مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

عصر فضای مجازی
صدوبیست وشش

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

به روزرسانی نمایه قدرت سایبری ملی؛ ۲۰۲۲

مرکز بلفر؛ دانشگاه هاروارد، کالج کندی

National Cyber Power Index - 2022 Update

عصر فضای مجازی

شماره ۱۲۶
مرداد ۱۴۰۲

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

به‌روزرسانی نمایه قدرت سایبری ملی؛ ۲۰۲۲

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 شفیعی‌نسب

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: ۰۲۱-۲۲۰۷۳۰۳۱
کد پستی: ۱۹۹۷۹۸۷۶۲۹

فهرست

سخن نخست یک

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، نشانه مهم و آشکاری بر این مُدعاست 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 مُتفطن 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 گرداند.

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

چکیده مدیریتی

چکیده مدیریتی

در سال ۲۰۲۰ که برای اولین بار تعریفِ قدرت سایبری را مطرح و «نمایهٔ قدرت سایبری ملی» را منتشر کردیم، در وابستگی دولت‌ها به اینترنت و فناوری‌های دیجیتال برای دستیابی به اهداف ملی تردیدی نبود؛ اما این موضوع به‌طور دقیق حلاجی نشده بود. رابطهٔ این مبحث با قدرت ملی نیز به‌درستی درک نشده بود. مفهوم رایج قدرت سایبری در سطح دولت، پاره‌پاره و مناقشه‌برانگیز بود و عمدتاً بر قابلیت‌های مخرب و فقط بر چند کشور تمرکز داشت. درعین‌حال، همه‌گیری کرونا خطرات سایبریِ پیش روی دولت‌ها، زیرساخت‌ها، کسب‌وکارها و نیروی کار دورکاری‌شده را تشدید کرد.

تعریف همه‌جانبهٔ ما از قدرت سایبری و نمایهٔ همراه با آن، به مباحثهٔ جهانی در این زمینه بهره رساند و نقشهٔ شروع و ساختاری برای بررسی‌های آینده فراهم کرد؛ آن هم بر اساس دسته‌بندی کلی‌ترِ این‌گونه: چه‌کسی قدرت سایبری دارد و از راه سایبری در پی دستیابی به چه اهداف ملی‌ای است؟ نخستین نمایهٔ قدرت سایبری ملی در سال ۲۰۲۰، وسعت گفت‌وگو را از پنج کشور به سی کشور و از یک یا دو هدف، به هشت هدف رساند. مباحثات مربوط به قدرت سایبری بر بعضی دولت‌ها تأثیر گذاشته تا رویکردی سنجیده‌تر در قبال ارزیابی قابلیت‌های سایبری خود پیش بگیرند و بررسی عمیق‌تری از وسعت و کاربرد قدرت سایبری را

برانگیخته است.

می‌خواهیم اهمیت درک همه‌جانبهٔ قدرت سایبری را نشان دهیم و روشن کنیم که تأثیرات آن فراتر از دغدغه‌های دم‌دستی امنیت ملی است، که بسیج‌کردنش نیازمندِ رویکردی تمام‌کشوری است. همچنین بگوییم قابلیت‌های سایبری فقط یکی از ابزارهای موجود در جعبهٔ ابزار حکومت‌هاست. این تعریف کلی‌تر، همچون منشوری است که از طریق آن، دولت‌های سراسر دنیا منابع خود را در راستای نیل به اهداف ملی سودهی می‌کنند و زیربنای مشارکت بین‌المللی را نیز باید از طریق آن درک کرد و سروشکل داد. درک تکاملِ دولت‌ها و قدرت سایبری‌شان نقشی بنیادین در آیندهٔ سیاست‌گذاران و ژئوپلیتیک خواهد داشت. گروه «نمایهٔ قدرت سایبری ملی»، همچنان قدرت سایبری را، هم‌زمان با تکامل آن، بازنگری خواهد کرد و خواهد سنجید.

۱. مقدمه

۱. مقدمه

از پاییز ۲۰۲۰ که نخستین نمایهٔ قدرت سایبری ملی (ان‌سی‌پی‌آی)[1] را منتشر کردیم، بحث دربارهٔ قدرت سایبری (ازجمله گستره و کاربرد آن) بی‌وقفه ادامه یافته است. اهمیت این مبحث انکارناپذیر است. دولت‌های سراسر دنیا، توسعهٔ قابلیت‌های چندوجهی و انتشار راهبردهای سایبری جدید را در اولویت قرار داده‌اند؛ زیرا می‌خواهند نشان دهند در سطح بین‌المللی و ملی و محلی، چگونه قصد دارند قابلیت‌های داخلی خود را بسیج کنند و قدرت سایبری خود را توسعه دهند تا به هشت هدفی که دو سال پیش بررسی کردیم دست یابند.

طی دو سال اخیر که دولت‌ها در حال توسعهٔ خط‌مشی‌های همه‌جانبه و به‌کارگیری قدرت سایبری بوده‌اند، شاهد تعداد زیادی حملات سایبری چشمگیر بوده‌ایم؛ ازجمله سولار ویندز،[2] مایکروسافت اکسچنج،[3] کلونیال پایپ‌لاین[4] و جی‌بی‌اس[5]. به‌تازگی نیز حملات سایبری به‌عنوان یکی از چندین ابزار در حملهٔ روسیه به اوکراین استفاده شده‌اند. در دو سال گذشته، نه‌تنها تعداد حملات باج‌افزاری وسیع افزایش یافته است، بلکه شاهد افزایش استفاده از زنجیره‌های تأمین دیجیتال به‌عنوان بردارِ[6]

1 National Cyber Power Index (NCPI)
2 Solar Winds
3 Microsoft Exchange
4 Colonial Pipeline
5 JBS S.A.
6 در مباحث امنیت سایبری، بُردارِ حمله مسیری است که هکر از طریق آن به حفره‌های امنیت سایبری نفوذ می‌کند.

حملات سایبری بوده‌ایم. هرچه اتصال و یکپارچگی ما افزایش یابد، حملات سایبری برای بزهکاران و دولت‌ها جذاب‌تر خواهد بود. دولت‌ها باید قدرت سایبری خود را ارتقا دهند تا از منافع خود حفاظت کنند.

به‌منظور درک بهتر اقدامات دولت‌ها و قدرت ملیِ امروزی، بد نیست قدرت سایبری را متشکل از هشت هدف بدانیم که دولت‌ها از طریق فضای سایبری در پی نیل به آن‌ها هستند. دولت‌ها به‌جز تخریب و غیرفعال‌سازیِ زیرساخت‌ها و قابلیت‌های دشمن (تعریفی سنتی، اما محدود و گمراه‌کننده از قدرت سایبری)، درصدد تقویت و ارتقای دفاع سایبری ملی، جمع‌آوری اطلاعات در کشورهای دیگر، افزایش توانایی سایبری و فناوری تجاری ملی، کنترل و دست‌کاری محیط اطلاعاتی و گسترش نفوذ خود از طریق تعریف هنجارهای سایبری و استانداردهای فنی بین‌المللی نیز هستند. قدرت سایبری را باید در بستر اهداف ملی یک کشور لحاظ کرد. دولت‌ها نیز باید هنگام تلاش برای بسیج‌کردن آن، رویکردی تمام‌کشوری پیش بگیرند و البته روزبه‌روز هم بیشتر به این نوع رویکرد می‌گروند.

نمایهٔ سال ۲۰۲۲، با استفاده از شاخص‌هایی که توأمان دربرگیرندهٔ قصد و قابلیت هستند، سنجش تازه‌ای از قدرت سایبری ۳۰ کشور ارائه می‌دهد. ما برای سنجش قابلیت از ۲۹ شاخص قابلیت در زمینهٔ هشت هدف استفاده کرده‌ایم و راهبردهای ملی تمام کشورهای مدنظر را، هرجا که در دسترس بوده، بررسی و ارزیابی کرده‌ایم.

جابه‌جاییِ جایگاه کشورها در رده‌بندی، نشان‌دهندهٔ داده‌های موجود برای سنجش قدرت سایبری است. تأکید می‌کنیم که جابه‌جایی نزولی، لزوماً به این معنا نیست که قابلیت‌های کشور مدنظر، به‌صورت مطلق، کاهش یافته است. در اکثر موارد، دلیلش این است که داده‌هایی برای

کشورهای دیگر در دسترس قرار گرفته است که قابلیت و قصدشان را برای پیگیری اهداف ملی از راه سایبری نشان می‌دهد.

هدف اصلی ما این است که قدرت سایبری را به‌عنوان مجموعه‌ای به‌هم‌پیوسته از خط‌مشی‌ها و قابلیت‌ها بفهمیم که گستره‌ای به‌اندازهٔ تمام فعالیت‌های یک دولت دارد. اگر درک قصدها و قابلیت‌های دولت‌ها در فضای سایبری را همچون یک کوه یخ در نظر بگیریم، چهارچوب و نمایهٔ ما فقط نوک آن کوه یخ است. فضای پژوهش آکادمیک و خط‌مشی در زمینهٔ قدرت سایبری و ژئوپلیتیک در حال گسترش است. انتظار می‌رود این حوزه و مفهومِ قدرت سایبری طی سال‌های آتی همچنان تکامل یابد.

۲. مضامین کلیدی

۲. مضامین کلیدی

در این بخش، به‌اختصار دو موضوع را بررسی می‌کنیم که از سال ۲۰۲۰ و انتشار نمایه، خوانندگان علاقهٔ خاصی به آن داشته‌اند: ۱. رویکرد همه‌جانبه به قدرت سایبری؛ ۲. نیل به چندین هدف از راه سایبری.

۱/۲. رویکرد همه‌جانبه به قدرت سایبری

قدرت سایبری مفهومی چندوجهی است و بسیج‌کردن آن مستلزم رویکردی ملی[1] است. هدف انسی‌پی‌آی این است که در قیاس با نمایه‌های موجود و مطالعات غیررسمی و گمانه‌زنی‌های ژورنالیستی، سنجهٔ کامل‌تری از قدرت سایبری ارائه دهد. هرجا ممکن باشد، چنین رویکردی را در قبال سنجش قدرت سایبری پیش می‌گیریم. این رویکرد را بسیاری از دولت‌ها پسندیده‌اند؛ دولت‌هایی که به‌طور روزافزونْ قدرت سایبری را ابزاری کلی‌تر در زمینهٔ خط‌مشی خود به‌شمار می‌آورند. طی دو سال گذشته شاهد افزایش و توسعهٔ اسناد راهبردی‌ای بوده‌ایم که توضیح می‌دهند دولت‌ها چگونه می‌خواهند با رویکرد ملی، قدرت سایبری را بسیج کنند.

ما در انسی‌پی‌آی مقولاتی همچون استراتژی‌های حکومت‌ها، قابلیت‌های دفاعی و عملیات مخرب، تخصیص منابع، و نیز قابلیت‌های

1 whole-of-nation

بخش خصوصی در هر کشور را می‌سنجیم؛ قابلیت‌هایی همچون شرکت‌های فناوری، نیروی کار و نوآوری. ارزیابی ما هم‌زمان قابلیت‌های آشکار [و بالفعل] و بالقوه را مورد سنجش قرار می‌دهد. بنابراین نمرهٔ نهاییِ این شاخص نشان‌دهندهٔ این است که یک حکومت تا چه اندازه قادر به بهره‌گیری از این قابلیت‌ها در راستای منافع کشور خود است.

۲/۲. اهداف:

رصد و پایش گروه‌های داخلی:

کشور اقداماتی انجام داده تا مجوز قانونی و قابلیت رصدِ سایبری به‌منظور پایش و شناسایی و جمع‌آوری اطلاعات دربارهٔ تهدیدهای داخلی و کنشگران درون مرزها را به خود بدهد. از این اقدامات، می‌توان به تلاش برای رصد شهروندان، پایش ترافیک اینترنت، دورزدن رمزگذاری یا شناسایی و ایجاد اختلال در سرویس‌های اطلاعاتی خارجی و 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، 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، استفاده از ابزار الکترونیکی برای کنترل اطلاعات و تغییر روایت‌های درون‌مرزی و

برون‌مرزی را در اولویت قرار داده است. این هدف شامل گسترش پروپاگاندای داخلی و ایجاد و تقویت اطلاعات دروغ 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 و رد پروپاگاندای خارجی است.

جمع‌آوری اطلاعات خارجی برای امنیت ملی:

کشور رازهای ملیِ یک دشمن خارجی را از طریق شیوه‌های سایبری استخراج کرده است. این هدف به‌طور خاص 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 پی بهبودِ 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 ارتباطات شخصیت‌های رده‌بالای دولت را نیز در بر می‌گیرد.

افزایش توانایی سایبری و فناوری تجاری 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.

تخریب یا غیرفعال‌سازی زیرساخت‌ها و قابلیت‌های دشمن:

کشور از فنون و تاکتیک‌ها و رویه‌های سایبریِ مخرب استفاده می‌کند تا توانایی دشمن برای مبارزه در عرصه‌های سایبری و متعارف را مختل یا فرسوده یا تضعیف کند. این امر شامل حملات سایبری به زیرساخت‌های حیاتی و حملات منع سرویس توزیع‌شده به شبکه‌های ارتباطی دولت می‌شود. در این حوزه، می‌توان به حملات سایبری با هدف نشان‌دادنِ قصد و قابلیتِ بازداریِ دشمن از کنش نیز اشاره کرد.

