مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

عصر فضای مجازی
صد و بیست و پنج

HARVARD Kennedy School
BELFER CENTER
for Science and
International Affairs

نمایه قدرت سایبری ملی ۲۰۲۰
روش‌شناسی و ملاحظات تحلیلی

مرکز بلفر
دانشگاه هاروارد
کالج کندی

National Cyber Power Index 2020
Methodology and Analytical Considerations

عصر فضای مجازی

شماره ۱۲۵
مرداد ۱۴۰۲

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

نمایه قدرت سایبری ملی ۲۰۲۰
روش شناسی و ملاحظات تحلیلی

مرکز بلفر
دانشگاه هاروارد، کالج کندی

محتوای این اثر الزاماً بیانگر دیدگاه
مرکز ملی فضای مجازی نیست.

تهیه‌شده در پژوهشگاه فضای مجازی
گروه مطالعات فرهنگی و اجتماعی

مترجم:
علیرضا شفیعی نسب

ناظر علمی:
امیررضا باقرپور شیرازی (مدیر گروه مطالعات فرهنگی و اجتماعی)
علیرضا قبولی شاهرودی (کارشناس گروه مطالعات فرهنگی و اجتماعی)

نشانی: تهران، سعادت آباد، خیابان علامه شمالی، کوچه هجدهم غربی، پلاک ۱۷
تلفن: ۲۲۰۷۳۰۳۱-۰۲۱
کد پستی: ۱۹۹۷۹۸۷۶۲۹

فهرست

سخن نخست یک

یادداشتی برای خوانندگان ۳
چکیدهٔ مدیریتی ۶
۱. مقدمه ۱۳
۱/۱. هدف ان‌سی‌پی‌آی ۲۰۲۰ بلفر ۱۳
۱/۲. مقابلهٔ ان‌سی‌پی‌آی با دیگر نمایه‌های سایبری ۱۶
۲. نمایه قدرت سایبری ملی ۲۰۲۰ ۲۳
۲/۱. تفسیر نمایهٔ قدرت سایبری ملی ۲۰۲۰ ۲۵
۲/۲. محدودیت‌ها ۲۸
۳. چهارچوب نظری ۳۷
۳/۱. اهداف ملی ۳۷
۳/۲. فرمول نمایهٔ قدرت سایبری ملی ۴۲
۴. روش‌شناسی و بحث ۴۷
۴/۱. نمره‌دهی به قصد و منابع ۴۷
۴/۲. امتیازدهی به قابلیت‌ها و منابع ۶۳
۴/۳. ساختن ان‌سی‌پی‌آی تجمعی ۸۱
۵. نتیجه‌گیری ۸۹
۶. منابع و ضمایم ۹۱
ضمیمهٔ الف: نقشهٔ ان‌سی‌پی‌آی ۹۷
ضمیمهٔ ب: شرح تفصیلی شاخص‌های قصد بر اساس هدف ۱۰۱
ضمیمهٔ ج: شرح تفصیلی شاخص‌های قابلیت ۱۱۶
ضمیمهٔ د: نمودارهای راداری تمام قابلیت‌ها به تقسیم کشور ۱۳۱

سخن نخست

سخن نخست

ما امروزه در جهانی زندگی می‌کنیم که تحولات فضای مجازی همه عرصه‌های حیات بشری را به عصری جدید فراخوانده است؛ عصری مشحون از بیم و امید درباره تحولاتی عمیق و شتابان که آینده‌ای مبهم و غیرقابل‌پیش‌بینی را برای جوامع معاصر به تصویر می‌کشد. ایران اسلامی نیز در یک دهه گذشته تحت تأثیر تحولات پُردامنه و همه‌جانبهٔ این صحنه قرار گرفته و در تمامی ساحات فرهنگی، اجتماعی، اقتصادی و سیاسی با آنچه تحول دیجیتال خوانده می‌شود، روبرو بوده است.

در این میان اما ظهور انقلاب اسلامی در جهانی که نظم مدرنیستی و الگوی لیبرال دموکراسی را پایان تاریخ قلمداد می‌کرد، نشانهٔ مهم و آشکاری بر این مدعاست که با پایبندی به «مبانی اندیشه اسلامی و ارزش‌های انقلاب اسلامی» و «جهاد مستمر علمی و تولید دانش» می‌توان از میان دریای خروشان جهان دیجیتال گذر کرد، از تهدیدهای آن فرصت ساخت و افقی روشن برای استقرار نظمی نوین و تمدن اسلامی گشود. بنابراین، همواره این پرسش در مقابل اندیشمندان و حکمرانانِ دغدغه‌مند مطرح خواهد بود که جامعه ایرانی-اسلامی معاصر چگونه می‌تواند با تمهید مواجهه‌ای فعال و خردمندانه، از این پیچ تاریخی و تمدنی به سلامت عبور کرده و ضمن بهره‌برداری از فرصت‌های بی‌بدیل آن، نه‌تنها خلأها و کاستی‌های گذشته را جبران کند، بلکه فرآیند تحقق تمدن اسلامی را نیز در گام دوم انقلاب اسلامی تسهیل نماید.

در همین راستا، **پژوهشگاه فضای مجازی** در تلاش است که با رصد و تحلیل رخدادها، تحولات و روندهای آیندهٔ فضای مجازی، ارکان و ذی‌ربطان مختلف نظام حکمرانی کشور را مُتفطنِ فرصت‌ها، تهدیدها و چالش‌های جهان معاصر نماید؛ به این امید که با نقش‌آفرینی هوشمندانه و مجاهدانه در این تحولات روزآمد، مسیر تحقق جامعه اسلامی مجازی و ایران قوی در عصر فضای مجازی را هموارتر نماید.

سید محمدامین آقامیری
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

پیشـــگفتار

یادداشتی برای خوانندگان

قوی‌ترین کشور سایبریِ دنیا کدام است؟ جمعی از برجسته‌ترین پژوهشگران و اندیشمندان در «مرکز علم و امور بین‌الملل بلفر» در کالج کندی دانشگاه هاروارد گرد هم آمده و می‌کوشند با پژوهش‌هایی نوآورانه و روشنگر در زمینهٔ قدرت سایبری، به پاسخ این پرسش دست پیدا کنند. این پژوهش هم در عرصهٔ دانشگاهی و هم در صحنهٔ عمل و واقعیت از اهمیت زیادی برخوردار است؛ زیرا توانسته از بصیرت‌های دقیق آکادمیک به مدلی کارآمد برای خط‌مشی‌گذاری دست پیدا کند.

کنشگران سایبریِ تحت حمایت دولتْ یکی از بزرگ‌ترین تهدیدها برای امنیت ملی به حساب می‌آیند. من هنگام رهبریِ تلاش‌های وزارت دفاع برای مقابله با حملات سایبریِ روسیه به انتخابات ریاست جمهوری، حمله‌های کرهٔ شمالی به زیرساخت‌های حیاتیِ ایالات متحده و سرقت مالکیت فکری آمریکا از سوی چین، به‌طور مستقیم شاهد بودم که کشورها به‌واسطهٔ ابزارهای سایبری چه اهدافی را دنبال می‌کنند.

بزرگ‌ترین حملات سایبری دههٔ گذشته منبع مهمی از داده‌ها به‌شمار می‌آیند که نشان می‌دهند دولت‌ها برای گسترش نفوذ و قدرت خود در حوزهٔ سایبری چه تلاش‌هایی می‌کنند. اما بعضی کشورها با خیال‌بافی دربارهٔ گسترش مدل‌های اقتدارگرایانهٔ خود برای حکمرانیِ اینترنت، تلاش می‌کنند با پیگیریِ اقداماتِ دیپلماتیک در سازمان ملل، قدرت

سایبری خود را افزایش دهند. در مجامع دیگر، نمایندگان کشورها می‌کوشند استانداردهای فنی حاکم بر بافتار اینترنت را سروشکل بدهند تا بر ژئوپلیتیکِ فناوری و اطلاعات سیطره یابند.

بعضی از این اقدامات مشروع و سازنده‌اند؛ برخی دیگر در «فضای بینابینیِ» خاکستری‌ای قرار می‌گیرند که در آن، هنجارها و قانون بین‌الملل هنوز در مرحلهٔ نوپاست؛ و بعضی از این اقدامات بی‌تردید مخرب‌اند. اما نکته‌ای قدر مسلم است: این اقدامات همه در توانایی کلیِ هر کشور برای نیل به اهداف ملی نقش دارند و این یعنی قدرت به‌شکلِ سنتی‌اش.

متغیرهای زیربناییِ مؤثر در قدرت سایبری به‌خوبی درک نشده‌اند. هیچ بعید نیست که از صحنهٔ کلیِ مقاصد و قابلیت‌هایی که در قدرت سایبری یک کشور مؤثرند، غفلت شود. برای بهبود راهبرد و خط‌مشی سایبریِ کلانِ یک کشور، درک این صحنه بسیار بااهمیت ست.

من، در مقام دستیار وزیر دفاع، مدام در پی یافتن و به‌کارگیری شیوه‌های تحلیلی‌ای بوده‌ام تا تهدیدهای سایبری گوناگونِ کمین‌کرده برای امنیت ملی ایالات متحده را ارزیابی کنم. مدل‌های کمّی گاهی ممکن است نتایجی به دست دهند که با درک شهودی [خودمان] ناسازگار باشند؛ مثلاً بسیاری از افرادْ ناخودآگاه کرهٔ شمالی را تهدید سایبریِ مهمی برای ایالات متحده تلقی می‌کنند و تبعاً قدرت سایبری زیادی برایش قائل می‌شوند. اما بررسی دقیق‌ترِ جوانب گوناگون قدرت سایبری نشان می‌دهد که جمهوری دموکراتیک خلق کره، در بسیاری از عرصه‌های کلیدی، کنشگری ضعیف است.

در این پژوهش، گروه پژوهشیِ مرکز بلفر بهترین مدلِ موجود را برای ارزیابی قدرت سایبری ارائه کرده است. کار آن‌ها درخشان است: مدل‌های دقیق کمّی و کیفی را توسعه داده و به کار بسته‌اند؛ بیش از

هزار منبع داده را مرور کرده‌اند؛ ۲۷ شاخص منحصربه‌فرد برای سنجش قابلیت‌های سایبری هر کشور طراحی کرده‌اند؛ اکنون یکی از بهترین پایگاه‌های داده‌ایِ مرتبط با مسائل سایبری در سطح جهان را در اختیار دارند.

مأموریت مرکز بلفر طلایه‌داری در پیشبرد دانش خط‌مشیی ضروریِ ناظر به مسائل امنیتی مهم در سطح بین‌المللی است. نمایهٔ قدرت سایبری ملی دقیقاً همین کار را می‌کند. به سیاست‌گذاران سراسر دنیا توصیه می‌کنم از شاخص قدرت سایبری ملی در بحث‌های مربوط به سیاست سایبری استفاده کنند و آن را چهارچوبی جهت تقویت رویکرد سایبری خود بدانند.

به این گروه افتخار می‌کنم که در باورهای رایج تردید کردند و با خلاقیت و دقت، مشکلی پیچیده در زمینهٔ سیاست‌گذاری را حلاجی کردند. همهٔ ما باید قدردان تلاش آن‌ها در راستای درک بهتر حوزهٔ سایبری باشیم.

اریک روزنباک

مدیر مشترک مرکز بلفر
رئیس سابق ستاد و دستیار وزیر دفاع ایالات متحده

چکیدهٔ مدیریتی

نمایهٔ قدرت سایبری ملیِ (انسی‌پی‌آی) بلفر، قابلیت‌های سایبری سی کشور را در بستر هفت هدف ملی می‌سنجد و در این راه، از ۳۲ شاخصِ قصد[1] و ۲۷ شاخصِ توانایی[2] استفاده می‌کند که شواهد و مدارک آن‌ها از داده‌هایی در دسترس عموم گردآوری شده است.

برخلاف شاخص‌هایی که اکنون در رابطه با مقولهٔ سایبری وجود دارد، باور ما این است که قدرت سایبری سنجهٔ واحدی ندارد. قدرت سایبری از مؤلفه‌های متعددی تشکیل شده است و باید آن را در بستر اهداف ملی هر کشور در نظر گرفت. رویکرد ما در سنجش قدرت سایبری، «کل کشور» است. با لحاظ‌کردن «کل کشور»، هرجا که ممکن باشد تمام ابعادِ تحت‌کنترل دولت را در نظر می‌گیریم. در انسی‌پی‌آی، ما راهبردهای دولت، قابلیت‌های دفاعی و حمله‌ای، تخصیص منابع، بخش خصوصی، نیروی کار و نوآوری را می‌سنجیم. ارزیابی ما هم قدرت بالفعل و هم پتانسیل‌ها و قدرت بالقوه را مورد ارزیابی قرار می‌دهد؛ که در مورد اخیر، نمرهٔ نهایی بدان معناست که دولت آن کشور می‌تواند این قابلیت‌ها را به‌شکل کارآمدی به اجرا بگذارد.

انسی‌پی‌آی هفت هدفِ ملی را شناسایی کرده است که کشورها از راه سایبری در پی دستیابی به آن‌ها هستند. این هفت هدف عبارت‌اند از:

- پایش و رصد گروه‌های داخلی؛
- تقویت و ارتقای دفاع سایبری ملی؛
- کنترل و دست‌کاری محیط اطلاعاتی؛
- جمع‌آوری اطلاعات خارجی برای امنیت ملی؛

1 Intent indicator
2 Capability indicator

- سود تجاری یا ارتقای رشد صنعتی داخلی؛
- تخریب یا غیرفعال‌سازی زیرساخت‌ها و قابلیت‌های دشمن؛
- تعریف استانداردهای فنی و هنجارهای سایبری بین‌المللی.

برخلاف این دیدگاه رایج که قدرت سایبری به‌معنای تخریب یا غیرفعال‌سازی زیرساخت‌های دشمن (موسوم به عملیات سایبری تهاجمی) است، واقعیت این است که حمله فقط یکی از اهدافی است که کشورها از راه سایبری در پی دستیابی به آن‌ها هستند.

ان‌سی‌پی‌آی یک کشور را به‌طور جامع [و با نگاهی کل‌نگرانه] در مقام یک کنشگر سایبری می‌سنجد. این جامعیت، در بستر ان‌سی‌پی‌آی، به‌معنای استفادهٔ کشوری از شیوه‌های سایبری برای رسیدن به اهدافی متعدد (نه‌فقط چند هدف انگشت‌شمار) است. جامع‌ترین قدرت سایبری، کشوری است که دو مورد را داشته باشد: ۱. قصد دستیابی به اهداف ملی متعدد، از راه سایبری؛ ۲. قابلیت دستیابی به این اهداف.

$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{7}\sum_{x=1}^{7} Capability_x * Intent_x$$

National Cyber Power Index, NCPI: نمایهٔ قدرت سایبری ملی (ان‌سی‌پی‌آی)
Capability: قابلیت
Intent: قصد

در ان‌سی‌پی‌آیِ سال ۲۰۲۰، ده قدرت جامع سایبری بر اساس این هفت هدف، به‌ترتیب عبارت‌اند از: ایالات متحده، چین، بریتانیا، روسیه، هلند، فرانسه، آلمان، کانادا، ژاپن و استرالیا.

ما سه نمایهٔ گوناگون ارائه می‌دهیم: ان‌سی‌پی‌آی، نمایهٔ قصد سایبری

(سی‌آی‌آی)[1] و نمایهٔ قابلیت سایبری (سی‌سی‌آی)[2]. سی‌آی‌آی و سی‌سی‌آی، هر دو سنجه‌هایی مستقل‌اند. ان‌سی‌پی‌آی درواقع ترکیبی از این دو سنجه است.

ما به این نکته واقفیم که اهداف ملی سایبری از هم مجزا نیستند: قابلیت سایبری فقط بخشی از جعبهٔ ابزار است؛ یعنی در کنار شیوه‌های سنتیِ نظامی، دیپلماسی، سیاست عمومی، تمهیدات تأدیبی و خط‌مشیِ تجاری قرار می‌گیرد. کشورها می‌توانند برای دستیابی به اهداف ملی‌شان از آن بهره بگیرند.

ان‌سی‌پی‌آی بر پایهٔ داده‌های موجود استوار است که عناصر بخصوصی از قدرت سایبری را می‌سنجند و این داده‌ها را با شاخص‌های متعددی تطبیق می‌دهد که در خودِ سازمان تهیه شده‌اند. تحلیل داده‌های ما روش‌شناسی و رویهٔ دقیقی داشته که تمام آن بر اساس تقاضا در دسترس است.

ما تحلیل خود از راهبردهای سایبری ملی را با استفاده از پردازش زبان طبیعی صحت‌سنجی کردیم. شاخص ترکیبی ان‌سی‌پی‌آی را با پدیده‌های سنجیدنیِ مربوط (هم شاخص‌های ترکیبی مشابه و هم کمیت‌های مرتبط، همچون سرانهٔ تولید ناخالص داخلی و نمایهٔ امنیت سایبری اتحادیهٔ بین‌المللی مخابرات) مطابقت داده‌ایم تا شباهت‌ها و تفاوت‌ها را بیابیم.

نمایهٔ قصدِ سایبری نشان‌دهندهٔ اولویت‌بندی‌های گوناگونی است که بعضی کشورها بر توسعهٔ اهدافی مشخص قرار می‌دهند؛ درنتیجه، [این اهداف] در مفهوم‌سازی آن‌ها از قدرت سایبری مهم‌تر از بقیه هستند.

1 Cyber Intent Index (CII).
2 Cyber Capability Index (CCI).

دربارهٔ کرهٔ شمالی، نتوانستیم برای بسیاری از قابلیت‌هایی که در نمایه‌مان فهرست کرده‌ایم سنجهٔ معتبری بیابیم؛ درنتیجه، از چندین کارشناس خواستیم ارزیابی خود از قابلیت‌های این کشور در زمینهٔ ان‌سی‌پی‌آی را در اختیارمان بگذارند. پژوهشگران و دست‌اندرکاران باید در نظر داشته باشند که در بحث از نمرهٔ ان‌سی‌پی‌آی، کرهٔ شمالی در مقایسه با دیگر کشورهای حاضر در نمایه، موردی خاص است.

برای مقیاس‌بندی شاخص‌های قابلیت سایبری از روش نرمال‌سازی کمینه‌بیشینه[1] استفاده کرده‌ایم؛ زیرا (۱) به بهترین وجه چهارچوب مفهومی ما را انعکاس می‌دهد؛ (۲) برای مشخصات داده‌ها مناسب‌ترین است؛ (۳) کاربر به‌راحتی می‌تواند آن را تفسیر کند. بخشی از فرمول ما را که به قصد مربوط است، می‌توان مشابه همچون وزن دانست.

پژوهشگران و دست‌اندرکاران باید از ان‌سی‌پی‌آی استفاده کنند تا درک جامع‌تری از مؤلفه‌های تشکیل‌دهندهٔ قدرت سایبری و روش استفاده از ابزار سایبری برای دستیابی به انواعی از هدف‌ها کسب کنند. کاربرانی که به هدف ملیِ خاصی علاقه‌مند هستند، می‌توانند ان‌سی‌پی‌آی را مبتنی بر قصد و قابلیت [و] بر اساس هدف تحلیل کنند تا درک بهتری از کشور مدنظرشان به‌دست آورند.

در این مقاله، ما ان‌سی‌پی‌آی را با نمایه‌های موجودِ مرتبط با سایبر مقابله می‌دهیم، کلیتِ چهارچوب نظری‌مان را بیان می‌کنیم، نکاتی دربارهٔ روش تفسیر یافته‌هایمان می‌گوییم، روش‌شناسیِ نمره‌دهی به قصد و قابلیت و شاخصِ ترکیبی را به‌اشتراک می‌گذاریم، منابع استفاده‌شده را فهرست می‌کنیم و مروری از محدودیت‌های رویکردمان می‌آوریم.

1 Min-Max normalization technique

هدف ان‌سی‌پی‌آی گسترش بحث دربارهٔ قدرت سایبری و نشان‌دادن این نکته است که می‌توان از چنین شاخصی برای اهداف غیرخصمانه و بی‌ضرر نیز استفاده کرد؛ همچنین اینکه این شاخص ابزاری مهم برای دولت‌ها در مسیر دستیابی به اهداف مختلف است. ما باور داریم که در زمینهٔ اهداف و قابلیت‌های ملی سایبری، نیاز به شفافیت بیشتری وجود دارد؛ تا از این طریق به‌سمت طراحی و اتخاذ سیاست‌های مرتبط و مؤثر حرکت کرده و از درگیری‌های خطرناک بین کشورها جلوگیری کنیم. امید داریم که ان‌سی‌پی‌آی بتواند بحث قدرت سایبری و فایدهٔ افزایش شفافیت دربارهٔ قابلیت‌های سایبری را یک گام به جلو ببرد.

۱. مقـــدمه

۱. مقدمه

مردم جهان تنها از قدرت و اثرگذاریِ سایبریِ تعداد معدودی از کشورها مطلع هستند؛ به‌خصوص ایالات متحده، اسرائیل، ایران، چین، روسیه و کرهٔ شمالی. بیشتر مطالب خبری فقط از حملات سایبری متجاوزانه در مقیاس بزرگ می‌گوید. این بازنمودی غلط از گسترهٔ کامل قابلیت‌ها و اهداف و دامنهٔ کنشگران فضای سایبری است. ضمناً، هنگام گزارش دربارهٔ این موارد، سنجه‌ای نظام‌مند یا حتی مقایسه‌ای میان همین طیف محدود قابلیت‌های سایبری وجود ندارد.

۱/۱. هدف انسی‌پی‌آی ۲۰۲۰ بلفر

هدف نمایهٔ قدرت سایبری ملی (انسی‌پی‌آی) ۲۰۲۰ بلفر این است که، در مقایسه با نمایه‌های موجود، سنجه‌ای کامل‌تر برای قدرت سایبری در اختیار بگذارد.

ما در سنجش قدرت سایبری، رویکرد «کل کشور» را اتخاذ کرده‌ایم. با لحاظ‌کردن «کل کشور»، تا حدی که ممکن بوده تمام ابعاد تحت‌کنترل یک دولت را در نظر گرفته‌ایم. در انسی‌پی‌آی، ما راهبردهای دولت، قابلیت‌های دفاعی و حمله‌ای، تخصیص منابع، بخش خصوصی، نیروی کار و نوآوری را می‌سنجیم. ارزیابی ما هم سنجش قدرت ثابت‌شده است و هم قدرتِ بالقوه که طی نمرهٔ نهایی‌اش، بدان معناست که دولت آن کشور می‌تواند این قابلیت‌ها را به‌شکل کارآمدی اجرا کند.

برخلاف نمایه‌های موجود در رابطه با قدرت سایبری، ما این مفهوم

را که سنجهٔ مطلقی برای قدرت سایبری وجود دارد، زیر سؤال می‌بریم و مؤلفه‌های متعددی برای قدرت سایبری ارائه می‌کنیم. گذشته از این، هر سنجهٔ قدرتِ سایبری باید در رابطه با اهداف ملی کشورِ مدنظر و تصمیم آن‌ها مبنی بر استفاده از ابزار سایبری برای دستیابی به آن اهداف لحاظ شود.

ما هفت هدف ملی را شناسایی کرده‌ایم که کشورها از راه سایبری در پی دستیابی به آن‌ها هستند. ان‌سی‌پی‌ای، قدرت سایبری را در بستر این هفت هدف ملی در نظر می‌گیرد. هیچ رده‌بندی دیگری در زمینهٔ قدرت سایبری چنین تقسیم‌بندی‌ای ندارد.

ما قصد هر کشور برای تعقیب هریک از اهداف را از طریق ارزیابی راهبردها، رتوریک و عملیات سایبری ملی می‌سنجیم. اگر قصد کشوری برای تعقیب یک هدف کم باشد، نتیجه می‌گیریم که آن هدف اهمیت کمتری برای کشور مدنظر دارد.

سپس قابلیت کشور را برای هر هدف می‌سنجیم. شاخص‌هایی که در نظر می‌گیریم هم‌راستا با تعاریفِ نهادینه‌شدهٔ قدرت سایبری در امنیت ملی هستند؛ مثلاً، قدرت سایبری به‌عنوان کشوری تعریف شده «که در پاسداری از سلامت سایبری شهروندان و کسب‌وکارها و نهادهای خود شهرتی جهانی دارد؛ رژیم‌های حقوقی و اخلاقی و مقرراتی برای پرورش اعتماد عمومی دارد؛ این توانایی را دارد که از قدرت سایبری برای مختل‌کردن یا محروم‌سازی یا تحقیر دشمنان استفاده کند».[1] اما این را نیز در نظر داریم که اهداف ملی‌ای که از راه سایبری تعقیب می‌شوند، منزوی و جداجدا نیستند. قابلیت‌های سایبری فقط بخشی از جعبهٔ ابزار هر کشورند؛ یعنی در کنار شیوه‌های سنتیِ نظامی، دیپلماسی، تحریم و

1 Jeremy Fleming, Director GCHQ, "Keynote Speech: The UK is a Global Cyber Power". International Institute of Strategic Studies, Singapore. Published February 25, 2019.

تعرفه‌ها قرار می‌گیرد و کشورها می‌توانند برای دستیابی به اهداف ملی‌شان از آن‌ها بهره بگیرند.

قدرت سایبری در بستر انسی‌پی‌آی، هنگامی است که کشوری به‌طور مؤثر قابلیت‌های سایبری خود را برای دستیابی به اهداف ملی‌اش توسعه بدهد.[1] برای ایجاد تمایز میان سطوح قصد و قابلیتِ کشورها در تمام اهداف، اصطلاح «جامعیت» را به‌کار می‌بریم که یعنی استفادهٔ کشور از ابزار سایبری به‌منظور دستیابی به اهداف متعدد (نه فقط چند هدف).

با ترکیب نمرهٔ قصد و قابلیت در تمام هفت هدف، می‌توانیم «رده‌بندی جامع قدرت سایبری»[2] را بسازیم. جامع‌ترین قدرت سایبری، کشوری است که:

- قصد پیگیریِ چندین هدف ملی از راه سایبری را دارد؛
- قابلیت‌های اساسی لازم برای تعقیب و دستیابی به اهداف یاد شده را دارد.

جامع‌ترین قدرتِ سایبریْ بالاترین میزان قدرت و قابلیت را برای دستیابی به بیشترین اهداف از راه سایبری دارد و کم‌نمره‌ترین کشور آن است که کمترین اهداف را از راه سایبری دنبال می‌کند و کمترین میزان قصد و قابلیت را دارد.

انسی‌پی‌آی به سی کشور[3] بر اساس چهارچوب منحصربه‌فرد ما نمره می‌دهد. انتخاب این کشورها بر اساس تحقیق اولیهٔ گروه‌ها دربارهٔ پنج کشوری بود که بیش از همه به‌عنوان «ابرقدرت‌های سایبری»

1 Voo, Julia., Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach. "Reconceptualizing Cyber Power". Belfer Policy Paper. Published April 2020.
2 Comprehensive Cyper Power Ranking.
3 این سی کشور عبارت‌اند از: استرالیا، برزیل، کانادا، چین، کرهٔ شمالی، مصر، استونی، فرانسه، آلمان، هند، ایران، اسرائیل، ایتالیا، ژاپن، لیتوانی، مالزی، هلند، نیوزیلند، کرهٔ جنوبی، روسیه، عربستان سعودی، سنگاپور، اسپانیا، سوئد، سوئیس، ترکیه، اوکراین، بریتانیا، ایالات‌متحده و ویتنام.

یاد می‌شدند؛[1] کشورهایی که گروه‌های اِی‌پی‌تی به آن‌ها نسبت داده می‌شود[2] و بر اساس شایعات، قدرت سایبری‌شان روبه‌رشد است. به‌دلیل محدودیت‌های منابع و دسترسی به داده‌های منبع‌باز، نتوانستیم چندان کشورهای بیشتری را بگنجانیم. کشورهای آمده در ان‌سی‌پی‌آی، چه آشکار و چه پنهان، نشان داده‌اند که میل دارند قدرت سایبری محسوب شوند.

ما رویکردی شفاف را پیش گرفتیم و سنجه‌ای تفکیک‌شده در اختیار می‌گذاریم که هم از داده‌های در دسترسِ عموم بهره می‌گیرد و هم از ارزیابی‌های کارشناسان. در این مقاله، ما ان‌سی‌پی‌آی را با نمایه‌های موجودِ مرتبط با سایبر مقابله می‌دهیم، کلیتِ چهارچوب نظری‌مان را بیان می‌کنیم، نکاتی دربارهٔ روش تفسیر یافته‌هایمان می‌گوییم، روش‌شناسیِ نمره‌دهی به قصد و قابلیت و شاخصِ ترکیبی را به‌اشتراک می‌گذاریم، منابع استفاده‌شده را فهرست می‌کنیم و مروری از محدودیت‌های رویکردمان می‌آوریم.

ان‌سی‌پی‌آی چهارچوب مفهومی و داده‌های جدیدی برای بحث دربارهٔ قدرت سایبری فراهم می‌آورد. درک سنجیده‌تر از اینکه کدام کشورها از راه سایبری در پی بعضی اهداف و قابلیت‌ها هستند (و نیستند) به طراحیِ راهبردهای بلندمدت مرتبط و مؤثرتر بهره می‌رساند.

۱ / ۲. مقابلهٔ ان‌سی‌پی‌آی با دیگر نمایه‌های سایبری

طی دههٔ گذشته، چندین سازمان سنجه‌هایی برای ابعادی از قدرت سایبریِ ملی فراهم کرده‌اند. در این بخش، مقایسهٔ مفهومی سطحِ بالایی

[1] ایالات‌متحده، بریتانیا، اسرائیل، چین و روسیه. این نکته در این منبع آمده است:
Voo, Julia., Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach. "Reconceptualizing Cyber Power". Belfer Policy Paper. Published April 2020.

[2] «پنج چشم» (The Five Eyes)، اتحادی اطلاعاتی (سیگنال و انسانی و نظامی) میان استرالیا، کانادا، نیوزیلند، بریتانیا و ایالات‌متحده است.

از ان‌سی‌پی‌آی را با سه چهارچوب پرکاربردِ سنجش قدرت سایبری ارائه می‌دهیم. این چهارچوب‌های پراستفاده در پایین آمده‌اند:

نمایهٔ «امنیت سایبری جهانی[1] (جی‌سی‌آی)»[2] از اتحادیهٔ بین‌المللی مخابرات (آی‌تی‌یو)، طی دههٔ اخیر سه بار منتشر شده است. آی‌تی‌یو بدنه‌ای از سازمان ملل است و قدیمی‌ترین سازمان بین‌المللی جهانی است. جی‌سی‌آی به‌گونه‌ای طراحی شده که توسعهٔ تاب‌آوری سایبری بین‌المللی را میان کشورهای عضو آی‌تی‌یو بپرورد. تمرکز این نمایه بر تاب‌آوریِ سایبری داخلی است و مبنای آن ارزیابی کشورهای عضو از خودشان است.

