrm{N}_t$ نیز نیروی کار است. در این مدل $\mathrm{A(t)}$ نشان‌دهنده پیشرفت فناوری است که از آن با نام پسماند سولو نیز یاد می‌شود.

برای تبدیل تابع تولید سولو به مدل رشد اقتصادی لازم است از تابع تولید معرفی شده در معادله (۱) دیفرانسیل بگیریم. با دیفرانسیل گیری از تابع تولید سولو می‌توان تغییرات تولید را نسبت به تغییرات سرمایه و نیروی کار موجود، مورد بررسی قرار داد. دیفرانسیل کلی تابع تولید سولو به این صورت است:

(۲)

$$dQ_t = f(\mathrm{K}_t, \mathrm{N}_t).\mathrm{dA(t)} + \mathrm{A}.\frac{df}{dk}dK + A.\frac{df}{dN}dN$$

حال با تقسیم طرفین به $\mathrm{Q_{t-1}}$ خواهیم داشت:

(۳)

$$\frac{dQ_t}{Q_{t-1}} = f(k_t, \mathrm{N}_t).\frac{\mathrm{dA(t)}}{Q_{t-1}} + \mathrm{A}.\frac{df}{dk_t}.\frac{dk_t}{Q_{t-1}} + A.\frac{df}{dN_t}.\frac{dN_t}{Q_{t-1}}$$

با استفاده از معادله تولید (معادله ۱) می‌توان معادله بالا را به صورت زیر بازنویسی کرد:

---

۱ Solow

(۴)

$$\frac{dQ_t}{Q_{t-1}} = \frac{\mathrm{dA(t)}}{\mathrm{A(t)}} + \mathrm{A}.\frac{df}{dk_t}\frac{k_t}{Q_{t-1}}.\frac{dK_t}{k_t} + A.\frac{df}{dN_t}\frac{N_t}{Q_{t-1}}.\frac{dN_t}{N_t}$$

با توجه به اینکه داده‌های اقتصادی ناپیوسته هستند، معادله بالا را می‌توان به صورت زیر نوشت:

$$\frac{\Delta Q_t}{Q_{t-1}} = a_0 + a_1.\frac{\Delta k_t}{k_t} + a_2.\frac{\Delta N_t}{N_t} \qquad (۵)$$

که در آن $a_1$ کشش سرمایه و $a_2$ کشش نیروی کار را نشان می‌دهد(یاوری، مهرگان، ۱۳۸۰). صندوق بین‌المللی پول[۱] (پویرسان، ۱۹۹۸)[۲]، ارتباط بین امنیت اقتصادی، سرمایه‌گذاری خصوصی و رشد را مشخص کرده است: به این ترتیب که در مدل‌های رشد نئوکلاسیک، نرخ کلی سرمایه‌گذاری در اثر افزایش نرخ سرمایه‌گذاری خصوصی در هر سطح، افزایش یافته و این به نوبه خود، سطح تعادلی تولید سرانه (به ازای هر کارگر) را ارتقا می‌بخشد. در این مطالعه؛ سرمایه‌گذاری خصوصی و رشد، متغیرهای درون‌زای مدل هستند و تأثیر امنیت سرمایه‌گذاری بر آنها آزمون شده است. پویرسان متغیرهای امنیت اقتصادی را به معادلات رشد افزوده است. وی در این مطالعه که با استفاده از روش پانل دیتا انجام شده است، اثرپذیری عمیق سرمایه‌گذاری بخش خصوصی و رشد اقتصادی از مفهوم امنیت اقتصادی را نشان داده است.

سرمایه فرار است و در جایی استقرار می‌یابد که امنیت سرمایه‌گذاری در آن نقطه تأمین‌شده باشد. این مسئله در اقتصاد دیجیتال نیز مستثنی نبوده و برقرار است بطوریکه در مطالعات مختلف همچون الینگ و همکاران[۳] (۲۰۲۳) نیز رابطه مثبت بین فضای کسب‌وکار و امنیت سایبری نشان داده شده است.

با افزایش فشارهای اقتصادی و رشد تصاعدی در نوآوری‌های فناوری، شرکت‌ها به طور فزاینده‌ای به فناوری‌های دیجیتال برای نوآوری و خلق ارزش تکیه می‌کنند. اما، با افزایش سطوح نقض امنیت سایبری، قابل اعتماد بودن بسیاری از فناوری‌های جدید و جا افتاده نگران‌کننده است. در نتیجه، شرکت‌ها به شدت در حال افزایش امنیت سایبری دارایی‌های دیجیتالی موجود و جدید خود هستند. اکثر شرکت‌ها باید با این اولویت‌ها به طور هم‌زمان مقابله کنند که اغلب متناقض هستند و تنش ایجاد می‌کنند (نلسون و مانیک[۴]، ۲۰۱۷).

---

۱ IMF (International Monetary Fund)

۲ Poirson

۳ Eling and etc.

۴ Nelson and Manick

کوهن[۱] و همکاران(۲۰۱۷) به بررسی نقش امنیت سایبری در منتخبی از کشورها همچون بریتانیا، ایالات متحده آمریکا و... پرداخته اند. در این تحقیق اطلاعات موردنیاز به صورت میدانی و از طریق مصاحبه و پرسشنامه جمع آوری شده است. نتایج حکایت از آن دارد امنیت سایبری تاثیر معنی داری بر تحریک رشد اقتصادی به تفکیک مناطق و استان‌های کشورهای مورد بررسی دارد.

واسیو[۲] (۲۰۱۸) به منظور بررسی نقش امنیت سایبری در توسعه اقتصادی پایدار، از تحلیل اطلاعات پرونده‌های دادگاه‌ها درخصوص امنیت سایبری استفاده نموده است، در این مطالعه خطرات اصلی امنیت سایبری در سه دسته آسیب، سرقت و تقلب در پرداخت دسته‌بندی شده‌اند و برای هر دسته، مثال‌های واقعی ازمسائل اصلی مطرح شده است. یافته‌های این مطالعه بر نیاز به بهبود راهبردها، سیاست‌ها و برنامه‌های امنیت سایبری تأکید دارد و این مقاله به مجموعه اقداماتی در خصوص ایجاد شرایطی برای یک محیط توسعه اقتصادی امن‌تر و بهتر پرداخته است.

ژی جیان هه و همکاران[۳] (۲۰۲۰) بیان می‌کنند که حملات سایبری به کسب‌وکارها از سطح نوآوری شرکت‌ها می‌کاهد و هزینه‌های تحقیق و توسعه و سطح سرمایه‌گذاری در شرکت را کاهش می‌دهد و به طور کلی حملات سایبری بر تصمیمات راهبردی بنگاه اثرگذار است.

سعید و همکاران (۲۰۲۳) بیان کرده‌اند که تحول دیجیتال بهره وری و کارایی را افزایش می‌دهد اما باعث چالش‌های امنیت سایبری بیشتری می‌شود. بنابراین با بهبود امنیت فضای کسب و کار در محیط اقتصاد دیجیتال در واقع به بهبود کارایی و بهره وری در محیط کسب و کار کمک می‌شود.

پانتلیف[۴] (۲۰۲۳) امنیت سایبری را به عنوان یک محرک برای رشد اقتصاد دیجیتال در نظر گرفته است. وی بیان کرده است که دستورالعمل‌های تضمین تاب آوری در برابر تهدیدات سایبری از جمله عواملی هستند که در تحریک توسعه کارآفرینی در اقتصادهای دیجیتال نقش دارند.

آشیش[۵] و همکاران(۲۰۲۴) بیان می‌دارند که تعامل پیچیده‌ای بین فناوری‌های پیشرفته مانند بلاک‌چین، هوش مصنوعی و اینترنت اشیا و تأثیر آنها بر امنیت سایبری وجود دارد. بطوریکه درکنار توسعه این فناوری‌ها و نقش موثر آن‌ها بر پیشرفت اقتصاد دیجیتال، آسیب‌های امنیتی جدیدی مطرح است. همچنین در این مطالعه تأکید می‌شود اقدامات امنیت سایبری به عنوان محافظ‌های ضروری در برابر تهدیدات آنلاین است که پایداری و یکپارچگی بخش را در دراز مدت تضمین می‌کند. در این شرایط ضرورت اجرای پروتکل‌های کارآمد امنیت سایبری، شامل اقدامات پیشگیرانه،

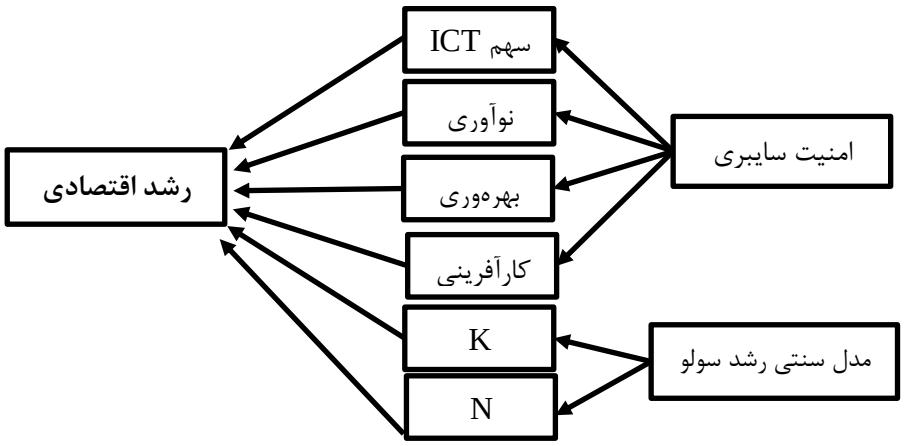
---

۱ Cohen
۲ Vasiu
۳ Zhijian He and etc.
۴ Panteleev
۵ Ashish

استراتژی‌های شناسایی و مکانیسم‌های واکنش سریع در برابر تهدیدات آنلاین ضروری است. بطورکلی این محققین بر اهمیت ترویج امنیت سایبری بر دیجیتالی شدن پایدار و رسیدن به رشد اقتصادی از طریق سرمایه گذاری در زیرساخت‌ها، ترویج استفاده اخلاقی از فناوری، همکاری بین ذینفعان، آموزش و امثال آن تاکید دارند.

