زاویه

نگاهی نو؛
به حکمرانی فضای مجازی

IDEBAN دیده‌بان

# شاخص قدرت سایبری ملی ۲۰۲۲

مرکز بلفر دانشگاه هاروارد

مرکز بلفر دانشگاه هاروارد

# شاخص قدرت سایبری ملی ۲۰۲۲


| | |
|---|---|
| نویسندگان | Julia Voo, Irfan Hemani, Daniel Cassidy |
| مترجمان | گروه دیده‌بان و زاویه |
| ناظر ترجمه | علی زرودی |

| | |
|---|---|
| تاریخ تنظیم | خرداد ۱۴۰۲ |
| تعدادکلمات | ۱۴۳۰۰ |
| کلیدواژه‌ها | قدرت سایبری، سنجش و اندازه‌گیری، ساخت شاخص ترکیبی، سیاست‌گذاری فضای مجازی |

# پیشگفتار

«قدرت» از مفاهیم بنیادی علوم انسانی است که از دیرباز مورد توجه اندیشمندان بوده؛ اما مانند سایر مفاهیم، بر سر تعریف آن اختلاف نظر وجود دارد. درواقع در مورد مفهوم قدرت نیز مانند مفاهیم فرهنگ، سرمایه اجتماعی، امنیت و... چالش مفهومی و برداشت‌های مختلف وجود دارد. موضوع، زمانی پیچیده‌تر می‌شود که سایر مفاهیم به مفهوم قدرت اضافه شده و ترکیب‌هایی همچون «قدرت سیاسی»، «قدرت اقتصادی»، «قدرت سایبری» و... به وجود بیایند.

از میان ترکیب‌های ذکر شده، «قدرت سایبری» پیچیدگی و سیالیت بیشتری دارد؛ چراکه در پنج دهه گذشته، فضای سایبری دائماً در حال تطور بوده و اِجماعی بر چیستی آن حاصل نشده است. بنابراین اولین اهمیت نگارش یا ترجمه متون در زمینه قدرت سایبری، تلاش برای حرکت از تکثر معنا به سمت وحدت بیشتر و از انتزاع به عینیت بیشتر درخصوص مفهوم قدرت سایبری است تا کیفیت سیاست‌گذاری و تصمیم‌گیری در این حوزه را افزایش دهد.

«قدرت سایبری» مفهومی است که در حوزه علمی و مدیریتی کشور مهجور واقع شده است. شهریور ۱۳۹۴ رهبر معظم انقلاب در بند سوم از حکم اعضای دومین دوره شورای عالی فضای مجازی، به «ارتقای جمهوری اسلامی ایران به قدرت سایبری در طراز قدرت‌های تأثیرگذار جهانی»[۱] تصریح فرموده است. پس از آن نیز در

۱) https://farsi.khamenei.ir/message-content?id=30658

مواردی در جلسات خصوصی و عمومی درمورد قدرت سایبری نکاتی از جانب ایشان مطرح شده است[۱] اما متأسفانه مورد غفلت بدنه برنامه‌ریزی و اجرایی کشور واقع شده است. در نهاد علم نیز معدود مقالاتی به این مفهوم پرداخته‌اند که همان‌ها نیز رویکرد نظامی داشته‌اند؛ درحالی‌که این حوزه نیازمند رویکردی جامع (اقتصادی، امنیتی، فرهنگی و...) است.

به فرض اهتمام و عدم انفعال دولت در این خصوص[۲]، برنامه‌ریزی، سرمایه‌گذاری و سایر انواع مداخلات دولتی نیازمند شاخص‌گذاری است؛ زیرا بدون وجود شاخص‌ها و نشانگرها[۳] امکان ارزیابی و سنجش برنامه‌ها و تصمیم‌های دولتی ممکن نیست. شاخص‌ها امکان بررسی‌های هم‌زمانی و درزمانی را فراهم می‌کنند. منظور از بررسی هم‌زمانی، مقایسه وضعیت کشورهای مختلف در یک مقطع زمانی است و منظور از بررسی درزمانی این است که اندازه‌گیری یک شاخص در طول زمان و مقاطع زمانی مختلف، کمک می‌کند تا مسیر طی شده توسط کشورها (صعود یا تنزل) در شرایط مختلف و در بازه‌های زمانی تحلیل شود.

مطابق گزارش «شاخص قدرت سایبری ملی ۲۰۲۲» مرکز بلفر، قدرت سایبری شامل هشت هدف در نظر گرفته شده که عبارتند از:

۱. نظارت و پایش در سطح داخل کشور؛
۲. تقویت دفاع سایبری ملی؛
۳. کنترل و دستکاری محیط اطلاعاتی (افکار عمومی در سطح داخل و خارج)؛
۴. جاسوسی در سطح خارج کشور؛
۵. رشد شایستگی در حوزه فناوری تجاری و سایبری در سطح ملی؛
۶. تخریب یا ازکارانداختن زیرساخت و قابلیت‌های دشمن؛
۷. مشارکت در تعیین هنجارهای سایبری و استانداردهای فنی بین‌المللی؛
۸. انباشت ثروت و/یا استخراج رمزارز.

در این گزارش وضعیت ۳۰ کشور در این شاخص و در هر یک از اهداف هشت‌گانه بالا ترسیم شده است. طبق گزارش تیم بلفر، ایران حائز رتبه دهم در میان قدرت‌های سایبری است.

با توجه به صبغه مرکز بلفر، این احتمال وجود دارد که اهدافی پشت پرده انتشار این گزارش وجود داشته باشد؛ به ویژه اینکه در متن اصلی گزارش در مواردی گزاره‌های نادرستی در خصوص ایران مطرح شده است[۴]؛ اما با این حال، به‌دلیل ضرورت‌هایی که پیش‌از این ذکر شد و همچنین ویژگی‌های برجسته گزارش مرکز

---

۱) آخرین مورد در بند ۱۹ سیاست‌های کلی برنامه هفتم است.

۲) به نظر می‌رسد با توجه به سیاست‌های کلی برنامه هفتم و بند دوم پیش‌نویس سیاست‌های کلی فضای مجازی مبنی بر ارتقای طراز قدرت سایبری، لازم است که در برنامه هفتم توسعه کشور ابعاد مختلف قدرت سایبری مورد اهتمام جدی واقع شود.

۳) Indicators

۴) این موارد بنا به صلاح دید مجموعه از متن ترجمه حذف شدند.

بلفر (که می‌توان از آن‌ها در طراحی بومی شاخص قدرت سایبری ملی استفاده کرد) این گزارش ترجمه شده است.

از ویژگی‌های گزارش «شاخص قدرت سایبری ملی ۲۰۲۲» مرکز بلفر این است که تلاش کرده رویکردی جامع به قدرت سایبری داشته باشد؛ هرچند که هنوز وجوه نظامی و امنیتی برجسته است. این گزارش به جنبه‌های اقتصادی و رسانه‌ای (دستکاری افکار عمومی و کنترل محیط اطلاعاتی) قدرت سایبری پرداخته، اما هنوز جای خالی وجوه دیگر قدرت سایبری (به ویژه وجوه فرهنگی) محسوس است که باید در طراحی بومی شاخص قدرت سایبری ملی به این موضوع توجه شود.

ویژگی دیگر این گزارش، ارائه جداول نشانگرها است که می‌تواند در طراحی بومی شاخص قدرت سایبری الهام‌بخش و قابل استفاده باشد. بنا نیست که در طراحی بومی شاخص، چرخ از ابتدا اختراع شود بلکه بسیاری از نشانگرها عیناً قابل استفاده هستند، برخی نشانگرها نیازمند اصلاح بوده و درمواردی به افزودن نشانگر نیاز داریم. موضوع مهم در یک شاخص، چارچوب مفهومی[۱] آن شاخص است که جهت‌دار و غایت‌مند می‌باشد وگرنه نشانگرها عموماً خالی از ارزش و ابزار اندازه‌گیری متغیرها هستند.

علی زرودی
اردیبهشت ۱۴۰۲

۱) نحوه طراحی شاخص شامل طراحی چارچوب مفهومی آن در گزارش Handbook on Constructing Composite Indicators OECD به تفصیل آمده است.

## فهرست مطالب

مرکز بلفر- دانشگاه هاروارد

# ۱) درباره گزارش

## ۱-۱) نویسندگان

### جولیا وو — Julia Voo

جولیا وو رهبر تیم تحقیقاتی شاخص قدرت سایبری ملی[۱] (NCPI) در مرکز بلفر[۲] است. او سابقاً مدیر تیم تحقیقاتی «ابتکار خط‌مشی سایبری چین»[۳] بود. جولیا پیش‌از این در سفارت بریتانیا در چین خدمت می‌کرد و خط‌مشی هوش مصنوعی و سایبری چین را از منظر بازرگانی، استانداردهای فنی و سایر امور مربوط به خط‌مشی تجاری، بررسی می‌کرد.

۱) National Cyber Power Index

۲) توضیح مترجم: مرکز بلفر (Belfer) مرکز تحقیقات علوم و امور بین‌المللی در مدرسهٔ کندی هاروارد (از مدارس مهم دانشگاه هاروارد) است.

۳) China Cyber Policy Initiative

### عرفان همانی Irfan Hemani

عرفان همانی نایب‌رئیس بخش خط‌مشی سایبری وزارت دیجیتال، فرهنگ، رسانه و ورزش بریتانیا است که مسئولیت تدوین خط‌مشی فناوری ایمن را که بخشی از راهکار سایبری ملی جدید بریتانیا است، به‌عهده دارد. او پیش‌از این در تیم مشاوره ریسک فناوری دیلویت[۱] مشغول به کار بود.

### دانیل کسیدی Daniel Cassidy

دانیل کسیدی از کارشناسان استراتژی و امنیت است که در حال حاضر یکی از مدیران دارتکایت[۲] (یک شرکت مشاوره تخصصی در امور بکارگیری داده برای پشتیبانی از تصمیم‌گیری‌های استراتژیک و خط‌مشی، خصوصاً موارد مربوط به سایبر و فضای سایبری) است. پیش‌از این، وی در نقش کارشناس استراتژی و مدیریت بحران و طیف وسیعی از مسائل (ازجمله کنترل تسلیحات، تحقیقات کاربردی و مهاجرت) برای دولت بریتانیا و اتحادیه اروپا کار می‌کرد.

## ۱-۲) پروژه سایبری مرکز بلفر

چهل سال پیش، گروهی بین‌رشته‌ای از متخصصان دانشگاه هاروارد (اساتید، محققان و شاغلان) گرد هم آمدند تا با بزرگ‌ترین تهدید جنگ سرد، یعنی ترس از جنگ هسته‌ای میان اتحاد شوروی و ایالات متحده، مقابله کنند. امروزه هدف این گروه بازآفرینی همان رویکرد بین‌رشته‌ای برای مقابله با تهدیدی جدید، یعنی

۱) Deloitte: شرکت خصوصی که دفتر مرکزی آن در لندن مستقر است؛ اما خدمات حرفه‌ای خود را در سطح جهانی عرضه می‌کند. این خدمات عبارت‌اند از: خدمات بیمه، مشاوره مالیاتی، حسابرسی، مشاوره مدیریت، مشاوره مالی و مدیریت ریسک سازمانی (توضیح مترجم).

۲) Dartkite

خطر درگیری در فضای سایبری است. مسائلی که پیش‌روی رهبران کنونی قرار دارند، قابل‌توجه و متنوع‌اند. برخی از این مسائل عبارت‌اند از:

- نحوه محافظت از مهم‌ترین زیرساخت‌های حیاتی کشور در مقابل حملات سایبری؛
- چگونگی سازماندهی، آموزش و تجهیز نیرویی نظامی برای کسب پیروزی در صورت بروز درگیری‌های آتی در فضای سایبری؛
- نحوه جلوگیری از دشمنان مختلف مانند دولت‌های ملی و تروریست‌ها درخصوص اقدام به حملات در فضای سایبری؛
- نحوه مهار تشدید تنش در صورت بروز درگیری در فضای سایبری؛
- نحوه بهره‌گیری از ابزارهای حقوقی و خط‌مشی‌گذارانه برای کاهش سطح حمله ملی[۱] بدون سرکوب نوآوری.

این‌ها صرفاً نمونه‌ای از مسائلی است که انگیزه تحقیقات این گروه شده‌اند. هدف پروژه سایبری مرکز بلفر تبدیل این پروژه به جایگاهی ممتاز برای مطالعه دقیق و خط‌مشی‌گذارانه این مسائل و سایر پرسش‌های مرتبط است.

## ۱-۳) یادداشتی برای خوانندگان

رسالت مرکز بلفر این است که پیشرفت دانش خط‌مشی‌گذاری و انتقادی را درباره مسائل مهم امنیت بین‌المللی راهبری کند. انتشار این گزارش با همین هدف صورت گرفته است. شاخص قدرت سایبری ملی طی دو سال گذشته، بحث و گفتگو میان خط‌مشی‌گذاران، دانشگاهیان و دست‌اندرکاران صنعت درباره مفهوم قدرت سایبری را تسریع کرده است. همچنین چگونگی بهره‌برداری از قابلیت‌ها را برای افزایش توانایی کلی و دستیابی به اهداف ملی کشورها تسریع نموده است.

لازمه بهره‌برداری از قدرت سایبری در یک کشور، اتخاذ رویکرد ملی فراگیر[۲] است. دولت‌های[۳] ملی نباید تنها به فکر عملیات مخرب، جاسوسی یا بهبود تاب‌آوری سایبری خود باشند، بلکه باید به تلاش‌های سایر کشورها در زمینه نظارت[۴]، کنترل اطلاعات، رقابت فناورانه، انگیزه‌های مالی و شکل‌دادن به امور قابل‌قبول و ممکن از طریق هنجارها و استانداردهای سایبری (از طریق مشارکت در مجامع بین‌المللی) نیز توجه داشته باشند.

طی دوران خدمتم در دولت آمریکا، برای ارزیابی تهدیدات سایبری علیه امنیت ملی آمریکا، همواره در جستجوی روش‌های تحلیلی بودم و این روش‌ها را به کار می‌گرفتم. امروزه باتوجه به افزایش چالش‌ها در

۱) national attack surface

۲) whole-of-nation approach

۳) Government

۴) Surveillance

حوزه سایبری، دسترسی به ابزارهای تحلیلی، مطرح‌کردن طیف کامل قدرت سایبری و راه‌اندازی بحث‌های عمومی انتقادی از اهمیتی ویژه برخوردار است. چارچوب ارائه‌شده توسط NCPI این امکان را فراهم می‌سازد تا خط‌مشی‌گذاران طیف کامل‌تری از دشواری‌ها و تهدیدات ناشی از سایر بازیگران دولتی را مدنظر قرار دهند. به‌کارگیری مدل‌های کمی و کیفی با بیش از ۱۰۰۰ منبع داده موجود و ۲۹ نشان‌گر برای اندازه‌گیری قابلیت کشورها موجب شده است تا NCPI از همه روش‌های کنونی برای اندازه‌گیری قدرت سایبری جامع‌تر باشد.

شاخص قدرت سایبری ملی ۲۰۲۲ بر مبانی شرح داده شده در گزارش ۲۰۲۰ بنا شده است و باید به‌منزله تصویر لحظه‌ای از وضعیت موجود در ۳۰ کشور مدنظر قرار گیرد و مرحله‌ای خطی نسبت به شاخص ۲۰۲۰ در نظر گرفته نشود. [توضیح بیشتر اینکه] به دلیل روش‌شناسی گروه پژوهش، جابه‌جایی رو به پایین یک کشور (کاهش نمره شاخص یک کشور) به طور مطلق به معنای کاهش قدرت سایبری آن کشور نیست؛ بلکه این جابه‌جایی باید در مقایسه با برآورد قدرت سایبری سایر کشورها که تنها از منابع موجود در دسترس عموم استخراج شده‌اند، تفسیر شود. از همه مهم‌تر اینکه هدف این شاخص ارائه قضاوت‌های ارزشی درباره نحوه استفاده از قدرت سایبری در کشورهای مختلف نیست، بلکه این شاخص صرفاً حاکی از آن است که این کشورها «قابلیت[۱] سایبری» و «قصد[۲] خود برای استفاده از آن» را نشان داده‌اند. تصمیمات خط‌مشی‌گذارانه درخصوص اینکه چه چیزی مسئولانه و به صلاح کشورها، کنوانسیون‌های بین‌المللی و جهان است (یعنی قضاوت‌ها)، نیازمند این ابزار و ابزارهای مشابه است.

مدل قدرت سایبری گروه مرکز بلفر تا به امروز جامع‌ترین و بهترین مدل برای سنجش قدرت سایبری است. من به کاری که این گروه همچنان انجام می‌دهند تا این مبحث مهم را پیش‌ببرند و بر موضوعی سابقاً انتزاعی و پیوسته در حال تغییر (که امروزه برای قدرت کشورها و جغرافیای سیاسی اهمیتی فوق‌العاده دارد) نوری بتابانند، افتخار می‌کنم.

اریک روزنباخ
از مدیران مرکز بلفر، رئیس سابق ستاد
و معاون وزیر در وزارت دفاع آمریکا

۱) Capability

۲) Intent

# ۲) خلاصه مدیریتی

هنگامی که برای اولین بار در سال ۲۰۲۰ موضوع تعریف قدرت سایبری را مطرح کردیم و در همان سال «شاخص قدرت سایبری ملی» را منتشر کردیم، وابستگی دولت به اینترنت و فناوری‌های دیجیتال و استفاده از آن‌ها برای دستیابی به اهداف ملی کاملاً شناخته شده بود، ولی به طور کارآمد فهرست‌بندی نشده بود و رابطه آن‌ها با قدرت ملی هم به‌درستی درک نشده بود. مفهوم رایج قدرت سایبری در سطح کشور، نامنسجم و مورد مناقشه بود و عمدتاً بر قابلیت‌های مخرب و همچنین بر معدودی از کشورها تمرکز داشت. درعین‌حال همه‌گیری کووید ۱۹ به تشدید مخاطرات سایبری که دولت‌ها، زیرساخت‌ها، کسب‌وکارها و نیروهای کار پراکنده و دورکار با آن‌ها مواجه‌اند، منجر شده بود.

تعریف جامع ما از قدرت سایبری و شاخص همراه آن در مباحث جهانی نقش ایفا کرد و ساختاری به‌عنوان نقطه آغاز به وجود آورد که برای تفکر آتی درباره گروه‌بندی گسترده‌تر از کشورهای دارای قدرت سایبری و اهدافی که مایل‌اند با روش‌های سایبری به آن‌ها دست یابند، بسیار مفید است. اولین شاخص قدرت سایبری ملی در سال ۲۰۲۰ دامنه بحث را از ۵ کشور به ۳۰ کشور و از یک یا دو هدف به هشت هدف گسترش داد. مباحث مربوط به قدرت سایبری بر برخی دولت‌ها تأثیر گذاشته تا درباره سنجش قابلیت‌های سایبری خود رویکردی سنجیده‌تر اتخاذ کرده و موجبات کاوش عمیق‌تر در دامنه و کاربرد قدرت سایبری را فراهم کرده است.

هدف ما تأکید بر اهمیت درک قدرت سایبری به‌صورت جامع‌تر است؛ یعنی فهم این مسئله که آثار قدرت سایبری از مسائل فوری امنیت ملی بسیار گسترده‌تر است. بنابراین لازمه بهره‌برداری از آن [قدرت]، اتخاذ رویکرد ملی فراگیر (جامع) است و اینکه قابلیت‌های سایبری تنها یکی از ابزارهای موجود در جعبه ابزار کشور هستند. این تعریف گسترده‌تر، چشم‌اندازی ایجاد می‌کند که دولت‌های سرتاسر جهان باتوجه به آن منابع خود را در جهت دستیابی به اهداف ملی به کار می‌گیرند و سنگ بنای مشارکت بین‌المللی هم باید از طریق آن درک شود و شکل بگیرد. درک تحول کشورها و قدرت سایبری متعلق به آن‌ها در آینده نزدیک همچنان برای متخصصان خط‌مشی‌گذاری و جغرافیای سیاسی اساسی است. تیم «شاخص قدرت سایبری ملی» نیز همچنان در جریان تکامل قدرت سایبری به بازبینی و سنجش آن می‌پردازد.

# ۳) مقدمه

از پاییز ۲۰۲۰ که اولین شاخص قدرت سایبری ملی (NCPI) را منتشر کردیم تا به امروز، بحث قدرت سایبری (شامل دامنه و کاربرد آن) بی‌وقفه ادامه یافته است. اهمیت این مسئله غیرقابل انکار است و در حال حاضر دولت‌های سرتاسر جهان، توسعه قابلیت‌های چندوجهی[۱] و انتشار استراتژی‌های سایبری جدید را در اولویت قرار داده‌اند. چنین استراتژی‌هایی مشخص می‌کنند که این دولت‌ها چگونه قصد داشتند قابلیت‌های داخلی خود را در سطح بین‌المللی، ملی و محلی به کار گیرند تا قدرت سایبری خود را توسعه داده و به هشت هدف تشریح‌شده در گزارش دو سال پیش، دست پیدا کنند.

درحالی‌که دولت‌ها طی دو سال گذشته سرگرم تدوین خط‌مشی‌های کلی‌نگر برای توسعه و استفاده از قدرت سایبری بوده‌اند، شاهد تعداد زیادی از حمله‌های سایبری قابل ملاحظه از جمله حمله به شرکت سولار

۱) Multifaceted capabilities

ویندز[۱]، سرور مایکروسافت اکسچنج[۲]، خط لوله کولونیال[۳]، جی‌بی‌اس[۴] و اخیراً استفاده از حملات سایبری به‌عنوان یکی از ابزارهای متعدد در حمله روسیه به اوکراین بوده‌ایم. نه‌تنها تعداد حملات باج‌افزاری گسترده در دو سال گذشته افزایش یافته است، بلکه شاهد افزایش استفاده از زنجیره‌های تأمین دیجیتال به عنوان مسیری برای حمله سایبری[۵] نیز بوده‌ایم. هر مقدار که متصل‌تر و یکپارچه‌تر شویم، جذابیت حملات سایبری هم به همان نسبت برای مجرمان و حکومت‌ها افزایش می‌یابد. در نتیجه کشورها باید برای محافظت از منافع خود، قدرت سایبری را بهبود بخشند.

امروزه، مفهوم‌سازی از قدرت سایبری به صورتی که گویی از هشت هدف تشکیل شده و دولت‌ها در درون و از طریق فضای سایبری برای دستیابی به آن‌ها می‌کوشند، برای درک اقدامات کشورها و قدرت ملی بسیار مفید است. کشورها تلاش می‌کنند تا نه‌تنها زیرساخت‌ها و قابلیت‌های دشمن را نابود کنند و از کار بیندازند (مفهوم سنتی، ولی محدود و گمراه‌کننده قدرت سایبری)، بلکه دفاع سایبری ملی خود را مستحکم کرده و بهبود بخشند، در سایر کشورها به گردآوری اطلاعات پنهان (جاسوسی)[۶] پرداخته، شایستگی‌های[۷] مرتبط با فناوری‌های تجاری و سایبری را در سطح ملی افزایش دهند، محیط اطلاعاتی را کنترل و دستکاری کنند و از طرفی نفوذ خود را از طریق تعیین هنجارهای سایبری و استانداردهای فنی بین‌المللی گسترش دهند. قدرت سایبری را باید در بستر اهداف ملی کشور، مدنظر قرار داد و دولت‌ها باید هنگام تلاش برای بهره‌برداری از آن به نحوی روزافزون، رویکرد ملی فراگیر (جامع)[۸] اتخاذ کنند.

۱) Solarwinds: شرکت نرم‌افزاری آمریکایی که در سال ۱۹۹۹ تأسیس شده است و نرم‌افزارهای تجاری برای مدیریت شبکه و زیرساخت‌های فناوری اطلاعات تولید می‌کند (توضیح مترجم).