نمایهٔ «آمادگی سایبری (سی‌آرآی ۲٫۰)» از انستیتو پوتومک[3] به‌گونه‌ای طراحی شده که پختگی و تعهد هر کشور در قبال ایمن‌سازی زیرساخت‌ها و خدمات سایبری ملی‌اش را ارزیابی کند. این نمایه ۱۲۵ کشور (ازجمله ۷۵ کشور برترِ نمایهٔ توسعهٔ فناوری اطلاعات و ارتباطات از آی‌تی‌یو و نیز «گروه ۲۰») را بررسی می‌کند. جالب اینکه «سی‌آرآی ۲٫۰» به کشورهایی که تحلیل می‌کند، نمره یا رده‌بندی‌ای نمی‌دهد.

واحد اطلاعاتِ اقتصادی و بوز آلن همیلتون (ای‌آی‌یو اند بوز) در سال ۲۰۱۱ «نمایهٔ قدرت سایبری» (سی‌پی‌آی) را طراحی[4] و نوزده کشور از «گروه ۲۰» را رده‌بندی کرد.[5] برخلاف دو نمایهٔ دیگر که صرفاً امنیت سایبری را در ارتباط با قابلیت‌ها می‌سنجند، سی‌پی‌آی ادعا دارد که سنجه‌ای جامع‌تر دربارهٔ قدرت سایبری در اختیار می‌گذارد. اما گفتنی است که سی‌پی‌آی، برخلاف ان‌سی‌پی‌آیِ بلفر، قابلیت‌های تهاجمی را

1 International Telecommunications Union. 2018. Global Cybersecurity Index. Accessed May 6, 2020. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
2 Global Cybersecurity Index (GCI)
3 Potomac Institute for Policy Studies. 2015. Cyber Resilience Index. Accessed May 6, 2020. https://www.potomacinstitute.org/images/CRIndex2.0.pdf
4 Economist Intelligence Unit & Booz Allen Hamilton. 2011. Cyber Power Index. Accessed May 6, 2020. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf
5 اتحادیهٔ اروپا عضو بیستم «گروه ۲۰» است و در این رده‌بندی نیامده است.

نمی‌سنجد و عمدتاً بر شاخص‌های اقتصادی و منابع متمرکز است که هرچند برای درک پتانسیل توسعهٔ قدرت سایبری مهم‌اند، تصویر کاملی از قابلیت‌های سایبری در اختیار نمی‌گذارند.

جدول ۱، رده‌بندی ۱۰ قدرت سایبری برتر در ان‌سی‌پی‌آی را با رده‌بندی آی‌تی‌یو (۲۰۱۸) و واحد اطلاعات اقتصادی (۲۰۱۱) مقایسه می‌کند. رده‌بندی انستیتو پوتومک لحاظ نشده است؛ زیرا نمایهٔ آن‌ها کشورها را نمره‌دهی و رده‌بندی نمی‌کند.

جدول ۲، مقایسهٔ مفاهیم سطح‌بالایی است که ان‌سی‌پی‌آی و سه نمایهٔ دیگر را تشکیل می‌دهند.

جدول ۱: مقایسهٔ ده قدرت برتر

	مرکزبلفر: نمایهٔ قدرت سایبری ملی ۲۰۲۰	اتحادیهٔ‌بین‌المللی مخابرات: نمایهٔ امنیت سایبری جهانی ۲۰۱۸	واحد اطلاعات اقتصادی و بوز آلن همیلتون: نمایهٔ قدرت سایبری ۲۰۱۱
۱	ایالات متحده	بریتانیا	بریتانیا
۲	چین	ایالات متحده	ایالات متحده
۳	بریتانیا	فرانسه	استرالیا
۴	روسیه	لیتوانی	آلمان
۵	هلند	استونی	کانادا
۶	فرانسه	سنگاپور	فرانسه
۷	آلمان	اسپانیا	کرهٔ‌جنوبی
۸	کانادا	مالزی	ژاپن
۹	ژاپن	کانادا	ایتالیا
۱۰	استرالیا	نروژ	برزیل

جدول ۲: مقایسهٔ مفاهیم

	مرکز بلفر: نمایهٔ قدرت سایبری ملی ۲۰۲۰	اتحادیهٔ بین‌المللی مخابرات: نمایهٔ امنیت سایبری جهانی ۲۰۱۸	انستیتو پوتومَک: نمایهٔ آمادگی سایبری ۲/۰	واحد اطلاعات اقتصادی و بوز آلن همیلتون: نمایهٔ قدرت سایبری ۲۰۱۱
سال(های) انتشار	نمایهٔ قدرت سایبری ملی ۲۰۲۰	اتحادیهٔ بین‌المللی مخابرات:	۲۰۱۵	۲۰۱۱
تکرار	نمایهٔ امنیت سایبری جهانی ۲۰۱۸	انستیتو پوتومَک	۲	۱
هدف	نمایهٔ آمادگی سایبری ۲/۰	واحد اطلاعات اقتصادی و بوز آلن همیلتون:	سنجش تعهد کشورها در قبال ایمن‌سازی زیرساخت‌ها و خدمات سایبری ملی‌شان	سنجش قدرت سایبری کشورها
کشورهای ارزیابی‌شده	نمایهٔ قدرت سایبری ۲۰۱۱	۱۹۳ (۲۰۱۸)	۱۲۵	۱۹
شاخص‌ها	۲۷ قابلیت - ۳۲ قصد	۲۵	۷	۳۹
امتیاز	×	×		×
رده‌بندی	×	×		×
مضامین:				
اهداف ملی پیشرانِ توسعهٔ قابلیت‌ها	×			
شواهد مبنی بر حمله	×			
محتوای برخط ملی	×			
ساختارهای سایبری داخلی	×	×	×	×

	مرکز بلفر: نمایهٔ قدرت سایبری ملی ۲۰۲۰	اتحادیهٔ بین‌المللی مخابرات: نمایهٔ امنیت سایبری جهانی ۲۰۱۸	انستیتو پوتومَک: نمایهٔ آمادگی سایبری ۲٫۰	واحد اطلاعات اقتصادی و بوز آلن همیلتون: نمایهٔ قدرت سایبری ۲۰۱۱
کاهش آسیب‌پذیری سایبری	×	×	×	×
بخش خصوصی و تجارت و نوآوری	×	×	×	×
ارتباط‌پذیری	×	×	×	×
نیروی کار	×	×	×	×
چهارچوب‌های حقوقی و سیاسی داخلی و بین‌المللی	×	×	×	×

این مقایسه نشان می‌دهد که انسی‌پی‌آیْ ارزیابی دقیق و منحصربه‌فردی از اهداف ملی هر کشور را که از راه سایبری در پی نیل به آن هستند در اختیارمان می‌گذارد. گذشته از این، انسی‌پی‌آی هم مفاهیمی را لحاظ می‌کند که از دیرباز با ارزیابی‌های قدرت سایبری مرتبط بوده‌اند و هم مفاهیمی که تاکنون در ارزیابی‌های قبلی مغفول مانده‌اند.

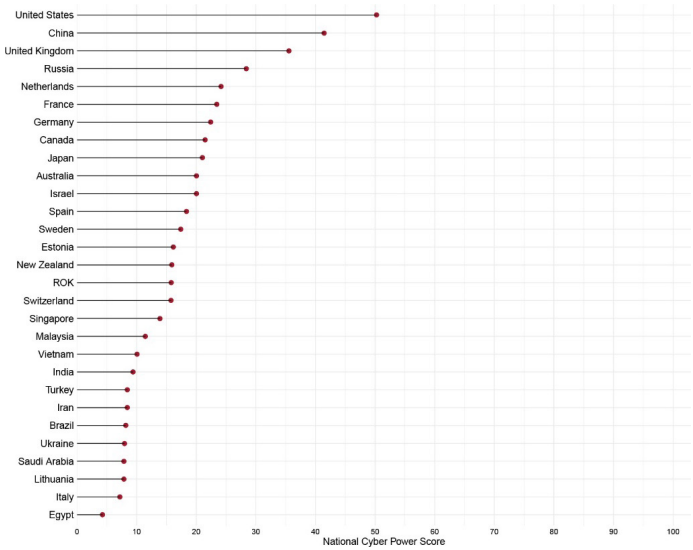
۲. نمایه قدرت سایبری ملی ۲۰۲۰

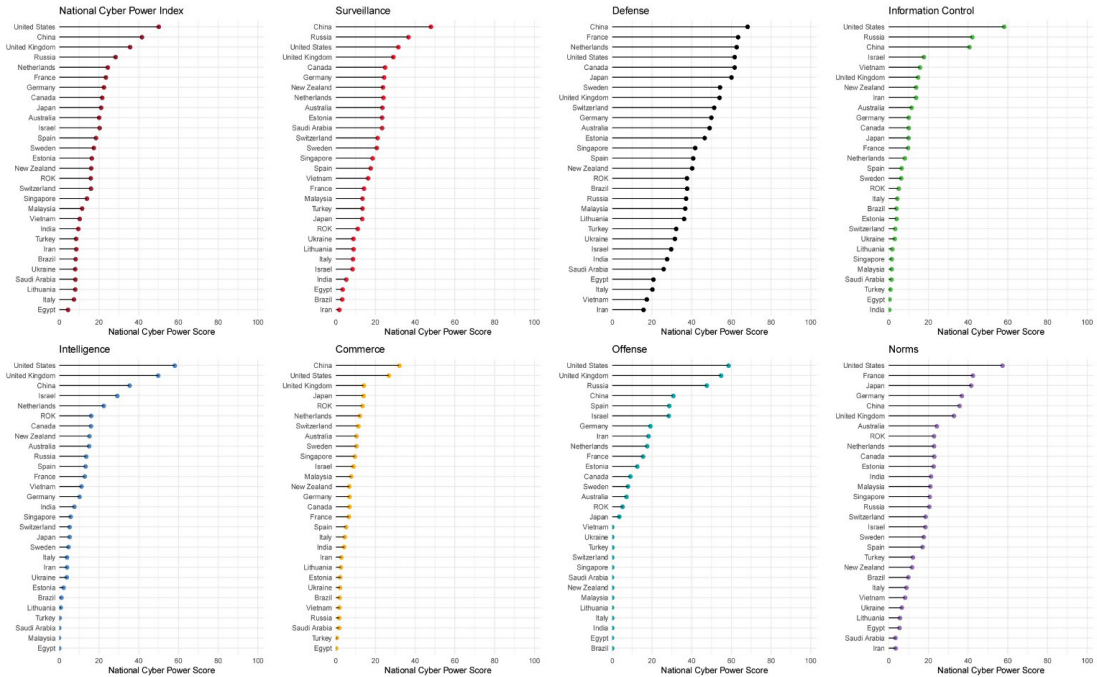
۲. نمایه قدرت سایبری ملی ۲۰۲۰

چنان‌که در شکل ۱ مشخص است، ده کشور جامعِ برتر با بالاترین میزان قصد و قابلیت در تمام اهداف هفت‌گانه به شرح زیر هستند. شکل ۲ رتبه‌بندی را بر اساس اهداف نشان می‌دهد.

۱. ایالات متحده؛ ۲. چین؛ ۳. بریتانیا؛ ۴. روسیه؛ ۵. هلند؛ ۶. فرانسه؛ ۷. آلمان؛ ۸. کانادا؛ ۹. ژاپن؛ ۱۰. استرالیا.

شکل ۱: انسی‌پی‌آی ۲۰۲۰؛ جامع‌ترین قدرت‌های سایبری

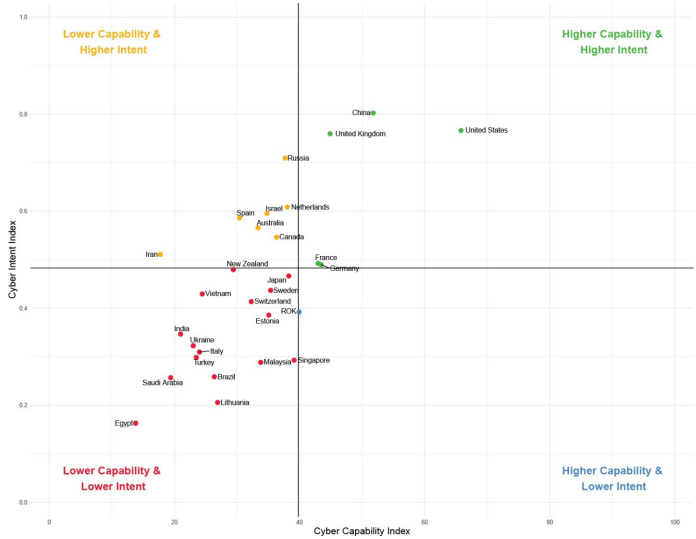




شکل ۲: انسی‌پی‌آی ۲۰۲۰ بر اساس اهداف ملی

۲/۱. تفسیر نمایهٔ قدرت سایبری ملی ۲۰۲۰

شاخص انسی‌پی‌آی می‌تواند به روش‌های گوناگونی مورد بهره‌برداریِ پژوهشگران و فعالان حوزهٔ سایبری قرار گیرد. در درجهٔ نخست اندیشمندان و خط‌مشی‌گذاران می‌توانند با استفاده از سنجهٔ تجمیعیِ انسی‌پی‌آی در زمینهٔ قدرت سایبری در تمام هفت هدف، جامع‌ترین قدرت سایبری را در میان کشورهای جهان شناسایی کنند؛ چیزی که در شکل ۱ نشان داده شده است. شکل ۱ کشورهایی را نشان می‌دهد که نمرات بالایی در زمینهٔ قصد و قابلیت برای چند هدف سایبری داشتند. این نکته ما را به این ارزیابی می‌رساند که این کشورها به‌طور مؤثری از شیوه‌های سایبری برای دستیابی به اهداف گوناگون در زمینهٔ خط‌مشی‌های خود استفاده می‌کنند. هر کشور بر اساس هر هدف نمرهٔ متفاوتی دارد.



شکل ۳: تقسیم رده‌بندی‌های قدرت سایبری در زمینهٔ قابلیت و قصد

ازآنجاکه تحلیل ما از قدرت سایبری نتیجهٔ قصد و قابلیت است، می‌توانیم کشورها را در زمینهٔ هر هدف به‌شکل چهار مربعی که در شکل ۳ دیده می‌شود، تقسیم‌بندی کنیم. دقت داشته باشید که ما این چهار مربع را بر اساس مقادیر میانگینِ قصد و قابلیت ترسیم کرده‌ایم (حداکثر مقداری که هر کشور در مجموعهٔ داده به آن دست یافته، نمرهٔ ۱۰۰ در زمینهٔ قصد و نمرهٔ ۸۰ در زمینهٔ قابلیت بود). اکثر کشورها حوالی مرکز این تقسیم‌بندی قرار می‌گیرند.

قابلیت بیشتر، قصد بیشتر

مثال: ایالات متحده، بریتانیا، چین، فرانسه، آلمان

کشورهایی که برای هدفی بخصوص (یا برای چند هدف، آن‌چنان‌که در شکل ۱ دیده می‌شود) سطح بالایی هم از قصد و هم از قابلیت دارند، رده‌بالاترین کشورها در انسی‌پی‌آی به‌شمار می‌آیند. این کشورها هم در راهبردها و هم در حملات سایبریِ قبلی‌شان نشان داده‌اند که قصد دارند از شیوه‌های سایبری برای دستیابی به اهداف سیاسی خود استفاده کنند و چنین قابلیتی هم دارند.

قابلیت بیشتر، قصد کمتر

مثال: کرهٔ جنوبی

کشورهایی که قابلیت زیادی دارند ولی میزان قصدشان برای یک یا چند هدفِ خاصْ کم باشد، تحت یکی از این دو امکان قرار می‌گیرند:

حالت اول این است که کشور مدنظر شاید فعالانه بکوشد از هدف بخصوصی بپرهیزد؛ مثلاً ازآنجاکه ایالات متحده مقر چندین شرکت بزرگ شبکهٔ اجتماعی است، تصویب قوانینی برای کنترل بهتر گفت‌وگوی

برخط، شیوه‌ای مؤثر است تا این کشور بتواند محتوای برخط را برای مخاطبان داخل کشور کنترل کند. اما ازآنجاکه این کشور پایبندِ حق آزادی بیان است که در متمم اول قانون اساسی‌اش آمده است، احتمالاً قصد چندانی برای این کار نداشته باشد.

امکان دیگر این است که کشور مدنظر بکوشد مخفیانه از قابلیت‌های سایبری خود استفاده کند، بی‌آنکه علناً اعلام کند که قصد دارد از قابلیت‌های سایبری خود برای اهدافی بخصوص بهره بگیرد.

قصد بیشتر، قابلیت کمتر

مثال: روسیه، ایران، اسرائیل، هلند

این کشورها فعالانه به دیگر کشورها نشان می‌دهند که قصد دارند قابلیت‌های سایبری خود را توسعه دهند؛ اما یا (۱) قابلیت‌های خود را (با اعلام یا عمل) افشا نکرده‌اند یا (۲) اکنون قابلیت لازم برای دستیابی به اهداف سایبری‌شان را ندارند.

در حالت دوم، این کشورها هرچند شاید آشکارا از برنامه‌های آینده بگویند، امروزه قابلیت تبدیل‌شدن به قدرت جامع سایبری را ندارند؛ مثلاً هلند در راهبرد سایبری ملی خود در سال ۲۰۱۸ اعلام کرده است که قصد دارد «از قابلیت‌های تهاجمی و واکنش وسیع‌تری در عرصهٔ سایبری ... استفاده کند»[1] به‌خصوص در برابر کنشگران اختلالگر سایبری.[2]

ایران هم مسئول انجام چندین حملهٔ سایبری شناخته شده است که

1 Netherlands National Cyber Security Strategy 2014, see https://www.enisa.europa.eu/topics/ national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/nation-al-cyber-security-strategy-1

2 هلند برای اثبات قابلیت‌هایش نه‌تنها واحدهای نظامی فعالی در زمینهٔ سایبری دارد، بلکه در سال ۲۰۱۵ به شبکه‌های اطلاعاتی روسیه نفوذ کرد. این کشورها احتمالاً اکنون قدرت سایبری خود را بر UU۳ای آینده برنامه‌ریزی می‌کنند و با قابلیت‌های سایبری خود به اهداف سیاسی دست می‌یابند و فعالانه به دیگر کشورها نشان می‌دهند که قصد توسعهٔ بیشتر قابلیت‌های فعلی‌شان را دارند. ن.ک:
https://nos.nl/nieuwsuur/artikel/2213767-dutch-intelligence-first-to-alert-u-s-about-russian-hack-of-democraticparty.html

نشان می‌دهد این کشور به‌شکلی پرخاشگرانه از طریق فضای سایبری در پی بعضی اهداف بوده است. اما یکی از کم‌امتیازترین کشورها در زمینهٔ قابلیت‌هایی است که دربارهٔ هنجارها، دفاع‌های سایبری، سود تجاری و کنترل اطلاعات برون‌مرزی دارد؛ عواملی که همه وزنی یکسان در ان‌سی‌پی‌آی دارند.

قصد کمتر، قابلیت کمتر

مثال: مصر، لیتوانی

کشورهایی که در این دسته قرار می‌گیرند، یا فعالانه در پی توسعهٔ قابلیت و قصدِ به‌کارگیری از قدرت در فضای سایبری نیستند یا اطلاعات کافی دربارهٔ راهبرد سایبری و حملات سایبری منسوب به آن‌ها یا قابلیت‌های استفاده‌شده برای سنجش قدرت سایبری در این پژوهش را منتشر نکرده‌اند (یا درباره‌شان منتشر نشده است).

تحلیل مخصوص هر کشور، با استفاده از نمودارهای راداری در بخش «ضمیمه» نشان داده شده است. افراد علاقه‌مند به هدف ملی بخصوصی در ان‌سی‌پی‌آی، می‌توانند منابع داده‌ای را که در فصل ۳ و ۴ برای قابلیت یا قصد انتخاب کرده‌ایم و به اهداف بخصوص بهره می‌رسانند، مشاهده کنند. علاوه بر نمایش امتیاز جامعیت کلی، پیشنهاد می‌کنیم سیاست‌گذاران، برای هر کشور، نمرات قابلیت و قصد را هم به‌صورت جداگانه در نظر بگیرند و هم نمرهٔ مجموع را.

۲/۲. محدودیت‌ها

تحلیل هدف‌مبنایِ ان‌سی‌پی‌آی از قدرت سایبری ملی، دچار محدودیت‌هایی هم است که عمدتاً مربوط به ماهیت موضوع «قدرت

سایبری» است. در اینجا به‌اختصار به مهم‌ترین محدودیت‌ها و مشکل‌های پیشِ روی گروه پژوهشی اشاره می‌کنیم.

۲/۲/۱. نداشتنِ داده‌های در دسترس عموم دربارهٔ قابلیت‌های سایبری

نمونه‌هایی وجود داشت که اطلاعات برای بعضی کشورها در دسترس بود، اما برای همهٔ کشورها نه. طبیعتاً مشکلاتی در کسب بعضی اطلاعات وجود داشت که طبقه‌بندی‌شده به‌شمار می‌روند؛ اطلاعاتی همچون تعداد کارکنان نظامی سایبری یا تعداد افراد فعال در سرویس‌های اطلاعاتی که حوزهٔ کاری‌شان فضای سایبری است. اما عرصه‌های دیگری وجود داشت که اطلاعات نه‌چندان حساس هم در دسترس نبودند؛ مواردی همچون تعداد کارکنان ماهر فناوری.

همچنین، کشورها ممکن است به‌عمد و بنا به اهداف راهبردی، قصد و قابلیت‌های خود را از عموم پنهان کنند. باید به این نکته توجه داشت: کشورهایی که به‌عمد ابهامی در این زمینه باقی می‌گذارند، رتبهٔ پایین‌تری در نمایه می‌گیرند. حدس می‌زنیم اسرائیل در این دسته قرار بگیرد. این نشان از مشکلِ سنجش قدرت سایبری دارد؛ هم برای تعیین قابلیت‌هایی که در زمینهٔ اهداف بخصوص قرار دارد و هم یافتن سنجه‌های این قابلیت‌های در منابعِ دسترسی‌پذیر. این را نیز اذعان می‌کنیم که گرچه هر کشور ممکن است قصدهایی داشته باشد که علنی نمی‌شوند، هر کشوری برای دستیابی به هدفی بخصوص هم به ارادهٔ سیاسی نیاز دارد و هم به‌کارگیری منابع ملی. هر دو را می‌توان از طریق انتشار راهبردها و دکترین‌های ملی نشان داد.

همچنین باوری راسخ داریم که «اندوختن ثروت یا استخراج رمزارز»

هدفی مهم برای بعضی کشورهاست و از راه‌های سایبری در پی دستیابی به آن هستند.[1] متأسفانه نتوانستیم داده‌های کافی گردآوری کنیم که با آن بتوانیم قصد و قابلیت هریک از کشورها را در زمینهٔ این هدف بسنجیم. این را هدفی مهم می‌دانیم که از راه سایبری می‌توان به آن دست یافت. امید داریم در نسخه‌های آیندهٔ ان‌سی‌پی‌آی، با دردسترس قرارگرفتنِ داده‌های بیشتر، این هدف را نیز بسنجیم.

دیگر موضوعی که به نداشتنِ نسبیِ اطلاعات در بعضی کشورها (و نه بعضی دیگر) بهره می‌رساند، این است که پژوهشگران و مفسران تا امروز عمدتاً بیشترین توجه را به کشورهای ثروتمندِ غربی نشان داده‌اند؛ درنتیجه، اطلاعات انگلیسی‌زبان بیشتری در دسترس عموم است. ارزیابی ما از راهبردهای سایبری ملی، در مواردی که نسخه‌های انگلیسی رسمی در دسترس نبود، بر ترجمه‌های انگلیسی متکی است. این ترجمه‌ها شاید چندان دقیق نباشند؛ مثلاً بعضی واژگان همچون «اطلاعات‌سازی»[2] در روسیه و چین به‌کار می‌روند، اما در کشورهای انگلیسی‌زبان نه. به همین دلیل، جایگاهِ واقعی اسرائیل و کرهٔ شمالی و ایران احتمالاً از آنچه در ان‌سی‌پی‌آی نمود یافته است بالاتر باشد.

۲/۲/۲. نداشتنِ داده دربارهٔ نایب‌ها در فضای سایبری

برای اینکه اطلاعات دربارهٔ کشورهای گوناگون (هم لیبرال‌دمکراسی و هم غیره) را بتوانیم مقایسه کنیم، از اطلاعات نیابتی دربارهٔ عملیات سایبری استفاده کردیم؛ مواردی همچون وجود راهبردهای نظامی سایبری و نسبت‌دادن حملاتِ تحت‌حمایتِ مالی دولت‌ها.

1 «اندوختن ثروت یا استخراج رمزارز» زمانی است که کشوری با استفاده از شیوه‌های سایبری، ثروت غیرقانونی یا قانونی تولید می‌کند. این امر شامل به‌کارگیری باج‌افزار و حمله به زیرساخت دیجیتالی بانک‌ها و مؤسسات مالی و اخاذی بر اساس اطلاعات کسب‌شده از طریق درز داده‌ها می‌شود. از شیوه‌های قانونی می‌توان به تولید رمزارز و مالیات‌ستانی اشاره کرد.

2 Informatization

انسی‌پی‌آی، در زمینهٔ نیابت، قدرت بعضی از کنشگران غیردولتی، همچون شرکت‌های فناوری، را نیز شامل می‌شود. هرجا شرکت‌های فناوری به قدرتِ اقتصادی کشوری و اکوسیستم نوآوری آن بهره‌ای برسانند، در امتیاز نمایهٔ تکامل دیجیتال[1] گنجانده شده‌اند. اما این شامل قدرت فوق‌العاده‌ای نمی‌شود که بعضی از شرکت‌های فناوریِ مستقل از دولت و صرفاً به‌واسطهٔ گسترهٔ جهانی و قدرت یارانش و توسعهٔ فناورانهٔ خودشان دارند. گوگل، فیسبوک، بایدو، و یا هوواوی شاید به‌تنهایی در نمایهٔ ما جایگاهی به‌اندازهٔ بعضی از کشورهای سطح‌بالا کسب کنند. کشورهای میزبان این شرکت‌ها به‌لحاظ قابلیت فنی و دسترسی به اطلاعات، مزایای آن‌ها را خواهند داشت.

نمونهٔ دیگر، یکی از پرکارترین ابزارهای جمع‌آوری اطلاعات است که در اسرائیل ساخته شد و بی‌گمان برای دولت اسرائیل فوایدی به‌ارمغان خواهد آورد. انسی‌پی‌آی شامل قدرت گروه‌های مزدوری نمی‌شود که درون مرزهای ملی کشوری جای دارند؛ چه وابسته به دولت باشند و چه نه. چندین حملهٔ مخربی که ریشه در چین و روسیه و دیگر کشورها داشته‌اند، به گروه‌های مزدور و دیگر کنشگران غیردولتی منسوب شده‌اند.

۳/۲/۲. ساده‌سازی‌ها

قدرت متعارف نظامی، در مقایسه با قابلیت‌های سایبری، معیارهای ملموس‌تری همچون تعداد آموزشگاه‌ها، سربازان، تانک‌ها و زرادخانه‌های هسته‌ای دارد. تعیین اینکه چه‌چیز «سلاح سایبری» محسوب می‌شود کار دشوارتری است.

فرض ما بر این است که شاخص‌های انسی‌پی‌آی انعکاس دقیقی

1 Digital Evolution index score

از ظرفیت و قابلیت واقعی یک کشور در دستیابی به آن اهداف است. در ان‌سی‌پی‌آی، هر هدف بین پنج تا ده شاخصِ قابلیت دارد. اگر قرار است قابلیت‌های کشورها را کمی‌سازی و مقایسه کنیم، از این ساده‌سازی گریزی نیست. اما به این نکته واقفیم که (۱) این شاخص‌ها شاید سنجهٔ دقیق و جامعی از کلیت قابلیت یک کشور نباشند و (۲) تمام داده‌های موجود در مالکیت عمومی کامل و دقیق نیستند.

هرجا میسر بوده، از داده‌هایی استفاده کرده‌ایم که دست‌اندرکاران و اساتید دانشگاه به‌طور گسترده‌ای از آن‌ها استفاده کرده‌اند و منبعشان مؤسسات شناخته‌شده‌ای همچون سازمان ملل یا بانک جهانی یا دولت‌های ملی و دیگر نمایه‌هایی است که روش‌های مطمئنی برای جمع‌آوری داده در سطح جهان دارند (مثلاً نمایهٔ خانهٔ آزادی[1]).

داده‌های نوآورانه و کم‌آوازه‌تری را نیز به‌کار گرفته‌ایم که کمک می‌کنند دامنهٔ وسیع‌تری از قابلیت‌های سایبری را ثبت کنیم؛ مثلاً برای سنجش توانایی هر کشور برای کنترل محیط اطلاعاتی، از داده‌هایی در زمینهٔ درخواست حذف از گوگل و آمارِ صد وب‌سایت برترِ آمازون الکسا استفاده کرده‌ایم.[2]

۲/۲/۴. ثبت دوگانگیِ قابلیت‌های سایبری

یکی از مشکل‌های سنجش قدرت سایبری، لحاظ‌کردنِ دوگانگیِ آن است. بعضی از قابلیت‌ها در راستای هدفی ملی به قدرتِ سایبری

1 ن.ک: www.freedomhouse.org

2 گوگل سرویس درخواست حذف دارد که طی آن، کاربران می‌توانند محتوایی از یک محصول گوگل را که به نظرشان تخطی از قانون یا حق‌وحقوقشان است، گزارش بدهند. گوگل سپس محصول را ارزیابی می‌کند و امکان مسدودکردن، محدودکردن یا حذف دسترسی به آن وجود دارد. ما از داده‌هایی دربارهٔ درخواست‌های دولت‌ها مبنی بر حذف محتوا از طریق گزارش شفافیت گوگل استفاده کردیم. ن.ک:
https://transparencyreport.google.com/government-removals/overview?hl=en
برای داده‌های جمع‌آوری‌شده از سوی آمازون دربارهٔ صد وب‌سایت برتری که کاربران اینترنت با مرورگرهای گوناگون باز کرده‌اند، ن.ک:
https//:alexa.com

می‌افزایند؛ اما برای هدف دیگری مضرند؛ مثلاً اگرچه جمعیتی با دسترسی گسترده به اینترنت می‌تواند برای تلاش‌های دولت در راستای پایش اینترنت مفید باشد، تأثیر بالقوهٔ حملاتْ محتمل‌تر و شدیدتر می‌شود. درنتیجه، درصد کاربران متصل به اینترنت در یک کشور را برای پایش اینترنتْ مفید و برای دفاعْ منفی در نظر می‌گیریم.

گذشته از این، در میان داده‌های متن‌باز و در دسترس، بعضی داده‌ها می‌توانند هم سنجهٔ قصد باشند و هم قابلیت؛ مثلاً هر عملیاتی در ردیاب عملیاتِ سایبریِ شورای روابط خارجی، هم سنجهٔ قصد است و هم قابلیت. دولت، با داشتن عملیاتی تحت‌حمایت مالی خود، هم قصدِ خود را برای دستیابی به هدفی در فضای سایبری نشان می‌دهد و هم قابلیتِ انجام این کار را؛ مثلاً هنگامی که مصالحهٔ شرکت سرگرمی «سونی پیکچرز» را به کرهٔ شمالی منسوب می‌کردند، جامعهٔ بین‌الملل دریافت که کرهٔ شمالی با ممنوعیت تماشای فیلم‌ها، هم قصد و هم قابلیت کنترل محیط اطلاعاتی را دارد.