آرویابه[۱] و همکاران(۲۰۲۴)، به بررسی نقش امنیت سایبری در ۲۴۰شرکت کوچک و متوسط (SMEs) در بریتانیا پرداخته‌اند. یافته‌های تحقیق دلالت بر نقش موثر اجرای امنیت سایبری برعملکرد بهترSMEها دارد.

با توجه به مباحث گفته شده، فرایند اثرگذاری امنیت سایبری بر روی رشد اقتصادی را می‌توان به صورت شکل ۱ نشان داد.




**شکل ۱. کانال اثرگذاری بر تولید ناخالص داخلی**

منبع: مستخرج از پژوهش

## مبانی تجربی

بیشتر ادبیات کار شده نزدیک به موضوع این پژوهش، ادبیات مربوط به اثرات اقتصاد دیجیتال بر رشد اقتصادی و همچنین ادبیات اثرات حملات سایبری یا درک سرمایه‌گذاری‌های امنیتی برای سازمان‌ها است. همچنین به صورت کلی اثرات امنیت بر روی اقتصاد بررسی شده است اما جای خالی پژوهشی با هدف تبیین اثرگذاری سرمایه‌گذاری در فناوری‌های امنیت سایبری در میان ادبیات موضوع کاملاً

۱ Arroyabe

محسوس است. در ادامه به برخی از مهم‌ترین ادبیات کار شده در موضوعات یاد شده پرداخته می‌شود. مطالعات این قسمت قابل تفکیک به دو دسته می‌باشند:

### ۱. مطالعات بررسی اثر اقتصاد دیجیتال بر رشد اقتصادی

مرادحاصل و کاظم پور (۱۴۰۱) اثر فناوری اطلاعات را بر رشد اقتصادی ایران بررسی کرده‌اند. بازه زمانی این پژوهش متعلق به ۲۰۱۰ الی ۲۰۱۹، روش ارزیابی اقتصادسنجی پانل دیتا و قلمرو پژوهش ۴۲ کشور منتخب بوده‌اند. از جمله نتایج ای پژوهش مثبت و معنادار بودن اثر فناوری اطلاعات بر رشد اقتصادی کشورهای مورد بررسی بوده است و هر یک درصد رشد در فناوری اطلاعات موجب ۰,۰۸ درصد رشد تولید ناخالص داخلی در کشورهای منتخب می‌شده است.

در مباحث توسعه اقتصادی به نقش و اهمیت کیفیت نهادی دولت بر رشد اقتصادی تأکید زیادی شده است. در این بین امنیت در بین شاخص‌های نهادی از اهمیت و جایگاه مهمی برخوردار است. هر چند در گذشته بیشتر توجه اقتصاددانان توسعه به امنیت مالکیت و ... بود ولی با گسترش فن‌آوری اطلاعات وجه به امنیت سایبری افزایش یافته است(خیاط رسولی، ۱۳۹۹).

داتا و آگاروال [۱](۲۰۰۴) با بررسی زیرساخت‌های مخابراتی بر روی رشد اقتصادی با رویکرد پانل دیتا نشان دادند که زیرساخت‌های مخابراتی از نظر آماری معنی‌دار است و با رشد تولید ناخالص داخلی واقعی سرانه کشورهای OECD همبستگی مثبت دارد. سرمایه‌گذاری در مخابرات مشمول بازدهی کاهشی است، که نشان می‌دهد کشورهایی که در مراحل اولیه توسعه هستند احتمالاً بیشترین سود را از سرمایه‌گذاری در زیرساخت‌های مخابراتی خواهند برد. بر اساس داده‌ها، ارائه زیرساخت‌های مخابراتی کارآمد برای تقویت رشد اقتصادی بسیار مهم است.

جعفری صمیمی و اختیاری (۱۳۸۸)، به بررسی رابطه بین امنیت و رشد اقتصادی در ایران کشورهای کنفرانس اسلامی پرداخته‌اند. بازه مطالعاتی ۱۹۹۷ الی ۲۰۰۵ بوده و نتایج حاصله از مدل پانل دیتا نشان‌دهنده تأثیر مثبت و معنادار امنیت بر روی رشد اقتصادی است.

صامتی و همکاران (۱۳۸۹)، رابطه بین امنیت حقوق مالکیت، قوانین و مقررات با رشد اقتصادی را مورد بررسی قرار داده‌اند. در این پژوهش بین سال‌های ۲۰۰۰ الی ۲۰۰۵ در ۸۰ کشور اثر امنیت حقوق مالکیت و قوانین و مقررات را بر رشد اقتصادی بررسی کرده‌اند. نتایج مدل‌های پانل دیتا در این پژوهش نشان‌دهنده اثر مثبت و معنادار امنیت حقوق مالکیت و همچنین قوانین بازار اعتبارات و بازار کار بر روی رشد اقتصادی است.

---

۱ Datta and Agarwal

اسماعیل نیا و وصفی اسفستانی (۱۳۹۵)، رابطه بین امنیت و رشد اقتصادی را در ۱۳۵ کشور بررسی کردند. بازه این بررسی سال‌های ۲۰۰۴ الی ۲۰۱۴ و روش بررسی پانل دیتا بوده است. نتایج به دست آمده نشان می‌دهد که مؤلفه‌های مخارج نظامی و شکنندگی دولت تأثیر منفی بر رشد اقتصادی دارد و به هر اندازه که دولت‌ها شکننده‌تر باشند، میزان رشد اقتصادی در آن کشورها پایین‌تر خواهد بود.

مهرگان و همکاران(۱۳۹۴) به تأثیر اقتصاد دیجیتال بر رشد اقتصادی از طریق کاهش فساد نیز پرداختند. یکی از موانع مهم رشد اقتصادی خصوصاً در کشورهای در حال توسعه گسترش فساد می‌باشد، فضاهای مجازی فرصت خوبی را فراهم نموده تا بسیاری از این فسادها برملا شده و فعالیت‌های زیرزمینی در این کشورها کاهش یابد.

ویجیان[۱] (۲۰۱۹) تأثیر برنامه هند دیجیتال بر اقتصاد و پیشرفت آن در دستیابی به اهداف توسعه پایدار را مورد بحث قرار می‌دهد. دولت هند برنامه هند دیجیتال را برای تحریک توسعه اقتصادی و ایجاد فرصت‌های شغلی برای جوانان آغاز کرد. هدف اصلی این برنامه ارائه کلیه خدمات به شهروندان از طریق درگاه‌های اینترنتی و وسایل الکترونیکی و روان و شفاف‌سازی معاملات است. دولت در حال سرمایه‌گذاری در فناوری است تا پول سیاه و فساد را از زندگی عمومی حذف کند. بر اساس نتایج این پژوهش انتظار می‌رود تحول دیجیتال در هند تأثیر قابل‌توجهی بر اقتصاد داشته باشد و به دستیابی به دستور کار اهداف پایدار سازمان ملل تا سال ۲۰۳۰ کمک کند. همچنین کمپین هند دیجیتال در هند در ایجاد فرصت‌های شغلی، بهبود نرخ سواد، حذف فساد و افزایش تولید ناخالص داخلی (GDP) موفق بوده است. استفاده از فن‌آوری‌های دیجیتال در خدمات عمومی و حکمرانی، ارتباطات مؤثر بین شهروندان و دولت را افزایش داده و منجر به شفافیت و قابلیت اطمینان در معاملات می‌شود.

اخلاقی (۱۳۹۸)، تأثیر متقابل امنیت، رشد و توسعه اقتصادی در اسلام را به روش توصیفی تحلیلی بررسی کرده است. یافته‌های این پژوهش بیانگر آن است که امنیت اقتصادی، رشد و توسعه برهمدیگر اثرگذارند و فقدان امنیت فعالیت‌های اقتصادی را مورد تهدید قرار می‌دهد.

جیائو و سان[۲] (۲۰۲۱) اثر توسعه اقتصاد دیجیتال بر رشد اقتصادی چین را بررسی می‌کنند، این مطالعه بر اهمیت در نظر گرفتن نرخ رشد اقتصادی، وضعیت زندگی دیجیتال و انعطاف‌پذیری محیط در هنگام توسعه یک استراتژی دیجیتالی سازی مؤثر در یک کشور تأکید می‌کند. یافته‌ها نیاز به مقررات قوی‌تر را برای تضمین رقابت بین شرکت‌ها و توسعه مهارت‌های سازگار با خواسته‌های اقتصاد مدرن برای بهره‌مندی کامل از دیجیتالی شدن نشان می‌دهد. توسعه اقتصاد دیجیتال چین تأثیر مستقیم مثبتی بر رشد اقتصادی منطقه و همچنین تأثیر غیرمستقیم مثبت (اثر سرریز) بر مناطق

---

۱ Vijayan

۲ Jiao and Sun

همسایه دارد. توسعه شدید اقتصاد دیجیتال نه تنها شتاب رشد فضایی را برای منطقه فراهم می‌کند، بلکه به رشد اقتصادی مناطق همسایه کمک می‌کند و در نهایت منجر به هماهنگی منطقه‌ای و توسعه پایدار می‌شود.