تعریف هنجارهای سایبری و استانداردهای فنی بین‌المللی:

کشور به‌صورت فعال، در مباحثات حقوقی و سیاسی و فنی دربارهٔ هنجارهای سایبری شرکت می‌کند. این امر شامل امضای پیمان‌های سایبری و مشارکت در کارگروه‌های فنی و عضویت در اتحادها و همکاری‌های سایبری برای مبارزه با جرایم سایبری و هم‌رسانی تخصص و قابلیت فنی است.

اندوختن ثروت یا استخراج رمزارز:

کشور از راه سایبری اقدام به تولید ثروت کرده است. این امر شامل سرقت از راه سایبری می‌شود؛ ازجمله به‌کارگیری باج‌افزار و اخاذی با استفاده از اطلاعات کسب‌شده از راه درز داده‌ها و حمله به زیرساخت‌های سایبریِ مؤسسات مالی.

ما قصد کشورها برای پیگیری هر هدف را با ارزیابی راهبردهای ملی و رتوریک و عملیات سایبریِ منتسب به آن‌ها می‌سنجیم. اگر قصد

کشوری برای پیگیری یک هدف کم باشد، ارزیابی ما این است که آن هدف برای کشور اهمیت کمتری دارد.

ما [همچنین] قابلیت کشورها در [دستیابی به] هر هدف را مورد ارزیابی قرار می‌دهیم. شاخص‌های ما یا به‌طور مستقیم شکل‌دهندهٔ قدرت سایبری هستند، و به‌عنوان واسط برای اندازه‌گیری قابلیت‌هایی طراحی شده‌اند که سنجش آن‌ها دشوار بوده است. فعالان و اهالی حوزه سایبری در مورد اجزا و عناصر دخیل در شکل‌گیری قدرت سایبری هنوز خام و ابتدایی است و با پیشرفت این صحنه، این شناخت هم تکامل خواهد یافت. [بنابراین] شاخص‌های ما نیز باید هم‌راستا با این روند، تکامل پیدا کنند. ما به این نکته واقف هستیم که اهداف ملی‌ای که کشورها با استفاده از [ابزارهای] سایبری در پی تحقق آن‌ها برمی‌آیند، اهدافی به‌هم‌پیوسته و درهم‌تنیده هستند. قابلیت‌های سایبری – در کنار ابزار نظامیِ سنتی، دیپلماسی، تحریم و تعرفه – تنها یکی از ابزارها و شیوه‌هایی هستند که حکومت‌ها در پیگیری اهداف ملی خود اتخاذ می‌کنند.

قدرت سایبری، یعنی استفادهٔ مؤثرِ یک کشور از قابلیت‌های سایبری برای دستیابی به اهداف ملی خود. برای تمایزگذاری میان سطوح قصد و قابلیت، میان کشورها و میان تمام اهداف ملی، از لفظ «جامعیت» استفاده می‌کنیم که منظور از آن، استفادهٔ دولت از قدرت سایبری برای رسیدن به اهداف متعدد است؛ نه فقط مواردی معدود.

با ترکیب نمرهٔ قصد و قابلیت در تمام هشت هدف، می‌توانیم «رده‌بندی جامع قدرت سایبری» را به‌دست آوریم که در آن جامع‌ترین قدرت سایبری کشوری است که:

- قصد پیگیری چندین هدف از راه سایبری را دارد؛

- قابلیت پیگیری و دستیابی به اهداف گفته‌شده را دارد.

جامع‌ترین قدرت سایبری، بالاترین قصد و بالاترین قابلیت را برای دستیابی به اکثر اهداف از راه سایبری دارد. کم‌نمره‌ترین کشور آن است که پیگیر کمترین اهداف از راه سایبری است و کمترین میزان قصد و قابلیت را دارد.

۳/۲. نیل به چندین هدفی از راه سایبری

در انسی‌پی‌آی ۲۰۲۲، این موضوع را بررسی می‌کنیم که کشورهای گوناگون تا چه حد از راه سایبری در پی اهداف متعددشان هستند. گفتنی است این سنجه، قابلیت‌های فنی یا «پیچیدگی یک حملهٔ سایبری» را در نظر نمی‌گیرد. در کارگاه‌های بازخوردِ ما، متخصصان خاطرنشان کردند که پیچیدگیِ حملات در نمایهٔ ۲۰۲۰ انعکاس نیافته بود. کشوری که حملهٔ سطح‌پایینی انجام می‌دهد، به‌شیوهٔ صفرویک شمرده می‌شود و همان «نمره»ای را می‌گیرد که به حملهٔ بسیار پیچیده و پیشرفته داده می‌شود. ما این ضعف را می‌پذیریم و اذعان می‌کنیم که نمی‌توانیم پیچیدگیِ فنی حملات منتسب‌شده [به یک عامل] را با استفاده از داده‌های در دسترس عموم بسنجیم. گذشته از این، حتی اگر سنجش پیچیدگیِ فنی عملیاتِ سایبری را لحاظ کنیم، باز هم نمی‌توان ارزیابی قاطعانه‌ای از قابلیت یک کنشگر ارائه کرد. پیچیدگیِ عملیات، ناگزیر، به مقتضیات هدف مرتبط است. جمع‌آوری اطلاعات، گسترش اطلاعات دروغ یا سرقت مالکیت فکری، همگی می‌توانند سطوح گوناگونِ پیچیدگیِ فنی را داشته باشند. درواقع، پیچیده‌ترین عملیات سایبری همیشه علنی نمی‌شوند. شاید به این علت باشد که قربانی خبر ندارد قربانیِ حمله شده است یا تمایلی به تصدیق این امر ندارد یا اقدامات مهاجم شناسایی نشده‌اند یا نمی‌توان

آن‌ها را به او نسبت داد.

در سال ۲۰۲۰، به ردیاب عملیات سایبریِ شورای روابط خارجی (سی‌اف‌آر)[1] اتکا کردیم. این بار، با عمل به بازخوردها، از منبع دیگری هم بهره می‌گیریم: پایگاه دادهٔ حوادث سایبریِ چشمگیر که متعلق به مطالعات راهبردی و بین‌المللی (سی‌اس‌آی‌اس)[2] است و حوادثی را می‌سنجد که تأثیر مالی‌شان بیش از ۱میلیون دلار بوده است. دلیل استفاده از این پایگاه داده این است که در پایگاه دادهٔ سی‌اف‌آر، روی کاغذ، چنین تمایزی مشخص نمی‌شود.

ما پیش‌تر حملاتی را که کشورها با اهداف گوناگون انجام داده‌اند، در نظر گرفته‌ایم تا سنجه‌ای باشد از توانایی نشان‌داده‌شدهٔ هر کشور برای انجام انواع خاص حملات. این شاخص مهم است؛ زیرا یکی از معدود شاخص‌های ملموس توانایی هر کشور برای تبدیل قدرت سایبری به اهرم فشاری به‌منظور دستیابی به هدفی خاص است. هرچند به این نکته نیز واقفیم که منابعمان به تمام عملیات سایبری انجام‌شده دسترسی کامل ندارند. امسال، برای تقویت این شاخص، از منبع دیگری بهره گرفته‌ایم و در ارزیابی یک قدرتِ جامع سایبری، از «چهارچوب انسی‌پی‌آی» استفاده کرده‌ایم؛ یعنی اینکه کدام کشورها با عملیات سایبری در پی دستیابی به اهداف متعددند.

1 Council on Foreign Relations (CFR)'s Cyber Operations Tracker
2 Strategic and International Studies (CSIS) Significant Cyber Incidents database.

۳. نمایه قدرت سایبری ۲۰۲۲

۳. نمایه قدرت سایبری ملی ۲۰۲۲

۱/۳. رده‌بندی کلی سال ۲۰۲۲[1]

چنان‌که در جدول ۱ می‌بینیم، دو کشور جامعی که بالاترین میزانِ قصد و قابلیت را در هر هشت هدف دارند ایالات متحده و چین هستند. جدول ۲ رده‌بندی را بر اساس اهداف تقسیم‌بندی می‌کند.

جدول ۱: انسی‌پی‌آی ۲۰۲۲؛ ده قدرت جامع سایبری

رتبه	کشور
۱	ایالات متحده
۲	چین
۳	روسیه
۴	بریتانیا
۵	استرالیا
۶	هلند
۷	کرهٔ جنوبی
۸	ویتنام
۹	فرانسه
۱۰	ایران

1 برای چهارچوب مفهومیِ انسی‌پی‌آی و تعریف هدف‌ها، ن.ک: ضمیمهٔ الف.

۲/۳. تفسیر نمایه

پژوهشگران و دست‌اندرکاران و سیاست‌گذاران می‌توانند از سنجهٔ تجمیعیِ قدرت سایبری ان‌سی‌پی‌آی در تمام هشت هدف استفاده کنند تا دریابند بر اساس داده‌های در دسترس عموم، کدام کشورها جامع‌ترین قدرت‌های سایبری‌اند. طبق ارزیابی ما، رده‌بالاترین کشورها آن‌هایی‌اند که با بالاترین کارایی از ابزار سایبری برای دستیابی به اهدافِ گوناگون استفاده می‌کنند.

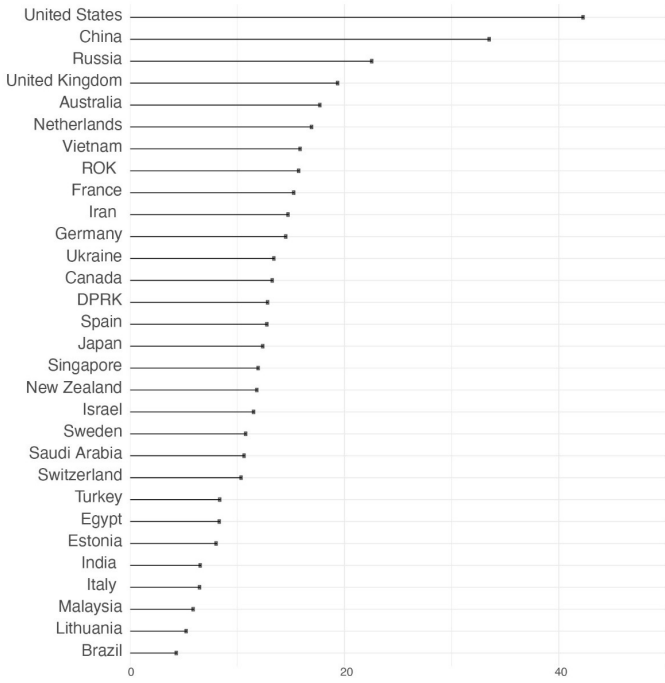
جابه‌جایی کشورها:

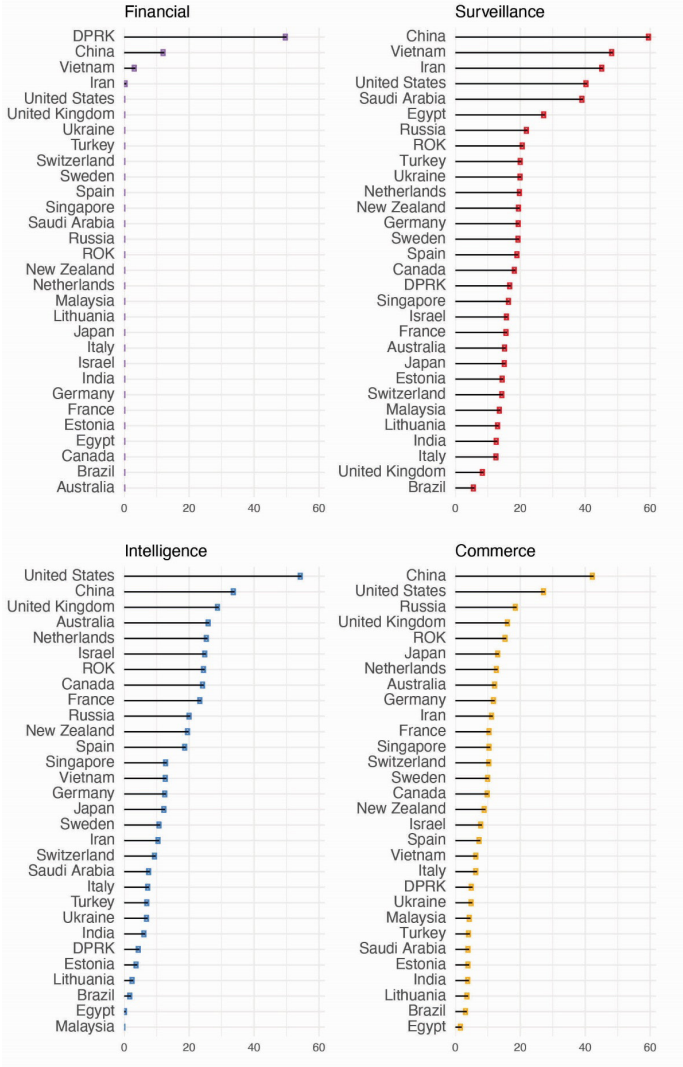
جدول ۲: مقایسهٔ ده قدرت برتر سایبری در سال ۲۰۲۰ و ۲۰۲۲