۲) Microsoft Exchange: یکی از بزرگ‌ترین پروژه‌های مایکروسافت و بخشی از خط تولید Microsoft Server است که امکان ارسال، دریافت و مدیریت Email، تماس‌ها و تقویم را فراهم می‌کند (توضیح مترجم).

۳) Colonial Pipeline: بزرگ‌ترین سیستم خط لوله برای محصولات نفتی تصفیه شده در ایالات متحده است. این خط لوله (متشکل از سه لوله) ۵۵۰۰ مایل طول دارد و می‌تواند روزانه ۳ میلیون بشکه سوخت را بین تگزاس و نیویورک حمل کند (توضیح مترجم).

۴) JBS: از شرکت‌های بزرگ تأمین گوشت در آمریکا (توضیح مترجم).

۵) Vector for cyberattacks

۶) توضیح مترجم: در متن دو کلمهٔ information و intelligence به‌کار گرفته شده است که در فارسی هر دوی آن‌ها به‌معنای اطلاعات هستند، ولی تفاوت آن‌ها در این است که information مفهومی کلی دارد و intelligence بیشتر به معنای اطلاعات پنهان و جاسوسی است. به همین دلیل و به منظور تمایزگذاری میان این دو intelligence به اطلاعات پنهان یا جاسوسی و information به اطلاعات ترجمه شده‌اند.

۷) Competence

۸) Whole-of-nation approach

شاخص ۲۰۲۲، از طریق بررسی نشانگرهای[۱] مرتبط با مقاصد و قابلیت‌ها، اندازه‌گیری جدیدی از قدرت سایبری ۳۰ کشور فراهم می‌کند. برای این کار ۲۹ نشانگر قابلیت را در هشت هدف به‌منظور اندازه‌گیری قابلیت‌ها به کار گرفته و استراتژی‌های ملی را در صورت وجود، برای همه کشورهای مورد نظر، ارزیابی کردیم.

تغییرات ایجادشده در رتبه‌بندی کشورها منعکس‌کننده داده‌های موجود برای اندازه‌گیری قدرت سایبری هستند. مجدداً تأکید می‌شود که هرگونه حرکت رو به پایین [تنزل رتبه کشور] نشان‌دهنده این نیست که قابلیت‌های کشور مورد نظر به طور مطلق کاهش یافته است؛ بلکه در اکثر موارد نشان می‌دهد که داده‌های قابل دستیابی برای عموم درباره سایر کشورها در دسترس قرار گرفته‌اند که [داده‌های جدید] حاکی از «قابلیت»[۲] و «قصد»[۳] آن کشورها برای دنبال کردن اهداف ملی با استفاده از روش‌های سایبری است.

هدف اصلی ما درک و پیگیری قدرت سایبری به‌مثابه مجموعه‌ای در حال تحول و متصل به‌هم از خط‌مشی‌ها و قابلیت‌ها است که وسعت فعالیت‌های کشور را پوشش می‌دهد. چارچوب و شاخص ما تنها مشتی نمونه خروار برای درک مقاصد و قابلیت‌های کشورها در فضای سایبری است. فضای تحقیقات دانشگاهی و خط‌مشی‌گذاری درباره قدرت سایبری و جغرافیای سیاسی در حال رشد است و انتظار داریم که این حوزه و مفهوم قدرت سایبری در سال‌های آتی همچنان متحول شود.

۱) توضیح مترجم: در متن اصلی از واژهٔ indicator استفاده شده است که در فارسی چندین معنا دارد از جمله نشانگر و شاخص. برای تمایزگذاری میان indicator و index که آن هم به معنای شاخص است، indicator را به نشانگر و index را به شاخص ترجمه کردم.

۲) Capability

۳) Intent

# ۴) مضامین کلیدی

در این بخش، به شرح مختصری از دو موضوع می‌پردازیم که از زمان انتشار شاخص در سال ۲۰۲۰ مورد توجه ویژه خوانندگان قرار گرفته است. این دو عبارت‌اند از رویکردی جامع (فراگیر)[۱] در قبال قدرت سایبری و دستیابی به اهداف متعدد با استفاده از روش‌های سایبری[۲].

## ۴-۱) رویکردی جامع (فراگیر) در قبال قدرت سایبری

قدرت سایبری چندوجهی است و لازمه بهره‌برداری از آن اتخاذ رویکرد ملی فراگیر[۳] است. هدف NCPI فراهم کردن اندازه‌گیری کامل‌تر از قدرت سایبری در مقایسه با شاخص‌های موجود، مطالعات روایتی یا گمانه‌زنی‌های ژورنالیستی است. در هرکجا که ممکن باشد، چنین رویکردی را برای اندازه‌گیری قدرت سایبری اتخاذ می‌کنیم. بسیاری از دولت‌هایی که به نحوی فزاینده قدرت سایبری را به‌منزله نوعی ابزار خط‌مشی‌گذاری گسترده‌تر در نظر می‌گیرند، با این رویکرد موافق‌اند. در دو دهه گذشته شاهد گسترش اسناد استراتژیک

۱) Holistic approach

۲) Cyber means

۳) Whole-of-nation approach: مطابق این رویکرد، تمرکز دولت‌ها نباید صرفاً بر عملیات تخریب و جاسوسی باشد؛ بلکه باید طیف متنوعی از اهداف (مثلاً مشارکت فعال بین‌المللی) را مدنظر داشته باشند (توضیح مترجم).

بوده‌ایم که نحوه تلاش دولت‌ها برای بهره‌برداری از قدرت سایبری از طریق رویکرد ملی فراگیر در آن‌ها شرح داده شده است.

با استفاده از شاخص قدرت سایبری ملی استراتژی‌های دولت‌ها، قابلیت‌های آن‌ها برای عملیات دفاعی و مخرب، تخصیص منابع و قابلیت‌های بخش خصوصی در داخل کشور (مثلاً شرکت‌های فناوری، نیروی کار و نوآوری) را اندازه‌گیری می‌کنیم. سنجش ما، هم شامل اندازه‌گیری قابلیتِ نمایش‌داده‌شده و هم شامل ظرفیت بالقوه است و در امتیاز (نمره) نهایی فرض بر این است که دولت‌ها قادرند این قابلیت‌ها را به‌صورت مؤثر به کار گرفته و یا کشور از آن‌ها منتفع می‌شود.

### ۴-۱-۱) اهداف هشت‌گانه

**۱) نظارت و پایش گروه‌های داخلی**

[برای این هدف] یک کشور اقداماتی صورت داده است تا مجوزهای قانونی و قابلیت‌های نظارت سایبری برای پایش[۱]، کشف و گردآوری اطلاعات پنهان (جاسوسی) مربوط به تهدیدات و بازیگران داخلی را در درون مرزهای خود فراهم سازد. این اقدامات ممکن است شامل تلاش‌هایی برای «نظارت بر شهروندان»، «پایش ترافیک اینترنتی»، «دورزدن رمزگذاری‌ها[۲]» یا «کشف و تخریب سرویس‌های اطلاعاتی خارجی، سازمان‌های تبهکار و گروه‌های تروریستی» باشد.

**۲) تقویت و بهبود دفاع سایبری ملی**

کشوری که بهبود دفاع خود، دارایی‌ها و سیستم‌های ملی و تقویت بهداشت و تاب‌آوری سایبری ملی[۳] را در اولویت قرار داده است. این امر شامل «دفاع فعالانه از دارایی‌های دولت»، «ارتقاء امنیت سایبری و بهداشت سایبری صنایع کلیدی و عموم مردم» و «افزایش آگاهی ملی از تهدیدات سایبری» است.

**۳) کنترل و دستکاری محیط اطلاعاتی**

کشوری که روش‌های الکترونیک را برای کنترل اطلاعات و تغییر روایت‌ها در داخل و خارج به کار گرفته است که بیانگر دوگانگی[۴] کنترل‌های اطلاعاتی است. این هدف شامل این موارد است: «انتشار پروپاگاندا در داخل»، «خلق و تشدید اطلاعات خلاف واقع[۵] در خارج» و «استفاده از قابلیت‌های سایبری

۱) Monitor

۲) Encryption

۳) improvement of national cyber hygiene and resilience

۴) Duality

۵) Disinformation

برای هدف قراردادن و تخریب گروه‌هایی که در خارج از حوزه قضایی آن قرار دارند». این مورد اخیر شامل از بین بردن مطالب افراط‌گرایانه در رسانه‌های اجتماعی و انکار پروپاگاندای خارجی است.

**۴) گردآوری اطلاعات پنهان (جاسوسی) خارجی برای امنیت ملی**

کشوری که اسرار ملی یکی از دشمنان خارجی را با استفاده از روش‌های سایبری استخراج کرده است. این هدف به طور مشخص بر گردآوری اطلاعاتی متمرکز است که فاقد حساسیت تجاری هستند و در عوض به گردآوری اطلاعات مربوط به فعالیت‌های دیپلماتیک، برنامه‌ریزی نظامی، پایش پیمان‌ها و سایر وضعیت‌هایی ارتباط دارد که دولت‌ها می‌کوشند در آن‌ها آگاهی و درک خود را از کشوری خارجی بهبود بخشند. این هدف شامل «هک»، «رخنه[۱] در مطالب طبقه‌بندی‌شده (مانند برنامه‌های نظامی)»، «سرقت سوابق پرسنل و دسترسی به ارتباطات شخصیت‌های ارشد دولتی» می‌شود.

**۵) رشد شایستگی در حوزه فناوری تجاری و سایبری در سطح ملی**

کشوری که کوشش کرده است تا صنعت فناوری داخلی خود را بهبود بخشد یا روش‌های سایبری را برای توسعه داخلی سایر صنایع به کار بگیرد. این کار ممکن است از طرق قانونی یا غیرقانونی صورت گیرد. روش‌های غیرقانونی شامل انجام جاسوسی صنعتی علیه شرکت‌ها و دولت‌های خارجی به‌منظور تسهیل انتقال فناوری است. روش‌های قانونی نیز شامل سرمایه‌گذاری در تحقیق‌وتوسعه امنیت سایبری و اولویت‌بندی توسعه نیروی کار امنیت سایبری است.

**۶) تخریب یا ازکارانداختن زیرساخت و قابلیت‌های دشمن**

کشوری که تکنیک‌ها، تاکتیک‌ها و روش‌های سایبری مخرب را برای بازداری، تخریب یا تقلیل توانایی دشمن برای مبارزه در حوزه‌های سایبری یا سنتیِ مرسوم به کار گرفته است. این امر شامل «حملات سایبری به زیرساخت‌های حیاتی»، «حمله توزیع‌شده قطع سرویس[۲] به شبکه‌های ارتباطی دولت» و همچنین «حملات سایبری برای نشان دادن قصد و قابلیت بازداری دشمن از انجام اقدامات» است.

**۷) تعیین هنجارهای سایبری و استانداردهای فنی بین‌المللی**

کشوری که به‌طور فعالانه در گفتگوهای بین‌المللی حقوقی، خط‌مشی‌گذارانه و فنی حول هنجارهای سایبری شرکت کرده است. این امر ممکن است شامل «امضای پیمان‌های سایبری»[۳]، «مشارکت در کارگروه‌های فنی»، «پیوستن به شراکت‌ها و اتحادهای سایبری برای مبارزه با جرائم سایبری» و «اشتراک‌گذاری تخصص و قابلیت‌های فنی» باشد.

---

۱) Breach

۲) Distributed Denial-of-Service attacks (DDOS)

۳) Signing cyber treaties

**۸) انباشت ثروت و/یا استخراج رمزارز[۱]**

کشوری که برای انباشت ثروت، عملیات سایبری انجام داده است. این امر شامل سرقت با استفاده از روش‌های سایبری مانند «باج‌افزار»، «اخاذی با استفاده از اطلاعات به دست آمده از طریق رخنه داده‌ها و حمله به زیرساخت دیجیتال مؤسسات مالی» و «اخاذی بر مبنای اطلاعات به‌دست آمده از طریق رخنه داده‌ها» است.

قصد[۲] کشورها برای پیگیری هر یک از اهداف را از طریق ارزیابی «استراتژی‌های ملی»، «رتوریک»[۳] و «عملیات سایبری منتسب به آن‌ها» اندازه‌گیری می‌کنیم. اگر دولتی قصد خاصی برای پیگیری یکی از این اهداف نداشته باشد، ارزیابی ما این است که هدف مربوطه برای آن دولت اهمیت چندانی ندارد.

علاوه بر این، قابلیت[۴] کشورها در دستیابی به هریک از این اهداف را نیز اندازه‌گیری می‌کنیم. نشانگرهایی که در نظر می‌گیریم یا به‌صورت مستقیم در قدرت سایبری نقش دارند یا جانشین‌هایی[۵] برای قابلیت‌هایی هستند که اندازه‌گیری آن‌ها دشوار است. درک جامعه سایبری از عوامل دخیل در قدرت سایبری در شرف تکوین است و با توسعه این حوزه، درک جامعه سایبری از عوامل دخیل در قابلیت‌های قدرت سایبری متحول خواهد شد و نشانگرهای ما هم باید به همراه آن متحول شوند. به این حقیقت واقفیم که اهداف ملی که با استفاده از روش‌های سایبری دنبال می‌شوند در خلأ شکل نمی‌گیرند. قابلیت‌های سایبری تنها ابزاری از مجموعه ابزارهای کشورها (در کنار شیوه‌های نظامی سنتی، دیپلماسی، تحریم‌ها و تعرفه‌هایی که دولت‌ها برای دستیابی به اهداف ملی‌شان به کار می‌گیرند) به شمار می‌روند.

**قدرت سایبری به معنای گسترش[۶] مؤثر قابلیت‌های سایبری توسط یک کشور برای دستیابی به اهداف ملی است.**

قدرت سایبری به معنای گسترش مؤثر قابلیت‌های سایبری توسط یک کشور برای دستیابی به اهداف ملی است. برای تمایزگذاری میان سطوح قصد و قابلیت میان کشورها در همه اهداف، واژه «جامعیت»[۷] را برای توصیف کاربرد قدرت سایبری توسط یک کشور برای دستیابی به چندین هدف در مقابل دستیابی به تعداد قلیلی از اهداف به کار می‌گیریم.

---

۱) Cryptocurrency

۲) Intent

۳) توضیح مترجم: معانی الفاظ و شعارهایی که به کار می‌برند.

۴) Capability

۵) Proxies

۶) Deployment

۷) Comprehensiveness

از طریق ترکیب امتیاز قصد و قابلیت در سطح همه اهداف هشت‌گانه، می‌توانیم بازتابی از «رتبه قدرت سایبری جامع»[۱] به دست آوریم که بر این اساس، جامع‌ترین قدرت سایبری به کشوری تعلق دارد که:

- قصد داشته باشد تا با استفاده از روش‌های سایبری اهداف متعددی را دنبال کند؛
- قابلیت پیگیری و دستیابی به اهداف مذکور را داشته باشد.

جامع‌ترین قدرت سایبری دارای بالاترین قصد و قابلیت برای دستیابی به اکثریت اهداف با استفاده از روش‌های سایبری است و پایین‌ترین نمره به کشوری تعلق دارد که کمترین اهداف را با استفاده از روش‌های سایبری دنبال کند و کمترین سطح قصد و قابلیت را داشته باشد.

## ۲-۴) دستیابی به اهداف متعدد با استفاده از روش‌های سایبری

در NCPI ۲۰۲۲، می‌توانیم از میزان استفاده از روش‌های سایبری توسط برخی کشورها برای دستیابی به اهداف متعدد مطلع شویم. برای روشن کردن مطلب، لازم به ذکر است که این میزان، اندازه‌گیری قابلیت فنی یا «پیچیدگی یک حمله سایبری»[۲] نیست. برخی متخصصان در کارگاه‌های بازخوردگیری ما ذکر کردند که پیچیدگی حملات در شاخص ۲۰۲۰ منعکس نشده، حمله سطح پایین[۳] یک کشور هم به شیوه دودویی شمارش شده است و «نمره» این حمله با نمره یک برای حمله به‌شدت پیچیده برابر بوده است. البته این نقطه‌ضعف مورد تأیید ما است؛ ولی چنین قضاوت می‌کنیم که ما نمی‌توانیم پیچیدگی فنی حملات منتسب به کشورها را با استفاده از داده‌های در دسترس عموم اندازه‌گیری کنیم. علاوه بر این، حتی اگر اندازه‌گیری پیچیدگی فنی عملیات سایبری هم به این شاخص افزوده شود، این امر امکان ارزیابی قطعی از قابلیت یک بازیگر را ایجاد نخواهد کرد. پیچیدگی عملیات قطعاً به الزامات هدف وابسته است. گردآوری اطلاعات، اشاعه اطلاعات خلاف واقع یا دزدی دارایی‌های فکری[۴] همگی با استفاده از سطوح مختلف پیچیدگی فنی امکان‌پذیر هستند. در حقیقت پیچیده‌ترین عملیات‌های سایبری در بسیاری از موارد به اطلاع عموم نمی‌رسد. دلیل ممکن است این باشد که قربانی از اینکه مورد حمله قرار گرفته است، آگاه نیست و یا مایل نیست که این مسئله را تأیید کند که هدف حمله بوده است و یا اینکه اقدامات حمله‌کننده کشف نشده‌اند یا امکان انتساب این اقدامات به حمله‌کننده وجود ندارد.

۱) Comprehensive Cyber Power Ranking

۲) Sophistication of a cyberattack

۳) Low-level attack

۴) Intellectual property

درباره شاخص ۲۰۲۰ به ردیاب عملیات سایبری[۱] شورای روابط خارجی[۲] (CFR) متکی بودیم و با پیگیری بازخوردها توانستیم از منبعی دیگر یعنی پایگاه داده حوادث سایبری مهم[۳] مرکز مطالعات استراتژیک و بین‌المللی[۴] (CSIS) که حوادثی با تأثیر مالی بیش از یک میلیون دلار را اندازه‌گیری می‌کند، بهره‌برداری کنیم؛ زیرا در پایگاه داده CFR چنین تمایزی لحاظ نمی‌شود.

پیش از این، حملاتی را که کشورها با اهداف مختلف انجام داده بودند به‌مثابه سنجه‌ای[۵] از توانایی آشکار آن کشورها برای عملیاتی‌سازی انواع خاصی از حملات، اندازه‌گیری می‌کردیم. این نشانگر بسیار مهم است؛ زیرا یکی از نشانگرهای عینی توانایی یک کشور برای بهره‌برداری[۶] از قدرت سایبری به منظور دستیابی به هدفی خاص است؛ اما تصدیق می‌کنیم که منابع مختلف به همه عملیات‌های سایبری صورت‌گرفته دسترسی ندارند. امسال با استفاده از منبعی دیگر و اعمال چارچوب NCPI برای لحاظ کردن «قدرت سایبری جامع»[۷]، این نشانگر را بهبود بخشیدیم.

۱) Cyber Operations Tracker

۲) Council on Foreign Relations

۳) Significant Cyber Incidents database

۴) Center for Strategic and International Studies

۵) Measure

۶) Leverage

۷) جامعیت قدرت سایبری یعنی حکومت‌هایی که در عملیات سایبری‌شان چندین هدف را دنبال می‌کنند.

# ۵) شاخص قدرت سایبری ملی ۲۰۲۲

## ۵-۱) رتبه‌بندی کلی برای سال ۲۰۲۲[۱]

همان‌گونه که در جدول ۱ مشاهده می‌شود، جامع‌ترین کشورها با بالاترین سطح قصد و قابلیت در بین هر هشت هدف به شرح ذیل هستند.

جدول ۱) ۱۰ قدرت سایبری جامع برتر مطابق NCPI ۲۰۲۲

| رتبه | ۲۰۲۲ |
|---|---|
| ۱ | ایالات متحده |
| ۲ | چین |
| ۳ | روسیه |
| ۴ | بریتانیا |
| ۵ | استرالیا |
| ۶ | هلند |
| ۷ | کره جنوبی |

۱) برای اطلاع از چارچوب مفهومی NCPI و تعریف اهداف، لطفاً به پیوست الف نگاه کنید.

| رتبه | ۲۰۲۲ |
|---|---|
| ۸ | ویتنام |
| ۹ | فرانسه |
| ۱۰ | ایران |

## ۵-۲) تفسیرشاخص

محققان، متخصصان و خط‌مشی‌گذاران برای درک اینکه کدام کشورها، بر مبنای داده‌های در دسترس عموم، جامع‌ترین قدرت‌های سایبری هستند، می‌توانند از مقیاس تجمعی[۱] قدرت سایبری NCPI در سطح هر هشت هدف استفاده کنند. بر اساس ارزیابی ما، کشورهای رده‌بالا، در استفاده از روش‌های سایبری برای دستیابی به اهدافی در حوزه‌های متعدد از همه کارآمدتر هستند.

