ریاست جمهوری
مرکز همکاری‌های تحول و پیشرفت

سند راهبردِ ملی امنیت سایبری ۲۰۲۰ هند

ارائه شده توسط

شورای امنیت داده هند (DSCI)


بسم الله الرحمن الرحيم

مقدمه

در سند راهبرد ملی امنیت سایبریِ ۲۰۲۰ هند[1]، شورای امنیت داده هند (DSCI)[2]، چشم‌انداز خود را در زمینه راهبرد ملی امنیت سایبریِ هند، در مشورت با موسسات فعال در حوزه‌های مختلف (نظیر انرژی، بانکداری، خدمات مالی و بیمه‌ای، فناوری اطلاعات و غیره) ارائه کرده‌است. این شورا نهادی صنعتی و غیرانتفاعی برای حفاظت از داده در هند است که در سال ۲۰۰۸ توسط انجمن ملی شرکت‌های نرم‌افزاری و خدماتی[3] تاسیس شده‌است. شورای امنیت داده با تدوین شیوه‌نامه‌ها، استانداردها، گزارش‌های مطالعاتی، چهارچوب‌ها و ابتکار عمل‌های مناسب در حوزه امنیت سایبری و حریم شخصی، به ایمنی، امنیت و قابل اعتماد بودن فضای سایبری کمک می‌کند. شورای امنیت داده هند با دولت‌ها، سازمان‌ها، نهادهای تنظیمی (رگولاتورها)، انجمن‌های صنایع و اتاق‌های فکر جهت سیاست‌گذاری، پیشتازی در اندیشه‌ورزی[4]، ایجاد ظرفیت و فعالیت‌های ارتقای دسترسی عمومی همکاری می‌کند.

---

[1] National Cyber Security Strategy 2020
[2] Data Security Council of India (DSCI)
[3] National Association of Software and Service Companies (NASSCOM)
[4] Thought Leadership

مروری بر جایگاه و وضعیت هند

بر اساس آمار موسسه جهانی مکنزی[1]، در میان ۱۷ کشور برترِ اقتصاد دیجیتال، هند دومین کشور سریع در به‌کارگیری فناوری‌های دیجیتال است. همچنین بر اساس شاخص امنیت سایبری[2] (سال ۲۰۱۸) هند در جایگاه ۴۷ دنیا قرار دارد. در سال ۲۰۱۸-۲۰۱۷ بخش‌های کلیدی اقتصاد دیجیتال هند حدود ۱۷۰ میلیارد دلار معادل ۷ درصدِ تولید ناخالص داخلی این کشور را به‌خود اختصاص دادند و انتظار می‌رود تا سال ۲۰۲۵، این رقم ۸ تا ۱۰ درصد افزایش یابد. نظر به اینکه کشور هند در شرف دستیابی به اقتصاد تریلیون دلاری[3] است، به‌منظور ارتقای جایگاه جهانی خود، در حال به‌روزرسانی «راهبرد ملی امنیت سایبری کشور» است (آخرین نسخه مربوط به سال ۲۰۱۳ بود). در لزوم اهمیت توجه دولت هند به مباحث امنیت سایبری همین بس که بین سال‌های ۲۰۱۶ و ۲۰۱۸، هند دومین کشوری بود که بیشترین حملات سایبری را متحمل شد و به‌دلیل نفوذ به داده‌ها[4]، بیش از ۱/۷ میلیون دلار خسارت به این کشور وارد شد. در سال ۲۰۱۷، تیم پاسخگویی به فوریت‌های کامپیوتری هند[5] بیش از ۵۳ هزار حادثه را مدیریت کرد درحالی‌که در سال ۲۰۱۸ این رقم به بیش از ۲۰۰ هزار مورد رسید. این افزایش ناگهانی در حملات سایبری، ناشی از رشد دیجیتالی شدن اقتصاد هند است. مطابق گزارش بیمه سایبری شورای امنیت داده هند، بیش از ۵۶۰ میلیون مشترکِ اینترنت در هند وجود دارد و این کشور در حال تبدیل شدن به دومین بازار بزرگ برنامه‌های کاربردی (اپلیکیشن) در جهان است. لذا، ضروری است دولت جهت ارتقای امنیت سایبری بخش‌های مختلف وارد عمل شود.

مروری بر سند راهبرد ملی امنیت سایبریِ ۲۰۲۰ هند

در سند راهبرد ملی امنیت سایبریِ ۲۰۲۰ هند به سه حوزه کلان به‌همراه ۲۱ موضوع فرعی که متضمن شکوفایی هند در جهت ایجاد یک فضای سایبریِ امن و ایمن، قابل اعتماد، منعطف و چالاک می‌شوند، اشاره شده‌است.

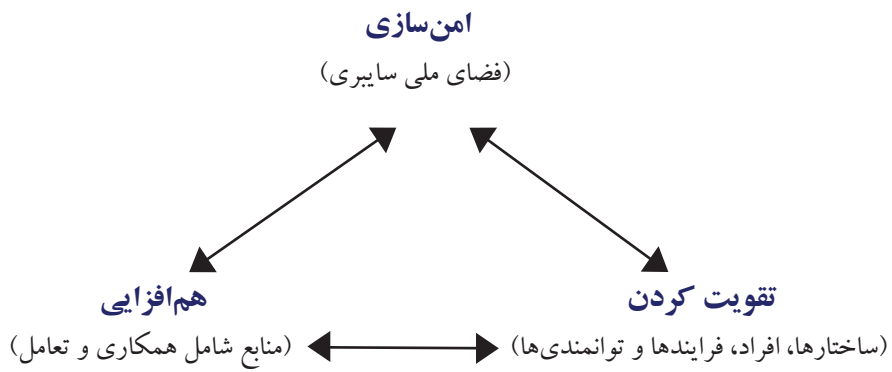
---

[1] McKinsey Global Institute
[2] Global Cybersecurity Index
[3] becoming USD 1Tn Economy
[4] Data Breach
[5] Indian Computer Emergency Response Team (CERT-In): اداره‌ای زیرمجموعه وزارت فناوری اطلاعات و الکترونیک هند است که مسئول رسیدگی به تهدیدهای امنیت سایبری است.