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

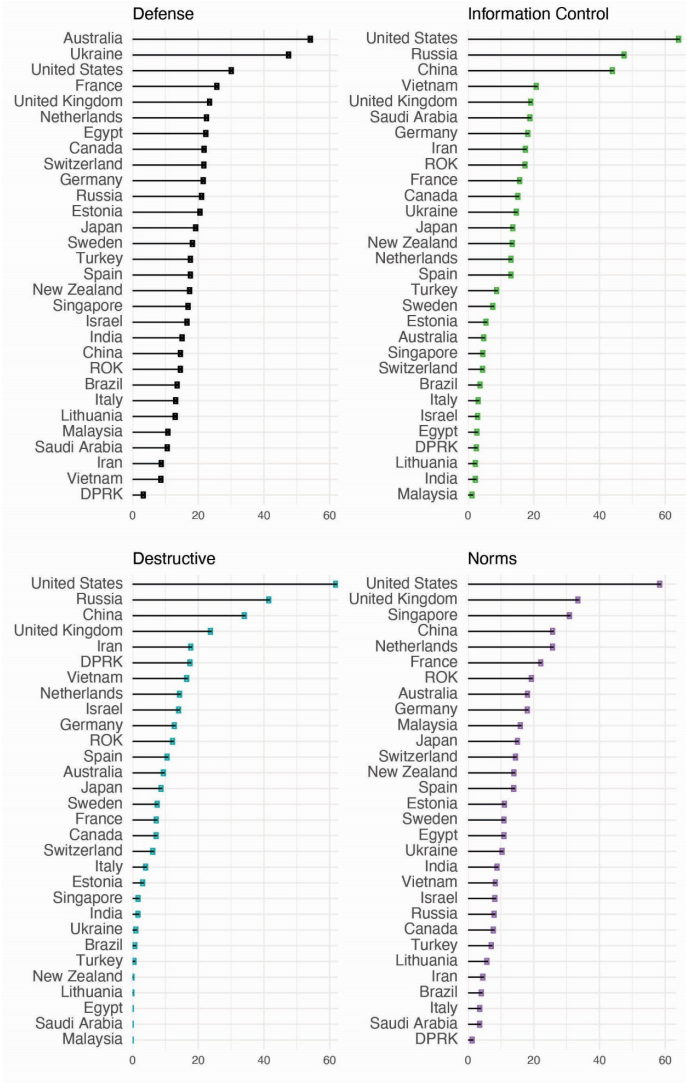
نمایهٔ قدرت سایبری ملی

شکل ۲: رده‌بندی کلی ۱ تا ۳۰





شکل ۳ الف: رده‌بندی کشورها بر اساس هدف



شکل ۳ ب: رده‌بندی کشورها بر اساس هدف

در رده‌بندی ما از ده قدرت سایبری برتر، بعضی کشورها جابه‌جا شده‌اند. جالب‌توجه‌ترینِ آن‌ها روسیه است که از جایگاه چهارم به سوم رسیده و بریتانیا که یک رتبه پایین رفته است. در دو هدف، یعنی سود تجاری و قابلیت مخرب، قدرت روسیه نسبت به بریتانیا افزایش یافته است؛ به‌ویژه به این دلیل که در این دو عرصه، از آن‌ها عملیات سایبری بیشتری آشکارا گزارش شده است.

دو جابه‌جاییِ جالب‌توجه در رده‌بندی ما مربوط به ایران و اوکراین بوده است. ایران از جایگاه ۲۲ نمایه به جایگاه ۱۰ رسیده است. در رده‌بندی قابلیت نیز از ۲۸ به ۱۵ رسیده که دلیلش افزایش نمره‌های تخریبی و رصد بوده است؛ البته هدف تازه‌امتیازدهی‌شده، یعنی مالی، که در آن جایگاه سوم را به‌دست آورده است. اوکراین از ۲۹ به ۱۲ رسیده است، به‌طوری‌که رده‌بندیِ قابلیتش دو جایگاه افزایش یافته و در رده‌بندی قصد نیز از جایگاه ۲۱ به ۶ رسیده است؛ به‌ویژه به‌دلیل افزایش رتبهٔ دفاعی و اطلاعاتی و تخریبی. اما در حوزه‌های دیگر نیز پیشرفت کرده است.

دو تا از همسایه‌های منطقه‌ای چین نیز پیشرفت‌های چشمگیری در نمایه داشته‌اند. جمهوری کره از جایگاه ۱۶ به ۷ رسیده است؛ به این صورت که قابلیتِ آن ثابت مانده، اما قصدش به دلایل گوناگونی از جایگاه ۱۸ به ۹ رسیده است، به‌ویژه در رصد، کنترل اطلاعات، اطلاعاتی، تجاری و هنجارها.

رتبهٔ ویتنام از ۲۰ به ۸ رسیده است؛ قابلیت این کشور ثابت مانده، اما قصدِ آن بنا به پیشرفت‌های دفاعی، تجاری، تخریبی و هنجارها، از جایگاه ۱۶ به ۳ رسیده است.

با توجه به ماهیت داده‌هایی که گردآوری می‌کنیم، این جابه‌جایی‌های رده‌بندی به‌معنای افزایش یا کاهش مطلق قدرت سایبری در مقایسه با

سال ۲۰۲۰ نیست؛ بلکه حکایت از تغییر نسبی قدرت سایبری، نسبت به کشورهای دیگر، بر اساس اطلاعاتِ در دسترس عموم است.

۳/۳. محدودیت‌ها

تحلیل هدف‌محورِ انسی‌پی‌آی از قدرت سایبری ملی، محدودیت‌هایی دارد که بیشتر به ماهیت درحال‌تکامل و مناقشه‌برانگیزِ «قدرت سایبری» و نیز محدودیت داده‌های در دسترس دربارهٔ قصدها و قابلیت‌های سایبری کشورها مربوط است. محدودیت‌هایی که در بخش روش‌شناسیِ نمایهٔ ۲۰۲۰ توضیح دادیم، به قوت خود باقی‌اند. در اینجا دوباره به‌صورت خلاصه بیانشان می‌کنیم:

فقدان داده‌های عمومی دربارهٔ قصد و قابلیت سایبری:

داده‌هایی که گردآوری کرده‌ایم برای اکثر کشورهای مدنظر در دسترس است؛ اما برای همه نه. یکی از مشکل‌های ساخت این نمایه آن است که مؤلفه‌هایِ بهره‌رسان به قدرت سایبری یک کشور، حساس و درنتیجه محرمانه‌اند؛ مثلاً تعداد کارکنان نظامی یا قابلیت‌های اطلاعاتی. حوزه‌هایی وجود دارد که داده‌ها در آن‌ها حساسیت کمتری دارد؛ مثلاً تلاش برای افزایش نیروی کار ماهر و داده‌های مربوط به صنعت. اما این داده‌ها معمولاً برای کشورهایی که ساختارهای حاکمیتی‌شان چندان شفاف و پاسخ‌گو نیست یا منابع کمتری در اختیار دارند، به‌راحتی در دسترس نیست.

به‌دلیل حساسیت‌های بعضی ابعاد قدرت سایبری، به‌ویژه قابلیت‌های تخریبی و دفاعی و جاسوسی و اتکای آن‌ها به ساختارهای امنیت ملی، کشورها ممکن است بنا به اهداف راهبردی، قصد و قابلیت‌های خود را

عامدانه از دانش عموم پنهان کنند. حدس می‌زنیم این قضیه برای اکثر کشورها در زمینهٔ قابلیت‌های مخفی یا نظامی صادق باشد؛ اما به‌طور ویژه برای چین، اسرائیل، ایران و کرهٔ شمالی صادق است. در سال‌های اخیر، شاهد بوده‌ایم که دمکراسی‌های غربیْ اطلاعات بیشتری دربارهٔ قابلیت‌های سایبری ارتش خود منتشر می‌کنند؛ چه برای بازدارندگی دشمنان، چه به‌دلیل خط‌مشی‌های ملی شفافیت و چه برای نشان‌دادن رهبری و شکل‌دهی مباحثات جهانی. این شفافیت‌نداشتن، به‌طور ویژه در آن سه هدفِ یادشده صدق می‌کند، اما با افزایش تنش‌های ژئوپلیتیکی، در حوزه‌های دیگر هم وجود دارد. [ما البته] از این نکته غافل نیستیم که وقتی یک کشور به‌عمد از شفافیت در فعالیت‌هایش پرهیز می‌کند، رتبهٔ آن در حوزه‌های مختلفِ شاخص ان‌سی‌پی‌آی پایین‌تر از واقعیت خواهد بود. به‌عنوان مثال، هیچ کشوری آشکارا اقرار نمی‌کند که از ابزارهای سایبری، همچون باج‌افزار، برای کسب منافع مالی استفاده می‌کند. ازاین‌رو، ان‌سی‌پی‌آی برای جبران این کمبود، حملات سایبریِ منتسب‌شده ذیل این هدف را لحاظ می‌کند؛ زیرا به‌نظر ما، انجام عملیات سایبری از سوی یک کشور، نشان‌دهندهٔ قصد آن‌هاست. همچنین، کمتر کشوری شمار کارکنانِ فعال خود در عملیات سایبریِ مخرب یا عملیات‌های در دست انجام در این زمینه را منتشر می‌کند؛ به همین دلیل، به‌شدت سخت می‌توان قابلیت یک کشور را از این لحاظ سنجید؛ به‌ویژه اگر آن عملیات به‌حدی موفق باشد که شناسایی نشود و گزارشی علنی دربارهٔ آن در دست نباشد.

۴. نتیجه‌گیری

۴. نتیجه‌گیری

کشورها همچنان برای دستیابی به اهداف مختلفی مشغول ارتقای قابلیت‌های [سایبری] خود هستند. برای درک بهترِ اقدامات کشورها و قدرت ملی [آن‌ها]، لازم است قدرت سایبری را مفهومی چندبُعدی در نظر بگیریم و وسعت تحلیل را گسترش دهیم؛ به‌گونه‌ای که انواع اهدافِ دولت‌ها از راه سایبری را در بر بگیرد. از تحلیل ما مشخص می‌شود که کشورها غیر از تخریب و غیرفعال‌سازی زیرساخت‌ها و قابلیت‌های دشمن، در پی تقویت و ارتقای دفاع سایبری ملی، جمع‌آوری اطلاعات در کشورهای دیگر، افزایش توانایی سایبری و فناوری تجاری ملی، کنترل و دست‌کاریِ محیط اطلاعاتی و گسترش نفوذ خود از طریق تعریف هنجارهای سایبری و استانداردهای فنی بین‌المللی نیز هستند. قدرت سایبری را باید در بستر اهداف ملی یک کشور لحاظ کرد و دولت‌ها نیز باید هنگام تلاش برای بسیج‌کردن آن، رویکردی تمام‌کشوری پیش بگیرند و البته روزبه‌روز هم بیشتر به این نوع رویکرد می‌گروند.

اگر یک گام از نمایه به عقب برداریم، می‌بینیم راهبری و زیرساختی که در پس اینترنت قرار گرفته، چندپاره است و پیوسته چندپاره‌تر می‌شود. کشورها، متأثر از جابه‌جایی‌های قدرت و رویدادهای ژئوپلیتیک و افزایش نفوذ چین، به‌ویژه در عرصهٔ سایبری، اکنون بیش از هر زمان دیگری در پی ایجاد ائتلاف در مسائل سایبری هستند تا بتوانند حوزهٔ

سایبری را بنا به منافع خودشان شکل دهند. چه در زمینهٔ رسیدن به اجماع دربارهٔ رفتار مقبولِ کشورها و هنجارهای فضای سایبری در سازمان ملل باشد، چه راهبری فناوری از طریق استانداردهای فنی برای تقویت یا پیشگیری از تعامل‌پذیری و چه نقشه‌هایی برای تنوع‌بخشی به زنجیره‌های تأمین و ایجاد اکوسیستم‌های جدید در کشورهای متحدتر، درهرصورت، پیوندگاه فناوری و ارزش‌ها محل اختلاف‌نظرهایی جدی در مسائل جهانی است.