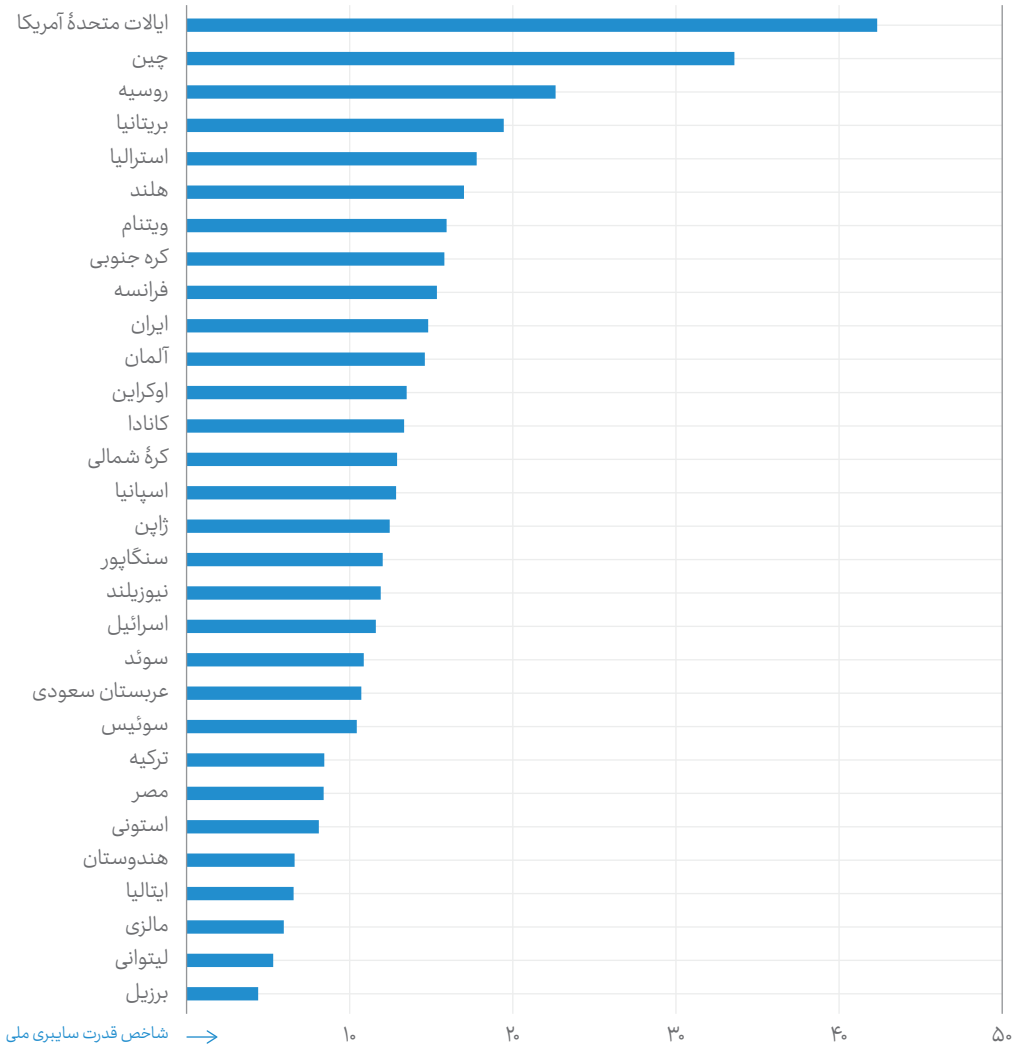
### ۵-۲-۱) تغییرات کشورها

**جدول ۲) مقایسه بین ۱۰ قدرت سایبری برتر در سال‌های ۲۰۲۰ و ۲۰۲۲**

| رتبه | ۲۰۲۰ | ۲۰۲۲ |
|---|---|---|
| ۱ | ایالات متحده | ایالات متحده |
| ۲ | چین | چین |
| ۳ | بریتانیا | روسیه |
| ۴ | روسیه | بریتانیا |
| ۵ | هلند | استرالیا |
| ۶ | فرانسه | هلند |
| ۷ | آلمان | کره جنوبی |
| ۸ | کانادا | ویتنام |
| ۹ | ژاپن | فرانسه |
| ۱۰ | استرالیا | ایران |

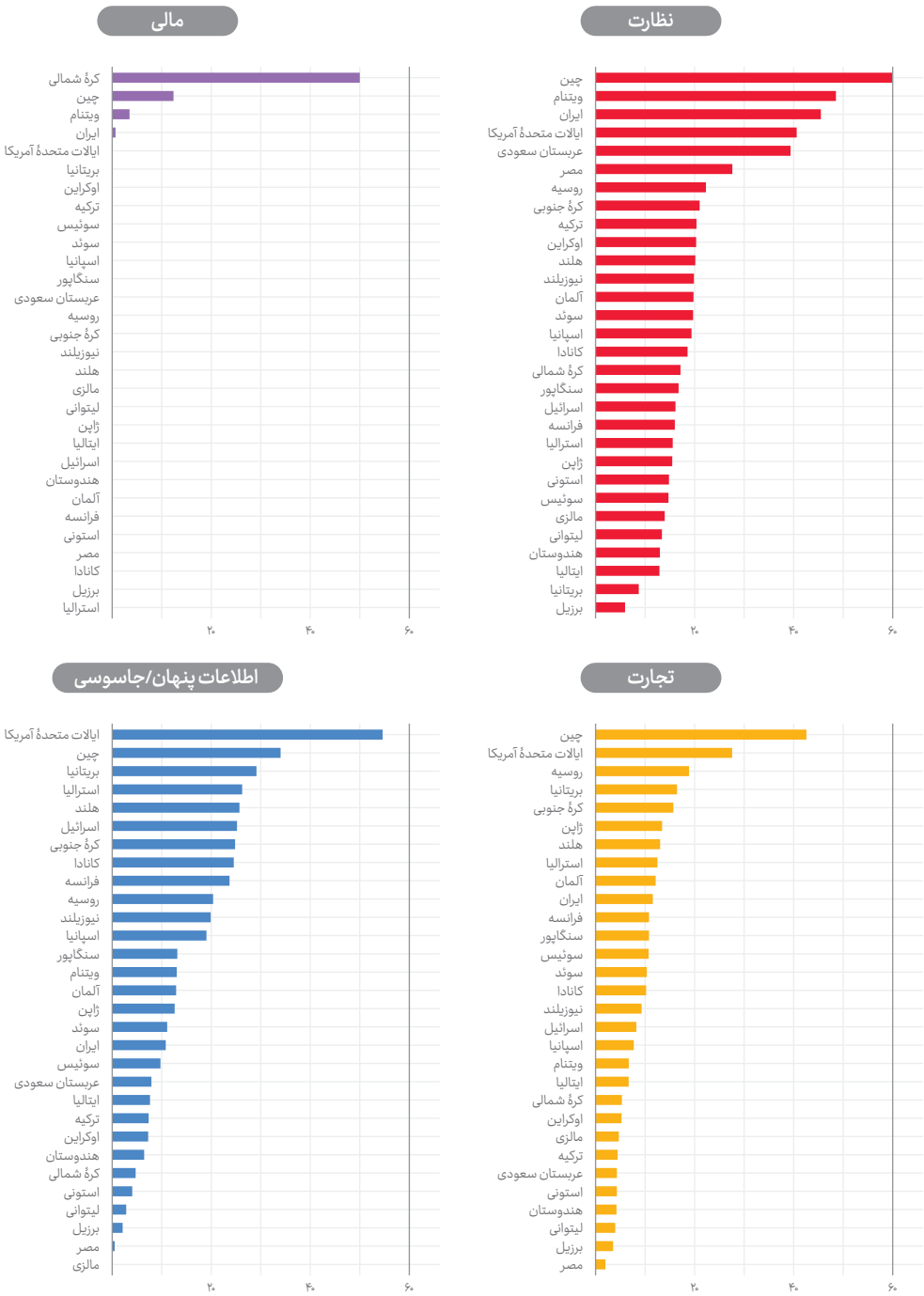
۱) Aggregated measure

**شکل ۱) رتبه‌بندی کلی (جایگاه ۳۰ کشور در شاخص ۲۰۲۲)**

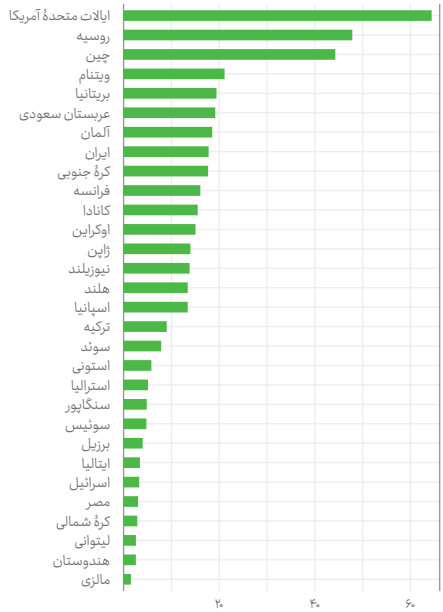



در ادامه، این رتبه‌بندی بر حسب اهداف هشت‌گانه تفکیک شده است.

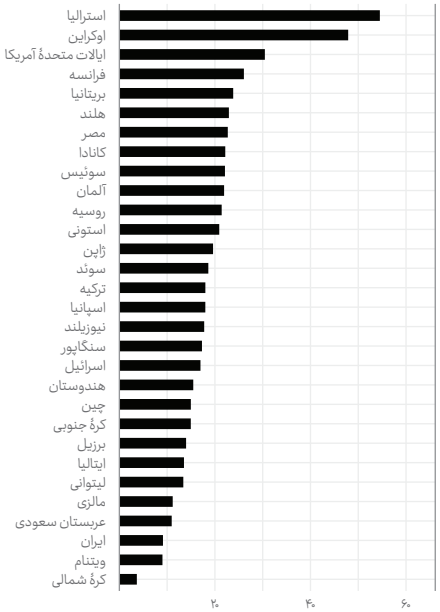
**شکل ۲)** رتبه‌بندی کشورها برحسب هدف



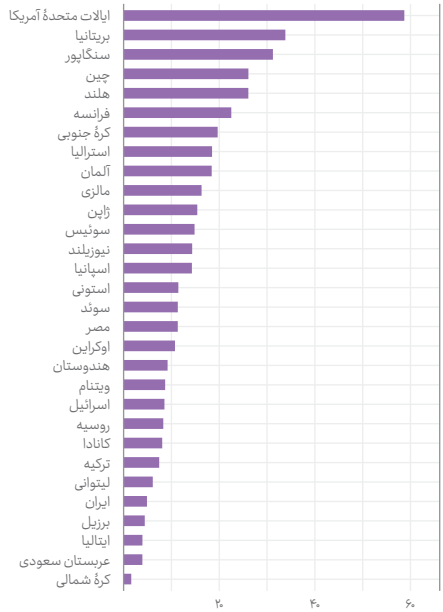
## کنترل اطلاعات



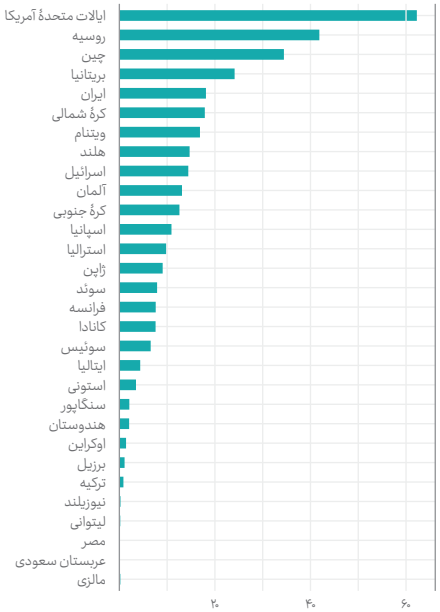

## دفاع




## هنجارها




## تخریب



برخی جابه‌جایی‌ها در میان ۱۰ قدرت سایبری برتر مشاهده می‌شود. از همه قابل‌توجه‌تر این است که روسیه از جایگاه چهارم به سوم رسیده و بریتانیا یک رتبه تنزل کرده است. در بین دو مورد از اهداف، یعنی سود تجاری و قابلیت مخرب، قدرت سایبری روسیه، در مقایسه با بریتانیا، افزایش یافته که عمدتاً به دلیل انجام عملیات سایبری بیشتر نسبت به موارد گزارش‌شده عمومی در این حوزه‌ها است.
سایر جابه‌جایی‌های جالب در رتبه‌بندی‌های ما ایران و اوکراین هستند. ایران از رتبه ۲۲ شاخص به رتبه ۱۰ رسیده و رتبه قابلیت آن از بیست و هشتم به پانزدهم رسیده است. اوکراین هم از رتبه بیست و نهم به رتبه دوازدهم صعود کرده و رتبه‌بندی قابلیت آن دو پله افزایش یافته و رتبه‌بندی قصد آن از بیست و یکم به ششم رسیده که عمدتاً ناشی از افزایش در رتبه‌های دفاع، اطلاعات پنهان (جاسوسی) و تخریب بوده است، ولی رتبه‌های آن به‌طورکلی افزایش یافته است.

رتبه دو کشور از همسایگان منطقه‌ای چین هم در شاخص ۲۰۲۲ افزایش قابل‌ملاحظه‌ای پیدا کرده است. کره جنوبی از رتبه شانزدهم به هفتم صعود کرده که از نظر قابلیت یکسان باقی مانده است؛ ولی رتبهٔ قصد آن به دلیل افزایش‌های کلی (به‌ویژه افزایش در نظارت، کنترل اطلاعات، جاسوسی، تجارت و هنجارها) از هجدهم به نهم صعود کرده است.

رتبه ویتنام هم از بیستم به هشتم رسیده که از نظر قابلیت یکسان باقی مانده؛ ولی رتبه قصد آن به دلیل افزایش در دفاع، تجارت، تخریب و هنجارها از شانزدهم به سوم رسیده است.

با توجه به ماهیت داده‌هایی که گردآوری می‌کنیم، این تغییرات رتبه‌ها به افزایش یا کاهش مطلق در قدرت سایبری در مقایسه با سال ۲۰۲۰ اشاره ندارند؛ بلکه نشان‌دهنده تغییری نسبی در قدرت سایبری بر مبنای اطلاعات قابل‌دسترس برای عموم در مقایسه با سایر کشورها هستند.

## ۵-۳) محدودیت‌ها

تحلیل هدف‌گرای NCPI از قدرت سایبری ملی، با برخی محدودیت‌ها مواجه است که عمدتاً به ماهیت در حال تغییر و بحث‌برانگیز «قدرت سایبری» و میزان محدود داده‌های موجود در حوزه عمومی درمورد قابلیت‌ها و مقاصد سایبری کشورهای مختلف ارتباط دارند. محدودیت‌هایی که در روش‌شناسی شاخص ۲۰۲۰ شرح دادیم، به‌طور خلاصه عبارت‌اند از:

### ۵-۳-۱) فقدان داده‌های قابل دسترسی عمومی درباره قابلیت‌ها و مقاصد سایبری

داده‌های گردآوری‌شده برای اکثریت کشورهای مورد ارزیابی (نه همه آن‌ها) موجود است. یکی از چالش‌های ساخت این شاخص، محرمانگی مؤلفه‌های مؤثر در قدرت سایبری کشورها است؛ مثلاً [اطلاعات مربوط به] تعداد پرسنل نظامی یا قابلیت‌های جاسوسی آن‌ها، حساس و به‌تبع آن محرمانه‌اند. البته داده‌ها در برخی حوزه‌ها (مثلاً تلاش‌های صورت‌گرفته در جهت افزایش نیروی کار ماهر و داده‌های مرتبط با صنعت)

حساسیت کمتری دارند؛ اما دستیابی به این داده‌ها برای کشورهایی با ساختارهای حکمرانی نه‌چندان شفاف و پاسخگو یا با منابع کمتر، دشوارتر است.

به دلیل حساسیت‌های برخی از جنبه‌های قدرت سایبری، به‌ویژه قابلیت‌های مخرب، دفاعی و جاسوسی و وابستگی آن‌ها به ساختارهای داخلی امنیت ملی، احتمال دارد که برخی کشورها عمداً از قصد و قابلیت‌های خود محافظت کنند و به دلایل استراتژیک، مانع از دستیابی عموم به این اطلاعات شوند. از نظر ما، این امر درباره اکثر کشورها و به طور مشخص درباره چین، اسرائیل و کره شمالی در رابطه با قابلیت‌های سری یا نظامی صادق است. در سال‌های اخیر، شاهد آن بوده‌ایم که دموکراسی‌های غربی اطلاعات بیشتری را درباره قابلیت‌های سایبری نظامی خود به اشتراک می‌گذارند؛ اما دلیل این کار آن‌ها یا بازدارندگی[۱] در مقابل دشمنان است یا نتیجه خط‌مشی‌های ملی درباره شفافیت یا رهبری سیگنال[۲] و شکل دادن به گفتگوی جهانی. این فقدان شفافیت به‌ویژه درباره سه هدف فوق‌الذکر و کمابیش در مورد سایر حوزه‌ها به دلیل افزایش تنش‌های ژئوپلیتیکی، صادق است. تصدیق می‌کنیم که رتبه کشوری که عامدانه از شفاف‌سازی اجتناب می‌کند، در حوزه‌های مربوط به NCPI پایین‌تر از حد واقعی خواهد بود. برای مثال هیچ کشوری آشکارا اعلام نمی‌کند که از روش‌های سایبری، مانند باج‌افزار، برای انباشت ثروت استفاده می‌کند و برای مقابله با فقدان اطلاعات در این حوزه، NCPI شامل حملات سایبری منتسب به این کشورها در هدف مربوطه می‌باشد؛ زیرا از نظر ما انجام عملیات سایبری توسط یک کشور نشان‌دهنده قصد این کشور است. به همین ترتیب تعداد بسیار معدودی از کشورها تعداد پرسنل مشغول به کار در عملیات سایبری مخرب یا عملیات صورت‌گرفته با این هدف را منتشر می‌کنند؛ بنابراین اندازه‌گیری قابلیت کشور را بسیار دشوار می‌سازد، به‌ویژه اگر آن عملیات چنان موفق باشند که کشف نشده و علناً گزارش نشوند.

۱) Deterrent

۲) Signal leadership: منظور از سیگنال، سیستم‌های ارتباطاتی است. یعنی می‌خواهد رهبری خود در حوزه سایبر را به نمایش بگذارد (توضیح مترجم).

# ۶) نتیجه‌گیری

کشورهای مختلف همچنان قابلیت‌های خود را توسعه می‌دهند تا در فضای سایبری به اهداف متعددی دست پیدا کنند. برای درک بهتر اقدامات دولت‌ها و قدرت ملی، «مفهوم‌سازی قدرت سایبری به‌مثابه امری چندبعدی» و «گسترش حوزه تحلیل و در نظر گرفتن وسعت اهدافی که دولت‌ها تلاش می‌کنند با استفاده از روش‌های سایبری به آن‌ها دست پیدا کنند» بسیار مهم است. با توجه به تحلیل ما، کاملاً آشکار است که کشورها می‌کوشند نه‌تنها زیرساخت و قابلیت‌های دشمنان خود را تخریب و بی‌اثر کنند، بلکه دفاع سایبری ملی را تقویت کرده و بهبود بخشند، در سایر کشورها به گردآوری اطلاعات پنهان (جاسوسی) بپردازند، شایستگی در حوزه فناوری تجاری و سایبری در سطح ملی را افزایش دهند، محیط اطلاعاتی را کنترل و دستکاری کنند و از طریق تعیین هنجارهای سایبری و استانداردهای فنی بین‌المللی نفوذ خود را گسترش دهند. کشورها باید قدرت سایبری را در بستر اهداف ملی مدنظر قرار داده و در هنگام تلاش برای بهره‌برداری از آن، به نحوی روزافزون رویکرد ملی فراگیر (جامع) اتخاذ کنند.

اگر از این شاخص اندکی به عقب بازگردیم، مشاهده می‌کنیم که حکمرانی و زیرساختی که از اینترنت پشتیبانی می‌کند، به نحوی روزافزون چندتکه[۱] شده است. با تسریع این چندپارگی به دلیل نقل و انتقالات قدرت، رویدادهای ژئوپلیتیکی و افزایش نفوذ چین (به‌ویژه در حوزه سایبری) حکومت‌ها اکنون بیش از

۱) Fragmented

هرزمان دیگری می‌کوشند درباره مسائل سایبری با سایر کشورها ائتلاف[۱] کنند و شکل حوزه سایبری را به نفع خود تغییر دهند. این کار خواه جستجویی برای اجماع[۲] بر رفتار قابل‌قبول حکومت‌ها و اجماع بر هنجارهای فضای سایبری در سازمان ملل باشد (حکمرانی فناوری از طریق استانداردهای فنی برای پیشبرد یا ممانعت از قابلیت همکاری[۳])، خواه طرح‌هایی برای متنوع‌سازی زنجیره‌های تأمین و ایجاد اکوسیستم‌های جدیدتر در حکومت‌هایی با رفتار دوستانه‌تر، نشان‌دهنده آن است که پیوند فناوری و ارزش‌ها، محل اختلاف روبه‌رشد در فضای جهانی است.

حمله روسیه به اوکراین که طیف کاملی از قدرت سایبری در آن مورد استفاده قرار گرفته، موجب تسریع رشد این محل اختلاف در امور جهانی شده است. پیش‌بینی گسترش حملات سایبری روسیه به خارج از مناطق درگیری به‌صورت ناخواسته و یا کاربرد این حملات به‌مثابه سلاحی هدفمند علیه کشورهایی که خود را متحد اوکراین اعلام کرده‌اند، موجب شده است که جامعه سایبری به جنب‌وجوش افتاده و پشتیبانی خود را برای دفاع از دارایی‌های دیجیتال اوکراین، با ظرفیت‌سازی و فراهم‌کردن تجهیزات، اعلام کند. کشورها دفاع سایبری خود را افزایش داده‌اند تا برای هر دو سناریو آماده شوند.[۴] در زمان انتشار این مقاله، به نظر می‌رسد که عملکرد روسیه (با حمله به زیرساخت، خدمات و کسب‌وکارهای اوکراین) در استفاده از قدرت سایبری مخرب، به عنوان بخشی از درگیری، هدفمند بوده است. گزارش‌ها حاکی از آن است اگرچه حملات نظامی و سایبری پشت سر هم[۵] صورت گرفته‌اند، مقیاس آن‌ها از حد مورد انتظار کوچک‌تر بوده و ظاهراً اهداف مشترک داشته‌اند.[۶] کنترل محیط اطلاعاتی داخلی، بخشی کلیدی از کوشش‌های جنگی روسیه بوده است و تضمین می‌کند که مردم این کشور تنها دورنمایی محدود از رویدادها را مشاهده می‌کنند. روسیه می‌کوشد تا قدرت خود را برای بی‌اعتبارسازی روایات اوکراین و غرب در صحنه بین‌المللی به کار گیرد. این درگیری ماهیت درهم‌تنیده زنجیره‌های تأمین جهانی را آشکار ساخته است و (با خروج شرکت‌های خارجی از روسیه به دلیل تحریم‌های غرب و ورود شرکت‌های داخلی روسیه یا شرکت‌های غیرغربی به صحنه برای پرکردن این خلأ[۷] و در عین‌حال اتکا به اجزاء غربی برای قابلیت نظامی خود[۸]) شکی نیست که موردی بسیار مهم به مباحث مربوط به دوشاخگی[۹] فناوری‌ها می‌افزاید. کشورها به‌تدریج زنجیره‌های تأمین داخلی و

۱) Coalition

۲) Consensus

۳) Interoperability

۴) https://www.washingtonpost.com/technology/۲۸/۰۲/۲۰۲۲/internet-war-cyber-russia-ukraine/

۵) In tandem

۶) اکونومیست (آنلاین)، به نظر می‌رسد که روسیه حملات سایبری‌اش را با کارزار نظامی‌اش هماهنگ ساخته است، لندن، ۱۰ مه ۲۰۲۲ و https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE۴Vwwd.

۷) https://www.reuters.com/world/europe/foreign-digital-firms-leave-russias-domestic-providers-pounce-2022-04-01/

۸) https://www.nytimes.com/2022/06/02/business/economy/russia-weapons-american-technology.html

۹) Bifurcation

قدرت تجاری داخلی خود در این حوزه را دوباره امتحان می‌کنند. می‌توانیم انتظار داشته باشیم که روسیه همچنان در زمینه نظارت داخلی و گردآوری اطلاعات پنهان (جاسوسی) در سایر کشورها قدرت‌نمایی کند[۱]، زیرا این قابلیت‌ها به‌سادگی می‌توانند از سایر اهداف، به‌ویژه نابودکردن زیرساخت‌های دشمن، پشتیبانی کنند.

در محیط ژئوپلیتیکی کنونی، کاملاً واضح است که کشورها خواهان دستیابی به مجموعه‌ای جامع‌تر از قابلیت‌های قدرت سایبری هستند. بنابراین مقایسه و درک طیفی گسترده‌تر از بازیگران این حوزه امری حیاتی و مهم به‌شمار می‌رود. طبق پیش‌بینی بلفر، دو چالش همگام‌شدن با مفهوم درحال تغییر قدرت سایبری و به طور هم‌زمان اندازه‌گیری قدرت سایبری ۳۰ کشور یا بیشتر با استفاده از داده‌های قابل دسترس برای عموم، به امتداد گفتگو منجر خواهد شد و لازمه آن انعطاف‌پذیری است. ولی ازآنجاکه دولت‌های ملی می‌کوشند تا برای افزایش قدرت سایبری خود نسبت به سایرین یا در همکاری با سایرین، درون اکوسیستم‌های ملی و میان کشورها گفتگوهایی ایجاد کنند و ائتلاف‌هایی بسازند، یافتن راهی برای مقایسه و ایجاد درکی مشترک بسیار مهم است. امیدواریم که سایر محققان همچنان این پژوهش را توسعه دهند و چشم به راهیم تا مباحث اجتناب‌ناپذیر و پرمایه درباره تحول قدرت سایبری و ژئوپلیتک پیشرفت کنند.

۱) Flex

# ۷) پیوست الف:
## روش‌شناسی

در فاصله بین شاخص‌های ۲۰۲۰ و ۲۰۲۲، تیم مربوطه فرایند بسیار دشوار به چالش‌کشیدن نشانگرهای به کار گرفته‌شده را پشت سر گذاشت تا متوجه شود که آیا داده‌های در دسترس بهتر یا نشانگرهای بهتری وجود دارند که به اندازه‌گیری انواع قابلیت‌ها کمک کنند یا خیر. چندین کارگاه آموزشی برگزار شد و با متخصصان جاسوسی، دفاعی و سایبری مصاحبه‌های عمیقی انجام گرفت تا مفروضات زیربنایی NCPI ۲۰۲۰ را مورد آزمایش قرار داده و پیشنهادهایی درباره نحوه اصلاح روش‌شناسی با استفاده از داده‌های در دسترس برای عموم دریافت کنیم. بدین ترتیب، برخی اصلاحات در نشانگرهای به‌کارگرفته‌شده اعمال شد.

