وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

نظام پایش شاخص های فناوری اطلاعات و ارتباطات ایران
Measuring the Information Society of IRAN

شاخص جهانی امنیت سایبری

(فضای تولید و تبادل اطلاعات)

و رتبه بندی کشور های جهان
۲۰۱۴

برگرفته از مجموعه گزارشات منتشر شده توسط :

ABIresearch | Global Cybersecurity Index

ITU

خرداد ۱۳۹۴

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

نظام پایش شاخص های فناوری اطلاعات و ارتباطات ایران
Measuring the Information Society of IRAN

شاخص جهانی امنیت سایبری

(فضای تولید و تبادل اطلاعات)

و رتبه‌بندی کشورهای جهان

۲۰۱۴

برگرفته از مجموعه گزارشات منتشر شده توسط :

ABIresearch | Global Cybersecurity Index

ITU

خرداد ۱۳۹۴

سرشناسه	: سازمان فناوری اطلاعات ایران
عنوان و نام پدیدآور	: گزارش شاخص جهانی امنیت سایبری و رتبه بندی کشورهای جهان ۲۰۱۴/ طرح تدوین طرح جامع فناوری اطلاعات کشور؛ ؛ مرکز برنامه ریزی و نظارت راهبردی فناوری اطلاعات سازمان فناوری اطلاعات ایران،
مشخصات نشر	: تهران: دانشگاه تربیت مدرس، مرکز نشر آثار علمی، ۱۳۹۴.
مشخصات ظاهری	: و ، ۲۹ ص.: صور(رنگی)، جدول(رنگی)، نمودار(رنگی).
شابک	:
وضعیت فهرست نویسی	: فیپا
یادداشت	: عنوان اصلی: .The Global Cybersecurity Index (GCI) 2014
یادداشت	:
موضوع	: تکنولوژی اطلاعات و ارتباطات
موضوع	: تکنولوژی اطلاعات -- جنبه‌های امنیت فضای مجازی
موضوع	: تکنولوژی اطلاعات -- جنبه‌های امنیت فضای تولید و تبادل اطلاعات
موضوع	: جامعه اطلاعاتی
شناسه افزوده	: دانشگاه تربیت مدرس
رده بندی کنگره	:
رده بندی دیویی	:
شماره کتابشناسی ملی	:

سایبری و رتبه بندی کشورهای جهان ۲۰۱۴ گزارش شاخص جهانی امنیت

The Global Cybersecurity Index (GCI)- 2014

- مجری طرح : نصراله جهانگرد

گروه مترجمین : امیرحسین محب‌علی، صبا حسینیون، فریبا حسنی

- طراحی جلد: سید محمدعلی اعتصامی
- ناشر: دانشگاه تربیت مدرس، مرکز نشر آثار علمی

تعداد صفحات : ۲۹

- نوبت چاپ: اول
- شمارگان: ۵۰۰
- سال چاپ: ۱۳۹۴
- هزینه: رایگان، غیرقابل فروش

پیشگفتار

اندازه‌گیری شاخص جهانی امنیت سایبری (GCI) به طور موثر سطح توسعه امنیت فضای تولید و تبادل اطلاعات در هرکشور را نشان می‌دهد و هدف نهایی آن کمک به ترویج فرهنگ جهانی امنیت سایبری و ادغام آن در هسته فناوری اطلاعات و ارتباطات(ICT) است. این اندازه‌گیری در چارچوب روال‌های اندازه‌گیری اتحادیه بین‌المللی مخابرات (ITU) و پروژه‌های مرتبط و فعالیت‌های دفتر توسعه مخابراتITU ، BDT است. در این قالب کشورها تلاش می‌کنند تا با اجرای برنامه‌های کلان در این حوزه نسبت به ارتقاء وضعیت فناوری اطلاعات و ارتباطات در کشورشان اقدام نمایند.

ITU به عنوان تسهیل‌کننده هدایت جهانی در نیل به اهداف خط عملC5 WSIS (اجلاس جهانی جامعه اطلاعاتی) در کمک به ذینفعان در ایجاد اطمینان و امنیت در استفاده از ICT در سطوح ملی، منطقه‌ای و بین‌المللی است .در این چارچوب، دستور کار جهانی امنیت (GCA) توسط دبیر کل ITU به عنوان چارچوبی برای همکاری ذی نفعان بین‌المللی در جهت توسعه جامعه اطلاعاتی امن‌تر و بی‌خطرتر و با تمرکز بر پنج حوزه‌ی کاری به شرح ذیل تبیین شده است:

- اقدامات قانونی،
- اقدامات فنی و روندی،
- ساختارهای سازمانی،
- ظرفیت‌سازی
- همکاری‌های بین‌المللی.

این پنج بخش تعیین شده فوق چارچوب اندازه‌گیری شاخص‌ها را برای GCI تشکیل می‌دهند. اندازه‌گیری شاخص جهانی امنیت سایبری تلاش مشترک بین دفتر توسعه مخابرات BDT اتحادیه جهانی مخابرات ITU و بخش امنیت سایبری و برنامه‌های کاربردی ICT (CYB) موسسه تحقیقاتی .ABI است.

براساس تکلیف تبصره ۳ ماده ۴۶ قانون برنامه پنجم توسعه جمهوری اسلامی ایران، وزارت ارتباطات و فناوری اطلاعات می‌تواند جهت ارزیابی شاخص‌ها و وضعیت کشور در ابعاد ملی، منطقه‌ای و بین‌المللی، نظام پایش شاخص‌های فناوری اطلاعات و ارتباطات را تدوین و به صورت سالیانه نتایج ارزیابی و پایش را به مراجع فرادست اعلام نماید.

سازمان فناوری اطلاعات ایران به عنوان بازوی اجرایی وزارت ارتباطات و فناوری اطلاعات در حوزه فناوری اطلاعات در کشور، با درک اهمیت این موضوع نسبت به پیگیری روند ارزیابی شاخص‌های فناوری اطلاعات کشور در ارزیابی‌های بین‌المللی اقدام نموده است. به همین دلیل سازمان فناوری اطلاعات ایران از سوی وزارت ارتباطات و فناوری اطلاعات به عنوان مجری نظام پایش شاخص‌های فناوری اطلاعات و ارتباطات کشور تعیین شده است. همچنین در چارچوب تعامل سازمان فناوری اطلاعات ایران با بخش آمار و اطلاعات اتحادیه جهانی مخابرات، مسئولیت هماهنگ‌کننده ملی را سازمان مذکور عهده‌دار می‌باشد و در جهت ظرفیت‌سازی فنی در راستای ارتقای جایگاه فناوری اطلاعات و ارتباطات کشور در ارزیابی‌های مجامع بین‌المللی اقدام می‌نماید.

گزارش The Global Cybersecurity Index (GCI) که آخرین ارزیابی ITU از وضعیت توسعه کشورها از منظر امنیت فضای سایبری می‌باشد در سال ۲۰۱۴ منتشر شده است. متاسفانه این گزارش به صورت یک مجلد متمرکز و منسجم از سوی ITU منتشر نشده است و شامل گزارشاتی مجزا می‌باشد. به جهت اهمیت موضوع امنیت سایبری و اولین ارزیابی جهانی در این حوزه، مجری نظام پایش شاخص‌های فناوری اطلاعات کشور از بین بیش از ۲۰ گزارش پروژه ای مرتبط برخی را انتخاب، ترجمه، تلفیق و به صورت یک گزارش منسجم جهت بهره‌برداری ذینفعان این حوزه در کشور آماده کرده است.

این گزارش به عنوان یکی از خروجی‌های نظام پایش شاخص‌های فناوری اطلاعات و ارتباطات از طریق درگاه پایش جامعه اطلاعاتی ایران به آدرس mis.iran.ir برای کلیه فارسی زبانان در جهان نیز قابل دسترس خواهد بود.

و در خاتمه جا دارد از جناب آقای دکتر واعظی مقام عالی وزارت ارتباطات و فناوری اطلاعات و سایر معاونین ارجمند وزارت، که با حمایت‌ها و رهنمودها، این سازمان را همواره مورد لطف قرار داده‌اند کمال تشکر را داشته باشیم. همچنین از تمام عزیزانی که در تهیه و انتشار این مستند به خصوص همکاران شاغل در مرکز برنامه‌ریزی و نظارت راهبردی سازمان فناوری اطلاعات ایران به عنوان مجری نظام پایش شاخص‌های فناوری اطلاعات و ارتباطات کشور و مشاورین مجری در بخش خصوصی و دانشگاهی کشور تلاش نموده‌اند، تشکر و قدردانی می‌شود.

سازمان فناوری اطلاعات ایران

فهرست مطالب

مقدمه

امنیت سایبری (فضای تولید و تبادل اطلاعات) یک مسئله حیاتی برای پشتیبانی از اقتصاد دیجیتال، برای مبارزه با جرایم سایبری و برای حمایت از توسعه و سرمایه‌گذاری است.

أ. نقش اتحادیه بین‌المللی مخابراتITU در اندازه‌گیری شاخص امنیت سایبری

برای بهره‌مند شدن از امکانات یک تشکل ساختاریافته بین‌المللی

برای توسعه یک چارچوب اطمینان بخش ملی پایدار

برای سهیم شدن و به اشتراک گذاشتن اطلاعات و"بهترین روش‌ها[۱]" با سایر کشورها

ب. نقش موسسه پژوهشی ABI

بکارگیری راهکار فرابخشی و مشارکت‌های دولت و بخش خصوصی

بهره‌برداری از دانش کاربردی صنعتی و توسعه فرصت‌های سرمایه‌گذاری تجاری

دریافت مشاوره حرفه ای و تخصصی از جانب یکی از موسسات پژوهشی راهبردی ذی ربط

مشارکت در توسعه شاخص امنیت سایبری بین‌المللی به منظور توسعه امنیت سایبری در کشورها بوده که پرسشنامه کشوری و چارچوب مفهومی برای شاخص امنیت سایبری بین‌المللی در وبگاه زیر قابل دسترسی است:

http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

سازمان‌های مسئول راهبری این پایش اتحادیه بین‌المللی مخابرات – معاونت امنیت سایبری و بخش کاربردهای فناوری اطلاعات و ارتباطات و موسسه پژوهشی ABI بخش پژوهش‌های کاربردی امنیت سایبری با مشارکت IMPACT (تهدیدات مشارکت بین‌المللی چند جانبه علیه سایبر) و متحدان تابعه و شرکای همکار می‌باشند.