آنچه این محلِ اختلاف‌نظر در مسائل جهانی را تشدید کرده است، حملهٔ ویرانگر و یک‌جانبهٔ روسیه به اوکراین بوده که در آن از طیفِ کامل قدرتِ سایبری استفاده شده است. احتمال اینکه حملات سایبری روسیه یا ناخواسته به فراتر از مناطق درگیری برسد یا اینکه به‌عنوان سلاحی علیه متحدان اوکراین استفاده شود، باعث شده اجتماع سایبری به تکاپو بیفتند و برای دفاع از قلمرو دیجیتال اوکراین و قابلیت‌سازی و تهیهٔ تجهیزات، از این کشور پشتیبانی کنند. کشورهای گوناگون دفاع سایبری خود را تقویت کردند تا آمادهٔ هر دو احتمال باشند.[1] اکنون که این مقاله منتشر می‌شود، روسیه ظاهراً در استفاده از قدرت سایبری مخرب خود به‌صورت هدفمند عمل می‌کند و به زیرساخت‌ها و خدمات و کسب‌وکارهای اوکراینی حمله می‌کند. گزارش‌ها حاکی از آن است که هرچند ارتش و حملات سایبری هم‌زمان به‌کار گرفته شده‌اند، مقیاس از آنچه انتظار می‌رفت کوچک‌تر بوده و ظاهراً در بعضی اهداف هم‌پوشانی به‌وجود آمده است.[2] کنترل محیط اطلاعاتیِ داخلی، یکی از بخش‌های کلیدی تلاش‌های روسیه در جنگ است و باعث شده روس‌ها رویدادها را فقط

1 https://www.washingtonpost.com/technology/2022/02/28/internet-war-cyber-russia-ukraine/
2 The economist (online), Russia seems to be co-ordinating cyber-attacks with its military campaign, London, May 10, 2022 and https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

از زاویهٔ دید محدودی ببینند. روسیه از این قدرت برای بی‌اعتبارکردن روایت‌های اوکراین و غرب در سطح بین‌المللی نیز استفاده می‌کند. این تعارض، ماهیت به‌هم‌پیوستهٔ زنجیره‌های تأمین جهانی را نشان می‌دهد و بی‌گمان، موضوع مهمی به مباحثه دربارهٔ انشعاب فناوری‌ها خواهد افزود؛ به‌گونه‌ای‌که شرکت‌های خارجی به‌دلیل تحریم‌های غرب، از روسیه خارج می‌شوند و شرکت‌های داخلیِ روسی یا شرکت‌های غیرغربی وارد می‌شوند تا جای خالی آن‌ها را پر کنند؛[1] درحالی‌که این کشور برای قابلیت نظامی خود هم به تجهیزات غربی متکی است.[2] کشورها از حالا شروع به ارزیابی دوبارهٔ زنجیره‌های تأمین و قدرتِ تجاری داخلی خود در این زمینه کرده‌اند. انتظار می‌رود روسیه همچنان قابلیت‌های رصدِ داخلی و جمع‌آوری اطلاعات در کشورهای دیگر را به‌کار بگیرد؛ قابلیت‌هایی که به‌راحتی می‌توانند در خدمت اهداف دیگر باشند؛ به‌خصوص تخریب زیرساخت‌های دشمن.

در محیط ژئوپلیتیکِ امروز کاملاً روشن است که کشورها در پی مجموعهٔ جامع‌تری از قابلیت‌های قدرت سایبری‌اند. مقایسه و درک طیف وسیع‌تری از کنشگران، امروزه بیشترین اهمیت را دارد. پیش‌بینی می‌کنیم که مشکلِ دوگانهٔ هم‌پاماندن با مفهوم درحال‌تکاملِ قدرت سایبری و درعین‌حال، سنجش قدرت سایبری سی کشور یا بیشتر، با استفاده از داده‌های در دسترس عموم، همچنان الهام‌بخش مباحثات خواهد ماند و نیازمند انعطاف‌پذیری خواهد بود. اما مهم است راهی بیابیم که بتوانیم مقایسه کنیم و به درک مشترک برسیم؛ زیرا دولت‌های ملی می‌کوشند در دل اکوسیستم‌های ملی و میان کشورها گفت‌وگو

1 https://www.reuters.com/world/europe/foreign-digital-firms-leave-russias-domestic-providers-pounce-2022-04-01/
2 https://www.nytimes.com/2022/06/02/business/economy/russia-weapons-american-technology.html

و ائتلاف تشکیل دهند تا قدرت سایبری خود را در نسبت با دیگران و هماهنگ با آن‌ها ارتقا دهند. امید داریم که دیگر پژوهشگران چیزی به این تحقیق بیفزایند و مباحثات ناگزیر و روشنی‌بخش دربارهٔ تکامل قدرتِ سایبری و ژئوپلیتیک، همچنان روبه‌جلو ادامه یابد.

۵. ضـــمایم

۵. ضمایم

ضمیمهٔ الف: روش‌شناسی

بین نمایهٔ ۲۰۲۰ و ۲۰۲۲، گروه تحقیقاتی طی فرایندی دقیق، شاخص‌های استفاده‌شده را به پرسش گرفت تا مشخص شود آیا اکنون داده‌های بهتری وجود دارد؟ آیا شاخص‌های بهتری وجود دارد که به سنجش قابلیت‌های گوناگون کمک کند؟ کارگاه‌های متعددی برگزار کردیم و مصاحبه‌های مفصلی با متخصصان اطلاعات و دفاع و سایبری انجام دادیم تا مفروضات ان‌سی‌پی‌آی ۲۰۲۰ را بیازماییم و پیشنهادهایی برای پالایش روش‌شناسی‌مان با استفاده از آنچه اکنون در دسترس است، دریافت کنیم. به همین دلیل، اصلاحاتی در شاخص‌های استفاده‌شده انجام دادیم.

الف ۱: چهارچوب مفهومی

جدول ۳: اهداف مدنظر

هدف	توضیح
اندوختن ثروت و حفاظت از آن	کشور، عملیاتی سایبری را با هدف اندوختنِ ثروت انجام داده است. این امر شامل سرقت، از جمله به‌کارگیری باج‌افزار، اخاذی با اطلاعات کسب‌شده از راه درز داده‌ها و حمله به زیرساخت‌های دیجیتالی مؤسسات مالی می‌شود.
کنترل و دست‌کاری محیط اطلاعاتی	کشور، با انعکاس دوگانگی کنترل اطلاعات، استفاده از ابزار الکترونیکی برای کنترل اطلاعات و تغییر روایت‌های درون‌مرزی و برون‌مرزی را در اولویت قرار داده است. این هدف شامل گسترش پروپاگاندای داخلی و ایجاد و تقویت اطلاعات دروغین در سطح بین‌المللی 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 و رد پروپاگاندای خارجی است.
تعریف هنجارهای سایبری و استانداردهای فنی بین‌المللی	کشور به‌صورت فعال در مباحثات حقوقی و سیاسی و فنی دربارهٔ هنجارهای سایبری شرکت می‌کند. این امر شامل امضای پیمان‌های سایبری و مشارکت در کارگروه‌های فنی و عضویت در اتحادها و همکاری‌های سایبری برای مبارزه با جرایم سایبری و هم‌رسانی تخصص و قابلیت فنی است.
تخریب یا غیرفعال‌سازی زیرساخت‌ها و قابلیت‌های دشمن	کشور از فنون و تاکتیک‌ها و رویه‌های سایبری 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 به شبکه‌های ارتباطی دولت می‌شود. در این حوزه، می‌توان به حملات سایبری با هدف نشان‌دادن قصد و قابلیتِ بازداریِ دشمن از کنش نیز اشاره کرد.
جمع‌آوری اطلاعات خارجی با هدف امنیت ملی	کشور رازهای ملی یک دشمن 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 پی 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 ارتباطات شخصیت‌های رده‌بالای دولت را نیز در بر می‌گیرد.
افزایش توانایی سایبری و فناوری تجاری 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 جاسوسی 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.
تقویت و ارتقای دفاع سایبری	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.
رصد و پایش گروه‌های داخلی	کشور اقداماتی انجام داده تا مجوز قانونی و قابلیت رصد سایبری به‌منظور پایش و شناسایی و جمع‌آوری اطلاعات دربارهٔ تهدیدهای داخلی و کنشگران درون مرزها را به خود بدهد. از این اقدامات، می‌توان به تلاش برای رصد شهروندان، پایش ترافیک اینترنت، دورزدن رمزگذاری یا شناسایی و ایجاد اختلال در سرویس‌های اطلاعاتی خارجی و سازمان‌های مجرم و گروه‌های تروریستی اشاره کرد.

الف۲: فرمول نمایهٔ قدرت سایبری ملی

$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{8}\sum_{x=1}^{8} Capability_x \times Intent_x$$

شکل ۴: فرمول انسی‌پی‌آی ۲۰۲۲

الف۳: ساخت انسی‌پی‌آی تجمیعی

داده‌های ناموجود و نرمال‌سازی شاخص‌ها:

ما نتوانستیم برای تمام سی کشورِ مدنظر در انسی‌پی‌آی ۲۰۲۲ و برای تک‌تک شاخص‌هایمان داده بیابیم. تمام شاخص‌های لحاظ‌شده در نمایه، نشان‌دهندهٔ موجودبودن داده برای دست‌کم ۲۱ (۷۰درصد) از ۳۰ کشور هستند؛ هم آن و هم نقاط داده‌ای که در آن‌ها جایگزین‌های معقولی برای داده‌های ناموجود داشتیم. محاسبات بر اساس کشورهایی انجام شد که ویژگی‌های مشابه کشور مدنظرمان را دارند (جمعیت و قدرت اقتصاد و جغرافیا) یا بر اساس شاخص‌های دیگری که به آنچه می‌سنجیم نزدیک بودند. شاخص‌هایی که به این حدنصاب نرسیدند، لحاظ نشدند. ما چند شاخص را درون‌سازمانی تهیه کردیم و نقشه و رویهٔ کدگذاری دقیقی را دنبال کردیم.

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

شاخص	تخمین برای این کشورها
نمایهٔ سواد و تحصیلات خطر سایبری	کرهٔ شمالی، مصر، ایران، مالزی، اوکراین و ویتنام
تأمین نیروی ارتش سایبری	کرهٔ شمالی، مصر، هند، لیتوانی، مالزی، نیوزیلند، عربستان سعودی، اوکراین و ویتنام
قوانین محرمانگی داده‌ها	کرهٔ شمالی
آزادی در اینترنت	کرهٔ شمالی، اسرائیل، لیتوانی، هلند، نیوزیلند، اسپانیا، سوئد و سوئیس
نمایهٔ قدرت نرم جهانی	کرهٔ شمالی و لیتوانی
نرخ آلودگی موبایل/رایانه	کرهٔ شمالی، استونی، لیتوانی و نیوزیلند
سازمان استانداردهای ملی	کرهٔ شمالی، برزیل، چین، مصر، اسرائیل، لیتوانی، مالزی، روسیه، کرهٔ جنوبی و عربستان سعودی
جمعیت متصل به اینترنت	کرهٔ شمالی
استفاده از شبکه‌های اجتماعی	کرهٔ شمالی
رصد	کرهٔ شمالی، مصر، کرهٔ جنوبی، عربستان، ترکیه، اوکراین و ویتنام

جدول ۴: شاخص‌های تخمینیِ قابلیت کشورها

پیش از تجمیع داده‌ها، اصلاحاتی در شاخص‌هایمان انجام دادیم تا مقادیر بالاتر با عملکرد سایبریِ بهتر در تمام شاخص‌ها تناظر داشته باشد. تحلیل هم‌بستگی دوبه‌دو را با تمام شاخص‌ها انجام داده‌ایم.

پیش از تجمیع، شاخص‌ها را نرمال‌سازی کردیم تا مقیاس مشترکی داشته باشند. از تکنیک کمینه‌بیشینه به‌عنوان تکنیک نرمال‌سازی استفاده کردیم؛ زیرا (۱) بهتر از همهٔ تکنیک‌ها انعکاس‌دهندهٔ چهارچوب نظری‌مان است؛ (۲) برای ویژگی‌های داده‌ها مناسب‌تر است؛ (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 قصد 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 (ن.ک: جدول ۱۴). این شمارش چندباره مبتنی بر تأمل نظری 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 شاخصِ قابلیت نمرهٔ بالایی می‌گیرد، به‌صورت خودکار نمره را هم در انسی‌پی‌آی و هم نمایهٔ قابلیت سایبری افزایش می‌دهد.

برای محاسبهٔ نمرهٔ قصد انسی‌پی‌آی، قابلیت‌های هر کشور را (برای هر هدف) در قصد 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 معادل وزن دانست. نمرهٔ قصد انسی‌پی‌آی نشان‌دهندهٔ اولویت‌های گوناگونی است که بعضی کشورها برای بعضی قابلیت‌های سایبریِ بخصوص قائل می‌شوند. این یعنی هر کشور فقط درصورتی می‌تواند از قابلیت‌های سایبری خود در عرصه‌ای، مثلاً رصد ملی، استفاده کند که قصد نسبتاً بالایی برای انجام این کار داشته باشد.

الف۴: تغییرات انجام‌شده در روش‌شناسی انسی‌پی‌آی ۲۰۲۲

امسال ۲۹ شاخصِ قابلیت استفاده کرده‌ایم که سپس از آن‌ها میانگین‌گیری می‌شود تا نمایهٔ قابلیت سایبری به‌دست آید. مثل سال ۲۰۲۰، بعضی از معیارها به بیش از یک هدف بهره می‌رسانند. اگر اطلاعات جدیدی برای شاخص‌های استفاده‌شده در سال ۲۰۲۰ در دسترس قرار گرفته است، آن‌ها را به‌روزرسانی کرده‌ایم. شاخص‌هایی جدید را هم لحاظ کرده‌ایم تا هدف هشتم را نیز در نمایه بگنجانیم.

اضافه‌کردنِ هدف هشتم: اندوختن ثروت و محافظت از آن

انسی‌پی‌آی هشت هدف را بررسی کرده است که کشورها از راه سایبری در پی آن‌ها هستند. در نمایهٔ ۲۰۲۰، سنجه‌ای برای هدف هشتم ارائه نکردیم: اندوختن ثروت و محافظت از آن. این حذف تا حدی به‌دلیل دشواربودنِ جمع‌آوری داده دربارهٔ این هدف بود. امسال، با آنکه همچنان جمع‌آوری داده‌های مفید برای این هدف دشوار است، از شاخص واحدی برای سنجش قابلیت هر کشور در این هدف استفاده کردیم؛ شاخصی که هرچند بی‌عیب‌ونقص نیست، وجهی ارتقایافته را برای نمایه به‌ارمغان می‌آورد.