جنبه‌های امنیت ملی سایبری

- آمادگی بخشی
- امنیت سایبری در سطح ایالت‌ها
- آمادگی کسب‌وکارهای کوچک و متوسط
- فناوری پیشرفته (5G، وایرلس، ابر، اینترنت اشیا، هوش مصنوعی/یادگیری ماشینی، رباتیک، واقعیت افزوده/واقعیت مجازی، محاسبات با عملکرد بالا/محاسبات کوآنتومی، سخت‌افزار/شبه‌رساناها، فناوری دفتر کل توزیع‌شده، پهپادها، رابط دیجیتال سریالی و علم مواد)
- دیجیتال‌سازی خدمات عمومی در مقیاس بالا
- امنیت زنجیره عرضه
- اطلاعات اساسی
- حفاظت از زیرساخت‌ها
- امنیت پرداخت‌های دیجیتال

- ساختارها، نهادهای ذی‌ربط و حاکمیت
- تخصیص بودجه
- تحقیق، نوآوری و توسعه فناوری
- توانمندسازی و مهارت‌افزایی
- ارزیابی و بازرسی
- مدیریت حادثه/بحران
- امنیت داده و حاکمیت



- زیرساخت اینترنت
- توسعه استانداردها
- بیمه سایبری
- برند هند
- دیپلماسی سایبری
- بررسی جرایم سایبری

حوزه‌های اصلی سند عبارتند از: (۱) امنیت فضای ملی سایبری؛ (۲) تقویت ساختارها، فرآیندها و توانمندی‌ها؛ و (۳) هم‌افزایی در زمینه‌های مختلفِ همکاری. در ادامه به مهمترین موارد هر حوزه به‌اختصار پرداخته خواهد شد.

۱) امنیت

دیجیتال‌سازی خدمات دولتی در سطح وسیع: تلاش‌های مستمر و اقدامات نوآورانه هند در زمینه دیجیتالی شدن، سبب شهرت جهانی این کشور شده‌است. در صورت عدم توجه به مبحث امنیت، قطعا اعتماد شهروندان به بسترهای (پلتفرم‌های) دیجیتال و خدمات برخط از بین خواهد رفت و دسترسی امن به خدمات امکان‌پذیر نخواهد بود. در حوزه امنیت توجه به این موارد بسیار اهمیت دارد:

- توجه به امنیت از مراحل اولیه طراحی ابتکارعمل‌های دیجیتال‌سازی در کشور و تعیین و تعریف مناصب و مسئولیت‌های مرتبط با این حوزه
- توسعه ظرفیت نهادی برای ارزیابی و سنجش و صدور گواهی (تاییدیه) برای امنیت تجهیزات مورد استفاده
- ارتقای فرهنگ حاکمیت امنیت ضمن گسترش استفاده از فناوری‌های جدید
- ضرورت گزارش‌دهی همه موارد نقاط ضعف امنیتی و تهدیدهای پیش‌آمده

امنیت زنجیره تامین: با توجه به روند روبه‌رشد دیجیتال‌سازی صنعت و تلاش بی‌وقفه هند برای توسعه محصولات «ساخت هند»، برقراری امنیت در فضای سایبری از اهمیت بالایی برای این کشور برخوردار است زیرا خریدِ دولتی وسیع کالاهای دیجیتال خارجی و داخلی مستلزم وجود امنیت برای به‌کارگیری آن‌ها است.

- پایش مستمر زنجیره عرضه محصولات الکترونیک و فناوری اطلاعات و ارتباطات و رتبه‌بندی آن‌ها از نظر سطح ضرورت و سهم کشور در تولید آن‌ها با هدف افزایش سهم هند در زنجیره عرضه از طریق افزایش سرمایه‌گذاری در ظرفیت‌های فنی ضروری

- ارتقا سطح فعالیت‌های تست و صدور گواهی هند با سرمایه‌گذاری وسیع و همکاری بخش خصوصی
- تقویت و حمایت از پیشتازی کشور در طراحی شبه‌رساناها
- طراحی و تحقیقات مهندسی (**ERnD**)[۱]
- توسعه نوآوری در فناوری‌های عمیق[۲] جهت ارتقای امنیت زنجیره عرضه در سطح راهبردی، فنی و تاکتیکی در عرصه جهانی

حفاظت از زیرساخت‌های اطلاعاتی مهم: افزایش حملات متمرکز و نظام‌مند به زیرساخت‌های اطلاعاتی مهم از سوی بازیگران دولتی و غیردولتی لزوم به‌کارگیری راهبردهای هوشمند امنیتی را برای این زیرساخت‌ها دوچندان کرده‌است.

- ارتقا امنیت زیرساخت‌ها جهت تضمین خدمات‌رسانی حتی در زمان حملات
- ارتقا مقررات و دستورالعمل‌های امنیتی
- ادغام سیستم امنیت اسکادا[۳]/فناوری‌های عملیاتی در امنیت کلی سازمان‌ها/شرکت‌ها
- پایش مستمر روند دیجیتال‌سازی و اکتساب فناوری در سازمان‌ها و ارزیابی وسایل و فناوری‌های امنیتی مورد استفاده جهت تعیین نقاط ضعف و رفع آنها
- به‌کارگیری رویکردهای تخصصی و متناسب با ویژگی‌های بخش‌ها (حمل‌ونقل، صنعت، توزیع برق و غیره) در استفاده از سیستم‌های اسکادا جهت تضمین و ارتقا سطح امنیت در این بخش‌ها
- ترویج فرهنگ امنیت از مرحله طراحی با سرمایه‌گذاری متناسب و تدوین مقررات و دستورالعمل‌های مرتبط
- گسترش نوآوری و ساخت مشترک سیستم‌های امنیت اسکادا با حمایت از

---

[1] Engineering Research and Design

[۲] فناوری عمیق یا deep tech به فناوری‌های لبه پیشرفت مانند هوش مصنوعی و یادگیری ماشینی و غیره گفته می‌شود.