## ۱-۷) چارچوب مفهومی

جدول ۳) اهداف دنبال‌شده

| هدف | توصیف |
|---|---|
| انباشت و محافظت[۱] از ثروت | کشوری که برای انباشت ثروت، عملیات سایبری انجام داده است. این امر شامل سرقت با استفاده از روش‌های سایبری است: «باج‌افزار»، «اخاذی با استفاده از اطلاعات به‌دست آمده از طریق رخنه داده‌ها و حمله به زیرساخت دیجیتال مؤسسات مالی» و «اخاذی بر مبنای اطلاعات به‌دست آمده از طریق رخنه داده‌ها». |
| کنترل و دستکاری محیط اطلاعاتی | کشوری که روش‌های الکترونیک را برای کنترل اطلاعات و تغییر روایت‌ها در داخل و خارج به کار گرفته است که بیانگر دوگانگی[۲] کنترل‌های اطلاعاتی می‌باشد. این هدف شامل این موارد است: «انتشار پروپاگاندا در داخل»، «خلق و تشدید اطلاعات خلاف واقع[۳] در خارج» و «استفاده از قابلیت‌های سایبری برای هدف قراردادن و تخریب گروه‌هایی که در خارج از حوزه قضایی آن قرار دارند». مورد اخیر شامل از بین بردن مطالب افراط‌گرایانه در رسانه‌های اجتماعی و انکار پروپاگاندای خارجی است. |
| تعیین هنجارهای سایبری و استانداردهای فنی بین‌المللی | کشوری که به طور فعالانه در گفتگوهای بین‌المللی حقوقی، خط‌مشی‌گذارانه و فنی حول هنجارهای سایبری شرکت کرده است. این امر ممکن است شامل «امضای پیمان‌های سایبری»[۴]، «مشارکت در کارگروه‌های فنی»، «پیوستن به شراکت‌ها و اتحادهای سایبری برای مبارزه با جرائم سایبری» و «اشتراک‌گذاری تخصص و قابلیت‌های فنی» باشد. |
| تخریب یا ازکارانداختن زیرساخت و قابلیت‌های دشمن | کشوری که تکنیک‌ها، تاکتیک‌ها و روش‌های سایبری مخرب را برای بازداری، تخریب یا تقلیل توانایی دشمن برای مبارزه در حوزه‌های سایبری یا سنتی مرسوم به کار گرفته است. این امر شامل «حملات سایبری به زیرساخت‌های حیاتی»، «حمله توزیع‌شده قطع سرویس[۵] به شبکه‌های ارتباطی دولت» و همچنین «حملات سایبری برای نشان دادن قصد و قابلیت بازداری دشمن از انجام اقدامات» است. |
| گردآوری اطلاعات پنهان (جاسوسی) خارجی برای امنیت ملی | کشوری که اسرار ملی یکی از دشمنان خارجی را با استفاده از روش‌های سایبری استخراج کرده است. این هدف به طور مشخص بر گردآوری اطلاعاتی متمرکز است که فاقد حساسیت تجاری هستند و درعوض به گردآوری اطلاعات مربوط به فعالیت‌های دیپلماتیک، برنامه‌ریزی نظامی، پایش پیمان‌ها و سایر وضعیت‌هایی ارتباط دارد که دولت‌ها می‌کوشند در آن‌ها آگاهی موقعیتی و درک خود را از کشوری خارجی بهبود بخشند. این هدف شامل «هک»، «رخنه در مطالب طبقه‌بندی‌شده (مانند برنامه‌های نظامی)»، «سرقت سوابق پرسنل و دسترسی به ارتباطات شخصیت‌های ارشد دولتی» می‌شود. |

۱) توضیح مترجم: البته در این شاخص، هنوز نشانگری برای محافظت ندارند.

۲) Duality

۳) Disinformation

۴) Signing cyber treaties

۵) Distributed Denial-of-Service attacks (DDOS)

| هدف | توصیف |
|---|---|
| رشد شایستگی در حوزه فناوری تجاری و سایبری در سطح ملی | کشوری که کوشش کرده است تا یا صنعت فناوری داخلی خود را بهبود بخشد یا روش‌های سایبری را برای توسعه داخلی سایر صنایع به کار گرفته است. این کار ممکن است از طرق قانونی یا غیرقانونی صورت گیرد. طرق غیرقانونی شامل انجام جاسوسی صنعتی علیه شرکت‌ها و دولت‌های خارجی به منظور تسهیل انتقال فناوری است. طرق قانونی شامل سرمایه‌گذاری در تحقیق و توسعه امنیت سایبری و اولویت‌بندی توسعه نیروی کار امنیت سایبری است. |
| تقویت و بهبود دفاع سایبری | کشوری که بهبود دفاع خود، دارایی‌ها و سیستم‌های ملی و تقویت بهداشت و تاب‌آوری سایبری ملی[۱] را در اولویت قرار داده است. این امر شامل «دفاع فعالانه از دارایی‌های دولت»، «ارتقاء امنیت سایبری و بهداشت سایبری صنایع کلیدی و عموم مردم» و «افزایش آگاهی ملی از تهدیدات سایبری» است. |
| نظارت و پایش گروه‌های داخلی | [برای این هدف] یک کشور اقداماتی صورت داده است تا مجوزهای قانونی و قابلیت‌های نظارت سایبری برای پایش[۲]، کشف و گردآوری اطلاعات پنهان (جاسوسی) مربوط به تهدیدات و بازیگران داخلی را در درون مرزهایش فراهم سازد. این اقدامات ممکن است شامل تلاش‌هایی برای «نظارت بر شهروندان»، «پایش ترافیک اینترنتی»، «دورزدن رمزگذاری‌ها[۳]» یا «کشف و تخریب سرویس‌های اطلاعاتی خارجی، سازمان‌های تبهکار و گروه‌های تروریستی» باشند. |

## ۷-۲) فرمول شاخص قدرت سایبری ملی

شکل ۳) فرمول NCPI ۲۰۲۲

$$\text{شاخص قدرت سایبری ملی (NCPI)} = \frac{1}{8}\sum_{x=1}^{8} \text{قابلیت}_x \times \text{قصد}_x$$

## ۷-۳) ساخت NCPI تجمعی

### ۷-۳-۱) داده‌های ناموجود[۴] و نرمال‌سازی نشانگرها

گروه پژوهشگر نتوانست داده‌های مربوط به همه نشانگرها را برای تمامی ۳۰ کشور موجود در NCPI ۲۰۲۲ به‌دست آورد. همه نشانگرهای موجود در شاخص، منعکس‌کننده داده‌های موجود برای دست‌کم ۲۱

۱) Improvement of national cyber hygiene and resilience

۲) Monitor

۳) Encryption

۴) Missing Data

کشور (۷۰٪) از ۳۰ کشور هستند که در آن جانشین‌های قابل‌قبولی برای نقاط داده ناموجود در نظر گرفته شد. برآوردها بر مبنای کشورهای دارای خصوصیات مشابه (اندازه جمعیت، قدرت اقتصادی، وضعیت جغرافیایی) یا بر مبنای سایر نشانگرهای نزدیک به آنچه که اندازه‌گیری می‌کنیم، محاسبه شده‌اند. نشانگرهایی که این آستانه[۱] را برآورده نمی‌کنند، لحاظ نشده‌اند. چندین نشانگر را در درون کشورها منبع‌یابی و از روال و طرح کدگذاری[۲] بسیار دقیقی پیروی کردیم.

هیچ‌گونه مقدار گم‌شده‌ای[۳] در مجموعه داده‌ها[۴] وجود ندارد. برای همه نشانگرها و کشورهایی که اطلاعات آن‌ها ناموجود بود، نوعی مقدار تخمینی ارائه داده‌ایم. به‌طور مشخص، برخی مقادیر برای نشانگرهای ذیل برآورد شده‌اند:

**جدول ۴) نشانگرهای قابلیت کشورها که به‌طور تقریبی برآورد شده‌اند.**

| نشانگر | برآوردشده برای کشورهای زیر |
|---|---|
| شاخص سواد و آموزش ریسک سایبری | کره شمالی، مصر، ایران، مالزی، اوکراین، ویتنام |
| ستاد نظامی سایبری[۵] | کره شمالی، مصر، هندوستان، لیتوانی، مالزی، نیوزیلند، عربستان سعودی، اوکراین، ویتنام |
| قوانین حریم خصوصی داده‌ها | کره شمالی |
| آزادی در اینترنت | کره شمالی، اسرائیل، لیتوانی، هلند، نیوزیلند، اسپانیا، سوئد، سوئیس |
| شاخص قدرت نرم جهانی | کره شمالی، لیتوانی |
| نرخ آلودگی موبایل/کامپیوتر | کره شمالی، استونی، لیتوانی، نیوزیلند |
| نهاد استانداردهای ملی | کره شمالی، برزیل، چین، مصر، اسرائیل، لیتوانی، مالزی، روسیه، کره جنوبی، عربستان سعودی |
| جمعیت موجود در اینترنت | کره شمالی |
| مصرف رسانه‌های اجتماعی | کره شمالی |
| نظارت | کره شمالی، مصر، کره جنوبی، عربستان سعودی، ترکیه، اوکراین، ویتنام |

۱) Threshold

۲) Coding scheme and procedure

۳) Missing values

۴) Data set

۵) Cyber Military Staffing

پیش از تجمیع داده‌ها، نشانگرها را به صورت جهت‌دار اصلاح کردیم تا در همه نشانگرها مقادیر بالاتر با عملکرد بهتر قدرت سایبری متناظر باشند. گروه پژوهشی، تحلیل همبستگی دوگانه را بر روی کلیه نشانگرها انجام داده است.

پیش از تجمیع داده‌ها، نشانگرها را نرمال‌سازی کردیم تا آن‌ها را روی مقیاسی مشترک منتقل کنیم. تکنیک حداقل-حداکثر را به عنوان تکنیک نرمال‌سازی به کار گرفتیم، زیرا این تکنیک: (۱) به بهترین وجه منعکس‌کننده چارچوب مفهومی است؛ (۲) برای ویژگی‌های داده‌ها از همه مناسب‌تر است؛ و (۳) کاربران به‌سادگی می‌توانند آن را تفسیر کنند.

### ۷-۳-۲) تجمیع و وزن‌دهی به NCPI

برای اندازه‌گیری نمره (امتیاز) هر هدف، از نمرات نرمال‌سازی‌شده قابلیت برای آن هدف میانگین گرفتیم. سپس نمرات نرمال‌سازی‌شده و میانگین قابلیت هدفی خاص را در نمره قصد همان هدف ضرب کردیم تا نمره NCPI را برای هدفی واحد به دست آوریم. برای محاسبه NCPI در سطح همه اهداف، نمرات اهداف را با هم جمع کردیم تا نوعی نمره تجمیعی ایجاد کنیم.

این رویکرد هدف‌گرا دارای پیامدهای مهمی برای ساخت NCPI است؛ زیرا نوعی وزن ایجاد می‌کند و برخی نشانگرها چندین بار شمارش می‌شوند (نگاه کنید به جدول ۱۴). شمارش چندباره مبتنی‌بر تأمل نظری دقیق درباره نحوه انطباق قابلیت‌های سایبری مختلف با اهداف سایبری متعدد است.

طبق پیش‌فرض، هر نشانگری که چندین بار شمارش شده باشد، نمره NCPI و شاخص قابلیت سایبری را برای کشوری که در آن نشانگر قابلیت نمره بالایی داشته باشد، افزایش می‌دهد.

برای هر هدف، با ضرب قابلیت‌های کشور در قصد آن برای دستیابی به هدف مذکور، نمرات قصد NCPI را محاسبه می‌کنیم. برای هر کشور، از طریق اندازه‌گیری قصد، عملاً وزنی برای قابلیت‌های آن قائل می‌شویم. بخش قصد NCPI ما را می‌توان معادل وزن در نظر گرفت. نمره قصد NCPI منعکس‌کننده اولویت‌بندی‌های مختلف برخی کشورها برای بهره‌برداری از قابلیت‌های سایبری خاص است. در اینجا فرض بر این است که هر کشور تنها در صورتی در حوزه‌ای خاص (مثلاً نظارت ملی) سرمایه‌گذاری می‌کند و قابلیت‌های سایبری خود را به کار می‌گیرد که قصد آن برای انجام این کار نسبتاً زیاد باشد.

## ۷-۴) تغییرات ایجادشده در روش‌شناسی NCPI ۲۰۲۲

امسال ۲۹ نشانگر قابلیت را به کار گرفتیم و سپس آن‌ها را به شکل «شاخص قابلیت سایبری» میانگین‌گیری کردیم. درست مانند سال ۲۰۲۰، برخی متریک‌ها در بیش از یک هدف نقش دارند. اگر اطلاعات جدیدی برای نشانگرهای به‌کاررفته در سال ۲۰۲۰ موجود بود، آن‌ها را به‌روزرسانی کردیم. به علاوه، برای لحاظ‌کردن هشت هدف، برخی نشانگرهای جدید را هم افزودیم.

### ۷-۴-۱) لحاظ کردن هدف هشتم: انباشت و محافظت از ثروت

در NCPI هشت هدف که کشورها خواهان دستیابی به آن‌ها با استفاده از روش‌های سایبری هستند، مشخص شده است. در شاخص ۲۰۲۰ سنجه‌ای برای هدف هشتم، یعنی انباشت و محافظت از ثروت، ارائه نداده بودیم. این از قلم افتادن، تا حدودی به دلیل دشواری در گردآوری داده‌های مربوط به آن هدف بود. سال ۲۰۲۲ گرچه همچنان دستیابی به داده‌های مفید برای این هدف دشوار است، از نشانگری واحد برای اندازه‌گیری قابلیت کشور در دستیابی به این هدف استفاده کردیم که هرچند ناقص است؛ اما بُعدی بهبودیافته از این شاخص ایجاد می‌کند.

انباشت و محافظت از ثروت را به مثابه استفاده از عملیات سایبری برای انباشت ثروت تعریف کردیم. این امر شامل سرقت با استفاده از روش‌های سایبری، از جمله باج‌افزار، است. درخواست باج برای عدم انتشار اطلاعات به دست آمده از طریق رخنه داده‌ها و حمله به زیرساخت دیجیتال مؤسسات مالی صورت می‌گیرد.

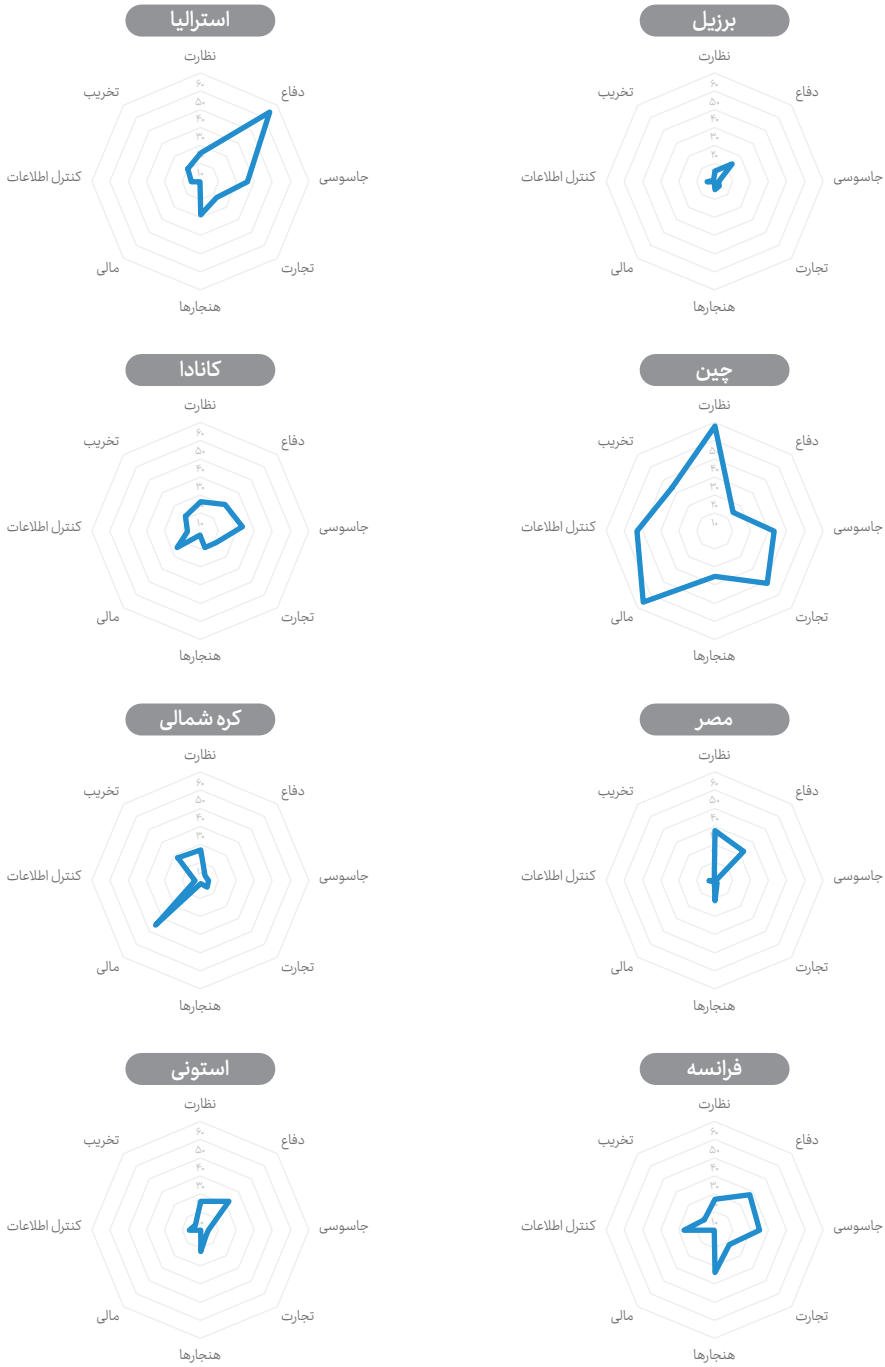
کشورهایی که در این حوزه نمره‌های بالا گرفتند عبارت‌اند از: چین، کره شمالی و ویتنام. ناهنجاری موجود در این رتبه‌بندی، عدم قرارگیری روسیه در رتبه‌های بالاست. اگرچه طبق گزارش‌ها تعدادی از گروه‌های باج‌افزاری شناخته‌شده، در روسیه و کشورهای روس زبان مستقر هستند؛ اما تولید نقدینگی از حملات سایبری در زمره مقاصد آشکار، منتشرشده یا بیان‌شده از سوی دولت روسیه نیست. به‌علاوه، در این شاخص رابطه نزدیک میان گروه‌های مجرمان سایبری یا جانشینان آن‌ها و حکومت، برای نمره‌دهی مدنظر قرار نگرفته است. همکاری میان حکومت روسیه و گروه‌های مجرم، رویکردی راهبردی و تاکتیکی در قدرت سایبری و آرمان‌های خط‌مشی جهانی این حکومت است.

در شاخص ۲۰۲۲ برای این هدف، تعداد حملات شناسایی‌شده موجود در پایگاه‌های داده‌های متن‌باز با هدف منافع مالی، بررسی شده است.

# ۸) پیوست ب:

شاخص قدرت سایبری ملی، نمودارهای نتایج

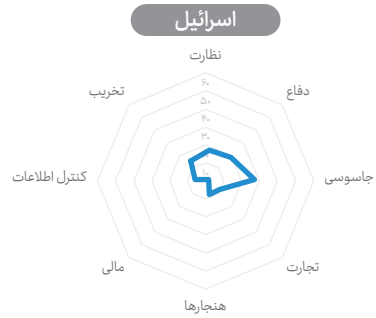
**شکل ۴)** نمودار راداری قدرت سایبری ملی برحسب هدف