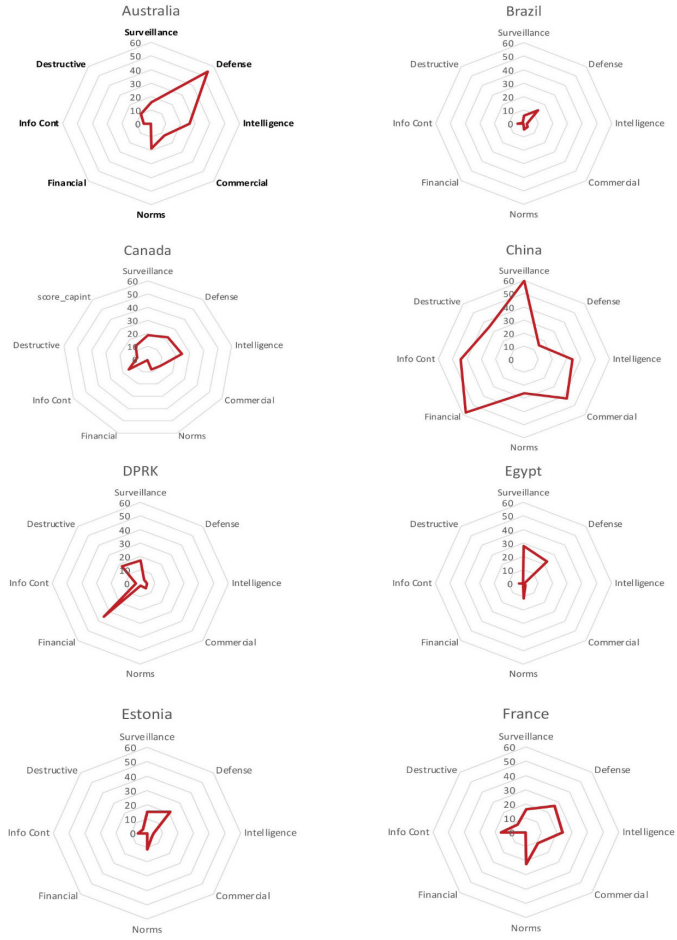
اندوختن ثروت و محافظت از آن را به‌عنوان به‌کارگیری عملیات سایبری برای اندوختن ثروت تعریف کرده‌ایم. این امر شامل سرقت از راه سایبری، ازجمله باج‌افزار و باج‌گیری برای منتشرنکردن اطلاعاتی که از طریق درز داده به‌دست آمده است و حمله به زیرساخت‌های دیجیتالی مؤسسات مالی می‌شود.

چهار کشوری که در این عرصه رکورد زدند، چین، کرهٔ شمالی، ویتنام

و ایران بودند. نکتهٔ غیرمنتظرهٔ این رده‌بندی، جای خالی روسیه در رده‌های بالاست. با آنکه طبق گزارش‌ها، مقر بعضی از گروه‌های باج‌افزارِ پیشرفته در روسیه و کشورهای روسی‌زبان است، تولید پول نقد از راه حملات سایبری جایی در قصد علنی و منتشرشده و بیان‌شدهٔ دولت روسیه ندارد. این نمایه، برای نمره‌دهی، رابطهٔ نزدیک میان گروه‌های جرایم سایبری (یا نایب‌ها) و دولت را هم در نظر نمی‌گیرد. همکاری میان دولت روسیه و گروه‌های مجرم، رویکردی راهبردی و تاکتیکی به قدرتِ سایبری و بلندپروازی‌های سیاسی این کشور در سطح جهان است.

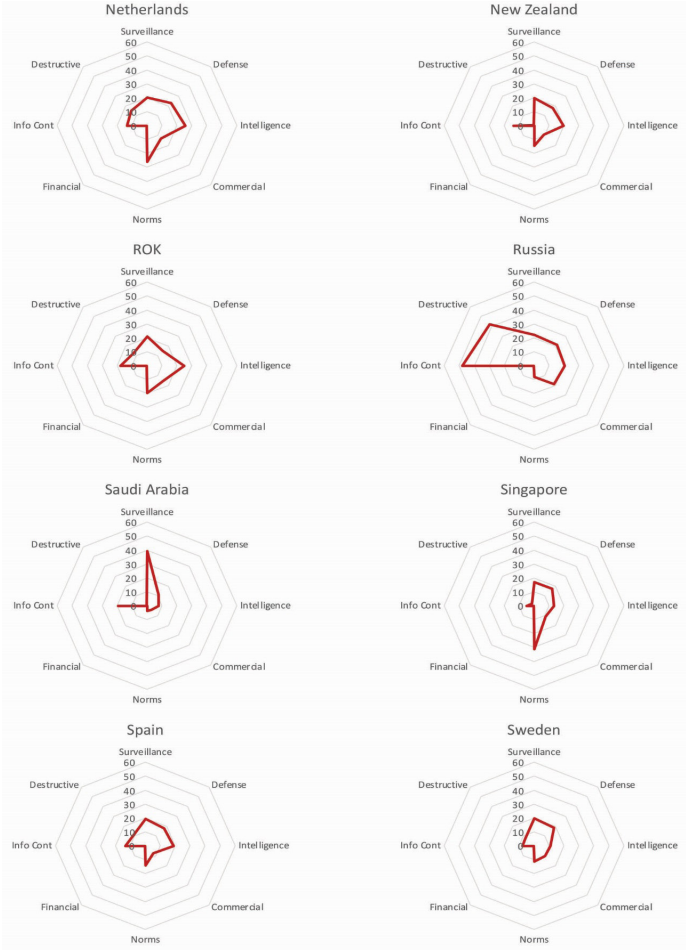
برای این هدف، به تعداد حملات شناسایی‌شده در پایگاه‌های دادهٔ منبع‌باز نظر داشتیم که هدفشان سود مالی بوده است.

ضمیمهٔ ب: نمایهٔ قدرت سایبری ملی؛ نمودارهای نتایج

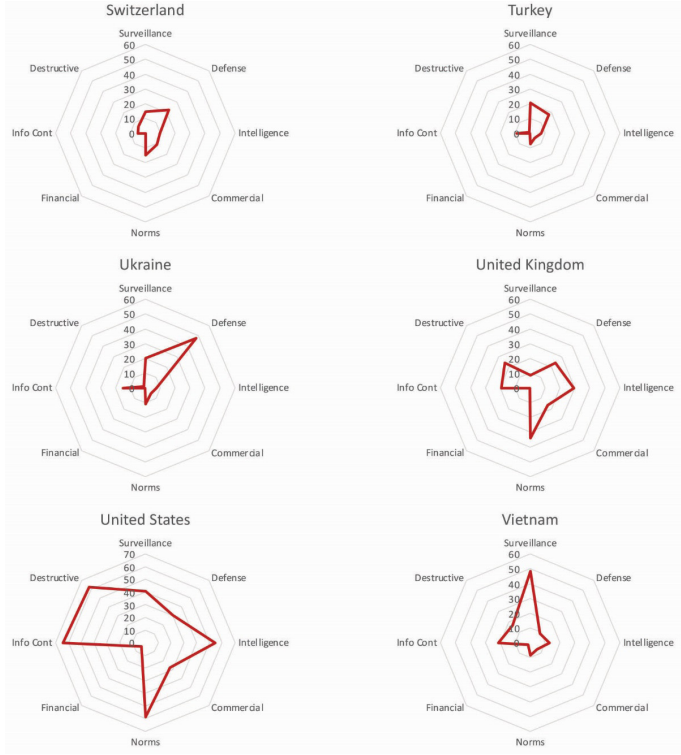


شکل ۵ الف: نمودارهای راداری قدرت سایبری ملی به تقسیم هدف

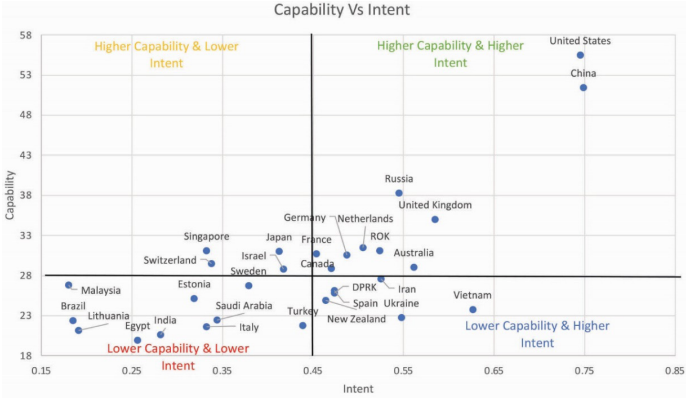
شکل ۵ ب: نمودارهای راداری قدرت سایبری ملی به تقسیم هدف



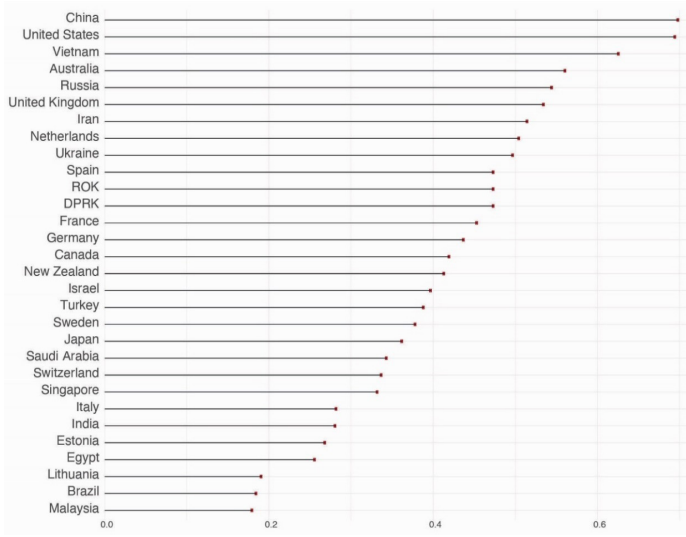
شکل ۵ ج: نمودارهای راداری قدرت سایبری ملی به تقسیم هدف



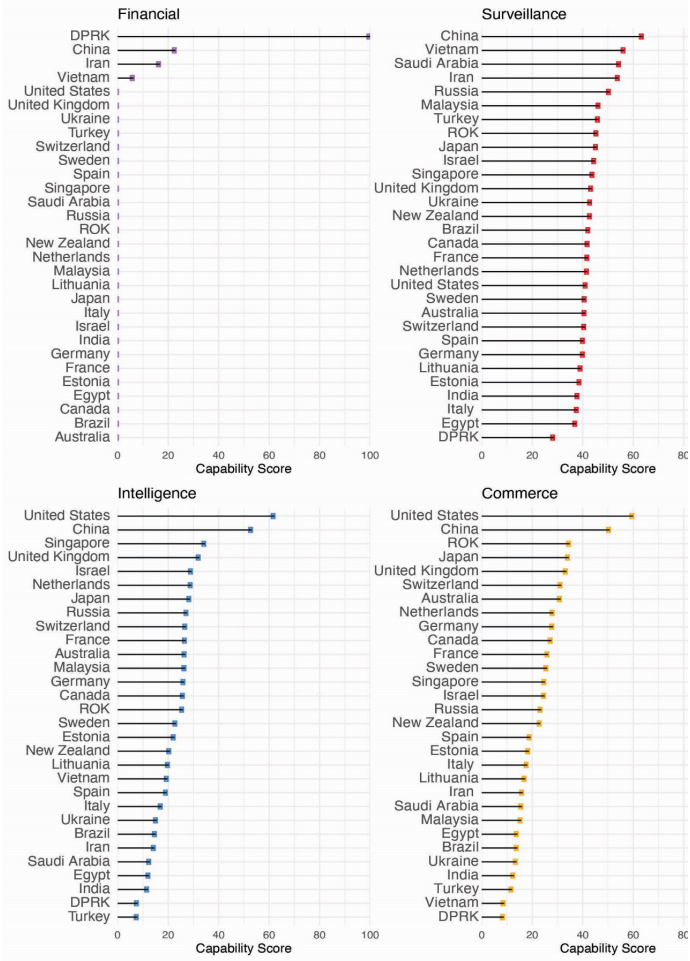
شکل ۵ د: نمودارهای راداری قدرت سایبری ملی به تقسیم هدف



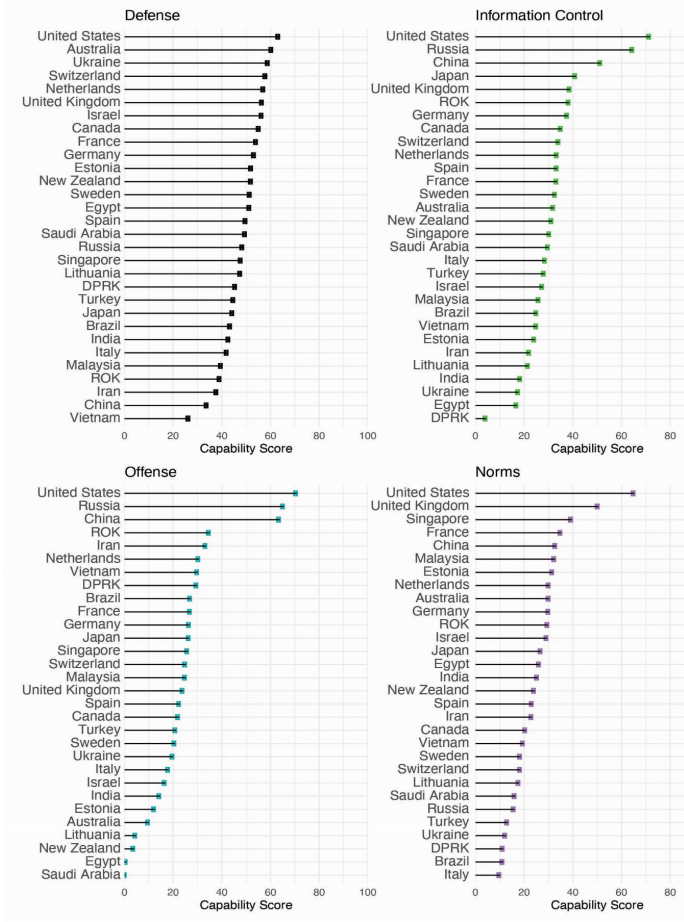
شکل ۶: نمودار نقطه‌ای قابلیت در برابر قصد