[۳] اسکادا یا Supervisory Control and Data Acquisition (SCADA) سیستم جمع‌آوری داده و کنترل نظارتی صنعتی است که از رایانه‌ها، ارتباط داده شبکه‌ای و رابط کاربری گرافیکی استفاده می‌کند تا فرآیندهای نظارتی دستگاه‌ها و تجهیزات را مدیریت کند.

استارتاپ‌ها و مراکز رشد و فراهم کردن شرایط تجاری‌سازی نتایج تحقیقات مشترک

- تعیین خط مبنای امنیتی برای بخش‌ها و سازمان‌ها و پایش مستمر آن از طریق نظارت بر فناوری‌های مورد استفاده/روش‌های مدیریت امنیت و غیره
- ارتقا مهارت‌های منابع انسانی در زمینه امنیت اسکادا
- توسعه محصولات بیمه سایبری متناسب با خطرات امنیتی محیط‌های اسکادا/فناوری‌های عملیاتی

امنیت پرداخت دیجیتال و تراکنش‌های مالی: دیجیتال‌سازی پرداخت‌ها و مبادلات مالی از مهم‌ترین پیش‌ران‌های دیجیتال‌سازی اقتصاد است. لذا، این امر باید با سرعت و حداکثر امنیت تحقق یابد.

- ترویج نگاشت[1] و مدل‌سازی:
  - زنجیره عرضه پردازش مبادلات
  - وسیله‌ها و بسترهای مورد استفاده
  - نوع نهادهایی که در پردازش مبادلات مشارکت دارند
  - مسیرها و جریان‌های پرداخت
  - تبادل داده و اطلاعات
- ترویج مدل‌سازی تهدیدهای متداول و بزرگ جهت تعیین نقاط ضعف و آسیب پذیری ها
- افزایش هماهنگی مقررات جهت ارتقا کارایی و آمادگی
- ترویج تحقیقات حوزه تهدیدها و به‌اشتراک‌گذاری نتایج آنها
- اجباری نمودن عملیات‌های امنیت سایبری در زنجیره‌های پردازش مبادلات مالی
- ارتقا استانداردها از مرحله انتخاب فناوری تا ارزیابی و نظارت و افزایش سهم هند در تعیین استانداردهای بین‌المللی صنعت پرداخت

[1] Mapping

- توسعه سیستم‌های پاسخ‌گویی به تهدید در بخش تامین مالی

آمادگی بخش‌ها: بخش‌های اقتصادی به‌سرعت در حال دیجیتال‌سازی فرایندها و عملیات‌های خود هستند، اما سطح آمادگی آنها در برابر خطرات ناشی از دیجیتال‌سازی هنوز مناسب نیست.

- تهیه نمایه بخش‌ها شامل نقشه دیجیتال‌سازی/پیشرفت‌های معماری/به‌کارگیری فناوری/نقاط ضعف احتمالی و خطرات آن‌ها جهت تعیین اولویت‌های مداخله
- ارزیابی بخش‌ها و شرکت‌های آن‌ها از نظر نقشی که در زنجیره عرضه دارند جهت شناسایی تهدیدهای امنیت ملی ناشی از حملات سایبری به آنها
- ارتقا مقررات امنیتی در جهت افزایش تناسب آن‌ها با شرایط بخش‌ها
- توجه ویژه به بخش‌های حساس در سیاست‌ها/چهارچوب‌ها/مقررات و استانداردها
- توسعه عملیات‌های امنیت سایبری در شرکت‌ها و تمایز آن‌ها از فعالیت‌های عادی حوزه فناوری اطلاعات
- ارزیابی و سنجش سطح آمادگی بخش‌ها و ایجاد فرهنگ مدیریت خطر
- ارائه مشوق به بخش خصوصی برای فعالیت‌های تحقیقاتی مشترک با مراکز رشد/دانشگاه‌ها و موسسات تحقیقاتی در حوزه امنیت سایبری
- ترویج به‌اشتراک‌گذاری اطلاعات/گزارش رویدادهای خطر در بخش‌های صنعتی.

توسعه متوازن امنیت سایبری در سطح ایالتی: بسیاری از ایالت‌ها اقدامات منسجمی در جهت دیجیتال‌سازی اقتصاد و ارائه خدمات دولتی بر بسترهای دیجیتال در دست اجرا دارند. دیجیتال‌سازی موفق مستلزم فضای امن سایبری است، اما اقدامات حوزه امنیت سایبری بدون سهیم‌شدن ایالت‌ها در راهبردها و برنامه‌های ملی توسعه امنیت فضای سایبری موفقیت چندانی نخواهند داشت.

- تضمین ادغام امنیت سایبری در دستور کار صنعتی‌سازی و دیجیتال‌سازی ایالت‌ها

- ترغیب و تشویق ایالت‌ها به سرمایه‌گذاری در امنیت سایبری از طریق تدوین سیاست‌های ایالتی امنیت سایبری:
  - تخصیص بودجه
  - تعیین نقش‌ها و مسئولیت‌های حوزه امنیت سایبری
  - توسعه زیرساخت‌ها و ظرفیت‌ها
  - ارزیابی و سنجش کارایی برنامه‌های امنیت سایبری
  - تدوین و صدور دستورالعمل‌های لازم برای ارتقا کیفیت عملیات‌ها و حاکمیت در امنیت سایبری
- تهیه سازوکار نظارت و پایش آمادگی و عملکرد ایالت‌ها در امنیت سایبری
- اجرای برنامه‌های توسعه مهارت در سطح ایالتی
- مشارکت در تبدیل هند به قطب جهانی محصولات و خدمات امنیت سایبری از طریق هماهنگ‌سازی همه فعالیت‌های ایالتی

امنیت کسب‌وکارهای کوچک و متوسط: شتاب فزاینده تجارت الکترونیک، دیجیتال‌سازی پرداخت‌ها، ابری‌سازی داده‌ها و استفاده روزافزون از صنایع انقلاب صنعتی چهارم ضرورت تضمین امنیت فضای سایبری برای فعالیت‌های کسب‌وکارهای کوچک و متوسط را بیش از پیش می‌کند.