هند


آلمان


اسرائیل




ایران


ژاپن


ایتالیا

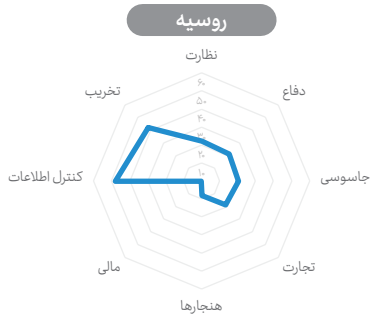

مالزی


لیتوانی

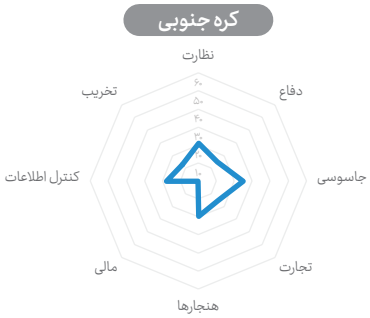
## نیوزیلند


## هلند

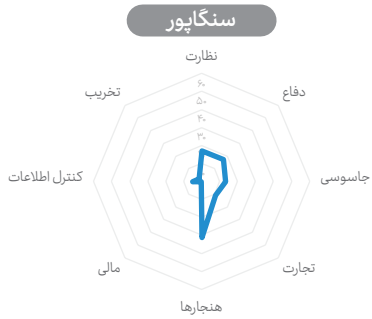

## روسیه



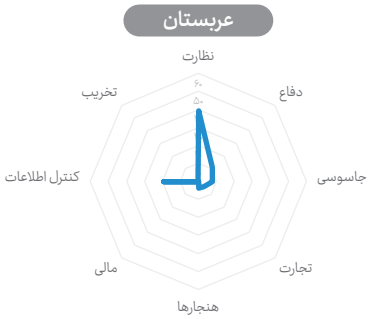

## کره جنوبی



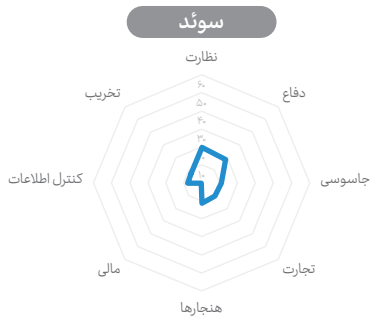

## سنگاپور




## عربستان




## سوئد



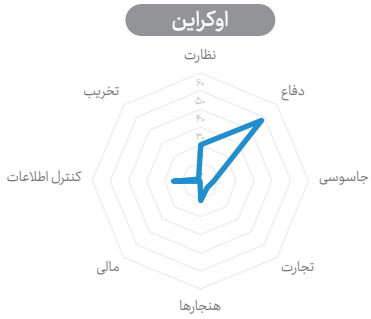

## اسپانیا

## ترکیه


## سوئیس

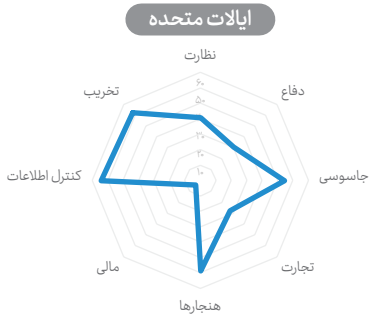

## بریتانیا


## اوکراین

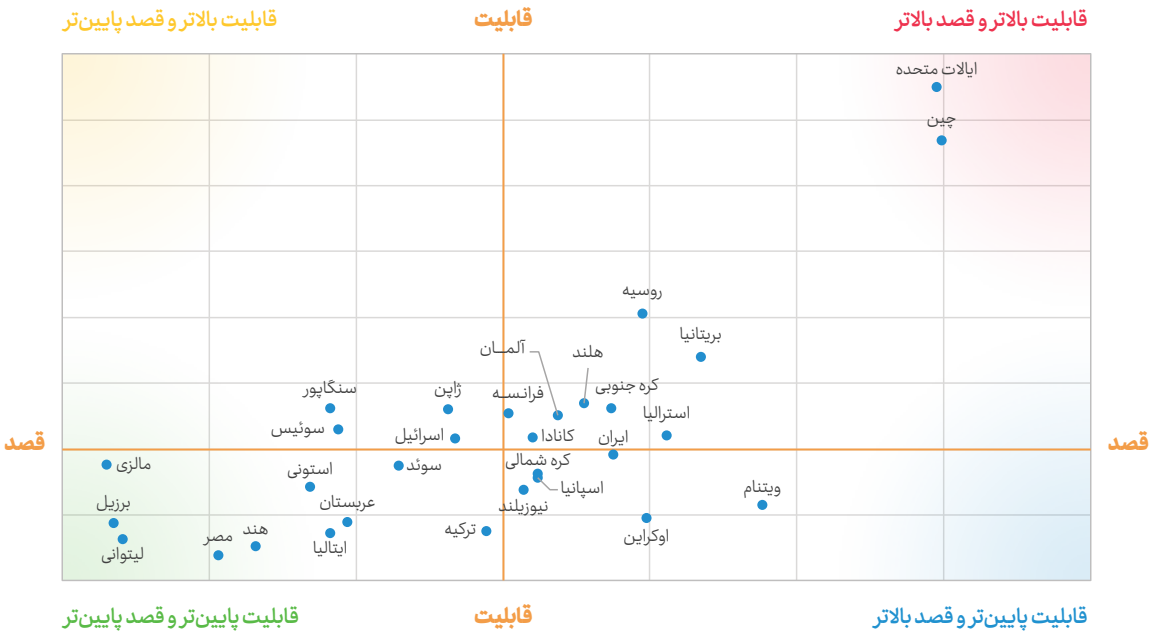



## ویتنام

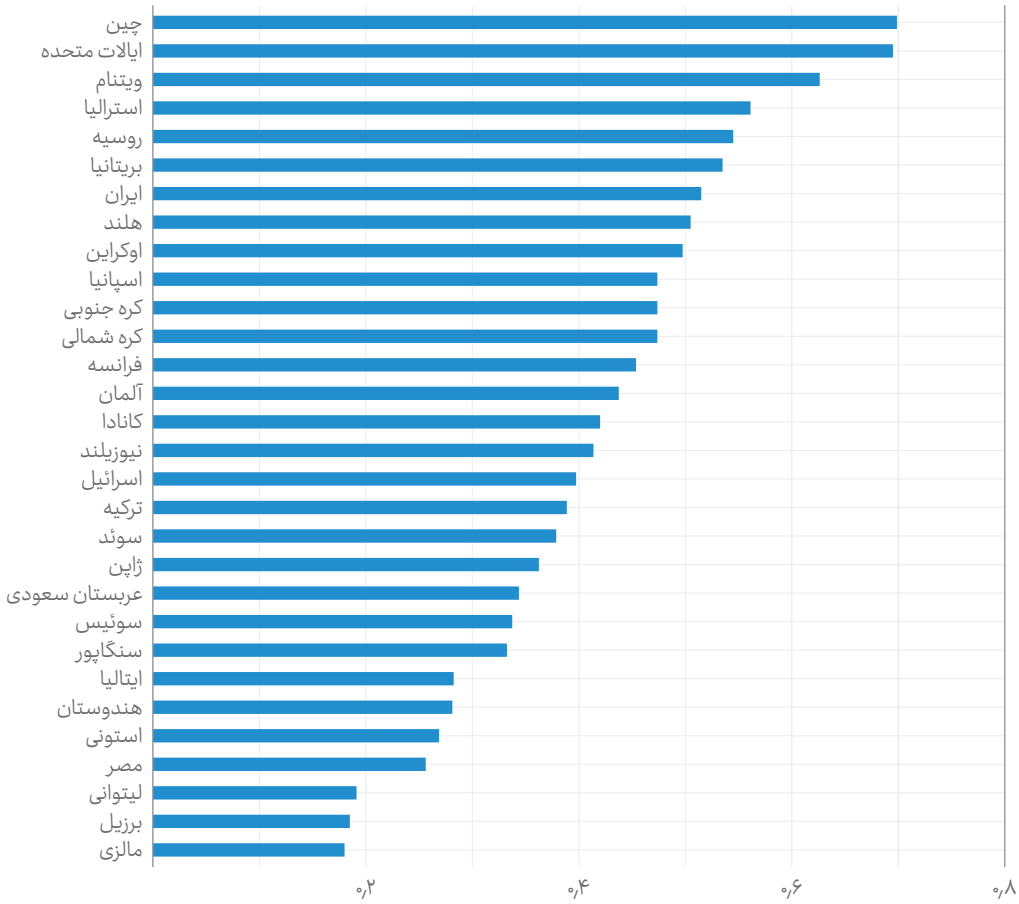

## ایالات متحده



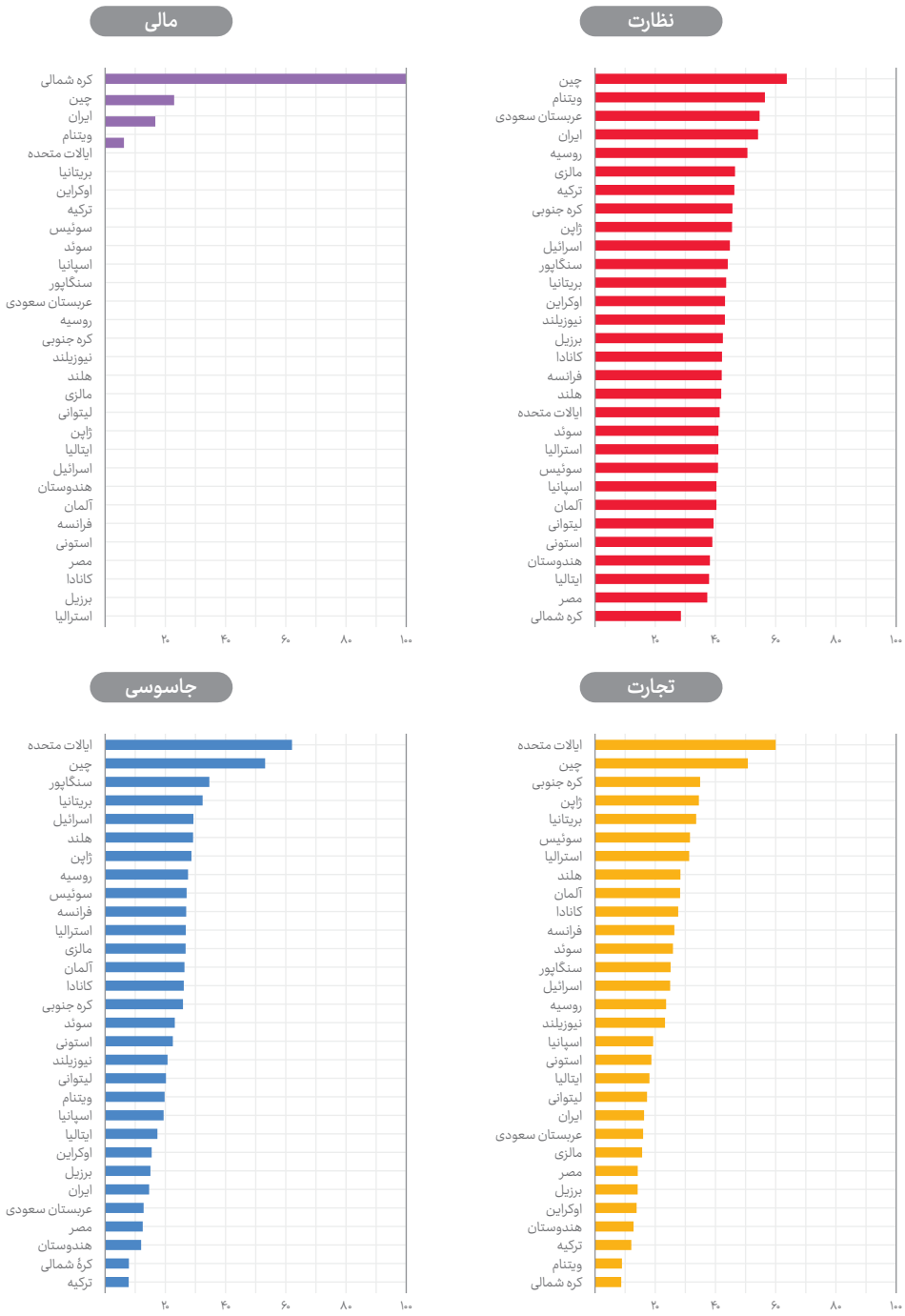
شکل ۵) نمودار پراکندگی قابلیت در مقابل قصد



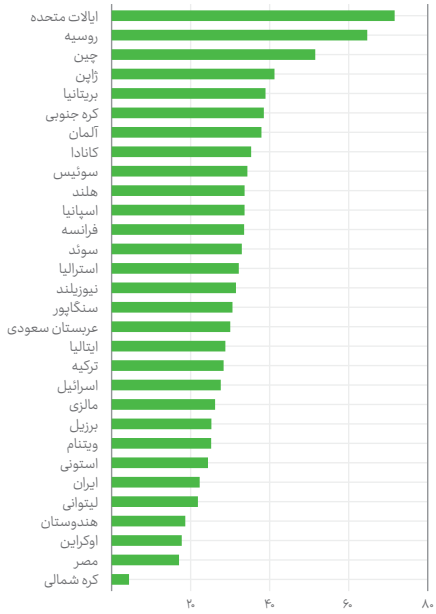
**شکل ۶)** رتبه‌بندی شاخص قصد سایبری



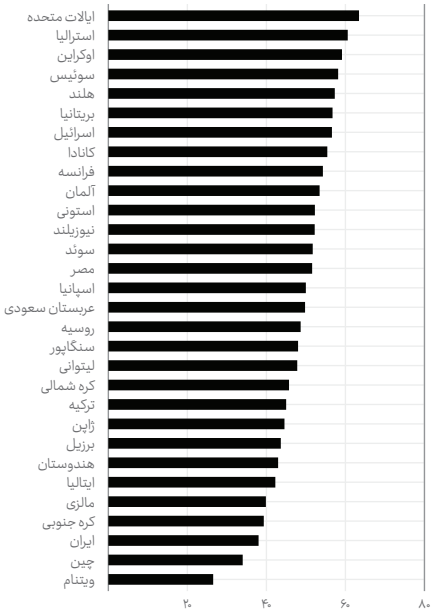
## شکل ۷) نتایج برحسب هدف (قابلیت)



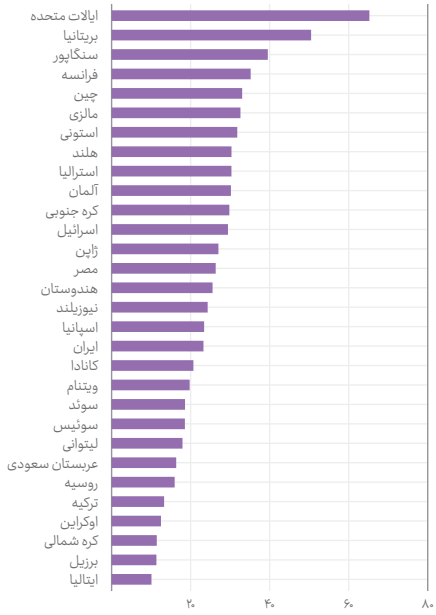
## کنترل اطلاعات



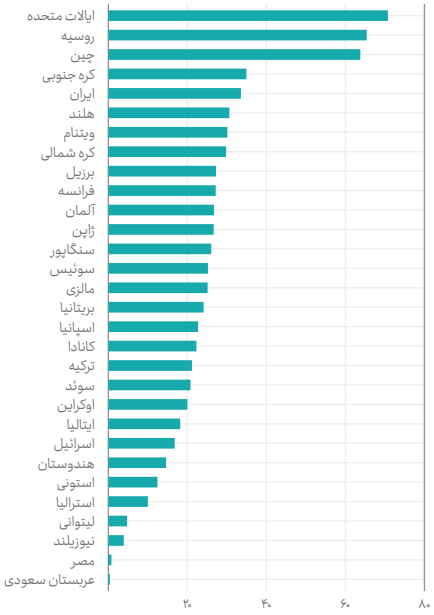

## دفاعی



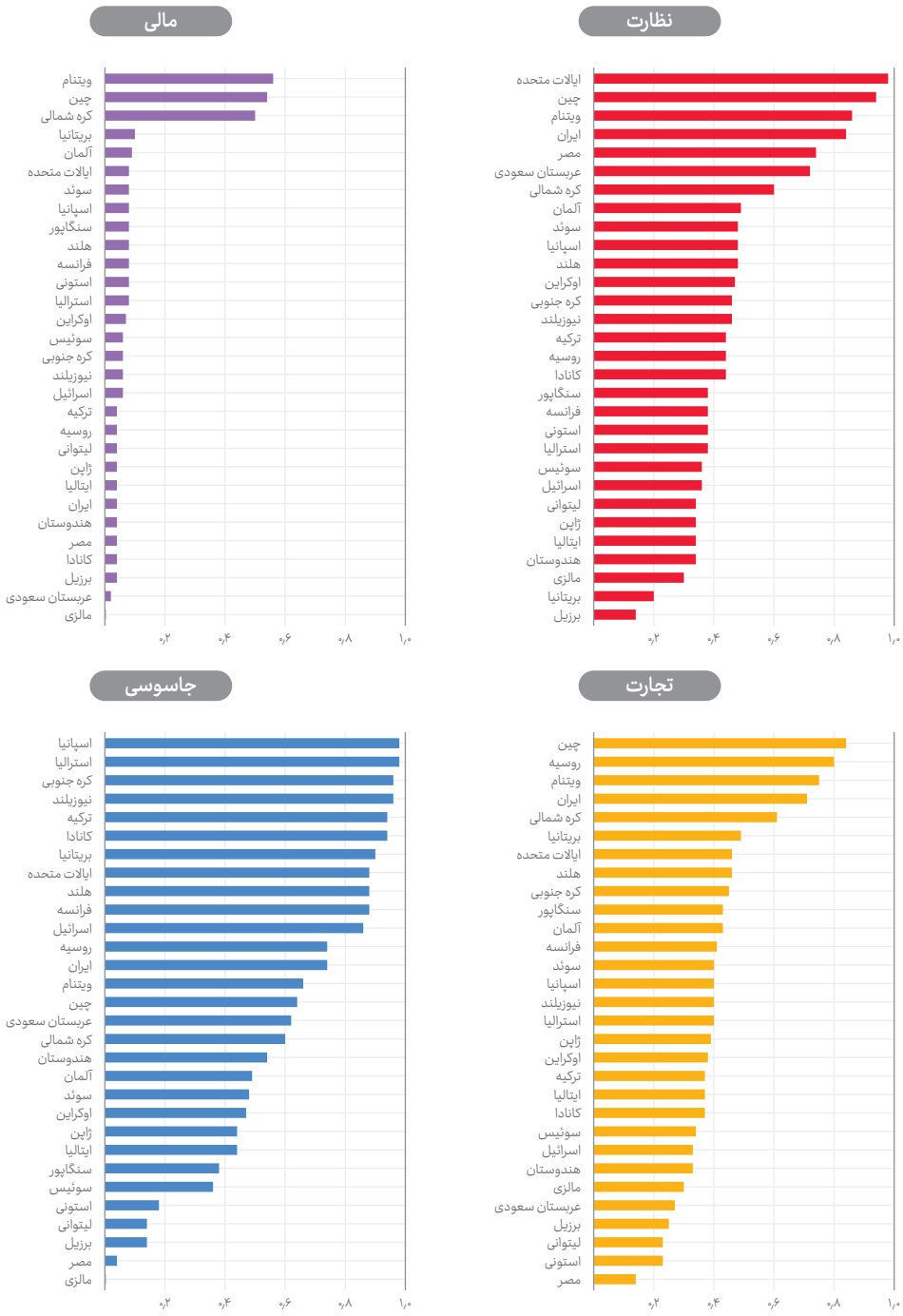

## هنجارها



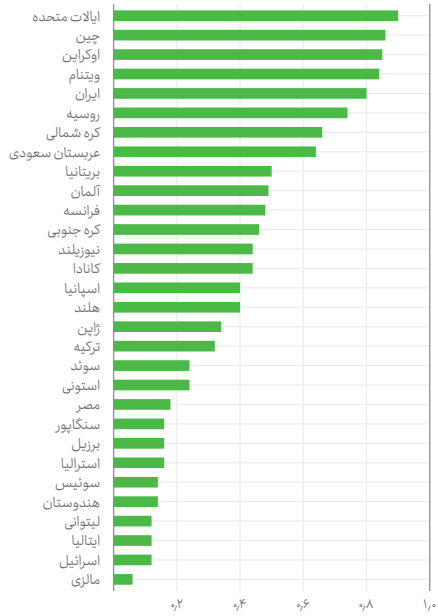

## تهاجمی



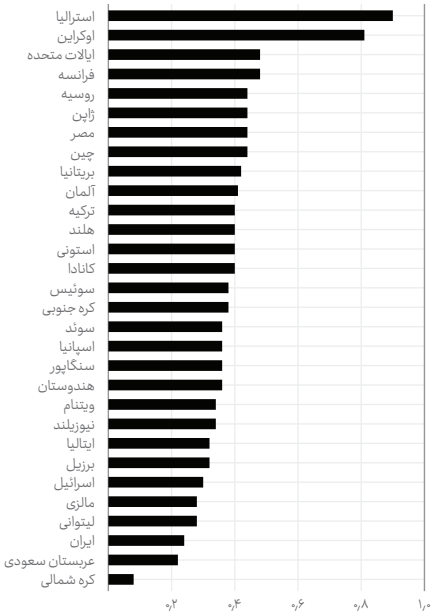
## شکل ۸) نتایج برحسب هدف (قصد)



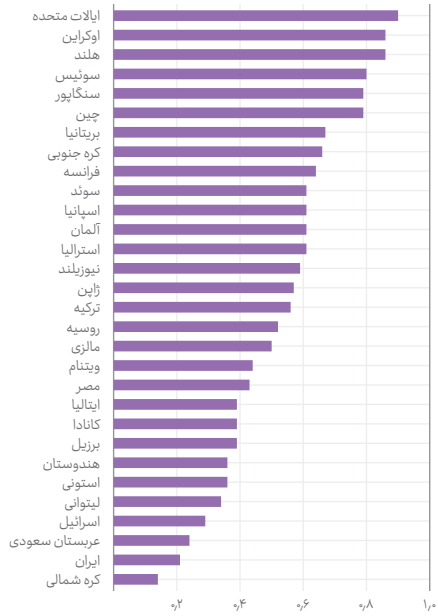
## کنترل اطلاعات



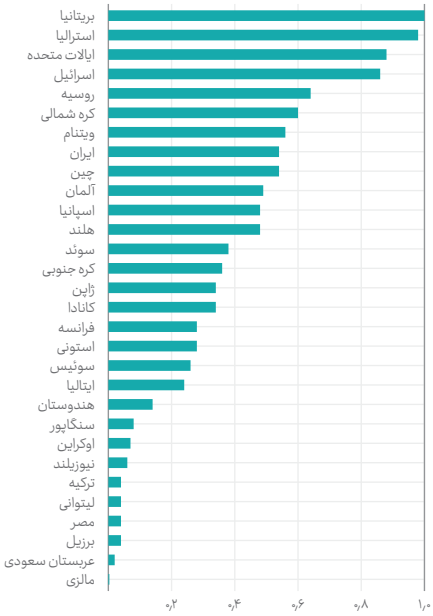

## دفاعی




## هنجارها




## تهاجمی



# ۹) پیوست ج:
## شرح تفصیلی نشانگرهای قصد

### ۹-۱) نشانگرهای قصد برحسب هدف

#### ۹-۱-۱) انباشت و محافظت از ثروت

جدول ۵)

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| مشاهده‌شده در حمله سایبری منتسب | برخلاف سایر نشانگرهای قصد که نشان‌دهنده قصدی خاص هستند (و نیازمند برنامه‌ریزی از قبل و آمادگی هستند)، می‌توان قصد کلی را (که احتمالی از انجام یک فرمان دارد) از اقدامات کشور استنتاج نمود. | استفاده از ارقام ردیاب عملیات سایبری شورای روابط خارجی برای سنجش اینکه آیا به کشوری یک حمله یا بیشتر منتسب شده است [برای اینکه مشخص شود چه تعداد حمله به یک کشور منتسب شده است]؟ | مشاهده‌شده در یک حمله یا بیشتر: بله/خیر |

## ۹-۱-۲) کنترل و دستکاری محیط اطلاعاتی

جدول ۶)

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| قدرت قانون حفاظت از داده | نظام حفاظت از داده در هر کشور تا چه اندازه معین و تعریف‌شده است. | استفاده از رتبه‌بندی محافظت از داده دی‌ال‌ای پایپر[۱] برای هر کشور<br>https: //www. /dlapiperdataprotection.com | دشوار[۲]/ سخت[۳]/ متعادل/ محدود/ فاقد اطلاعات |
| آیا برنامه‌ریزی سایبری نظامی [یعنی برنامه‌های مربوط به ارتش سایبری][۴] یا اسناد استراتژی حکومت و یا برنامه‌ریزی نظامی یا اسناد استراتژی کلان‌تر تأیید می‌کنند که آن کشور دارای قابلیت‌های سایبری برای کنترل و دستکاری محیط اطلاعاتی است؟ | ارتش‌ها، درست مانند همه بوروکراسی‌های بزرگ، به سلسله مراتب واضح و برنامه‌های کارآمد متکی‌اند. ارتش تنها در صورتی می‌تواند به صورت کارآمد عوامل سایبری را به کار گیرد که فرماندهان چگونگی و زمان استفاده از آن‌ها را درک کنند و بدانند که این عوامل چگونه قابلیت‌های سنتی را تکمیل می‌کنند. علاوه‌براین، همه ارتش‌ها، درباره قابلیت‌هایی که خواهان دستیابی به آن‌ها هستند، با هزینه-فرصت‌هایی مواجه‌اند و از آن‌ها انتظار می‌رود که ارزش عوامل سایبری را در اسناد برنامه‌ریزی دفاع ملی توجیه کنند. | تحلیل حضور آنلاین وزارت دفاع (MOD) و/یا نیروهای مسلح هر کشور برای یافتن اسناد مربوطه. اسناد مربوطه عبارت‌اند از: برنامه‌های دفاعی، استراتژی‌های دفاعی، دکترین نظامی، وایت‌پیپرهای[۵] دفاعی، طرح‌های دفاع سایبری، استراتژی‌های دفاع سایبری، دکترین سایبری نظامی، وایت‌پیپرهای دفاع سایبری، بیانیه‌های رهبران ارشد ارتش، بیانیه‌های سیاستمداران وزارت دفاع درباره قابلیت‌های سایبری کشور. | بله/خیر |

۱) DLA Piper: شرکت حقوقی چندملیتی، (توضیح مترجم).

۲) Heavy

۳) Robust

۴) Cyber military planning

۵) White Papers: گزارش‌های دولت یا سایر نهادهای حکمران که اطلاعات یا پیشنهاده‌ای درخصوص یک موضوع ارائه می‌کنند (توضیح مترجم).