نمونهٔ دیگر مربوط به قانون‌گذاری ملی در زمینهٔ سایبری است. قانون‌گذاری ملی در زمینهٔ سایبری، هم گسترهٔ قصد یک کشور برای کنترل فعالیت‌های سایبری را نشان می‌دهد و هم قابلیت یا بودجه‌ای را که دولت برای این کار اختصاص می‌دهد. برای رفع تضاد در این دو مثال، سنجه‌های متفاوتی از مجموعه‌داده‌های مشابه ایجاد کرده‌ایم. برای ردیاب عملیات سایبری، اگر کشوری دست‌کم یک عملیات انجام داده که به هدف مدنظر نایل شده است، آن را شاخص قصد در نظر گرفته‌ایم.[1] سپس تعداد عملیات منسوبی را که به این هدف نایل شده‌اند، به‌عنوان سنجهٔ قابلیت در نظر گرفته‌ایم. برای قانون‌گذاری سایبری، قصد را با

1 یکی از محدودیت‌های پژوهش ما این است که نمی‌توانیم عملیات سایبری غیرمنسوبی را که رخ داده است، در نظر بگیریم.

تحلیل قوانین و راهبردهای بخصوص می‌سنجیم و برای سنجش قابلیت، انواع قانون‌گذاری سایبری و تسلسل زمانی به‌روزشدن آن‌ها را در نظر می‌گیریم.

۳. چهارچوب نظری

۳. چهارچوب نظری

کشورها از قابلیت‌های سایبری برای دستیابی به اهداف سیاسی کلی خود استفاده می‌کنند. در این بخش، اهداف ملی‌ای را زیر ذره‌بین قرار می‌دهیم که کشورها از دیرباز از راه سایبری در پی دستیابی به آن‌ها بوده‌اند. سپس بررسی می‌کنیم قصد یک کشور برای تعقیب این اهداف و قابلیت‌های لازم برای نیل به آن‌ها چگونه فرمول ما برای قدرت سایبری را ایجاد می‌کند.

۳/۱. اهداف ملی

با آنکه فرض درستی به نظر می‌آید که هر کشوری بیشترین قابلیت فنی و بهترین تجهیزات را داشته باشد، قوی‌ترین کشور است، ما استدلال می‌کنیم که قدرت سایبری از اجزای گوناگونی تشکیل شده است. ما رویکردی همه‌جانبه داریم و تمام اجزا را در ارزیابی قدرتِ سایبریِ کلی لحاظ می‌کنیم. قدرت سایبری را باید در نسبت با اهداف ملی هر کشور سنجید.

جامع‌ترین قدرتِ سایبری متعلق به کشوری است که با بیشترین توانایی، از طریق شیوه‌های سایبری، به بیشترین اهداف نایل می‌شود. ما به این نکته واقفیم که کشورها شیوه‌هایی غیرسایبری نیز برای دستیابی به اهداف خود دارند و یک کشور ممکن است سراغ آن شیوه‌ها برود؛ اما در چهارچوب انسی‌پی‌آی، ابزارهای دیگری را که در اختیار هر کشور

است، لحاظ نمی‌کنیم؛ مثلاً کشوری که در پی پایش و رصد گروه‌های داخلی است، می‌تواند از راه‌های سایبری برای تکمیل ابزار سنتیِ موجود استفاده کند؛ مانند جمع‌آوری اطلاعات انسانی و انجام پایش فیزیکی. تمرکز پژوهش ما بر این موضوع است که یک کشور چگونه قابلیت سایبریِ خود را توسعه می‌دهد و در راستای رسیدن به اهداف ملی از آن استفاده می‌کند.

برای درک میزان توانمندی هر کشور ابتدا انواع اهداف ملی‌ای را شناسایی کردیم که هر کشور ممکن است با ابزارهای سایبری در پی دستیابی به آن‌ها باشد. نظریهٔ روابط بین‌الملل زیربنای درک ما از این است که کشورها چگونه اهداف خود را به‌شکل نظری درمی‌آورند. پایگاه دادهٔ عملیات سایبریِ شورای روابط خارجی[1] دربارهٔ رویدادهایی که رسماً به حمایت یک دولت منسوب شده‌اند، به ما اطلاعاتی می‌دهد از اینکه بعضی کشورها چگونه از قابلیت‌های سایبری خود استفاده کرده‌اند. بر اساس این پژوهش، هفت هدف سایبری را شناسایی کرده‌ایم که کشورها بین سال‌های ۲۰۰۵ تا ۲۰۱۹ در پی دستیابی به آن‌ها بوده‌اند. این اهداف در جدول ۳ آمده‌اند.

1 بیشتر اهداف از طریق تحلیل «ردیاب عملیات سایبری» شورای روابط خارجی شناسایی شدند. ن.ک:
https://www.cfr.org/interactive/cyber-operations
ما همچنین هر حملهٔ سایبریِ درون پایگاه داده را (تا دسامبر ۲۰۱۹) با اهداف یادشده مطابقت داده‌ایم تا حملات سایبری واقعی و تاریخی را به سنجه‌ای برای قابلیت سایبری تبدیل کنیم.

جدول ۳: تعریف اهداف ملی[1]

اهداف قدرت سایبری؛ اهداف رایجی که کشورها از طریق فضای سایبری در پی دستیابی به آن‌ها هستند (بر اساس پژوهش گروه قدرت سایبری مرکز بلفر)
پایش و رصد گروه‌های داخلی؛ کشور اقداماتی انجام داده تا به خود مجوز قانونی و قابلیت رصدِ سایبری برای پایش و شناسایی و جمع‌آوری اطلاعات دربارهٔ تهدیدهای داخلی و کنشگران درون مرزهای خود بدهد. از این اقدامات می‌توان به تلاش برای رصد شهروندان، پایش ترافیک اینترنت، دورزدن رمزگذاری یا شناسایی و ایجاد اختلال در سرویس‌های اطلاعاتیِ خارجی، سازمان‌های مجرم و گروه‌های تروریستی اشاره کرد.
تقویت و ارتقای دفاع سایبری ملی؛ کشور ارتقای دفاع از دولت و دارایی‌ها و سیستم‌های ملی را در اولویت قرار داده و بهداشت و تاب‌آوری سایبری ملی را افزایش داده است. این امر شامل دفاع فعال از دارایی‌های دولت و ترویج امنیت سایبری و بهداشت سایبری در صنایع کلیدی و عموم مردم و نیز افزایش آگاهی ملی از تهدیدهای سایبری است.
کنترل و دست‌کاری محیط اطلاعاتی؛ کشور با انعکاس دوگانگیِ کنترل اطلاعات و استفاده از ابزار الکترونیکی برای کنترل اطلاعات و تغییر روایت‌های درون‌مرزی و برون‌مرزی را در اولویت قرار داده است. یا کوشیده است از محرمانگیِ اینترنت و آزادی بیان شهروندانش پاسداری کند. این هدف شامل گسترش پروپاگاندای داخلی و ایجاد و تقویت دروغ‌پراکنی و استفاده از قابلیت‌های سایبری برای هدف‌گرفتن و ایجاد اختلال در گروه‌هایی است که در حالت عادی، خارج از حوزهٔ اختیارات آن کشور قرار می‌گیرند. هدف آخر، شامل حذف مطالب افراطی از شبکه‌های اجتماعی ورد پروپاگاندای خارجی است.
جمع‌آوری اطلاعات در کشورهای دیگر برای امنیت ملی؛ کشور رازهای ملیِ دشمنی خارجی را از طریق شیوه‌های سایبری استخراج کرده است. این هدف متمرکز بر جمع‌آوری اطلاعاتی نیست که به‌لحاظ تجاری حساس باشد؛ بلکه اطلاعاتی است که بر فعالیت‌های دیپلماتیک، برنامه‌ریزی نظامی، پایش پیمان‌ها و دیگر موقعیت‌هایی تأثیر می‌گذارد که کشور در پیِ بهبود آگاهی موقعیتی خود و درک یک کشور خارجی است. از این موارد می‌توان به هک و نفوذ به مواد طبقه‌بندی‌شده، همچون برنامه‌ریزی‌های نظامی، اشاره کرد؛ اما سرقت سوابق کارکنان و دسترسی به ارتباطاتِ شخصیت‌های رده‌بالای دولت، همچون اعضای مجلس، را نیز در بر می‌گیرد.
افزایش قابلیت سایبری و فنی ملی؛ کشور یا کوشیده صنعت فناوری داخلی خود را تقویت کند یا از ابزار سایبری برای توسعهٔ دیگر صنایع داخلی استفاده کرده است. این کار می‌تواند از طریق شیوه‌های قانونی و غیرقانونی انجام شود. از شیوه‌های غیرقانونی می‌توان به انجام جاسوسیِ صنعتی در شرکت‌ها و کشورهای خارجی برای تسهیل انتقال فناوری اشاره کرد. از شیوه‌های قانونی می‌توان به سرمایه‌گذاری در تحقیق و توسعهٔ امنیت سایبری و اولویت‌بخشی به توسعهٔ نیروی کار امنیت سایبری اشاره کرد.

1 جدول را مؤلفانِ پژوهش نوشته‌اند.

اهداف قدرت سایبری؛ اهداف رایجی که کشورها از طریق فضای سایبری در پی دستیابی به آن‌ها هستند (بر اساس پژوهش گروه قدرت سایبری مرکز بلفر)
تخریب یا غیرفعال‌سازی زیرساخت‌ها و قابلیت‌های دشمن؛ کشور از فنون و تاکتیک‌ها و رویه‌های سایبریِ مخرب استفاده می‌کند تا توانایی دشمن در مبارزه در عرصه‌های سایبری و متعارف را مختل یا فسوده یا تضعیف کند. این امر شامل حملات سایبری به زیرساخت‌های حیاتی و حملات منع سرویس توزیع‌شده (ddos) به شبکه‌های ارتباطی دولت می‌شود. در این حوزه، می‌توان به حملات سایبری با هدف نشان‌دادن قصد و قابلیتِ بازدارِی دشمن از کنش نیز اشاره کرد.
تعریف استانداردهای فنی و هنجارهای سایبری بین‌المللی؛ کشور به‌صورت فعال در مباحثات حقوقی و سیاسی و فنی دربارهٔ هنجارهای سایبری شرکت می‌کند. این امر شامل امضای پیمان‌های سایبری، مشارکت در کارگروه‌های فنی، عضویت در اتحادها و همکاری‌های سایبری برای مبارزه با جرایم سایبری و هم‌رسانیِ تخصص و قابلیت فنی است.

هدف هشتم: اندوختن ثروت یا استخراج رمزارز

انسی‌پی‌آیِ ۲۰۲۰، کشورها را در راستای هفت هدف می‌سنجد؛ اما جای یک هدف مشخصاً خالی است؛ که آن را «اندوختن ثروت یا استخراج رمزارز» می‌نامیم. تعریف این هدف عبارت است از «تولید ثروت قانونی یا غیرقانونی به‌واسطهٔ ابزارها و روش‌های سایبری». این امر شامل به‌کارگیری باج‌افزار، حمله به زیرساخت‌های سایبری بانک‌ها و مؤسسات مالی و اخاذی برا اطلاعات کسب‌شده از راه هک یا درز داده‌ها می‌شود. شیوه‌های قانونی، همچون ایجاد مشوق و ترغیب کنشگران داخلی به توسعهٔ محصولات صادرکردنیِ امنیت سایبری و نیز توسعهٔ رمزارز، مشمول این مفهوم می‌شوند.

ما کوشیدیم داده‌های خودمان را جمع‌آوری کنیم تا «اندوختن ثروت و استخراج رمزارز» را از طریق بررسی داده‌های موجود دربارهٔ نقدکردن بیت‌کوین و آمار حفاری و شیادی‌های موفقِ منسوب به کنشگران مجرمِ

درون یک کشورِ بخصوص نشان دهیم. البته به این نکته هم واقفیم که بخش زیادی از این فعالیت‌ها تحت‌حمایت دولت‌ها نیست.[1]

متأسفانه برای نمایهٔ امسال نتوانستیم داده‌های بالا را بیابیم؛ سنجه‌هایی برای قابلیت‌هایی که بتواند نایب قابلیت‌های مدنظرمان باشد هم نیافتیم. درنتیجه، این هدف را از پژوهش امسال خارج کردیم؛ زیرا داده‌هایِ موجودْ نتایج را تحریف می‌کرد. امیدواریم داده‌های مرتبط برای سنجش قابلیت‌های «اندوختن ثروت و استخراج رمزارز» طی سال‌های آینده در دسترس قرار بگیرد تا بتوانیم آن را در نسخه‌های آتی ان‌سی‌پی‌آی بگنجانیم.

چه اهدافی برای کشورها اولویت دارند و چگونه می‌توان آن‌ها را شناسایی کرد؟

برای سنجش قدرت سایبری یک کشور، باید به پرسش‌های زیر پاسخ دهیم:

- کشور چه هدف یا اهدافی را می‌خواهد از طریق فضای سایبری دنبال کند؟
- کشور چه قابلیت‌هایی برای نیل به آن هدف یا اهداف دارد؟

پرسش نخست، سنجهٔ قصد است و پرسش دوم، سنجهٔ قابلیت. هر دو اصطلاح در تعریف کلاسیکِ قدرت ملی و بحث از تهدید دشمنان استفاده‌می‌شوند.[2]

قصد سنجهٔ کم‌وکیفِ طرح‌های برنامه‌ریزی دولت (یعنی راهبردهای امنیت سایبری و برنامه‌های بحران و دیگر اسناد برنامه‌ریزی دولتی) است.

1 https://qz.com/1194051/a-new-world-bank-project-shows-that-wealth-not-gdp-is-the-bestgauge-of-a-countrys-progress/ ن.ک:
2 https://www.heritage.org/military-strength/introduction and https://www.dhs.gov/xlibrary/ assets/dhs_risk_lexicon.pdf ن.ک:

قصد، ارزیابیِ سوبژکتیو «رفتار مشاهده‌شدهٔ» دولت در رابطه با موضوعات سایبری است.[1]

قابلیت‌ها سنجه‌های کم‌وکیفِ برون‌داد کشور در رابطه با یک یا چند هدف سایبری‌اند (یعنی تعداد حق امتیازهای ثبت‌شده در سال و تعداد شرکت‌های امنیتیِ برتر در سطح جهان و تعداد کارکنان ماهر).

تمایز میان **قصد** و **قابلیت** به دو دلیل اهمیت دارد:

در حالت اول، یک دولت ممکن است قابلیتِ دستیابی به یک هدف از راه سایبری را داشته باشد؛ اما قصد چنین کاری نداشته باشد.

حالتِ دیگر این است که یک دولت ممکن قصد نیل به هدفی از راه سایبری را داشته باشد، اما فاقد قابلیت یا منابع موردنیاز برای انجام این کار باشد.

۲/۳. فرمول نمایهٔ قدرت سایبری ملی

برای فرمول انسی‌پی‌آی، از اطلاعات و ادبیات پژوهشی قدرت ملی استفاده می‌کنیم.[2] در این منابع، شاخصه‌های قصد و قابلیت در هم ضرب می‌شوند تا برآوردهای تهدید و قدرت به‌دست آید.[3]

رابطه‌ای پویا میان قابلیت و قصد وجود دارد. اگر قابلیت را توانایی پایهٔ اعمال قدرت سایبری در نظر بگیریم، پس قصد کشور هم بُردار آن است؛ یعنی هم گستره و هم جهتِ حرکت قدرت سایبری را مشخص می‌کند. قصد قوی، اثرات قابلیت سایبری را بزرگ‌نمایی می‌کند؛ حال آنکه نمرهٔ پایینِ قصد، بازدارندهٔ قابلیتِ بالاست.

ما هر کشور را بر اساس قصدِ تعقیب هریک از هفت هدف و قابلیتِ

1 https://www.mitre.org/sites/default/files/pdf/10_2914.pdf
2 Singer, J. D. (1958). Threat-perception and the armament-tension dilemma. Journal of Conflict Resolution, 2(1), 90-105.
3 Cline, R. S. (1993). The power of nations in the 1990s: a strategic assessment. University Press of America.

دستیابی به آن‌ها نمره‌دهی می‌کنیم. نمرات قصد انسی‌پی‌آی را با ضرب قابلیت‌های هر کشور در قصد آن (برای هر هدف ملی) محاسبه می‌کنیم. نمرهٔ قصدِ انسی‌پی‌آی، انعکاس اولویت‌های گوناگونی است که بعضی کشورها بر قابلیت‌های سایبریِ بخصوص می‌گذارند؛ درنتیجه، می‌توان آن را عاملی مهم به‌شمار آورد. این یعنی اگر کشوری قصد ۱۰۰درصدی برای انجام کاری را نشان دهد، می‌تواند در یک عرصه، مثلاً رصد ملی، به‌طور کامل از قابلیتِ سایبریِ خود استفاده کند.

درنتیجه، در انسی‌پی‌آی، کشور فقط در صورتی برای یک هدف نمرهٔ بالا می‌گیرد که هم قصدِ زیادی داشته باشد و هم قابلیت‌های لازم برای دستیابی به آن را؛ زیرا قابلیت یا قصد هیچ‌یک به‌تنهایی کافی نیستند. در قالب فرمول، قدرت سایبری ملیِ یک کشور حاصل‌ضرب قابلیت و قصد است:

$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{7}\sum_{x=1}^{7} Capability_x * Intent_x$$

که در آن، x درواقع یکی از این هفت هدف است:

- پایش و رصد گروه‌های داخلی؛
- تقویت و ارتقای دفاع سایبری ملی؛
- کنترل و دست‌کاری محیط اطلاعاتی؛
- جمع‌آوری اطلاعات در کشورهای دیگر برای امنیت ملی؛
- افزایش قابلیت سایبری و فنی ملی؛
- تخریب یا غیرفعال‌سازی زیرساخت‌ها و قابلیت‌های دشمن؛
- تعریف استانداردهای فنی و هنجارهای سایبری بین‌المللی.

۴. روش‌شناسی و بحث

۴. روش‌شناسی و بحث

۴/۱. نمره‌دهی به قصد و منابع

برای پی‌بردن به اینکه هر کشور در پی چه هدف یا اهدافی است، مجموعه‌ای ایجاد کردیم از ۳۲ شاخص منحصربه‌فردِ قصد، ارزیابی‌های افزوده‌ای که «فاکتورهای قصد» نامیده شده‌اند و داده‌های مربوط به حمله‌های منسوب که در مجموع، نمرهٔ قصد را در اختیارمان می‌گذارند. نیمی از نمرهٔ قصد با استفاده از شاخص‌هایی رقم می‌خورد که از اسناد سایبری عمومی هر کشور و اعلامیه‌های عمومی و راهبردهای سایبری ملی، ازجمله شواهد مربوط به بودجه‌رسانی، به‌دست آمده‌اند. با توجه به اهمیتی که برای قصدِ نشان‌داده‌شده قائل شده‌ایم، ۵۰درصدِ باقیِ نمره به شواهد مربوط به حملات منسوب اختصاص دارد.

از این شواهدِ مربوط به حملات منسوب، در کنار دیگر شاخص‌هایی که نشان از برنامه‌ریزی و تمایل قبلی دارند، می‌توان قصد کلی را استنباط کرد؛ آنچه «از ارتکاب»، یعنی از اقدامات یک کشور مفروض داشته می‌شود.[1] درنتیجه، مقاصد یک کشور را می‌توان از حملات سایبری و فعالیت‌هایش نیز استنباط کرد.

ما قصد نشان‌داده‌شده را نیز لحاظ کرده‌ایم؛ زیرا یک کشور ممکن است مقاصدِ خود برای دستیابی به هدفی خاص را بنا به دلایل راهبردی

1 Riverside City Sheriff's Department (1975). Element of Intent in Criminal Law. Mount San Jacinto College.

آشکارا اعلام نکند. اما شاید شواهدی در دسترس باشد که نشان دهد فلان کشور از طریق عملیات سایبریِ منسوب، در پی نیل به این اهداف بوده است؛ مثلاً دولت چین سال‌ها جاسوسیِ سایبری برای سرقت مالکیت فکری را انکار کرده و این اتهامات را «افتراآمیز» خوانده است.[1] اما چندین سازمان بخشِ خصوصی، در تحلیل‌های خود، عملیات سایبری علیه سازمان‌های ایالات متحده را به کنشگران دولتی چین نسبت داده‌اند.[2]

ما مدخل‌های ردیاب عملیات سایبریِ شورای روابط خارجی را از ۲۰۱۵ تا دسامبر ۲۰۱۹ بررسی کردیم تا مشخص کنیم چه زمانی عملیاتی سایبری را به کشوری نسبت داده‌اند و این عملیات در دستیابی آن کشور به یکی از هفت هدف کمک کرده است. اگر یک یا چند عملیات سایبری به کشوری منسوب شده بود، نمرهٔ کامل قصدِ نشان‌داده‌شده برای آن هدف را به کشور می‌دهیم. به‌دلیل ماهیت پنهانِ عملیات سایبری، فرضمان بر این است که اگر عملیاتی سایبری به کشوری نسبت داده شود، احتمالاً این کشور عملیات سایبری دیگری نیز برای دستیابی به اهداف مشابه انجام داده است و احتمالاً در آینده نیز از همین روش‌ها استفاده خواهد کرد.

در رابطه با قصد اعلام‌شده، رویکردی دوسویه را پیش گرفتیم: ارزیابی قصد اعلام‌شدهٔ هر کشور بر اساس اهداف علنی و نیز تحلیل ژرف قصد کلی.

تعدادی از نهادهای بین‌المللی، همچون سازمان ملل و اتحادیهٔ اروپا، توصیه می‌کنند کشورها راهبرد سایبری ملی تولید کنند. اتحادیهٔ

1 Philip Wen. (2018) "China Denies Slanderous Economic Espionage Charges from US allies". Reuters.
2 بسیاری از این حملات در ردیابِ عملیات سایبریِ شورای روابط خارجی ثبت شده‌اند.

بین‌المللی مخابرات خاطرنشان می‌کند که «با توسعه و اجرای راهبرد امنیت سایبری ملی، هر کشوری می‌تواند امنیت زیرساخت دیجیتالی خود را تقویت کند و سرانجام به آرزوهای اجتماعی‌اقتصادی گسترده‌ترِ خود بهره برساند. رهبران ملی باید برای فرصت‌های پیش آمده و نیز خطراتی که در کمیتِ کشورشان وجود دارد، از محیط دیجیتال استفادهٔ راهبردی کنند؛ همچنین باید چشم‌اندازی شفاف از آیندهٔ دیجیتالی مطلوبشان ترسیم کنند».[1] بر این مبنا، ما به چند عامل نگریستیم که به راهبردهای سایبری هر کشور مرتبط‌اند، عواملی ازجمله:

- راهبرد سایبری کشور تا چه حد جامع است؟ آیا اقدامات و مالکان و اهدافِ بخصوص را در بر می‌گیرد؟
- کشور چه مدت راهبردی سایبری داشته است؟
- کشور هر چند وقت یک بار راهبرد سایبری خود را روزآمد می‌کند؟
- آخرین باری که کشور راهبرد سایبریِ خود را روزآمد کرده است کی بوده؟
- آیا کشور از زمان انتشار آخرین راهبرد خود، افزایش بودجهٔ سایبری را اعلام کرده است؟

ما راهبرد سایبری هر کشور و نیز دیگر اسنادِ مشابه را تحلیل متنی کردیم تا مشخص کنیم چه اهدافی در هر سند ترسیم شده است. برای صحت‌سنجیِ یافته‌ها، از پردازش زبان‌های طبیعی (ان‌ال‌پی)[2] استفاده کردیم تا واژگان و سه‌واژه‌ها (مجموعهٔ سه واژهٔ پیاپی) را از دل هر راهبرد استخراج کنیم. هرجا یک‌واژه یا سه‌واژه، که به هدفی ارجاع دارد، با استفاده از ان‌ال‌پی ظاهر شد، اما از طریق اسکن دستی نشد، ارزیابی‌مان

1 International Telecommunications Union. (2018). "Guide to Developing a National Cybersecurity Strategy—Strategic Engagement in Cybersecurity".
2 Natural language processing (NLP).

را دوباره انجام دادیم؛ مثلاً واژه‌های «هنجارها و بین‌المللی و اینترپل» احتمالاً به هنجارهای بین‌المللی ارجاع داشته باشد؛ حال آنکه منظور از سه‌واژهٔ «فعالانه و مجازات و دشمن» احتمالاً تخریب زیرساخت‌های دشمن باشد. کشورهایی همچون ایران که راهبردشان در دسترس عموم نیست، با استفاده از تحلیل کارشناسانه و اسناد طرف سوم بررسی شدند تا قصدشان برای دستیابی به اهداف شناسایی و نمره‌دهی شود.

کشوری که راهبرد سایبری دیرینه و در دسترسی دارد و راهبردش بودجهٔ دولتی دریافت می‌کند، چهارچوب حاکمیتِ نهادینه‌شده‌تری دارد که اجرای راهبرد را تسهیل می‌کند.[1] راهبرد سایبریِ دیرینه و در دسترس، نمرهٔ قصد یک کشور را افزایش می‌دهد. با توجه به ماهیت پویای فضای سایبری و تهدیدها و فرصت‌های دائم‌التغییر، هر کشور که مرتب راهبرد خود را بازبینی نکند، کمتر احتمال دارد از پیشگامان تفکر سایبری باشد.

مطالعهٔ نسخه‌های گوناگونِ راهبردهای سایبری ملی نشان داد که کاربستِ شیوهٔ سایبری چقدر به‌مرور زمان تکامل یافته است. نگاه به اینکه آیا عملیاتی سایبری که به یکی از هفت هدف نایل شده، منسوب به دولتِ یک کشور بوده است یا نه، نشان‌دهندهٔ عزم کشور برای دستیابی به آن هدف از راه سایبری است. کشورهایی که در مدت طولانی‌تری، پیوسته در پیِ اهداف سایبری بوده‌اند، نمرهٔ بالاتری می‌گیرند.

ما تحقیق گسترده‌ای دربارهٔ وب‌سایت‌ها و نشریات برخط و نظرات چهره‌های مطرح سیاسی هر کشور در رسانه‌ها انجام دادیم. به‌استثنای کرهٔ شمالی، فقط منابع منسوب یا رسمی دولت را بررسی کردیم. از منابع طرف سوم یا اطلاعات درزکرده یا هک‌شده استفاده نکردیم؛ زیرا می‌خواستیم پیام خاصی را مشخص کنیم که کشور دربارهٔ اهداف

1 البته ما به این نکته واقفیم که بعضی از ناهنجاری‌ها می‌توانند خط‌مشی دولت را اجرا کنند و بدون هیچ راهبرد عمومی و مسیر مشخصی، مؤثر واقع شوند.

و مقاصدش می‌خواهد مخابره کند. سرانجام، عضویت و مشارکت در نهادها و سازمان‌های بین‌المللی را تحلیل کردیم.

جدول ۴ نشان می‌دهد این نمرات شاخصِ راهبردمحور چگونه در نمرهٔ کلی قصد می‌گنجند. جدول ۵ مجموعهٔ کامل پرسش‌هایی را نشان می‌دهد که شاخص‌های قصد به آن‌ها می‌پردازند. شیوهٔ نمره‌دهی این شاخص‌های قصد، بر اساس اهداف گوناگون، در ضمیمهٔ ج آمده است.