- ارزیابی بخش‌های مختلف کسب‌وکارهای کوچک و متوسط و نقش آنها در زنجیره عرضه فناوری‌ها از نظر اقتصادی و راهبردی بسیار حائز اهمیت است، زیرا تعیین‌کننده بخش‌های اولویت‌دار و نوع کارهای لازم است.
- پایش دیجیتال‌سازی در این بخش و نظارت بر ابزارها و تجهیزات موردِاستفاده و میزان در معرض خطر بودن آن‌ها
- ترویج اهمیت امنیت سایبری و آگاهی از مصادیق حریم خصوصی در این بخش

- مداخلات سیاستی از قبیل ارائه مشوق‌های تدارکات برای افزایش آمادگی امنیت سایبری
  - یارانه یا گرنت سرمایه‌گذاری در امنیت سایبری
  - ترغیب نهادهای ذی‌ربط به ادغام امنیت سایبری در برنامه‌های توسعه‌ای ایالتی
  - گزارش میزان آمادگی امنیت سایبری و موارد نقض آن
- ارتقای چهارچوب‌ها، مقررات و استانداردهای فنی به‌کارگیری اینترنت اشیاء و صنایع انقلاب صنعتی چهارم جهت افزایش امنیت سایبری/حریم خصوصی و ایمنی
- توسعه فناوری‌های امنیت سایبری ویژه بخش کسب‌وکارهای کوچک و متوسط

فناوری‌های پیشرفته (5G، وایرلس، ابر، اینترنت اشیا، هوش مصنوعی/یادگیری ماشینی، رباتیک، واقعیت افزوده/واقعیت مجازی، سخت‌افزار/شبه‌رساناها، محاسبات کوآنتوم و محاسبات با عملکرد بالا، دفتر کل توزیع‌شده (DLT)[1]، پهپادها، رابط سریال دیجیتال(SDI)[2]، علم مواد): پیشرفت‌های لبه فناوری در بسیاری از حوزه‌ها موجب بروز مسائل امنیتی جدیدی شده‌است که مستلزم رویکرد امنیت سایبری متناسب با شرایط جدید و همواره متغیر کنونی است. لذا، راهبرد ملی امنیت سایبری ۲۰۲۰ که برای دوره ۵ ساله طراحی شده‌است گزینه‌های امنیتی ناشی از فناوری‌های پیشرفته و مرزی را در نظر گرفته‌است.

- سرمایه‌گذاری در پیش‌بینی روند آینده (۱) فناوری‌ها و نقش آنها در شکل‌گیری اجتماع، اقتصاد، صنعت و کسب‌وکارها و ارزیابی اثرات آنها بر امنیت سایبری از نظر:
  - پردازش مبادلات شخصی
  - تعاملات اجتماعی
  - پردازش مبادلات مالی و تجاری

---

[1] Distributed Ledger Technology: دفتر کل توزیع شده در واقع دفتر کلی است که به‌اشتراک گذاشته می‌شود. به بیان دیگر، مانند دفتر کل سنتی سیستمی برای مدیریت و ثبت حساب‌ها است که تفاوت آن با نوع کلاسیک در این است که دفتر کل توزیع شده پایگاه داده‌ای است که در شبکه‌ای گسترده از گره‌ها (node) به‌اشتراک گذاشته می‌شود.

[2] Serial Digital Interface

- تعاملات فرامرزی مانند جریان‌های داده و تجارت

- پیش‌بینی روند آینده (۲) فناوری‌ها از طریق تحقیقات در حوزه‌های:
  - شناخت جامع و ساختارمند وضعیت موجود و نگاشت و دسته‌بندی عناصر آینده و سنجش تهدیدها
  - سنجش پیشرفت‌های کنونی و تحقیقات در دست اجرا که می‌توانند نقشه راه آینده فناوری را ترسیم کنند
- شناخت عوامل و شرایط تعیین‌کننده در تغییرات تبدیل دیجیتال و مطالعه اثرات امنیت سایبری این تغییرات
- پیش‌بینی روند آینده (۳)؛ شناسایی حوزه‌های راهبردی یا متضمن تغییرات بنیادین از طریق:
  - نگاشت فناوری‌ها و ظرفیت‌های موثر کنونی
  - ارزیابی نقش ظرفیت‌های فناورانه در زنجیره عرضه خطوط کلیدی تولید (سنجش سهم هند در این زنجیره)
  - شناسایی حوزه‌های مهم زنجیره عرضه از نظر امنیت سایبری
- فراهم کردن شرایط زیرساختی و نهادی لازم برای ارزیابی امنیتی فناوری‌ها/تجهیزات/بسترها
- مشارکت فعال در تهیه استانداردهای لازم برای فناوری‌های جدید
- سرمایه‌گذاری در تحقیقات نهادی و استارتاپ‌ها در حوزه‌های حیاتی فناوری و با تاکید ویژه بر امنیت سایبری
- تهیه دستورالعمل‌های شناسایی و ارزیابی مسائل امنیت سایبری و نوع مداخلات موردنیاز
- تامین سرمایه خطرپذیر برای توسعه ظرفیت‌های مهم امنیت سایبری با تاکید بر حل

مسائل تبدیل فناورانه

- توسعه مهارت‌ها و تخصص‌های کلیدی برای مسائل پیچیده امنیت سایبری در حوزه‌های جدید فناوری

۲) تقویت

ساختار، نهادها و حاکمیت: چالش‌های ناشی از تحول فناوری‌ها، دیجیتال‌سازی گسترده و تهدیدهای سایبریِ پیش‌رو، نیازمند توجه ویژه به ساختارها، نهادها و نحوه حمکرانی بر کشوری در مقیاس هند است. اولویت‌های این حوزه عبارتند از:

- کاهش تهدیدهای سایبری اثرگذار بر روند پیشرفت به‌سوی هدف اقتصاد یک تریلیون دلاری
- برنامه‌ها و ابتکارعمل‌های ملی جهت تقویت آمادگی، افزایش قدرت دفاعی و توان پاسخگویی سریع به تهدیدها
- افزایش هم‌افزایی و هماهنگی بین کارکردها و مسئولیت‌های نهادهای مختلف و همسوسازی آنها با راهبرد و سند ملی اجرایی
- سنجش آمادگی در سطح ملی، ایالتی و بخشی و سازماندهی همه فعالیت‌های این حوزه جهت افزایش سطح آمادگی ملی سایبری
- هدایت همه منابع به‌سوی منافع اقتصادی و ژئوپلیتیک و دستورِ کار رشد کشور و تبدیل هند به الگوی دفاع و پاسخ سایبری
- احیای «دستور کار نوآوری امنیت سایبری» و «راهبرد تحقیق و توسعه» کشور جهت تقویت مشارکت‌های دولت-صنعت-دانشگاه به‌منظور دستیابی به اهداف مدنظر راهبرد ملی امنیت سایبری
- توسعه تحقیقات حقوقی و خطِ مشی در حوزه پیشرفت‌های آینده فناوری و اثرات آن

بر اجتماع و اقتصاد و خطرات سایبری بالقوه به‌منظور در خدمت گرفتن فناوری‌های جدید برای منافع مردم

- هماهنگ‌سازی همه فعالیت‌های دولت در توافق‌های همکاری سایبری دوجانبه، چندجانبه و منطقه‌ای و مشارکت در مجامع جهانی همسو با منافع موردِنظر هند در حوزه فضای سایبری و امنیت

تامین بودجه: با توجه به اهمیت امنیت سایبری برای امنیت ملی ضرورت دارد بودجه مستقلی برای آن تعریف شود.

- با یکپارچه‌سازی بودجه‌های سازمان‌ها و وزارت‌های مختلف برای امنیت سایبری باید در سبد بودجه کشور ردیف مجزایی به این حوزه تخصیص یابد. حدود ۰/۲۵ درصد کل بودجه کشور می‌تواند به ردیف بودجه امنیت سایبری اختصاص یابد و در آینده با دستیابی به اقتصاد ۵ تریلیون دلاری این ردیف تا ۱ درصد می‌تواند افزایش یابد.
- با توجه به سطح کنونی آمادگی و روند فزاینده تهدیدها بهتر است همه وزارت‌ها و نهادها ۱۵ تا ۲۰ درصد مخارج فناوری اطلاعات/فناوری خود را به امنیت سایبری تخصیص دهند.
- تخصیص بودجه باید متناسب با نتایج مورد انتظار باشد و سازوکار مناسب جهت سنجش این موضوع ایجاد شود.

تحقیقات، نوآوری و توسعه فناوری: اقدامات هماهنگ در حوزه تقویت تحقیقات، نوآوری و توسعه فناوری و به‌ویژه تجاری‌سازی نتایج تحقیقات در تامین منافع راهبردی و تجاری کشور بسیار حائز اهمیت است.

- سرمایه‌گذاری کلان در فناوری اطلاعات و ارتباطات، مدرن‌سازی و دیجیتال‌سازی به‌منظور تحریک توسعه فناوری‌های امنیت سایبری

- شناسایی موارد جدید کاربرد امنیت سایبری و توسعه فناوری‌ها متناسب با آن‌ها
- هدایت سرمایه‌گذاری‌های تحقیق و توسعه امنیت سایبری در جهت تولید محصول/ خدمات و تجاری‌سازی آنها با ایجاد پیوند با صنعت و برنامه‌های حمایتی منسجم و جامع
- تدوین دستور کار کوتاه‌مدت و بلندمدت تحقیقات امنیت سایبری از طریق برنامه‌های نتیجه‌محور و حمایت از تحقیقات آینده‌نگر جهت تعیین و شناسایی اولویت‌های پژوهشی
- تخصیص بودجه به حوزه‌های اولویت‌دار تحقیقات
- تشویق صنایع به همکاری با دانشگاه و استارتاپ‌ها در توسعه فناوری‌های امنیت سایبری و حمایت از صنایع در تبدیل نتایج تحقیقات با بودجه دولتی به محصول/ خدمات و تجاری‌سازی آن‌ها
- ایجاد محیطی مولد برای کارآفرینی امنیت سایبری از طریق حمایت از مراکز رشد، تامین سرمایه خطرپذیر برای نوآوری در امنیت سایبری فناوری‌های عمیق
- ایجاد فراصندوق[1] امنیت سایبری
- ایجاد بازاری پویا و سالم برای محصولات نوآورانه امنیت سایبری با کاهش خطرات فعالیت استارتاپ‌ها
- اصلاح فرایند تدارک دولتی به‌منظور افزایش مشارکت استارتاپ‌ها در تدارک محصولات امنیت سایبری
- جذب سرمایه به تحقیق و توسعه امنیت سایبری و افزایش حضور کشور در بازارهای سرمایه جهانی
- سرمایه‌گذاری در پرورش مهارت‌های موردنیاز تحقیق و توسعه امنیت سایبری و ترویج ایده‌سازی نوآورانه با محوریت فناوری امنیتی از طریق برنامه‌های تخصصی

[1] Fund of Funds : نوعی نهاد مالی که به‌جای سرمایه‌گذاری مستقیم در اوراق قرضه، سهام، کسب‌وکارها و غیره، روی صندوق‌هایی سرمایه‌گذاری می‌کند که ترکیبی از سبد دارایی سرمایه‌گذاری‌های مختلف هستند.

- هدایت فعالیت‌های محققان، استارتاپ‌ها و شرکت‌های حوزه امنیت سایبری به نیازهای ملی و منطقه‌ای کشور

توانمندسازی و مهارت‌افزایی: هند در پرورش مهارت‌های امنیت سایبری پیشتاز است و لذا راهبرد مهارت کشور باید ضمن حفظ این موقعیت موجب ارتقا همه‌جانبه آن نیز شود.