گومز و همکاران[۱] (۲۰۲۲) با روش GMM تأثیر اقتصاد دیجیتال بر رشد اقتصادی در کشورهای OECD را تحلیل می‌کنند. فناوری اطلاعات و ارتباطات (ICT) تأثیر مثبتی بر توسعه اقتصادهای OECDدارد و می‌تواند به عنوان ابزاری توسط سیاست‌گذاران استفاده شود. سیاست‌گذاران باید سیاست‌هایی را اجرا کنند که زیرساخت‌های فیزیکی و فناوری ICT را تقویت کند، توانمندسازی دیجیتالی سرمایه انسانی را ارتقا بخشد و عدالت اجتماعی بیشتری را در دسترسی به ICT تضمین کند.

الکساندروا و همکاران[۲] (۲۰۲۲) اثر دیجیتالی شدن بر رشد اقتصادی روسیه را بررسی کرده‌اند، این مطالعه نشان می‌دهد که محیط کلان فعلی و آمادگی جمعیت در روسیه اجازه نمی‌دهد فناوری های دیجیتال به طور قابل‌توجهی بر نرخ رشد اقتصادی تأثیر بگذارد. این مطالعه بر اهمیت در نظر گرفتن نرخ رشد اقتصادی، وضعیت زندگی دیجیتال و انعطاف پذیری محیط در هنگام توسعه یک استراتژی دیجیتالی سازی مؤثر در یک کشور تأکید می‌کند .یافته‌ها نیاز به مقررات قوی‌تر را برای تضمین رقابت بین شرکت‌ها و توسعه مهارت‌های سازگار با خواسته‌های اقتصاد مدرن برای بهره‌مندی کامل از دیجیتالی شدن نشان می‌دهد.

## ۲. مطالعات اقتصادی در حوزه امنیت سایبری

مور[۳] (۲۰۱۰) بیان می‌کند که نگاهی اقتصادی به امنیت سایبری بهتر از نگاهی صرفاً فنی به آن است. زیرا برخی شکست‌ها در فراهم سازی امنیت سایبری به این دلیل است که هزینه‌های حمله سایبری تماماً به شرکت‌ها منتقل نشده و افراد جامعه نیز هزینه می‌دهند (وجود اثرات جانبی منفی). او همچنین عدم تقارن اطلاعاتی و انگیزه‌های نادرست را دیگر چالش‌های اقتصادی حوزه امنیت سایبری می‌داند.

نلسون و مانیک (۲۰۱۷) بیان می‌دارند با افزایش فشارهای اقتصادی و رشد تصاعدی در نوآوری‌های فناوری، شرکت‌ها به طور فزاینده‌ای به فناوری های دیجیتال برای نوآوری و خلق ارزش تکیه می‌کنند. اما، با افزایش سطوح نقض امنیت سایبری، قابل‌اعتماد بودن بسیاری از فناوری‌های

---

۱ Gomes and etc.

۲ Aleksandrova and etc.

۳ Moore

جدید و جاافتاده نگران‌کننده است. در نتیجه، شرکت‌ها به شدت در حال افزایش امنیت سایبری دارایی‌های دیجیتالی موجود و جدید خود هستند. اکثر شرکت‌ها باید با این اولویت‌ها به طور هم‌زمان مقابله کنند که اغلب متناقض هستند و تنش ایجاد می‌کنند.

ژی جیان و همکاران (۲۰۲۰) بیان می‌کنند که حملات سایبری به کسب و کارها از سطح نوآوری شرکت‌ها می‌کاهد و هزینه‌های تحقیق و توسعه و سطح سرمایه‌گذاری در شرکت را کاهش می‌دهد و به طور کلی حملات سایبری بر تصمیمات راهبردی بنگاه اثرگذار است.

پانتلیف (۲۰۲۳) امنیت سایبری را به عنوان یک محرک برای رشد اقتصاد دیجیتال در نظر گرفته است. وی بیان کرده است که دستورالعمل‌های تضمین تاب آوری در برابر تهدیدات سایبری از جمله عواملی هستند که در تحریک توسعه کارآفرینی در اقتصادهای دیجیتال نقش دارند.

سعید و همکاران (۲۰۲۳) بیان کرده‌اند که هزینه‌های امنیت سایبری و جرائم سایبری در سطح جهانی روند رو به افزایشی را نشان می‌دهند و برخی مطالعات نشان‌دهنده این موضوع هستند که این هزینه توسط عوامل اقتصادی کمتر از حد برآورد می‌شوند. همچنین تحول دیجیتال بهره‌وری و کارایی را افزایش می‌دهد اما باعث چالش‌های امنیت سایبری بیشتری می‌شود. بنابراین با بهبود امنیت فضای کسب و کار در محیط اقتصاد دیجیتال در واقع به بهبود کارایی و بهره‌وری در محیط کسب و کار کمک می‌شود.

با مرور مطالعات فوق می‌توان عوامل اثرگذاری امنیت به صورت کلی در رشد اقتصادی و همچنین اثرگذاری اقتصاد دیجیتال در رشد اقتصادی را در مطالعات انجام شده داخلی و خارجی ملاحظه نمود. همچنین اثرگذاری امنیت سایبری بر فضای اقتصادی نیز در مطالعات مورد بررسی قرار گرفت. همچنین مشاهده می‌شود که در ادبیات موضوع با اینکه اثرگذاری امنیت سایبری در کشورهای پیشرفته یا اقتصادهای بزرگ بررسی شده است، اما در ایران این مطالعات انجام نپذیرفته و لازم است که اثر این مقوله مهم بر اقتصاد ایران و سایر کشورهای اسلامی در نظر گرفته شود. به دلیل اینکه با گذشت زمان سهم اقتصاد سایبری در اقتصاد کشورهای اسلامی نیز افزایش یافته و برخی از این کشورها نیز اکنون به دنبال مطرح کردن خود به عنوان مدعیان حوزه اقتصاد دیجیتال در سطح جهانی هستند. ایران نیز در سال‌های اخیر نگاه ویژه‌ای به اقتصاد دیجیتال و رشد زیرساخت و ... داشته است که این مهم را می‌توان در رشد سهم بازار گاه‌های دیجیتالی در اقتصاد ایران در سال‌های اخیر یافت. به همین دلیل امنیت سایبری بیش از پیش می‌تواند بر رشد اقتصادی ایران اثرگذار باشد. در همین راستا در ادامه پژوهش با توجه به مطالعاتی که انجام شده و بررسی‌شده‌اند، از مدل اقتصادسنجی پانل دیتا برای برآورد اثرگذاری امنیت سایبری بر ایران و کشورهای منتخب اسلامی که داده‌های آن‌ها موجود بود پرداخته می‌شود.

## روش‌شناسی

این پژوهش کاربردی بوده و اطلاعات آن به صورت کتابخانه‌ای جمع‌آوری شده است. داده‌های اقتصادی و جمعیت از پایگاه داده بانک جهانی[۱] و داده شاخص جهانی امنیت سایبری از اتحادیه بین‌المللی مخابرات گرفته شده است.

روش تحلیلی مقاله تحلیلی-علی بوده و از مدل اقتصاد سنجی پانل دیتا استفاده شده است. برای برآورد مدل از نسخه ۱۳ نرم افزار EViews استفاده شده است.

برای تخمین مدل پانل دیتا، بر اساس مطالعات صورت گرفته و مبانی نظری پژوهش، مدل برآوردی به صورت رابطه رگرسیونی ۶ مطرح است:

(۶)

$$L\log(GDP)_{it} = \beta_0 + \beta_1 Log(\mathrm{LF})_{it} + \beta_2 \mathrm{Log(KF)}_{it} + \beta_3 \mathrm{Log(GCI)}_{it} + \varepsilon_{it}$$

متغیرهای مدل:

$L\log(GDP)_{it}$: لگاریتم تولید ناخالص داخلی (به قیمت ثابت ۲۰۱۵) کشور i در سال t

$Log(\mathrm{LF})_{it}$: لگاریتم نیروی کار کشور i در سال t

$\mathrm{Log(KF)}_{it}$: لگاریتم تشکیل سرمایه (به قیمت ثابت سال ۲۰۱۵) کشور i در سال t

$\mathrm{Log(GCI)}_{it}$: لگاریتم شاخص جهانی امنیت سایبری کشور i در سال t

$\varepsilon_{it}$: جزء اخلال

برای برآورد مدل پانل دیتا ابتدا لازم است آزمون لیمر انجام شود تا تائید شود که داده‌ها ترکیبی بوده و استخری[۲] نمی‌باشند. پس از محاسبه، نتیجه آزمون F لیمر برای مدل، آماره برابر با ۱۱,۳۰ و احتمال برابر با ۰ دارد که نشان‌دهنده تائید ترکیبی (پانل) بودن داده‌های مورد استفاده است. همچنین برای تعیین تخمین مدل اثرات ثابت یا تصادفی از آزمون هاسمن استفاده می‌شود. فرضیه صفر این آزمون مبنی بر تصادفی بودن اثرات است. نتیجه آماره این آزمون برابر با ۳۳,۸۹ و احتمال برابر با ۰ می‌شود. نتیجه آزمون هاسمن نشان می‌دهد که فرض اثرات تصادفی رد شده و باید از مدل با اثرات ثابت استفاده کرد (اشرف زاده و مهرگان، ۱۳۹۵، صص ۴۰-۵۰).