جدول ۴: کلید نمره‌دهی شاخص‌های قصد در راهبردهای سایبری

شاخص		شیوهٔ نمره‌دهی
کل دوره‌ای که کشور راهبرد سایبری داشته است		تعداد سال‌ها از نخستین راهبرد تا ۲۰۲۰
بسامد راهبردها		مدتِ سپری‌شده از نخستین تا آخرین راهبرد، تقسیم بر تعداد راهبردهای منتشرشده
سال‌های گذشته از آخرین به‌روزرسانی		تعداد سال‌ها از آخرین راهبرد تا ۲۰۲۰
نمرهٔ مرور راهبرد	**نمره بر اساس اینکه چه تعداد از مؤلفه‌های زیر در راهبرد آمده‌اند:**	
	۱	مرور کلی تهدیدها و اولویت‌ها
	۲	تحلیل دقیق تهدیدها و اولویت‌های آشکارا ترسیم‌شده
	۳	تقسیم مسئولیت‌ها میان بخش‌های گوناگون دولت
	۴	تسلسل زمانی دقیق یا معیارهای موفقیت
	۵	تسلسل زمانی دقیق و معیارهای موفقیت

جدول ۵: پرسش‌های مطرح‌شده در نمره‌دهیِ قصد کلی (بر اساس هدف)

#	رصد	دفاع	کنترل	اطلاعات
۱	آیا کشور دست‌کم یک خط‌مشی یا آژانس اعمال قانون دارد که تخصصش جرایم سایبری باشد یا شهروندان را به گزارش جرایم سایبری ترغیب کند؟	آیا کشور نقشهٔ امنیت‌سایبری‌ای منتشر کرده است که ترسیم کند چگونه از سیستم‌های دولتی یا زیرساخت‌های حیاتی ملی محافظت می‌کند؟	توان محافظت قانونِ داده	آیا برنامه‌ریزی نظامی یا اسناد راهبردیِ سایبری کشور اذعان می‌کند که کشور قابلیت سایبری جمع‌آوری اطلاعات دارد؟
۲	آیا آژانس اطلاعات داخلی کشور به رصد قابلیت‌های سایبری اذعان می‌کند؟	آیا کشور کارزارهای آگاهی سایبری و بهداشت سایبری برگزار می‌کند؟	آیا برنامه‌ریزی نظامی یا اسناد راهبردی سایبری یا برنامه‌ریزی نظامی یا اسناد راهبردی کلی، اذعان می‌کنند که کشور قابلیت سایبری برای کنترل و دست‌کاری محیط اطلاعاتی دارد؟	آیا آژانس اطلاعاتی کشور یا سرویس اطلاعات خارجی، اذعان می‌کند که کشور قابلیت سایبری جمع‌آوری اطلاعات دارد؟
۳	آیا جرم سایبری یا تروریسم سایبری یا رصد داخلی از راه سایبری در راهبرد یا طرح یا قانون امنیت داخلی یا مبارزه با تروریسم داخلی مطرح شده است؟	آیا کشور اعلام کرده که قصد دارد در زمینهٔ دفاع ملی، تلاش‌های فعال سایبری کند؟	آیا واحد سایبری ارتش اذعان می‌کند که کشور قابلیت سایبری برای کنترل و دست‌کاری محیط اطلاعاتی دارد؟	آیا آژانس اطلاعاتی کشور یا سرویس اطلاعاتی خارجی آن اذعان کرده که کشور قابلیت سایبری جمع‌آوری اطلاعات دارد؟
۴	ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	آیا آژانس اطلاعاتی کشور یا سرویس اطلاعات خارجی آن اذعان می‌کنند که کشور قابلیت‌های سایبری برای کنترل یا دست‌کاری محیط اطلاعاتی را دارد؟	ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟

#	رصد	دفاع	کنترل	اطلاعات
۵	اگر فعالیت رصد در راهبرد سایبری ملی کشور به رسمیت شناخته شده است، نمرهٔ راهبرد را بیاورید.	اگر فعالیت در راستای تقویت و ارتقای فعالیت‌های دفاع سایبری ملی در راهبرد سایبری ملی کشور به رسمیت شناخته شده است، نمرهٔ راهبرد را بیاورید.	ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	اگر فعالیت اطلاعاتی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ راهبرد را بیاورید.
۶	اگر فعالیت رصد در راهبرد سایبری ملی کشور به رسمیت شناخته شده است، نمرهٔ مالی را بیاورید.	اگر فعالیت در راستای تقویت و ارتقای فعالیت‌های دفاع سایبری ملی در راهبرد سایبری ملی کشور به رسمیت شناخته شده است، نمرهٔ مالی را بیاورید.	اگر فعالیت کنترل و دست‌کاری محیط اطلاعاتی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ راهبرد را بیاورید.	اگر فعالیت اطلاعاتی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ مالی را بیاورید.
۷	آیا حمله‌ای سایبری را به کشور نسبت داده‌اند که به این هدف کمک کرده باشد؟ (۵۰درصد از نمره)		اگر فعالیت کنترل و دست‌کاری محیطِ اطلاعاتی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ مالی را بیاورید.	آیا حمله‌ای سایبری را به کشور نسبت داده‌اند که به این هدف کمک کرده باشد؟ (۵۰درصد از نمره)
۸			آیا حمله‌ای سایبری را به کشور نسبت داده‌اند که به این هدف کمک کرده باشد؟ (۵۰درصد از نمره)	

ادامهٔ جدول ۵: پرسش‌های مطرح‌شده در نمره‌دهیِ قصد کلی (بر اساس هدف)

	مالی	تجاری	حمله	هنجارها
۱	آیا کشور عضو چینش تشخیص معیارهای مشترک (سی‌سی‌آرای) هست؟	کیفیت مشارکت در تمام ۲۲ کمیتهٔ مشترکِ فنی ایزو/آی‌ای‌سی چقدر است؟	آیا برنامه‌ریزی نظامی یا اسناد راهبردی سایبری یا برنامه‌ریزی نظامی یا اسناد راهبردی کلی، اذعان می‌کند که کشور قابلیت سایبری تخریبی دارد؟	کشور در چند رایزنی گروه کارشناسان دولت سایبری (جی‌جی‌ای) شرکت کرده است؟
۲	آیا کشور عضو سیستم طرح‌های ارزیابی سازگاری برای تجهیزات و اجزای الکتروتکنیکی در کمیسیون بین‌المللی الکتروتکنیک (آی‌ای‌سی) است؟	آیا کشور طرح همکاری خصوصی/دولتی خاصی برای پرورش صنعت سایبری داخلی و نیروی کار و آگاهی افزایی در زمینهٔ مسائل سایبری دارد؟	آیا واحد سایبری ارتش کشور اذعان می‌کند که قابلیت سایبری مخرب دارد؟	کشور از سال ۲۰۱۲ تا ۲۰۱۶ چند بار از قطع‌نامه‌های سازمان ملل در زمینهٔ جی‌جی‌ای حمایت کرده است؟ از مجموعِ پنج بار.
۳	آیا کشور نقشه یا راهبردی برای جذب سرمایه‌گذاری در شرکت‌های سایبری یا افزایش صادرات سایبری خود منتشر کرده است؟	آیا شواهدی هست که نشان دهد کشور در تحقیقات سایبری سرمایه‌گذاری کرده یا به آن بودجه رسانده است؟	آیا آژانس اطلاعاتی کشور یا سرویس اطلاعات خارجی آن اذعان می‌کند که کشور قابلیت سایبری مخرب دارد؟	کشور بین سال‌های ۲۰۱۵ و ۲۰۱۹ چند بار در انجمن راهبری اینترنت (آی‌جی‌اف) شرکت کرده است؟
۴	ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	آیا کشور در فعالیت‌های قابلیت‌سازِ انجمن جهانی تخصص سایبری شرکت کرده است؟
۵	اگر فعالیت اندوختن ثروت یا استخراج رمزارز در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ راهبرد را بیاورید.	اگر افزایش توانایی سایبری و فنی ملی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ راهبرد را بیاورید.	اگر فعالیت مخرب در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ راهبرد را بیاورید.	کیفیت مشارکت در تمام ۲۲ کمیتهٔ مشترک فنی ایزو/آی‌ای‌سی چقدر است؟

	مالی	تجاری	حمله	هنجارها
۶	اگر فعالیت اندوختن ثروت یا استخراج رمزارز در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ مالی را بیاورید.	اگر افزایش توانایی سایبری و فنی ملی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ مالی را بیاورید.	اگر فعالیت مخرب در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ مالی را بیاورید.	کیفیت مشارکت در گروه‌های مطالعاتی استانداردسازی اتحادیهٔ بین‌المللی مخابرات چقدر است؟ گروه ۱۳ (شبکه‌های آینده)، گروه ۱۷ (امنیت) و «گروه ۲۰» (اینترنت اشیا و شهرهای هوشمند).
۷	آیا حمله‌ای سایبری را به کشور نسبت داده‌اند که به این هدف کمک کرده باشد؟ (۵۰درصد از نمره)	آیا حمله‌ای سایبری را به کشور نسبت داده‌اند که به این هدف کمک کرده باشد؟ (۵۰درصد از نمره)	آیا حمله‌ای سایبری را به کشور نسبت داده‌اند که به این هدف کمک کرده باشد؟ (۵۰درصد از نمره)	آیا کشور در مشق‌های دوجانبه یا چندجانبهٔ دفاع سایبری مشارکت کرده است؟
۸				ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟
۹				اگر تعریف استانداردهای فنی و هنجارهای سایبری بین‌المللی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ راهبرد را بیاورید.
۱۰				اگر تعریف استانداردهای فنی و هنجارهای سایبری بین‌المللی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ مالی را بیاورید.

نمایهٔ قصد سایبری (سی آی آی)

نمایهٔ قصد سایبری، مبتنی بر نمره‌بندی ۳۲ شاخص است که ذیل هفت هدف ملی قرار می‌گیرند:

۱. رصد؛ ۲. دفاع؛ ۳. کنترل؛ ۴. اطلاعات؛ ۵. تجارت؛
۶. حمله؛ ۷. هنجارها.

این‌ها پس از ترکیب با نمرهٔ شاخص‌های قصد در راهبردهای سایبری، به‌علاوهٔ نمرهٔ حملات منسوب، نمرهٔ کلی قصد را تشکیل می‌دهند.

نمرهٔ کلی یک کشور، میانگینِ تمام هفت هدف ملی است. ما از ترکیبی از سیستم نمره‌دهی دوبخشی (یک برای بله و صفر برای نه) و سه‌بخشی (امکان نمرهٔ ۰/۵ هم برای نشان‌دادن «مناطق خاکستری» وجود دارد) و درصد (به‌شکل اعشاری، بین ۰/۰۰ و ۱/۰۰) استفاده کردیم.[1]

نمرهٔ کلیِ یک کشور، میانگین هفت هدف ملی است که به مقیاسی از ۰درصد تا ۱۰۰درصد تبدیل می‌شود.

نتایج

پس از نمره‌دهی سی کشور در هفت هدف، ده کشور که بالاترین نمره را برای قصد داشتند، به شرح زیر بودند:

۱. چین؛
۲. ایالات متحده؛
۳. بریتانیا؛
۴. روسیه؛
۵. هلند؛

1 شاخص دمکراسی واحد اطلاعات اکونومیست و نیز نمایهٔ آزادی در جهانِ خانهٔ آزادی، رویکردی مشابه را پیش می‌گیرند.

۶. اسرائیل؛
۷. اسپانیا؛
۸. استرالیا؛
۹. کانادا؛
۱۰. ایران.

جدول ۶، ده کشور برتر را به‌لحاظ قصد برای هر هدف نشان می‌دهد.

جدول ۶: بالاترین نمرات قصد، بر اساس هدف

#	رصد	دفاع	کنترل	اطلاعات	تجارت	حمله	هنجارها
۱	روسیه	بریتانیا	ایالات متحده	بریتانیا	چین	بریتانیا	بریتانیا
۲	چین	هلند	چین	ایالات متحده	ایران	ایالات متحده	آلمان
۳	ویتنام	فرانسه	روسیه	اسپانیا	بریتانیا	اسرائیل	ایالات متحده
۴	عربستان	ایالات متحده	ویتنام	هلند	ژاپن	اسپانیا	ژاپن
۵	بریتانیا	چین	اسرائیل	اسرائیل	سوئیس	روسیه	فرانسه
۶	استونی	ژاپن	ایران	روسیه	هلند	ایران	سوئیس
۷	هلند	کانادا	بریتانیا	نیوزیلند	سوئد	چین	هلند
۸	استرالیا	سوئد	آلمان	کانادا	استرالیا	هلند	چین
۹	ایالات متحده	استونی	نیوزیلند	استرالیا	ایالات متحده	استونی	کانادا
۱۰	سوئیس	استرالیا	فرانسه	چین	روسیه	استرالیا	استرالیا

تحلیل

هریک از دَه کشور پرامتیاز در سی‌آی‌آی، طیف وسیعی از شواهد را در تمام اهداف دارند. تعجبی ندارد که این کشورها امتیاز بالایی در «تقویت و ارتقای دفاع سایبری ملی» داشتند. با توجه به تمرکز بلندمدت این کشورها در مصون‌کردن خود در برابر حملات سایبری، اکثرشان علاوه بر تلاش برای افزایش تاب‌آوری جمعیت کشورشان، فعالانه در پی تمهیدات دفاعی سایبری نیز بوده‌اند؛ مواردی همچون راهبرد مشارکتِ پایدار فرماندهی سایبری ایالات متحده.

وزنی که با استفاده از داده‌های حملاتِ منسوب برای قصدِ نشان‌داده قائل شدیم، دلیل رتبهٔ بالای بعضی از کشورها بود. این تا حدی نشان می‌دهد که چرا چین بالاترین نمره را برای قصد دریافت کرد و بالاتر از کشورهایی قرار گرفت که در مستندسازیِ راهبردی از قصدشان صریح‌تر بودند یا در انجمن‌های بین‌المللی همان قدر فعالیت داشتند.

نمرات قصدِ سایبریِ مخرب، بیشترین قطبیت را ایجاد کردند. کمتر از نیمی از کشورهای نمایهٔ ما یا فعالانه در پی این هدف نیستند یا آشکارا تأیید نکرده‌اند که در پی آن هستند یا در حال پیگیری این هدف مشاهده نشده‌اند. از نظر ما، این امر دو دلیل اصلی دارد: اول، میزان بالای توانایی فنی لازم برای دستیابی به این اهداف و دوم، مباحثهٔ بین‌المللی دربارهٔ اینکه قابلیت‌های سایبریِ مخرب تا چه حد با قوانین بین‌الملل در راستای تعارض مسلحانه سازگاری دارند. کشورهایی که بالاترین نمره را در دستهٔ تخریب گرفتند، بریتانیا و ایالات متحده بودند، پس از آن‌ها روسیه جای داشت و امتیاز دیگر کشورها به‌سرعت کاهش می‌یافت. کمتر کشوری مشاهده شده است که با استفاده از قابلیت سایبری درصدد اقدامی مخرب باشد. چین، کرهٔ شمالی، هلند، ایران، اسرائیل، روسیه، اسپانیا،

بریتانیا و ایالات متحده تنها کشورهایی بودند که ذیل این هدف نمره‌ای دریافت کردند. بسیاری از کشورها در این مقوله نمرهٔ کمی گرفتند یا اصلاً نمره نگرفتند؛ چون دربارهٔ اینکه آیا ممکن است عملیات سایبری مخربی انجام دهند یا نه، رسماً سکوت کرده‌اند. در این زمینه، نمرهٔ قصدِ چین برای حمله بسیار جالب‌توجه است؛ زیرا موضع رسمی‌شان این است که با هرگونه حملهٔ سایبری مخالف‌اند و خواهان استفادهٔ صلح‌آمیز از فضای سایبری‌اند.

قصدِ اطلاعاتی پانزده کشور، آنجا نشان داده شد که حملات سایبریِ متمرکز بر جمع‌آوری اطلاعات انجام دادند تا آگاهی موقعیتی و درکِ خود از کشوری خارجی را افزایش دهند. جالب آنکه ۲۱ کشور اذعان کردند فعالیت‌هایی اطلاعاتی از راه سایبری انجام می‌دهند؛ چه از طریق ارتش خود و چه از طریق سیگنال‌ها یا آژانس اطلاعات خارجی. برعکس، فقط سه کشور در حال انجام حملات سایبری با قصدِ جاسوسیِ صنعتی مشاهده شده‌اند؛ اما ۲۹ کشور در پی افزایش توانایی سایبری و فنی داخلی خود از راه‌های قانونی بوده‌اند.

با آنکه ۲۹ کشور در حال تولید ثروت قانونی از راه سایبری مشاهده شده‌اند، فقط یک کشور در حال انجام این کار از راه غیرقانونی مشاهده شد: کرهٔ شمالی. فقط بررسیِ یک کشور نشان داد که اصلاً قصدی برای تولید ثروت ندارد: مصر.

این تحلیل محدودیت‌های متعددی دارد؛ که از جملهٔ آن‌ها می‌توان به این موارد اشاره کرد:

اول، این پروژه جست‌وجوهایی به زبان انگلیسی و زبان بومی هر کشور (با استفاده از نرم‌افزارهای تجاری موجودِ ترجمهٔ زبانی و هرجا میسر بود نیز ترجمهٔ انگلیسی اسناد غیرانگلیسی) انجام داد. با آنکه

رویکرد ما سعی در جامعیت داشته است، ممکن است بعضی اسناد از قلم افتاده باشد یا بعضی روحیات در هنگام ترجمه از دست رفته باشد. اما رویکرد ما در قبال این تحلیل این بوده که اگر کشوری بخواهد قصد بخصوص خود را نشان دهد، باید مقاصد خود را به‌شکل مثبت و فعال به مردم خود و مفسران خارجی اعلام کند. درنتیجه، اسنادی که یافتن آن‌ها در وب‌سایت‌های گمنام یا در پشت فایروال دشوار بود، نشان‌دهندهٔ قصد نیستند و به نظر ما، محدودیت‌های زبانی هم ضربه‌ای اساسی به فرایند جست‌وجوی ما نزده است.

دوم، بعضی از کشورها، مشخصاً تمایل کمتری به شفافیت و علنی‌سازی اطلاعات دارند؛ به‌ویژه در مسائل نظامی و اطلاعاتی. کرهٔ شمالی پنهان‌کارترین کشور بود. برای این کشور، به منابع معتبر غیردولتی اتکا کردیم تا بتوانیم برای تمام هفت هدفْ نمره در نظر بگیریم. تنها منابع رسمیِ کرهٔ شمالی که از آن‌ها استفاده کردیم، دانشگاه‌ها بود. یافتن اطلاعات دربارهٔ نقش و اولویت‌های ارتش و جامعهٔ اطلاعاتیِ مصر و نیز همتایان آن‌ها در چندین کشور دیگر نیز بسیار دشوار بود.

تعجبی ندارد، کشورهایی که قصد خود را هم اعلام کرده و هم نشان داده بودند، بالاترین نمره را برای هر هدف گرفتند. بریتانیا، عمدتاً به‌دلیل شفافیت خود دربارهٔ مسائل سایبری و نیز انجام عملیات اطلاعاتی و تهاجمیِ سایبری، بالاترین جایگاه را در چهار مقولهٔ قصد به خود اختصاص داده است.

رصد: روسیه، چین، ویتنام و عربستان برای هدف رصدِ داخلی بالاترین جایگاه‌ها را کسب کردند. علاوه بر چهار کشوری که دیدیم

«محتوای غیرقانونی»[1] را از میان جمعیت داخلی‌شان حذف می‌کنند، تمام کشورها سازمان‌های اعمالِ قانون و آژانس‌های اطلاعاتیِ داخلی با قابلیت‌های سایبری ویژه داشتند و تمام آن‌ها، به‌جز عربستان، به تهدیدهای سایبری برای امنیت داخلی یا راهبردها و نقشه‌های تروریسم داخلی می‌پرداختند.

کنترل: این هدفْ انعکاس دوگانگیِ ابزار سایبری است. کشوری که در این هدف نمرهٔ بالا گرفته، کنترلگری از خود نشان داده است؛ چه از طریق حذف مطالب افراطی و رد پروپاگاندای خارجی و چه از طریق پروپاگاندای داخلی و ایجاد و تقویت دروغ‌پراکنی در بیرون از مرزها. ایالات متحده، به‌دلیلی که اول گفته شد، بالاترین جایگاه این هدف را به خود اختصاص داد. دلیل نمرهٔ بالای این کشور، نقش ارتش و آژانس‌های اطلاعاتی آن در مختل‌کردن توانایی داعش در جذب نیرو و ارتباط با ستیزه‌جویان و نیز تلاش در راستای محدودسازی توانایی تهران برای گسترش پروپاگاندا پس از حادثهٔ ۱۱سپتامبر است. برعکس، نمرهٔ بالای چین و روسیه عمدتاً به‌دلیل کارزارهای دروغ‌پراکنی است که از سال ۲۰۱۶ به این دو کشور نسبت داده شده است.

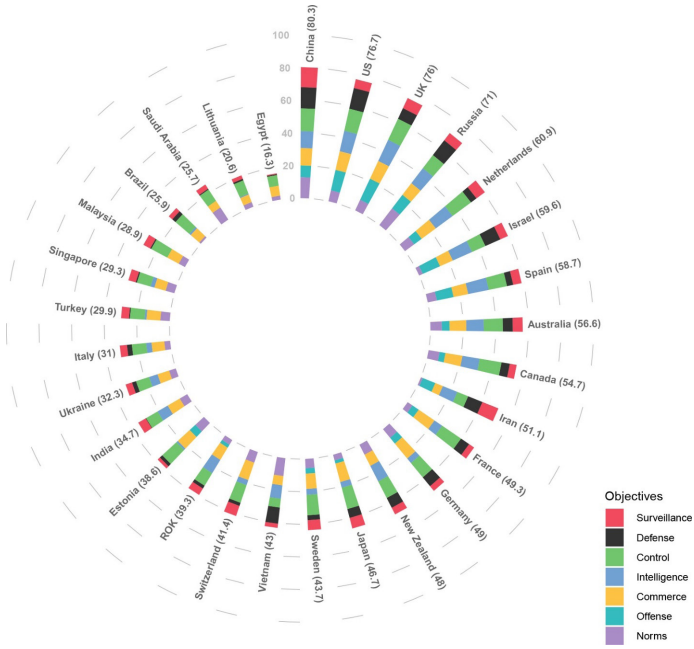
تخریب: راهبردهای سایبری و نظامیِ بریتانیا و اسرائیل و ایالات متحده اذعان می‌کنند که این کشورها قابلیت سایبری مخرب را توسعه داده‌اند. به‌علاوه، هر سه کشور یادشده این قابلیت‌ها را در عملیات تهاجمی به نمایش گذاشته‌اند.

اطلاعات: با توجه به اطلاعاتی که اسنودن افشا کرده است، تعجبی ندارد که بریتانیا و ایالات متحده در بالاترین جایگاه برای هدف اطلاعات

1 Russell, Jon. "Vietnam Threatens to Penalize Facebook for Breaking Its Draconian Cybersecurity Law." TechCrunch, TechCrunch, 9 Jan. 2019, techcrunch.com/2019/01/09/vietnam-threatens-to-penalize-facebook/.

جا بگیرند. شاید اینکه اسپانیا جایگاه سوم را به خود اختصاص داده است، جالب‌تر باشد. ارتش و آژانس‌های اطلاعاتی اسپانیا نیز، مانند بریتانیا و آمریکا، قصد خود برای جمع‌آوری اطلاعات از راه سایبری را اعلام کرده و نشان داده‌اند.

تجارت: هم‌راستا با سرتیترهای اخیر در کشورهای غربی، چین در هدف افزایش توانایی سایبری و فنیِ ملی، جایگاه نخست را به خود اختصاص داده است. چین، در کنار کرۀ شمالی و ایران، یکی از تنها سه کشوری است که هم از راه قانونی و هم غیرقانونی، در پی نیل به این



هدف است. مشاهده شده که این کشور جاسوسیِ صنعتی انجام می‌دهد

و در پی مشوق‌سازی و افزایش تخصص سایبریِ داخلی خود از طریق تحقیق و توسعه و مشارکت‌های خصوصی/دولتی است.

شکل ۴: سی‌آی‌آی ۲۰ با تقسیم کشور

هنجارها: از میان ۲۹ کشوری که برایشان راهبرد سایبری یافتیم، ۲۷ کشور در راهبرد خود از تلاش برای دستیابی به هدف تعریفِ استانداردهای فنی و هنجارهای سایبری بین‌مللی گفته‌اند. فقط مصر و هند به‌دنبال چنین هدفی نبوده‌اند. آلمان در این شاخص دوم شد که با حمایت کلی‌ترِ این کشور از نهادهای بین‌المللی و طرح‌های قابلیت‌ساز بین‌المللی سازگار است.

دفاع: پنج کشور برتر در زمینهٔ هدف دفاع سایبری، هم به‌دنبال افزایش تاب‌آوری سایبری و هم تمهیدات دفاع فعال سایبری بوده‌اند.

شکل ۴، سی‌آی‌آی را با تقسیم‌بندی کشورها و تمام هفت هدف نشان می‌دهد. شکل ۵ نیز سی‌آی‌آی را بر اساس هریک از اهداف تقسیم می‌کند.

۴/۲. امتیازدهی به قابلیت‌ها و منابع

هر کشوری، برای داشتنِ قدرت سایبری، نیازمند قابلیت‌هایی برای نیل به اهداف مدنظر است. قابلیت‌های سایبری به ایجاد و کنترل و مخابرهٔ زیرساخت‌های اطلاعات الکترونیکی و رایانه‌ای، شبکه‌ها، نرم‌افزارها و مهارت‌های انسانی مربوط می‌شود.[1] درنتیجه، کشورها در طیفِ وسیعی از منابع سرمایه‌گذاری می‌کنند؛ ازجمله: عرصه‌هایی همچون

1 Daniel T. Kuehl. 2009. 'From Cyberspace to Cyberpower: Defining the Problem', In Franklin Kramer, Stuart Starr and Larry K. Wentz (eds.) Cyberpower and National Security. Washington DC: National Defense University Press. p24

قابلیت‌های سایبری نظامی و دفاع سایبری و رصد و البته قابلیت انسانی و تقویتِ نهادی و خط‌مشی داخلی. علاوه بر این، توانایی تأثیرگذاری در بستر جهانیِ فضای سایبری، از طریق استانداردهای فنی یا هنجارهای بین‌المللی یا صادرات، این امکان را به کشورها می‌دهد تا فضایی بپرورند که در آن بتوانند از منافع خود پاسداری کنند و برای گسترش حوزهٔ نفوذ، از قدرت خود بهره بگیرند. بدین ترتیب، کشورها می‌کوشند فضای سایبری را کنترل کنند؛ هم درون مرزهای خود و هم به‌صورت برون‌مرزی. ما تمام این عناصر را در ارزیابی قابلیت‌های سایبری کشورها بر اساس هدف‌های گوناگون لحاظ کرده‌ایم.

با توجه به منبع پیچیدهٔ قدرت سایبری، هریک از اهداف ملی را با شاخص‌هایی مطابقت داده‌ایم که قابلیت کشور برای دستیابی به آن هدف را نشان می‌دهند. بسیاری از شاخص‌ها به بیش از یک هدف بهره می‌رسانند؛ درنتیجه، بعضی از شاخص‌ها در چند هدف به‌شمار آمده‌اند تا این هم‌پوشانی لحاظ شود. جدول ۷ مطابقت شاخص‌ها با اهداف ملی و نیز مروری سطح بالا از رویکرد ما به امتیازدهی را عرضه می‌کند. پیوست ب نیز توضیح مفصل‌تری دربارهٔ امتیازدهی هر شاخص قابلیت است.

۲۷ شاخص قابلیتی که در ان‌سی‌پی‌آی لحاظ شده‌اند، انعکاس‌دهندهٔ فهرستی از قابلیت‌ها هستند؛ جامع‌تر از آنچه پیش‌تر موجود بود. همین امر ما را به درک واقع‌بینانه‌تر و مطابقتی‌تری از قدرت سایبری در سطح ملی می‌رساند. داده‌های جمع‌آوری دربارهٔ قابلیت‌ها را می‌توان در هشت مضمون دسته‌بندی کرد: شواهد حمله؛ محتوای برخط ملی؛ ساختارهای سایبری داخلی؛ کاهش آسیب‌پذیری سایبری؛ بخش خصوصی و تجارت و نوآوری؛ قابلیت اتصال؛ نیروی کار؛ چهارچوب‌های حقوقی و خط‌مشی.

شکل ۵: سی‌آی‌آی ۲۰۲۰ با تقسیم اهداف و کشورها

جدول ۷: مطابقت شاخص‌های قابلیت با اهداف مختلف

شاخص	رصد/پایش داخلی	دفاع سایبری ملی	کنترل اطلاعات	جمع‌آوری اطلاعات	سود تجاری	غیرفعال‌سازی زیرساخت‌های دشمن	هنجارهای سایبری بین‌المللی	توضیح مطابقت اهداف
قوانین امنیت سایبری	X	X					X	قوانین امنیت سایبریُ کشور را قادر می‌سازند کنترل بهتری بر داده‌های جمعیت خود داشته باشد، بهتر با دیگر کشورها تعامل کند، دفاع خود را تقویت کند، و نیز سرمشقی برای نحوهٔ تعامل با شریکان خارجی ایجاد کند.
حمله با حمایت دولت	X		X	X	X	X		حملات سایبری با حمایت دولتْ باعث می‌شوند کشور بتواند اطلاعات خارجی گردآوری کند، جاسوسی سازمانی انجام دهد، دگراندیشان را رصد کند، اطلاعات دروغ بپراکند و زیرساخت‌های دشمن را غیرفعال کند.
توافق‌های سایبری دوجانبه							X	تعیین هنجار سایبری بین‌المللی را می‌توان براین اساس سنجید که یک کشور تا چه حد در ایجاد بیانیه‌های رسمی و غیررسمیِ مشارکت بین‌المللی فعال بوده است.

شاخص	رصد/پایش داخلی	دفاع سایبری ملی	کنترل اطلاعات	جمع‌آوری اطلاعات	سود تجاری	غیرفعال‌سازی زیرساخت‌های دشمن	هنجارهای سایبری بین‌المللی	توضیح مطابقت اهداف
توافق‌های سایبری چندجانبه							X	تعیین هنجار سایبری بین‌المللی را می‌توان براین‌اساس سنجید که یک کشور تا چه حد در ایجاد بیانیه‌های رسمی و غیررسمیِ مشارکت بین‌المللی فعال بوده است. توافق‌های چندجانبه ایجاد اجماع بین چند کشور را نشان می‌دهند.
دکترین نظامی سایبری						X		دکترین‌های نظامی سایبریْ منابع میان‌دولتی را تسهیل می‌کنند و به‌سوی توسعهٔ قابلیت تهاجمی سوق می‌دهند.
فرماندهی سایبری ملی						X		فرماندهی‌های سایبری مرکزی به دولت‌های ملی این امکان را می‌دهند که چندین قابلیت سایبری را هماهنگ و مهار کنند تا در صورت نیاز، از ابزار سایبری نظامی بهره بگیرند.
۱۰۰ شرکت برتر فناوری در دنیا				X	X		X	شرکت‌های فناوریِ یک کشور باعث رشد صنعت داخلی می‌شوند و بر صنایع برون‌مرزی کشور تأثیر می‌گذارند؛ به‌ویژه اگر شرکت کاربران خارجی زیادی داشته باشد.

شاخص	رصد/پایش داخلی	دفاع سایبری ملی	کنترل اطلاعات	جمع‌آوری اطلاعات	سود تجاری	غیرفعال‌سازی زیرساخت‌های دشمن	منجارهای سایبری بین‌المللی	توضیح مطابقت اهداف
صادرات فناوری پیشرفته				X	X	X	X	صادرات محصولات فناوری پیشرفته به کشورهای خارجی می‌تواند به اقتصاد کشور منفعت برساند و (بسته به کشورش) ممکن است سرویس اطلاعات خارجی را در دسترسی به داده‌هایی توانا کند که محصولات درباره شهروندان خارجی گردآوری می‌کنند. این می‌تواند به وابستگی خارجی‌ها به صادرات فناوری پیشرفته بینجامد که آن نیز شاید به کندشدن یا توقف قابلیت‌های دشمن، در صورت توقف صادرات، منجر شود.
کارکنان ماهر در صنعت فناوری		X		X	X			این قابلیت مبتنی بر این پرسش است: «در کشورتان چقدر آسان است که شرکت‌ها کارمندانی با مهارت‌های متناسب با نیازهای کسب‌وکار بیابند؟» دردسترس‌بودنِ کارکنان ماهر باعث جذب بهترِ نیروی کار به شغل‌های امنیتِ سایبری (و رشد بخش خصوصی) یا جذب نیروی بهتر برای کارهای دولتی (همچون اطلاعات) می‌شود. آن‌گاه، تعداد بیشتری از کارکنان ماهرِ در امنیت سایبری و در حوزه‌های مختلف به دفاع سایبری کمک می‌کنند.

شاخص	رصد/پایش داخلی	دفاع سایبری ملی	کنترل اطلاعات	جمع‌آوری اطلاعات	سود تجاری	غیرفعال‌سازی زیرساخت‌های دشمن	هنجارهای سایبری بین‌المللی	توضیح مطابقت اهداف
تأمین نیروی کار ارتش سایبری				X		X		«تعداد کارکنانی را نشان می‌دهد که نقش سایبری آن‌ها در ارتش علناً اذعان شده است. این شاخص شمار مطلق افرادی را گزارش می‌دهد که در نقش‌های سایبری نظامی در هر کشور کار می‌کنند»
۵۰۰ شرکت برتر امنیت سایبری در دنیا		X			X			هرچه تعداد شرکت‌های امنیت سایبری که مقرشان در دولت است بیشتر باشد، صنعت امنیت سایبری رشد بیشتری می‌کند.
نرخ آلودگی رایانه‌ای		X						هرچه رایانه‌های بیشتری تحت‌تأثیر بدافزارهای خارج از حمایت دولت قرار گیرند، دفاع سایبری ملی احتمالاً آسیب‌پذیرتر باشد.
نرخ آلودگی موبایل‌ها		X						هرچه گوشی‌های بیشتری تحت‌تأثیر بدافزارهای خارج از حمایت دولت قرار گیرند، دفاع سایبری ملی احتمالاً آسیب‌پذیرتر باشد.