- تهیه چهارچوبی جامع و ملی برای اجرای برنامه‌های ارتقا مهارت بازارمحور، صدور گواهی‌های حرفه‌ای جهانی و مداخلات نهادی مانند آگاهی و آموزش امنیت اطلاعات (ISEA)[1]
- فراهم کردن زیرساخت‌های مناسب برای توسعه مهارت‌های امنیت سایبری از طریق ارائه مشوق به فعالان بخش رسمی و غیررسمی برای مشارکت در توسعه زیرساخت‌ها
- ایجاد مرکز عالی توسعه ظرفیت و مهارت‌های امنیت سایبری
- تاکید بر ادغام امنیت سایبری در برنامه‌های کلان بازآموزی و ارتقا مهارت
- اقدامات هماهنگ در راستای مهارت‌افزایی مانند برگزاری مسابقات هکاتون[2]، برگزاری کارگاه‌های حضوری و عملی و تمرکز بر جنبه‌های توسعه فناوری
- برنامه‌های ویژه برای ارتقا ظرفیت‌های شرکت‌های بخش دولتی با تمرکز ویژه بر فناوری، عملیات‌ها، حاکمیت و رهبری
- برگزاری آزمون خدمات امنیت سایبری برای استخدام بهترین نیروی انسانی در شرکت‌های دولتی
- تشویق و ترغیب استعدادهای جوان به تحصیل در رشته امنیت سایبری و فراهم کردن فرصت‌های شغلی برای آن‌ها. اجرای برنامه‌های ملی برای انتقال فارغ‌التحصیلان

---

[1] Information Security Education and Awareness

[2] هکاتون یا Hackathon رویدادی است که در آن برنامه‌نویسان رایانه و سایر متخصصان این حوزه مانند طراحان گرافیکی، طراحان واسط کاربری و مدیران پروژه گردهم می‌آیند و در توسعه پروژه‌های نرم‌افزاری و گاهی سخت‌افزاری با یکدیگر همکاری می‌کنند. این رویداد ممکن است صرفا جنبه آموزشی داشته باشد و یا به‌صورت رقابت برگزار شود.

مقطع کارشناسی و ارشد در رشته‌های علوم غیرکامپیوتر به‌ویژه الکترونیک و ریاضی به گرایش امنیت سایبری

- پایش دقیق شکاف عرضه و تقاضا در حوزه امنیت سایبری از طریق مطالعات و تحقیقات علمی و انجام اقدامات لازم برای از بین بردن این شکاف

بازرسی و ارزیابی: با توجه به گستردگی دامنه و شتاب سریع و پیچیدگی بالای تغییرات حوزه فناوری‌های دیجیتال و تهدیدهای سایبری لازم است اقدامات مرتبط با بازرسی و ارزیابی نیز متناسب با شرایط مورد بازبینی و اصلاح قرار گیرند.

- اعمال رویکردی دقیق‌تر در توسعه محیط بازرسی و سنجش به‌منظور ارتقا فرایند انتخاب بازرس/ارزیاب
  - تدوین استانداردهای ارزیابی یا معیارهای بازرسی دقیق‌تر و جزئی‌تر به‌نحوی که همه جنبه‌های موضوع پوشش داده شود.
  - انتخاب افراد کاملا مجرب برای پروژه‌های بازرسی و ارزیابی
  - فرایند ارزیابی، بازرسی و سنجش باید کاملا مستند و مبتنی بر اطلاعات باشد تا میزان آمادگی در برابر تهدیدها و آسیب‌پذیری‌ها به‌طور دقیق تعیین شود.
  - ترویج بازرسی مستمر و مداوم به‌جای بازرسی یک‌باره و دفعی
  - حمایت از به‌کارگیریِ فناوری برای پایش آمادگی، بهبود خط مبنای امنیت سایبری و تعیین میزان خطر
  - رصد دقیق فناوری‌ها و ابزارهای جدید برای ارزیابی و بازرسی
- اصلاح مقررات و ظرفیت‌های حقوقی به‌منظور افزایش دامنه بازرسی و ارزیابی برای پوشش دادن حوزه‌های نوظهور در تهدیدهای سایبری

مدیریت حادثه و بحران: علم، نوآوری فرایند و فناوری در شناسایی پیشگیرانه و مدیریت به‌موقع حوادث و بحران‌های ناشی از آن‌ها می‌توانند بسیار موثر باشند.

- ارتقا اقدامات حوزه شناسایی و ثبت تهدیدها و حوادث محتمل و اولویت‌بندی آن‌ها از نظر میزان اثرات و عواقب
- حمایت از برنامه‌ریزی برای مدیریت حوادث و بحران‌های احتمالی و تعیین نقش‌ها و مسئولیت‌های مرتبط
- اجرای اقدامات حوزه برنامه‌ریزی حوادث و شبیه‌سازی موقعیت‌ها
  - گسترش دامنه تمرینات امنیت سایبری به‌منظور شمول موقعیت‌های واقعی
  - ارتقای اقدامات شناسایی تهدیدهای دارای بیشترین اثر در شرکت‌ها که مقابله با آن‌ها مستلزم برنامه‌های ملی است.
  - اجرای برنامه‌های شبیه‌سازی برای بخش‌های حساس در سطح شرکت‌ها، صنایع و سطح ملی
  - اجرای برنامه‌های شبیه‌سازی بین کشوری برای تهدیدهای فرامرزی
- بهره‌برداری از دانش به‌دست آمده از حوادث گذشته در مدیریت موثر حوادث پیشِ‌رو
- ترویج استفاده از سازوکارهای جدید به‌اشتراک‌گذاری اطلاعات، جمع‌آوری اطلاعات تهدیدها، عملیات‌های شکار (شناسایی) تهدید، تحقیقات امنیت سایبری جهت تعیین نقاط ضعف احتمالی و رفع آن‌ها
- ترویج مشارکت در برنامه‌ها و ابتکارعمل‌های جهانی دسته‌بندی حوادث، یافتن شاخص‌های خطر و شاخص‌های حمله (**IOC and IOA**)[1] در حملات جدید و پیشنهاد مراحل مقابله

امنیت داده و حکمرانی: بنیان دیجیتال‌سازی بر محصولات و خدمات داده‌محور استوار است، لذا راهبرد ملی امنیت سایبری باید ارتقای حاکمیت داده را مدنظر داشته باشد و امنیت داده‌ها را نظام‌مند نماید.