---

۱ World Bank

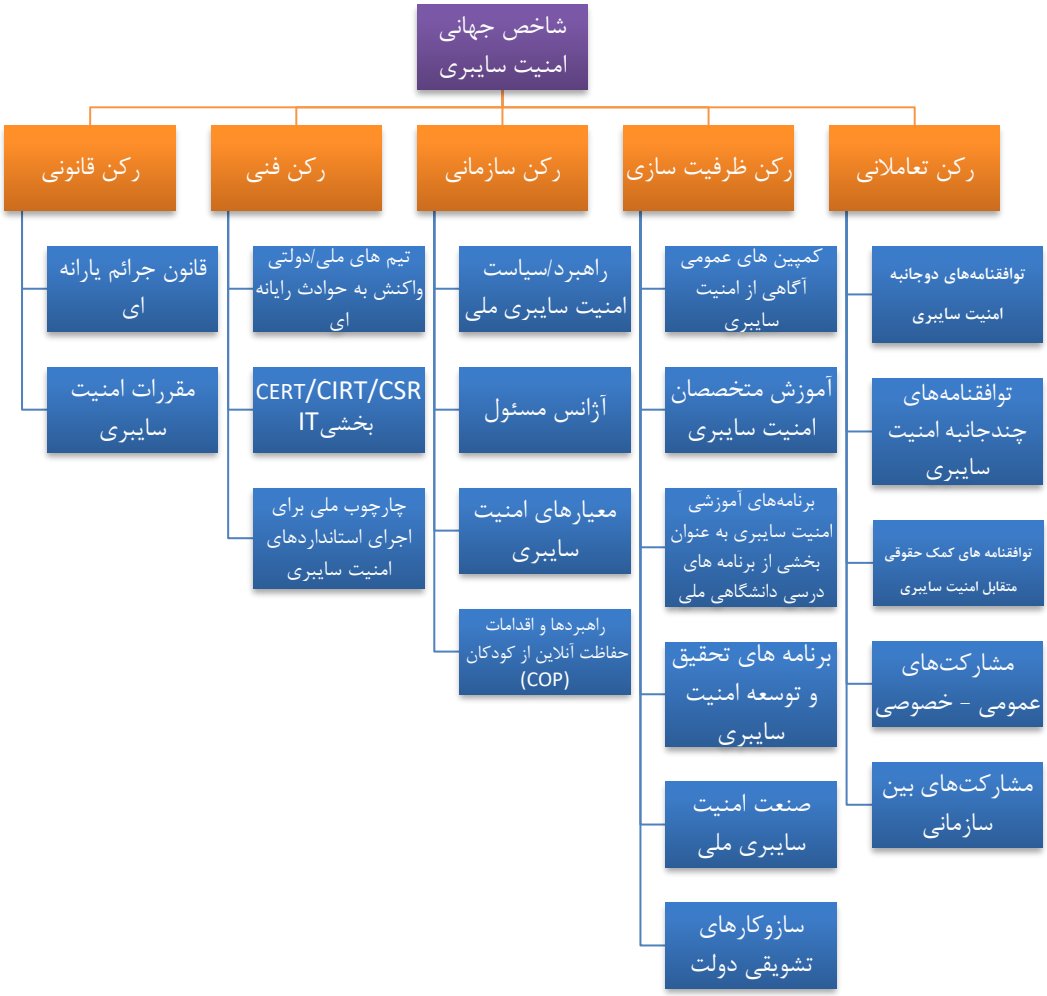
۲ Pool

بازه زمانی داده‌ها از سال ۲۰۱۲ الی ۲۰۲۲ به صورت سالانه و قلمرو مکانی پژوهش کشورهای اسلامی که داده‌های آن‌ها برای شاخص امنیت سایبری در دسترس بود شامل: ایران، عربستان سعودی، مصر، لیبی، تونس، الجزایر، سودان، عراق، کویت، قطر، بحرین، عمان، امارات متحده عربی، مغرب، لبنان و فلسطین (کرانه باختری و نوار غزه) است. داده شاخص جهانی امنیت سایبری تنها توسط اتحادیه جهانی مخابرات (ITU) درگزارش سال‌های ۲۰۱۴، ۲۰۱۷، ۲۰۱۸ و ۲۰۲۰ منتشر شده و در این پژوهش استفاده شده است.

## معرفی شاخص امنیت سایبری

گزارش شاخص جهانی امنیت سایبری(GCI[۱]) توسط اتحادیه جهانی مخابرات (ITU) تا به حال در ۴ دوره منتشر شده است. با توجه به گستردگی و شمول آن به تمامی کشورهای عضو سازمان ملل متحد می‌توان آن را یک شاخص بسیار مناسب برای ارزیابی امنیتی کشورها در فضای سایبری در نظر گرفت( مرادی، ۱۴۰۰). وضعیت امنیت سایبری یک کشور به عنوان یک پایه اساسی برای تسهیل پیشرفت اقتصاد دیجیتال عمل می‌کند. شاخص جهانی امنیت سایبری چارچوب برجسته‌ای را ارائه می‌کند که بلوغ و استحکام زیست بوم امنیت سایبری ملی را محک می‌زند.

۱ Global Cybersecurity Index




منبع: اتحادیه بین‌المللی مخابرات

**شکل ۲- ارکان و شاخص‌های شاخص جهانی امنیت سایبری بر اساس نسخه ۵ (۲۰۲۳)**

از آنجا که امکان جمع‌آوری مستقیم سرمایه‌گذاری در امنیت سایبری کشورهای مختلف برای پژوهشگران وجود ندارد، می‌توان از این شاخص که از ۰ الی ۱۰۰ کشورها را نمره‌دهی کرده است استفاده نمود. ایران در آخرین آمار منتشره اتحادیه بین‌المللی (جهانی) مخابرات، با کسب رتبه ۵۴ و امتیاز ۸۱، وضعیت نسبتاً خوبی در مقایسه با متوسط جهانی در حوزه امنیت سایبری دارد و همچنین،

امتیاز ایران و متوسط کشورهای اسلامی از متوسط جهانی بهتر است، هرچند که این کشورها همچنان با کشورهای توسعه‌یافته فاصله‌ای معنادار دارند. این اطلاعات نشان‌دهنده پیشرفت ایران در این حوزه است و نیاز به توجه بیشتر به امنیت سایبری را نمایان می‌سازد. جدول(۱) رتبه برخی کشورهای برتر این شاخص و کشور ایران را نشان می‌دهند.

**جدول ۱- امتیاز و رتبه‌بندی شاخص امنیت سایبری جهانی (GCI) در سال ۲۰۲۰**

| کشور | امتیاز | رتبه |
|---|---|---|
| **ایالات‌متحده آمریکا** | ۱۰۰ | ۱ |
| **بریتانیا** | ۹۹,۵۴ | ۲ |
| **عربستان سعودی** | ۹۹,۵۴ | |
| **استونی** | ۹۹,۴۸ | ۳ |
| **کره جنوبی** | ۹۸,۵۲ | ۴ |
| **سنگاپور** | ۹۸,۵۲ | |
| **اسپانیا** | ۹۸,۵۲ | |
| **روسیه** | ۹۸,۰۶ | ۵ |
| **امارات متحده عربی** | ۹۸,۰۶ | |
| **مالزی** | ۹۸,۰۶ | |
| **لیتوانی** | ۹۷,۹۳ | ۶ |
| **ژاپن** | ۹۷,۸۲ | ۷ |
| **کانادا** | ۹۷,۶۷ | ۸ |
| **فرانسه** | ۹۷,۶ | ۹ |
| **هند** | ۹۷,۵ | ۱۰ |
| ... | ... | ... |
| **بنگلادش** | ۸۱,۲۷ | ۵۲ |
| **گرجستان** | ۸۱,۰۷ | ۵۳ |
| **ایران** | ۸۱,۰۶ | ۵۴ |
| **متوسط کشورهای جهان** | ۵۳,۶۲ | مابین۸۵-۸۶ |
| **متوسط کشورهای اسلامی** | ۶۶,۹۳ | مابین ۷۷-۷۸ |

منبع: اتحادیه بین‌المللی مخابرات، گزارش ۲۰۲۰

شاخص جهانی امنیت سایبری بر پنج رکن زیر به عنوان حوزه‌های فراگیر تعهدات امنیت سایبری کشورها تمرکز دارد:

**رکن قانونی:**

اقدامات مبتنی بر وجود چارچوب‌های قانونی در ارتباط با امنیت سایبری و جرائم سایبری

-اقدامات قانونی: قوانین و مقررات مهار هرزنامه

-چارچوب قانونی: وجود قوانین کافی به منظور هماهنگی شیوه‌ها در سطح منطقه‌ای/بین‌المللی و ساده‌سازی مبارزه بین‌المللی با جرائم سایبری

**رکن فنی:**

اقدامات مبتنی بر وجود نهادهای فنی و چارچوبی که با امنیت سایبری سروکار دارند.

-توسعه و استفاده کارآمد از فناوری اطلاعات و ارتباطات. ایجاد و نصب معیارهای حداقل امنیتی مورد قبول و طرح‌های اعتباربخشی برای برنامه‌ها و سیستم‌های نرم‌افزاری

-وجود نهاد ملی رسیدگی به حوادث سایبری ( مشاهده، هشدار و واکنش به حوادث)

**رکن سازمانی:**

وجود نهادهای هماهنگ‌کننده، سیاست‌ها و راهبردهای توسعه امنیت سایبری در سطح ملی

- اقدامات سازمانی شامل شناسایی اهداف امنیت سایبری و برنامه‌های استراتژیک و تعریف رسمی نقش‌ها، مسئولیت‌ها و توانایی‌های سازمانی برای اطمینان از اجرای آن‌ها

-تعیین اهداف استراتژیک گسترده توسط دولت، همراه با یک برنامه همه جانبه در اجرا

-اجرای استراتژی و ارزیابی توسط آژانس‌های ملی

**رکن ظرفیت‌سازی:**

-تقویت ظرفیت از طریق اقدامات مبتنی بر تحقیق و توسعه، آموزش‌وپرورش، برنامه‌ها، متخصصان خبره و سازمان‌های بخش دولتی. ظرفیت‌سازی (شامل کمپین‌های آگاهی عمومی، تعیین چارچوب برای صدور گواهینامه و اعتبارسنجی متخصصان امنیت سایبری، دوره‌های آموزشی حرفه‌ای در حوزه امنیت سایبری، برنامه‌های آموزشی یا برنامه‌های درسی دانشگاهی) رکن ذاتی سه رکن اول (حقوقی، فنی و سازمانی) است.