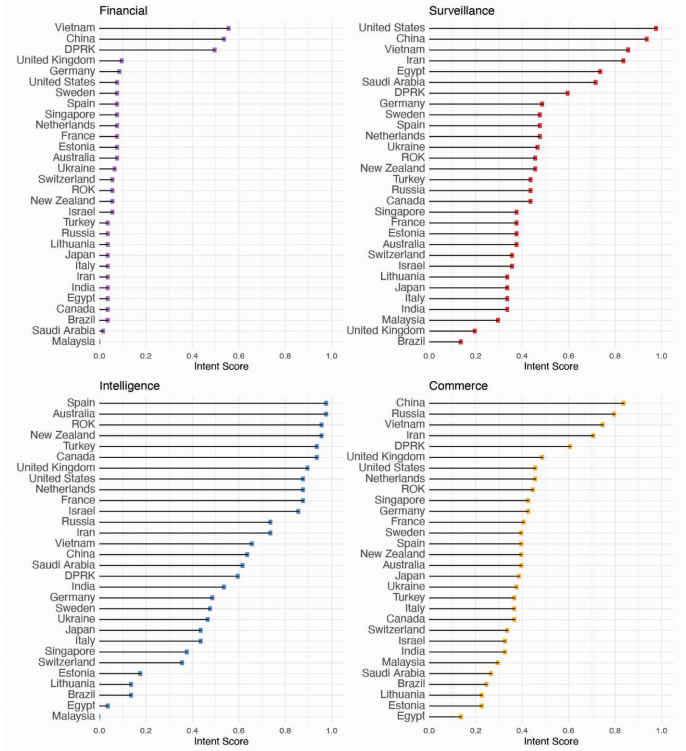
شکل ۷: رده‌بندی نمایهٔ قصد سایبری



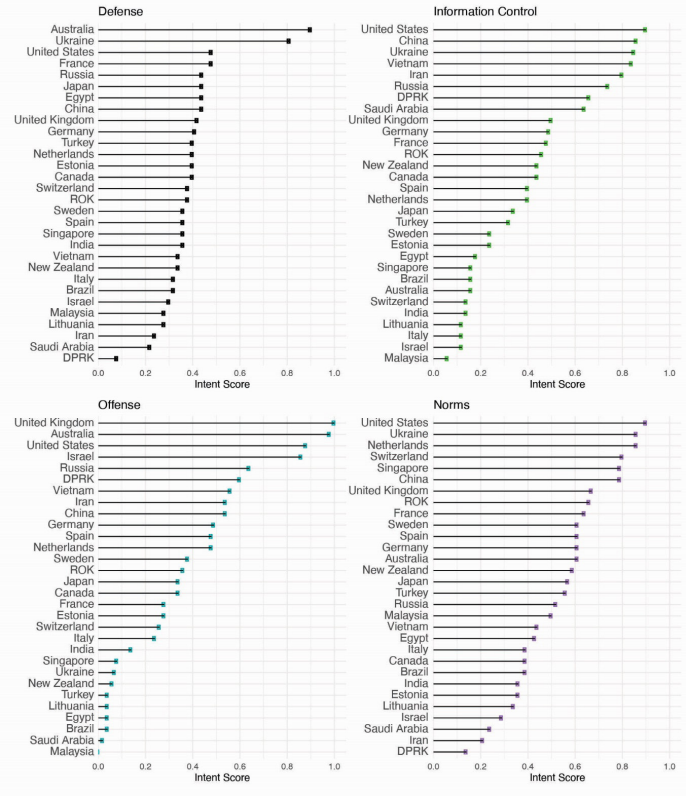
شکل ۸ الف: نتایج به تقسیم هدف (قابلیت)



شکل ۸ ب: نتایج به تقسیم هدف (قابلیت)



شکل ۹ الف: نتایج به تقسیم هدف (قصد)



شکل ۹ب: نتایج به تقسیم هدف (قصد)

ضمیمهٔ ج: تشریح مفصل شاخص‌های قصد

ج۱: شاخص‌های قصد بر اساس هدف

اندوختن ثروت و محافظت از آن

جدول ۵:

شاخص	معنا	توضیح منبع	روش نمره‌دهی
در حملهٔ سایبری منسوب مشاهده‌شده است	برخلاف دیگر 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) 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.	مشاهده‌شده در یک یا چند حمله: بله/خیر

کنترل و دست‌کاری محیط اطلاعاتی

جدول ۶:

شاخص	معنا	توضیح منبع	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: https://www.dlapiperdataprotection.com/	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 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 برخطِ 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 و بیانیه‌های سیاست‌مداران وزارت دفاع دربارهٔ قابلیت‌های سایبری کشور	بله/خیر
آیا واحد یا فرماندهی سایبری ارتش کشور اذعان می‌کند که کشور دارای قابلیت سایبری کنترل و دست‌کاری محیط اطلاعاتی است؟	داشتن یک واحد یا فرماندهیِ 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 که عرضه می‌کنند خواهند بود.	تحلیل حضور برخطِ 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 دربارهٔ قابلیت‌هایی بودیم که واحدهای نظامی گوناگون از آن‌ها برخوردارند	بله/خیر
آیا آژانس اطلاعاتی کشور یا سرویس اطلاعات خارجی آن اذعان می‌کنند که کشور دارای قابلیت سایبری برای کنترل و دست‌کاری محیط اطلاعاتی است؟	اذعان به اینکه آژانس اطلاعاتیِ کشور مأموریتی سایبری دارد	تحلیل حضور برخطِ 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 اطلاعاتیِ سایبری دربارهٔ قابلیت‌هایی بودیم که اجتماع اطلاعاتی از آن‌ها برخوردار است.	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 پیشین (اگر وجود داشته باشد).	هدف حاضر در یک راهبرد: بله/خیر

در حملهٔ سایبری منسوب مشاهده شده است	برخلاف دیگر شاخص‌های قصد که قصدِ خاصی را (که نیازمند برنامه‌ریزی و تمایل قبلی است) نشان می‌دهد، از اقدامات یک کشور نیز می‌توان قصد کلی را (که از ارتکاب مفروض داشته می‌شود) 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.	مشاهده‌شده در یک یا چند حمله: بله/خیر

تعریف هنجارهای سایبری و استانداردهای فنی بین‌المللی

جدول ۷:

شاخص	معنا	توضیح منبع	روش نمره‌دهی
از بین پنج مورد آخر، کشور در چند رایزنی گروه کارشناسانِ دولت سایبری (جی‌جی‌ای) سازمان ملل شرکت کرده است؟	کمیتهٔ نخست مجمع عمومی سازمان ملل دربارهٔ خلع‌سلاح و امنیت بین‌المللی، که از طریق گروه‌های پیاپی کارشناسان دولت (جی‌جی‌ای) در زمینهٔ تحولات عرصهٔ اطلاعات و مخابرات در بستر امنیت بین‌المللی، بعضی از نخستین تلاش‌ها برای رسیدن به اجماعی جهانی دربارهٔ هنجارهای الزام‌آور و غیرالزام‌آور را تسهیل کرده است؛ هنجارهایی که در محیط دیجیتال و رفتار کشورها در استفاده از فناوری اطلاعات و ارتباطات اعمال می‌شوند. نمرهٔ بالاتر در این شاخص به‌معنای این است که کشور در رایزنی‌های جی‌جی‌ایِ سازمان ملل حضور داشته است.	اعداد و ارقام برگرفته از: https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en691-.pdf	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 افراد را از گروه‌های ذی‌نفع گوناگون در جایگاه هم‌تراز گرد هم آورد تا دربارهٔ مسائل خط‌مشی عمومی پیرامون 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 روش بیشینه‌سازی فرصت‌های اینترنت و رسیدگی به خطرات و مشکل‌های آن است	اعداد و ارقام برگرفته از: https://www.intgovforum.org/multilingual/content/mag-2020-members و https://www.intgovforum.org/multilingual/igf-2020-1st-mag-attendees	۰٫۲۵ برای دولت/جامعهٔ‌مدنی/اجتماع فنی/بخش خصوصی

آیا کشور در فعالیت‌های قابلیت‌سازِ انجمن جهانیِ تخصص سایبری (جی‌اف‌سی‌اف) شرکت کرده است؟	جی‌اف‌سی‌اف می‌گوید مأموریتش تقویت «همکاری بین‌المللی در زمینهٔ قابلیت‌سازیِ سایبری از طریق پیوند نیازها و 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 باهم در میان بگذارند	اعداد و ارقام برگرفته از: https://thegfce.org/member-overview/	بله/خیر
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	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 کشورِ 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 دستورالعمل استانداردها در حوزهٔ فناوری اطلاعات و ارتباطات دارد.	https://www.iso.org/technical-committees.html	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) و گروه ۱۷ (امنیت) و گروه ۲۰ (اینترنت اشیا و شهرهای هوشمند)	بدنهٔ بین‌المللی دیگر که نمایندگی ملی برای تعیین استانداردهای فنی برای فناوری‌های اطلاعات را دارد، اتحادیهٔ بین‌المللی مخابرات است. 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)	https://www.itu.int/en/ITU-T/studygroups/2020-2017/Pages/default.aspx	به هر کشور بر اساس نقشش در هریک از سه گروه مطالعاتی، امتیازی داده شد. امتیاز به این شکل بود: ۱ = سرپرست ۰/۷۵ = معاون سرپرست ۰/۵ = عضو WP ۰/۲۵ = کشور عضو اتحادیهٔ بین‌المللی مخابرات سپس میانگین مشارکت هر کشور در تمام سه گروه اعمال شد تا امتیاز نهایی بین ۰ تا ۱ باشد.
آیا کشور در مشق‌های دوجانبه یا چندجانبهٔ دفاع سایبری شرکت 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	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 پیشین (اگر وجود داشته باشد).	مشاهده‌شده در یک یا چند حمله: بله/خیر
اگر تعریف استانداردهای فنی و هنجارهای سایبری بین‌المللی در راهبرد سایبری ملی کشور به‌رسمیت شناخته می‌شود، نمرهٔ راهبرد را بیاورید.	ن.ک: جدول نمرهٔ راهبرد	ن.ک: جدول نمرهٔ راهبرد	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

تخریب یا غیرفعال‌سازی زیرساخت یا قابلیت‌های دشمن

جدول ۸:

شاخص	معنا	توضیح منبع	روش نمره‌دهی
آیا برنامه‌ریزی نظامی یا اسناد راهبردی سایبری یا برنامه‌ریزی نظامی یا اسناد راهبردی کلی، اذعان می‌کنند که کشور قابلیت سایبری تخریبی 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 برمی‌آیند، با بهای فرصتی روبه‌رو می‌شوند و از آن‌ها انتظار می‌رود در اسناد برنامه‌ریزی دفاع ملی، ارزش فعالیت‌های سایبری را توجیه کنند	تحلیل حضور بر خطِ 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 و بیانیه‌های سیاست‌مداران وزارت دفاع دربارهٔ قابلیت‌های سایبری کشور	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 که عرضه می‌کنند خواهند بود.	تحلیل حضور بر خطِ 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 دربارهٔ قابلیت‌هایی بودیم که واحدهای نظامی گوناگون از آن‌ها برخوردارند	بله/خیر
آیا آژانس اطلاعاتی کشور یا سرویس اطلاعات خارجی آن اذعان می‌کنند که کشور قابلیت سایبری مخرب دارد؟	اذعان به اینکه آژانس اطلاعاتی کشور مأموریتی سایبری دارد	تحلیل حضور بر خطِ آژانس اطلاعاتی هر کشور برای ارزیابیِ اینکه آیا به این هدف اذعان می‌کند یا نه. همچنین دنبال نظرات عمومی از سوی سیاست‌مداران یا رهبران ارشد آژانس‌های اطلاعاتیِ سایبری دربارهٔ قابلیت‌هایی بودیم که اجتماع اطلاعاتی از آن‌ها برخوردار است	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).	هدف حاضر در یک راهبرد: بله/خیر
در یک حملهٔ سایبری منسوب مشاهده شده است	برخلاف دیگر 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) 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.	مشاهده‌شده در یک یا چند حمله: بله/خیر

جمع‌آوری اطلاعات خارجی با هدف امنیت ملی

جدول ۹:

شاخص	معنا	توضیح منبع	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 برخطِ 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 و بیانیه‌های سیاست‌مداران وزارت دفاع دربارهٔ قابلیت‌های سایبری کشور	بله/خیر
آیا واحد یا فرماندهی سایبری ارتش کشور اذعان می‌کند که کشور قابلیت سایبری مخرب دارد؟	داشتن یک واحد یا فرماندهیِ 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 که عرضه می‌کنند خواهند بود.	تحلیل حضور برخطِ 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 دربارهٔ قابلیت‌هایی بودیم که واحدهای نظامی گوناگون از آن‌ها برخوردارند	بله/خیر

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 درباره قابلیت‌هایی بودیم که اجتماع اطلاعاتی از آن‌ها برخوردار است	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).	هدف حاضر در یک راهبرد: بله/خیر
در یک حملهٔ سایبری منسوب مشاهده‌شده است	برخلاف دیگر 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) 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.	مشاهده‌شده در یک یا چند حمله: بله/خیر

افزایش توانایی سایبری و فناوری تجاری ملی

جدول ۱۰:

شاخص	معنا	توضیح منبع	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	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 استانداردسازی بین‌المللی در دستورالعمل فناوری اطلاعات و ارتباطات دارد.	https://www.iso.org/technical-committees.html	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 کمیسیون‌فنی مشترک ایزو/ آی‌ای‌سی ۰ = بدون وابستگی
آیا کشور طرح مشارکت بخش دولتی و خصوصی‌ای برای رشد صنعت سایبری داخلی، 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.	بله/خیر
آیا شواهدی هست که نشان دهد کشور راهبرد نیروی کار سایبری یا راهبرد مدیریت زنجیرهٔ تأمین سایبری دارد؟	ساخت نیروی کار سایبری داخلی، نقشی حیاتی در افزایش توانایی سایبری و فنی ملی دارد. درنتیجه، لازم است کشورها برای ساخت نیروی کار سایبری خود راهبردهایی را توسعه دهند یا راهبردِ مدیریت زنجیرهٔ تأمین سایبری طراحی کنند.	تحلیل حضور برخط آژانس اطلاعات هر کشور برای ارزیابی اینکه آیا به هدف مدنظر نایل شده است یا نه.	بله/خیر
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/	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 دوطرفه) نتایج آزمایش‌ها برای دریافت مجوز در سطح ملی استفاده می‌کنند». عضویت در این سازمان موانع مجوزدهی میان کشورها را از میان برمی‌دارد و آن‌ها را قادر به صادرات و واردات محصولات امنیت سایبری و فناوری می‌کند.	اعداد و ارقام برگرفته از: https://www.iecee.org/dyn/www/f?p=106:40:0	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 راهنمای خاصی برای صادرکنندگان امنیت سایبری یا تلاش برای جذب سرمایه‌گذاران خارجی به‌منظور سرمایه‌گذاری در محصولات و شرکت‌های امنیت سایبری ملی.	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 برخطِ 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.	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).	هدف حاضر در یک راهبرد: بله/خیر
در یک حملهٔ سایبری منسوب مشاهده شده است	برخلاف دیگر 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) استنباط کرد.	استفاده از آمار و ارقام رديابی عملیات سایبری شورای روابط خارجی برای ارزیابی اینکه آیا یک یا چند حمله به کشور نسبت داده شده است یا نه.	مشاهده‌شده در یک یا چند حمله: بله/خیر

تقویت و ارتقای دفاع سایبری

جدول ۱۱:

شاخص	معنا	توضیح منبع	روش نمره‌دهی
آیا کشور نقشهٔ امنیت‌سایبری‌ای منتشر کرده که ترسیم کند چگونه از سیستم‌های دولتی و/یا زیرساخت‌های حیاتی ملی محافظت 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	بله/خیر
آیا کشور کارزارهای آگاهی سایبری و بهداشت سایبری برگزار می‌کند؟	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.	بله/خیر
آیا کشور اعلام کرده قصد دارد فعالانه اقدامات سایبری ملی برای دفاع 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 تمهیدات سایبری فعال ملی برای دفاع. همچنین دنبال نظرات عمومی سیاست‌مداران و رهبران ارتش و آژانس‌های اطلاعاتی بودیم.	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).	هدف موجود در یک راهبرد: بله/خیر
در حملهٔ سایبری منسوب مشاهده شده است	برخلاف دیگر 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) 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.	مشاهده‌شده در یک یا چند حمله: بله/ خیر

رصد و پایش گروه‌های داخلی:

جدول ۱۲:

شاخص	معنا	توضیح منبع	روش نمره‌دهی
آیا کشور دست‌کم یک پلیس یا آژانس اعمال قانونی دارد که تخصص جرایم سایبری باشد یا شهروندان را ترغیب به گزارش جرایم سایبری کند؟	نشان می‌دهد که کشور توانایی پیگرد قانونی جرایم سایبری و انجام رصد سایبری را به آژانس‌های اعمال قانون خود داده است.	تحلیل حضور برخط هر کشور برای یافتن ارجاعاتی به تخصص اعمال قانون. همچنین دنبال نظرات عمومی سیاست‌مداران ملی و افسران رده‌بالای پلیس گشتیم	بله/خیر
آیا آژانس اطلاعات داخلی کشور به رصد قابلیت‌های سایبری اذعان می‌کند؟	اذعان به اینکه آژانس اطلاعاتی کشور دارای مأموریتی سایبری است	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 از آن‌ها برخوردار است	بله/خیر
آیا راهبرد، نقشه یا قانون ضدتروریسم و امنیت داخلی کشور جزئیاتی دربارهٔ جرایم سایبری، تروریسم سایبری یا رصد داخلی از راه سایبری دارد؟	نشان می‌دهد که کشور در حال کاوش فعالیت سایبری از طریق ضدتروریسم و امنیت داخلی است.	تحلیل حضور برخط وزارت امور داخلی یا بخش امنیت داخلی برای یافتن راهبردها و نقشه‌ها و نقشه‌های ضدتروریستی یا امنیت داخلی و اینکه آیا به فعالیت‌های سایبری ارجاع دارد یا نه.	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).	هدف حاضر در یک راهبرد: بله/خیر
در یک حملهٔ سایبری منسوب مشاهده شده است	برخلاف دیگر 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) 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.	مشاهده‌شده در یک یا چند حمله: بله/خیر

ج۲: کیفیت ارزیابی راهبرد در زمینهٔ قصد

جدول ۱۳:

نمره	توضیح
۱	مرور کلی تهدیدها و اولویت‌ها
۲	تحلیل دقیق تهدیدها و اولویت‌های آشکارا تعریف‌شده
۳	تقسیم مسئولیت‌ها میان بخش‌های گوناگون دولت
۴	تسلسل زمانی دقیق یا معیارهای موفقیت
۵	تسلسل زمانی دقیق و معیارهای موفقیت
۶	راهبرد طی پنج سال اخیر یا از زمان انقضا، روزآمد نشده است.

ضمیمهٔ د: شاخص‌های قابلیت

د۱: تشریح مفصل مطابقت شاخص‌های قابلیت با اهداف گوناگون

جدول ۱۴:

	شاخص	اثربخشی ثروت و محافظت از آن	کنترل اطلاعات	هنجارهای سایبری بین‌المللی	غیرفعال‌سازی زیرساخت‌های دشمن	جمع‌آوری اطلاعات	افزایش توانایی سایبری و فنی ملی	دفاع سایبری ملی	رصد رایش داخلی	توضیح مطابقت اهداف
	مجموع	۴	۱۰	۸	۷	۸	۱۰	۹	۸	
۱	آگاهی از امنیت سایبری و خطرات					×	×	×		سنجش دانش جمعیت دربارهٔ امنیت سایبری به‌منظور دفاع مقابل حملات و انجام اقدامات سایبری ایمن.
۲	توافق‌های سایبری دوجانبه			×						تعریف هنجارهای سایبری بین‌المللی را می‌توان از این طریق سنجید که یک کشور چقدر در زمینهٔ ایجاد بیانیه‌های رسمی و غیررسمیِ همکاری بین‌المللی فعال بوده است.
۳	نرخ آلودگی رایانه‌ای							×		هرچه رایانه‌های بیشتری تحت‌تأثیر بدافزارهای خارج از حمایت دولت قرار گیرند، دفاع سایبری ملی احتمالاً آسیب‌پذیرتر باشد.
۴	پروژه‌های قابلیت‌سازی سایبری/ امداد رسانی خارجی			×						تعیین هنجارهای سایبری بین‌المللی را می‌توان از این طریق سنجید که یک کشور چقدر در زمینهٔ ترویج قابلیت‌های سایبری در کشورهای دیگر فعال بوده است.

۵	تأمین نیروی کار ارتش سایبری			×	×				تعداد کارکنانی را نشان می‌دهد که نقش سایبری آن‌ها در ارتش آشکارا اذعان شده است.
۶	قوانین امنیت سایبری					×		×	قوانین امنیت سایبری 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.
۷	قوانین و راهبردی محرمانگیِ داده‌ها								قوانین امنیت سایبری 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. ×
۸	اقتصاد تجارت الکترونیکی						×		فروش بیشتر تجارت الکترونیک امکان ورود سود بیشتر به خرده‌فروشان بخش خصوصی کشور را فراهم می‌آورد که باعث تقویت اقتصاد داخلی می‌شود.
۹	وجود گروه‌های واکنش به اختلال در امنیت سایبری							×	وجود این گروه‌ها نشان می‌دهد که کشور منابعی برای کاهش آسیب‌های سایبری و بحران‌های مرتبط فراهم کرده است.
۱۰	نمرهٔ آزادی در اینترنت		×						هرچه آزادی شهروندان کشوری در اینترنت کمتر باشد، احتمال بیشتری دارد که دولت بتواند شهروندان خود را رصد و پایش کند و گردش اطلاعات را کنترل نماید. ×
۱۱	قدرت نرم جهانی		×						کشور هرچه قدرت نرم بیشتری داشته باشد، بیشتر می‌تواند در زمینهٔ اتخاذ و حفظ هنجارهای بین‌المللی بر کشورهای دیگر تأثیر بگذارد.

۱۲	صد شرکت برتر فناوری در دنیا			×			×			شرکت‌های فناوری یک کشور باعث رشد صنعت داخلی می‌شوند و بر صنایع برون‌مرزی کشور تأثیر می‌گذارند، به‌خصوص اگر شرکت دارای کاربران خارجی زیادی باشد.
۱۳	۱۵۰ شرکت برتر دنیا در زمینهٔ امنیت سایبری				×	×	×	×		هر چه تعداد شرکت‌های امنیت سایبری که مقرشان در یک کشور است بیشتر باشد، صنعت امنیت سایبری بیشتر رشد می‌کند.
۱۴	حملات تأثیرگذار تحت حمایت دولت	×	×		×	×	×	×	×	منظور از حملات پیشرفته با حمایت دولت، حملاتی است که آژانس‌های دولتی یا شرکت‌های دفاعی و فناوری پیشرفته انجامش می‌دهند یا جرایم سایبری‌ای که میزان صدماتشان بیش از یک میلیون دلار است. این شاخص نیز، مانند شاخص کلی حملات تحت‌حمایت دولت، طرح و پیچیدگی کشور در دستیابی به اهدافش را می‌سنجد.
۱۵	صادرات فناوری پیشرفته			×	×	×	×			صادرات محصولات فناوری پیشرفته به کشورهای خارجی می‌تواند به اقتصاد کشور منفعت برساند و (بسته به کشورش) ممکن است سرویس اطلاعات خارجی را قادر به دسترسی به داده‌هایی کند که محصولات دربارهٔ 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.

۱۶	واردات فناوری اطلاعات و ارتباطات						×	×		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 احساس کند.
۱۷	نرخ آلودگی موبایل‌ها							×		هرچه گوشی‌های بیشتری تحت‌تأثیر بدافزارهای خارج از حمایت دولت قرار گیرند، دفاع سایبری ملی احتمالاً آسیب‌پذیرتر باشد.
۱۸	توافق‌های سایبری چندجانبه			×						تعیین هنجار سایبری بین‌المللی را می‌توان بر این اساس سنجید که یک کشور تا چه حد در ایجاد بیانیه‌های رسمی و غیررسمی مشارکت بین‌المللی فعال بوده است. توافق‌های چندجانبه ایجاد اجماع بین چند کشور را نشان می‌دهند.
۱۹	فرماندهی سایبری ملی				×					فرماندهی‌های سایبری مرکزی، به دولت‌های ملی این امکان را می‌دهند که چندین قابلیت سایبری را هماهنگ و بسیج کنند تا در صورت نیاز، از ابزار سایبری نظامی بهره بگیرند.
۲۰	درخواست ثبت امتیاز			×				×		هرچه تعداد درخواست‌های ثبت امتیاز در کشوری بیشتر باشد، نیروی کار آن کشور نوآوری بیشتری دارد که شاید به سود تجاری بینجامد.