[1] Indicators of Compromise and Indicators of Attack

- ترویج آن دسته از روش‌های حاکمیت داده که مبتنی بر اصولی مانند کشف، ملموس‌بودن، دسته‌بندی و خطرمحور بودن هستند.
- ترغیب نهادهای دولتی و بخش‌های عمومی به استفاده از روش‌های جدید حاکمیت داده
- تاکید بر رویکرد داده‌محوری در همه مراحل برنامه‌ریزی، طراحی، به‌کارگیری و عملیات‌ها

۳) هم‌افزایی

زیرساخت‌های اینترنت: صنعت فناوری اطلاعات هند در سال مالی ۲۰۱۹ ارزشی معادل ۱۸۱ میلیارد دلار داشت و انتظار می‌رود تا ۲۰۲۵ این رقم به ۳۵۰ میلیارد دلار افزایش یابد. بنابراین رویکرد هند در راهبرد ملی امنیت سایبری نسبت به صنعت فناوری اطلاعات باید متناسب با این واقعیت اقتصادی باشد.

- مشارکت فعال در ابتکارعمل‌های حوزه تعیین هنجارهای سایبری، حاکمیت فضای سایبری و تنظیم و کنترل جریان‌های داده
- سرمایه‌گذاری مناسب در تحقیقات جهت پیشبرد اهداف هند در عرصه‌های دیپلماتیک شکل‌دهنده فضای سایبری جهانی
- تسهیل مشارکت ذینفعان و شمول همه ابعاد و جنبه‌های مهم در ساخت افق ملی
- افزایش حضور ذینفعان مختلف از داخل و خارج مرزها در ابتکارعمل‌های چندبعدی مانند ساخت ظرفیت داخلی به‌منظور تقویت زیرساخت‌ها و آوردن سرور اصلی[1] به داخل کشور

تدوین استانداردها: تاکنون بیشترین سهم هند در استانداردهای بین‌المللی امنیت سایبری در زمینه به‌کارگیری استانداردها و یا در تهیه استانداردهای مدیریتی و اجرایی

[1] Root Server

بوده‌است. با توجه به اینکه مدیریت مسائل امنیتی روزبه‌روز بیشتر وابسته به فناوری می‌شود و نیز نوآوری‌های فناورانه با روندی شتابان رو به پیشرفت هستند، ضرورت دارد هند در تهیه و تدوین استانداردهای فنی مشارکت فعال داشته باشد.

- افزایش آگاهی نسبت به اهمیت مشارکت در تدوین استانداردهای فناوری و تشویق استعدادها به فعالیت در این حوزه
- ارتقای فعالیت‌های حوزه مهارت‌افزایی برای تدوین استانداردهای امنیتی و فناوری‌های اساسی
- تشویق افراد، نهادها و شرکت‌ها به مشارکت در تدوین استانداردها
- رصد دقیق فعالیت‌های جهانی حوزه تدوین استاندارد و نهادها و موسسات سهیم در آن جهت شناسایی استانداردهای حائز اهمیت برای اقتصاد و منافع کشور
- توسعه ظرفیت نهادهای موجود یا ایجاد سازوکارهای نهادی جدید برای افزایش مشارکت هند در تدوین استانداردها

بیمه سایبری: بیمه سایبری یکی از ابزارهای کلیدی در مدیریت خطر سایبری است که انتظار می‌رود ارزش بازار جهانی آن از ۴/۲ میلیارد دلار در سال ۲۰۱۷ به ۲۲/۴ میلیارد دلار در سال ۲۰۲۴ افزایش یابد. لذا، هند باید با اجرای اقدامات منسجم و هماهنگ سهم خود را در این بازار افزایش دهد.

- افزایش آگاهی نسبت به بیمه سایبری در همه بخش‌های اقتصاد
- حمایت از توسعه علوم اکچوئری[1] به‌منظور محاسبه و پیش‌بینی خطرات پیچیده امنیت سایبری در بخش‌های صنعت، کسب‌وکار، فناوری‌ها و غیره.
- مشاوره با ذینفعانی مانند مالکان و اپراتورهای زیرساخت‌ها، بیمه‌گران و مدیران ارشد امنیت اطلاعات و مدیران خطر

[1] Actuarial Science: اکچوئری یک سری علم محاسباتی است که در بانک‌ها و موسسات بیمه‌ای و اعتباری کاربرد دارد، بنابراین علم اکچوئری مرجع اساسی جهت فعالیت‌های مالی محسوب می‌شود و نوعی روش محاسبه خطر به‌کمک علوم ریاضی و آمار است که در صنعت بیمه، تامین مالی، تجارت و غیره استفاده می‌شود.

- حمایت از توسعه گنجینه اطلاعات حوادث سایبری و به‌اشتراک‌گذاری این اطلاعات به‌منظور تقویت عملیات‌های علوم اکچوئری
- حمایت از پرورش استعداد و تخصص در حوزه‌های مدیریت خطر، علوم اکچوئری سایبری و تحقیقات و بازرسی‌های جرم‌شناسی
- حمایت از ساخت محصولات بیمه سایبری برای زیرساخت‌های مهم اطلاعاتی مانند بسترهای اسکادا/عملیات‌های فناوری و بخش کسب‌وکارهای کوچک و متوسط
- حمایت از رشد بازار بیمه سایبری و پایش مستمر آن

برند هند: نظر به سابقه طولانی هند در عرضه خدمات فناوری اطلاعات، اقدامات فراگیر این کشور در دیجیتال‌سازی اقتصاد داخلی، صادرات فزاینده خدمات امنیتِ سایبری، افزایش تعداد استارتاپ‌های امنیتِ سایبری و اشتیاق جهانی به انتخاب هند به‌عنوان مرکز عملیات‌های مهندسی، این کشور یکی از بازیگران مهم عرصه امنیت سایبری دنیا محسوب می‌شود. حفظ و ارتقای این موقعیت مستلزم اقدامات راهبردی در سطح ملی و جهانی است.