-امنیت سایبری اغلب از منظر فناوری مورد بررسی قرار می‌گیرد، حتی اگر مسائل اجتماعی-اقتصادی و سیاسی متعددی وجود داشته باشد.

-مفاهیم ایجاد ظرفیت‌های انسانی و نهادی برای افزایش آگاهی و دانش در سراسر بخش‌ها، برای ارائه راه‌حل‌های سیستماتیک و مناسب، و ارتقای دانش متخصصان واجد شرایط ضروری است.

**رکن تعاملاتی:**

اقدامات مبتنی بر وجود مشارکت‌ها، چارچوب‌های تعاونی و شبکه‌های اشتراک‌گذاری اطلاعات

-با توجه به سطح بالای ارتباط متقابل بین کشورها، امنیت سایبری یک مسئولیت مشترک و یک چالش فراملی است. همکاری بیشتر می‌تواند امکان توسعه قابلیت‌های امنیت سایبری بسیار قوی‌تر را فراهم کرده، به کاهش خطرات سایبری کمک کند و تحقیقات، دستگیری و تعقیب بهتر عوامل مخرب را امکان‌پذیر سازد.

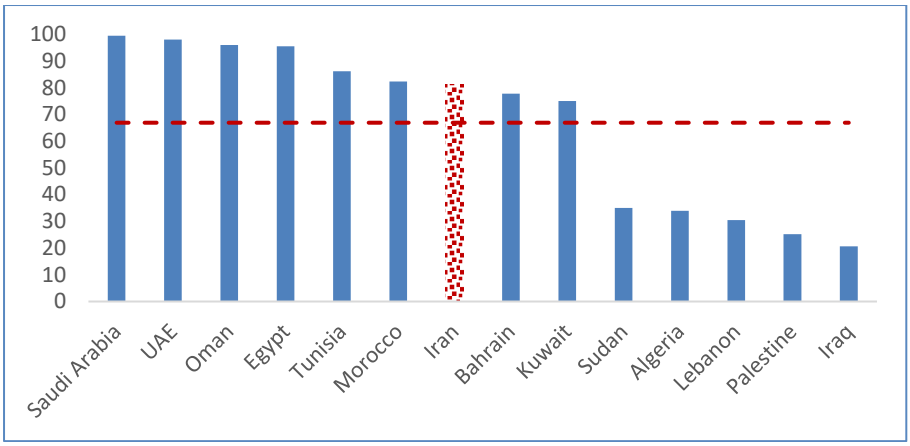
نمره ایران در آخرین گزارش منتشر شده در ارکان پنجگانه این شاخص به شرح جدول(۲) است.

**جدول ۲- امتیاز ایران در ارکان پنجگانه GCI**

| کشور | شاخص GCI | ارکان | | | | |
|---|---|---|---|---|---|---|
| | | قانونی | فنی | ظرفیت‌سازی | سازمانی | تعاملاتی |
| ایران | ۸۱/۰۶ | ۱۶/۴۸ | ۱۴/۶۳ | ۱۶/۸۲ | ۱۷/۸ | ۱۵/۳۳ |

منبع: اتحادیه بین‌المللی مخابرات

کسب نمرات GCI بالا، نشان‌دهنده سیاست‌های دقیق امنیت سایبری، چارچوب‌های قانونی، و سیستم‌های سازمانی، در کنار قابلیت‌های فن‌آوری دفاعی دقیق و مکانیسم‌های واکنش مشترک است. پایین‌ترین نمره ایران در بین این ارکان در سال ۲۰۲۰ رکن فنی است. این مسئله باید مورد توجه جدی سیاست‌گذاران قرار بگیرد. بالاترین نمره نیز متعلق به رکن سازمانی است. در شکل (۳) وضعیت ایران در بین کشورهای اسلامی که در این پژوهش استفاده‌شده‌اند از منظر شاخص جهانی امنیت سایبری بررسی شده است. خط نقطه‌چین نشان‌دهنده میانگین نمره این کشورها است.




**شکل ۳- وضعیت ایران و کشورهای مورد بررسی در شاخص جهانی امنیت سایبری ۲۰۲۰**

منبع: اتحادیه بین‌المللی مخابرات

ملاحظه می‌شود که ایران نسبت به برخی رقبای منطقه‌ای مانند عربستان، امارات، عمان و مصر (همچنین قطر که به دلیل نبود آمار مورد نیاز در این پژوهش حذف شده است) امتیاز پایین‌تری در شاخص جهانی امنیت سایبری دارد. نکته قابل ملاحظه‌ای که نشان می‌دهد کشورهایی که در سال‌های اخیر به‌سوی رشد اقتصادی خیز برداشته و برنامه جدی دارند، در این شاخص نیز امتیازات خوبی را کسب کرده‌اند.

## برآورد مدل

در روش داده‌های تلفیقی، برای تعیین حالت برابری عرض از مبـداء کشورهای مختلف با حالت تفاوت در عرض از مبداء کشورها از آزمون اف- لیمر[۱] ( چاو[۲]) و برای تعیین روش اثـر ثابـت[۳] و یـا اثر تصادفی[۴] از آزمون هاسمن[۵] استفاده می‌شود. در این تحقیق، نتایج آزمون اف- لیمرحاکی از رد فرضیه صفر به مفهوم عدم تخمین داده‌ها به صورت داده پول[۶] بوده است و همچنین، نتایج آزمون

۱ F-Limer test
۲ Chow
۳ Fixed effects
۴ Random effects
۵ Hasman test
۶ pool data

هاسمن نیز رد فرضیه صفر بوده است که نشان می‌دهد مدل نباید به صورت اثر تصادفی برآورد شود. لذا برای به دست آوردن اثر امنیت سایبری در طول زمان (دوره)[۱] مدل به صورت اثرات ثابت برآورد شده است. نتایج مدل برآوردی به صورت زیر است:

**جدول ۳- نتایج مدل پانل دیتا اثرات ثابت دوره**

| متغیر | ضریب | آماره t | احتمال |
|---|---|---|---|
| **عرض از مبدأ** | -۰,۲۷ | -۳,۰۷۹ | ۰,۰۰۳۴ |
| **log(lf)** | ۰,۲۶۶۹۲ | ۱,۸۰۱۷۳ | ۰,۰۷۷۹ |
| **log(kf)** | ۰,۰۰۸۳۵ | ۲,۱۳۳۱۲ | ۰,۰۳۸۱ |
| **log(gci)** | ۰,۰۱۹۳۹ | ۲,۹۲۴۴۷ | ۰,۰۰۵۳ |
| **Fixed effect(period)** | | | |
| **2014—C** | ۰,۰۳ | 2018—C | ۰,۰۱ |
| **2017—C** | ۰,۰۱ | 2020—C | -۰,۰۶ |
| **R^2** | ۰,۶۴ | R^2 adj | ۰,۵۹ |
| **F** | ۱۴,۰۲ | | ۰ |

منبع: یافته پژوهش

ضرایب به دست آمده از مدل برآوردی نشان می‌دهد متغیرهای تشکیل سرمایه ناخالص در سطح ۹۷ درصد و شاخص جهانی امنیت سایبری در سطح ۹۹ درصد و متغیر نیروی کار در سطح ۹۳ درصد معنی‌دار می‌باشند.

بر اساس یافته مدل برآورد شده، اثر نیروی کار، تشکیل سرمایه ناخالص و همچنین شاخص جهانی امنیت سایبری بر تولید ناخالص داخلی کشورهای اسلامی مثبت می‌باشد. توضیح دهندگی مدل ۶۰ درصد است که با توجه به ادبیات اقتصاد رشد این میزان از توضیح دهندگی برای مدل برآوردی رضایت‌بخش است. سایر شاخص‌ها نیز اعتبار مدل در کلیت خود را تائید می‌کند.

در بین متغیرهای اصلی منظور شده در مدل به عنوان متغیر مستقل، شاخص جهانی امنیت سایبری بیشترین معنی داری را در رشد اقتصادی کشورهای اسلامی داشته است. این نتیجه اهمیت این متغیر بر رشد اقتصادی آینده کشورها را نشان می‌دهد. همچنین این برآورد نشان می‌دهد که با افزایش یک درصدی در شاخص جهانی امنیت سایبری، رشد اقتصادی به میزان ۰,۰۱۹ درصد افزایش

۱ Period

خواهد یافت. به عبارت دیگر با توجه به اینکه میانگین شاخص امنیت سایبری برای کشورهای مورد برآورد منطقه ۶۶,۹۳ می‌باشد اگر این شاخص ده درصد رشد کند و به ۷۳,۶ برسد انتظار می‌رود رشد اقتصادی به میزان ۰,۱۹ درصد در کشورهای اسلامی که در این پژوهش بررسی شده است، افزایش یابد. بنظر می‌رسد این یافته با نتایج مطالعات انجام شده در این حوزه همچون مطالعه ژی جیان و همکاران (۲۰۲۰) در زمینه اثرات منفی حملات سایبری بر عملکرد بنگاه‌ها، مطالعه سعید و همکاران (۲۰۲۳) درخصوص تاثیر بهبود امنیت فضای کسب و کار بر افزایش کارایی و بهره‌وری در محیط کسب و کار، مطالعه پانتلیف(۲۰۲۳) درمورد اثرمثبت امنیت سایبری بر رشد اقتصاد دیجیتال، مطالعه کوهن و همکاران(۲۰۱۷) در خصوص نقش امنیت سایبری بر توسعه مناطق، مطالعه واسیو (۲۰۱۸) در مورد نقش امنیت سایبری در توسعه اقتصادی پایدار، مطالعه آرویابه و همکاران(۲۰۲۴) در خصوص نقش امنیت سایبری برعملکرد SMEها و مطالعه آشیش و همکاران(۲۰۲۴) در رابطه با تاثیر مثبت امنیت سایبری بر اقتصاد دیجیتال هماهنگ است. ذکر این نکته ضروری است که تقریباً در اکثر مطالعات انجام شده با توجه به عدم دسترسی به داده کمّی، مطالعات بصورت تحلیلی- توصیفی و مبتنی بر داده‌های کیفی انجام شده‌اند. حال آنکه در مطالعه حاضر روش‌شناسی تحقیق به صورت کمی مبتنی بر داده‌های کلان بین کشوری انجام شده است که به نوعی وجه تمایز مطالعه حاضر نسبت به مطالعات انجام شده در ادبیات موضوع می‌باشد.