شاخص	رصد/پایش داخلی	دفاع سایبری ملی	کنترل اطلاعات	جمع‌آوری اطلاعات	سود تجاری	غیرفعال‌سازی زیرساخت‌های دشمن	منجارهای سایبری بین‌المللی	توضیح مطابقت اهداف
درصدی از جمعیت که در شبکه‌های اجتماعی حضور دارند	X		X					هر چه تعداد شهروندان کاربر شبکه‌های اجتماعی بیشتر باشد، احتمال بیشتری دارد که داده‌هایشان در اینترنت باشد و افراد بیشتری تحت‌تأثیر رصد داخلی یا قوانین داده قرار بگیرند. اما حضور بیشتر افراد در شبکه‌های اجتماعی (در بسیاری از موارد) ممکن است به آسیب‌پذیری بیشتر جمعیت مردم به کارزارهای دروغ‌پراکنی خارجی هم بینجامد.
درصدی از جمعیت که به اینترنت متصل‌اند	X	X	X					هر چه تعداد شهروندان متصل به اینترنت بیشتر باشد، احتمال بیشتری دارد که داده‌هایشان در اینترنت باشد و افراد بیشتری تحت‌تأثیر رصد داخلی یا قوانین داده قرار بگیرند. اما حضور بیشتر افراد در اینترنت (در بسیاری از موارد) ممکن است به آسیب‌پذیری بیشتر جمعیت مردم به کارزارهای دروغ‌پراکنی خارجی یا جرایم سایبری یا تلاش برای جاسوسی سایبری هم بینجامد.
وجود فناوری رصد بخش خصوصی	X			X				بالاتر بودن تعداد شرکت‌های رصد درون یک کشور، راه‌ها و فرصت‌های بیشتری برای پایش شهروندان کشور به‌وجود می‌آورد. هر چه تعداد این شرکت‌ها بیشتر باشد، صنعت رصد درون این کشور می‌تواند سود بیشتری بیافریند.

شاخص	رصد/پایش داخلی	دفاع سایبری ملی	کنترل اطلاعات	جمع‌آوری اطلاعات	سود تجاری	غیرفعال‌سازی زیرساخت‌های دشمن	هنجارهای سایبری بین‌المللی	توضیح مطابقت اهداف
وب‌سایت‌های برتر در «۵۰ وب‌سایت برتر الکسا»			X		X			وب‌سایت‌هایی که بیشترین ترافیک بین‌المللی را دارند، قدرت بیشتری به کشوری می‌دهند که مقرشان در آن است. آن کشور می‌تواند از طریق اینترنت، روایت‌ها یا آرمان‌های متداول و محبوبش را تقویت کند و شرکتِ مالکِ هر وب‌سایت را قادر به تولید سود تبلیغاتی بیشتر و ارائهٔ محصولات بیشتر به مصرف‌کنندگان می‌کند.
وب‌سایت‌های خبری برتر در «۵۰ وب‌سایت برتر الکسا»			X					وب‌سایت‌هایی خبری که بیشترین ترافیک بین‌المللی را دارند، به کشورِ محل استقرارشان قدرتِ بیشتری می‌دهد تا از طریق اینترنت، روایت‌ها یا آرمان‌های متداول و محبوب در آن کشور را تقویت کند.
درخواست‌های موفق حذف محتوا از گوگل			X					موفقیتِ بیشتر درخواست‌های حذف محتوا از گوگل نشان می‌دهد که یک کشور اطلاعات را به‌شیوه‌ای مؤثر از اینترنت حذف کرده است. این نشان از مقدار کنترل بر فضای اطلاعاتی دارد.
نمرهٔ آزادی در اینترنت	X							هرچقدر آزادیِ شهروندان کشوری در اینترنت کمتر باشد، احتمال بیشتری دارد که دولت بتواند شهروندان خود را رصد و پایش کند و گردش اطلاعات را کنترل.

شاخص	رصد/پایش داخلی	دفاع سایبری ملی	کنترل اطلاعات	جمع‌آوری اطلاعات	سود تجاری	غیرفعال‌سازی زیرساخت‌های دشمن	هنجارهای سایبری بین‌المللی	توضیح مطابقت اهداف
واردات فناوری اطلاعات و ارتباطات		X			X		X	هرچه فناوری اطلاعات و ارتباطات بیشتری وارد شود، نیاز بازاری به راهکارهای داخلی احتمالاً کاهش یابد و کشور ممکن است خطر بیشتری در زنجیرهٔ تأمین در زیرساخت سایبری داخلی خود تحمیل کند.
حق امتیاز برنامک‌ها					X			هرچه در یک کشور حق امتیاز بیشتری برای برنامک‌ها وجود داشته باشد، نشان‌دهندهٔ نوآوری است که شاید به سود تجاری بینجامد.
سرعت پهن‌باند		X						هرچه سرعت پهن‌باند بیشتر باشد، احتمالش بیشتر است که زیرساخت اینترنت به‌روز باشد؛ در حالت ایدئال، احتمال سازوکارهای دفاعی بهتر را افزایش می‌دهد.
سرعت موبایل		X						هرچه سرعت موبایل بیشتر باشد، احتمالش بیشتر است که زیرساخت اینترنت به‌روز باشد؛ در حالت ایدئال، احتمال سازوکارهای دفاعی بهتر را افزایش می‌دهد.
اقتصاد تجارت الکترونیک					X			فروش بیشتر تجارت الکترونیک، امکان ورود سود بیشتر به خرده‌فروشان بخش خصوصی کشور را فراهم می‌آورد که باعث تقویت اقتصاد داخلی می‌شود.

شاخص	رصد/پایش داخلی	دفاع سایبری ملی	کنترل اطلاعات	جمع‌آوری اطلاعات	سود تجاری	غیرفعال‌سازی زیرساخت‌های دشمن	هنجارهای سایبری بین‌المللی	توضیح مطابقت اهداف
آسیب‌پذیری‌های فهرست‌شده در وب‌سایت Shodan که بر ماشین‌های داخلی تأثیر می‌گذارد		X						هر چه رایانه‌های یک کشور آسیب‌پذیرتر باشد، کشور بیشتر در معرض حمله است.
وجود تیم‌های واکنش به اختلال در امنیت سایبری		X						وجود این تیم‌ها نشان می‌دهد که کشور منابعی برای کاهش آسیب‌های سایبری و بحران‌های مرتبط فراهم کرده است.
قدرت نرم جهانی							X	کشور هر چه قدرت نرم بیشتری داشته باشد، بیشتر می‌تواند در زمینهٔ اتخاذ و حفظ هنجارهای بین‌المللیْ بر کشورهای دیگر تأثیر بگذارد.

نمایهٔ قابلیت سایبری (سی‌سی‌آی)

سی‌سی‌آی سنجش قابلیت‌ها از ۰ درصد تا ۱۰۰ درصد است و مبتنی بر نمره‌دهی ۲۷ شاخص که طبق هفت هدف ملی دسته‌بندی شده‌اند.

سی‌سی‌آی را می‌توان بر اساس هدف تقسیم‌بندی کرد و آن امتیاز بر مبنای مقدار متوسطِ شاخص‌های نرمال‌شده‌ای است که بر آن هدف تأثیر می‌گذارند. نمرهٔ کلی سی‌سی‌آی میانگین تمام هفت هدف است.

پیش از تجمیع شاخص‌ها، آن‌ها را با استفاده از روشِ نرمال‌سازیِ کمینه‌بیشینه مقیاس‌بندی کردیم که داده‌ها را در بازه‌های گوناگون بر اساس مقادیرِ کمینه و بیشینه مقیاس‌بندی می‌کند. بعضی از شاخص‌های ما از توزیع گاوسی تبعیت نمی‌کنند؛ گاوسی نمی‌گذارد از دیگر فنون نرمال‌سازی (همچون استانداردسازی z) استفاده کنیم. فن کمینه‌بیشینه کاربردِ گسترده‌ای برای ساخت شاخص‌های ترکیبی دارد.[1] برتری این فن در آن است که حدومرزِ تمام شاخص‌ها را درون یک رنج برابر (کمینهٔ صفر و بیشینهٔ یک) تعیین می‌کند. برای هر شاخص قابلیت، مقدار کمینه به صفر تبدیل می‌شود و مقدار بیشینه به یک؛ هر مقدار دیگری، به رقمی اعشاری بین ۰ و ۱ بدل می‌گردد.

یکی از ضعف‌های این فن آن است که مبتنی بر مقادیر دورافتادهٔ توزیع است که تأثیر چشمگیری بر برون‌داد نهایی می‌گذارد. ما با استفاده از دیگر روش‌های نرمال‌سازی، مجموعه‌ای از بررسی‌های حساسیت انجام داده‌ایم تا سوگیری بالقوهٔ حاصل از مقادیر دورافتاده آزموده شود (ن.ک: بخش ۴، قسمت مربوط به تحلیل حساسیت).

نتایج

ده کشور برتر بر اساس هدف، در جدول ۸ نشان داده شده‌اند. قابلیت‌ها بر اساس کشور و رده‌بندی‌های خاص‌تر را می‌توان در بخش ضمایم مشاهده کرد.

1 Patro, S., and Kishore Kumar Sahu. “Normalization: A preprocessing stage.” arXiv preprint arXiv:1503.06462 (2015).

جدول ۸: سی‌سی‌آی ۲۰۲۰ بر اساس تقسیم هدف

#	رصد	دفاع	کنترل اطلاعات	اطلاعات	تجارت	حمله	هنجارها
۱	ایالات متحده	چین	ایالات متحده	ایالات متحده	ایالات متحده	روسیه	ایالات متحده
۲	بریتانیا	سنگاپور	روسیه	بریتانیا	کرۀ‌جنوبی	ایالات متحده	فرانسه
۳	فرانسه	کانادا	چین	چین	چین	چین	ژاپن
۴	چین	فرانسه	کرۀ‌جنوبی	آلمان	ژاپن	آلمان	چین
۵	ژاپن	سوئیس	سوئد	سنگاپور	بریتانیا	بریتانیا	آلمان
۶	سوئد	هلند	سنگاپور	اسرائیل	سنگاپور	فرانسه	سنگاپور
۷	کانادا	ایالات متحده	بریتانیا	فرانسه	هلند	هلند	بریتانیا
۸	آلمان	ژاپن	نیوزیلند	مالزی	آلمان	اسپانیا	مالزی
۹	نیوزیلند	آلمان	عربستان	استونی	فرانسه	استونی	کرۀ‌جنوبی
۱۰	اسرائیل	سوئد	کانادا	هلند	سوئیس	کانادا	هند

تحلیل

از میان هفت هدف، ایالات متحده در پنج تا جایگاه اول را به خود اختصاص داده است. روسیه، که در نمرۀ کلی سی‌سی‌آی ردۀ دهم را دارد، در فهرست هدفِ حمله جایگاه اول را از آن خود کرده است.[1] چین در زمینۀ قابلیت‌های دفاع سایبری پیشتاز است. ایالات متحده، در میان

1 حمله، گونۀ کوتاه‌شدۀ هدف نابودی و غیرفعال‌سازی زیرساخت‌های دشمن است.

قابلیت‌های سایبری خود، در زمینهٔ دفاع سایبری ملی کمترین نمره را گرفت و از میان سی کشور، هفتم شد.

چین برای تک‌تک اهداف جزء پنج کشور نمره‌بالاست. طی سال‌های اخیر، چین سرمایه‌گذاری زیادی در تحقیق و توسعهٔ فناوری‌هایی کرده که با آن‌ها بتواند در فضای سایبری به اهداف متعددی نایل شود. این نتایج نشان‌دهندهٔ جایگاه چین در فضای مجازی است که روزبه‌روز سیطرهٔ بیشتری بر آن می‌یابد؛ اما شکاف وسیعِ قابلیت چین و ایالات متحده در بیشتر عرصه‌ها را نیز نشان می‌دهد.[1]

بریتانیا، به‌ویژه در دو حوزه، نمرهٔ بالایی گرفته است و در رده‌بندی کلی جایگاه سوم را دارد: اطلاعات و رصد (در هر دو، فقط ایالات متحده بالاتر از این کشور جای دارد). جای شگفتی نیست؛ بریتانیا از دیرباز مواضع محکمی هم در گردآوری اطلاعات خارجی برای اهداف امنیت ملی و هم در رصد و پایش گروه‌های داخلی داشته است.[2] این کشور همچنین بودجهٔ زیادی برای تقویت قابلیت‌های خود در راستای نیل به چندین هدف بررسی‌شده اختصاص داده است.

قابلیت‌های مقولهٔ هنجارها، مبتنی بر ترکیبی از معاهده‌های بین‌المللی و بدنه‌های تعیین استاندارد بود و همچنین هنجارهای تعریف‌شده از سوی فناوری‌هایی که کشور صادر می‌کند. به همین دلیل، ژاپن و ایالات متحده نزدیک به صدر فهرست هستند.

روسیه در هدفِ حمله پیشتاز است. این کشور فرماندهی سایبری

1 Inkster, N., 2018. China's Cyber Power. Routledge.
Cheung, T.M., 2018. The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities. Journal of Cyber Policy, 3(3), pp.306-326.
2 Kris, D.S., 2015. Trends and predictions in foreign intelligence surveillance: The FAA and beyond. J. Nat'l Sec. L. & Poly, 8, p.377.
Leigh, I., 2010. Intelligence and the Law in the United Kingdom. In The Oxford Handbook of National Security Intelligence.

نهادینه‌شده و دکترین نظامی سایبری مفصلی دارد و سال‌هاست در این فضا خبرساز می‌شود.[1] این کشور، به‌طور ویژه، حملات سایبری مختل‌کنندهٔ زیادی طی سال‌های اخیر انجام داده است.[2] این امر آشکارا نشان‌دهندهٔ قابلیت روسیه در تخریب و مختل‌کردن زیرساخت‌های دشمن است.

سنگاپور تمرکز عمده‌ای بر دفاع ملی داشته است.[3] این کشور (تا جایی که اطلاعات در دسترس است) هیچ اقدام مختل‌کننده‌ای در فضای سایبری انجام نداده است و منابع خود را صرف تقویت و ارتقای قابلیت‌های دفاعی خود کرده است. بعد از سنگاپور، چین و کانادا و فرانسه و سوئیس‌اند که به‌سوی پرورش محیطی برای نیل به هدفی یکسان گرایش دارند.

عرصه‌ای که در آن رتبه‌بندی برخلاف تصورِ شمی است، به اسرائیل مربوط می‌شود. مفسران معمولاً اسرائیل را در صدر رده‌بندی‌های کاذب قرار می‌دهند و به‌طور ویژه بر قابلیت‌های این کشور در زمینهٔ حملهٔ سایبری و جمع‌آوری اطلاعات تأکید می‌کنند. ما به این نکته واقفیم که این قسمت از رده‌بندیْ نابهنجار به نظر می‌آید و این را می‌توان به چند عامل نسبت داد. نکتهٔ مهم این است که این نمایه فقط از داده‌های منبع‌باز استفاده می‌کند. بخش زیادی از برنامهٔ سایبری اسرائیل به‌صورت مخفیانه هماهنگ و مدیریت می‌شود، نه در بخش‌های عمومی و کسب‌وکار. دوم، این بخش از انسی‌پی‌آی، قابلیت‌ها را می‌سنجد. وقتی به قصد بنگریم، اسرائیل نمرهٔ بالایی در آن دو هدف دارد؛ اما لزوماً

1 Giles, K., 2012, June. Russia's public stance on cyberspace issues. In 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 1-13). IEEE.

2 حملات در ردیاپ عملیات سایبری شورای روابط خارجی آمده‌اند.

3 Ventre, D. ed., 2013. Cyber Conflict: competing national perspectives. John Wiley & Sons.
Ad'ha Aljunied, S.M., 2019. The securitization of cyberspace governance in Singapore. Asian Security, pp.1-20.

قابلیتِ صنعتی سایبری‌نظامی یا قدرت اقتصادی یا دیگر سنجه‌های کلیدی‌ایِ استفده‌شده برای سنجش قابلیت را ندارد.

نمایه همچنین نشان می‌هد چند کشوری که عموماً قدرت سایبری به‌شمار نمی‌آیند، درواقع در بعضی عرصه‌ها قابلیت‌های بسیاری دارند. مالزی در چهار عرصه جزء ده کشور برتر است: کنترل اطلاعات، اطلاعات، سود تجاری و هنجارها و قوانین. سوئد در سه هدف جزء ده کشور برتر است: رصد و دفاع سایبری و کنترل اطلاعات. سوئیس نیز در اهداف دفاع سایبری و سود تجاری جزء ده کشور برتر است.

استونی، که معمولاً آن را طلایه‌دار قابلیت سایبری و دیجیتالی می‌دانند، فقط برای دو هدف جزء ده کشور برتر قرار گرفت: اطلاعات و حمله. هرچند این برای کشوری با جمعیت ۱٫۵ میلیون نفر حیرت‌آور است، آن‌قدری که گروه پژوهشی انتظار داشتند بالا نیست.

آلمان، کشوری که معمولاً در بحث از قابلیتِ سایبری نامی از آن به میان نمی‌آید، برای اطلاعات و حمله و هنجارها جزء پنج کشور برتر بود و می‌توانست از پایگاه صنعتیِ قوی خود و قابلیت‌های نظامی و غیرنظامی سازمان‌یافته‌اش بهره بگیرد.

شکل ۶: سی‌سی‌آی ۲۰۲۰ در تمام اهداف

شکل ۷: سی‌سی‌آی بر اساس هر هدف

۴/۳. ساختن انسی‌پی‌آی تجمعی

داده‌های ناموجود و عادی‌سازی شاخص‌ها

با آنکه شاخص‌های متأثر بر انسی‌پی‌آی را با دقت انتخاب کرده‌ایم، نتوانستیم برای تمام سی کشورِ مدنظر و تک‌تک شاخص‌هایمان داده بیابیم. تمام شاخص‌های لحاظ‌شده در نمایهٔ انسی‌پی‌آی نشان‌دهندهٔ موجودبودن داده برای دست‌کم ۲۱ کشور (۷۰درصد) از ۳۰ کشور هستند و همچنین نقاطی که نایب‌های معقولی برای داده‌های ناموجود داشتیم. شاخص‌هایی که به این حدنصاب نرسیدند، لحاظ نشدند. ما چند شاخص را درون‌سازمانی تهیه و نقشه و رویهٔ کدگذاری دقیقی را دنبال کردیم که، در صورت درخواست، امکان دسترسی به آن وجود دارد.

مجموعه‌داده حاوی هیچ مقدارِ ناموجودی نیست. برای تمام شاخص‌ها و کشورهایی که اطلاعاتشان ناموجود بود، مقداری تخمینی در نظر گرفتیم. بعضی از مقادیر برای شاخص‌های زیر تخمین زده شده‌اند:

- نرخ آلودگی رایانه‌ای: مقادیر تخمینی برای اسرائیل و نیوزیلند.
- نرخ آلودگی موبایل: مقادیر تخمینی برای اسرائیل و نیوزیلند.
- درخواست حق امتیاز: مقادیر تخمینی برای لیتوانی.
- واردات اطلاعات و ارتباطات: مقادیر تخمینی برای مصر، عربستان، سنگاپور، سوئیس و ویتنام.
- تجارت الکترونیک: مقادیر تخمینی برای اسرائیل.
- آزادی در اینترنت: مقادیر تخمینی برای کرهٔ شمالی، اسرائیل، لیتوانی، هلند، نیوزیلند، اسپانیا، سوئد و سوئیس.

پیش از تجمیع داده‌ها، در شاخص‌هایمان اصلاحات مدیریتیِ خاصی انجام دادیم تا مقادیر بالاتر با عملکردِ بهتر قدرت سایبری، در تمام شاخص‌ها تناظر داشته باشد. تحلیل هم‌بستگی دوگانه را برای تمام شاخص‌ها انجام داده‌ایم.

پیش از تجمیع، شاخص‌ها را نرمال‌سازی کردیم تا به مقیاسی مشترک درآیند. برای فن نرمال‌سازی‌مان از فن کمینه‌بیشینه استفاده کردیم؛ زیرا (۱) بهتر از همهٔ روش‌ها انعکاس‌دهندهٔ چهارچوب نظری‌مان است و (۲) برای خاصیت‌های داده مناسب‌تر است و (۳) کاربران راحت می‌توانند آن را تفسیر کنند.

تجمیع و وزن‌دهی انسی‌پی‌آی

برای سنجش نمره برای هر هدف، میانگین نمرات نرمال‌شدهٔ قابلیت را برای آن هدف در نظر گرفتیم. سپس نمرات میانگین و نرمال‌شدهٔ قابلیت را برای هر هدف در نمرهٔ قصدِ برای همان هدف ضرب کردیم تا نمرهٔ انسی‌پی‌آی برای آن هدفِ بخصوص به‌دست آید. برای محاسبهٔ انسی‌پی‌آی کلیِ تمام اهداف، نمرات تک‌هدفی را با هم مجموع‌یابی کردیم تا نمرهٔ تجمیعی به‌دست آید.

رویکرد هدف‌محور پیامدهای مهمی برای ساخت انسی‌پی‌آی دارد؛ زیرا وزن را وارد کار می‌کند و بعضی از شاخص‌ها چند بار حساب می‌شوند؛ مثلاً فناوری رصد، هم با هدف ملی رصد داخلی و هم هدف ملیِ جمع‌آوری اطلاعات مطابقت می‌یابد. درنتیجه، دو بار در انسی‌پی‌آی لحاظ می‌شود. این شمارش چندباره مبتنی بر تأمل نظریِ دقیق بر این نکته است که قابلیت‌های سایبری گوناگون چگونه با هدف‌های سایبری متعدد مطابقت می‌یابند.

هر شاخصی که چند بار شمرده می‌شود، برای کشوری که در آن شاخص قابلیت نمرهٔ بالایی می‌گیرد، به‌صورت خودکار، نمره را هم در سی‌سی‌آی و هم در انسی‌پی‌آی افزایش می‌دهد.

برای محاسبهٔ نمرهٔ قصد انسی‌پی‌آی، قابلیت‌های هر کشور را (برای هر هدف) در قصدِ آن برای دستیابی به آن هدف ضرب می‌کنیم. برای هر کشور، از طریق سنجهٔ قصد، عملاً وزنی برای قابلیت‌هایش قائل می‌شویم. جنبهٔ قصد در نمایهٔ انسی‌پی‌آی را می‌توان معاون وزن دانست. نمرهٔ قصدِ انسی‌پی‌آی نشان‌دهندهٔ اولویت‌های گوناگونی است که بعضی کشورها برای بعضی قابلیت‌های سایبریِ بخصوص قائل می‌شوند. این یعنی هر کشور فقط زمانی می‌تواند از قابلیت‌های سایبری خود در عرصه‌ای، مثلاً رصد ملی، استفاده کند که قصد ۱۰۰درصدی انجام این کار را داشته باشد. در تمام موارد دیگر، مقادیر شاخص‌های قابلیت را بر اساس اهمیت راهبردی‌ای که هر کشور برای آن‌ها قائل است، اصلاح کردیم.

تحلیل حساسیت

تحلیل حساسیت را برای نمایه انجام داده‌ایم تا تأثیر چهارچوب نظری‌مان را بیازماییم. مهم‌تر از همه، در محاسبهٔ انسی‌پی‌آی، برای هر قابلیت وزن یکسانی در نظر گرفته‌ایم. این چهارچوب بدیل تأثیر چشمگیری بر رده‌بندی ما ندارد.

شاخص‌های قابلیت در مقیاس‌های گوناگونی سنجیده شده‌اند. ما هر شاخص را استانداردسازی کرده‌ایم تا متغیرهای دارای مقیاس‌های واکنشِ گوناگون را به واحد اندازه‌گیری یکسانی درآوریم. تصمیم گرفتیم رویه‌ای موسوم به «نرمال‌سازی کمینه‌بیشینه» را پیش بگیریم که در

رشته‌های گوناگون برای دگرگونیِ داده‌های خام کاربرد گسترده‌ای دارد. اما این روشِ نرمال‌سازی محدودیت‌هایی هم دارد؛ ازجمله اینکه مقادیر دورافتاده بر نمرهٔ نهایی تأثیر می‌گذارند. دیگر تکنیک‌ها، همچون استانداردسازی z در رابطه با مقادیر دورافتاده دقیق‌ترند و بهتر می‌توانند گوناگونی سنجه‌ها را انعکاس دهند.[1] بعضی از سنجه‌های ما توزیع نرمال ندارند که باعث می‌شود فقط بتوانیم نرمال‌سازی کمینه‌بیشینه را انتخاب کنیم؛ اما با دیگر سنجه‌هایی که توزیع نرمال دارند، کنترل کیفیت انجام داده‌ایم؛ ازجمله اینکه نمایهٔ قابلیت را با استانداردسازی z محاسبه و نتایج را با روش انتخابی‌مان مقایسه کرده‌ایم.

هم شاخص ترکیبی و هم ابعاد آن را با دیگر سنجه‌های موجود مطابقت داده‌ایم؛ مثلاً شاخص ترکیبی را با پدیده‌های سنجش‌پذیر مرتبط (شاخص‌های ترکیبی مشابه و نیز کمیت‌های مرتبط، همچون تولید ناخالص داخلی و سرانهٔ تولید ناخالص داخلی) مطابقت داده‌ایم تا شباهت‌ها یا تفاوت‌ها را شناسایی کنیم.

چنان‌که انتظار می‌رفت، ان‌سی‌پی‌آی هم با نمایهٔ سایبری اتحادیهٔ بین‌المللی مخابرات (شکل ۸) و هم سرانهٔ تولید ناخالص داخلی (شکل ۹) هم‌بستگی مثبتی دارد. این هم‌بستگی نشان می‌دهد که هرچه تاب‌آوری سایبری یک کشور بالاتر و ثروتش بیشتر باشد، قدرت سایبری ملی بیشتری هم دارد.

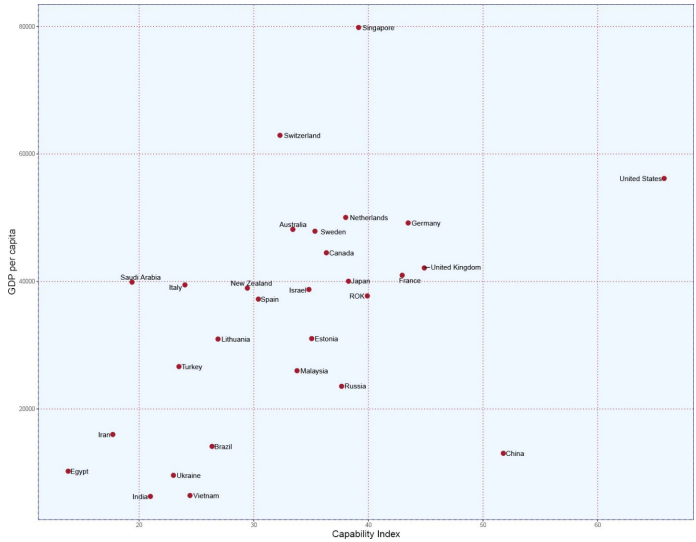
چنان‌که شکل ۸ نشان می‌دهد، تفاوت‌های مهمی هم وجود دارد؛ مثلاً در هنگام مقایسهٔ ان‌سی‌پی‌آی با نمایهٔ سایبری جهانی اتحادیهٔ بین‌المللی مخابرات، درمی‌یابیم که مصر، لیتوانی، ترکیه و عربستان

1 Carrino, L. (2017). The role of normalization in building composite indicators. rationale and consequences Of different strategies applied to social inclusion. In Complexity in Society: From Indicators Construction to their Synthesis (pp. 251-289). Springer, Cham.

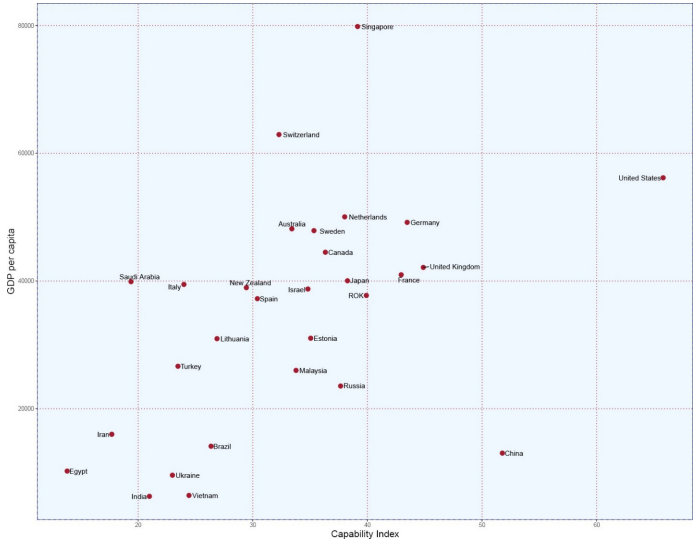
امتیاز نسبتاً بالایی در این اتحادیه دارند، اما امتیازشان در انسی‌پی‌آی پایین است.

نتایج مطابقت هم‌بستگی بین انسی‌پی‌آی و سرانهٔ تولید ناخالص داخلی، حکایت از رابطه‌ای خطی میان این دو سنجه دارد: سرانهٔ تولید ناخالص داخلیِ بالاتر با قدرت سایبری ملیِ بالاتر برابر است؛ البته استثنائات مهمی هم وجود دارد که چین نمونهٔ بارزش است. گرچه سرانهٔ تولید ناخالص داخلی در چین پایین است، رتبهٔ انسی‌پی‌آی آن بسیار بالاست.

شکل ۸: هم‌بستگی میان انسی‌پی‌آی بلفر و نمایهٔ سایبری جهانی اتحادیهٔ بین‌المللی مخابرات



شکل ۹: هم‌بستگی میان ان‌سی‌پی آی بلفر و سرانهٔ تولید ناخالص داخلی



۵. نتیجه‌گیری

۵. نتیجه‌گیری

نمایهٔ قدرت سایبری ملیِ بلفر، تلاشی ستودنی برای مفهومی‌سازی و سنجش قدرتِ سایبری در مقیاس کشورها است. ما سنجه‌ای چندبعدی و تفصیلی از قدرت سایبری ملی فراهم کرده‌ایم که پیچیدگی این مفهوم را انعکاس می‌دهد. این سنجه میان هفت هدف اصلیِ قدرت سایبری تمایز قائل می‌شود: (۱) رصد و پایش گروه‌های داخلی؛ (۲) تقویت و ارتقای دفاع سایبری ملی؛ (۳) کنترل و دست‌کاری محیط اطلاعاتی؛ (۴) جمع‌آوری اطلاعات در کشورهای دیگر به هدف امنیت ملی؛ (۵) افزایش توانایی سایبری و فنی ملی؛ (۶) نابودی یا غیرفعال‌سازی زیرساخت‌ها و قابلیت‌های دشمن؛ (۷) تعریف استانداردهای فنی و هنجارهای سایبری بین‌المللی.

قابلیت‌های سایبری چندمنظوره‌اند؛ هر سنجهٔ قدرت سایبری در آن واحد می‌تواند آن را هم توانمند کند و هم آسیب‌پذیر.