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا واحد یا فرماندهی سایبری نظامی حکومت تأیید می‌کند که کشور دارای قابلیت‌های سایبری برای کنترل و دستکاری محیط اطلاعاتی است؟ | داشتن واحد یا فرماندهی سایبری اختصاصی نشان می‌دهد که آن کشور خواهان بهبود و رشد تخصص سایبری نظامی خود و استخدام نیروهایی برای تأمین این نیاز است. با توجه به کمبود نیروهای سایبری ماهر که همه کشورها با آن مواجه هستند، واحدهای سایبری نظامی باید برای جذب بهترین نیروها رقابت کنند. بنابراین واحدهای نظامی مایل به شرح نقش قابلیت‌های خود هستند. | تحلیل حضور آنلاین نیروی سایبری نظامی هر کشور برای سنجش اینکه آیا این هدف را تأیید می‌کند یا خیر. به علاوه، اظهارنظرهای عمومی سیاستمداران ملی و رهبران نظامی سایبری ارشد درباره قابلیت‌هایی که واحدهای نظامی خاص دارند، بررسی می‌شود. | بله/خیر |
| آیا آژانس اطلاعات سیگنال[1] یا سرویس اطلاعاتی خارجی حکومت تأیید می‌کند که کشور دارای قابلیت‌های سایبری برای کنترل و دستکاری محیط اطلاعاتی است؟ | تأیید اینکه آژانس اطلاعات حکومت دارای مأموریت سایبری است. | تحلیل حضور آنلاین آژانس اطلاعاتی هر کشور برای سنجش اینکه آیا این هدف را تأیید می‌کند یا خیر. به علاوه اظهارنظرهای عمومی سیاستمداران ملی و رهبران ارشد آژانس‌های اطلاعاتی سایبری درباره قابلیت‌هایی که جامعه اطلاعاتی دارد بررسی می‌شود. | بله/خیر |
| پیوستگی (انسجام) هدف: آیا این هدف در بیش از یک استراتژی دنبال می‌شود؟ | کشورهایی که هدف خاصی را در خلال چندین استراتژی دنبال می‌کنند، تعهد خود برای دستیابی به آن هدف را نشان می‌دهند و درک آن‌ها از این امر احتمالاً بالاتر است. | مقایسه اهداف فهرست‌شده در جدیدترین استراتژی [مثلاً سند استراتژی یا اظهارات استراتژیست‌های کشور ] با اهداف فهرست‌شده در استراتژی قبلی (در صورت وجود). | هدف در بیش از یک استراتژی موجود است: بله/خیر |
| مشاهده‌شده در حمله سایبری منتسب | برخلاف سایر نشانگرهای قصد که نشان‌دهنده قصدی خاص هستند (و نیازمند برنامه‌ریزی از قبل و آمادگی هستند)، می‌توان قصد کلی را (که احتمالی از انجام یک فرمان دارد) از اقدامات کشور استنتاج نمود. | استفاده از ارقام ردیاب عملیات سایبری شورای روابط خارجی برای سنجش تعداد حمله‌های منتسب به یک کشور | مشاهده‌شده در یک حمله یا بیشتر: بله/خیر |

۱) signals intelligence agency: سازمانی که از طریق سایبر جاسوسی می‌کند یعنی از طریق سیستم‌های الکترونیکی و ارتباطاتی و رادارهای دشمن به اطلاعات مدنظر دست پیدا می‌کند (توضیح مترجم).

## ۹-۱-۳) تعیین هنجارهای سایبری و استانداردهای فنی بین‌المللی

جدول ۷)

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| حکومت مورد نظر در چند مورد از پنج جلسه مشاوره‌ای گذشته گروه متخصصان دولتی[۱] (GGE) سایبری سازمان ملل مشارکت داشته است؟ | کمیته اول مجمع عمومی سازمان ملل متحد در رابطه با خلع سلاح و امنیت ملی (از طریق گروه‌های متوالی متخصصان دولتی (GGEها) درباره پیشرفت‌های حاصله در حوزه اطلاعات و ارتباطات از راه دور در بستر امنیت ملی)، برخی از اولین کوشش‌ها برای دستیابی به اجماعی جهانی درباره هنجارهای الزام‌آور و غیرالزام‌آوری که بر محیط دیجیتال و رفتار دولت‌ها در کاربرد فاوا[۲] (ICT) اِعمال می‌شود را تسهیل کرده است. نمره بالاتر در این نشانگر حاکی از آن است که حکومت مربوطه در جلسات مشاوره‌ای GGE سازمان ملل مشارکت داشته است. | ارقام برداشت‌شده از: https: //www.unidir. org/files/publications/pdfs/the-unit-ed-nations-cy-berspace-and-in-ternation-al-peace-and-secu-rity-en-691.pdf | ۱ = پنج بار؛<br>۰/۸ = ۴ بار؛<br>۰/۶ = ۳ بار؛<br>۰/۴ = ۲ بار؛<br>۰/۲ = ۱ بار؛<br>۰ = عدم شرکت در جلسات |
| حکومت مربوطه در فاصله سال‌های ۲۰۱۵ تا ۲۰۱۹ چند بار در مجمع حکمرانی اینترنت[۳] (IGF) شرکت کرده است؟ | هدف از مجمع حکمرانی اینترنت (IGF) گردهم آوردن افراد از گروه‌های مختلف ذی‌نفعان به عنوان افرادی برابر است که در بحث‌های مربوط به مسائل خط‌مشی عمومی در رابطه با اینترنت مشارکت می‌کنند. اگرچه هیچ‌گونه نتیجه[۴] توافق‌شده‌ای وجود ندارد، IGF برای خط‌مشی‌گذاران در بخش‌های عمومی و خصوصی آگاهی‌بخش و الهام‌بخش است. نمایندگان در جلسات سالیانه به بحث، تبادل اطلاعات و اشتراک‌گذاری به‌روش‌ها[۵] با یکدیگر می‌پردازند. IGF تسهیل‌کننده نوعی درک مشترک از نحوه بیشینه‌سازی فرصت‌های اینترنتی و مقابله با ریسک‌ها و چالش‌های حاصله است. | ارقام برداشت‌شده از: https: //www.intgovforum. org/multilingual/con-tent/ mag-2020-members and https: //www.intgovforum.org/multilingual/igf-2020-1st-mag-attendees | ۰/۲۵ برای هر یک از بخش‌های دولت/ جامعه مدنی/ جامعه فنی/ بخش خصوصی |

۱) Government Group of Experts

۲) Information and Communications Technology

۳) Internet Governance Forum

۴) Outcome

۵) Good practices

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا حکومت مربوطه در فعالیت‌های قابلیت‌سازی «انجمن جهانی تخصص سایبری»[۱] (GFCE) مشارکت کرده است؟ | به گفته GFCE، مأموریت این انجمن تحکیم «همکاری بین‌المللی در زمینه قابلیت‌سازی سایبری به وسیله اتصال نیازها، منابع و تخصص و با دسترس‌پذیر کردن دانش کاربردی برای جامعه جهانی» است. مشارکت حکومت‌ها حاکی از تمایل آن‌ها به کمک در اشتراک‌گذاری بهترین اقدامات و هنجارهای[۲] سایبری است. | ارقام برداشت‌شده از: https: //thegfce.org/ /member-overview | بله/خیر |
| نرخ مشارکت در کمیته‌های فنی مشترک[۳] فاوا در ISO/IEC چقدر است؟ | سازمان بین‌المللی استانداردسازی[۴] (ISO) و کمیسیون بین‌المللی الکتروتکنیک[۵] (IEC) مشترکاً استانداردهای بین‌المللی مبتنی بر اجماع و مرتبط با بازار را برای فناوری‌های اطلاعات ارائه می‌دهند. شکل‌دهی و پیروی از کمیته‌های فنی مشترک ISO/IEC حاکی از تعهد به بهبود این عناصر در داخل کشور است. بالا بودن نمره مربوطه حاکی از فعالیت بیشتر حکومت مورد نظر در تعیین استانداردهای بین‌المللی است که برای تعامل‌پذیری بازار داخلی آن با بازارهای بین‌المللی بسیار مهم است. | https: //www.iso.org/technical-committees. html | تعداد کمیته‌های فنی مشترک ISO/IEC (یا X) یکی از اعضاء تقسیم بر ۲۲ (تعداد کل کمیته‌های فنی مشترک ISO/IEC). نمره حاصله درصدی از کمیته‌های فنی است که حکومت مربوطه در آن‌ها حضور داشته است. |

۱) Global Forum for Cyber Expertise

۲) Best practice and norms

۳) Joint Technical Committees (JTC)

۴) International Organization for Standardization

۵) International Electrotechnical Commission

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| کیفیت مشارکت در هر ۲۲ کمیته فنی مشترک ISO/IEC چگونه است؟ | سازمان بین‌المللی استانداردسازی (ISO) و کمیسیون بین‌المللی الکتروتکنیک (IEC) مشترکاً استانداردهای بین‌المللی مبتنی بر اجماع و مرتبط با بازار را برای فناوری‌های اطلاعات ارائه می‌دهند. شکل‌دهی و پیروی از کمیته‌های فنی مشترک ISO/IEC حاکی از تعهد به بهبود این عناصر در داخل کشور است. بالا بودن نمره مربوطه حاکی از «اقتدار رسمی بیشتر حکومت به طور متوسط در کمیته‌های فنی» و «مشارکت بیشتر آن حکومت و صنعت آن در شکل دادن به دستورکار[1] استانداردهای بین‌المللی فاوا» است. | https: //www.iso.org/technical-committees. html | به هر کشور بر مبنای نقش آن، نمره‌ای برای هر کمیته فنی تعلق گرفته است. نمرات به شرح ذیل اختصاص یافتند:<br>۱ = دبیرخانه؛<br>۰/۷۵ = شرکت‌کننده؛<br>۰/۵ = ناظر؛<br>۰/۲۵ = عضو کمیته‌های فنی مشترک ISO/IEC؛<br>۰ = عدم وابستگی. سپس میانگین مشارکت در سطح همه کمیته‌ها مشخص شد تا نمره نهایی بین ۰ و ۱ باشد. |
| کیفیت مشارکت حکومت در گروه‌های مطالعاتی شماره ۱۳ (شبکه‌های آینده)، ۱۷ (امنیت) و ۲۰ (اینترنت اشیاء و شهرهای هوشمند) اتحادیه بین‌المللی ارتباطات راه دور[2] (ITU) چگونه است؟ | یکی دیگر از نهادهای بین‌المللی که دارای نمایندگان ملی به‌منظور تعیین استانداردهای فنی برای فناوری‌های اطلاعات است، اتحادیه بین‌المللی ارتباطات راه دور است. فرض ما بر این است که بالاتر بودن نمره به معنای بالاتر بودن کیفیت مشارکت حکومت و نفوذ بیشتر آن در تعیین استانداردها و هنجارهای بین‌المللی، به‌ویژه در فاوا است (زیرا این امر بیشتر دولت‌محور است تا صنعت‌محور). | https://www.itu.int/en/ITU-T/study-groups/2017-2020/Pages/default.aspx | به هر کشور بر مبنای مشارکت آن در هر یک از سه گروه مطالعاتی نمره‌ای تعلق گرفت. این نمره به شرح ذیل اختصاص یافت:<br>۱ = رئیس؛<br>۰/۷۵ = معاون رئیس؛<br>۰/۵ = رئیس WP؛<br>۰/۲۵ = کشورهای عضو اتحادیه بین‌المللی مخابرات.<br>سپس میانگین مشارکت کشور در همه این سه گروه گرفته شد و نمره نهایی بین ۰ و ۱ است. |
| آیا حکومت مربوطه در تمرین‌های دفاع سایبری دو یا چند جانبه شرکت کرده است؟ | حاکی از تمایل به اشتراک‌گذاری تخصص و تلاش‌های قابلیت‌سازی با سایر کشورها است. | جستجوی اینترنتی در وبسایت‌های دولتی و منابع معتبر برای یافتن ارجاعاتی درباره مشارکت در تمرین‌های دفاع سایبری دو یا چند جانبه. | بله/خیر |

۱) Agenda

۲) International Telecommunication Union (ITU)

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| پیوستگی (انسجام) هدف: آیا این هدف در بیش از یک استراتژی دنبال می‌شود؟ | کشورهایی که هدف خاصی را در خلال چندین استراتژی دنبال می‌کنند، تعهد خود برای دستیابی به آن هدف را نشان می‌دهند و درک آن‌ها از این امر احتمالاً بالاتر است. | مقایسه اهداف فهرست‌شده در جدیدترین استراتژی با اهداف فهرست‌شده در استراتژی قبلی (در صورت وجود). | هدف در بیش از یک استراتژی موجود است: بله/خیر |
| آیا تعیین هنجارهای سایبری و استانداردهای فنی بین‌المللی در استراتژی سایبری کشور تصدیق شده است یا خیر: لحاظ کردن نمره استراتژی [در صورت وجود موضوع تعیین هنجارها در استراتژی سایبری کشور] | نگاه کنید به جدول نمره استراتژی. | نگاه کنید به جدول نمره استراتژی. | نگاه کنید به جدول نمره استراتژی. |
| آیا تعیین هنجارهای سایبری و استانداردهای فنی بین‌المللی در استراتژی سایبری کشور تصدیق شده است یا خیر: لحاظ کردن نمره امور مالی | حکومت مربوطه به اندازه کافی به ارائه استراتژی خود به صندوق‌های ملی مناسب برای تأمین خروجی‌های خود متعهد است. | حکومت از زمان انتشار جدیدترین استراتژی اعلام کرده است که بودجه سایبری را افزایش می‌دهد. | بله/خیر |

### ۹-۱-۴) تخریب یا ازکارانداختن زیرساخت یا قابلیت‌های دشمنان

جدول ۸)

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا برنامه‌ریزی سایبری نظامی [یعنی برنامه‌های مربوط به ارتش سایبری] یا اسناد استراتژی حکومت و یا برنامه‌ریزی نظامی یا اسناد استراتژی کلان‌تر تأیید می‌کنند که آن کشور دارای قابلیت‌های سایبری مخرب است؟ | ارتش‌ها، درست مانند همه بوروکراسی‌های بزرگ، به سلسله مراتب واضح و برنامه‌های کارآمد متکی‌اند. ارتش تنها در صورتی می‌تواند به صورت کارآمد عوامل سایبری را به کار گیرد که فرماندهان چگونگی و زمان استفاده از آن‌ها را درک کنند و بدانند که این عوامل چگونه قابلیت‌های سنتی را تکمیل می‌کنند. علاوه بر این، همه ارتش‌ها، درباره قابلیت‌هایی که خواهان دستیابی به آن‌ها هستند، با هزینه-فرصت مواجهند و از آن‌ها انتظار می‌رود که ارزشی که آن عوامل سایبری به همراه دارد را در اسناد برنامه‌ریزی دفاع ملی توجیه کنند. | تحلیل حضور آنلاین وزارت دفاع (MOD) و/یا نیروهای مسلح هر کشور برای یافتن اسناد مربوطه. اسناد مربوطه عبارت‌اند از: برنامه‌های دفاعی، استراتژی‌های دفاعی، دکترین نظامی، وایت‌پیپرهای دفاعی، طرح‌های دفاع سایبری، استراتژی‌های دفاع سایبری، دکترین سایبری نظامی، وایت‌پیپرهای دفاع سایبری، بیانیه‌های رهبران ارشد ارتش، بیانیه‌های سیاستمداران وزارت دفاع درباره قابلیت‌های سایبری کشور | بله/خیر |
| آیا واحد یا فرماندهی سایبری نظامی حکومت تأیید می‌کند که کشور دارای قابلیت‌های سایبری مخرب است؟ | داشتن واحد یا فرماندهی سایبری اختصاصی نشان می‌دهد که آن کشور خواهان بهبود و رشد تخصص سایبری نظامی خود و استخدام نیروهایی برای تأمین این نیاز است. با توجه به کمبود نیروهای سایبری ماهر که همه کشورها با آن مواجهند، واحدهای سایبری نظامی باید برای جذب بهترین نیروها رقابت کنند. بنابراین واحدهای نظامی مایلند شرح دهند که چه نقشی ایفا می‌کنند و چه قابلیت‌هایی ارائه می‌کنند. | تحلیل حضور آنلاین نیروی سایبری نظامی هر کشور برای سنجش اینکه آیا این هدف را تأیید می‌کند یا خیر. به علاوه، اظهارنظرهای عمومی سیاستمداران ملی و رهبران نظامی سایبری ارشد درباره قابلیت‌هایی که واحدهای نظامی خاص دارند بررسی می‌شود. | بله/خیر |

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا آژانس اطلاعات سیگنال یا سرویس اطلاعاتی خارجی حکومت تأیید می‌کند که کشور دارای قابلیت‌های سایبری مخرب است؟ | تأیید اینکه آژانس اطلاعات حکومت دارای مأموریت سایبری است. | تحلیل حضور آنلاین آژانس اطلاعاتی هر کشور برای سنجش اینکه آیا این هدف را تأیید می‌کند یا خیر. به علاوه اظهارنظرهای عمومی سیاستمداران ملی و رهبران ارشد آژانس‌های اطلاعاتی سایبری درباره قابلیت‌هایی که جامعه اطلاعاتی دارد بررسی می‌شود. | بله/خیر |
| پیوستگی (انسجام) هدف: آیا این هدف در بیش از یک استراتژی دنبال می‌شود؟ | کشورهایی که هدف خاصی را در خلال چندین استراتژی دنبال می‌کنند، تعهد خود برای دستیابی به آن هدف را نشان می‌دهند و درک آن‌ها از این امر احتمالاً بالاتر است. | مقایسه اهداف فهرست‌شده در جدیدترین استراتژی با اهداف فهرست‌شده در استراتژی قبلی (در صورت وجود). | هدف در بیش از یک استراتژی موجود است: بله/خیر |
| مشاهده‌شده در حمله سایبری منتسب | برخلاف سایر نشانگرهای قصد که نشان‌دهنده قصدی خاص هستند (و نیازمند برنامه‌ریزی از قبل و آمادگی هستند)، می‌توان قصد کلی را (که احتمالی از انجام یک فرمان دارد) از اقدامات کشور استنتاج نمود. | استفاده از ارقام ردیاب عملیات سایبری شورای روابط خارجی برای سنجش تعداد حمله‌های منتسب به یک کشور. | مشاهده‌شده در یک حمله یا بیشتر: بله/خیر |

## ۹-۱-۵) گردآوری اطلاعات پنهان (جاسوسی) خارجی برای امنیت ملی

جدول ۹)

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا برنامه‌ریزی سایبری نظامی [یعنی برنامه‌های مربوط به ارتش سایبری] یا اسناد استراتژی حکومت و یا برنامه‌ریزی نظامی یا اسناد استراتژی کلان‌تر تأیید می‌کنند که آن کشور دارای قابلیت‌های سایبری برای گردآوری اطلاعات پنهان (جاسوسی) است؟ | ارتش‌ها، درست مانند همه بوروکراسی‌های بزرگ، به سلسله مراتب واضح و برنامه‌های کارآمد متکی‌اند. ارتش تنها در صورتی می‌تواند به صورت کارآمد عوامل سایبری را به کار گیرد که فرماندهان چگونگی و زمان استفاده از آن‌ها را درک کنند و بدانند که این عوامل چگونه قابلیت‌های سنتی را تکمیل می‌کنند. علاوه بر این، همه ارتش‌ها، درباره قابلیت‌هایی که خواهان دستیابی به آن‌ها هستند، با هزینه-فرصت مواجهند و از آن‌ها انتظار می‌رود که ارزشی که آن عوامل سایبری به همراه دارد را در اسناد برنامه‌ریزی دفاع ملی توجیه کنند. | تحلیل حضور آنلاین وزارت دفاع (MOD) و/یا نیروهای مسلح هر کشور برای یافتن اسناد مربوطه. اسناد مربوطه عبارت‌اند از: برنامه‌های دفاعی، استراتژی‌های دفاعی، دکترین نظامی، وایت‌پیپرهای دفاعی، طرح‌های دفاع سایبری، استراتژی‌های دفاع سایبری، دکترین سایبری نظامی، وایت‌پیپرهای دفاع سایبری، بیانیه‌های رهبران ارشد ارتش، بیانیه‌های سیاستمداران وزارت دفاع درباره قابلیت‌های سایبری کشور. | بله/خیر |
| آیا واحد یا فرماندهی سایبری نظامی حکومت تأیید می‌کند که کشور دارای قابلیت‌های سایبری برای گردآوری اطلاعات پنهان (جاسوسی) است؟ | داشتن واحد یا فرماندهی سایبری اختصاصی نشان می‌دهد که آن کشور خواهان بهبود و رشد تخصص سایبری نظامی خود و استخدام نیروهایی برای تأمین این نیاز است. با توجه به کمبود نیروهای سایبری ماهر که همه کشورها با آن مواجهند، واحدهای سایبری نظامی باید برای جذب بهترین نیروها رقابت کنند. بنابراین واحدهای نظامی مایلند شرح دهند که چه نقشی ایفا می‌کنند و چه قابلیت‌هایی ارائه می‌کنند. | تحلیل حضور آنلاین نیروی سایبری نظامی هر کشور برای سنجش اینکه آیا این هدف را تأیید می‌کند یا خیر. به علاوه، اظهارنظرهای عمومی سیاستمداران ملی و رهبران نظامی سایبری ارشد درباره قابلیت‌هایی که واحدهای نظامی خاص دارند بررسی می‌شود. | بله/خیر |

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا آژانس اطلاعات سیگنال یا سرویس اطلاعاتی خارجی حکومت تأیید می‌کند که کشور دارای قابلیت‌های سایبری برای گردآوری اطلاعات پنهان (جاسوسی) است؟ | تأیید اینکه آژانس اطلاعات حکومت دارای مأموریت سایبری است. | تحلیل حضور آنلاین آژانس اطلاعاتی هر کشور برای سنجش اینکه آیا این هدف را تأیید می‌کند یا خیر. به علاوه اظهارنظرهای عمومی سیاستمداران ملی و رهبران ارشد آژانس‌های اطلاعاتی سایبری درباره قابلیت‌هایی که جامعه اطلاعاتی دارد بررسی می‌شود. | بله/خیر |
| پیوستگی (انسجام) هدف: آیا این هدف در بیش از یک استراتژی دنبال می‌شود؟ | کشورهایی که هدف خاصی را در خلال چندین استراتژی دنبال می‌کنند، تعهد خود برای دستیابی به آن هدف را نشان می‌دهند و درک آن‌ها از این امر احتمالاً بالاتر است. | مقایسه اهداف فهرست‌شده در جدیدترین استراتژی با اهداف فهرست‌شده در استراتژی قبلی (در صورت وجود). | هدف در بیش از یک استراتژی موجود است: بله/خیر |
| مشاهده‌شده در حمله سایبری منتسب | برخلاف سایر نشانگرهای قصد که نشان‌دهنده قصدی خاص هستند (و نیازمند برنامه‌ریزی از قبل و آمادگی هستند)، می‌توان قصد کلی را (که احتمالی از انجام یک فرمان دارد) از اقدامات کشور استنتاج نمود. | استفاده از ارقام ردیاب عملیات سایبری شورای روابط خارجی برای سنجش تعداد حمله‌های منتسب به یک کشور. | مشاهده‌شده در یک حمله یا بیشتر: بله/خیر |

## ۹-۱-۶) رشد شایستگی در حوزه فناوری تجاری و سایبری در سطح ملی

جدول ۱۰)