همچنین ضریب نیروی کار نیز مثبت بوده که نشان‌دهنده رشد تولید ناخالص داخلی بر اثر رشد نیروی کار در کشورهای اسلامی می‌باشد. به ازای یک درصد افزایش در نیروی کار، تولید ناخالص داخلی در این کشورها برابر ۰,۲۶ درصد افزایش می‌یابد. ضریب سرمایه‌گذاری نیز مثبت است و ۱ درصد در رشد تشکیل سرمایه ناخالص باعث رشد ۰,۰۰۸ درصدی در تولید ناخالص داخلی کشورهای مورد بررسی است. این نتیجه نشان‌دهنده تأثیر کمتر تشکیل سرمایه در رشد اقتصادی کشورهای مورد بررسی نسبت به رشد نیروی کار در این کشورهاست و این مسئله تا حد زیادی با ساختار کشورهای اسلامی نیز سازگار است.

همچنین نتایج برآوردی نشان می‌دهد که علیرغم اینکه با پیشرفت فنّاوری انتظار می‌رود تأمین امنیت سایبری اهمیت بیشتری در رشد اقتصادی داشته باشد، اما در سال ۲۰۲۰ به دلیل شیوع بیماری کرونا و قرنطینه سراسری تولید ناخالص داخلی کشورهای مورد بررسی کاهش داشته است.
همچنین با توجه به هدف این پژوهش که بررسی اثرگذاری شاخص جهانی امنیت سایبری بر روی تولید ناخالص داخلی کشورهای اسلامی است، مدل با اثرات ثابت مقاطع هم برای عرض از مبدأ و هم برای شیب‌ها در نظر گرفته شد(اشرف زاده و مهرگان، ۱۳۹۵) تا اهداف مقاله تأمین شود و به تفکیک

کشورها اثرگذاری شاخص جهانی امنیت سایبری بر رشد اقتصادی مشخص شود. نتایج به صورت جدول (۴) می‌باشد:

**جدول۴- نتایج مدل با اثرات ثابت مقطع**

| متغیر | ضریب | آماره t | احتمال |
|---|---|---|---|
| C | ۱۳,۷۷۱ | ۱۴,۸۹۷۸ | ۰ |
| LOG(LF?) | ۰,۴۴۸۲۱ | ۷,۰۴۲۴۵ | ۰ |
| LOG(KF?) | ۰,۱۹۱ | ۱۳,۳۴۷۷ | ۰ |
| (GCI_SAU) | ۰,۰۲۳۹ | ۰,۴۸۳۹۷ | ۰,۶۳۲۶ |
| (GCI_UAE) | ۰,۰۷۴۷۶ | ۲,۵۷۳۳۳ | ۰,۰۱۶۴ |
| (GCI_OMAN) | ۰,۰۹۵۷۳ | ۰,۹۱۹۸ | ۰,۳۶۶۵ |
| (GCI_EGY) | ۰,۴۳۶۶۷ | ۴,۲۵۴۸۱ | ۰,۰۰۰۳ |
| (GCI_TUN) | ۰,۱۴۳۴۶ | ۲,۵۷۳۳۳ | ۰,۰۱۹۳ |
| (GCI_MOR) | -۰,۰۷۹ | -۰,۰۷۸۷ | ۰,۹۳۷۹ |
| (GCI_IRN) | ۰,۰۵۵۴۶ | ۱,۵۰۵۷۷ | ۰,۱۴۴۷ |
| (GCI_BAH) | ۰,۰۰۹۵۱ | ۰,۸۲۱۱۸ | ۰,۴۱۹۳ |
| (GCI_KUW) | -۰,۰۴۰۶ | -۱,۳۳۸۱ | ۰,۱۹۲۹ |
| (GCI_SUD) | ۰,۵۰۶۵ | -۸,۲۲۸۲ | ۰ |
| (GCI_ALG) | ۰,۰۳۶۴۳ | ۱,۴۳۵۶۵ | ۰,۱۶۳۵ |
| (GCI_LBN) | ۰,۰۱۱۷۹ | ۰,۶۰۲۲۴ | ۰,۵۵۲۴ |
| (GCI_PLS) | ۰,۰۱۳۶۸ | ۰,۲۲۳۳۲ | ۰,۸۲۵۱ |
| (GCI_IRQ) | ۰,۰۲۵۹۴ | ۰,۷۴۳۲ | ۰,۴۶۴۳ |
| | **Fixed Effects (Cross)** | | |
| SAU—C | ۱,۰۲۰۴۳ | BAH—C | -۰,۰۹۷۳ |
| UAE—C | ۰,۷۴۷۵۲ | KUW—C | ۰,۶۱۷۶۱ |
| OMAN—C | -۰,۲۵۵ | SUD—C | ۱,۵۴۴۳۱ |
| EGY—C | -۱,۴۹۴۷ | ALG—C | -۰,۱۴۶۳ |
| TUN—C | -۱,۰۱۲۷ | LBN—C | -۰,۱۳۴۷ |
| MOR—C | -۰,۲۱۳۲ | PLS—C | -۰,۸۶۸۹ |
| IRN—C | -۰,۱۸۹۳۷ | IRQ—C | ۰,۲۵۸۰۸ |
| Adjusted R-squared | -۰,۹۹۹۶۱ | R^2 | ۰,۹۹ |

منبع: یافته‌های پژوهش

نتایج نشان می‌دهد که مدل از اعتبار لازم برخوردار است و با در نظر گرفتن ناهمگنی کشورها توضیح دهی مدل به‌طور قابل‌ملاحظه‌ای افزایش یافته است.

در این مدل همانند سایر مطالعات تجربی و مباحث نظری سهم نیروی کار نسبت به سرمایه در رشد اقتصادی بیشتر است و اثر هر دوی این متغیرها بر رشد اقتصادی به‌طور قریب به یقین مثبت است.

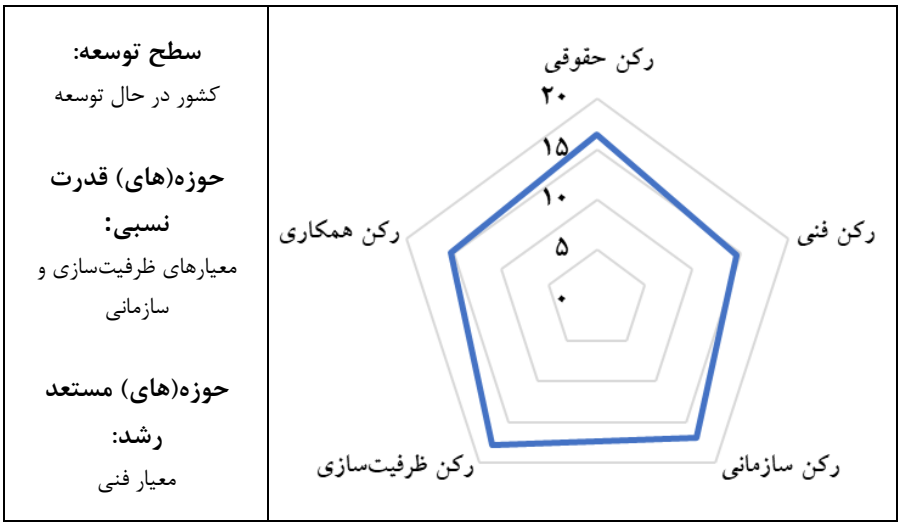
به منظور شناسایی میزان اثرگذاری شاخص جهانی امنیت سایبری بر رشد اقتصادی هر کشور به‌طور جداگانه ناهمگنی شیب‌ها در مدل پانل دیتا مورد استفاده قرار گرفت. نتایج مدل نشان‌دهنده این است که شیب اثرگذاری شاخص جهانی امنیت سایبری در کشورهای اسلامی با یکدیگر متفاوت است. در عین حال این مدل نشان می‌دهد که در برخی از این کشورها GCI اثر معنی داری بر تولید ناخالص داخلی ندارد و در کشورهایی که اثرگذاری این شاخص معنی دار است اثرات متفاوت بوده و در برخی کشورها مثبت و در برخی کشورها منفی است. GCI در کشورهای امارات، مصر، تونس اثر معنی دار و مثبتی روی تولید ناخالص داخلی دارد. در کشور سودان نیز اثر معنی دار اما منفی بر تولید ناخالص داخلی داشته است.