پژوهشگران و دست‌اندرکاران می‌توانند به شکل‌های گوناگونی از ان‌سی‌پی‌آی استفاده کنند: اول، می‌توانند از سنجهٔ تجمیعی ان‌سی‌پی‌آی برای قدرت سایبری در تمام هفت هدف استفاده کنند تا بفهمند کدام کشور جامع‌ترین قدرت سایبری است؛ دوم، چهارچوب ان‌سی‌پی‌آی می‌تواند به مخاطبان گسترده‌تری کمک کند تا بهتر بفهمند که هر هدف چگونه به قدرت سایبری بهره می‌رساند و چگونه کشورهایی که مقادیر گوناگونی از قصد و قابلیت دارند، در فضای سایبری تعامل می‌کنند؛

سوم، کاربرانی که به اهداف ملیِ بخصوص یا بعضی از مؤلفه‌های ان‌سی‌پی‌آی علاقه دارند، می‌توانند تحلیل ما را به طرق گوناگون بنگرند: از طریق یکی از هفت هدفِ ملی برای شناسایی قابل‌ترین کشورها در آن عرصه یا از طریق قصد یا از طریق قابلیت.

ما ان‌سی‌پی‌آی را ایجاد کرده‌ایم تا با این سنجه به دست‌اندرکاران و اساتید دانشگاه کمک کنیم گفت‌وگو دربارهٔ خط‌مشی سایبری را پیش ببرند. بر اساس وضعیت فعلیِ این عرصه، هنوز فضا برای توسعهٔ چهارچوب دقیق‌تر و ظریف‌تری به‌منظور درک قدرت سایبری وجود دارد؛ اما چهارچوب ما و داده‌هایی که گردآوری کرده‌ایم، می‌تواند گفت‌وگو دربارهٔ خط‌مشی سایبری را پیش ببرد و از تمرکز صرف بر حملهٔ سایبری، که وضعیت فعلی آن است، بگذراند. در پایان، امید داریم که این مطالعه شفافیت بیشتری را دربارهٔ قابلیت‌ها و قصد سایبری بپرورد؛ زیرا مؤلفه‌ای مهم برای جلوگیری از بالاگیریِ تعارضات خطرناک میان کشورهاست.

۶. منابع و ضمایم

کتاب‌شناسی

1. Anderson, C., & Sadjadpour, K. (2018). Iran's cyber threat, espionage, sabotage, and revenge. Retrieved from https:// carnegieendowment.org/04/01/2018/iran-s-cyber-threat-espionage-sabotage-and- revenge-pub75134-

2. Barker, T. (2017, May 26). Germany Strengthens its Cyber Defense. Foreign Affairs. Retrieved from https://www. foreignaffairs.com/articles/germany/26-05-2017/germany-strengthens-its-cyber-de- fense0%D

3. Bellingcat. (2018, October 305 .(4 car registrations may point to massive GRU security breach. Belling- cat. Retrieved from https://www.bellingcat.com/news/-305/04/10/2018car-registrations-may- point-massive-gru-security-breach/

4. Breene, K. (2016) "Who are the cyberwar superpowers?" World Economic Forum. Date accessed, 30 January 2020. https://www.weforum.org/agenda/05/2016/who-are-the-cyberwar-superpowers/

5. Connell, M. (2014). Deterring Iran's Use of Offensive Cyber. Retrieved from https://apps.dtic.mil/dtic/tr/ fulltext/u2/a617308.pdf

6. Council on Foreign Relations (2019), 'Cyber Operations Tracker'. Accessed December 2019. https://www. cfr.org/interactive/cyber-operations.

7. Curley, M. G. (2018). The Provision of Cyber Manpower. MCU Journal, 217–191 ,(1)9.

8. Curtis E Lemay Center for Doctrine Development and Education. (2016). "An Effects-Based Approach to Planning," Air University Alabama. Last modified, 4 November 2016. Date accessed, 30 January 2020. https://www.doctrine.af.mil/

Portals/61/documents/Annex_-0-3/0-3D-190PS-Effects-Based-Plan.pdf

9. Denning, D. (2017, December 12). Iran's cyber warfare program is now a major. Newsweek. Retrieved from https://www.newsweek.com/irans-cyber-warfare-program-now-major-threat-united- states745427-

10. DOD. (2016, October 24). All Cyber Mission Force Teams Achieve Initial Operating Capability. Www.

11. Defence.Com. Retrieved from https://www.defense.gov/Newsroom/News/Article/Article/984663/ all-cyber-mission-force-teams-achieve-initial-operating-capability/

12. DOJ. (2018). Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps. Retrieved from https://www.justice.gov/opa/pr/nine-irani- ans-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

13. Economist Intelligence Unit (2006) Democracy Index. Accessed June 2020 ,30. https://www.economist. com/media/pdf/DEMOCRACY_INDEX_2007_v3.pdf

14. Economist Intelligence Unit & Booz Allen Hamilton (2011) ""Cyber Power Index: Findings and Methodol- ogy 2011", Date accessed, 30 January 2020. https://www.sbs.ox.ac.uk/cybersecurity-capacity/sys- tem/files/EIU20%20%-Cyber20%Power20%Index20%Findings20%and20% Methodology.pdf

15. Freedom House. (2020) Freedom in the World Methodology. Accessed June 2020 ,30. (https://freedom-house.org/reports/freedom-world/freedom-world-research-methodology).

16. Gao. (2019). Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations, (August). Retrieved from https://www.gao. gov/assets/700940/710.pdf

17. GlobalStats (2020). "Search Engine Market Share Worldwide—May 2020-2019". Statcounter. Accessed June

20th, 2020. https://gs.statcounter.com/search-engine-market-share

18. Guzzini, S. (2009). "On the Measure of Power and the Power of Measure in International Relations," Danish Institute for International Studies Working Paper. Date accessed, 30 January 2020. https:// www.diis.dk/files/media/publications/import/extra/wp28-2009_measure_of_power_internation- al_relations_web_2.pdf

19. Hanson, F., & Uren, T. (2018). Australia's Offensive Cyber Capability. Retrieved from https://www.aspi. org.au/report/australias-offensive-cyber-capability0%D

20. Hathaway, M., Demchak, C., Kerben, J., Mcardle, J., & Spidalieri, F. (2016). Germany Cyber Readiness at a Glance. Retrieved from www.potomacinstitute.org

21. International Telecommunications Union. (2018). "Global Cybersecurity Index 2018," Published 2019.

22. Date accessed, 30 January 2020.

23. Jiji. (2018, December 1). Japan working on ability to counter cyberattacks. Japan Times.

24. Joshi, S. (2013, June 19). An IT superpower, India has just 556 cyber security experts. The Hindu. Retrieved from https://www.thehindu.com/news/national/an-it-superpower-india-has-just-556-cy- ber-security-experts/article4827644.ece

25. Kuehl, D. (2009). "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., Cyberpower and National Security. Washington, D.C.: National Defense University Press

26. Langner, R. (2016) "Cyber Power—An Emerging Factor in National and International Security". Center for International Relations and Sustainable Development. Autumn, Issue No.8. Accessed on June 2020 ,7.

27. Laudrain, A. (2019, February 26). France's new offensive cyber doctrine. Lawfare. Retrieved from https:// www.lawfareblog.com/frances-new-offensive-cyber-doctrine

28. Lewis, J. A. (2019). Iran and Cyber Power. Retrieved from

https://www.csis.org/analysis/iran-and-cyber- power

29. Mandiant. (2013). Apt1: Exposing One of China's Cyber Espionage Units. https://doi.org/102_8-30683 -540-3/10.1007

30. McGhee, A. (2017, June 30). Cyber Warfare unit set to be launched by Australian Defence Forces. ABC News. Retrieved from https://www.abc.net.au/news/30-06-2017/cyber-warfare-unit-to-be- launched-by-australian-defence-forces/8665230

31. Mueller, R. S. (2019). Report by Special Counsel Robert S. Mueller on the Investigation into Russian Inter- ference in the 2016 Presidential Election. Volume I.

32. OECD (2008). 'Handbook on Constructing Composite Indicators: Methodology and User Guide". Organi- sation for Economic Co-operation and Development. Date accessed September 4th 2020. Available here: www.oecd.org/publishing/corrigenda

33. Oliphant, R. (2017, May 6). Who are Russia's Cyber-warriors and what should the west do about them? Telegraph. Retrieved from https://www.telegraph.co.uk/news/16/12/2016/russias-cyber-warriors- should-west-do/

34. Oliphant, R. (2018, October 4). What is Unit 26165, Russia's elite military hacking center? The Telegraph. Retrieved from https://www.telegraph.co.uk/news/04/10/2018/unit-26165 russias-elite-mili- tary-hacking-centre/

35. Tkacheva, O., Schwartz, L., Libicki, M., Taylor, J., Martini, J. and Baxter, C., (2013) "Internet Freedom and Political Space". RAND Corporation. Santa Monica, CA: RAND Corporation Accessed on June 2020 ,7. https://www.rand.org/pubs/research_reports/RR295.html. Also available in print form.

36. The Associated Press. (2015, January 6). South Korea: North Korea has -6,00member cyber army. Re- trieved from https://phys.org/news/-01-2015south-korea-north-member-cyber.html

37. U.S. Department of Commerce & U.S. Department of Homeland Security, "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity

Workforce: Building the Foundation for a More Secure American Future," National Institute of Standards and Technology: Computer Security Resource Center. Published 10 May 2018. Accessed 30 January 2020. https:// csrc.nist.gov/publications/detail/white-paper/30/05/2018/supporting-growth-and-sustain- ment-of-the-cybersecurity-workforce/final

38. Vavra, S. (2017). axios.com. Retrieved from https://www.axios.com/the-worlds-top-cyber-powers-4-1513304669fa-53675b7e-4276-6a2bf4-a84b4986fe9.html

39. Vidoli, Francesco, and Elisa Fusco (2019). Compind: Composite Indicators Functions. Date accessed September 4th 2020. Available here: https://CRAN.R-project.org/package=Compind

40. Voo, Julia., Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach (2020). "Reconceptualizing Cyber Power". Belfer Policy Paper.

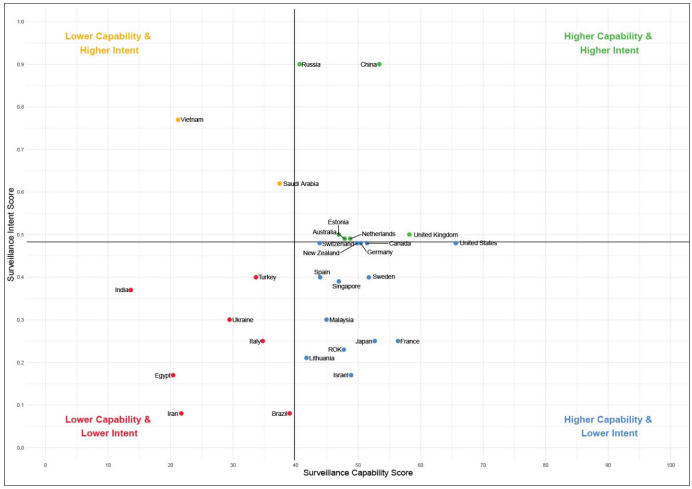
41. Wen, Philip. (2018) "China Denies 'Slanderous' Economic Espionage Charges from US allies". Reu- ters. Published December 2018 ,18. Accessed June 2020 ,30. https://www.reuters.com/article/

42. us-china-cyber-usa-ministry/china-denies-slanderous-economic-espionage-charges-from-u-s-allies-idUSKCN1OK03Y

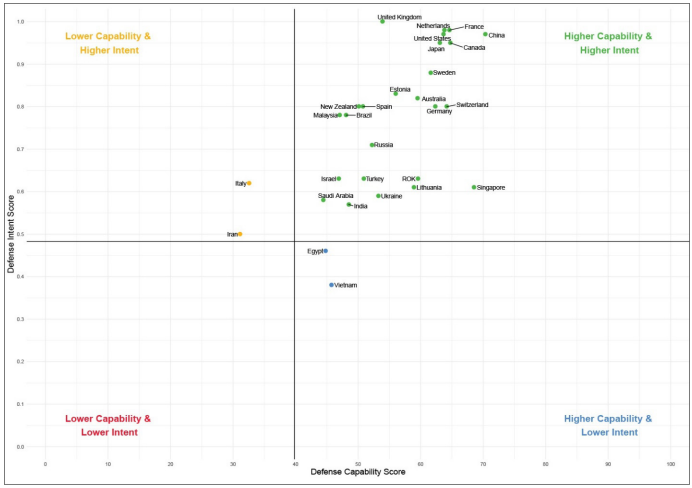
43. White House. (2018). "National Cyber Strategy of the United States of America Cyber Strategy". Pub- lished September 2018. Accessed 30 January 2020. https://www.whitehouse.gov/wp-content/ uploads/09/2018/National-Cyber-Strategy.pdf

44. Zaaiman, J., & Louise, L. (2015). Proceedings of the 10th International Conference on Cyber Warfare and Security ICCWS2015-. Reading: Academic Conferences and Publishing International Limited. Retrieved from https://books.google.co.uk/books?hl=en&lr=&id=piikBwAAQBAJ&oi=fnd&p-g=PA20&dq=compare+Military+Cyber+power+manpower&ots=EXxOscvBdz&sig=BYSy1JGfa- j76m1TKHb8UD8W8wqY#v=onepage&q=compare Military Cyber power manpower&f=false

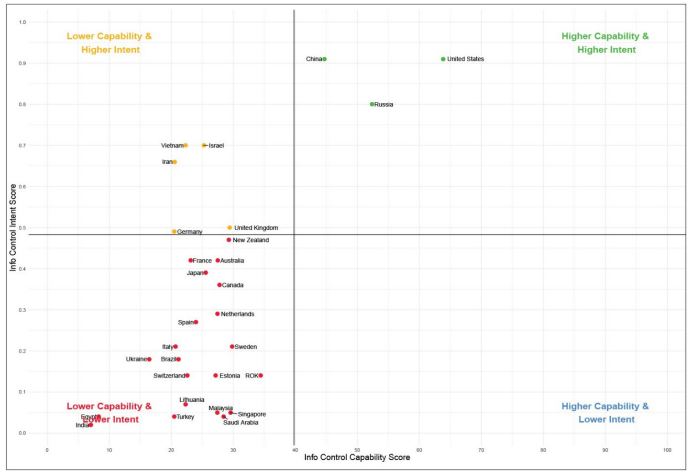
ضمیمهٔ الف: نقشهٔ انسی‌پی‌آی
نمودارها بر اساس هدف
رصد



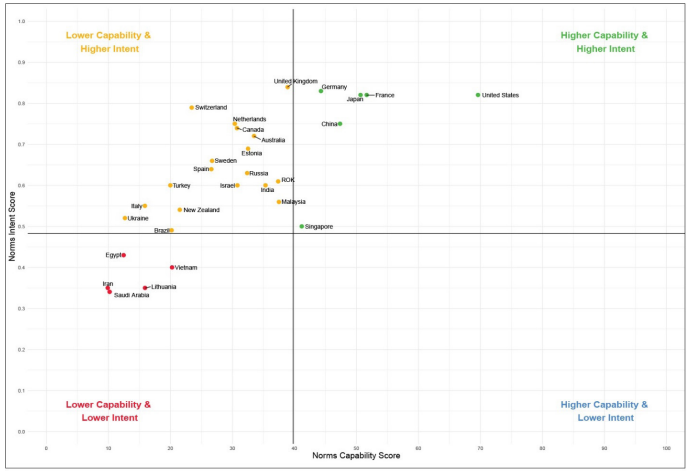
دفاع



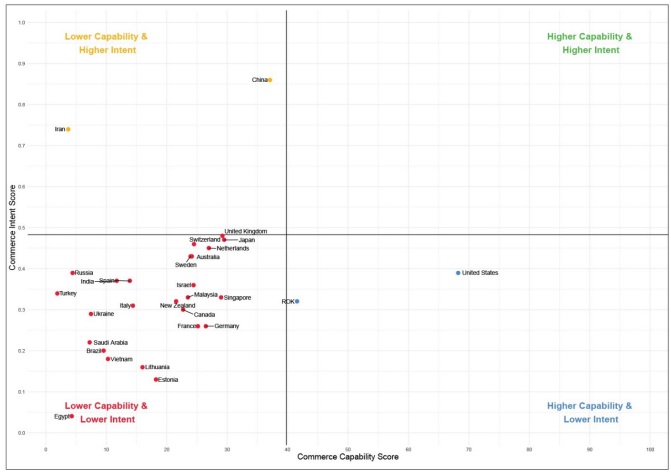
هنجارها



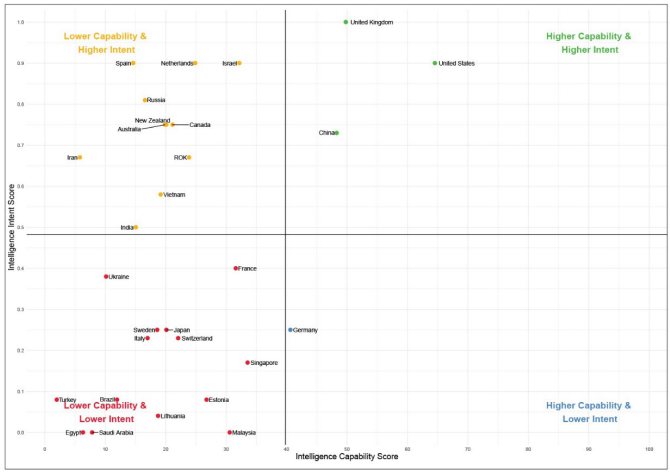
کنترل اطلاعات



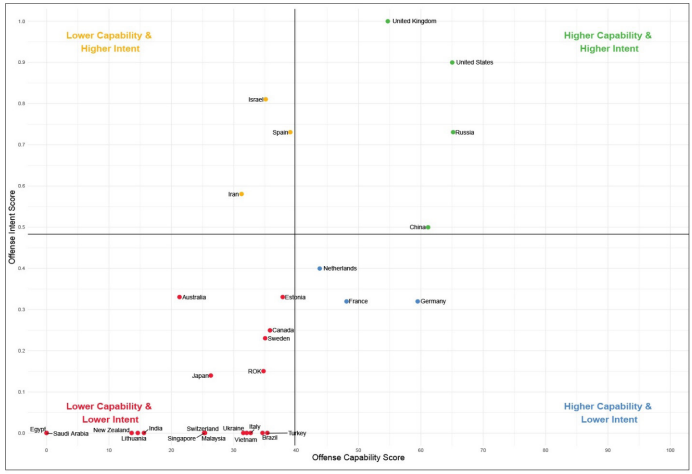
تجارت



اطلاعات



حمله


Lower Capability &
Higher Intent
Higher Capability &
Higher Intent
Lower Capability &
Lower Intent
Higher Capability &
Lower Intent
United Kingdom
United States
Israel
Spain
Russia
Iran
China
Netherlands
Australia
Estonia
France
Germany
Canada
Sweden
Japan
ROK
Egypt
Saudi Arabia
New Zealand
India
Lithuania
Switzerland
Singapore
Malaysia
Ukraine
Italy
Vietnam
Brazil
Turkey
Offense Intent Score
Offense Capability Score

ضمیمهٔ ب: شرح تفصیلی شاخص‌های قصد براساس هدف

- نظارت

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
آیا کشور اسناد برنامه‌ریزی یا راهبرد نظامی سایبری دارد و اذعان می‌کند که قابلیت سایبری مخرب دارد؟	ارتش‌ها نیز مانند تمام بروکراسی‌های بزرگ، سلسله‌مراتب روشن و نقشه‌هایی مؤثر دارند. ارتش فقط در صورتی می‌تواند استفادهٔ کارآمدی از شیوه‌های سایبری کند که فرماندهان بدانند این شیوه‌ها را چه زمان و چگونه باید به‌کار گرفت و اینکه چگونه می‌توانند قابلیت‌های متعارف را تکمیل کنند. علاوه بر این، تمام ارتش‌ها بابت قابلیت‌هایی که درصدد کسب آن‌ها بر می‌آیند، با بهای فرصتی روبه‌رو می‌شوند و از آن‌ها انتظار می‌رود در اسناد برنامه‌ریزی دفاع ملی، ارزش فعالیت‌های سایبری را توجیه کنند.	تحلیل حضور برخط وزارت دفاع هر کشور یا نیروهای مسلح آن برای یافتن اسناد مرتبط. اسناد مرتبط عبارت‌اند از: نقشه‌های دفاعی؛ راهبردهای دفاعی؛ دکترین نظامی؛ دفاع از گزارش‌های دولتی سایبری؛ بیانیه‌های رهبران ارشد ارتش؛ بیانیه‌های سیاست‌مداران وزارت دفاع دربارهٔ قابلیت‌های سایبری کشور.	۲۰۲۰	بله/خیر
آیا واحد یا فرماندهی سایبری ارتش کشور اذعان می‌کند که کشور قابلیت سایبری مخرب دارد؟	داشتن یک واحد یا فرماندهی مختص فعالیت‌های سایبری در ارتش، نشان می‌دهد که کشور به‌دنبال ارتقا و افزایش تخصص سایبری نظامی خود و جذب نیرو برای برآوردن نیازهای خود است. با توجه به کمبود کارکنان ماهر سایبری در تمام کشورها، واحدهای نظامی سایبری باید برای جذب بهترین‌ها با یکدیگر رقابت کنند. پس واحدهای نظامی به‌دنبال توضیح نقش خود و قابلیت‌هایی خواهند بود که عرضه می‌کنند.	تحلیل حضور برخط نیروی سایبری ارتش هر کشور برای ارزیابی اینکه آیا به این هدف اذعان می‌کند یا نه. همچنین دنبال نظرات عمومی از سوی سیاست‌مداران یا رهبران ارشد ارتش سایبری درباب قابلیت‌هایی بودیم که واحدهای نظامی گوناگون از آن‌ها برخوردارند.	۲۰۲۰	بله/خیر

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
آیا آژانس اطلاعاتی کشور یا سرویس اطلاعات خارجی آن اذعان می‌کنند که کشور دارای قابلیت سایبری مخرب است؟	اذعان به اینکه آژانس اطلاعاتی کشور دارای مأموریتی سایبری است	تحلیل حضور بر خط آژانس اطلاعاتی هر کشور برای ارزیابی اینکه آیا به این هدف اذعان می‌کند یا نه. همچنین دنبال نظرات عمومی از سوی سیاست‌مداران یا رهبران ارشد آژانس‌های اطلاعاتی سایبری دربارهٔ قابلیت‌هایی بودیم که اجتماع اطلاعاتی از آن‌ها برخوردار است.	۲۰۲۰	بله/خیر
ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	کشورهایی که با راهبردهای گوناگونی در پی هدف بخصوصی بوده‌اند و تعهد خود را برای نیل به آن هدف نشان می‌دهند، احتمال اینکه درک پخته‌تری داشته باشند، بیشتر است.	مقایسهٔ اهداف برشمرده در جدیدترین راهبرد، با اهداف برشمرده در راهبرد قبلی (اگر وجود داشته باشد).	۲۰۲۰	هدف حاضر در یک راهبرد: بله/خیر
در یک حملهٔ سایبری منسوب مشاهده‌شده است	برخلاف شاخص‌های قصد که قصد خاصی را (که نیازمند برنامه‌ریزی و تمایل قبلی است) نشان می‌دهند، از اقدامات یک کشور نیز می‌توان قصد کلی را (که از ارتکاب مفروض داشته می‌شود) از اقدامات یک کشور استنباط کرد.	استفاده از آمار و ارقام ردیاب عملیات سایبری شورای روابط خارجی برای ارزیابی اینکه آیا یک یا چند حمله به کشور نسبت داده شده است یا نه.	۲۰۲۰	مشاهده‌شده در یک یا چند حمله: بله/خیر
اگر در راهبرد سایبری ملی کشور به فعالیت مخرب اذعان می‌کنند، نمرهٔ راهبرد را بیاورید.	ن.ک: جدول امتیاز راهبرد	ن.ک: جدول امتیاز راهبرد	۲۰۲۰	ن.ک: جدول امتیاز راهبرد
اگر در راهبرد سایبری ملی کشور به فعالیت مخرب اذعان می‌کنند، نمرهٔ مالی را بیاورید.	کشور به حد کافی تعهد دارد تا راهبردی ارائه دهد که از بودجهٔ ملی برای رسیدن به برون‌داد مدنظر خود استفاده کند.	کشور از زمان انتشار جدیدترین راهبرد خود، افزایش بودجهٔ سایبری را اعلام کرده است.	۲۰۲۰	بله/خیر

- دفاع

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
آیا کشور نقشهٔ امنیت‌سایبری‌ای منتشر کرده که تعریف کند چگونه از سیستم‌های دولتی یا زیرساخت‌های حیاتی ملی پاسداری می‌کند؟	حتی تلاش برای محافظت از سیستم‌های فناوری اطلاعات دولت هم نیازمند مشارکت و برنامه‌ریزی فروشندگان بخش خصوصی است. نقشه یا راهبرد، ضامن این خواهد بود که درک روشن و ثابتی از نیازمندی‌ها و معیارهایی وجود دارد که باید به آن‌ها دست یافت.	تحلیل حضور برخط هر کشور برای نقشه‌ها یا راهبردِ پاسداری از زیرساخت‌های حیاتی ملی یا نقشه برای پاسداری از سیستم‌های فناوری اطلاعات دولت	۲۰۲۰	بله/خیر
آیا کشور درصدد برگزاری کارزارهای آگاهی سایبری و بهداشت‌سایبری است؟	آیا کشور اقداماتی برای ایمن داشتن تمام جمعیت و استفادهٔ خصوصی‌شان از اینترنت از هرگونه خطر سایبری انجام می‌دهد؟	جست‌وجوی اینترنتی وب‌سایت‌های دولتی برای مشاهدهٔ محبوبیت مردمی و کارزارهای هشداری.	۲۰۲۰	بله/خیر
آیا کشور اعلام کرده که قصد دارد به‌طور فعالانه اقدامات‌سایبری ملی برای دفاع را انجام دهد؟	گرایش از دفاع سایبری ملی واکنشی به دفاع فعال (نیاز این است که این مقوله تعریف شود، اما اصولاً: فایروال بزرگ چین، الگوی دفاع سایبری فعال بریتانیا، بازرسی بسته‌ای روسیه، شاید دفاع رو به جلو فرماندهی سایبری آمریکا)	جست‌وجوی اینترنتی وب‌سایت‌های دولتی برای مشاهدهٔ ارجاعات به تمهیداتِ سایبری فعال ملی برای دفاع. همچنین دنبال نظرات عمومی سیاست‌مداران و رهبران ارتش و آژانس‌های اطلاعاتی بودیم.	۲۰۲۰	بله/خیر
ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	کشورهایی که با راهبردهای گوناگونی در پی هدف بخصوصی بوده‌اند و تعهد خود را برای نیل به آن هدف نشان می‌دهند، احتمال اینکه درک پخته‌تری داشته باشند، بیشتر است.	مقایسهٔ اهداف برشمرده در جدیدترین راهبرد، با اهداف برشمرده در راهبرد قبلی (اگر وجود داشته باشد).	۲۰۲۰	هدف موجود در یک راهبرد: بله/ خیر

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
اگر راهبرد سایبری ملی کشور، تقویت و ارتقای فعالیت دفاعی سایبری ملی را به رسمیت می‌شناسد، نمرهٔ راهبرد را بیاورید.	ن.ک: جدول نمرهٔ راهبرد	ن.ک: جدول نمرهٔ راهبرد	۲۰۲۰	ن.ک: جدول نمرهٔ راهبرد
اگر راهبرد سایبری ملی کشور، تقویت و ارتقای فعالیت دفاعی سایبری ملی را به رسمیت می‌شناسد، نمرهٔ راهبرد را بیاورید.	کشور به حد کافی تعهد دارد تا راهبردی ارائه دهد که از بودجهٔ ملی برای رسیدن به برون‌داد مدنظر خود استفاده کند.	کشور از زمان انتشار جدیدترین راهبرد خود، افزایش بودجهٔ سایبری را اعلام کرده است.	۲۰۲۰	بله/خیر
اگر راهبرد سایبری ملی کشور به رشد فعالیت در راستای افزایش توانایی سایبری و فنی ملی اذعان می‌کند، نمرهٔ راهبرد را بیاورید.	ن.ک: جدول نمرهٔ راهبرد	ن.ک: جدول نمرهٔ راهبرد	۲۰۲۰	ن.ک: جدول نمرهٔ راهبرد
اگر راهبرد سایبری ملی کشور به رشد فعالیت در راستای افزایش توانایی سایبری و فنی ملی اذعان می‌کند، نمرهٔ مالی را بیاورید.	کشور به حد کافی تعهد دارد تا راهبردی ارائه دهد که از بودجهٔ ملی برای رسیدن به برون‌داد مدنظر خود استفاده کند.	کشور از زمان انتشار جدیدترین راهبرد خود، افزایش بودجهٔ سایبری را اعلام کرده است.	۲۰۲۰	بله/خیر

- اطلاعات

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
آیا برنامه‌ریزی نظامی یا اسناد راهبردی سایبری یا برنامه‌ریزی نظامی یا اسناد راهبردی کلی، اذعان می‌کنند که کشور قابلیت سایبری جمع‌آوری اطلاعات دارد؟	ارتش‌ها نیز مانند تمام بروکراسی‌های بزرگ، سلسله‌مراتب روشن و نقشه‌هایی مؤثر دارند. ارتش فقط در صورتی می‌تواند استفادهٔ کارآمدی از شیوه‌های سایبری کند که فرماندهان بدانند این شیوه‌ها را چه زمان و چگونه باید به‌کار گرفت و اینکه چگونه می‌توانند قابلیت‌های متعارف را تکمیل کنند. علاوه بر این، تمام ارتش‌ها بابت قابلیت‌هایی که درصدد کسب آن‌ها بر می‌آیند، با بهای فرصتی روبه‌رو می‌شوند و از آن‌ها انتظار می‌رود در اسناد برنامه‌ریزی دفاع ملی، ارزش فعالیت‌های سایبری را توجیه کنند.	تحلیل حضور برخط وزارت دفاع هر کشور یا نیروهای مسلح آن برای یافتن اسناد مرتبط. اسناد مرتبط عبارت‌اند از: نقشه‌های دفاعی؛ راهبردهای دفاعی؛ دکترین نظامی؛ دفاع از گزارش‌های دولتی سایبری؛ بیانیه‌های رهبران ارشد ارتش؛ بیانیه‌های سیاست‌مداران وزارت دفاع دربارهٔ قابلیت‌های سایبری کشور.	۲۰۲۰	بله/خیر
آیا واحد یا فرماندهی سایبری ارتش کشور اذعان می‌کند که کشور قابلیت سایبری جمع‌آوری اطلاعات دارد؟	داشتن یک واحد یا فرماندهی مختص فعالیت‌های سایبری در ارتش، نشان می‌دهد که کشور به‌دنبال ارتقا و افزایش تخصص سایبری نظامی خود و جذب نیرو برای برآوردن نیازهای خود است. با توجه به کمبود کارکنان ماهر سایبری در تمام کشورها، واحدهای نظامی سایبری باید برای جذب بهترین‌ها با یکدیگر رقابت کنند. پس واحدهای نظامی به‌دنبال توضیح نقش خود و قابلیت‌هایی خواهند بود که عرضه می‌کنند.	تحلیل حضور برخط نیروی سایبری ارتش هر کشور برای ارزیابی اینکه آیا به این هدف اذعان می‌کند یا نه. همچنین دنبال نظرات عمومی از سوی سیاست‌مداران یا رهبران ارشد ارتش سایبری درباب قابلیت‌هایی بودیم که واحدهای نظامی گوناگون از آن‌ها برخوردارند.	۲۰۲۰	بله/خیر