۲۱	درصدی از جمعیت که در شبکه‌های اجتماعی حضور دارند		×							هرچه 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.
۲۲	درصدی از جمعیت که به اینترنت متصل‌اند		×					×	×	هرچه 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، جرایم سایبری یا تلاش برای جاسوسی سایبری هم بینجامد.
۲۳	شرکت‌های رصد بخش خصوصی		×		×	×	×			قابلیت‌های جدید رصد را یک کشور به‌طور فزاینده‌ای از شرکت‌های خصوصی می‌خرد تا فناوری‌های خود در زمینهٔ رهگیری و نفوذ را تقویت کند و برای اهداف اطلاعاتی و رصد به‌کار گیرد. شرکت‌های خصوصی هرچقدر بیشتر از این فناوری‌های رصد در یک کشور توسعه دهند، آن کشور دسترسی بیشتری به این فناوری‌ها دارد.
۲۴	حجم سازمان‌های استاندارد ملی			×						حجم سازمان‌های استاندارد ملی می‌تواند نشان دهد که چقدر توجه و تلاش صرف تعیین هنجارهای سایبری می‌شود.

۲۵	حملات تحت حمایت دولت	×	×			×	×	×		حملات سایبری با حمایت دولت، 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.
۲۶	درخواست‌های موفقِ حذف محتوا از گوگل		×							موفقیتِ بیشتر درخواست‌های حذف محتوا از گوگل، نشان می‌دهد که یک کشور به شیوه‌ای مؤثر اطلاعات را از اینترنت حذف کرده که نشان از مقدار کنترل بر فضای اطلاعاتی دارد.
۲۷	سایت‌های خبری برتر		×							وب‌سایت‌های خبری‌ای که بیشترین ترافیک بین‌المللی را دارند، به کشوری که مقرشان در آن است قدرت بیشتری می‌دهند تا از طریق اینترنت، روایت‌ها یا آرمان‌های متداول و محبوب در آن کشور را تقویت کند.
۲۸	سایت‌های برتر		×			×	×			وب‌سایت‌هایی که بیشترین ترافیک بین‌المللی را دارند به کشوری که مقرشان در آن است قدرت بیشتری می‌دهند تا از طریق اینترنت، روایت‌ها یا آرمان‌های متداول و محبوب در آن کشور را تقویت کند و شرکتِ مالک هر وب‌سایت را قادر به تولید سود تبلیغاتی بیشتر و ارائهٔ محصولات بیشتر به مصرف‌کنندگان می‌کند.
۲۹	آسیب‌پذیری‌های دستگاه‌های داخلی							×		هرچه رایانه‌های یک کشور آسیب‌پذیرتر باشد، کشور بیشتر در معرض حمله است.

د۲: تشریح نمره‌دهی شاخص‌های قابلیت

جدول ۱۵:

#	شاخص	معنا	منبع	سال	روش نمره‌دهی
۱	آگاهی از امنیت سایبری و خطرات	نمرهٔ کشورها در آگاهی از خطرات سایبری جهانی	انجمن اولیور وایمن	۲۰۲۱	نمرات را انجمن اولیور وایمن محاسبه کرده است. همین نمرات برای نمایهٔ قدرت سایبری بلفر استفاده شد.
۲	توافق‌های سایبری دوجانبه	تعداد و کیفیت توافق‌های رسمی یا غیررسمی دوجانبه‌ای که دولت ملی در فضای سایبری امضا کرده است. مبنای نمره‌دهی، جدیدبودن آن است.	پروژهٔ قدرت سایبری ملی بلفر، هاروارد	۲۰۲۲	برای هریک از توافق‌های میان کشورها: ۱ = جلسه/گفت‌وگو ۲ = بیانیهٔ مشترک/همکاری/چهارچوب ۳ = توافق/یادداشت تفاهم
۳	نرخ آلودگی رایانه‌ای	درصدی از رایانه‌های یک کشور که با بدافزار آلوده شده‌اند.	کمپاری‌تک	۲۰۲۱	درصد رایانه‌هایی که آلودگی بدافزاری در آن‌ها شناسایی شده است.
۴	پروژه‌های قابلیت‌سازی سایبری/امدادرسانی خارجی	تحلیل پروژه‌های قابلیت‌سازی سایبری بین‌المللی در گذشته و حال	پروژهٔ قدرت سایبری ملی بلفر، هاروارد	۲۰۲۲	پروژه‌های برشمرده در پرتال سیبیل را گروه نمایهٔ قدرت سایبری ملی بلفر تحلیل کرد. هرچه تعداد پروژه‌های قابلیت‌ساز سایبری بیشتر باشد، نمرهٔ کشور بالاتر است.
۵	تأمین نیروی ارتش سایبری	تعداد افراد شاغل در سمت‌های ثابت نیروهای ارتش سایبری	پروژهٔ قدرت سایبری ملی بلفر، هاروارد	۲۰۲۱	تعداد افرادی که طبق گزارش‌های منبع‌باز، در واحدهای سایبری ارتش‌ها کار می‌کنند.
۶	قوانین امنیت سایبری	سنجش اینکه کشور در اجرای قوانین محتوا و محرمانگی و جرایم سایبری چقدر فعال بوده است.	پروژهٔ قدرت سایبری ملی بلفر، هاروارد	۲۰۲۱	۰ = هیچ قانونی ۱ = قوانینی که فقط یکی از سه مورد (محتوا و محرمانگی و جرم) را پوشش می‌دهند ۲ = قوانینی که دو تا از این سه مورد را پوشش می‌دهند. ۳ = قوانینی که هر سه مورد را پوشش می‌دهند، اما منسوخ هستند (پیش از سال ۲۰۰۰) ۴ = قوانینی که هر سه مورد را پوشش می‌دهند و جدیداً روزآمد شده‌اند (سال ۲۰۰۰ و پس از آن).

۷	راهبری و قوانین محرمانگی داده‌ها	تحلیل قوانین محرمانگی داده‌ها در یک کشور	DLA Piper	۲۰۲۱	نمره‌دهی و تحلیل را DLA Piper انجام داد. هرچه نمره بالاتر باشد، تمهیدات قانونی برای محافظت از داده‌های شخصی بهتر است.
۸	اقتصاد تجارت الکترونیکی	فروش ملی تجارت الکترونیک به‌عنوان درصدی از تولید ناخالص داخلی	استاتیستا، UNCTAD و موارد دیگر	۲۰۲۱	نمرهٔ بالاتر به‌معنای فروش بیشترِ تجارت الکترونیکی است.
۹	وجود گروه‌های واکنش به اختلال در امنیت‌سایبری (تیم‌های سی‌اس‌آی‌آرتی)	وجود گروه واکنش به اختلال در امنیت سایبری	پروژهٔ قدرت سایبری ملی بلفر، هاروارد	۲۰۲۱	۰ = بدون گروه پاسخ‌گویی ۱ = قصد تأسیس سی‌اس‌آی‌آرتی ۲ = گروه سی‌اس‌آی‌آرتی ملی جدی (پنج سال یا کمتر) ۳ = گروه سی‌اس‌آی‌آرتیِ ملی نهادینه‌شده (بیش از پنج سال) ۴ = گروه سی‌اس‌آی‌آرتی ملی نهادینه‌شده (بیش از پنج سال) + عضویت در نخستین گروه پاسخ‌گویی
۱۰	آزادی در اینترنت	نمرهٔ خانهٔ آزادی به اینکه شهروندان چقدر در فضای اینترنت آزادند	خانهٔ آزادی و آزادی جهان	۲۰۲۱	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.
۱۱	قدرت نرم جهانی	نمرات کشورها در نمایهٔ قدرت نرم جهانی	برَندفایننس	۲۰۲۱	امتیازات محاسبه‌شده از سوی برند فایننس، بخشی از نمایهٔ قدرت نرمشان بود. همین امتیازات برای نمایهٔ قدرت سایبری بلفر استفاده شدند.
۱۲	صد شرکت برتر فناوری	تعدادی از شرکت‌های کشور که در میان صد شرکت برتر فناوری در جهان جای دارند	تامسون رویترز	۲۰۲۱	شمار شرکت‌های فناوری برتر برای هر کشور
۱۳	۱۵۰ شرکت برتر در زمینهٔ امنیت سایبری	تعدادی از شرکت‌های برتر امنیت سایبری در سطح جهان که مقرشان در کشور مدنظر است	شرکت‌های اجتماع سایبری	۲۰۲۱	تعدادی از ۱۵۰ شرکت برتر امنیت سایبری که در رده‌بندی برشمرده شده‌اند.

۱۴	حملات سایبری تأثیرگذار با حمایت دولت	تعداد حملات سایبری‌ای که به کسی نسبت داده شده‌اند.	مرکز مطالعات راهبردی و بین‌المللی (سی‌اس آی‌اس)	۲۰۲۲	شمار حملات سایبری منسوب به کنشگران تحت حمایت دولت
۱۵	صادرات فناوری پیشرفته	درصد صادرات فناوری پیشرفته در میان مجموع صادرات	بانک جهانی	۲۰۲۱	مقادیر بالاتر نشان‌دهندهٔ صادرات فناورانهٔ بیشتر است.
۱۶	واردات فناوری اطلاعات و ارتباطات	درصد واردات فناوری اطلاعات و ارتباطات در میان مجموع واردات	UNCTAD	۲۰۱۹	مقادیر بالاتر، نشان‌دهندهٔ وابستگی بیشتر به واردات است و دفاع سایبری کشور را بیشتر در معرض نفوذ دشمن قرار می‌دهد.
۱۷	نرخ آلودگی موبایل	درصد موبایل‌هایی در یک کشور که به بدافزار آلوده شده‌اند.	کمپاری‌تک	۲۰۲۱	درصد کاربرانی که رایانه‌هایشان دچار آلودگی به بدافزار شده است.
۱۸	توافق‌های سایبری چندجانبه	تعداد و کیفیتِ توافق‌های رسمی یا غیررسمی چندجانبه‌ای که دولت ملی در فضای سایبری امضا کرده است. مبنای نمره‌دهی، جدیدبودن آن است.	پروژهٔ قدرت سایبری ملی بلفر، هاروارد	۲۰۲۱	برای هریک از توافق‌های میان کشورها: ۱ = غیررسمی/همایش/منطقه‌ای ۲ = غیررسمی/همایش/جهانی ۳ = توافق رسمی منطقه‌ای/عضویت در سازمان منطقه‌ای ۴ = توافق رسمی چندجانبه/عضویت در سازمان جهانی
۱۹	فرماندهی سایبری مرکزی	وجود و سنِ فرماندهی سایبری ملیِ	پروژهٔ قدرت سایبری بلفر، هاروارد	۲۰۲۱	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)
۲۰	درخواست ثبت امتیاز	تعداد درخواست‌های ثبت امتیاز داخلی از سوی ساکنان یک کشور	شاخص‌های توسعهٔ جهانی	۲۰۱۹	تعداد درخواست‌های ثبت امتیاز داخلی (فقط ساکنان). سنجهٔ سرانه.
۲۱	درصد کاربران شبکه‌های اجتماعی	درصد حساب‌های فعال در شبکه‌های اجتماعی	استاتیستاو موارد دیگر	۲۰۲۱	درصد کاربران اینترنتی که از سایت‌های شبکه‌های اجتماعی دیدن می‌کنند

۲۲	درصد کاربران اینترنت	نرخ نفوذ اینترنت در هر کشور	استاتیستاو موارد دیگر	۲۰۲۱	هرچه بیشتر باشد، افراد بیشتری از اینترنت استفاده می‌کنند.
۲۳	شرکت‌های رسد بخش خصوصی	تعداد شرکت‌های رصد بخش خصوصی که مقرشان در کشور است و در نمایشگاه‌های بین‌المللی تسلیحات حضور می‌یابند	شورای آتلانتیک	۲۰۲۱	تعداد شرکت‌های رصدی که درون یک کشور فعالیت دارند و در نمایشگاه‌های بین‌المللی تسلیحات حضور یافته‌اند.
۲۴	حجم سازمان‌های استاندارد ملی	تعداد افراد شاغل در سازمان استاندارد ملی کشور	پروژهٔ قدرت سایبری ملی بلفر، هاروارد	۲۰۲۱	هرچه بالاتر باشد، افراد بیشتری در سازمان استاندارد ملی کشور کار می‌کنند.
۲۵	حملات تحت‌حمایت دولت	تعداد حملات سایبری‌ای که آشکارا به کسی نسبت داده شده است.	شورای روابط خارجی	۲۰۲۲	شمار حملات سایبری منسوب به کنشگران تحت‌حمایت دولت
۲۶	درخواست‌های موفق حذف محتوا از گوگل	تعداد درخواست‌های حذف محتوا از گوگل از سوی یک نهاد دولتی	گوگل	۲۰۲۱-۲۰۲۰	تعداد درخواست‌ها
۲۷	سایت‌های خبری برتر	تعداد سایت‌های خبری موجود در پنجاه وب‌سایت خبری برتر سیمیلاروب که مقرشان در یک کشور است.	سیمیلاروب	۲۰۲۱	تعداد سایت‌های موجود در پنجاه وب‌سایت برتر
۲۸	سایت‌های برتر	تعداد سایت‌های موجود در پنجاه وب‌سایت برتر سیمیلاروب که مقرشان در یک کشور است.	سیمیلاروب	۲۰۲۱	تعداد سایت‌های موجود در پنجاه وب‌سایت برتر
۲۹	آسیب‌پذیری‌های دستگاه‌های داخلی	درصد انبوهشی آسیب‌پذیری‌هایی که پایگاه داده Shodan برای زیرساخت‌های یک کشور برمی‌شمرد.	پروژهٔ قدرت سایبری ملی بلفر، هاروارد	۲۰۲۱	درصد انبوهشی نتایج جست‌وجوی Shodan.

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