[۱] best practices

۱. **اطلاعات تماس به شرح ذیل است :**

- اتحادیه بین‌المللی مخابراتInternational Telecommunication Union

مارکو اوبیسو هماهنگ‌کننده امنیت سایبریmarco.obiso@itu.int

- موسسه پژوهشی ای بی آی ABI Research

میشلا منتینگ رئیس بخش کاربرد menting@abiresearch.com

آرون بوید رئیس کل بخش استراتژی boyd@abiresearch.com

استوارت کارلا رئیس کل بخش پژوهشcarlaw@abiresearch.com

- GCI Website

وبگاه شاخص جهانی امنیت سایبری http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

اهداف

هدف نهایی از تدوین و اجرای شاخص جهانی امنیت سایبری سنجش و رتبه بندی میزان توسعه‌یافتگی امنیت سایبری در سطح هر کشور است که در قالب ۴ زیر بخش قابل تقسیم می‌باشد.

تقویت راهبرد های دولت ها در سطح ملی

یاری دادن به تلاش های مربوط در طیف صنایع و بخش های ذی ربط

ادغام امنیت با کانون پیشرفت های فناورانه

اشاعه و تقویت یک فرهنگ جهانی درباره امنیت سایبری

اهمیت شاخص بین‌المللی امنیت سایبری

شاخص بین‌المللی امنیت سایبری می‌تواند برای انجام فعالیت‌های زیر یاری رساند:

- پیاده‌سازی ساز و کارهای حقوقی برای مبارزه با جرایم سایبری و تقویت امنیت سایبری
- توسعه و ایجاد مراکز ملی با توان اجرایی و قانونی CERT[۱]/CSIRT[۲]
- تدوین راهبرد امنیت سایبری ملی و نقشه راه دقیق
- اختصاص یک سازمان ملی به عنوان مسئول امنیت سایبری
- حمایت از توسعه حرفه ای، برنامه‌های آموزشی و یاددهی – یادگیری به منظور ارتقاء میزان آگاهی عمومی
- اشاعه مشارکت‌های بخش‌های دولتی و خصوصی
- انجام همکاری‌های بین‌المللی، تبادل و سهیم شدن دراطلاعات

چارچوب مفهومی

نظام شاخص بین‌المللی امنیت سایبری از مجموع ۵ گروه نشانگر تشکیل شده است:

۱. قانونی /حقوقی

- ✓ حقوق جزایی
- ✓ قوانین، مقررات و تبعیت از آنها

۲. فنی

- ✓ CIRT[۳] تیم پاسخگویی رخدادهای رایانه ای، CERT گروه واکنش اضطراری رایانه و CSIRT تیم پاسخگویی حوادث امنیتی رایانه ای

---

۱ Computer Emergency Response Team گروه واکنش اضطراری رایانه

۲ Computer Security Incident Response Team تیم پاسخگویی حوادث امنیتی رایانه ای

۳ Computer Incident Response Team تیم پاسخگویی رخدادهای رایانه ای

- ✓ استانداردها
- ✓ گواهی نامه‌ها

۳. سازمانی

- ✓ سیاست‌ها
- ✓ نقشه راه برای حکمرانی
- ✓ بنگاه مسئول و پاسخگو
- ✓ الگوبرداری ملی

٤. ظرفیت‌سازی

- ✓ توسعه استانداردها
- ✓ توسعه نیروی انسانی
- ✓ صدور گواهینامه‌های حرفه ای
- ✓ صدور گواهینامه‌های سازمانی

۵. مشارکت و همکاری

- ✓ مشارکت و همکاری درون دولت
- ✓ مشارکت و همکاری درون سازمانی
- ✓ مشارکت و همکاری بین دولت و بخش خصوصی
- ✓ مشارکت و همکاری بین‌المللی

تعاریف و دسته‌بندی‌های شاخص جهانی امنیت سایبری

شاخص جهانی امنیت سایبری معیار رتبه بندی پایش قابلیت‌های توسعه امنیت سایبری در کشورها می‌باشد. این شاخص اساساً یک نشانگر ترکیبی از تجمیع تعدادی از شاخص‌های فردی است. روند توسعه امنیت سایبری می‌توان به پنج دسته گسترده مهم تفکیک کرد. نشانگرها و زیر گروه‌ها زیر کشورها را مورد سنجش قرار خواهند گرفت.

أ. اقدامات قانونی

تنظیم مقررات معیاری حیاتی در ارائه یک چارچوب هماهنگ برای کشورها است تا خودشان را با مقررات مشترک پایه همسو کنند، اگرچه در ماده منع رفتار کیفری و یا حداقل الزامات، قانونی مشخص شده باشد. تدابیر حقوقی نیز به دولت کشورها اجازه می‌دهد

تا با نوشتن مکانیسم‌های اساسی پاسخگویی برای شکستن موانع از طریق تحقیقات و تعقیب قانونی جرایم و اعمال تحریم به سبب عدم رعایت یا نقض قانون اقدام کنند. یک چارچوب قانونمند حداقل استانداردهای رفتاری را در سطح کل، و قابل اعمال برای همه، که در آن قابلیت‌های امنیت سایبری بیشتری می‌تواند ایجاد گردد، تنظیم می‌کند.

در نهایت، هدف توانمند ساختن تمام دولت‌ها با تنظیم مقررات مناسب در آن کشور به منظور هماهنگ‌سازی اقدامات فراملی و با ارائه یک مجموعه اقدامات سازگار، که مقابله بین‌المللی با جرایم اینترنتی را تسهیل کند.

یک محیط حقوقی می‌تواند بر اساس وجود و تعداد موسسات حقوقی و چارچوبشان در برخورد با مسائل امنیتی سایبری و جرم‌های رایانه ای اندازه‌گیری شود. زیر گروه‌ها از شاخص‌های عملکردی زیر تشکیل شده است:

۱. حقوق جزایی

قوانین جرایم اینترنتی قوانین مربوط به دسترسی غیر مجاز (بدون حقوق کیفری)، تداخل، رهگیری کامپیوتری، سیستمی و داده‌ها را تعیین میکند :قوانین را می‌توان در سطح‌های زیر رتبه بندی کرد: فاقد، جزئی یا جامع.

قوانین جزئی اشاره دارد به درج ساده ای از عبارات مربوط به کامپیوتر که در قوانین کیفری و یا در آیین نامه‌ها موجود است، به عنوان مثال تقلب، جعل و یا نظارت و سرقت در فضای مجازی.

تنظیم مقررات جامع به تصویب قانون یا اعمال اختصاصی در برخورد با جنبه‌های خاص از جرائم کامپیوتری اشاره دارد (مثلا رفتار سو استفاده کامپیوتری انگلیس ۱۹۹۰). این رده می‌تواند شامل یک سری قوانین جزئی باشد که در آن به صورت موردی، آن قانون توسعه یافته شده باشد. در این بخش کشورها نوع قوانین و مقررات را مشخص کرده و تعیین می‌کنند که جزو کدام دسته‌بندی فاقد، جزئی و یا جامع هستند.

۲. قوانین، مقررات و تبعیت از آنها

مقررات حاکم بر امنیت فضای سایبری در ارتباط با حفاظت از اطلاعات، نقض اطلاع‌رسانی و الزامات گواهینامه / استاندارد تعیین شده است. قوانین را می‌توان در سطح‌های زیر رتبه بندی کرد: فاقد، جزئی یا جامع.

قوانین جزئی اشاره به درج عبارت مربوط به کامپیوتر در قانون کیفری یا مدنی موجود و یا جدید دارد، به طوری که قانون به صورت کاربردی در فضای مجازی در تنظیم مواردی که به طور خاص به امنیت سایبری مربوط نیستند، توسعه داده می‌شود. (مثلا قوانین اتحادیه اروپا EU[۱] در رابطه با 95/46/EC در حمایت از افراد با توجه به پردازش اطلاعات شخصی و انتقال آزادانه چنین داده‌هایی). مقررات جامع اشاره دارد به تصویب قانون تختصیص داده شده، اعمال یا بخشنامه‌ای که امنیت سایبری به آن نیازمند است. در این بخش کشورها نوع قوانین و مقررات را مشخص کرده و تعیین می‌کنند که جزو کدام دسته‌بندی فاقد، جزئی و یا جامع هستند.

[۱] European Union

ب. اقدامات فنی

فناوری اولین خط دفاع در برابر تهدیدات سایبری و عوامل مخرب برخط (آنلاین) است. بدون اقدامات فنی کافی و داشتن توانایی برای شناسایی و پاسخ به حملات سایبری، دولت‌های ملی و نهادهای مربوطه نسبت به تهدیدات سایبری آسیب پذیر باقی می‌ماند. ظهور و موفقیت فناوری اطلاعات و ارتباطات تنها در یک فضای اعتماد بخش و امن قابل تحقق است. بنابراین دولت‌های ملی باید توانایی توسعه راهبردهایی برای ایجاد معیارهای حداقل امنیت و طرح مجوز رسمی برای نرم افزارهای کاربردی و سیستمها را داشته باشد. این تلاش‌ها باید توسط ایجاد یک نهاد ملی با تمرکز بر مقابله با حوادث سایبری در سطح ملی، حداقل با یک سازمان دولتی مسئول و با یک چارچوب ملی همراه برای نظارت، هشدار و پاسخ به رخدادها همراه باشد.اقدامات فنی را می‌توان بر اساس وجود و تعداد موسسات فنی و چارچوب آنها که در ارتباط با برخورد با امنیت سایبری هستند و توسط دولت ملی تایید و یا ایجاد شده، انجام داد. زیر گروه‌ها بر اساس شاخص‌های عملکرد زیر تشکیل شده است:

۱. CERT/CIRT/CSIRT

CIRT تیم پاسخگویی رخدادهای رایانه ای، CERT تیم پاسخگویی امداد رایانه ای و CSIRT تیم پاسخگویی حوادث امنیتی رایانه ای است. استقرار این گروه‌های ملی باعث تامین قابلیت شناسایی، دفاع، پاسخ و مدیریت تهدیدات سایبری و افزایش امنیت فضای مجازی در دولت‌ها شده است. این قابلیت باید با جمع آوری اطلاعات خود، به جای تکیه بر گزارش ثانویه از حوادث امنیتی که آیا از حوزه CIRT است یا از منابع دیگر همراه شود. در این بخش کشورها نام و تعداد تیم‌های دارای تائیدیه رسمی ملی و یا تیمهای بخش خاصCERT یاCSIRT را مشخص کرده و تعیین می‌کنند آیا آنها که از نظر قانونی موظف هستند یا نه.