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
آیا آژانس اطلاعاتی کشور یا سرویس اطلاعات خارجی، اذعان می‌کند که کشور قابلیت سایبری جمع‌آوری اطلاعات دارد؟	اذعان به اینکه آژانس اطلاعاتی کشور، مأموریتی سایبری دارد	تحلیل حضور برخط آژانس اطلاعاتی هر کشور برای ارزیابی اینکه آیا به این هدف اذعان می‌کند یا نه. همچنین دنبال نظرات عمومی از سوی سیاست‌مداران یا رهبران ارشد آژانس‌های اطلاعاتی سایبری دربارهٔ قابلیت‌هایی بودیم که اجتماع اطلاعاتی آن‌ها را دارد.	۲۰۲۰	بله/خیر
ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	کشورهایی که با راهبردهای گوناگونی در پی هدف بخصوصی بوده‌اند و تعهد خود را برای نیل به آن هدف نشان می‌دهند، احتمال اینکه درک پخته‌تری داشته باشند، بیشتر است.	مقایسهٔ اهداف برشمرده در جدیدترین راهبرد، با اهداف برشمرده در راهبرد قبلی (اگر وجود داشته باشد).	۲۰۲۰	هدف حاضر در یک راهبرد: بله/خیر
در یک حملهٔ سایبری منسوب مشاهده شده است	برخلاف شاخص‌های قصد، که قصد خاصی را (که نیازمند برنامه‌ریزی و تمایل قبلی است) نشان می‌دهند، از اقدامات یک کشور نیز می‌توان قصد کلی را (که از ارتکاب مفروض داشته می‌شود) از اقدامات یک کشور استنباط کرد.	استفاده از آمار و ارقام ردیابِ عملیات سایبری شورای روابط خارجی برای ارزیابی اینکه آیا یک یا چند حمله به کشور نسبت داده شده است یا نه.	۲۰۲۰	مشاهده‌شده در یک یا چند حمله: بله/خیر
اگر در راهبرد سایبری ملی کشور به فعالیت اطلاعاتی اذعان می‌کنند، نمرهٔ راهبرد را بیاورید.	ن.ک: جدول امتیاز راهبرد	ن.ک: جدول امتیاز راهبرد	۲۰۲۰	ن.ک: جدول امتیاز راهبرد
اگر در راهبرد سایبری ملی کشور به فعالیت اطلاعاتی اذعان می‌کنند، نمرهٔ راهبرد را بیاورید.	کشور به حد کافی تعهد دارد تا راهبردی ارائه دهد که از بودجهٔ ملی برای رسیدن به برون‌داد مدنظر خود استفاده کند.	کشور از زمان انتشار جدیدترین راهبرد خود، افزایش بودجهٔ سایبری را اعلام کرده است.	۲۰۲۰	بله/خیر

- کنترل اطلاعات

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
قدرت قانون محافظت از داده	قوانین محافظت از داده در هر کشور چقدر صریح و دقیق است	استفاده از نمره‌دهی حفاظت دادهٔ DLA Piper برای هر کشور	۲۰۲۰	سنگین/ پررنگ/ متوسط/ محدود/بدون اطلاعات
آیا برنامه‌ریزی نظامی یا اسناد راهبردی سایبری یا برنامه‌ریزی نظامی یا اسناد راهبردی کلی اذعان می‌کنند که کشور قابلیت سایبری برای کنترل و دست‌کاری محیط اطلاعاتی دارد؟	ارتش‌ها نیز مانند تمام بروکراسی‌های بزرگ، سلسله‌مراتب روشن و نقشه‌هایی مؤثر دارند. ارتش فقط در صورتی می‌تواند استفادهٔ کارآمدی از شیوه‌های سایبری کند که فرماندهان بدانند این شیوه‌ها را چه زمان و چگونه باید به‌کار گرفت و اینکه چگونه می‌توانند قابلیت‌های متعارف را تکمیل کنند. علاوه بر این، تمام ارتش‌ها با بت قابلیت‌هایی که درصدد کسب آن‌ها بر می‌آیند، با بهای فرصتی رو به‌رو می‌شوند و از آن‌ها انتظار می‌رود در اسناد برنامه‌ریزی دفاع ملی، ارزش فعالیت‌های سایبری را توجیه کنند.	تحلیل حضور برخط وزارت دفاع هر کشور یا نیروهای مسلح آن برای یافتن اسناد مرتبط. اسناد مرتبط عبارت‌اند از: نقشه‌های دفاعی؛ راهبردهای دفاعی؛ دکترین نظامی؛ دفاع از گزارش‌های دولتی سایبری؛ بیانیه‌های رهبران ارشد ارتش؛ بیانیه‌های سیاست‌مداران وزارت دفاع دربارهٔ قابلیت‌های سایبری کشور.	۲۰۲۰	بله/خیر
آیا واحد یا فرماندهی سایبری ارتش کشور اذعان می‌کند که کشور دارای قابلیت سایبری مخرب است؟	داشتن یک واحد یا فرماندهی مختص فعالیت‌های سایبری در ارتش نشان می‌دهد که کشور به دنبال ارتقا و افزایش تخصص سایبری نظامی خود و جذب نیرو و برای برآوردن نیازهای خود است. با توجه به کمبود کارکنان ماهر سایبری در تمام کشورها، واحدهای نظامی سایبری باید برای جذب بهترین‌ها با یکدیگر رقابت کنند. پس واحدهای نظامی به دنبال توضیح نقش خود و قابلیت‌هایی که عرضه می‌کنند خواهند بود.	تحلیل حضور برخط نیروی سایبری ارتش هر کشور برای ارزیابی اینکه آیا به این هدف اذعان می‌کند یا نه. همچنین دنبال نظرات عمومی از سوی سیاستمداران یا رهبران ارشد ارتش سایبری در باب قابلیت‌هایی بودیم که واحدهای نظامی مختلف از آن‌ها برخوردارند.	۲۰۲۰	بله/خیر

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
آیا آژانس اطلاعاتی کشور یا سرویس اطلاعات خارجی آن اذعان می‌کنند که کشور قابلیت سایبری برای کنترل و دست‌کاری محیط اطلاعاتی دارد؟	اذعان به اینکه آژانس اطلاعاتی کشور مأموریتی سایبری دارد	تحلیل حضور برخطِ آژانس اطلاعاتیِ هر کشور برای ارزیابی اینکه آیا به این هدف اذعان می‌کند یا نه. همچنین دنبال نظرات عمومی از سوی سیاست‌مداران یا رهبران ارشد آژانس‌های اطلاعاتی سایبری دربارهٔ قابلیت‌هایی بودیم که اجتماع اطلاعاتی آن‌ها را دارد.	۲۰۲۰	بله/خیر
ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	کشورهایی که با راهبردهای گوناگونی در پی هدف بخصوصی بوده‌اند و تعهد خود را برای نیل به آن هدف نشان می‌دهند، احتمال اینکه درک پخته‌تری داشته باشند، بیشتر است.	مقایسهٔ اهداف برشمرده در جدیدترین راهبرد با اهداف برشمرده در راهبرد قبلی (اگر وجود داشته باشد).	۲۰۲۰	هدف حاضر در یک راهبرد: بله/ خیر
در یک حملهٔ سایبری منسوب مشاهده شده است.	برخلاف شاخص‌های قصد، که قصد خاصی را (که نیازمند برنامه‌ریزی و تمایل قبلی است) نشان می‌دهند، از اقدامات یک کشور نیز می‌توان قصد کلی را (که از ارتکاب مفروض داشته می‌شود) از اقدامات یک کشور استنباط کرد.	استفاده از آمار و ارقام ردیاب عملیات سایبری شورای روابط خارجی برای ارزیابی اینکه آیا یک یا چند حمله به کشور نسبت داده شده است یا نه.	۲۰۲۰	مشاهده‌شده در یک یا چند حمله: بله/خیر
اگر راهبرد سایبری ملی کشور، فعالیت‌های مربوط به کنترل و دست‌کاری محیط اطلاعاتی را به رسمیت می‌شناسد، نمرهٔ راهبرد را بیاورید.	ن.ک: جدول نمرهٔ راهبرد	ن.ک: جدول نمرهٔ راهبرد	۲۰۲۰	ن.ک: جدول نمرهٔ راهبرد
اگر راهبرد سایبری ملی کشور، فعالیت‌های مربوط به کنترل و دست‌کاری محیط اطلاعاتی را به رسمیت می‌شناسد، نمرهٔ راهبرد را بیاورید.	کشور به حد کافی تعهد دارد تا راهبردی ارائه دهد که از بودجهٔ ملی برای رسیدن به برون‌داد مدنظر خود استفاده کند.	کشور از زمان انتشار جدیدترین راهبرد خود، افزایش بودجهٔ سایبری را اعلام کرده است.	۲۰۲۰	بله/خیر

- مالی

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
آیا کشور عضو چینش تشخیص معیارهای مشترک (سی‌سی‌آرای) هست؟	معیارهای مشترک استانداردی است که تضمین می‌کند «محصولات فناوری اطلاعات و (ارزیابی‌ها و) پروفایل‌های محافظتی طبق استانداردهای بالا و پایدار انجام می‌شوند». سی‌سی‌آرای تشخیص متقابل ارزیابی‌های معیارهای مشترک را ممکن می‌سازد و کشورها می‌توانند بدون ارزیابی مجدد، محصولات و خدمات را صادر و وارد کنند.	اعداد و ارقام برگرفته از: https://www.commoncriteriaportal.org/ccra/members/	۲۰۲۰	بله/خیر
آیا کشور عضو سیستم طرح‌های ارزیابی سازگاری برای تجهیزات و اجزای الکتروتکنیکی در کمیسیون بین‌المللی الکتروتکنیک (آی‌ای‌سی) است؟	این سیستم «سامانهٔ مجوزدهی چندگانه‌ای مبتنی بر استانداردهای بین‌المللی آی‌ای‌سی است. اعضای آن در سراسر دنیا از اصل تشخیص متقابل (پذیرش دوطرفهٔ) نتایج آزمایش‌ها برای دریافت مجوز در سطح ملی استفاده می‌کنند.	اعداد و ارقام برگرفته از: https://www.iecee.org/dyn/www/f?p=106:40:0	۲۰۲۰	بله/خیر
آیا کشور نقشه یا راهبردی برای جذب سرمایه‌گذاری در شرکت‌های سایبری یا افزایش صادرات سایبری خود منتشر کرده است؟	کشور به‌صورت فعال در پی افزایش سود صنعت امنیت سایبری است.	جست‌وجوی اینترنتی وب‌سایت‌های دولتی برای یافتن شواهدی مبنی بر توصیه یا راهنمایی خاصی برای صادرکنندگانِ امنیت سایبری یا تلاش برای جذب سرمایه‌گذاران خارجی به‌منظور سرمایه‌گذاری در محصولات و شرکت‌های امنیت سایبری ملی.	۲۰۲۰	بله/خیر

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	کشورهایی که با راهبردهای گوناگونی در پی هدف بخصوصی بوده‌اند و تعهد خود برای نیل به آن هدف را نشان می‌دهند، احتمال اینکه درک پخته‌تری داشته باشند، بیشتر است.	مقایسهٔ اهداف برشمرده در جدیدترین راهبرد با اهداف برشمرده در راهبرد قبلی (اگر وجود داشته باشد).	۲۰۲۰	هدف حاضر در یک راهبرد: بله/خیر
در یک حملهٔ سایبری منسوب مشاهده شده است	برخلاف شاخص‌های قصد، که قصد خاصی را (که نیازمند برنامه‌ریزی و تمایل قبلی است) نشان می‌دهند، از اقدامات یک کشور نیز می‌توان قصد کلی را (که از ارتکاب مفروض داشته می‌شود) از اقدامات یک کشور استنباط کرد.	استفاده از آمار و ارقام ردیاب عملیات سایبری شورای روابط خارجی برای ارزیابی اینکه آیا یک یا چند حمله به کشور نسبت داده شده است یا نه.	۲۰۱۹	مشاهده‌شده در یک یا چند حمله: بله/خیر
اگر راهبرد سایبری ملی کشور، فعالیت‌های مربوط به اندوختن ثروت یا استخراج رمزارز را به رسمیت می‌شناسد، نمرهٔ راهبرد را بیاورید.	ن.ک: جدول نمرهٔ راهبرد	ن.ک: جدول نمرهٔ راهبرد	۲۰۲۰	ن.ک: جدول نمرهٔ راهبرد
اگر راهبرد سایبری ملی کشور، فعالیت‌های مربوط به اندوختن ثروت یا استخراج رمزارز را به رسمیت می‌شناسد، نمرهٔ مالی را بیاورید.	کشور به حد کافی تعهد دارد تا راهبردی ارائه دهد که از بودجهٔ ملی برای رسیدن به برون‌داد مدنظر خود استفاده کند.	کشور از زمان انتشار جدیدترین راهبرد خود، افزایش بودجهٔ سایبری را اعلام کرده است.	۲۰۲۰	بله/خیر

- تجاری

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
نرخ مشارکت در کمیتهٔ مشترک فنی ایزو/ آی‌ای‌سی برای فناوری اطلاعات و ارتباطات چقدر است؟	سازمان بین‌المللی استانداردسازی (ایزو) و کمیسیون بین‌المللی الکتروتکنیک (آی‌ای‌سی) استانداردهای مشترک اجماع‌مبنایی برای فناوری‌های اطلاعات عرضه می‌کنند که برای بازار موضوعیت داشته باشند. شکل‌دهی کمیته‌های فنی مشترک ایزو/آی‌ای‌سی و پایبندی به آن، نشان از تعهد به بهبود این عناصر در کشور خودشان دارد. امتیاز هرچه بالاتر باشد، کشور مربوط فعالیت بیشتری در استانداردسازی بین‌المللی دارد که برای سازگاری صنعت داخلی‌اش با بازارهای بین‌المللی مهم است.	https://www.iso.org/technical-committees.html	۲۰۲۰	تعداد کمیته‌های فنی مشترک ایزو/ آی‌ای‌سی که فلان کشور عضو آن‌هاست، تقسیم بر ۲۲ (تعداد کل کمیته‌های فنی مشترک ایزو/ آی‌ای‌سی). امتیازِ به‌دست‌آمده درصدی از کمیته‌های فنی است که کشور مدنظر در آن‌ها شرکت کرده است.
کیفیت مشارکت در تمام ۲۲ کمیتهٔ مشترک فنی ایزو/آی‌ای‌سی چقدر است؟	سازمان بین‌المللی استانداردسازی (ایزو) و کمیسیون بین‌المللی الکتروتکنیک (آی‌ای‌سی) استانداردهای مشترک اجماع‌مبنایی برای فناوری‌های اطلاعات عرضه می‌کنند که برای بازار موضوعیت داشته باشند. شکل‌دهی کمیته‌های فنی مشترک ایزو/آی‌ای‌سی و پایبندی به آن، نشان از تعهد به بهبود این عناصر در کشور خودشان دارد. امتیاز هرچه بالاتر باشد، کشور مربوط مرجعیتِ رسمی بیشتری در کمیته‌های فنی داشته است و صنعتش نقش بیشتری در شکل‌دهی استانداردهای بین‌المللی در دستورالعمل فناوری اطلاعات و ارتباطات دارد.	https://www.iso.org/technical-committees.html	۲۰۲۰	به هر کشور بر اساس نقشش در هر کمیتهٔ فنی، امتیازی داده شد. امتیاز به این شکل بود: ۱ = دبیر ۰٫۷۵ = مشارکت‌کننده ۰٫۵ = ناظر ۰٫۲۵ = عضو کمیسیون فنی مشترک ایزو/آی‌ای‌سی ۰ = بدون وابستگی. سپس میانگین مشارکت هر کشور در تمام کمیته‌ها اعمال شد تا امتیاز نهایی بین ۰ تا ۱۰۰ باشد.

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
آیا کشور طرح مشارکت بخش دولتی و خصوصی‌ای برای رشد صنعت سایبری داخلی و نیروی کار و افزایش آگاهی از مسائل سایبری دارد؟	سازمان‌های بخش خصوصی، منبعی از قابلیت برای رشد تخصص ملی و نیز بردار حمله‌ای هستند که دشمنان می‌توانند از آن بهره بگیرند. درنتیجه، لازم است کشورها با بخش خصوصی خود همکاری داشته باشند تا با هم به تهدیدها رسیدگی کنند و به اهداف سایبری ملی نایل شوند.	تحلیل حضور برخط هر کشور برای یافتن شواهدی مبنی بر همکاری بخش دولتی و خصوصی با هدف افزایش دانش مهارت‌ها و تمرکز کلی کشور بر امنیت سایبری.	۲۰۲۰	بله/خیر
آیا شواهدی هست که نشان دهد کشور در تحقیقات سایبری سرمایه‌گذاری کرده یا به آن بودجه رسانده است؟	سرمایه‌گذاری در تحقیق و توسعه، بخش مهمی از افزایش قابلیت و ظرفیت فضای سایبری است.	تحلیل حضور برخط هر کشور برای یافتن شواهدی مبنی بر بودجه‌رسانی ملی برای تحقیقات امنیت سایبری یا بودجه‌رسانی کشور به دانشگاه‌های ملی و مؤسسات پژوهشی که برون‌داد امنیت سایبری دارند.	۲۰۲۰	بله/خیر
ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	کشورهایی که با راهبردهای گوناگونی در پی هدف بخصوصی بوده‌اند و تعهد خود برای نیل به آن هدف را نشان می‌دهند، احتمال اینکه درک پخته‌تری داشته باشند، بیشتر است.	مقایسهٔ اهداف برشمرده در جدیدترین راهبرد با اهداف برشمرده در راهبرد قبلی (اگر وجود داشته باشد).	۲۰۲۰	هدف حاضر در یک راهبرد: بله/خیر
در یک حملهٔ سایبری منسوب مشاهده‌شده است.	برخلاف شاخص‌های قصد، که قصد خاصی را (که نیازمند برنامه‌ریزی و تمایل قبلی است) نشان می‌دهند، از اقدامات یک کشور نیز می‌توان قصد کلی را (که از ارتکاب مفروض داشته می‌شود) از اقدامات یک کشور استنباط کرد.	استفاده از آمار و ارقام ردیابِ عملیات سایبری شورای روابط خارجی برای ارزیابی اینکه آیا یک یا چند حمله به کشور نسبت داده شده است یا نه.	۲۰۲۰	مشاهده‌شده در یک یا چند حمله: بله/خیر
اگر افزایش توانایی سایبری و فنی ملی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ راهبرد را بیاورید.	ن.ک: جدول نمرهٔ راهبرد	ن.ک: جدول نمرهٔ راهبرد	۲۰۲۰	ن.ک: جدول نمرهٔ راهبرد
اگر افزایش توانایی سایبری و فنی ملی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ مالی را بیاورید.	کشور به حد کافی تعهد دارد تا راهبردی ارائه دهد که از بودجهٔ ملی برای رسیدن به برون‌داد مدنظر خود استفاده کند.	کشور از زمان انتشار جدیدترین راهبرد خود، افزایش بودجهٔ سایبری را اعلام کرده است.	۲۰۲۰	بله/خیر

-هنجارها

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
کشور از سال ۲۰۱۲ تا ۲۰۱۶ چند بار از قطع‌نامه‌های سازمان ملل در زمینهٔ جی‌جی‌ای حمایت کرده است؟ از مجموعِ پنج بار.	نمرهٔ بالاتر در این شاخص نشان می‌دهد کشور تعهد دارد توصیه‌های جی‌جی‌ایِ سازمان ملل را بپذیرد و اقدامات رسمی‌تری در راستای شکل‌دهی هنجارهای بین‌المللی دربارهٔ فعالیت سایبری انجام دهد.	آمار و ارقام برگرفته از: https://cpi.ee/wp-content/uploads/-2017/12/2017Tikk-Kerttunen-Demise-of-theUN-GGE--17-12-2017ET.pdf	۲۰۱۷	۱ = پنج بار ۰/۸ = ۴ بار ۰/۶ = ۳ بار ۰/۴ = ۲ بار ۰/۲ = ۱ بار ۰ = هیچ‌گاه
کشور بین سال‌های ۲۰۱۵ و ۲۰۱۹ چند بار در انجمن راهبری اینترنت (آی‌جی‌اف) شرکت کرده است؟	انجمن راهبری اینترنت (آی‌جی‌اف) در تلاش است تا افراد را از گروه‌های ذی‌نفع گوناگونی در جایگاه هم‌تراز گرد هم آورد تا دربارهٔ مسائل خط‌مشی عمومی دربارهٔ اینترنت بحث کنند. با آنکه نتیجهٔ مذاکره‌شده‌ای وجود ندارد، آی‌جی‌اف بر سیاست‌گذاران بخش دولتی و خصوصی تأثیر می‌گذارد و به آن‌ها الهام می‌بخشد. در جلسات بحث سالانه، نمایندگان با یکدیگر بحث و تبادل اطلاعات می‌کنند و اقدامات مناسب را با هم در میان می‌گذارند. آی‌جی‌اف تسهیل‌کنندهٔ درک مشترک از نحوهٔ بیشینه‌سازی فرصت‌های اینترنت و رسیدگی به خطرات و مشکل‌های آن است.	اعداد و ارقام برگرفته از: https://www.intgovforum.org/multilingual/content/mag--2020members و https://www.intgovforum.org/multilingual/igf1-2020-st-mag-attendees	۲۰۲۰	۱ = پنج بار ۰/۸ = ۴ بار ۰/۶ = ۳ بار ۰/۴ = ۲ بار ۰/۲ = ۱ بار ۰ = هیچ‌گاه
آیا کشور در فعالیت‌های قابلیت‌سازِ انجمن جهانیِ تخصص سایبری (جی‌اف‌سی‌اف) شرکت کرده است؟	جی‌اف‌سی‌اف بیان می‌کند که مأموریتش تقویت «همکاری بین‌المللی در زمینهٔ قابلیت‌سازی سایبری از طریق پیوند نیازها، منابع و تخصص و نیز از طریق قراردادن دانش عملی در دسترس جامعهٔ جهانی» است. کشورهایی که مشارکت می‌کنند، نشان می‌دهند که مایل‌اند بهترین اقدامات و هنجارهای سایبری را در میان بگذارند.	اعداد و ارقام برگرفته از: https://thegfce.org/member-overview/	۲۰۲۰	بله/خیر

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
نرخ مشارکت در کمیتهٔ مشترک فنی ایزو/آی‌ای‌سی برای فناوری اطلاعات و ارتباطات چقدر است؟	سازمان بین‌المللی استانداردسازی (ایزو) و کمیسیون بین‌المللی الکتروتکنیک (آی‌ای‌سی) استانداردهای مشترک اجماع‌مبنایی برای فناوری‌های اطلاعات عرضه می‌کنند که برای بازار موضوعیت داشته باشند. شکل‌دهی کمیته‌های فنی مشترک ایزو/آی‌ای‌سی و پایبندی به آن نشان از تعهد به بهبود این عناصر در کشور خودشان دارد. امتیاز هرچه بالاتر باشد، کشور مربوط فعالیت بیشتری در استانداردسازی بین‌المللی دارد که برای سازگاری صنعت داخلی‌اش با بازارهای بین‌المللی مهم است.	https://www.iso.org/technical-committees.html	۲۰۲۰	تعداد کمیته‌های فنی مشترک ایزو/آی‌ای‌سی که فلان کشور عضو آن‌هاست، تقسیم بر ۲۲ (تعداد کل کمیته‌های فنی مشترک ایزو/آی‌ای‌سی). امتیازِ به‌دست‌آمده درصدی از کمیته‌های فنی است که کشور مدنظر در آن‌ها شرکت کرده است.
کیفیت مشارکت در تمام ۲۲ کمیتهٔ مشترک فنی ایزو/آی‌ای‌سی چقدر است؟	سازمان بین‌المللی استانداردسازی (ایزو) و کمیسیون بین‌المللی الکتروتکنیک (آی‌ای‌سی) استانداردهای مشترک اجماع‌مبنایی برای فناوری‌های اطلاعات عرضه می‌کنند که برای بازار موضوعیت داشته باشند. شکل‌دهی کمیته‌های فنی مشترک ایزو/آی‌ای‌سی و پایبندی به آن، نشان از تعهد به بهبود این عناصر در کشور خودشان دارد. امتیاز هرچه بالاتر باشد، کشور مربوط مرجعیت رسمی بیشتری در کمیته‌های فنی داشته است و صنعتش نقش بیشتری در شکل‌دهی استانداردهای بین‌المللی در دستورالعمل فناوری اطلاعات و ارتباطات دارد.	https://www.iso.org/technical-committees.html	۲۰۲۰	به هر کشور بر اساس نقشش در هر کمیتهٔ فنی، امتیازی داده شد. امتیاز به این شکل بود: ۱ = دبیر ۰٫۷۵ = مشارکت‌کننده ۰٫۵ = ناظر ۰٫۲۵ = عضو کمیسیون فنی مشترک ایزو/آی‌ای‌سی ۰ = بدون وابستگی. سپس میانگین مشارکت هر کشور در تمام کمیته‌ها اعمال شد تا امتیاز نهایی بین ۰ تا ۱ باشد.
کیفیت مشارکت کشور در گروه‌های مطالعاتی اتحادیهٔ بین‌المللی مخابرات چقدر است؟ گروه ۱۳ (شبکه‌های آینده)، گروه ۱۷ (امنیت) و «گروه ۲۰» (اینترنت اشیا و شهرهای هوشمند).	بدنهٔ بین‌المللی دیگری که دارای نمایندگی ملی برای تعیین استانداردهای فنی برای فناوری‌های اطلاعات است، اتحادیهٔ بین‌المللی مخابرات نام دارد. فرض ما این است که هرچه نمره بالاتر باشد، یعنی هرچه کیفیت مشارکت بیشتر باشد، کشور تأثیر بیشتری در تعیین استانداردها و هنجارهای بین‌المللی، به‌خصوص در فناوری اطلاعات و ارتباطات دارد (زیرا این مورد بیشتر متأثر از دولت است تا صنعت)			

شاخص	معنا	توضیح منبع	سال	روش نمره‌دهی
آیا کشور در مشق‌های دوجانبه یا چندجانبهٔ دفاع سایبری مشارکت کرده است؟	نشان می‌دهد که کشور مایل است تخصص و تلاش‌های قابلیت‌ساز خود را با دیگر کشورها در میان بگذارد.	جست‌وجوی اینترنتی وب‌سایت‌های دولتی و منابع معتبر برای ارجاعاتی به مشارکت در مشق‌های دوجانبه یا چندجانبهٔ دفاع سایبری	۲۰۲۰	بله/خیر
ثبات هدف: آیا در یک راهبرد پی گرفته می‌شود؟	کشورهایی که با راهبردهای گوناگونی در پی هدف بخصوصی بوده‌اند و تعهد خود را برای نیل به آن هدف نشان می‌دهند، احتمال اینکه درک پخته‌تری داشته باشند، بیشتر است.	مقایسهٔ اهداف برشمرده در جدیدترین راهبرد با اهداف برشمرده در راهبرد قبلی (اگر وجود داشته باشد).	۲۰۲۰	هدف حاضر در یک راهبرد: بله/خیر
اگر تعریف استانداردهای فنی و هنجارهای سایبری بین‌المللی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ راهبرد را بیاورید.	ن.ک: جدول نمرهٔ راهبرد	ن.ک: جدول نمرهٔ راهبرد	۲۰۲۰	ن.ک: جدول نمرهٔ راهبرد
اگر تعریف استانداردهای فنی و هنجارهای سایبری بین‌المللی در راهبرد سایبری ملی کشور به رسمیت شناخته می‌شود، نمرهٔ مالی را بیاورید.	کشور به حد کافی تعهد دارد تا راهبردی ارائه دهد که از بودجهٔ ملی برای رسیدن به برون‌داد مدنظر خود استفاده کند.	کشور از زمان انتشار جدیدترین راهبرد خود، افزایش بودجهٔ سایبری را اعلام کرده است.		بله/خیر

ضمیمهٔ ج: شرح تفصیلی شاخص‌های قابلیت

#	شاخص	معنا	منبع	سال	روش نمره‌دهی
۱	قوانین مرتبط با فعالیت های سایبری	سنجش اینکه کشور چقدر در اجرای قوانین محتوا و محرمانگی و جرایم سایبری فعال بوده است.	پروژهٔ قدرت سایبری‌بلفر	۲۰۲۰	۰ = بدون قانون ۱ = قوانینی که یکی از این موارد را پوشش می‌دهند (محتوا و محرمانگی و جرایم) ۲ = قوانینی که دو تا از این موارد را پوشش می‌دهند (محتوا و محرمانگی و جرایم) ۳ = قوانینی که محتوا و محرمانگی و جرایم را پوشش می‌دهند؛ اما منسوخ‌اند (پیش از سال ۲۰۰۰) ۴ = قوانینی که محتوا و محرمانگی و جرایم را پوشش می‌دهند و اخیراً روزآمد شده‌اند (پس از سال ۲۰۰۰)
۲	حملات سایبری با حمایت دولت	تعداد حملات سایبری پیچیده‌ای که به کشور منسوب شده‌اند	مرکز مطالعات راهبردی و بین‌المللی (سی‌اس آی‌اس)	۲۰۱۹ / ۲۰۱۸	شمار حملات سایبری منسوب به کنشگران تحت حمایت دولت
۳	توافق‌های سایبری دوجانبه	تعداد و کیفیت توافق‌های دوجانبهٔ رسمی یا غیررسمی‌ای که دولت ملی در فضای سایبری امضا کرده است. نمره بر اساس جدیدبودن.	پروژهٔ قدرت سایبری‌بلفر	۲۰۲۰	برای هریک از توافق‌های بین کشورها: ۱ = جلسه و بیانیه ۲ = بیانیهٔ مشترک و همکاری و چهارچوب ۳ = توافق/یادداشت تفاهم
۴	توافق‌های سایبری چندجانبه	تعداد و کیفیت توافق‌های چندجانبهٔ رسمی یا غیررسمی‌ای که دولت ملی در فضای سایبری امضا کرده است. نمره بر اساس جدیدبودن.	پروژهٔ قدرت سایبری‌بلفر	۲۰۲۰	برای هریک از توافق‌های بین کشورها: ۱ = غیررسمی/همایش/منطقه‌ای ۲ = غیررسمی/همایش/جهانی ۳ = توافق منطقه‌ای رسمی/عضو سازمان منطقه‌ای ۴ = توافق چندجانبهٔ رسمی/عضو سازمان جهانی