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| نرخ مشارکت در کمیته‌های فنی مشترک ISO/IEC برای فاوا چقدر است؟ | سازمان بین‌المللی استانداردسازی[۱] (ISO) و کمیسیون بین‌المللی الکتروتکنیک[۲] (IEC) مشترکاً استانداردهای بین‌المللی مبتنی بر اجماع و مرتبط با بازار را برای فناوری‌های اطلاعات ارائه می‌دهند. شکل‌دهی و پیروی از کمیته‌های فنی مشترک ISO/IEC حاکی از تعهد به بهبود این عناصر در داخل کشور است. بالا بودن نمره مربوطه حاکی از فعالیت بیشتر حکومت مورد نظر در تعیین استانداردهای بین‌المللی است که برای تعامل‌پذیری بازار داخلی آن با بازارهای بین‌المللی بسیار مهم است. | https: //www.iso.org/technical-committees.html | تعداد کمیته‌های فنی مشترک ISO/IEC (یا X) یکی از اعضاء تقسیم بر ۲۲ (تعداد کل کمیته‌های فنی مشترک ISO/IEC). نمره حاصله درصدی از کمیته‌های فنی است که حکومت مربوطه در آن‌ها حضور داشته است. |
| کیفیت مشارکت در هر ۲۲ کمیته فنی مشترک ISO/IEC چگونه است؟ | سازمان بین‌المللی استانداردسازی (ISO) و کمیسیون بین‌المللی الکتروتکنیک (IEC) مشترکاً استانداردهای بین‌المللی مبتنی بر اجماع و مرتبط با بازار را برای فناوری‌های اطلاعات ارائه می‌دهند. شکل‌دهی و پیروی از کمیته‌های فنی مشترک ISO/IEC حاکی از تعهد به بهبود این عناصر در داخل کشور است. بالا بودن نمره مربوطه حاکی از «اقتدار رسمی بیشتر حکومت به طور متوسط در کمیته‌های فنی» و «مشارکت بیشتر آن حکومت و صنعت آن در شکل دادن به دستورکار[۳] استانداردهای بین‌المللی فاوا» است. | https: //www.iso.org/technical-committees.html | به هر کشور بر مبنای نقش آن، نمره‌ای برای هر کمیته فنی تعلق گرفته است. نمرات به شرح ذیل اختصاص یافتند:<br>۱ = دبیرخانه؛<br>۰/۷۵ = شرکت‌کننده؛<br>۰/۵ = ناظر؛<br>۰/۲۵ = عضو کمیته‌های فنی مشترک ISO/IEC؛<br>۰ = عدم وابستگی. سپس میانگین مشارکت در سطح همه کمیته‌ها مشخص شد تا نمره نهایی بین ۰ و ۱ باشد. |

۱) International Organization for Standardization

۲) International Electrotechnical Commission

۳) Agenda

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا کشور مربوطه طرحی ابتکاری برای مشارکت بخش عمومی و خصوصی به‌منظور رشد دادن صنعت و نیروی کار سایبری خود و افزایش آگاهی از مسایل سایبری دارد؟ | سازمان‌های بخش خصوصی نمایش‌دهنده منبعی از قابلیت برای تقویت تخصص ملی هستند و علاوه بر آن نوعی بردار حمله‌اند[1] که دشمنان می‌توانند از آن بهره‌برداری کنند. بنابراین مهم است که کشورهای مختلف، بخش خصوصی خود را در این کار درگیر کنند و برای مقابله با تهدیدات و تأمین اهداف سایبری ملی با آن‌ها شریک شوند. | تحلیل حضور آنلاین هر کشور برای یافتن شواهدی از مشارکت عمومی-خصوصی با هدف افزایش دانش و مهارت‌های امنیت سایبری و متمرکز کردن کشور به شکل کلیتی فراگیر. | بله/خیر |
| آیا شواهدی وجود دارد که نشان دهند کشور دارای نوعی استراتژی نیروی کار سایبری و/یا استراتژی مدیریت زنجیره تأمین سایبری است؟ | ایجاد نیروی کار سایبری داخلی برای رشد شایستگی‌های سایبری و فناوری ملی بسیار مهم است. بنابراین کشورها باید استراتژی‌هایی برای ایجاد نیروی کار سایبری خود تدوین کنند و با استفاده از آن، استراتژی مدیریت زنجیره تأمین سایبری را تدوین نمایند. | تحلیل حضور آنلاین آژانس اطلاعاتی هرکشور برای سنجش اینکه آیا چنین هدفی را تأیید می‌کند یا خیر. | بله/خیر |
| آیا کشور از اعضاء «توافق شناخت معیارهای مشترک»[2] (CCRA) است؟ | معیارهای مشترک[3] استانداردی است که تضمین می‌کند «محصولات و پروفایل‌های محافظتی [و ارزشیابی‌های] فناوری اطلاعات (IT) برحسب استانداردهای بالا و منسجم ساخته و اجرا می‌شوند.» CCRA شناختی متقابل از ارزشیابی معیارهای مشترک ارائه می‌دهد و در نتیجه کشورها می‌توانند محصولات و خدمات را بدون ارزشیابی مجدد وارد و صادر کنند. | ارقام برداشت‌شده از: https: //www.com-moncriteriaportal. /org/ccra/members | بله/خیر |

۱) Attack vector: بردار حمله یک مسیر، روش یا سناریوی خاص است که می‌تواند برای نفوذ به یک سیستم فناوری اطلاعات مورد سوء استفاده قرار گیرد و در نتیجه امنیت آن را به خطر بیندازد (توضیح مترجم).

۲) Common Criteria Recognition Arrangement

۳) Common Criteria

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا کشور از اعضاء سیستم طرح‌های سنجش انطباق کمیسیون بین‌المللی الکتروتکنیک (IEC) برای اجزا و تجهیزات الکتروتکنیکی[1] (IECEE) است؟ | IECEE نوعی «سیستم صدور مجوز چندجانبه بر مبنای استانداردهای بین‌المللی IEC است. اعضاء آن در سرتاسر جهان از اصل شناخت متقابل (پذیرش دوجانبه) نتایج آزمایش برای کسب مجوز یا تأییدیه در سطوح ملی استفاده می‌کنند.» ملحق شدن به این نهاد باعث حذف موانع مربوط به مجوز در میان کشورها می‌شود و امکان صادرات و واردات محصولات امنیت سایبری و فناوری را برای آن‌ها فراهم می‌سازد. | ارقام برداشت‌شده از:<br>https: //www.iecee.org/dyn/ww-w/f?p=106: 40: 0 | بله/خیر |
| آیا کشور استراتژی یا برنامه‌ای درباره جلب سرمایه‌گذاری داخلی به سوی شرکت‌های سایبری یا رشد صادرات سایبری خود منتشر کرده است؟ | کشور به صورت فعالانه می‌کوشد تا درآمدهای صنعت امنیت سایبری را افزایش دهد. | جستجوی اینترنتی در وبسایت‌های دولت برای یافتن شواهدی از توصیه‌ها یا دستورالعمل‌های خاص برای صادرکنندگان [محصولات و خدمات] امنیت سایبری یا تلاش برای جلب سرمایه‌گذاران خارجی به‌منظور سرمایه‌گذاری در محصولات و شرکت‌های امنیت سایبری ملی. | بله/خیر |
| آیا شواهدی از سرمایه‌گذاری کشور در تحقیقات سایبری یا تأمین بودجه این تحقیقات موجود است؟ | سرمایه‌گذاری در تحقیق و توسعه یکی از مولفه‌های اساسی رشد قابلیت و ظرفیت امنیت سایبری است. | تحلیل حضور آنلاین هر کشور برای یافتن شواهدی از سرمایه‌گذاری خاص ملی در تحقیقات امنیت سایبری یا برای مشخص کردن اینکه دولت بودجه دانشگاه‌های ملی و مؤسسات تحقیقاتیِ دارای خروجی امنیت سایبری را تأمین می‌کند یا خیر. | بله/خیر |

۱) IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| پیوستگی (انسجام) هدف: آیا این هدف در بیش از یک استراتژی دنبال می‌شود؟ | کشورهایی که هدف خاصی را در خلال چندین استراتژی دنبال می‌کنند، تعهد خود برای دستیابی به آن هدف را نشان می‌دهند و درک آن‌ها از این امر احتمالاً بالاتر است. | مقایسه اهداف فهرست‌شده در جدیدترین استراتژی با اهداف فهرست‌شده در استراتژی قبلی (در صورت وجود). | هدف در بیش از یک استراتژی موجود است: بله/خیر |
| مشاهده‌شده در حمله سایبری منتسب | برخلاف سایر نشانگرهای قصد که نشان‌دهنده قصدی خاص هستند (و نیازمند برنامه‌ریزی از قبل و آمادگی هستند)، می‌توان قصد کلی را (که احتمالی از انجام یک فرمان دارد) از اقدامات کشور استنتاج نمود. | استفاده از ارقام ردیاب عملیات سایبری شورای روابط خارجی برای سنجش تعداد حمله‌های منتسب به یک کشور. | مشاهده‌شده در یک حمله یا بیشتر: بله/خیر |

## ۷-۱-۹) تقویت و بهبود دفاع سایبری

جدول ۱۱)

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا کشور مورد نظر برنامه امنیت سایبری منتشر کرده است که نحوه محافظت از سیستم‌های دولت و/ یا زیرساخت‌های حیاتی ملی را شرح دهد؟ | حتی تلاش‌های صورت‌گرفته برای محافظت از سیستم‌های IT دولت هم به مشارکت و برنامه‌ریزی فروشندگان بخش خصوصی نیاز دارد. برنامه یا استراتژی، وجود درکی شفاف و منسجم از الزامات و استانداردهایی که لازم است تأمین شوند را تضمین می‌کند. | تحلیل حضور آنلاین هر کشور برای طرح‌ها یا استراتژی‌های محافظت از زیرساخت‌های ملی حیاتی یا برنامه‌هایی برای محافظت از سیستم‌های IT دولت. | بله/خیر |
| آیا در این کشور کمپین‌های آگاهی سایبری و بهداشت سایبری[1] اجرا می‌شوند؟ | آیا حکومت مربوطه برای محافظت از کل جمعیتش اقداماتی صورت می‌دهد و از کاربرد خصوصی اینترنت توسط جمعیت کشور در برابر تهدیدات سایبری محافظت می‌کند؟ | جستجوی اینترنتی وبسایت‌های دولت ملی برای یافتن کمپین‌های اطلاع‌رسانی و مشاوره عمومی. | بله/خیر |

۱) Cyber hygiene

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا کشور مورد نظر برنامه‌هایش را برای اجرای دفاع سایبری ملی به صورت فعالانه اعلام کرده است؟ | گذار از دفاع سایبری ملی واکنشی به دفاع بیش‌فعال[۱] [به تعریف نیاز دارد ولی به طور کلی برخی مثال‌های آن عبارت‌اند از: فایروال عظیم چین، مدل دفاع سایبری فعالانه بریتانیا، بازرسی بسته‌ها در روسیه[۲] و احتمالاً دفاع روبه‌جلوی سایبرکام[۳]] | جستجوی اینترنتی وبسایت‌های دولت برای یافتن ارجاعاتی در خصوص سنجه‌های دفاع سایبری فعالانه ملی. به علاوه، جستجوی اظهارنظرهای عمومی سیاستمداران ملی و رهبران آژانس‌های اطلاعاتی یا ارتش. | بله/خیر |
| پیوستگی (انسجام) هدف: آیا این هدف در بیش از یک استراتژی دنبال می‌شود؟ | کشورهایی که هدف خاصی را در خلال چندین استراتژی دنبال می‌کنند، تعهد خود برای دستیابی به آن هدف را نشان می‌دهند و درک آن‌ها از این امر احتمالاً بالاتر است. | مقایسه اهداف فهرست‌شده در جدیدترین استراتژی با اهداف فهرست‌شده در استراتژی قبلی (در صورت وجود). | هدف در بیش از یک استراتژی موجود است: بله/خیر |
| مشاهده‌شده در حمله سایبری منتسب | برخلاف سایر نشانگرهای قصد که نشان‌دهنده قصدی خاص هستند (و نیازمند برنامه‌ریزی از قبل و آمادگی هستند)، می‌توان قصد کلی را (که احتمالی از انجام یک فرمان دارد) از اقدامات کشور استنتاج نمود. | استفاده از ارقام ردیاب عملیات سایبری شورای روابط خارجی برای سنجش تعداد حمله‌های منتسب به یک کشور. | مشاهده‌شده در یک حمله یا بیشتر: بله/خیر |

## ۹-۱-۸) نظارت و پایش گروه‌های داخلی

جدول ۱۲)

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا حکومت مربوطه دست‌کم یک نیروی پلیس یا آژانس مجری قانون با تخصص در جرائم سایبری دارد یا شهروندانش را به گزارش جرائم سایبری ترغیب می‌کند؟ | حاکی از آن است که حکومت مربوطه به آژانس‌های مجری قانون خود، توانایی پیگرد جرائم سایبری و نظارت مبتنی بر روش‌های سایبری را داده است. | تحلیل حضور آنلاین هر کشور برای یافتن ارجاعاتی در خصوص تخصص مجریان قانون. به علاوه، جستجوی اظهارنظرهای عمومی سیاستمداران ملی و افسران ارشد پلیس. | بله/خیر |

۱) Proactive

۲) Russia’s packet inspection

۳) فرماندهی سایبری ایالات متحده

| نشانگر | معنی | توصیف منبع | روش امتیازدهی |
|---|---|---|---|
| آیا آژانس اطلاعاتی داخلی حکومت، قابلیت‌های نظارت سایبری را تأیید می‌کند؟ | تأیید اینکه آژانس اطلاعات کشور دارای مأموریت سایبری است. | تحلیل حضور آنلاین آژانس اطلاعاتی هر کشور برای سنجش اینکه آیا چنین هدفی را تأیید می‌کند یا خیر. به علاوه، جستجوی اظهارنظرهای عمومی سیاستمداران ملی و رهبران ارشد آژانس‌های اطلاعاتی سایبری درباره قابلیت‌هایی که جامعه اطلاعاتی دارد. | بله/خیر |
| آیا در استراتژی، برنامه یا قانون «ضد تروریستی یا امنیت داخلی» حکومت، به جرم سایبری، تروریسم سایبری یا نظارت داخلی از طریق روش‌های سایبری استناد شده است یا خیر؟ | نشان می‌دهد که حکومت مورد نظر در حال کاوش در فعالیت‌های سایبری از منظر ضدتروریستی و امنیت ملی است. | تحلیل حضور آنلاین وزارت کشور یا وزارتخانه متمرکز بر امنیت داخلی درخصوص استراتژی‌ها، برنامه‌ها و قوانین ضد تروریستی یا امنیت داخلی و اینکه آیا این وزارتخانه به فعالیت‌های سایبری استناد می‌کند یا خیر. | بله/خیر |
| پیوستگی (انسجام) هدف: آیا این هدف در بیش از یک استراتژی دنبال می‌شود؟ | کشورهایی که هدف خاصی را در خلال چندین استراتژی دنبال می‌کنند، تعهد خود برای دستیابی به آن هدف را نشان می‌دهند و درک آن‌ها از این امر احتمالاً بالاتر است. | مقایسه اهداف فهرست‌شده در جدیدترین استراتژی با اهداف فهرست‌شده در استراتژی قبلی (در صورت وجود). | هدف در بیش از یک استراتژی موجود است: بله/خیر |
| مشاهده‌شده در حمله سایبری منتسب | برخلاف سایر نشانگرهای قصد که نشان‌دهنده قصدی خاص هستند (و نیازمند برنامه‌ریزی از قبل و آمادگی هستند)، می‌توان قصد کلی را (که احتمالی از انجام یک فرمان دارد) از اقدامات کشور استنتاج نمود. | استفاده از ارقام ردیاب عملیات سایبری شورای روابط خارجی برای سنجش تعداد حمله‌های منتسب به یک کشور. | مشاهده‌شده در یک حمله یا بیشتر: بله/خیر |

## ۹-۲) کیفیت قصد برای سنجش استراتژی

جدول ۱۳)

| نمره (امتیاز) | توضیح دهنده |
|---|---|
| ۱ | مرور کلی تهدیدها و اولویت‌ها |
| ۲ | تحلیل دقیق تهدیدها و اولویت‌های به‌وضوح بیان‌شده |
| ۳ | تقسیم مسئولیت‌ها میان وزارتخانه‌های دولت |
| ۴ | نوار زمانی دقیق یا معیارهای موفقیت |
| ۵ | نوار زمانی دقیق و معیارهای موفقیت |
| -۱ | استراتژی در پنج سال گذشته یا از زمان انقضاء به‌روزرسانی نشده است |

# ۱۰) پیوست د:
## نشانگرهای قابلیت

### ۱۰-۱) شرح تفصیلی نگاشت نشانگرهای قابلیت برحسب هدف

در جداول زیر، علاوه بر شرح هر نشانگرِ قابلیت، کاربرد آن نشانگر نیز در اهداف هشتگانه نمایش داده شده است. اهداف مذکور با تیک آبی مشخص شده‌اند.

| نشانگر | آگاهی از امینت سایبری و سواد ریسک | | |
|---|---|---|---|
| شرح | اندازه‌گیری دانش امنیت سایبری جامعه برای دفاع علیه حملات و انجام روش‌های سایبری امن | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | ✓ |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | ✓ |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | ✓ |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| نشانگر | توافق‌های سایبری دوجانبه | | |
|---|---|---|---|
| شرح | تعیین هنجارهای سایبری بین‌المللی را می‌توان بر اساس میزان فعالیت یک حکومت در تدوین بیانیه‌های غیررسمی و رسمی درخصوص همکاری بین‌المللی، اندازه‌گیری کرد. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | ✓ | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| نشانگر | نرخ‌های آلودگی کامپیوتری | | |
|---|---|---|---|
| شرح | هرقدر که تعداد کامپیوترهای آلوده‌شده با بدافزارهای تحت حمایت مالی غیرحکومتی افزایش یابد، احتمال آسیب‌پذیری دفاع سایبری ملی نیز به همان نسبت افزایش می‌یابد. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | ✓ |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| نشانگر | پروژه‌های ظرفیت‌سازی سایبری/ کمک خارجی | | |
|---|---|---|---|
| شرح | تعیین هنجارهای سایبری بین‌المللی را می‌توان بر اساس میزان فعالیت یک حکومت در ارتقاء ظرفیت‌های سایبریِ حکومت‌های دیگر، اندازه‌گیری کرد. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | ✓ | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| نشانگر | پرسنل نظامی سایبری (پرسنل ارتش سایبری) | | |
|---|---|---|---|
| شرح | تعداد پرسنل منصوب‌شده در پست‌های نظامی سایبری که به اطلاع عموم رسیده است را شناسایی می‌کند. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | ✓ |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | ✓ | پایش/ نظارت داخلی | |

| نشانگر | قوانین امنیت سایبری | | |
|---|---|---|---|
| شرح | قوانین امنیت سایبری موجب می‌شوند یک حکومت بهتر بتواند داده‌ای مربوط به جمعیت خود را کنترل کند، با سایر کشورها تعامل کند، دفاع خود را تقویت کند و همچنین روالی برای نحوه تعامل خود با شرکای خارجی در آینده ایجاد کند. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | ✓ | دفاع سایبری ملی | ✓ |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| نشانگر | حکمرانی و قوانین حریم خصوصی داده | | |
|---|---|---|---|
| شرح | قوانین حریم خصوصی داده موجب می‌شوند یک حکومت بهتر بتواند داده‌ای مربوط به جمعیت خود را کنترل کند، با سایر کشورها تعامل کند، دفاع خود را تقویت کند و همچنین روالی برای نحوه تعامل خود با شرکای خارجی در آینده ایجاد کند. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | ✓ |

| نشانگر | اقتصاد تجارت الکترونیک | | |
|---|---|---|---|
| شرح | فروش بیشتر از طریق تجارت الکترونیک امکان سرازیر شدن درآمد بیشتر به درون شرکت‌های خرده‌فروشی بخش خصوصی را فراهم می‌سازد و موجب رشد اقتصاد داخلی می‌شود. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | ✓ |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| | |
|---|---|
| نشانگر | وجود تیم‌های رویارویی با پیشامدهای امنیت سایبری[1] (CSIRTها) |
| شرح | وجود CSIRT نشانگر آن است که حکومت منابعی برای کاهش آسیب‌پذیری‌های سایبری و بحران‌های مربوطه فراهم کرده است. |

| | | | |
|---|---|---|---|
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | ✓ |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| | |
|---|---|
| نشانگر | نمره آزادی در اینترنت |
| شرح | کاهش آزادی اینترنت در یک کشور، احتمال نظارت و پایش کارآمد شهروندان و کنترل موثر جریان اطلاعات از سوی حکومت را افزایش می‌دهد. |

| | | | |
|---|---|---|---|
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | ✓ | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | ✓ |

| | |
|---|---|
| نشانگر | قدرت نرم جهانی |
| شرح | با افزایش قدرت نرم کشور، قدرت آن کشور در اعمال نفوذ بر سایر کشورها برای اتخاذ یا حفظ هنجارهای بین‌المللی افزایش خواهد یافت. |

| | | | |
|---|---|---|---|
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | ✓ | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| | |
|---|---|
| نشانگر | ۱۰۰ شرکت برتر فناوری در جهان |
| شرح | شرکت‌های فناوری در هر کشور موجب رشد صنعت داخلی آن می‌شوند و بر صنایع سایر کشورهای خارجی تأثیر می‌گذارند، به‌ویژه اگر تعداد کاربران خارجی آن شرکت بسیار زیاد باشد. |

| | | | |
|---|---|---|---|
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | ✓ |
| هنجارهای سایبری بین‌المللی | ✓ | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