۲. استانداردها

این شاخص وجود یک چارچوب مورد تایید دولت را برای اجرای استانداردهای امنیت سایبری (که در سطح بین‌المللی شناخته شده) در بخش عمومی و در زیرساخت‌های حیاتی، اندازه‌گیری می‌کند.(حتی اگر توسط بخش خصوصی انجام شود). این استانداردها دربرگیرنده (اما نه محدود به) ارگان‌های زیر هستند: ISO [۱], ITU[۲], IETF[۳], IEEE[۴], ATIS[۵], OASIS[۶], 3GPP[۷], 3GPP2[۸], IAB[۹], ISOC[۱۰], ISG[۱۱], ISI, ETSI[۱۲], ISF[۱۳], RFC[۱۴], ISA[۱۵], IEC[۱۶], NERC[۱۷], NIST[۱۸], FIPS[۱۹], PCI DSS[۲۰],. .

در این شاخص کشورها هر گونه چارچوبهای رسما تایید شده ملی برای اجرای استانداردهای امنیت سایبری که در سطح بین‌المللی شناخته شده را مشخص می‌کنند.

۳. گواهی نامه‌ها

این شاخص وجود یک چارچوب مورد تایید دولت را برای صدور گواهینامه و مجوز رسمی از سازمان‌های ملی و حرفه ای بخش دولتی با استانداردهای امنیت سایبری شناخته شده بین‌المللی سنجش می‌کند. این گواهی نامه، مجوز و استانداردها شامل (اما نه محدود به) به موارد زیر هستند:

CISSP[۲۱], SSCP[۲۲], CSSLP CBK[۲۳], (ISC²), GIAC[۲۴], GIAC GSSP (SANS), CISM[۲۵], CISA[۲۶], CRISC (ISACA)[۲۷], CompTIA[۲۸], C|CISO, CEH[۲۹], ECSA[۳۰], CHFI (EC Council)[۳۱], OSSTMM (ISECOM), PCIP[۳۲]/CCISP,Q/ISP[۳۳], CPP[۳۴], PSP[۳۵], PCI (ASIS)[۳۶], LPQ[۳۷], CFE[۳۸] ,CERT (SEI), CSFA[۳۹], CIPP (IAPP)[۴۰],

ABCP[۴۱], CBCP[۴۲], MBCP (DRI)[۴۳], BCCP[۴۴], BCCS[۴۵], BCCE[۴۶], DRCS[۴۷], DRCE (BCM)[۴۸], CIA[۴۹], CCSA[۵۰], PMP[۵۱] …

در این شاخص کشورها هر گونه چارچوب ملی به طور رسمی تایید برای صدور گواهینامه و مجوز رسمی از سازمان‌های ملی و حرفه ای بخش دولتی را مشخص می‌کنند.

ت. سنجش سازمانی

اندازه‌گیری سازمان و رویه‌های آن برای اجرای مناسب هر گونه ابتکار ملی ضروری هستند. بدین منظور یک هدف راهبردی کلان با یک طرح جامع در پیاده‌سازی، تحویل و اقدام باید توسط دولت تنظیم شود. ساختارهایی مانند سازمان‌های ملی به منظور اجرایی کردن استراتژی‌ها و ارزیابی موفقیت یا شکست طرح باید در جای خود قرار داده شوند. بدون یک راهبرد ملی، الگوی حاکمیت و بدنه نظارت، تلاش‌ها در بخش‌های متفاوت و صنایع به صورت منفک و جدا از هم در خواهند آمد که این کار سبب خنثی شدن تلاش‌ها برای رسیدن به هماهنگی ملی از منظر قابلیت توسعه امنیت سایبری خواهد بود.

ساختارهای سازمانی را می‌توان بر اساس موجودیت و تعداد موسسات و راهبردهای سازماندهی توسعه امنیت در سطح ملی سنجش نمود. ایجاد ساختارهای سازمانی موثر برای ارتقاء امنیت سایبری، مبارزه با جرایم رایانه ای و ترویج نقش نظارت، هشدار و عکس‌العمل هنگام رخداد برای تضمین درون تشکیلات، بخش‌های متقاطع و هماهنگی مرزی بین طرح‌های موجود و جدید لازم است.

زیر گروه‌ها برمبنای شاخص‌های عملکرد این بخش به شرح زیر است:

۱. سیاست

توسعه یک خط مشی برای پیشبرد امنیت سایبری به عنوان یک اولویت شناخته شده است .یک راهبرد ملی برای امنیت شبکه و سیستم‌های اطلاعاتی باید دارای زیرساخت‌های اطلاعاتی انعطاف‌پذیر و قابل اعتماد باشد که با هدف اطمینان از ایمنی شهروندان، محافظت از اجسام و دارایی‌های ذهنی شهروندان، سازمان‌ها و دولت، جلوگیری از حملات سایبری علیه زیرساخت‌های حیاتی و به حداقل رساندن آسیب و زمان بازیابی از حملات سایبری بوجود آمده است.

سیاست‌ها در استراتژی ملی امنیت سایبری یا برنامه‌های ملی برای حفاظت از زیر ساخت‌های اطلاعاتی، مواردی هستند که به طور رسمی تعریف شده و توسط یک دولت ملی تایید شده است و می‌تواند شامل تعهدات زیر باشد :

ایجاد مسئولیت روشنی برای امنیت سایبری در تمام سطوح (دولت، محلی، منطقه‌ای و فدرال و یا ملی) با تعریف صریحی از نقش‌ها و مسئولیت‌ها، ایجاد یک تعهد روشن برای امنیت سایبری که عمومی و شفاف باشد و تشویق همکاری بخش خصوصی و مشارکت در طرح‌ها به رهبری دولت برای پیشبرد امنیت سایبری.

۲. شیوه حاکمیت

نقشه راه حاکمیت در امنیت سایبری به طور کلی توسط یک استراتژی/ سیاست ملی برای امنیت سایبری ایجاد میگردد و ذینفعان کلیدی را شناسایی می‌کند. توسعه یک چارچوب سیاست‌های ملی یک اولویت در توسعه حکمرانی در سطح بالا برای امنیت سایبری است. چارچوب سیاست‌های ملی باید نیازهای حفاظت از زیرساخت‌های اطلاعاتی ملی و حیاتی را شامل شود. همچنین باید به دنبال

ارتقائ اشتراک گذاری اطلاعات در میان بخش‌های دولتی و خصوصی و همچنین بین بخشی دولتی باشد. اداره امنیت سایبری باید در یک چارچوب ملی با پرداختن به چالش‌ها و امنیت اطلاعات و شبکه در سطح ملی، که می‌تواند شامل موارد زیر باشد، ایجاد گردد:

استراتژی و سیاست ملی؛ بنیانهای حقوقی برای انتقال قوانین امنیتی به محیطهای برخط (آنلاین) و شبکه ای ؛ مشارکت تمام ذینفعان .توسعه یک فرهنگ برای امنیت سایبری .متدلوژی برای پرداختن به نقض امنیت ICTو مدیریت حادثه (گزارش‌گیری، به اشتراک‌گذاری اطلاعات، مدیریت هشدارها، همکاری دادگستری و پلیس)، اجرای موثر سیاست امنیت سایبری ملی، کنترل برنامه‌های امنیتی سایبری، ارزیابی، اعتبارسنجی و بهینه‌سازی.

۳. سازمان مسئول

سازمان مسئول برای اجرای یک راهبرد امنیت سایبری/ سیاست ملی می‌تواند شامل کارگروه‌های دائمی، کارگروه‌های رسمی، شوراهای مشورتی و یا مراکز متقابل انضباطی باشد. اکثر سازمان‌های ملی به طور مستقیم مسئول نظارت و سیستم‌های هشدار دهنده و پاسخگوی رخدادها خواهند بود. برای توسعه ساختار سازمانی، هماهنگی پاسخ به حملات سایبری مورد نیاز خواهد بود.

۴. الگوبرداری کشوری

این شاخص وجود هر گونه معیار به رسمیت شناخته ملی یا در بخشی خاص که فعالیت‌ها یا ارجاعات الگوبرداری شده که سابقا برای سنجش توسعه امنیت سایبری بکار برده می‌شود را اندازه‌گیری می‌کند.

به عنوان مثال، بر اساس ISO / IEC 27002-2005، یک استاندارد امنیت ملی (NCSecu) می‌تواند به دولت‌های ملی برای تشخیص نیازهای امنیت سایبری کمک کند. این ارجاع به پنج حوزه تقسیم می‌شود:

- استراتژی و سیاست NCSecu.
- ساختارهای‌های سازمانیNCSecu ،
- اجرای NCSec،
- هماهنگی ملی
- فعالیت‌های آگاه‌کننده امنیت سایبری

کشورها در این بخش هرگونه اقدام سنجشی (الگوبرداری) یا استنباطی سایبری به رسمیت شناخته شده ی ملی یا بخشی که سابقاً جهت اندازه‌گیری توسعه امنیت سایبری استفاده می‌شود را مشخص و اعلام می‌نمایند.