#	شاخص	معنا	منبع	سال	روش نمره‌دهی
۵	دکترین نظامی سایبری	راهبردهای سایبری حاوی جزئیات قابلیت‌های نظامی تهاجمی یا دفاعی در فضای سایبری	پروژهٔ قدرت سایبری بلفر	۲۰۲۰	۰ = بدون راهبرد نظامی سایبری ۱ = پیش‌نویس یک راهبرد نظامی سایبری ۲ = راهبرد نظامی سایبریِ احتمالاً منسوخ (پنج سال یا بیشتر) ۳ = راهبرد نظامی سایبری جدید (کمتر از پنج سال)/راهبرد نظامی احتمالاً منسوخ، اما پیوسته استفاده‌شده ۴ = راهبرد نظامی سایبری نهادینه‌شده و به‌روز (راهبرد کمتر از پنج سال، اما راهبرد نظامی سایبری پیوسته استفاده‌شده)
۶	صد شرکت برتر فناوری در جهان	تعدادی از شرکت‌های کشور که در میان صد شرکت برتر فناوری در جهان جا دارند	تامسون رویترز	۲۰۱۸	شمار شرکت‌های فناوری برتر برای هر کشور
۷	صادرات فناوری پیشرفته	درصد صادرات فناوری پیشرفته در میان مجموع صادرات	بانک جهانی	۲۰۱۸	مقادیر بالاتر نشان‌دهندهٔ صادرات فناورانهٔ بیشتر است
۸	سرمایهٔ انسانی	سنجش اینکه یافتن کارکنان ماهر در کشور چقدر آسان است	مجمع جهانی اقتصاد	۲۰۱۹	سنجش علاقه بر اساس این پرسش: «در کشورتان چقدر آسان است که شرکت‌ها کارمندانی با مهارت‌های متناسب با نیازهای کسب‌وکار بیابند؟» (۱ = بسیار دشوار؛ ۷ = بسیار آسان). این سنجه سپس به مقیاس ۰ تا ۱۰۰ مقیاس‌بندی شده است که در آن، مقادیر بالا نشانهٔ دردسترس‌بودن کارکنان ماهر است
۹	تأمین نیروی ارتش سایبری	تعداد افرادی که کادری نیروهای سایبریِ ارتش هستند	پروژهٔ قدرت سایبری بلفر	۲۰۲۰	تعداد افراد گزارش‌شده در منابع باز که در نیروهای سایبری کار می‌کنند

#	شاخص	معنا	منبع	سال	روش نمره‌دهی
۱۰	فرماندهی سایبری مرکزی	وجود و سن فرماندهی سایبری ملی	پروژهٔ قدرت سایبری بلفر	۲۰۱۴ تا ۲۰۲۰	۰ = بدون فرماندهی سایبری ۱ = نقشه برای تأسیس فرماندهی سایبری ۲ = فرماندهی سایبری جدید (کمتر از دو سال) ۳ = فرماندهی سایبری نهادینه‌شده (دو تا پنج سال) ۴ = فرماندهی سایبری نهادینه‌شده (بیش از پنج سال)
۱۱	شرکت‌های برتر در زمینهٔ امنیت سایبری	تعدادی از شرکت‌های برتر امنیت سایبری در سطح جهان که مقرشان در کشور مدنظر است	طرح‌های اجتماع سایبری	۲۰۱۹	تعدادی از ۱۵۰ شرکت برتر امنیت سایبری که در رده‌بندی برشمرده شده‌اند
۱۲	آلودگی رایانه‌ای	درصدی از رایانه‌های کشور که به بدافزار آلوده شده‌اند	کمپاریتِک	Q۳ ۲۰۱۹	درصد کاربرانی که در این دوره به آنان حمله شده است (دسترسی غیرمجاز، تخریب، اختلال)
۱۳	آلودگی موبایل	درصدی از موبایل‌های کشور که به بدافزار آلوده شده‌اند	کمپاریتِک	Q۳ ۲۰۱۹	درصد کاربرانی که در این دوره به آنان حمله شده است (دسترسی غیرمجاز، تخریب، اختلال)
۱۴	کاربران شبکه‌های اجتماعی	درصد حساب‌های فعال در شبکه‌های اجتماعی	استاتیستا	۲۰۲۰	درصد کاربران اینترنتی که سایت‌های شبکه‌های اجتماعی را می‌بینند
۱۵	کاربران اینترنت	نرخ نفوذ اینترنت در هر کشور	بانک جهانی	۲۰۱۷ تا ۲۰۱۸	هرچه بیشتر باشد، افراد بیشتری از اینترنت استفاده می‌کنند
۱۶	فناوری رصد	تعداد شرکت‌های رصد بخش خصوصی که مقرشان در کشور است	پرایوسی اینترنشنال	۲۰۱۶	تعداد شرکت‌های رصدی که درون یک کشور فعالیت دارند

#	شاخص	معنا	منبع	سال	روش نمره‌دهی
۱۷	سایت‌های برتر	تعدادی از پنجاه وب‌سایت برتر الکسا که به سازمان‌های درون یک کشور تعلق دارند	الکسا	۲۰۱۹	تعداد سایت‌ها در میان پنجاه وب‌سایت برتر
۱۸	سایت های خبری برتر	تعدادی از سایت‌های خبری در میان پنجاه وب‌سایت برتر الکسا که به سازمان‌های درون یک کشور تعلق دارند	الکسا	۲۰۱۹	تعداد سایت‌ها در میان پنجاه وب‌سایت برتر
۱۹	درخواست های حذف محتوا	تعداد درخواست‌های حذف محتوا از گوگل که نهادی دولتی خواسته است	گوگل	۲۰۱۸ تا ۲۰۱۹	تعداد درخواست‌ها
۲۰	آزادی در اینترنت	نمرهٔ خانهٔ آزادی برای اینکه شهروندان در فضای اینترنت چقدر آزادند	خانهٔ آزادی و آزادی جهان	۲۰۱۹	۰ تا ۱۰۰: سه امتیاز جداگانه که تجمیع می‌شوند: الف. موانع دسترسی ب. محدودیت محتوا ج. تخطی از حقوق کاربران برای هفت کشور، از رده‌بندی‌های آزادی جهان استفاده کردیم؛ زیرا خانهٔ آزادی اطلاعات نداشت
۲۱	درخواست ثبت امتیاز	تعداد درخواست‌های ثبت امتیاز داخلی از سوی شهروندان یک کشور	شاخص‌های توسعهٔ جهانی	۲۰۱۸	تعداد درخواست‌های ثبت امتیاز داخلی (فقط شهروندان). سنجهٔ سرانه.
۲۲	سرعت پهن‌باند	سنجش سرعت پهن‌باند در ارتباط با سریع‌ترین نرخ‌های پهن‌باند در جهان	نمایهٔ جهانی تست سرعت	مارس ۲۰۲۰	۱۰ از ۱۰ سنگاپور است که بالاترین سرعت پهن‌باند را در جهان دارد
۲۳	سرعت موبایل	سنجش سرعت موبایل در ارتباط با سریع‌ترین نرخ‌های موبایل در جهان	نمایهٔ جهانی تست سرعت	مارس ۲۰۲۰	۱۰ از ۱۰ امارات است که بالاترین سرعت موبایل را در جهان دارد

#	شاخص	معنا	منبع	سال	روش نمره‌دهی
۲۴	تجارت الکترونیک	سهم فروش تجارت الکترونیکی ملی از تولید ناخالص داخلی	UNCTAD	۲۰۱۷ و ۲۰۲۰	هرچه بیشتر باشد، فروش تجارت الکترونیکی بیشتر است
۲۵	گروه پاسخ‌گویی حوادث رایانه‌ای (سی‌اس آی‌آرتی)	وجود یک گروه پاسخ‌گویی حوادث امنیت سایبری	پروژهٔ قدرت سایبری بلفر	۲۰۲۰	۰ = بدون گروه پاسخ‌گویی ۱ = قصد تأسیس سی‌اس‌آی‌آرتی ۲ = گروه سی‌اس‌آی‌آرتی ملی جدی (پنج سال یا کمتر) ۳ = گروه سی‌اس‌آی‌آرتی ملی نهادینه‌شده (بیش از پنج سال) ۴ = گروه سی‌اس‌آی‌آرتی ملی نهادینه‌شده (بیش از پنج سال) + عضویت در نخستین گروه پاسخ‌گویی
۲۶	آسیب پذیری‌ها	درصد انبوهشی آسیب‌پذیری‌هایی که در پایگاه دادهٔ Shodan برای زیرساخت یک کشور برشمرده شده است	پروژهٔ قدرت سایبری بلفر	۲۰۲۰	درصد انبوهشی نتایج جست‌وجوی Shodan
۲۷	قدرت نرم جهانی	نمرات کشور در نمایهٔ قدرت نرم جهانی	برندفایننس	۲۰۱۹	امتیازات محاسبه‌شده از سوی برند فایننس، بخشی از نمایهٔ قدرت نرم‌شان بود. همین امتیازات برای نمایهٔ قدرت سایبری بلفر استفاده شدند

داده‌های گردآوری‌شده دربارهٔ قابلیت‌ها را می‌توان به هشت مضمون دسته‌بندی کرد:

۱. شواهد مبنی بر حمله؛
۲. محتوای برخط ملی؛
۳. ساختارهای سایبری داخلی دولت؛
۴. کاهش آسیب‌پذیری سایبری؛
۵. بخش خصوصی و تجارت و نوآوری؛
۶. ارتباط‌پذیری؛
۷. نیروی کار؛
۸. چهارچوب‌های حقوقی و خط‌مشی.

شواهد مبنی بر حمله

شاخص‌های استفاده‌شده:

- ردیاب عملیات سایبری شورای روابط خارجی

سابقهٔ یک کشور در انجام عملیات سایبری، یکی از معیارهای کلیدی برای قابلیت است. هرجا کشوری حمله‌ای سایبری را برای یکی از هفت هدف انجام داده است، مشخصاً در آن عرصه قابلیت دارد. اما عملیات‌های شناخته‌شده تمام ماجرا نیستند؛ زیرا تمام کشورها قابلیت خود را نشان نمی‌دهند و حتی آن‌ها هم که چنین می‌کنند، ممکن است طیفِ کامل قابلیت‌های خود را به نمایش نگذارند که هم به‌لحاظ راهبردی منطقی است و هم اغلب نیازی به این کار نیست. برای این شاخص، بر اساس هدف‌های گوناگون، عملیات سایبری نسبت‌داده‌شده را تحلیل کردیم که در ردیاب عملیات سایبری شورای روابط خارجی آمده‌اند. داده‌های شورای روابط خارجی از پایگاه‌های دادهٔ پیشین دربارهٔ حملات سایبریِ تحت حمایت دولت[1] و نیز جمع‌آوری دادهٔ درون‌سازمانی دربارهٔ موارد جدیدترِ گزارش‌شده در رسانه‌ها و بیانیه‌های دولت برگرفته شده است. این شاخص نشان‌دهندهٔ قصد یک کشور هم است، چنان‌که در بخش ۳ توضیح داده شد.

محتوای برخط ملی

شاخص‌های استفاده‌شده:

- وب‌سایت‌های برتر فهرست‌شده در الکسا؛
- وب‌سایت‌های خبری برتر فهرست‌شده در الکسا؛

1 همچون صفحهٔ گستردهٔ گروه‌ها و عملیات ای‌پی‌تی، فلوریان راث، فهرست سی‌اس‌آی‌اس از رویدادهای مهم سایبری و رخدادنگاشت حملات سایبری هدفمند کسپرسکی‌لب.

- درخواست‌های حذف محتوا از گوگل؛
- نمرهٔ آزادی در اینترنت

توانایی یک کشور برای ایجاد و کنترل محتوای برخط، به چند هدف ملی مربوط است. کشور می‌تواند از طریق تولید محتوای برخط، تأثیر بهتری بر شهروندان خود و شهروندان دیگر کشورها بگذارد. همچنین، کشور هرچه کنترل بیشتری بر محتوای برخط داشته باشد (موضوعی که می‌توانیم از طریق تحلیل درخواست‌های موفقِ یک کشور برای حذف محتوا از گوگل، آن را بسنجیم)، بیشتر سعی در کنترل محیط اطلاعاتی خود دارد.

این شاخص محدودیت‌هایی دارد. اطلاعات مربوط به بهترین وب‌سایت‌ها و وب‌سایت‌های خبری، سانسور را لحاظ نمی‌کنند. بعضی وب‌سایت‌ها، به‌رغم رتبهٔ بالای جهانی، در بعضی کشورها کاملاً مسدودند. استفادهٔ ما از حذف محتوای گوگل، دیگر موتورهای جست‌وجو را لحاظ نمی‌کند.[1] علاوه بر این، آزادی عمومی (استفاده‌شده در رده‌بندی دیگری دربارهٔ آزادی در اینترنت) با آزادی اینترنتی یکسان نیست. آزادی اینترنتی، در مواردی به‌عنوان جایگزین استفاده شد که رده‌بندی آزادی در اینترنت نمره‌ای برای یکی از سی کشورِ مدنظرِ ان‌سی‌پی‌آی نداشت.

ساختارهای سایبری داخلی دولت

شاخص‌های استفاده‌شده:

- وجود فرماندهی سایبری ملی؛

1. بر اساس اسنت‌کانتر گلوبال‌استتس، از مي ۲۰۱۹ تا مي ۲۰۲۰، سهم بازار موتورهای جست‌وجو در سطح جهان به این شرح بود: گوگل (۹۲٫۰۶درصد)، بینگ (۲٫۶۱درصد)، بایدو (۱٫۱۶درصد)، یاندکس (۰٫۵۶درصد) و یاندکس آریو (۰٫۵۲درصد).

- وجود گروه پاسخ‌گویی حوادث امنیتی رایانه‌ای (سی‌اس‌آی‌آرتی).

ساختارهای داخلی به کشورها امکان هماهنگی و مهار منابع داخلی برای دستیابی به اهداف ملی را می‌دهد.

فرماندهی‌های سایبریِ مرکزیْ کار هماهنگی و مهار چند قابلیت سایبری را در داخل کشور تسهیل می‌کنند. این هماهنگی مرکزی حامی به‌کارگیری شیوه‌های سایبری در هنگام نیاز است. این شاخص، بر اساس منابع دولتی و ارزیابی متخصصان، تعداد سال‌هایی را ارزیابی می‌کند که فرماندهی سایبری وجود داشته است؛ اما سوابق این واحدها را بررسی نمی‌کند.

همچنین، کشورهایی که سی‌اس‌آی‌آرتی ملی دارند، روی کاغذ بهتر می‌توانند به حوادث سایبری بزرگ‌مقیاس و هماهنگ واکنش نشان دهند. علاوه بر این، هماهنگی بین‌المللی میان گروه‌های پاسخ‌گویی، باعث افزایش توانایی واکنش به تهدیدهای سایبری می‌شود و این همکاری بین‌المللی در نمره‌دهی انعکاس می‌یابد.

کاهش آسیب‌پذیری سایبری

شاخص‌های استفاده‌شده:

- درصد نرخ آلودگی رایانه‌ای؛
- درصد نرخ آلودگی موبایل؛
- آسیب‌پذیری‌های فهرست‌شده در Shodan که بر دستگاه‌های داخلی تأثیر می‌گذارند.

نرخ آلودگی رایانه‌ای و موبایل و آسیب‌پذیری‌های شناخته‌شده در دستگاه‌های داخلی، شاخصی‌اند برای میزان رسیدگی نظام‌مند یک کشور

به آسیب‌پذیری‌های سایبری که در آسیب‌پذیری کلی زیرساخت‌های دیجیتال یک کشور نقش دارد. نرخ بالای آلودگی ارتباطی منفی با قدرت سایبری کشور دارد.

برای کرهٔ شمالی و نیوزیلند، داده‌ای برای نرخ آلودگی رایانه‌ای و موبایل در دسترس نیست. تصور را بر این گذاشتیم که نرخ آلودگی کرهٔ شمالی صفر درصد است؛ زیرا دسترسی به اینترنت در سراسر کشور بسیار ضعیف است. برای نیوزیلند، از همان نمرهٔ استرالیا استفاده کردیم؛ زیرا هر دو کشورهایی با فناوری پیشرفته‌اند و دسترسی‌شان به اینترنت در یک حد است. برای اسرائیل، فقط مقدار نرخ آلودگی موبایل را داریم. ازآنجاکه این دو مقدار ارتباط تنگاتنگی دارند، برای نرخ آلودگی رایانه‌ای نیز همان رقم را در نظر گرفتیم.

این شاخص‌ها فقط یک وجه از امنیت سایبری را پوشش می‌دهند و فقط نمونه‌ای از آلودگی‌ها و آسیب‌پذیری‌های رایانه‌ای هستند.

بخش خصوصی، تجارت و نوآوری

شاخص‌های استفاده‌شده:

- بازار فعال تجارت الکترونیک؛
- وجود شرکت‌های رصد بخش خصوصی؛
- تعدادی از ۱۵۰ شرکت برتر امنیت سایبری در جهان که مقرشان در کشور است؛
- سهم صادرات فناوری پیشرفته از کل صادرات؛
- تعدادی از صد شرکت برتر فناوری در جهان که مقرشان در کشور است؛
- تعداد درخواست‌های ثبت امتیاز؛

بازار فعال تجارت الکترونیک نشان می‌دهد که کشور به‌صورت فعال در پی راهبردهایی برای ترویج کسب‌وکارهای برخط است. با آنکه ما این شاخص را دارای ارتباط مثبتی با قدرت سایبری می‌دانیم، فعالیت زیاد در تجارت الکترونیک کشور را در خطر فعالیت‌های بالقوهٔ اختلال‌آفرین نیز قرار می‌دهد.

تعداد شرکت‌های خصوصیِ امنیت سایبری در کشوری بخصوص، بسته به نوع شرکت، به قدرت سایبری کشور بهره می‌رساند. سازمان‌هایی که قابلیت‌های دفاعی بهتر فراهم می‌کنند، می‌توانند به تقویت دفاع دولت کمک کنند؛ حال آنکه سازمان‌های رصد می‌توانند ابزار بهتری برای اعمال قانون داخلی در اختیار دولت‌ها قرار دهند.

صادرات محصولات تولیدی نشان می‌دهد که قابلیت صنعتِ سایبری کشور چقدر توسعه‌یافته است و کشور الف تا چه حد می‌تواند با صادرات فناوری و استانداردهای خود بر محیط الکترونیکی کشور ب تأثیر بگذارد. البته این شاخص نقص‌هایی دارد؛ زیرا فقط محدود به فناوری اطلاعات و ارتباطات نیست و به‌دلیل پیچیدگی زنجیره‌های تأمین، نشان نمی‌دهد مالکیت فکری از کجا می‌آید.

تعداد شرکت‌های برتر فناوری که در یک کشور فعالیت دارند، نشان می‌دهد کشور چه میزان نیروی کار و دانش لازم برای نوآوری دارد. پروژه، در قالب نیابت، شامل داده‌هایی بود مبنی بر اینکه چه تعداد از صد شرکت برتر فناوری و امنیت سایبری در جهان در هر کشور فعالیت دارند.

ما تعداد درخواست ثبت امتیاز به‌ازای هر شهروند را سنجه‌ای برای نوآوری در نظر گرفتیم. تعداد بالای درخواست‌های ثبت امتیاز نشان می‌دهد که کشور در تحقیق و توسعه، که لازمهٔ پیشبرد امنیت سایبری و

فناوری است، سرمایه‌گذاری کرده است.[1]

کوشیدیم داده‌هایی گردآوری کنیم تا نشان دهیم هر دولت چقدر منابع مالی به توسعهٔ قابلیت‌های سایبری تخصیص می‌دهد. برای بعضی کشورها، ارقام علنی بودند و برای برخی دیگر، بعضی ارقام با ایجاد سازمانی جدید یا بودجهٔ سرمایه‌گذاری برای تحقیق یا همکاری با صنعت برای امنیت سایبری مرتبط بود. درمجموع، داده‌هایی تطبیقی که با آن‌ها بتوان سرمایه‌گذاری سایبری را در کشورهای مختلف ارزیابی کرد، کار دشواری بود. گسترهٔ فعالیت سایبری به نهاد دولتی واحدی محدود نمی‌شود و عناصر قدرت سایبری، همچون گردآوری اطلاعات وسط یک آژانس اطلاعاتی یا هزینه‌های نظامی، حتی در کشورهایی هم که شفافیت بالایی دارند، بنا به دغدغه‌های امنیت ملی در دسترس عموم نیست.

ارتباط‌پذیری

شاخص‌های استفاده‌شده:

- درصدی از کاربران اینترنت که از شبکه‌های اجتماعی استفاده می‌کنند؛
- درصدی از افراد که از اینترنت استفاده می‌کنند؛
- سرعت اینترنت پهن‌باند و اینترنت موبایل؛
- استفاده از شبکه‌های اجتماعی و اینترنت درون یک کشور نشان می‌دهد که سطح حملهٔ یک کشور چقدر بزرگ یا کوچک است؛ یعنی هم میزان ارتباط‌پذیری را نشان می‌دهد و هم آسیب‌پذیری

1 خود نظام‌های ثبت امتیاز تغییرات مهمی را تجربه کرده‌اند که منجر به افزایش ثبت امتیاز شده است. ن.ک:
.http://www.oecd.org/science/inno/24508541.pdf

بالقوهٔ مردم در برابر عملیات تأثیرگذاری از سوی کنشگران معاند.

ما سرعت [اینترنت] پهن‌باند و [اینترنت] موبایل را نیز به‌عنوان نمایانگرِ دیگری برای ارتباط‌پذیری خوب در نظر گرفتیم، که می‌تواند بر چند قابلیت و هدف تأثیر بگذارد. این شاخص‌ها نشان می‌دهند که هرچه سرعت اینترنت و موبایل بیشتر باشد، اقتصاد ملی توسعه‌یافته‌تر و دیجیتال‌تر و نوآورانه‌تر است. درعین‌حال، به این نکته نیز واقفیم که زیرساخت دیجیتالی که امنیت سایبری آن کم باشد، کشور را در معرض آسیب‌های مهمی قرار می‌دهد. علاوه بر این، شاخص سرعت پهن‌باند و موبایل با مشکل دیگری نیز روبه‌روست: داده‌ها فقط از طریق کاربرانی گردآوری شد که تصمیم گرفته بودند سرعت پهن‌باند یا موبایلشان را از طریق برنامک نمایهٔ جهانیِ آزمایش سرعت «بیازمایند».[1]

نیروی کار

شاخص‌های استفاده‌شده:

- سرمایهٔ انسانی/کارکنان ماهر؛
- کارمندان نظامی سایبری.

قابلیت امنیت سایبری یک کشور بسته به این است که تا چه حد به کارکنان بسیار ماهر دسترسی داشته باشد. دفاع سایبری مستلزم انواعی از مهارت‌هاست؛ از برنامه‌نویسی و کدنویسی فنی گرفته تا تحلیل و مدیریت پروژه و پژوهش.

نخستین معیار، مبتنی بر سنجهٔ سرمایهٔ انسانی از مجمع اقتصادی

1 نکته: به‌دلیل تأثیرات جهانی ویروس جدید کرونا، مارس ۲۰۲۰ شاید بهترین نمونه نباشد. ن.ک: مقالهٔ آزمایش سرعت در:
"Tracking COVID-19's Impact on Global Internet Performance". Updated May 4, 2020.
https://www.speedtest.net/insights/blog/tracking-covid-19-impact-global-internet-performance/#/

جهانی است. منظور از آن، دردسترس‌بودن کارکنان بسیار ماهری است که می‌توانند در صنعت سایبری کشور (هم بخش دولتی و هم خصوصی) کار کنند و به قابلیت کشور بهره‌ای برسانند. ضعف این شاخص آن است که صرفاً مهارت‌های مرتبط با امنیت سایبری را نمی‌سنجد.

معیار دوم، شاخص قابلیت نظامی سایبری یک کشور است. قابلیت تهاجمی و دفاعی بسیاری از کشورها در نیروهای نظامی آن‌ها بروز پیدا می‌کند. این شاخص، شمار مطلق افراد شاغل در سمت‌های سایبری ارتش درون هر کشور را گزارش می‌دهد. داده‌ها از جست‌وجوی درون‌سازمانیِ اطلاعاتِ در دسترسِ عموم و گزارش‌های رسانه‌ها و ارزیابی‌های آکادمیک گردآوری شده‌اند. تعیین دقیق ارقام دشوار بود و اطمینان کلی ما به دقت آن، کم است. مشکل این شاخص Mآن است که مشخص نیست آیا کشور کارکنانی را که در شمارش دیگر آژانس‌ها لحاظ شده‌اند، در ارتش خود نیز می‌شمارد یا نه. این ضعف با دغدغه‌های مربوط به امنیت ملی بدتر هم می‌شود؛ زیرا این دغدغه از شفافیت دربارهٔ شمار کارکنان ارتش می‌کاهد.

چهارچوب‌های حقوقی و خط‌مشی داخلی و بین‌المللی

شاخص‌های استفاده‌شده:

- توافق‌های چندجانبه و دوجانبه؛
- قانون‌گذاری داخلی (یعنی ارتباط محتوای برخط و محرمانگی و امنیت سایبری)؛
- نمایهٔ قدرت نرم جهانی؛
- دکترین نظامی سایبری.

هنجارهای بین‌المللی ثابت نیستند و به‌مرور، بسته به تغییرات فرهنگی و اجتماعی و سیاسی اصلاح می‌شوند؛[1] با گسترش فضای سایبری، مقررات و قواعد و هنجارهای مربوط به روش فعالیت‌های کشورها و کسب‌وکارها و افراد در آن نیز زیاد شده است. طی قرن‌ها (چنان‌که در راهبردهای سایبری ملی آمده است) کارکردن با دیگران برای مواجهه با معضلاتی همچون جرایم سایبری و نیز رسیدن به توافق برای تعیین رفتار مقبول در حوزهٔ سایبری، همواره یک اولویت بوده است.[2] ما در پی این بودیم تا با سنجش روش اعلام بیانیه‌های رسمی و غیررسمی مبنی بر قصد همکاری بین‌المللی، به‌صورت کمّی نشان دهیم یک کشور در پیگیری همکاری بین‌المللی چقدر فعال بوده است. برای این شاخص، از داده‌هایی استفاده کردیم که نهاد سازمان ملل متحد برای پژوهش خلع سلاح گردآوری و در پرتال خط‌مشی سایبری خود منتشر کرده بود.

به هر توافق، بسته به اینکه بیانیهٔ غیررسمیِ همکاری بود یا توافق رسمی دوجانبه یا توافق چندجانبه، نمره‌ای عددی دادیم. بیشترین وزن را به توافق‌های رسمی دادیم؛ به‌طوری‌که توافق‌های چندجانبه بیشترین نمره را دریافت کردند. یکی از ضعف‌های این شاخص آن است که قصد همکاری را می‌سنجد، نه تحقق یک تعهد و مقیاس و بسامد آن را. مشکل دیگر مربوط به هم‌سازی میان دولت‌هاست که میزان توافق میان کشورها چه معیارهایی باید داشته باشد.

توانایی یک کشور برای تأثیرگذاری بر دیگر شهروندان و دولت‌ها و به‌تبع، بهره‌رسانی به هنجارسازی جهانی در گرو چندین مؤلفه است؛

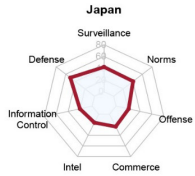
1 Ann Florini. 1996. 'The Evolution of International Norms'. International Studies Quarterly. Vol 40, No.3. pp 363-389).

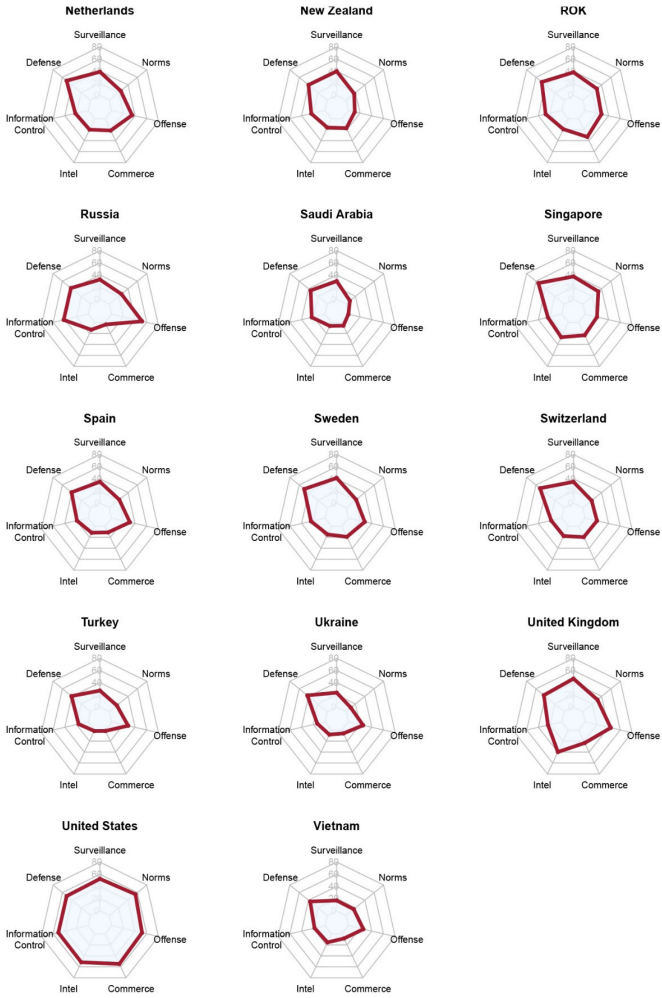
2 چنان‌که دربارهٔ قانون بین‌الملل در حوزه‌های سنتی نیز رقم خورده است.

ازجمله چهارچوب‌های حقوقی داخلی و فعالیت در مجمع‌های چندجانبه و درک دیگر کشورها از آن.

سرانجام، کشوری که در پی توسعهٔ قابلیت نظامی سایبری خود برای انجام عملیات تهاجمی است، احتمالاً به دکترین یا راهبرد نظامی نیاز دارد. این سنجه مبتنی بر انتشار راهبرد رسمی نظامی دولت و ارزیابی کارشناسان است. اگر دکترین مدنظر چند نسخه داشته باشد، ارزیابی ما این بود که هماهنگی میان دولت‌ها و درنتیجه قابلیت، بهتر و جاافتاده‌تر خواهد بود.

ضمیمهٔ د: نمودارهای راداریِ تمام قابلیت‌ها به تقسیم کشور





کلید:

- تجاری: افزایش توانایی سایبری و فنی ملی؛
- دفاع: تقویت و ارتقای دفاع سایبری ملی؛
- اطلاعات: جمع‌آوری اطلاعات W2. نمایهٔ قدرت سایبری ملی ۲۰۲۰

چنان‌که در شکل ۱ مشخص است، ده کشور جامعِ برتر با بالاترین میزان قصد و قابلیت در تمام اهداف هفت‌گانه به شرحِ زیرند. شکل ۲ رتبه‌بندی را بر اساس اهداف تقسیم می‌کند.

۱. ایالات متحده؛
۲. چین؛
۳. بریتانیا؛
۴. روسیه؛
۵. هلند؛
۶. فرانسه؛
۷. آلمان؛
۸. کانادا؛
۹. ژاپن؛
۱۰. استرالیا.

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

حوزهٔ فضای مجازی به اندازهٔ انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانهٔ پر از آب خروشان است که می‌آید و دائماً هم بر آب آن افزوده و خروشان‌تر می‌شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه‌کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می‌شود فرصت؛ اگر رهایش کنیم و برنامه‌ای برای آن نداشته باشیم، می‌شود یک تهدید...

csri.majazi.ir