اثرگذاری GCI در ایران مثبت بوده و در سطح ۸۶ درصد قابل اتکا و معنی دار است، با توجه به رتبه نه چندان مطلوب ایران در این شاخص (۵۴)، در کشور از ظرفیت سرمایه‌گذاری در ساختار امنیت سایبری چندان بهره گرفته نشده است و با تمرکز و توجه بیشتر بر بهبود موارد این شاخص می‌توان امید داشت که اثرگذاری امنیت فضای سایبری نیز منجر به اثرگذاری مثبت در تولید ناخالص داخلی و نهایتاً رشد اقتصادی کشور شود.

برآورد اثر GCI بر رشد اقتصادی ایران نشان می‌دهد که با افزایش یک درصدی در شاخص امنیت سایبری رشد اقتصادی به میزان ۰،۰۵۵ درصد افزایش خواهد یافت. به عبارت دیگر با توجه به اینکه نمره شاخص امنیت سایبری برای ایران ۸۱ است. اگر این شاخص ده درصد رشد کند و به ۹۰ برسد انتظار می‌رود رشد اقتصادی به میزان ۰،۵۵ درصد افزایش یابد. هرچند این میزان در نگاه اول ممکن است ناچیز به نظر برسد اما باید در نظر گرفت که اولاً هزینه ده درصد افزایش نمره در شاخص جهانی امنیت سایبری چندان بالا نیست و کاملاً دست‌یافتنی است، ثانیاً با افزایش امنیت سایبری به رشد و شکوفایی اقتصاد دیجیتال کمک کرده و بهبود فضای کسب و کار در این حوزه را شاهد خواهیم بود و همانطور که در ادبیات نیز ملاحظه شد، امنیت یکی از عوامل جذب سرمایه و عدم وجود آن از مهم‌ترین عوامل فرار سرمایه است. همچنین در ماده ۶۶ برنامه هفتم توسعه کشور به عنوان یک سند بالادستی صراحتاً ذکرشده است که سهم اقتصاد رقومی (دیجیتال) از تولید ناخالص ملی باید افزایش یابد. مسلماً برای دستیابی به این هدف نیاز است زیرساخت‌های مناسب آن نیز در

نظر گرفته شود، امنیت یکی از مهم‌ترین زیرساخت‌های یک بخش اقتصادی خواهد بود و نقش مهمی ایفا می‌کند و به همین دلیل باید توجه ویژه‌ای به این مسئله داشت.

بند ب ماده ۱۰۷ برنامه هفتم توسعه نیز بیان می‌دارد که "سازمان اداری و استخدامی کشور مکلف است با همکاری سایر دستگاه‌های اجرائی از محل تجمیع مأموریت، ساختار و نیروی انسانی واحدهای فناوری اطلاعات و امنیت فضای مجازی، مرکز نو سازی و تحول اداری، مراکز تحقیق و توسعه و عناوین مشابه، نسبت به ایجاد معاونت یا مرکز یا سازمان «نوآوری، هوشمند سازی و امنیت» متناسب با مأموریت هر یک از دستگاه‌های اجرائی کشور تا پایان سال اول برنامه اقدام نماید." با توجه به این بند می‌توان انتظار داشت که ایران در شاخص جهانی امنیت سایبری بتواند امتیاز بهتر و بالاتری در سال‌های آینده کسب کند و در صورت طراحی و اجرای مناسب این بند در اجرا اثرگذاری انتظاری آن بر امنیت سایبری مثبت می‌باشد.




منبع: اتحادیه جهانی مخابرات (۲۰۲۰)

**شکل ۴- وضعیت ایران در ارکان ۵گانه شاخص جهانی امنیت سایبری**

با توجه به امتیازات ایران در ارکان پنجگانه شاخص جهانی امنیت سایبری ملاحظه می‌شود که ضعف اساسی ایران در معیارهای همکاری و فنی می‌باشد. ایران نسبت به رقبای منطقه مانند عربستان، امارات متحده عربی، عمان مصر، قطر و حتی ترکیه از نمره پایین‌تری در این شاخص برخوردار است.

به همین دلیل می‌توان گفت کشور به جایگاهی که شایسته آن است نرسیده و از ظرفیت‌های بالقوه موجود در این فضا بی‌بهره مانده است. با توجه به اینکه مهم‌ترین ضعف ایران در قسمت معیار فنی و همکاری است، از جمله دلایلی که می‌توان برای ضعف فنی امنیت سایبری در کشور بر شمرد، یکی دسترسی مشکل به سخت افزارهای امنیتی و دیگری نبود نیروی متخصص کافی در این حوزه در کشور است. باید توجه داشت مهاجرت نخبگان در صنعت تکنولوژی در ایران بعضاً به کشورهای رقیب منطقه‌ای انجام می‌شود و از این طریق علاوه بر اینکه کشور از وجود این متخصصین بی بهره می‌شود، کشورهای رقیب با استفاده از همین متخصصین قدمی بزرگ‌تر به سوی پیشرفت بر می‌دارند.

همچنین عدم وجود قوانین اساسی حفاظت اطلاعات در برابر کلاهبرداران و شرکتها، عدم همکاری شرکت‌های بزرگ بین‌المللی با کشور و نبود نمایندگی آنها درون کشور، باعث می‌شود از نظر قانونی نیز دست ایران برای همکاری با شرکتهای بزرگ و کشورهای دیگر در فضای وب و دفاع از حقوق مردم کشور در برابر تهدیدات سایبری بسته باشد. بهبود در این شاخصه و همچنین توافقات دوجانبه و چند جانبه، همچنین مشارکت بیشتر بخش خصوصی به بهبود رکن معیار تعاملاتی نیز کمک می‌کند.

اگرچه رتبه و امتیاز ایران در دو رکن دیگر، یعنی ظرفیت‌سازی و سازمانی نسبتاً قابل قبول است، لیکن همچنان جای رشد دارد. سرمایه‌گذاری در بخش امنیت فضای سایبری و ارتقای سواد فضای مجازی عموم مردم به خصوص حفاظت از کودکان در برابر تهدیدهای آنلاین از طریق اینترنت، برنامه‌های تلویزیونی و رسانه‌های اجتماعی در این دو رکن پیشنهاد می‌شود.

نتایج مطالعه حاضر یک یافته کلیدی به همراه دارد و آن اینکه هر چند در ادبیات موضوع مطالعات مختلفی اثر معنادار توسعه زیرساخت‌های فناوری اطلاعات و ارتباطات بر رشد اقتصادی را تایید نموده‌اند و عملاً نوعی اجماع در این خصوص وجود دارد. نتایج مطالعه حاضر تکمله‌ای را به این گزاره اضافه می‌نماید مبنی بر اینکه مقوله امنیت سایبری می‌تواند بصورت مضاعف تحریک‌کننده رشد اقتصادی باشد. لذا می‌توان اینگونه مطرح نمود که چنانچه توسعه زیرساخت‌های فناوری اطلاعات و ارتباطات را یکی از شروط لازم برای رشد اقتصادی بدانیم. ایجاد و گسترش مقوله امنیت سایبری می‌تواند شرط کافی در این حوزه به حساب آید.

## بحث پایانی و جمع‌بندی

با گسترش فناوری‌های دیجیتال در بخش‌های اقتصادی، تهدیدات فضای سایبری خطر بیشتری برای تداوم کسب و کار، عملیات زیرساخت‌های حیاتی و امنیت ملی ایجاد می‌کند. با این حال، بسیاری از کشورها فاقد چارچوب‌های قانونی، کنترل‌های فنی، و هماهنگی نهادی برای مقابله مناسب با حملات

سایبری پیچیده هستند. این شکاف دیجیتالی-امنیتی تهدیدی برای تضعیف رقابت اقتصادی و رشد در اقتصاد داده محور در حال ظهور است. از این رو، مداخلات سیاستی برای تقویت سیستماتیک اکوسیستم‌های امنیت سایبری ملی یک ضرورت فوری است.

مجمع جهانی اقتصاد تخمین می‌زند که «تقریباً یک‌میلیون نفر برای اولین بار هر روز آنلاین می‌شوند و دو سوم جمعیت جهان صاحب یک دستگاه تلفن همراه هستند.» در حالی که مزیت فناوری دیجیتال منافع اقتصادی و اجتماعی بسیار زیادی را به همراه دارد، خطرات سایبری می‌تواند مزایای دیجیتالی سازی را خنثی کند. ایمن سازی حوزه سایبری از طریق فعالیت‌های ظرفیت سازی امنیت سایبری کلیدی است زیرا به کاهش مسائلی مانند شکاف دیجیتال و خطرات سایبری کمک می‌کند[۱].

امنیت سایبری به مانند بسیاری از تحولات دیجیتال به تازگی اهمیت خود را در اقتصاد نشان داده است و داده‌های زیادی از آن در دسترس نیست. به همین دلیل نیز برآورد اثرگذاری دقیق این شاخص بر روی اقتصادهای مختلف مشکل است. همان‌طور که در این پژوهش نیز ملاحظه شد به طور کلی و با یک دیدگاه بین کشوری، سرمایه‌گذاری در امنیت سایبری می‌تواند با بهبود فضای کسب و کار به طور معنی داری بر روی تولید ناخالص داخلی کشورهای اسلامی اثرگذار باشد.

همچنین باید در نظر داشت که پیگیری تعاملات بین‌المللی می‌تواند به ارکان فنی، حقوقی و همکاری کمک کند، در این راستا پیشنهاد می‌شود وزارت امور خارجه یکی از خط مشی‌های دیپلماسی خود با کشورهای مورد ارتباط را در راستای بهبود تعاملات در راستای بهبود شاخصه‌های امنیت فناوری اطلاعات کشور بگذارد. تلاش در راستای رفع تحریم‌ها علیه کشور نیز می‌تواند به بهبود این ارکان به خصوص شاخصه فنی کمک کند.