ث. ظرفیت‌سازی

ظرفیت‌سازی در سه اقدام اولیه (حقوقی، فنی و سازمانی) ذاتی می‌باشد. درک از فناوری، مخاطرات و الزامات آن می‌تواند در بهبود قانون گذاری بهتر، سیاست‌ها، راهبردها و سازماندهی بهتر مرتبط با نقش‌ها و مسئولیت‌های مختلف کمک نماید. امنیت سایبری یک بحث نسبتا جدید است که از خود بحث شبکه اینترنت قدیمی تر نیست.

این حوزه مطالعه ای اغلب با جنبه‌های فنی سر و کار دارد. هنوز مفاهیم اجتماعی – اقتصادی و سیاسی متعددی موجود است که در این زمینه کاربرد دارد. به منظور ارتقاء دانش و چگونگی گسترش آن در سرتاسر بخش‌ها، به کار بردن راه حل‌های مناسب و ترویج توسعه شایستگی حرفه ای ظرفیت‌سازی نیروی انسانی و سازمانی لازم است.

چارچوب ظرفیت‌سازی برای ارتقاء امنیت سایبری باید شامل افزایش آگاهی‌ها و در دسترس بودن منابع شود. ظرفیت‌سازی را می‌توان بر اساس موجودیت و تعداد فعالیت‌های تحقیق و توسعه ای، برنامه‌های آموزش و پرورش، متخصصان تایید شده و سازمان‌ها در بخش دولتی سنجش نمود. زیر شاخه‌های این بخش از شاخص‌های عملکرد مشتمل بر زیر.

۱. توسعه استاندارد

استاندارد شاخص خوبی از سطح بلوغ یک فناوری است، و ظهور استانداردهای جدید در زمینه‌های کلیدی و با تاکید بر اهمیت حیاتی استاندارد را شامل می‌شود. اگر چه امنیت سایبری همواره یک مسئله برای امنیت ملی بوده است و در کشورهای مختلف رفتارهای متفاوتی با آن صورت گرفته است، با این وجود رویکردهایی مشترک با استانداردهای معمول به رسمیت شناخته شده پشتیبانی می‌شوند. این استانداردها شامل، نه محدود، به ارگان‌های زیر می‌شوند:

ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS.. و سایر.

در این بخش کشورها هر گونه سازماندهی ملی و تحقیق و توسعه ای و استانداردهای امنیت سایبری را به تفکیک بخش‌های عمومی و خصوصی مشخص می‌کنند.

۲. توسعه نیروی انسانی

توسعه نیروی انسانی باید معرف تلاش‌های دولت‌ها برای ترویج کمپین گسترده تبلیغاتی برای رسیدن به تعداد هرچه بیشتر مردم و همچنین استفاده از سازمان‌های غیر دولتی، نهادها، سازمان‌ها، سرویس دهندگان اینترنت، کتابخانه‌ها، سازمان‌های تجاری محلی، مراکز انجمن‌ها، فروشگاه کامپیوتر، انجمن کالج‌ها و برنامه‌های آموزش و پرورش بزرگسالان، مدارس و سازمان‌های اولیا و مربیان باشد که هدف آن انتقال حس امن در رفتار سایبری برخط (آنلاین) است.

این شامل اقداماتی از قبیل راه اندازی درگاه‌های اینترنتی (پورتال) و وب سایت برای ترویج آگاهی، انتشار موارد پشتیبانی برای مربیان و ایجاد دوره‌های آموزشی حرفه ای و برنامه‌های آموزش و پرورش است.

در این بخش کشورها برنامه‌های آموزشی را در حوزه امنیت سایبری را به صورت هفتگی و ماهیانه مشخص می‌کنند.

۳. صدور گواهینامه‌های حرفه ای

این شاخص عملکردی را می‌توان از طریق تعدادی از متخصصان بخش دولتی که تحت برنامه‌های استاندارد صدور گواهینامه بین‌المللی که شامل موارد ذیل می‌شوند و تایید شده اند مورد ارزیابی قرار داد (البته تنها محدود به این موارد نمی‌شود):

- ابر امنیتی دانش (معاهده ابر امنیتی)، CISSP، SSCP، CSSLP CBK،

- تحلیل گر قانونی امنیت سایبری (ISC²)، GIAC، GIAC GSSP (SANS)، CISM، CISA، CRISC (ISACA)، CompTIA، C|CISO، CEH، ECSA، CHFI (EC Council)، OSSTMM (ISECOM)، PCIP/CCISP(موسسه زیرساخت‌های حیاتی)،
- صدور گواهینامه، Q/ISP،
- صدور گواهینامه مهندسی امنیت نرم افزار(دانشگاه امنیت)، CPP، PSP، PCI (ASIS)، LPQ، LPC(موسسه پیشگیری از زیان، CFE(انجمن خبره تخلف بازرسان)، CERT
- صدور گواهینامه مربی حوادث امنیتی کامپیوتر (SEI))، CITRMS(گواهی تحصیلات مالی مصرف‌کننده)، CSFA(موسسه امنیت سایبری)، CIPP (IAPP)، ABCP، CBCP، MBCP (DRI)، BCCP، BCCS، BCCE، DRCS، DRCE (BCM)، CIA، CCSA(موسسه حسابرسان داخلی)، (مدیران ریسک حرفه ای انجمن بین‌المللی)، PMP(موسسه مدیریت پروژه)

در این بخش کشورها تعدادی از گواهینامه‌های حرفه ای در بخش دولتی که تحت برنامه‌های صدور گواهینامه‌های بین‌المللی تایید شده اند را مشخص می‌کنند.

۴. نمایندگی صدور گواهینامه

این شاخص عملکردی را می‌توان از طریق تعدادی از گواهی‌های دولتی و آژانس‌های بخش دولتی که از طریق استانداردهای رسمی بین‌المللی تایید شده اند مورد ارزیابی قرار داد، این استانداردها شامل: (اما تنها محدود به نمایندگی‌های ذیل نمی‌شود):

ISO ، ITU، IETF، IEEE، ATIS، OASIS، 3GPP، 3GPP2، IAB، ISOC، ISG، ISI، ETSI، ISF، RFC، ISA، IEC، NERC، NIST، FIPS، PCI DSS و غیره.

در این بخش کشورها تعدادی از گواهینامه‌های بخش دولتی و سازمانهای بخش دولتی که تحت استانداردهای رسمی بین‌المللی تایید شده اند را بیان می‌نمایند.

ج. مشارکت و همکاری

استقرار امنیت سایبری نیاز به مشارکت و همکاری تمام بخش‌ها و رشته‌ها در این بخش است. به همین دلیل باید از یک روش چند ذینفعی استفاده نمود. بحث و گفتگو، همکاری‌ها را افزایش داده و منجر به ایجاد امنیت سایبری جامع تری را در سایر رشته‌ها فراهم می‌نماید. به اشتراک گذاری اطلاعات بین رشته‌های مختلف و نیز بین اپراتورهای بخش خصوصی نسبتا دشوار می‌باشد و همین امر در سطوح بین‌المللی به طور فزاینده ای مشکل تر خواهد بود. با این حال مسئله جرائم سایبری یکی از مسائل با اهمیت جهانی است و در آن مرزهای ملی و منطقه‌ای در نظر گرفته نمی‌شود. مشارکت و همکاری در امکان به اشتراک گذاری اطلاعات تهدید آمیز، سناریوهای تهاجم و بهترین روشهای واکنشی و دفاع را ایجاد می‌کند. طرحهای مشارکتی در مقیاس بزرگتر امکان توسعه قابلیت‌های بیشتر امنیت سایبری را فراهم می‌نماید و در امر جلوگیری از تهدیدات برخط (آنلاین) مکرر و مداوم موثر بوده و به بهتر شدن تحقیقات، رفع نگرانی‌ها و محاکمه عوامل مخرب کمک می‌کند.

همکاری‌های ملی و بین‌المللی می‌تواند بر اساس موجودیت‌ها و تعداد مشارکت‌ها، چارچوب همکاری‌ها و شبکه‌های اشتراک گذاری اطلاعات مورد ارزیابی قرار گیرند. زیرگروههای این حوزه از شاخص‌های عملکردی زیر تشکیل شده اند :

۱. همکاری‌های بین دولت‌ها

همکاری‌های بین دولتی به هرگونه همکاری ملی و بخش خصوصی رسمی اشاره دارد که داشته‌های امینت سایبری خود را دولت‌ها در سراسر مرزهایش با سایر کشورها به اشتراک می‌گذارند (به عنوان مثال، مشارکت‌های دو جانبه و یا چند جانبه به معنی امضاء تفاهم نامه‌های همکاری و تبادل اطلاعات، تخصص‌ها، فناوری‌ها و یا منابع). همکاری‌های بین دولتی شامل اقدامات در سطح منطقه‌ای می‌شود مانند موارد ذیل(تنها محدود به این موارد نمی‌باشد):

- آنهایی که توسط اتحادیه اروپا اقدام شده است مانند شورای اروپا،
- گروه G8
- سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه (APEC)،
- سازمان کشورهای آمریکایی(OAS)،
- انجمن سازمان ملل شرق آسیا (ASEAN)،
- اتحادیه عرب، اتحادیه آفریقا، سازمان همکاریهای شانگهای (SCO)
- گروه عملیات شبکه ای (NOG).

کشورها هرگونه مشارکت ملی و منطقه‌ای که به رسمیت شناخته شده اند را برای به اشتراک گذاری داشته‌های امنیت سایبری بین مرزها با سایر کشورها معرفی می‌نمایند.

۲. همکاری‌های درون سازمانی

همکاریهای درون سازمانی به برنامه‌های رسمی شناخته شده در سطح ملی و یا منطقه‌ای به منظور اشتراک گذاری داشته‌های امنیت سایبری (افراد، فرایندها، ابزار) با بخش دولتی اشاره دارد (به عنوان مثال مشارکت‌های رسمی بین دپارتمانها و سازمان‌ها بمنظور همکاری یا تبادل اطلاعات، تخصص، فناوری و یا منابع). این امر شامل طرح‌ها و برنامه‌ها بین بخش‌های مختلف می‌باشد (اجرای قانون، نیروهای نظامی، بهداشت و درمان، حمل و نقل، انرژی، زباله و مدیریت آب و غیره) همچنین در دپارتمانها/ وزارتخانه‌ها (دولت فدرال/محلی، منابع انسانی، میز سرویس‌های IT، . ..).