- طراحی اهداف برندسازی و اقدامات ارتقا موقعیت کشور:
  - جذب و پرورش استعداد در رشته‌های امنیت سایبری مستلزم تفکرِ عمیق
  - حمایت از پژوهش، نوآوری، کارآفرینی و سرمایه‌گذاری امنیت سایبری
  - تبدیل هند به مرکز پژوهش و تولید محصولات امنیت سایبری و جذب سرمایه
  - نمایش و عرضه توانمندی‌های هند در عرصه امنیت سایبری
- رصد دقیق توانمندی‌ها، ظرفیت‌ها، محصولات/خدمات ارزشمند، نوآوری‌ها و نمونه‌های موفق حوزه امنیت سایبری
- افزودن دستور کار امنیت سایبری به برنامه‌ها و ابتکارعمل‌های کنونی در حوزه برند هند
- ایجاد دستور کار امنیت سایبری در نمایندگی‌ها/سفارت‌های هند در سایر کشورها و

نهادهـای بین‌المللـی

دیپلماسـی سـایبری: بـا حمایت‌هـای مسـتمر و منظـم پیشـتازی هنـد در حاکمیـت جهانـی فضـای سـایبری بایـد محقـق شـود.

- تاکیـد بـر نقـاط قـوت هنـد ماننـد داشـتن دومیـن جمعیـت بـزرگ کاربـران اینترنـت، قطـب جهانـی فنـاوری، سـومین اکوسیسـتم بـزرگ اسـتارتاپ، مقصـد جهانـی تحقیـق و توسـعه، پیشـتاز در پـرورش مهارت‌هـا، تجـارب موفـق در دیجیتال‌سـازی و بـازار پویـای محصـولات و خدمـات دیجیتـال
- جـذب سـرمایه‌گذاری و تولیـد محصـولات جهانـی امنیـت سـایبری بـه هنـد، جـذب سـرمایه‌های داخلـی به‌سـمت امنیـت سـایبری، جـذب تحقیـق و توسـعه جهانـی حـوزه امنیـت سـایبری بـه هنـد
- ارتقای آمادگی امنیت سایبری مناطق کلیدی (از نظر اهمیت اقتصادی) کشور
- تقویت همکاری و مشارکت بین دولت، صنعت و دانشگاه
- حمایـت و تشـویق مشـارکت فعـال در فرایندهـای تدویـن اسـتاندارد جهانـی به‌ویـژه در زمینـه اسـتانداردهای فنـی
- ایفای نقش نماینده/فرستاده سایبری برای کشورها و مناطق کلیدی

تفحـص در زمینـه جرایـم سـایبری: بـا توجـه بـه نقـش فزاینـده فنـاوری در ارتـکاب و شناسـایی جرایـم، تحقیـق و تفحـص دربـاره جرایـم سـایبری بـا اسـتفاده از فناوری‌هـای پیشـرفته ماننـد فناوری‌هـای جرم‌شناسـی دیجیتـال بایـد از حوزه‌هـای کلیـدی راهبـرد ملـی دیجیتـال باشـد.

- اصلاحات قانونی: بسیج همه منابع و نیروها جهت اصلاح شکاف‌های قانونی
  - شناسـایی و توجـه بـه حوزه‌هـای حائـز اهمیتـی ماننـد اخبـار جعلـی و ایمیل‌هـای مزاحـم (اسـپم) [1]

[1] Spam

- تهیه نقشه‌راهی برای دستور کار پنج‌ساله آینده که همه موارد احتمالی تبدیل فناورانه را پوشش دهد
- حمایت از گردآوری و توزیع موثر و به‌موقع اطلاعات، داده‌ها و گزارش‌های مربوط به پرونده‌های جرایم سایبری، الگوها و روش‌های ارتکاب جرم
- ایجاد دادگاه‌های ویژه جرایم سایبری جهت تسریع در رسیدگی به امور
- حمایت از ارتقای ظرفیت‌ها و مهارت‌های مقامات، دادستان‌ها و قضات در سطح وسیع
- ارائه مشوق به اقدامات و برنامه‌های حوزه پرورش استعدادهای جرم‌شناسی پیشرفته و ارتقای ظرفیت‌های تفحص و تحقیقات موردنیاز مسائل هوش مصنوعی/یادگیری ماشینی، بلاک‌چین، اینترنت اشیا و سایر فناوری‌های عمیق
- حمایت از توسعه فناوری‌های جدید تفحص و تحقیق درباره جرم
- تهیه شاخص آمادگی تفحص درباره امنیت سایبری ایالت‌ها با در نظرگرفتن مواردی از قبیل میزان سرمایه‌گذاری، دامنه فعالیت‌ها، سطح به‌هنگام بودن پاسخ به مسائل و میزان بهبود نرخ ارتکاب جرم
- ترغیب سازمان‌های دولتی به ایجاد تیم‌های پاسخگویی به نقض امنیت سایبری/ جرایم سایبری
- رصد دقیق گروه‌های خاصی از جرایم سایبری که به نظم عمومی، منافع اقتصادی و سلامت فضای سایبری آسیب وارد می‌کنند.
- به‌کارگیری سازوکارهای موثر برای ارتقای همکاری و هماهنگی بین ایالتی در حل مسائل امنیت سایبری
- ترغیب مشارکت با نهادهای مجری قانون در خارج از کشور برای تبادل اطلاعاتی و همکاری فعال با نهادهای بین‌المللی در پاسخ به جرایم امنیت سایبری بین‌المللی

- ایجاد یک گروه ویژه از بازرسان جرایم سایبری در نهاد مجری قانون
- پیشنهاد ایجاد سیستمی الکترونیک در سطح بین‌المللی برای درخواست کمک و مدیریت و پاسخگویی به درخواست‌ها تحت پیمان حقوقی دوجانبه (MLAT)[1] که هند امضا کرده‌است.

منبع

https://www.dsci.in/sites/default/files/documents/resource_centre/National%20Cyber%20Security%20Strategy%202020%20DSCI%20submission.pdf

[1] Mutual Legal Assistance Treaty

مؤسسه پویندگان توسعه فناوری و نوآوری ایرانیان