از سوی دیگر با در نظر گرفتن ناهمگونی فضای بین کشورها ملاحظه شد تنها سه کشور امارات متحده عربی، مصر و تونس اثر مثبت و معناداری از این شاخص بر روی تولید ناخالص داخلی خود دریافت کردند. البته با سرمایه‌گذاری در زیرساخت‌های فناوری اطلاعات و ارتباطات و افزایش ضریب نفوذ این فناوری (بعنوان شرط لازم)، توجه به مقوله امنیت این حوزه (به عنوان شرط کافی) ضروری و اجتناب ناپذیر می‌باشد. ایران نیز می‌تواند با بهبود نقاط ضعف خود، اثرگذاری این شاخص را به گونه بهتری بر روی تولید کشور ملاحظه نماید. برای مطالعات آتی پیشنهاد می‌شود با انتشار جداول داده و ستانده جدید، سهم سرمایه‌گذاری‌های امنیت در فضای سایبری در اقتصاد با استفاده از تحلیل‌های داده ستانده مورد بررسی قرار بگیرد.

---

۱ Global Cybersecurity Index 2020, available at:
https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

**منابع**


۱. اخلاقی، رحمت‌الله (۱۳۹۸). شناسایی تأثیر متقابل امنیت، رشد و توسعه اقتصادی در اسلام، *دو فصلنامه معارف اسلامی و اقتصاد*، ۵(۱)، ۱-۳۷.

۲. اسعدی، مرضیه. (۱۳۹۸). انقلاب صنعتی چهارم و اقتصاد دیجیتال: پیشران‌های رشد اقتصادی پایدار. *نشریه مطالعات کاربردی در علوم مدیریت و توسعه*، ۴(۱۷).

۳. اسماعیل نیا, علی‌اصغر؛ وصفی‌اسفستانی, شهرام. (۱۳۹۵). تأثیر امنیت بر رشد اقتصادی در ایران و برخی کشورهای منتخب .پژوهشنامه اقتصادی ۱۶(۶۱)، ۱۵۴-۱۲۷.

۴. اشرف زاده، سید حمیدرضا؛ مهرگان، نادر (۱۳۹۲). *اقتصادسنجی پانل دیتا*، موسسه تحقیقات تعاون دانشگاه تهران، چاپ سوم، تهران.

۵. مرکز پژوهش‌های مجلس جمهوری اسلامی ایران، لایحه برنامه هفتم توسعه جمهوری اسلامی ایران،https://rc.majlis.ir/fa/news/show/1776775

۶. جعفری صمیمی، احمد؛ اختیاری، شهرام (۱۳۸۷). تأثیر امنیت اقتصادی بر فرآیند رشد اقتصادی در کشورهای عضو کنفرانس اسلامی با تأکید بر ایران، *فصلنامه اقتصاد مالی*، ۳(۲)، ۹۱-۷۰.

**۷.** خیاط رسولی، مینا؛ آل عمران، رؤیا؛ مهرگان، نادر ، محمد زاده، پرویز (۱۳۹۹). تأثیر کیفیت نهادی دولت و نوع سیستم‌های مالی روی رشد اقتصادی کشورهای منتخب اسلامی، *مجله اقتصاد و بانکداری اسلامی*، ۹(۳۳).

۸. صامتی، مجید؛ شهنازی، روح اله؛ دهقان شبانی، زهرا. (۱۳۸۹). امنیت حقوق مالکیت، قوانین و مقررات و رشد اقتصادی .*پژوهش‌های اقتصادی ایران*۱۵(۴۴)، ۸۵-۱۰۹.

۹. مرادحاصل، نیلوفر؛ محبی خواه، بیتا؛ تقی پور، زهرا (۱۴۰۰)، اقتصاد دیجیتال جلد اول، تالیف: دان تپ اسکات، پژوهشکده آمار، تهران، ایران.

۱۰. مرادحاصل، نیلوفر؛ میرسعید، کاظم پور (۱۴۰۱)، واکاوی تأثیر توسعه زیرساخت‌های شبکه حمل و نقل ریلی و فناوری اطلاعات و ارتباطات بر رشد اقتصادی کشورهای منتخب با استفاده از رهیافت GLS، نوزدهمین کنفرانس بین‌المللی مهندسی حمل و نقل و ترافیک، تهران، ایران.

۱۱. مرادی، علیرضا؛ شکری، نعیم؛ عظیم زاده ،نجمه (۱۴۰۰). دانشنامه شاخص‌های بین‌المللی (۱۰۱ شاخص)، تهران: نشر نور علم.

۱۲. مهرگان، نادر ، سحابی، بهرام ، محمدامینی، مریم (۱۳۹۴) تأثیر شاخص توسعه فناوری اطلاعات و ارتباطات ( (IDIبر فساد اداری در کشورها با درآمد متوسط، *فصلنامه نظریه‌های کاربردی اقتصاد*، ۲(۲). صص ۴۳-۶۰.

۱۳. یاوری، کاظم، مهرگان، نادر (۱۳۸۰) بهره‌وری سرمایه تأمین شده از خارج و تولید داخلی در اقتصاد ایران، *فصلنامه مفید*، شماره۲۷.

14. Aleksandrova, A., Truntsevsky, Y., & Polutova, M., (2022). Digitalization and its impact on economic growth. *Brazilian Journal of Political Economy*, *42*, 424-441.
15. Arroyabe, M. F., Arranz, C. F. A.& Arroyabe, I. F. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK, *Technology in Society, Volume 78,PP: 102-670.* https://doi.org/10.1016/j.techsoc.2024.102670
16. Ashish, J., Shankha, S & Surajit, M., (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges, *Journal of Technology Innovations and Energ*, https://doi.org/10.56556/jtie.v3i2.907
17. Barefoot, K., Curtis, D., Jolliff W., Nicholson JR., & Omohundro, R., (2018). Defining and measuring the digital economy. *Working paper. Bureau of Economic Analysis, United States Department of Commerce, Washington, DC*. Available at: https://www.bea.gov/system/files/papers/WP2018-4.pdf.
18. Chohan, Usman W., (2020). Some Precepts of the Digital Economy. *Critical Blockchain Research Initiative (CBRI) Working Papers, 2020*, Available at SSRN: https://ssrn.com/abstract=3512353 or http://dx.doi.org/10.2139/ssrn.3512353
19. Cohen, N., Hulvey, R., Mongkolnchaiarunya, J., Novak, A., Morgus, R., & Segal, A.,(2017). Cybersecurity as an engine for growth, *New America's Cybersecurity Initiative*. https://d1y8sb8igg2f8e.cloudfront.net/documents/FINAL_Clusters.pdf
20. Chris Zhijian He, Tracie Frost, Robert E. Pinsker (2020) ; The Impact of Reported Cybersecurity Breaches on Firm Innovation. *Journal of Information Systems* 1 June 2020; 34 (2): 187–209. https://doi.org/10.2308/isys-18-053
21. Cremer, F and others,(2022). Cyber risk and cybersecurity: a systematic review of data availability, *Geneva Pap Risk Insur Issues Pract*. 2022; 47(3): 698–736. DOI: 10.1057/s41288-022-00266-6

22. Datta, A., & Agarwal, S. (2004). Telecommunications and economic growth: a panel data approach. *Applied Economics*, *36*(15), 1649-1654.
23. Eling, M., Elvedi, M., & Falco, G. (2023). The economic impact of extreme cyber risk scenarios. *North American Actuarial Journal*, *27*(3), 429-443.
24. Global Cybersecurity Index 2020, available at: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
25. Gomes, S., Lopes, J. M., & Ferreira, L. (2022). The impact of the digital economy on economic growth: The case of OECD countries. *RAM. Revista de Administração Mackenzie*, *23*, eRAMD220029.
26. Jiao, S., & Sun, Q. (2021). Digital economic development and its impact on econimic growth in China: Research based on the prespective of sustainability. *Sustainability*, *13*(18), 10245.
27. Lynn., T. G. and others (2022). The Digital Economy and Digital Business, *In book: Digital Towns, Accelerating and Measuring the Digital Transformation of Rural Societies and Economies, February 2022*, DOI: 10.1007/978-3-030-91247-5_4
28. Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer fraud & security*, *2020*(2), 14-17.
29. Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3-4), 103-117.
30. Nelson, Natasha and Stuart Manick (2017) . "Studying the Tension Between Digital Innovation and Cybersecurity." 3rd International Conference on Information Systems Security and Privacy (SIGSEC), 19-21 February, 2017, Porto,
31. Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information & Computer Security*, *32*(1), 38-52.
32. Panteleev, D. N. (2023). Cybersecurity for the Stimulation of Entrepreneurship Development in the Digital Economy Markets. In *Anti-Crisis Approach to the Provision of the Environmental Sustainability of Economy* (pp. 263-271). Singapore: Springer Nature Singapore.
33. Poirson Ward, H. (1998). *Economic Security, Private Investment, and Growth in Developing Countries* (No. 98/4). International Monetary Fund.
34. Saeed, Saqib, Salha A. Altamimi, Norah A. Alkayyal, Ebtisam Alshehri, and Dina A. Alabbad. (2023) . "Digital Transformation and Cybersecurity

Challenges for Businesses Resilience: Issues and Recommendations" *Sensors* 23, no. 15: 6666. https://doi.org/10.3390/s23156666

35. Vasiu, L.,(2018). Cybersecurity as an Essential Sustainable Economic Development Factor, *European Journal of Sustainable Development, 7, 4, 171-178.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3262527
36. Vijayan, A., (2019). Digital India-A roadmap to sustainability. *International Journal of Innovative Technology and Exploring Engineering*, *8*(5), 571-576.