در این بخش کشورها هرگونه برنامه ملی و یا منطقه‌ای رسمی شناخته شده را بمنظور به اشتراک گذاری داشته‌های امینت سایبری در بخش دولتی می‌کنند.

۳. مشارکت‌های بین بخش‌های دولتی و خصوصی

مشارکت‌های دولتی – خصوصی (PPP) به سرمایه گذارها و همکاری‌های بین بخش‌های دولتی و خصوصی اشاره دارد. این شاخص عملکردی را می‌توان با تعداد مشارکت‌های عمومی–خصوصی (PPP) رسمی شناخته شده در سطح ملی و یا خصوصی بمنظور اشتراک گذاری داشته‌های امینت سایبری (افراد، فرایندها، ابزار) بین بخش خصوصی و دولتی ارزیابی نمود (به عنوان مثال مشارکت‌های رسمی بمنظور همکاری یا تبادل اطلاعات، تخصص، فناوری و یا منابع).

در این بخش کشورها هرگونه برنامه ملی و یا بخش خاص که به رسمیت شناخته شده بین بخش دولتی و خصوصی است را مشخص می‌نمایند.

۴. همکاری‌های بین‌المللی

این شاخص عملکردی به مشارکت‌های رسمی شناخته شده در زیر ساخت‌های تعاملات فی مابین و انجمن‌های مشترک حوزه امنیت سایبری بین‌المللی اشاره دارد. برخی از همکاری‌های بین‌المللی مشارکتی شناخته شده شامل موارد ذیل است (تنها محدود به موارد ذیل نمی‌شود):

- مجمع عمومی سازمان ملل متحد،
- اتحادیه بین‌المللی مخابرات(ITU)،
- Interpol / Europol،
- سازمان همکاری و توسعه اقتصادی(OECD)،
- سازمان ملل متحد بخش مبارزه با مواد مخدر و مسائل جنایی(UNODC)،
- سازمان ملل متحد بخش بین منطقه‌ای جرائم و موسسه تحقیقات فضایی(UNICRI)،
- شرکت‌های اینترنتی برای واگذاری نامه‌ها و شماره‌ها،
- سازمان بین‌المللی استاندارد(ISO)،
- کمیسیون علوم الکترونیکی بین‌المللی (IEC)،
- گروه ضربت مهندسی اینترنت،
- انجمن پاسخگو به حوادث و تیم‌های امنیتی FIRST
- اتحادیه آفریقا(AU)،
- اتحادیه کشورهای امریکایی(OAS)،
- اتحادیه عرب(LAS)،
- ارتباطات آسیا و اقیانوسیه(APT)،
- اتحادیه اروپا(AU)،
- مجمع اروپا (CoE).

در این بخش هرگونه مشارکت رسمی و عضویت در رابطه با مجامع‌ها و انجمن‌های امنیت سایبری منطقه‌ای /بین‌المللی توسط کشورها اعلام می‌شود.

برنامه زمان بندی و مراحل اجرایی پایش شاخص‌های امنیت سایبری در سال ۲۰۱٤

زمانبندی اجرا حدود ۱۸ ماه پیش بینی شده بود و انتظار می‌رفت که عملکرد شاخص به صورت کامل در سه ماهه چهارم سال ۲۰۱۴ احصا شود.

تقسیم بندی مناطق به شش حوزه جغرافیایی تقسیم بندی شده است:

کشورهای عربی

اروپا

اقیانوسیه

کشورهای امریکایی

کشورهای مشترک المنافع و خودگردان

افریقا

فازهای اجرایی در هر مرحله در مناطق

پژوهش اولیه: شامل تماس با ذی نفعان ملی جهت جمع آوری داده‌ها

پژوهش ثانویه: رصد پایگاه‌های داده‌های داخلی، منابع عمومی قابل دسترسی همگانی

استخراج داده‌ها: گردآوری و تلفیق داده‌های جمع آوری شده

ورود اطلاعات : در جهت امکان ارزیابی عملکرد اولیه برای هر کشور

تایید: بررسی داده‌های پژوهشی توسط هر کشور و جداول مقایسه ای و ارزیابی جهانی

---

[۱] International Organization for Standardization
[۲] International Telecommunication Union
[۳] Internet Engineering Task Force
[۴] Institute of Electrical and Electronics Engineers
[۵] Telecommunications Industry Solutions
[۶] Organization for the Advancement of Structured Information Standards
[۷] The 3rd Generation Partnership Project (3GPP) unites [Seven] telecommunications standard development organizations
[۸] The Third Generation Partnership Project 2 (3GPP2)

[۹] Internet Architecture Board
[۱۰] The Internet Society
[۱۱] International Support Group (ISG)
[۱۲] European Telecommunications Standards Institute
[۱۳] Information Security Forum
[۱۴] Request for Comments
[۱۵] International Society of Automation
[۱۶] International Electrotechnical Commission
[۱۷] North American Electric Reliability Corporation
[۱۸] National Institute of Standards and Technology
[۱۹] Federal Information Processing Standards
[۲۰]Payment Card Industry Data Security Standard
[۲۱] Certified Information Systems Security Professional
[۲۲] Single Strand Conformational Polymorphism
[۲۳] Certified Information Systems Security Professional
[۲۴] Global Information Assurance Certification
[۲۵] Certified Information Security Manager
[۲۶] Open Source Security Testing Methodology Manual - Certified Information Systems Auditor
[۲۷]Certified in Risk and Information Systems Control (CRISC) - Isaca
[۲۸] Information Technology (IT) Industry & Association
[۲۹] certified ethical hacker
[۳۰] Certified Security Analyst
[۳۱] Computer Hacking Forensic Investigator Course from EC-Council
[۳۲] The Payment Card Industry Professional
[۳۳] Qualified/ Information Security Professional
[۳۴] Certified Protection Professional Board Certification
[۳۵] Physical Security Professional
[۳۶] Professional Certified Investigator (PCI) - ASIS
[۳۷] Loss Prevention Qualified
[۳۸] Certified Fraud Examiner
[۳۹] CyberSecurity Forensic Analyst (CSFA)
[۴۰] Certified Information Privacy Professional (CIPP)-International Association of Privacy Professionals
[۴۱] Associate Business Continuity Professional
[۴۲] Certified Business Continuity Professional
[۴۳] Master Business Continuity Professional (DRI International)
[۴۴] Business Continuity Certified Planner (BCCP)
[۴۵] Business Continuity Certified Specialist (BCCS)
[۴۶] Business Continuity Certified Expert (BCCE)
[۴۷] Disaster Recovery Certified Specialist (DRCS)
[۴۸] Disaster Recovery Certified Expert (DRCE) - BCM Institute
[۴۹] Certified Internal Auditor (CIA) Certification
[۵۰] Certification in Control Self-Assessment (CCSA) Certification
[۵۱] Project Management Professional Certification

پرسشنامه الکترونیکی ارزیابی کشورها در شاخص جهانی امنیت سایبری

ABIresearch®

Global Cybersecurity Index

Please fill this questionnaire out electronically

via the http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

or email your responses to:

Ms Michela Menting, ABI Research menting@abiresearch.com

Mr Marco Obiso, ITU marco.obiso@itu.int

QUESTIONNAIRE

GLOBAL CYBERSECURITY INDEX

اهداف اندازه‌گیری شاخص جهانی امنیت سایبری (GCI) به طور موثر اندازه‌گیری سطح توسعه امنیت سایبری هر کشور است. و هدف نهایی آن کمک به ترویج فرهنگ جهانی امنیت سایبری و ادغام آن در هسته فناوری اطلاعات و ارتباطات(ICT) است. این اندازه‌گیری در چارچوب روال‌های اندازه‌گیری اتحادیه بین‌المللی مخابرات (ITU) و پروژه‌های مرتبط و فعالیت‌های دفتر توسعه مخابرات ITU، BDT است.

ITU به عنوان تسهیل‌کننده هدایت جهانی در نیل به اهداف خط عمل C5 WSIS(اجلاس جهانی جامعه اطلاعاتی) در کمک به ذینفعان در ایجاد اطمینان و امنیت در استفاده از ICT در سطوح ملی، منطقه‌ای و بین‌المللی است .در این چارچوب، دستور کار جهانی امنیت (GCA) توسط دبیر کل ITU به عنوان چارچوب ITU برای همکاری ذی نفعان بین‌المللی در جهت توسعه جامعه اطلاعاتی امن‌تر و بی‌خطرتر و با تمرکز بر پنج حوزه‌ی کاری منتشر شد. این بخش‌ها عبارتند از:

- اقدامات قانونی،
- اقدامات فنی و روندی،
- ساختارهای سازمانی،
- ظرفیت‌سازی
- همکاری‌های بین‌المللی.

این پنج بخش تعیین شده فوق چارچوب اندازه‌گیری شاخص‌ها را برای GCI تشکیل می‌دهند. اندازه‌گیری شاخص جهانی امنیت سایبری تلاش مشترک بین دفتر توسعه مخابرات BDTاتحادیه جهانی مخابرات ITU و بخش امنیت سایبری و برنامه‌های کاربردی ICT (CYB) موسسه تحقیقاتی .ABI است.

شما به شرکت در یک اقدام سنجشی با هدف بررسی وضعیت کنونی کشور خود در برابر شاخص امنیت جهانی(GCI) دعوت شدید. پاسخ شما به این پرسش نامه‌ها شایان تقدیر است. ITUتدوین و ارزیابی بین‌المللی از نتایج پس از دوره پایش انجام و نتایج را منتشر خواهد نمود.