۱) Cyber- security Incident Response Teams

| نشانگر | ۱۵۰ شرکت برتر امنیت سایبری در جهان | | |
|---|---|---|---|
| شرح | با افزایش تعداد شرکت‌های امنیت سایبری مستقر در یک کشور، رشد صنعت امنیت سایبری آن کشور هم بیشتر خواهد شد. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | ✓ |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | ✓ |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | ✓ |
| ازکار انداختن زیرساخت دشمن | ✓ | پایش/ نظارت داخلی | |

| نشانگر | حملات تحت حمایت مالی کشور با تأثیر بالا | | |
|---|---|---|---|
| شرح | حملات سایبری پیچیده تحت حمایت کشور یعنی حملاتی که آژانس‌های دولتی، شرکت‌های دارای فناوری پیشرفته و دفاعی یا مجرمان اقتصادی در آن‌ها نقش دارند و خسارات آن‌ها از یک میلیون دلار تجاوز می‌کند. این نشانگر، مشابه با نشانگر حملات عمومی تحت حمایت کشور، ابتکار و مهارت کشور را برای دستبابی به اهدافش اندازه‌گیری می‌کند. | | |
| گردآوری و محافظت از ثروت | ✓ | گردآوری اطلاعات (جاسوسی) | ✓ |
| کنترل اطلاعات | ✓ | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | ✓ |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | ✓ | پایش/ نظارت داخلی | ✓ |

| نشانگر | صادرات فناوری پیشرفته | | |
|---|---|---|---|
| شرح | صادرات محصولات دارای فناوری پیشرفته به کشوری خارجی ممکن است به نفع اقتصاد کشور باشد و (بسته به کشور مورد نظر) ممکن است دسترسی به داده‌هایی که آن محصول درباره شهروندان خارجی گردآوری می‌کند برای آژانس اطلاعاتی آن کشور امکان‌پذیر سازد. این امر ممکن است موجب وابستگی خارجی به صادرات فناوری‌های پیشرفته شود که می‌تواند موجب کندشدن یا توقف قابلیت‌های دشمن در صورت متوقف شدن صادرات شود. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | ✓ |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | ✓ |
| هنجارهای سایبری بین‌المللی | ✓ | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | ✓ | پایش/ نظارت داخلی | |

| نشانگر | واردات ICT | | |
|---|---|---|---|
| شرح | با افزایش واردات فناوری‌های اطلاعاتی و ارتباطی، نیاز بازار به راه‌حل‌های داخلی کاهش می‌یابد و در نتیجه ممکن است آن کشور متحمل ریسک‌های بالاتر زنجیره تأمین در زیرساخت سایبری داخلی خود شود. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | ✓ |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | ✓ |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| نشانگر | نرخ آلودگی موبایل‌ها | | |
|---|---|---|---|
| شرح | هرقدر که تعداد دستگاه‌هایی که می‌توانند با بدافزارهای تحت حمایت مالی غیرحکومتی آلوده شوند افزایش یابد، احتمال آسیب‌پذیری دفاع سایبری ملی نیز به همان نسبت افزایش می‌یابد. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | ✓ |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| نشانگر | توافق‌های سایبری چندجانبه | | |
|---|---|---|---|
| شرح | تعیین هنجارهای سایبری بین‌المللی را می‌توان بر اساس میزان فعالیت حکومت در تدوین بیانیه‌های غیررسمی و رسمی همکاری بین‌المللی اندازه‌گیری کرد. توافق‌های چندجانبه حاکی از ایجاد اجماع میان چندین حکومت است. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | ✓ | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| نشانگر | فرماندهی سایبری ملی | | |
|---|---|---|---|
| شرح | فرماندهی‌های سایبری متمرکز، هماهنگی و بهره‌برداری از قابلیت‌های متعدد سایبری به منظور کاربرد روش‌های سایبری نظامی در هنگام نیاز را برای دولت‌های ملی امکان‌پذیر می‌سازند. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | ✓ | پایش/ نظارت داخلی | |

| نشانگر | درخواست ثبت اختراعات | | |
|---|---|---|---|
| شرح | افزایش تعداد درخواست‌های ثبت اختراعات در کشور حاکی از وجود نوآوری در نیروی کار آن کشور است که ممکن است به سود اقتصادی منجر شود. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | ✓ |
| هنجارهای سایبری بین‌المللی | ✓ | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| نشانگر | درصد جمعیت کاربران رسانه‌های اجتماعی | | |
|---|---|---|---|
| شرح | هرقدر تعداد شهروندانی که از رسانه‌های اجتماعی استفاده می‌کنند بیشتر باشد، احتمال اینکه داده‌های آن‌ها در اینترنت یافت شود افزایش می‌یابد و این امر موجب می‌شود که افراد بیشتری تحت تأثیر نظارت داخلی یا قوانین داده قرار گیرند. اما (در بسیاری از موارد) افزایش تعداد افراد در رسانه‌های اجتماعی ممکن است موجب شود که میزان بیشتری از جمعیت کشور در معرض کمپین‌های اطلاعات خلاف واقع خارجی قرار گیرند. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | ✓ | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | ✓ |

| نشانگر | درصد جمعیت کاربران اینترنت | | |
|---|---|---|---|
| شرح | هرقدر تعداد شهروندانی که از اینترنت استفاده می‌کنند بیشتر باشد، احتمال اینکه داده‌های آن‌ها در اینترنت یافت شود افزایش می‌یابد و این امر موجب می‌شود که افراد بیشتری تحت تأثیر نظارت داخلی یا قوانین داده قرار گیرند. اما (در بسیاری از موارد) افزایش تعداد افراد در اینترنت ممکن است موجب شود که میزان بیشتری از جمعیت کشور در معرض کمپین‌های اطلاعات خلاف واقع خارجی، جرائم سایبری یا کوشش‌های جاسوسی سایبری قرار گیرند. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | ✓ | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | ✓ |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | ✓ |

| نشانگر | شرکت‌های نظارتی بخش خصوصی | | |
|---|---|---|---|
| شرح | قابلیت‌های جدید نظارت حکومت‌ها به نحوی فزاینده برای بهبود فناوری‌های استراق سمع و نفوذ و برای اهداف اطلاعاتی (جاسوسی) و نظارتی، از شرکت‌های خصوصی خریداری شده‌اند. با افزایش میزان تولید فناوری‌های نظارتی در شرکت‌های خصوصی درون کشور، دسترسی آن کشور به این فناوری‌ها هم افزایش می‌یابد. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | ✓ |
| کنترل اطلاعات | ✓ | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | ✓ | پایش/ نظارت داخلی | ✓ |

| نشانگر | اندازه نهادهای استاندارد ملی | | |
|---|---|---|---|
| شرح | اندازه نهادهای استاندارد ملی می‌تواند نشان‌دهنده میزان توجه و کوشش صورت گرفته در تعیین هنجارهای سایبری باشد. | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | ✓ | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| نشانگر | حملات [سایبری] تحت حمایت مالی کشور | | |
|---|---|---|---|
| شرح | حملات سایبری تحت حمایت کشور امکان گردآوری اطلاعات پنهان خارجی [جاسوسی در خارج]، انجام جاسوسی شرکتی، نظارت مخالفان، اشاعه اطلاعات خلاف واقع و از کار انداختن زیرساخت‌های دشمن را فراهم می‌سازند. | | |
| گردآوری و محافظت از ثروت | ✓ | گردآوری اطلاعات (جاسوسی) | ✓ |
| کنترل اطلاعات | ✓ | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | ✓ |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | ✓ | پایش/ نظارت داخلی | ✓ |

| نشانگر | درخواست‌های موفق حذف محتوا در گوگل | |
|---|---|---|
| شرح | هرچه درخواست‌های موفق برای حذف محتوای گوگل بیشتر باشد حاکی از آن است که حکومت توانسته است به طور کارآمد اطلاعات را از اینترنت حذف نماید و نشان‌دهنده میزان کنترل آن کشور بر فضای اطلاعاتی است. | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) |
| کنترل اطلاعات | ✓ | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی |

| نشانگر | سایت‌های خبری برتر | |
|---|---|---|
| شرح | وبسایت‌های خبری دارای ترافیک بین‌المللی بیشتر که دفاتر مرکزی آن‌ها در کشوری خاص مستقر باشد، قدرت بیشتری به آن کشور می‌دهند تا روایات متداول یا ایده‌آل‌های مردمی آن کشور را به درون اینترنت منتقل کنند | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) |
| کنترل اطلاعات | ✓ | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی |

| نشانگر | وبسایت‌های برتر | | |
|---|---|---|---|
| شرح | وبسایت‌های دارای ترافیک بین‌المللی بیشتر که دفاتر مرکزی آن‌ها در کشوری خاص مستقر باشد، قدرت بیشتری به آن کشور می‌دهند تا روایات متداول یا ایده‌آل‌های مردمی آن کشور را به درون اینترنت منتقل کنند و همچنین امکان تولید درآمد بیشتر از تبلیغات یا عرضه محصولات بیشتر به مصرف‌کنندگان را برای شرکت مالک وبسایت فراهم می‌سازد | | |
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | ✓ |
| کنترل اطلاعات | ✓ | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | ✓ |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

| | |
|---|---|
| نشانگر | آسیب‌پذیری‌های موجود در دستگاه‌های داخلی |
| شرح | به طور کلی هرچه کامپیوترهای یک کشور آسیب پذیرتر باشند، بیشتر مستعد آن هستند که در معرض حمله یک کشور دیگر قرار بگیرند. |

| | | | |
|---|---|---|---|
| گردآوری و محافظت از ثروت | | گردآوری اطلاعات (جاسوسی) | |
| کنترل اطلاعات | | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | |
| هنجارهای سایبری بین‌المللی | | دفاع سایبری ملی | ✓ |
| ازکار انداختن زیرساخت دشمن | | پایش/ نظارت داخلی | |

مجموع:

| | | | |
|---|---|---|---|
| گردآوری و محافظت از ثروت | ۴ | گردآوری اطلاعات (جاسوسی) | ۸ |
| کنترل اطلاعات | ۱۰ | رشد شایستگی در حوزه فناوری و سایبری در سطح ملی | ۱۰ |
| هنجارهای سایبری بین‌المللی | ۸ | دفاع سایبری ملی | ۹ |
| ازکار انداختن زیرساخت دشمن | ۷ | پایش/ نظارت داخلی | ۸ |

## ۲-۱۰) شرح نحوه نمره‌دهی به نشانگرهای قابلیت

جدول ۱۴)

| | نشانگر | معنا | منبع | سال | روش نمره‌دهی |
|---|---|---|---|---|---|
| ۱ | آگاهی از امینت سایبری و سواد ریسک | کشور مربوطه از نظر سواد ریسک سایبری جهانی نمره‌ای کسب می‌کند | انجمن اولیور وایمن[1] | ۲۰۲۱ | نمرات توسط انجمن اولیور وایمن محاسبه شد. همین نمرات برای شاخص قدرت سایبری بلفر به کار گرفته شدند. |
| ۲ | توافق‌های سایبری دوجانبه | تعداد و کیفیت توافق‌های دوجانبه رسمی و/یا غیررسمی امضاشده توسط دولت ملی در [مورد] فضای سایبری که برحسب تازگی نمره‌دهی می‌شود | پروژه قدرت سایبری ملی بلفر، هاروارد | ۲۰۲۲ | برای هریک از توافق‌های میان حکومت‌ها:<br>۱ = جلسات، اظهارنظرها؛<br>۲ = بیانیه‌های مشترک، همکاری، چارچوب؛<br>۳= توافق/ تفاهم‌نامه. |
| ۳ | نرخ‌های آلودگی کامپیوتری | درصد کامپیوترهای کشور که به بدافزار آلوده شده‌اند | کامپری‌تک[2] | ۲۰۲۱ | درصد کامپیوترهای آلوده به بدافزار |

۱) Oliver Wyman Forum

۲) Comparitech: شرکت تحلیل فناوری است که اطلاعات، ابزارها، بررسی‌ها و مقایسه‌ها را برای کمک به خوانندگان سایت با هدف بهبود امنیت سایبری و حریم خصوصی آنلاین ارائه می‌دهد (توضیح مترجم).

| | نشانگر | معنا | منبع | سال | روش نمره‌دهی |
|---|---|---|---|---|---|
| ۴ | پروژه‌های ظرفیت‌سازی سایبری/کمک خارجی | تحلیلی از پروژه‌های بین‌المللی ظرفیت‌سازی سایبری در گذشته و حال | پروژه قدرت سایبری ملی بلفر، هاروارد | ۲۰۲۲ | پروژه‌های فهرست‌شده در پورتال سیبل[۱] توسط تیم شاخص قدرت سایبری ملی بلفر تحلیل شدند. هرقدر که تعداد پروژه‌های ظرفیت‌سازی سایبری آن کشور بیشتر بود، نمره آن کشور هم بالاتر بود. |
| ۵ | پرسنل نظامی سایبری [پرسنل ارتش سایبری] | تعداد افرادی که پست‌های پرسنلی نیروهای سایبری نظامی را اشغال کرده‌اند | پروژه قدرت سایبری ملی بلفر، هاروارد | ۲۰۲۱ | تعداد افرادی که بر اساس گزارش‌های متن‌باز در واحدهای سایبری ارتش‌ها خدمت می‌کنند. |
| ۶ | قوانین امنیت سایبری | اندازه‌گیری میزان فعالیت یک حکومت در پیاده‌سازی قوانین مربوط به محتوا، حریم خصوصی و جرائم سایبری | پروژه قدرت سایبری ملی بلفر، هاروارد | ۲۰۲۱ | ۰ = عدم وجود قانون؛<br>۱= قوانینی که یکی از موارد ذیل را پوشش می‌دهند: محتوا، حریم خصوصی و جرم؛<br>۲ = قوانینی که دو مورد از موارد ذیل را پوشش می‌دهند: محتوا، حریم خصوصی و جرم؛<br>۳ = قوانینی که محتوا، حریم خصوصی و جرم را پوشش می‌دهند، [اما] منسوخ‌شده‌اند (مربوط به قبل از سال ۲۰۰۰ هستند)؛<br>۴ = قوانینی که محتوا، حریم خصوصی و جرم را پوشش می‌دهند و اخیراً به‌روزرسانی‌شده‌اند (پس از سال ۲۰۰۰). |
| ۷ | حکمرانی و قوانین حریم خصوصی داده | تحلیلی از قوانین حریم خصوصی داده در یک کشور | دی‌ال‌ای پایپر[۲] | ۲۰۲۱ | نمرات و تحلیل از سوی دی‌ال‌ای پایپر انجام شده‌اند. نمرات بالاتر حاکی از وجود مقررات قانونی بهتر برای محافظت از داده‌های شخصی است. |
| ۸ | اقتصاد تجارت الکترونیک | فروش تجارت الکترونیک در سطح ملی به‌مثابه درصدی از تولید ناخالص داخلی | استاتیستا[۳]، آنکتاد[۴] و سایرین | ۲۰۲۱ | نمرات بالاتر حاکی از فروش بیشتر در تجارت الکترونیک است. |

۱) Cybil Portal

۲) DLA Piper

۳) Statista

۴) توضیح مترجم: کنفرانس تجارت و توسعه سازمان ملل (UNCTAD: United Nations Conference on Trade and Development) که به اختصار آنکتاد نامیده می‌شود در سال ۱۹۶۴ میلادی با هدف یک‌پارچگی کشورهای در حال توسعه با اقتصاد جهانی تأسیس شد.

| | نشانگر | معنا | منبع | سال | روش نمره‌دهی |
|---|---|---|---|---|---|
| ۹ | وجود تیم‌های رویارویی با پیشامدهای امنیت سایبری (CSIRTها) | وجود تیم رویارویی با پیشامدهای امنیت سایبری | پروژه قدرت سایبری ملی بلفر، هاروارد | ۲۰۲۱ | ۰ = عدم وجود تیم؛<br>۱= طرح‌هایی برای تأسیس CSIRT؛<br>۲= تیم جدید CSIRT در سطح ملی (۵ سال یا کمتر)؛<br>۳ = تیم سابقه‌دار CSIRT در سطح ملی (بیش از ۵ سال)؛<br>۴ = تیم سابقه‌دار CSIRT در سطح ملی (بیش از ۵ سال) + عضوی از اولین تیم رویارویی. |
| ۱۰ | نمره آزادی در اینترنت | نمره «خانه آزادی»[۱] برای میزان آزادی آنلاین شهروندان | «خانه آزادی» و «آزادی جهان»[۲] | ۲۰۲۱ | ۰-۱۰۰: سه نمره جداگانه که با یکدیگر تجمیع می‌شوند:<br>الف) موانع دسترسی؛<br>ب) محدودیت‌های محتوا؛<br>ج) نقض حقوق کاربران.<br>برای هفت کشور رتبه‌بندی‌های «آزادی جهان» را به کار گرفتیم، زیرا «خانه آزادی» اطلاعات آن‌ها را در اختیار نداشت. |
| ۱۱ | قدرت نرم جهانی | نمره کشورها در شاخص قدرت نرم جهانی | برند فایننس[۳] | ۲۰۲۱ | نمرات محاسبه‌شده توسط برند فایننس بخشی از شاخص قدرت نرم آن‌ها بود. همین نمرات در شاخص قدرت سایبری ملی بلفر به کار گرفته شد. |
| ۱۲ | ۱۰۰ شرکت برتر فناوری در جهان | تعداد شرکت‌های مستقر در یک کشور که جزء ۱۰۰ شرکت برتر فناوری جهانی هستند. | تامسون رویترز[۴] | ۲۰۲۱ | شمارش شرکت‌های برتر فناوری به ازای هر کشور |

۱) Freedom House: سازمان مردم‌نهاد مستقر در آمریکا که با بودجه دولت فدرال آمریکا به پژوهش و کنشگری در زمینه آزادی و حقوق بشر می‌پردازد (توضیح مترجم).

۲) Freedom of the World

۳) Brand Finance: شرکت مشاور استراتژی و ارزیابی برند (توضیح مترجم).

۴) Thomson Reuters: شرکت چندملیتی، فعال در حوزه رسانه‌های جمعی (توضیح مترجم).

| | نشانگر | معنا | منبع | سال | روش نمره‌دهی |
|---|---|---|---|---|---|
| ۱۳ | ۱۵۰ شرکت برتر امنیت سایبری در جهان | تعداد شرکت‌های مستقر در یک کشور که جزء ۱۵۰ شرکت برتر امنیت سایبری جهانی هستند. | سایبرسکیوریتی ونچرز[1] | ۲۰۲۱ | تعداد شرکت‌هایی که در رتبه‌بندی ۱۵۰ شرکت برتر امنیت سایبری فهرست شده‌اند. |
| ۱۴ | حملات تحت حمایت مالی کشور با تأثیر بالا | تعداد حملات سایبری که به صورت علنی به یک کشور نسبت داده می‌شوند. | مرکز مطالعات استراتژیک و بین‌الملل[2] | ۲۰۲۲ | شمارش حملات سایبری منتسب به بازیگران تحت حمایت مالی کشور. |
| ۱۵ | صادرات فناوری پیشرفته | درصد صادرات فناوری پیشرفته در کل صادرات [بخش] تولید | بانک جهانی | ۲۰۲۱ | مقادیر بالاتر حاکی از صادرات بیشتر فناوری هستند. |
| ۱۶ | واردات ICT | واردات ICT به‌مثابه درصدی از کل واردات. | آنکتاد | ۲۰۱۹ | مقادیر بالاتر حاکی از وابستگی بیشتر به واردات است و دفاع سایبری کشور را بیشتر در معرض خطر نفوذ دشمن قرار می‌دهد. |
| ۱۷ | نرخ آلودگی موبایل‌ها | درصدی از موبایل‌های کشور که به بدافزار آلوده شده‌اند | کامپری‌تک | ۲۰۲۱ | درصد موبایل‌های کاربران که به بدافزار آلوده شده‌اند. |
| ۱۸ | توافق‌های سایبری چندجانبه | تعداد و کیفیت توافق‌های چندجانبه رسمی و/یا غیررسمی امضاشده توسط دولت ملی در [مورد] فضای سایبری که برحسب تازگی نمره‌دهی می‌شود | پروژه قدرت سایبری ملی بلفر، هاروارد | ۲۰۲۱ | برای هریک از توافق‌های میان حکومت‌ها:<br>۱ = غیررسمی/ کنفرانس/ منطقه‌ای؛<br>۲ = غیررسمی/ کنفرانس/ جهانی؛<br>۳= توافق منطقه‌ای رسمی / عضوی از سازمان منطقه‌ای؛<br>۴= توافق چندجانبه رسمی / عضوی از سازمان جهانی. |

۱) Cybersecurity Ventures

۲) Center for Strategic and International Studies: اندیشکده آمریکایی که در خصوص مسائل سیاست، اقتصاد و امنیت بین‌الملل در سراسر جهان با تمرکزی بر روابط بین‌الملل، تجارت، فناوری، دانش مالی، انرژی و جغرافیای راهبردی فعالیت می‌کند (توضیح مترجم).

| | نشانگر | معنا | منبع | سال | روش نمره‌دهی |
|---|---|---|---|---|---|
| ۱۹ | فرماندهی سایبری ملی | وجود و سابقه فرماندهی سایبری ملی | پروژه قدرت سایبری ملی بلفر، هاروارد | ۲۰۲۱ | ۰ = عدم وجود فرماندهی سایبری؛<br>۱= طرح‌هایی برای تأسیس فرماندهی سایبری؛<br>۲= فرماندهی سایبری جدید (۲ سال یا کمتر)؛<br>۳ = فرماندهی سایبری سابقه‌دار (۵-۲ سال)؛<br>۴ = فرماندهی سایبری سابقه‌دار (بیش از ۵ سال). |
| ۲۰ | درخواست ثبت اختراعات | تعداد درخواست‌های ثبت اختراع داخلی از سوی شهروندان آن کشور | «نشانگرهای توسعه جهان»[1] | ۲۰۱۹ | تعداد پرونده‌های ثبت اختراع داخلی (تنها از سوی ساکنان کشور). اندازه‌گیری سرانه. |
| ۲۱ | درصد جمعیت کاربران رسانه‌های اجتماعی | درصد حساب‌های فعال رسانه‌های اجتماعی | استاتیستا و سایرین | ۲۰۲۱ | درصد کاربران اینترنت که از سایت‌های شبکه‌های اجتماعی بازدید می‌کنند. |
| ۲۲ | درصد جمعیت کاربران اینترنت | ضریب نفوذ اینترنت در کشور | استاتیستا و سایرین | ۲۰۲۱ | رقم بالاتر نشان‌دهنده آن است که افرادی بیشتری از اینترنت استفاده می‌کنند. |
| ۲۳ | شرکت‌های نظارتی بخش خصوصی | تعداد شرکت‌های نظارتی بخش خصوصی مشغول به کار در کشور، که در نمایشگاه‌های بین‌المللی خدمات نظامی حضور دارند. | شورای آتلانتیک[2] | ۲۰۲۱ | شمارش تعداد شرکت‌های نظارتی که در کشوری فعالیت می‌کنند و در نمایشگاه‌های بین‌المللی خدمات نظامی منتخب، شرکت می‌کنند. |
| ۲۴ | اندازه نهادهای استاندارد ملی | تعداد پرسنل مشغول به کار در نهاد استاندارد ملی یک کشور | پروژه قدرت سایبری ملی بلفر، هاروارد | ۲۰۲۱ | عدد بالاتر حاکی از آن است که افراد بیشتری در نهاد استاندارد ملی آن کشور به کار مشغولند. |

۱) World Development Indicators: نخستین گردآوری نشانگرهای توسعه که توسط بانک جهانی و از منابع رسمی شناخته شده بین‌المللی گردآوری شده است (توضیح مترجم).

۲) Atlantic Council: اندیشکده آمریکایی در حوزه روابط بین‌الملل (توضیح مترجم).

| | نشانگر | معنا | منبع | سال | روش نمره‌دهی |
|---|---|---|---|---|---|
| ۲۵ | حملات سایبری تحت حمایت مالی کشور | تعداد حملات سایبری نسبت‌داده شده به صورت علنی | شورای روابط خارجی[۱] | ۲۰۲۲ | شمارش حملات سایبری منتسب به بازیگران تحت حمایت مالی کشور. |
| ۲۶ | درخواست‌های موفق حذف محتوا در گوگل | تعداد درخواست‌های حذف که یکی از نهادهای دولتی به گوگل ارسال می‌کند. | گوگل | ۲۰۲۰-۲۰۲۱ | تعداد درخواست‌ها |
| ۲۷ | سایت‌های خبری برتر | تعداد سایت‌های خبری موجود در فهرست ۵۰ سایت خبری برتر سیمیلاروب که به سازمان‌هایی تعلق دارند که دفتر مرکزی آن‌ها در کشور مربوطه مستقر است. | سیمیلاروب[۲] | ۲۰۲۱ | تعداد سایت‌ها در فهرست ۵۰ سایت خبری برتر |
| ۲۸ | وبسایت‌های برتر | تعداد وبسایت‌های موجود در فهرست ۵۰ وبسایت برتر سیمیلاروب که به سازمان‌هایی تعلق دارند که دفتر مرکزی آن‌ها در کشور مربوطه مستقر است. | سیمیلاروب | ۲۰۲۱ | تعداد سایت‌ها در فهرست ۵۰ وبسایت برتر |
| ۲۹ | آسیب‌پذیری‌های موجود در دستگاه‌های داخلی | درصد تجمعی آسیب‌پذیری‌های فهرست‌شده برای زیرساخت کشور در پایگاه‌داده شودان[۳] | پروژه قدرت سایبری ملی بلفر، هاروارد | ۲۰۲۱ | درصد تجمعی نتایج جستجوی شودان |

۱) Council on Foreign Relations (CFR): اندیشکده آمریکایی در حوزهٔ سیاست خارجی آمریکا و روابط بین‌الملل (توضیح مترجم).

۲) SimilarWeb: یک وب‌سایت است که خدمات تحلیل وب را برای اهداف تجاری ارائه می‌کند. این شرکت اطلاعاتی را در قالب خدمات به مشتریانش می‌دهد. این اطلاعات شامل میزان بازدید و مقدار ترافیک سایت، منابع و سایر اطلاعات از این دست می‌شود (توضیح مترجم).

۳) Shodan: موتور جستجو که اینترنت را برای یافتن دستگاه‌های در دسترس عموم اسکن می‌کند. شودان به کاربران امکان می‌دهد تا انواع مختلف سرورهای (وب کم، روتر و غیره) متصل به اینترنت را جستجو کنند (توضیح مترجم).

پایان

زاویه
نگاهی نو،
به حکمرانی فضای مجازی

نشانی تهران، ضلع غربی میدان فلسطین، خیابان آیت‌الله طالقانی، پلاک ۳۹۷
تلفن ۰۲۱-۸۶۰۵۴۲۹۱
وبسایت www.zaviehmag.ir
شبکه‌های اجتماعی @zaviehmag

IDEBAN دیده‌بان

نشانی بلوار آفریقا، خیابان یزدان‌پناه، نبش کوچه دبیر، پلاک ۳
کد پستی ۱۹۶۸۸۷۳۱۰۹
تلفن ۰۲۱-۸۶۰۸۷۱۹۸
شبکه‌های اجتماعی @dideban_majazi

Designed by Hossein Razaqnejad | ho3inr@gmail.com