RESPONDING COUNTRY (including contact information)	کشور پاسخ دهنده (شامل اطلاعات تماس)
QUESTIONS **RESPONSES**	**پاسخ‌ها** **سئوالات**
1A. Is there any criminal legislation regarding cyber activities? If so, please specify Include URL, title of laws/acts/articles, and/or wording	A۱. آیا قوانین کیفری راجع به فعالیت‌های سایبری وجود دارد؟ اگر چنین است، لطفا مشخص کنید. شامل URL، عنوان قوانین /اقدامات /مقالات، و / یا عبارت
1B. Is there any regulation regarding cybersecurity and compliance requirements? If so, please specify Include URL, title of laws/acts/articles, and/or wording	B۱. آیا مقرراتی در خصوص امنیت سایبری و فراهم کردن الزامات وجود دارد؟ اگر چنین است، لطفا مشخص کنید شامل URL، عنوان قوانین /اقدامات /مقالات، و / یا عبارت
2A. Is there one (or more) officially approved national or sector-specific CERT, CIRT or CSIRT team(s)? If so, please specify the names and number and whether they are legally mandated or not Include URL, official name, and contact details	A۲. آیا تیم(هایی) که بطور رسمی مورد تایید کشور یا در بخش خاص CERT، CSIRT CIRT وجود دارد؟ اگر چنین است، لطفا نام‌ها و تعداد، چه آنهایی که از نظر قانونی موظف هستند یا خیر را مشخص نمایید. شامل URL، نام رسمی و اطلاعات تماس
2B. Is there any officially-approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards? If so, please specify Include URL, official name of framework, responsible agency (and contact details) and short description	B۲. آیا چارچوب هایی که بطور رسمی مورد تایید کشور (و بخش خاص) در امنیت سایبری برای اجرای ا ستانداردهای بین‌المللی شناخته شده امنیت سایبری وجود دارد؟ اگر چنین است، لطفا مشخص کنید. شامل URL، نام رسمی چارچوب، ارگان مسئول (و جزئیات تماس) و شرحی کوتاه
2C. Is there any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals? If so, please specify	C۲. آیا چارچوب هایی که بطور رسمی مورد تایید کشور (و بخش خاص) در امنیت سایبری برای صدور گواهینامه و مجوز ر سمی از سازمان‌های ملی و حرفه ای در بخش دولتی وجود دارد؟ اگر چنین است، لطفا مشخص کنید

Include URL, official name of framework, responsible agency (and contact details) and short description	شامل URL، نام ر سمی چارچوب، ارگان م سئول (و جزئیات تماس) و شرح کوتاه
3A. Is there any officially recognized national or sector-specific cybersecurity strategy and/or policy? If so, please specify Include URL, official name of strategy/policy, responsible agency (and contact details) and short description	A۳. آیا ا ستراتژی و یا سیا ستی به ر سمیت شناخته شـده ی ملی یا بخشـی در امنیت سـایبری وجود دارد؟ اگر چنین است، لطفا مشخص کنید شامل URL، نام ر سمی ا ستراتژی / سیا ست، ارگان مسئول (و جزئیات تماس) و شرح کوتاه
3B. IS there any officially recognized national or sector-specific governance roadmap for cybersecurity? If so, please specify Include URL, official name of roadmap, responsible agency (and contact details) and short description	B۳. آیا نقشه راه حکومتی به رسمیت شناخته شده ی ملی یا بخشی در امنیت سایبری وجود دارد؟ اگر چنین است، لطفا مشخص کنید شامل URL، نام ر سمی نق شه راه، ارگان م سئول (و جزئیات تماس) و شرح کوتاه
3C. IS there any officially recognised national or sector-specific agency responsible for implementing a national cybersecurity strategy/policy/roadmap? If so, please specify Include URL, official name of responsible agency (and contact details) and short description of responsibilities	C۳. آیا ارگان مسئول به رسمیت شناخته شده ی ملی یا بخشی برای پیاده سازی یک ا ستراتژی / سیا ست / نقشه راه ملی امنیت سـایبری وجود دارد؟ اگر چنین اسـت، لطفا مشخص کنید شـامل URL، نام رسـمی ارگان مسـئول (و جزئیات تماس) و شرح کوتاهی از مسئولیت‌ها
3D. Is there any officially recognised national or sector-specific benchmarking exercises or referential used to measure cybersecurity development? If so, please specify Include URL, official name of benchmarking exercise, responsible agency (and contact details) and short description	D۳. آیا اقدام سـنجشـی(الگوبرداری) یا اسـتنباطی سایبری به رسمیت شناخته شده ی ملی یا بخشی که سابقا جهت اندازه‌گیری تو سعه امنیت سایبری ا ستفاده شود وجود دارد؟ اگر چنین است، لطفا مشخص کنید شامل URL، نام رسمی اقدام سنجشی، ارگان مسئول (و جزئیات تماس) و شرح کوتاه
4a. Is there any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector? If so, please specify Include URL, official name(s) of programs/projects/best practices/guidelines,	A۴.. آیـا برنـامـه / پروژه‌هـای تحقیق و توسـعـه ای(R&D) به رسمیت شناخته شده ی ملی یا بخشی برای اسـتانداردهای امنیت سـایبری وجود دارد، بهترین شـیوه‌ها و د ستورالعمل‌های در هر دو خ صو صی یا بخش دولتی اعمال شود ؟ اگر چنین است، لطفا مشخص کنید

شامل URL، نام ر سمی برنامه‌ها / پروژه‌ها/ بهترین شـیوه‌ها/ دسـتورالعمل‌ها، ارگان (های)مسـئول (و جزئیات تماس) و شرح کوتاه	responsible agency(ies) (and contact details) and short description
B۴. آیا برنامه‌های آموزشـی تحصـیلی و حرفه ای به ر سمیت شناخته شده ی ملی بخ شی برای بالا بردن سطح آگاهی عمومی مردم، ترویج دوره امنیت سـایبری در آموزش عالی و ترویج صدور گواهینامه حرفه ای در هر دو خصوصی یا بخش دولتی وجود دارد ؟ اگر چنین اسـت، لطفا مشـخص کنید شـامل URL، نام رسـمی برنامه‌ها / پروژه‌ها، ارگان (های)مسئول (و جزئیات تماس) و شرح کوتاه	4B. Is there any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sector? If so, please specify Include URL, official name(s) of programs/projects, responsible agency(ies) (and contact details) and short description
C۴. آیا متخ صصان بخش دولتی که تحت برنامه‌های گواهینامه بین‌المللی شناخته شده در زمینه امنیت سایبری تایید شـده باشـند، وجود دارد. اگر چنین اسـت، لطفا شـماره مشخص شامل نوع گواهینامه و ارگان صادرکننده گواهی	4C. Are there any public sector professionals certified under internationally recognized certification programs in cybersecurity? If so, please specify the number Include type of certification and certificating agency
D۴. آیا ارگان‌های دولتی یا خصـوصـی که تحت برنامه‌های گواهینامه بین‌المللی شناخته شده در زمینه امنیت سایبری تایید شده با شند، وجود دارد. اگر چنین ا ست، لطفا شماره مشخص شامل نوع گواهینامه و ارگان صادرکننده گواهی	4D. Are there any certified government and public sector agencies certified under internationally recognized standards in cybersecurity? If so, please specify the number Include type of certification and certificating agency
A۵. آیا م شارکت به ر سمیت شناخته شده ی ملی یا بخشی برای به اشتراک گذاری دارایی‌های امنیت سایبری در سراسر مرزها با ایالات دیگر وجود دارد؟ اگر چنین است، لطفا مشخص کنید. شامل URL، نام رسمی مشارکت، آژانس ملی مسئول (و جزئیات تماس)، کشـورهای شـرکت‌کننده و توضـیحات کوتاه	5A. Are there any officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders with other nation states? If so, please specify Include URL, official name of partnership, responsible national agency (and contact details), participating countries, and short description

5B. Are there any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector? If so, please specify Include URL, official name of program, responsible agency (and contact details), participating organizations, and short description	B۵. آیا برنامه‌های به ر سمیت شناخته شده ی ملی یا بخشی برای به اشتراک گذاری دارایی‌های امنیت سایبری در داخل بخش خصـوصـی وجود دارد؟ اگر چنین اسـت، لطفا مشخص کنید. شامل URL، نام ر سمی برنامه، سازمان م سئول (و جزئیات تماس)، ارگان‌های شرکت‌کننده و توضیحات کوتاه
5C. Are there any officially recognized national or sector-specific programs for sharing cybersecurity assets between the public and private sector? If so, please specify Include URL, official name of program, responsible national agency (and contact details), participating organizations, and short description	C۵ آیا برنامه‌های به ر سمیت شناخته شده ی ملی یا بخ شی برای به ا شتراک گذاری دارایی‌های امنیت سایبری بین بخش دولتی و خصـوصـی وجود دارد؟ اگر چنین اسـت، لطفا مشخص کنید شامل URL، نام ر سمی برنامه، ارگان ملی مسئول (و جزئیات تماس)، ارگان‌های شرکت‌کننده و توضیحات کوتاه
5D. Are there any officially recognized participation in regional and/or international cybersecurity platforms and forums? If so, please specify Include URL, official name of platform/forum, responsible national agency (and contact details), participating countries, and short description	D۵. آیا مشـارکت به رسـمیت شـناخته شـده در پلت فرم ها و انجمن های امن یت سـایبری منط قه‌ای و / یا بین‌المللی وجود دارد؟ اگر چنین است، لطفا مشخص کنید شامل URL، نام رسمی پلت فرم / انجمن، ارگان ملی مسـئول (و جزئیات تماس)، کشـورهای شـرکت‌کننده و توضیحات کوتاه

نتایج ارزیابی کشورها در پایش شاخص‌های جهانی امنیت سایبری در سال ۲۰۱٤

ردیف	کشور	مقدار عملکرد شاخص	رتبه جهانی
۱	ایالات متحده آمریکا *	۰.۸۲۴	۱
۲	کانادا *	۰.۷۹۴	۲
۳	استرالیا *	۰.۷۶۵	۳
۴	مالزی	۰.۷۶۵	۳
۵	عمان	۰.۷۶۵	۳
۶	نیوزلند *	۰.۷۳۵	۴
۷	نروژ *	۰.۷۳۵	۴
۸	برزیل	۰.۷۰۶	۵
۹	استونی *	۰.۷۰۶	۵
۱۰	آلمان *	۰.۷۰۶	۵
۱۱	هند *	۰.۷۰۶	۵
۱۲	ژاپن *	۰.۷۰۶	۵
۱۳	جمهوری کره	۰.۷۰۶	۵
۱۴	انگلستان	۰.۷۰۶	۵
۱۵	اتریش *	۰.۶۷۶	۶
۱۶	مجارستان *	۰.۶۷۶	۶
۱۷	اسرائیل *	۰.۶۷۶	۶
۱۸	هلند *	۰.۶۷۶	۶
۱۹	سنگاپور	۰.۶۷۶	۶
۲۰	لتونی *	۰.۶۴۷	۷
۲۱	سوئد *	۰.۶۴۷	۷
۲۲	ترکیه	۰.۶۴۷	۷
۲۳	فنلاند	۰.۶۱۸	۸
۲۴	قطر	۰.۶۱۸	۸
۲۵	اسلواکی	۰.۶۱۸	۸
۲۶	اروگوئه	۰.۶۱۸	۸
۲۷	کلمبیا	۰.۵۸۸	۹

ردیف	کشور	مقدار عملکرد شاخص	رتبه جهانی
۲۸	دانمارک *	۰.۵۸۸	۹
۲۹	مصر	۰.۵۸۸	۹
۳۰	فرانسه *	۰.۵۸۸	۹
۳۱	موریس	۰.۵۸۸	۹
۳۲	اسپانیا *	۰.۵۸۸	۹
۳۳	ایتالیا	۰.۵۵۹	۱۰
۳۴	مراکش	۰.۵۵۹	۱۰
۳۵	اوگاندا	۰.۵۵۹	۱۰
۳۶	آذربایجان	۰.۵۲۹	۱۱
۳۷	لهستان *	۰.۵۲۹	۱۱
۳۸	رواندا	۰.۵۲۹	۱۱
۳۹	تونس	۰.۵۲۹	۱۱
۴۰	جمهوری چک	۰.۵	۱۲
۴۱	گرجستان	۰.۵	۱۲
۴۲	روسیه *	۰.۵	۱۲
۴۳	اندونزی	۰.۴۷۱	۱۳
۴۴	لوکزامبورگ *	۰.۴۷۱	۱۳
۴۵	رومانی	۰.۴۷۱	۱۳
۴۶	بلژیک *	۰.۴۴۱	۱۴
۴۷	بلغارستان	۰.۴۴۱	۱۴
۴۸	چین *	۰.۴۴۱	۱۴
۴۹	لیتوانی	۰.۴۴۱	۱۴
۵۰	نیجریه	۰.۴۴۱	۱۴
۵۱	سودان	۰.۴۴۱	۱۴
۵۲	آرژانتین *	۰.۴۱۲	۱۵
۵۳	کامرون	۰.۴۱۲	۱۵
۵۴	کرواسی	۰.۴۱۲	۱۵
۵۵	کنیا	۰.۴۱۲	۱۵
۵۶	مغولستان	۰.۴۱۲	۱۵
۵۷	سری لانکا	۰.۴۱۲	۱۵
۵۸	تایلند *	۰.۴۱۲	۱۵

ردیف	کشور	مقدار عملکرد شاخص	رتبه جهانی
۵۹	برونئی دارالسلام	۰.۳۸۲	۱۶
۶۰	شیلی *	۰.۳۸۲	۱۶
۶۱	مولدووا *	۰.۳۸۲	۱۶
۶۲	مونته نگرو	۰.۳۸۲	۱۶
۶۳	میانمار	۰.۳۸۲	۱۶
۶۴	آفریقای جنوبی	۰.۳۸۲	۱۶
۶۵	کاستاریکا *	۰.۳۵۳	۱۷
۶۶	اکوادور	۰.۳۵۳	۱۷
۶۷	مالت *	۰.۳۵۳	۱۷
۶۸	فیلیپین	۰.۳۵۳	۱۷
۶۹	سویس	۰.۳۵۳	۱۷
۷۰	اوکراین *	۰.۳۵۳	۱۷
۷۱	امارات متحده عربی *	۰.۳۵۳	۱۷
۷۲	بورکینافاسو	۰.۳۲۴	۱۸
۷۳	مکزیک *	۰.۳۲۴	۱۸
۷۴	پرو *	۰.۳۲۴	۱۸
۷۵	ویتنام *	۰.۳۲۴	۱۸
۷۶	بحرین	۰.۲۹۴	۱۹
۷۷	بنگلادش	۰.۲۹۴	۱۹
۷۸	قبرس *	۰.۲۹۴	۱۹
۷۹	غنا *	۰.۲۹۴	۱۹
۸۰	ایران *	۰.۲۹۴	۱۹
۸۱	لیبی	۰.۲۹۴	۱۹
۸۲	پاناما	۰.۲۹۴	۱۹
۸۳	پرتغال *	۰.۲۹۴	۱۹
۸۴	عربستان سعودی *	۰.۲۹۴	۱۹
۸۵	افغانستان	۰.۲۶۵	۲۰
۸۶	صربستان	۰.۲۶۵	۲۰
۸۷	توگو	۰.۲۶۵	۲۰
۸۸	ساحل عاج	۰.۲۳۵	۲۱
۸۹	جامائیکا *	۰.۲۳۵	۲۱
۹۰	آلبانی	۰.۲۰۶	۲۲
۹۱	السالوادور*	۰.۲۰۶	۲۲
۹۲	یونان *	۰.۲۰۶	۲۲

ردیف	کشور	مقدار عملکرد شاخص	رتبه جهانی
۹۳	گواتمالا	۰.۲۰۶	۲۲
۹۴	ایسلند *	۰.۲۰۶	۲۲
۹۵	ایرلند *	۰.۲۰۶	۲۲
۹۶	اردن	۰.۲۰۶	۲۲
۹۷	لیبریا	۰.۲۰۶	۲۲
۹۸	پاراگوئه *	۰.۲۰۶	۲۲
۹۹	تانزانیا	۰.۲۰۶	۲۲
۱۰۰	ترینیداد و توباگو	۰.۲۰۶	۲۲
۱۰۱	ونزوئلا	۰.۲۰۶	۲۲
۱۰۲	الجزایر	۰.۱۷۶	۲۳
۱۰۳	ارمنستان	۰.۱۷۶	۲۳
۱۰۴	باربادوس	۰.۱۷۶	۲۳
۱۰۵	بلاروس *	۰.۱۷۶	۲۳
۱۰۶	بلیز *	۰.۱۷۶	۲۳
۱۰۷	بنین *	۰.۱۷۶	۲۳
۱۰۸	بوسنی و هرزگوین	۰.۱۷۶	۲۳
۱۰۹	بوتسوانا	۰.۱۷۶	۲۳
۱۱۰	قزاقستان *	۰.۱۷۶	۲۳
۱۱۱	مالاوی	۰.۱۷۶	۲۳
۱۱۲	پاکستان *	۰.۱۷۶	۲۳
۱۱۳	ساموآ	۰.۱۷۶	۲۳
۱۱۴	سنگال *	۰.۱۷۶	۲۳
۱۱۵	اسلوونی *	۰.۱۷۶	۲۳
۱۱۶	سوریه	۰.۱۷۶	۲۳
۱۱۷	باهاما *	۰.۱۴۷	۲۴
۱۱۸	موریتانی *	۰.۱۴۷	۲۴
۱۱۹	نیکاراگوئه *	۰.۱۴۷	۲۴
۱۲۰	سنت کیتس و نویس	۰.۱۴۷	۲۴
۱۲۱	دولت فلسطین *	۰.۱۴۷	۲۴
۱۲۲	تاجیکستان *	۰.۱۴۷	۲۴
۱۲۳	مقدونیه *	۰.۱۴۷	۲۴
۱۲۴	ازبکستان *	۰.۱۴۷	۲۴
۱۲۵	وانواتو	۰.۱۴۷	۲۴
۱۲۶	زامبیا	۰.۱۴۷	۲۴

ردیف	کشور	مقدار عملکرد شاخص	رتبه جهانی
۱۲۷	آنتیگوا و باربودا *	۰.۱۱۸	۲۵
۱۲۸	بوتان	۰.۱۱۸	۲۵
۱۲۹	بولیوی *	۰.۱۱۸	۲۵
۱۳۰	بروندی	۰.۱۱۸	۲۵
۱۳۱	کامبوج	۰.۱۱۸	۲۵
۱۳۲	جمهوری دومینیکن	۰.۱۱۸	۲۵
۱۳۳	گرانادا	۰.۱۱۸	۲۵
۱۳۴	گویان *	۰.۱۱۸	۲۵
۱۳۵	قرقیزستان *	۰.۱۱۸	۲۵
۱۳۶	لیختن اشتاین *	۰.۱۱۸	۲۵
۱۳۷	میکرونزی	۰.۱۱۸	۲۵
۱۳۸	نپال *	۰.۱۱۸	۲۵
۱۳۹	پاپوآ گینه نو	۰.۱۱۸	۲۵
۱۴۰	سنت لوسیا *	۰.۱۱۸	۲۵
۱۴۱	سیشل *	۰.۱۱۸	۲۵
۱۴۲	سورینام *	۰.۱۱۸	۲۵
۱۴۳	آنگولا *	۰.۰۸۸	۲۶
۱۴۴	گامبیا	۰.۰۸۸	۲۶
۱۴۵	کیریباتی	۰.۰۸۸	۲۶
۱۴۶	لبنان	۰.۰۸۸	۲۶
۱۴۷	ماداگاسکار	۰.۰۸۸	۲۶
۱۴۸	مالدیو	۰.۰۸۸	۲۶
۱۴۹	مالی	۰.۰۸۸	۲۶
۱۵۰	موناکو *	۰.۰۸۸	۲۶
۱۵۱	نیجر *	۰.۰۸۸	۲۶
۱۵۲	سودان جنوبی *	۰.۰۸۸	۲۶
۱۵۳	تونگا	۰.۰۸۸	۲۶
۱۵۴	ترکمنستان *	۰.۰۸۸	۲۶
۱۵۵	زیمبابوه	۰.۰۸۸	۲۶
۱۵۶	آندورا *	۰.۰۵۹	۲۷
۱۵۷	کنگو	۰.۰۵۹	۲۷
۱۵۸	جیبوتی	۰.۰۵۹	۲۷
۱۵۹	دومینیکا *	۰.۰۵۹	۲۷
۱۶۰	فیجی	۰.۰۵۹	۲۷

ردیف	کشور	مقدار عملکرد شاخص	رتبه جهانی
۱۶۱	هائیتی *	۰.۰۵۹	۲۷
۱۶۲	کویت *	۰.۰۵۹	۲۷
۱۶۳	لائوس	۰.۰۵۹	۲۷
۱۶۴	موزامبیک *	۰.۰۵۹	۲۷
۱۶۵	سائوتومه و پرینسیپ	۰.۰۵۹	۲۷
۱۶۶	سیرا لئون	۰.۰۵۹	۲۷
۱۶۷	سوازیلند	۰.۰۵۹	۲۷
۱۶۸	تووالو	۰.۰۵۹	۲۷
۱۶۹	یمن *	۰.۰۵۹	۲۷
۱۷۰	کیپ ورد	۰.۰۲۹	۲۸
۱۷۱	چاد *	۰.۰۲۹	۲۸
۱۷۲	کومور	۰.۰۲۹	۲۸
۱۷۳	کوبا *	۰.۰۲۹	۲۸
۱۷۴	جمهوری دموکراتیک کنگو	۰.۰۲۹	۲۸
۱۷۵	اریتره *	۰.۰۲۹	۲۸
۱۷۶	اتیوپی *	۰.۰۲۹	۲۸
۱۷۷	گابن	۰.۰۲۹	۲۸
۱۷۸	گینه	۰.۰۲۹	۲۸
۱۷۹	گینه بیسائو *	۰.۰۲۹	۲۸
۱۸۰	عراق *	۰.۰۲۹	۲۸
۱۸۱	نائورو	۰.۰۲۹	۲۸
۱۸۲	پالائو *	۰.۰۲۹	۲۸
۱۸۳	جزایر سلیمان	۰.۰۲۹	۲۸
۱۸۴	سومالی	۰.۰۲۹	۲۸
۱۸۵	جمهوری آفریقای مرکزی *	۰	۲۹
۱۸۶	جمهوری دموکراتیک خلق کره *	۰	۲۹
۱۸۷	گینه استوایی *	۰	۲۹
۱۸۸	هندوراس *	۰	۲۹
۱۸۹	لسوتو	۰	۲۹
۱۹۰	جزایر مارشال	۰	۲۹
۱۹۱	نامیبیا	۰	۲۹
۱۹۲	سنت وینسنت و گرنادین	۰	۲۹
۱۹۳	تیمور لسته *	۰	۲۹

***براساس داده‌های ثانویه**

نتایج ارزیابی کشورهای آسیا و اقیانوسیه در پایش شاخص‌های جهانی امنیت سایبری در سال ۲۰۱٤

ردیف	آسیا و اقیانوسیه	قانونی/ حقوقی	فنی	سازمانی	ظرفیت‌سازی	مشارکت و همکاری	مقدار شاخص	رتبه منطقه‌ای
۱	استرالیا *	۰,۷۵	۰,۶۶۶۷	۰,۸۷۵	۰,۸۷۵	۰,۶۲۵	۰,۷۶۴۷	۱
۲	مالزی	۰,۷۵	۰,۸۳۳۳	۱	۰,۶۲۵	۰,۶۲۵	۰,۷۶۴۷	۱
۳	نیوزلند *	۱	۰,۸۳۳۳	۰,۸۷۵	۰,۶۲۵	۰,۵	۰,۷۳۵۳	۲
٤	هند *	۱	۰,۶۶۶۷	۰,۷۵	۰,۸۷۵	۰,۳۷۵	۰,۷۰۵۹	۳
۵	ژاپن *	۱	۰,۶۶۶۷	۰,۷۵	۰,۶۲۵	۰,۶۲۵	۰,۷۰۵۹	۳
٦	جمهوری کره	۱	۰,۶۶۶۷	۰,۸۷۵	۰,۶۲۵	۰,۵	۰,۷۰۵۹	۳
۷	سنگاپور	۰,۷۵	۰,۶۶۶۷	۰,۷۵	۰,۷۵	۰,۵	۰,۶۷۶۵	۴
۸	هنگ کنگ	۰,۷۵	۰,۶۶۶۷	۰,۵	۰,۷۵	۰,۵	۰,۶۱۷۶	۵
۹	اندونزی	۱	۰,۳۳۳۳	۰,۲۵	۰,۵	۰,۵	۰,۴۷۰۶	۵
۱۰	چین *	۰,۷۵	۰,۵	۰,۲۵	۰,۵	۰,۳۷۵	۰,۴۴۱۲	۶
۱۱	مغولستان	۰,۵	۰,۸۳۳۳	۰,۶۲۵	۰,۱۲۵	۰,۱۲۵	۰,۴۱۱۸	۷
۱۲	سری لانکا	۰,۵	۰,۳۳۳۳	۰,۲۵	۰,۵	۰,۵	۰,۴۱۱۸	۷
۱۳	تایلند *	۰,۵	۰,۳۳۳۳	۰,۵	۰,۲۵	۰,۵	۰,۴۱۱۸	۷
۱٤	برونئی دارالسلام	۰,۷۵	۰,۳۳۳۳	۰,۱۲۵	۰,۳۷۵	۰,۵	۰,۳۸۲۴	۸
۱۵	میانمار	۰,۲۵	۰,۵	۰,۲۵	۰,۵	۰,۳۷۵	۰,۳۸۲۴	۸
۱٦	فیلیپین	۱	۰,۳۳۳۳	۰,۳۷۵	۰,۳۷۵	۰	۰,۳۵۲۹	۹
۱۷	ویتنام *	۰,۵	۰,۳۳۳۳	۰,۱۲۵	۰,۵	۰,۲۵	۰,۳۲۳۵	۱۰
۱۸	بنگلادش	۰,۵	۰,۳۳۳۳	۰,۱۲۵	۰,۲۵	۰,۳۷۵	۰,۲۹۴۱	۱۱
۱۹	ایران *	۰,۵	۰,۳۳۳۳	۰,۵	۰,۱۲۵	۰,۱۲۵	۰,۲۹۴۱	۱۱
۲۰	افغانستان	۰	۰,۵	۰,۳۷۵	۰,۲۵	۰,۱۲۵	۰,۲۶۴۷	۱۲
۲۱	پاکستان *	۰,۲۵	۰,۱۶۶۷	۰	۰,۳۷۵	۰,۱۲۵	۰,۱۷۶۵	۱۳
۲۲	ساموآ	۰,۵	۰	۰,۱۲۵	۰,۱۲۵	۰,۲۵	۰,۱۷۶۵	۱۳
۲۳	وانواتو	۰	۰	۰,۲۵	۰,۱۲۵	۰,۲۵	۰,۱۴۷۱	۱۴
۲٤	بوتان	۰,۲۵	۰,۳۳۳۳	۰,۱۲۵	۰	۰	۰,۱۱۷۶	۱۵
۲۵	کامبوج	۰,۲۵	۰,۳۳۳۳	۰,۱۲۵	۰	۰	۰,۱۱۷۶	۱۵
۲٦	میکرونزی	۰	۰	۰,۲۵	۰,۱۲۵	۰,۱۲۵	۰,۱۱۷۶	۱۵
۲۷	نپال *	۰,۵	۰	۰,۱۲۵	۰	۰,۱۲۵	۰,۱۱۷۶	۱۵
۲۸	پاپوآ گینه نو	۰	۰	۰,۳۷۵	۰	۰,۱۲۵	۰,۱۱۷۶	۱۵
۲۹	کیریباتی	۰	۰	۰,۱۲۵	۰	۰,۲۵	۰,۸۸۲	۱۶

ردیف	آسیا و اقیانوسیه	قانونی/ حقوقی	فنی	سازمانی	ظرفیت‌سازی	مشارکت و همکاری	مقدار شاخص	رتبه منطقه‌ای
۳۰	مالدیو	۰	۰	۰,۱۲۵	۰	۰,۲۵	۰,۸۸۲	۱۶
۳۱	تونگا	۰,۵	۰	۰,۱۲۵	۰	۰	۰,۸۸۲	۱۶
۳۲	فیجی	۰,۲۵	۰	۰	۰	۰,۱۲۵	۰,۵۸۸	۱۷
۳۳	لائوس	۰	۰,۳۳۳۳	۰	۰	۰	۰,۵۸۸	۱۷
۳٤	تووالو	۰	۰	۰,۱۲۵	۰	۰,۱۲۵	۰,۵۸۸	۱۷
۳۵	نائورو	۰	۰,۱۶۶۷	۰	۰	۰	۰,۰۲۹۴	۱۸
۳٦	پالائو *	۰	۰	۰	۰	۰,۱۲۵	۰,۰۲۹۴	۱۸
۳۷	جزایر سلیمان *	۰	۰	۰	۰	۰,۱۲۵	۰,۰۲۹۴	۱۸
۳۸	جمهوری دموکراتیک خلق کره *	۰	۰	۰	۰	۰	۰	۱۹
۳۹	جزایر مارشال	۰	۰	۰	۰	۰	۰	۱۹
٤۰	تیمور لسته *	۰	۰	۰	۰	۰	۰	۱۹

*براساس داده‌های ثانویه

منابع :

- *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_2014_Results_for_Asia_Pacific.pdf.*
- *http://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/ABI%20Research_GCI%20Americas.pdf.*
- *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI.pdf.*
- *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Conceptual_Framework.pdf.*
- *http://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Global_2014_results.pdf.*

mis.iran.ir

سازمان فناوری اطلاعات ایران
مرکز برنامه ریزی و نظارت راهبردی فناوری اطلاعات
تهران، خیابان شریعتی نرسیده به پل سید خندان، ورودی ۲۲
تلفن: ۸۸۱۱ ۵۸۰۷(۹۸۲۱+)